



ORACLE

Oracle ECB and SBC interworking with MS
Teams and Multi-vendor IP-PBX Environment

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 ECB and SBC interworking with MS Teams and Multi-vendor IP-PBX Environment	25 th October 2021
1.1	Minor changes w.r.t formatting	12 th November 2021
1.2	Removed reference to sip-all FQDN from the app note document	10 th January 2022
1.3	Since sip-all FQDN is removed, add the following two sections: Enable refer call xfer on realm	22 nd July 2022



Table of Contents

1. INTENDED AUDIENCE	4
2. DOCUMENT OVERVIEW	4
3. INTRODUCTION	5
3.1. AUDIENCE	5
3.2. REQUIREMENTS.....	5
3.3. ARCHITECTURE	6
4. NEW ECB CONFIGURATION	6
4.1. ECB CLI INITIAL CONFIG	7
4.2 LOGGING INTO THE ECB	9
4.3. ADD NETWORK SETTINGS.....	11
4.4. CONFIGURE SIP INTERFACE	11
4.5. CONFIGURING THE AGENTS	12
4.6. ECB WITH LDAP CONFIGURATION	14
4.7. ECB PARALLEL FORKING WITH LDAP CONFIGURATION	22
4.8. ECB PARALLEL FORKING WITH ADDITIONAL TARGET GROUP (ATG) CONFIGURATION	25
5. CONFIGURING THE SBC	30
5.1. VALIDATED ORACLE SBC VERSION.....	30
6. NEW SBC CONFIGURATION	30
6.1. ESTABLISHING A SERIAL CONNECTION TO THE SBC.....	30
6.2. CONFIGURE SBC USING WEB GUI	34
6.3. CONFIGURE SYSTEM-CONFIG	36
6.4. CONFIGURE PHYSICAL INTERFACE VALUES	37
6.5. CONFIGURE NETWORK INTERFACE VALUES.....	38
6.6. ENABLE MEDIA MANAGER	40
6.7. CONFIGURE REALMS.....	41
6.8. ENABLE SIP-CONFIG	43
6.9. CONFIGURE SIP INTERFACES	44
6.10. CONFIGURE SESSION-AGENT	45
6.11. CONFIGURE LOCAL-POLICY.....	47
6.12. CONFIGURE STEERING-POOL.....	49
7. EXISTING SBC CONFIGURATION	50
8. VERIFICATION OF SAMPLE CALL FLOWS	51
APPENDIX A	55



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) and Oracle Enterprise Communication Broker (ECB). It is assumed that the reader is familiar with basic operations of the Oracle Enterprise Communication Broker platform along with Oracle Enterprise Session border controller platform along with on premise IP-PBX and MS Teams

2. Document Overview

This Oracle technical application note outlines how to use the Oracle ECB features to interwork between on premise IP-PBX and MS Teams. The solution contained within this document has been tested using Oracle Communication SBC with **software version 840p7** version and Oracle Communication ECB **with software version 330p1**.

This application note has been tested with **Oracle ECB and SBC with Microsoft Teams Media Bypass - Enterprise Model with Local Media Optimization (LMO) enabled**. There are other models of MS teams like Oracle ESBC with Microsoft Teams Media Bypass - Enterprise Model, Oracle SBC with Microsoft Teams Carrier Model, Oracle ESBC with Microsoft Teams Non Media Bypass - Enterprise Model, Oracle SBC with Microsoft Teams Survivable Branch Appliance (SBA) and Integration of Oracle SBC with Analog Devices and Microsoft Teams Direct Routing which customers can use based on their needs and the reference to these models can be found in the below link under “Microsoft Teams” Section.

<https://www.oracle.com/technical-resources/documentation/acme-packet.html>

In addition, it should be noted that the ECB configuration provided in this guide focuses strictly on the on premise IP- PBX and MS Teams. Many ECB and 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 note that the IP address, FQDN and config name and its details given in this document is used as reference purpose only. The same details cannot be used in customer config and the end users can use the configuration details according to their network requirements. Also, the configuration of on premise IP-PBX and MS teams are out of scope of this document. 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.

Please refer the below app notes given as an example for other configuration which is not covered on this app note for on premise PBX (CUCM/Avaya/Genesys) / MS Teams with Oracle SBC/ECB.

The actual config may differ somewhat but these docs can be only used as a reference.

<https://www.oracle.com/a/otn/docs/avaya-with-ms-teams-integration-with-verizon-trunk.pdf>

<https://www.oracle.com/a/otn/docs/ms-teams--sbc-ecb-with-cucm-integration-v1.1.pdf>

<https://www.oracle.com/a/otn/docs/avaya-remote-worker-with-tls.pdf>

https://www.oracle.com/a/otn/docs/oracle_sbc_with_genesys_sip_server_remote_worker.pdf



3. Introduction

3.1. Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring Oracle ECB specific features with Oracle SBC interworking with on premise IP-PBX and MS Teams. There will be steps that require navigating the ECB GUI interface and 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.

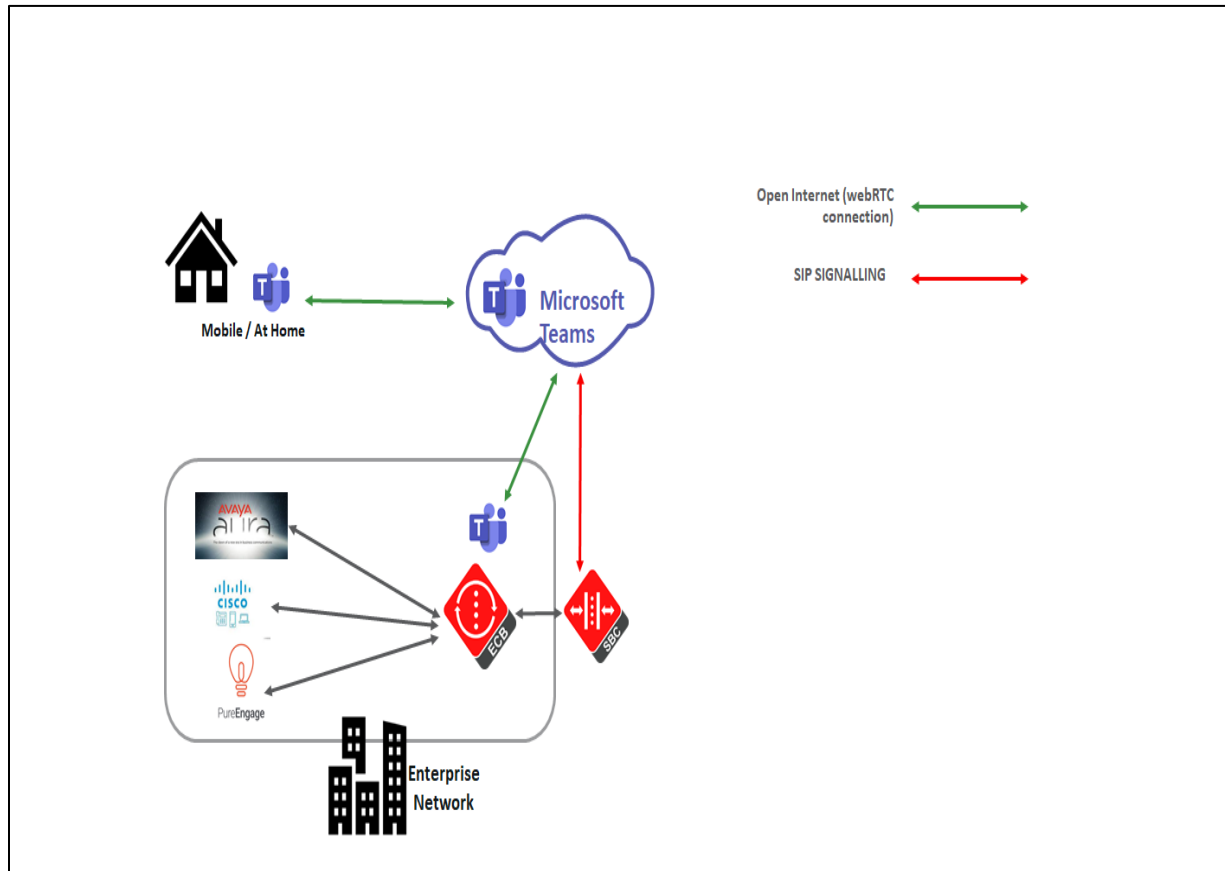
3.2. Requirements

- Oracle Enterprise Session Border Controller (hereafter Oracle SBC) running 8.4.0 version
- Oracle Enterprise Communication Broker (hereafter Oracle ECB) running 3.3.0 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	ECB Version
Revision 1	8.4.0	3.3.0

3.3. Architecture



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

- Phase 1 – Configuring the Oracle ECB.
- Phase 2 – Configuring the Oracle SBC.

4. New ECB Configuration

The Oracle ECB is available either as an appliance or as an application for operation on virtual machines. When running as an appliance, the Oracle ECB software is packaged with the Netra Server X3-2 and delivered to the end customers. When running as a virtual application, the Oracle ECB software can be deployed on any third-party COTS hardware that meets the specified guidelines.

Once the ECB is deployed (in the appliance mode or the application mode) and connected, you can power on the ECB. Software installation of the ECB is required upon first startup. Although the Oracle ECB is primarily configured through the GUI, you need to perform the software installation and certain steps via the CLI. For our testing, we will first configure certain common configuration and we will do some feature specific configuration after that specific to our testing.

4.1. ECB CLI initial config

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

The default username for the User level is “user” and the default password is “acme”.

The default username for an Administrator level is “admin”, and the default 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 ECB by setting the IP address in bootparam

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

Note: There is no management IP configured by default.

```
LabECB#
LabECB# conf t
LabECB(configure)# bootparam

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

Boot File       : /boot/nnPCZ330p1.bz
IP Address      : 10.138.194.175
VLAN            :
Netmask         : 255.255.255.192
Gateway        : 10.138.194.129
IPv6 Address    :
IPv6 Gateway    :
Host IP        :
FTP username    :
FTP password    :
Flags          :
Target Name     : LabECB
Console Device  : VGA
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.

LabECB(configure)#
LabECB(configure)#
```

Setup product type to Enterprise Communication broker as shown below.

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

```
LabECB#
LabECB#
LabECB# setup product

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

Last Modified 2017-02-03 09:44:20
-----
 1 : Product          : Enterprise Communication Broker

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

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

Save the changes and reboot the ECB.

```
LabECB#
LabECB# show entile
LabECB# show entil
LabECB# show entitlements
Provisioned Entitlements:
-----
Enterprise Communication Broker Base      : enabled
Session Capacity                          : 10000

Keyed (Licensed) Entitlements
-----

LabECB#
```


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

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

```
LabECB(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
  last-modified-by    @
  last-modified-date  2021-09-16 21:07:32

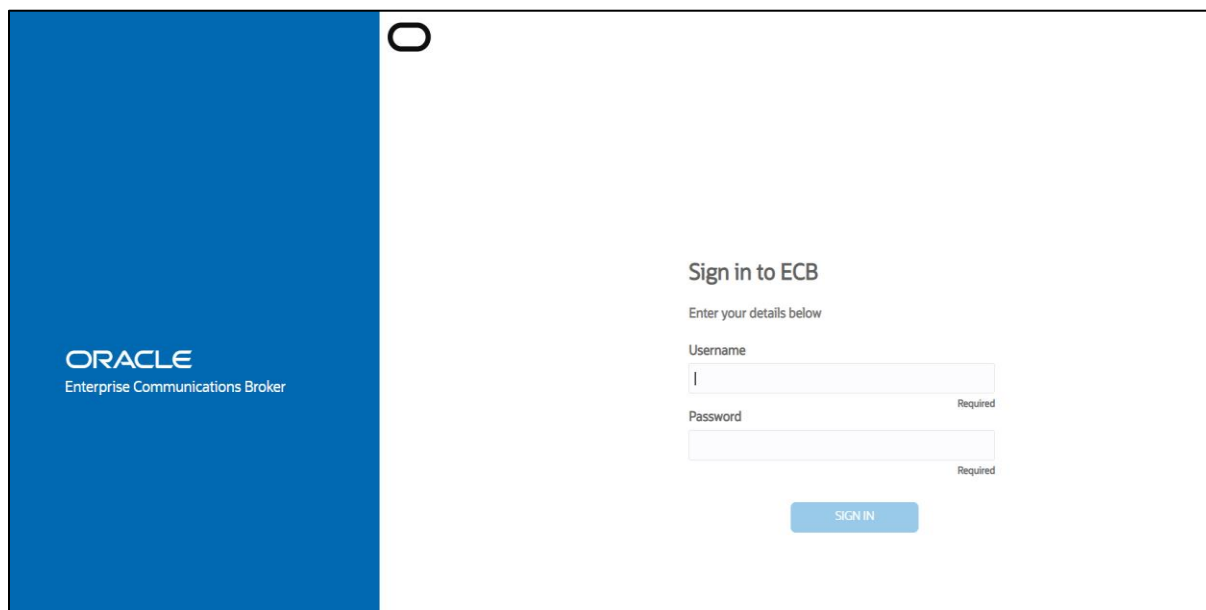
LabECB(http-server) #
LabECB(http-server) #
LabECB(http-server) #
```

4.2 Logging into the ECB

You can now access the ECB through the Web GUI.

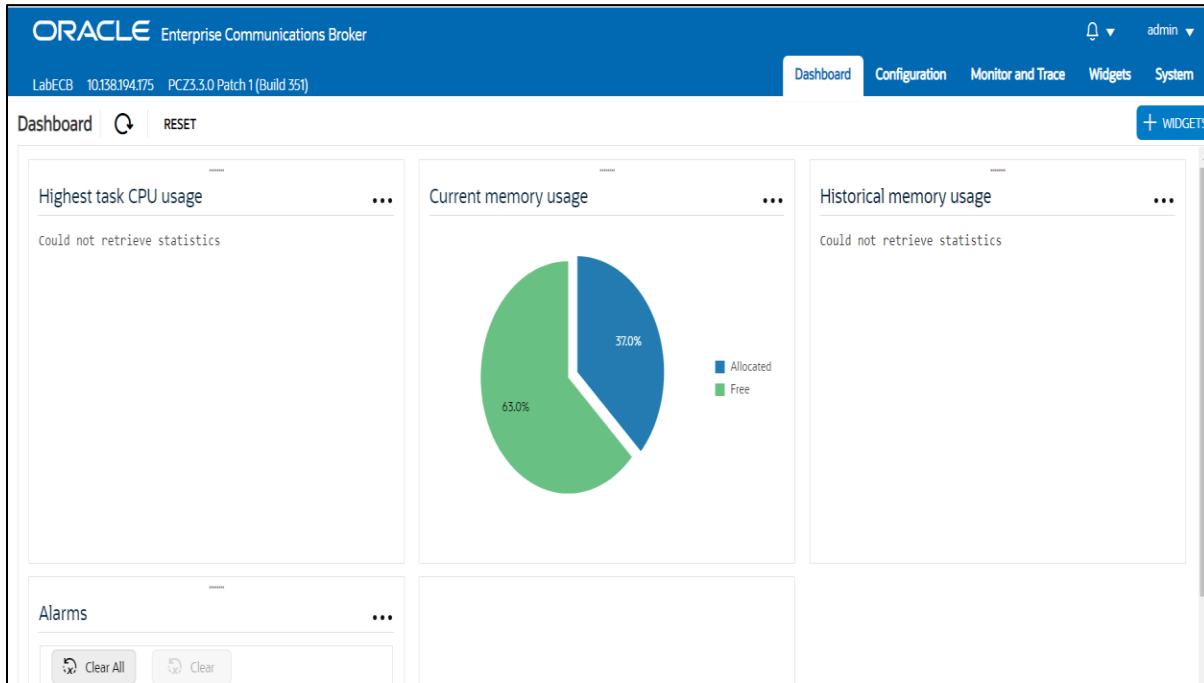
Start an Internet browser and start the GUI using the URL: http://server IP address/.

The login screen will appear.

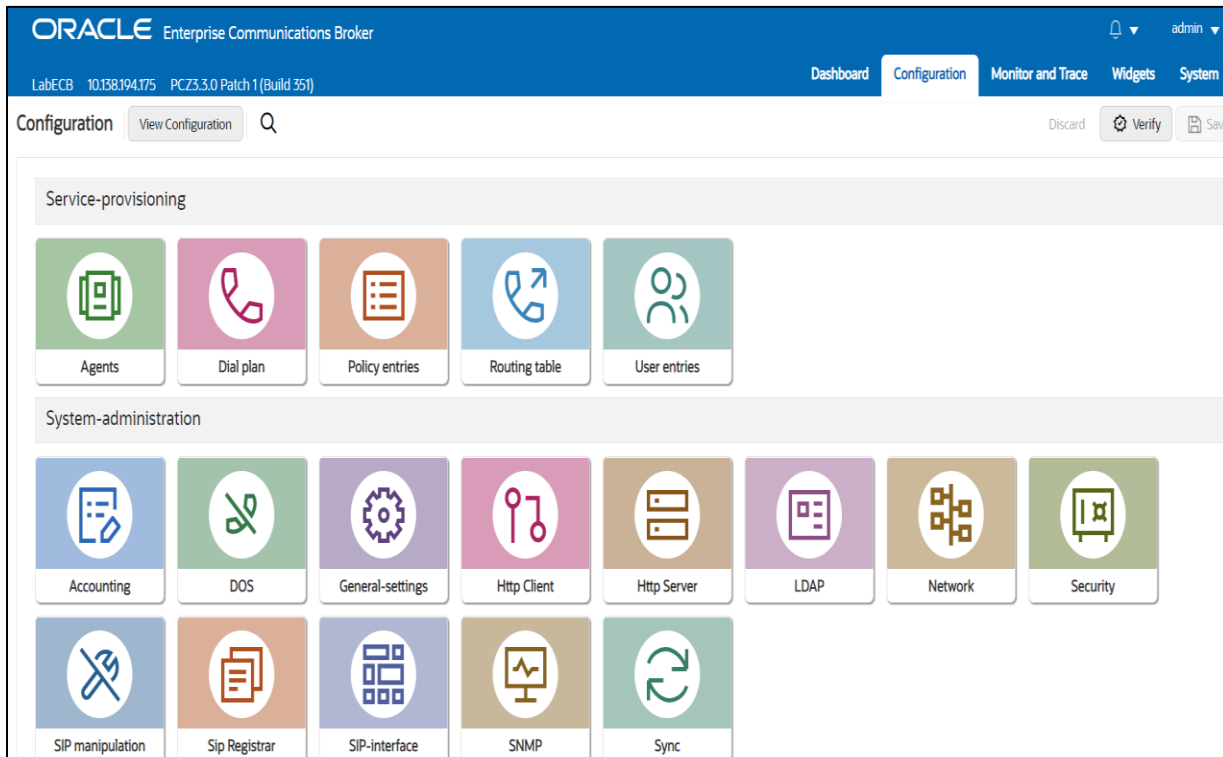


Enter the username and password and this is same as CLI username & password.

After logging into the ECB, the Home screen will be displayed. The Oracle ECB GUI has the screen shown below:



Please click Configuration tab and the tab appears as shown below:



4.3. Add Network Settings

Go to System Administration ---- Network --- Network Settings and Click Add

The screenshot shows the 'Add Network Interface' configuration page in the Oracle Enterprise Communications Broker. The page is titled 'Add Network Interface' and is part of the 'Configuration' section. The left sidebar shows 'Network settings' selected. The main form contains the following fields:

- Sub Port Id: 0 (Range: 0..4095)
- Enable Icmp: enable
- Gw Heartbeat: enable
- Realm ID: ecb (dropdown)
- Virtual Mac:
- Hostname:
- IP Address: 10.232.50.70
- Pri Utility Addr:
- Sec Utility Addr:
- Netmask: 255.255.255.0
- Gateway: 10.232.50.1

At the bottom, there is a checkbox for 'Gw Heartbeat' and 'OK' and 'Back' buttons.

4.4. Configure SIP Interface

Go to System Administration ---- SIP Interfaces --- Interfaces and Click Add

The screenshot shows the 'Modify SIP Interface' configuration page in the Oracle Enterprise Communications Broker. The page is titled 'Modify SIP Interface' and is part of the 'Configuration' section. The left sidebar shows 'Interfaces' selected. The main form contains the following fields:

- State: enable
- Enable Early Media Inhibit: enable
- Realm ID: ecb (dropdown)
- Description: ECB Interface

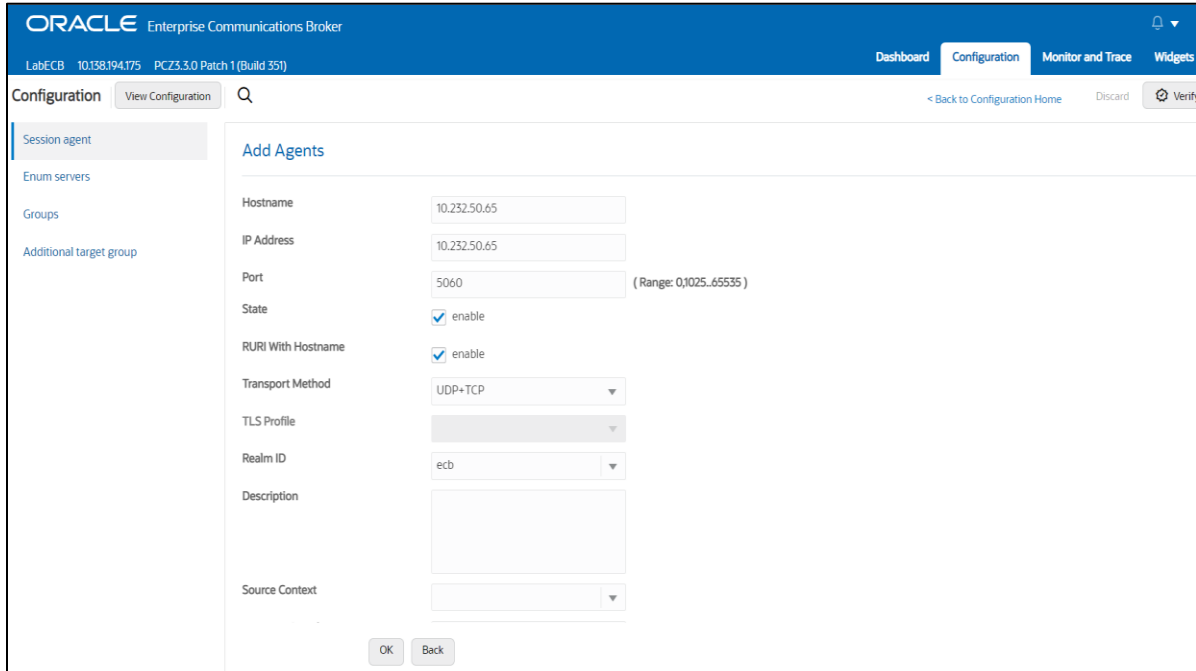
Below the form is a table for 'SIP Ports' with columns: Action, Select, Address, Port, Transport Protocol, and Allow Anonymous.

Action	Select	Address	Port	Transport Protocol	Allow Anonymous
:	<input type="checkbox"/>	10.232.50.70	5060	TCP	all
:	<input type="checkbox"/>	10.232.50.70	5060	UDP	all

At the bottom, there are 'OK' and 'Back' buttons.

4.5. Configuring the Agents

Click Configuration --- Service Provisioning ----- Agents --- Session Agents and Click Add. We will now add 10.232.50.65 as Agent to ECB (SBC SIP interface). This will be used to connect to PBX like Teams through SBC from the ECB.

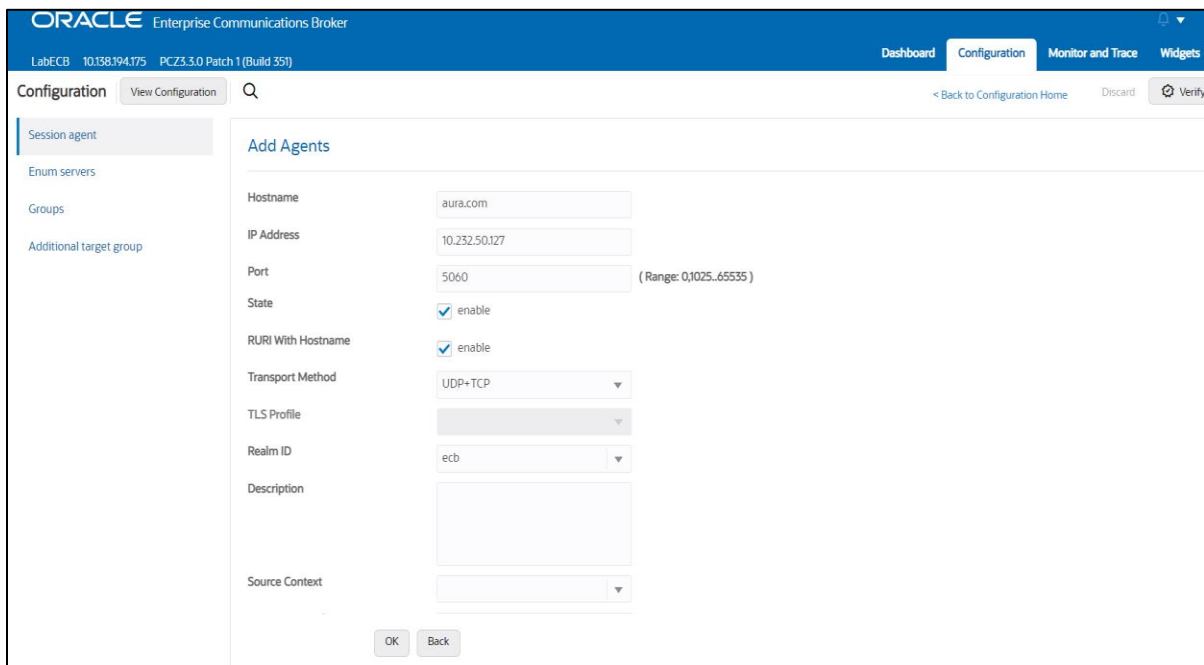


The screenshot shows the Oracle Enterprise Communications Broker configuration interface. The page title is "ORACLE Enterprise Communications Broker". The navigation bar includes "Dashboard", "Configuration", "Monitor and Trace", and "Widgets". The current page is "Configuration", and the sub-page is "Add Agents". The left sidebar shows "Session agent" selected. The main form fields are:

Hostname	10.232.50.65
IP Address	10.232.50.65
Port	5060 (Range: 0,1025..65535)
State	<input checked="" type="checkbox"/> enable
RURI With Hostname	<input checked="" type="checkbox"/> enable
Transport Method	UDP+TCP
TLS Profile	
Realm ID	ecb
Description	
Source Context	

Buttons: OK, Back

Similarly, add other IP-PBX (Core Side) as agents to ECB like given below. First add 10.232.50.127 (Avaya server) to the ECB.



The screenshot shows the Oracle Enterprise Communications Broker configuration interface. The page title is "ORACLE Enterprise Communications Broker". The navigation bar includes "Dashboard", "Configuration", "Monitor and Trace", and "Widgets". The current page is "Configuration", and the sub-page is "Add Agents". The left sidebar shows "Session agent" selected. The main form fields are:

Hostname	aura.com
IP Address	10.232.50.127
Port	5060 (Range: 0,1025..65535)
State	<input checked="" type="checkbox"/> enable
RURI With Hostname	<input checked="" type="checkbox"/> enable
Transport Method	UDP+TCP
TLS Profile	
Realm ID	ecb
Description	
Source Context	

Buttons: OK, Back

We can next add 10.232.50.89 or cucm-cisco.pe.oracle.com (Cisco CUCM) to the ECB.

The screenshot shows the Oracle Enterprise Communications Broker configuration interface. The page title is "ORACLE Enterprise Communications Broker". The navigation bar includes "Dashboard", "Configuration", "Monitor and Trace", and "Widgets". The current page is "Configuration", with a search bar and a "View Configuration" button. The left sidebar shows a tree view with "Session agent" selected. The main content area is titled "Add Agents" and contains the following fields:

- Hostname: cucm-cisco.pe.oracle.com
- IP Address: 10.232.50.89
- Port: 5060 (Range: 0,1025..65535)
- State: enable
- RURI With Hostname: enable
- Transport Method: UDP+TCP
- TLS Profile: (empty dropdown)
- Realm ID: ecb
- Description: (empty text area)
- Source Context: (empty dropdown)

At the bottom of the form are "OK" and "Back" buttons.

Finally, we can add 172.18.0.124 (Genesys Pure Engage) to the ECB.

The screenshot shows the Oracle Enterprise Communications Broker configuration interface, similar to the previous one. The page title is "ORACLE Enterprise Communications Broker". The navigation bar includes "Dashboard", "Configuration", "Monitor and Trace", and "Widgets". The current page is "Configuration", with a search bar and a "View Configuration" button. The left sidebar shows a tree view with "Session agent" selected. The main content area is titled "Add Agents" and contains the following fields:

- Hostname: 172.18.0.124
- IP Address: 172.18.0.124
- Port: 4080 (Range: 0,1025..65535)
- State: enable
- RURI With Hostname: enable
- Transport Method: UDP+TCP
- TLS Profile: (empty dropdown)
- Realm ID: ecb
- Description: (empty text area)
- Source Context: (empty dropdown)

At the bottom of the form are "OK" and "Back" buttons.

Please keep the parameter **“Egress Number Translation Mode = E164-no-plus”** for all Session Agent configured above in the ECB. With this, ECB common configurations are complete. We will proceed to feature specific configuration from the next section.

4.6. ECB with LDAP configuration

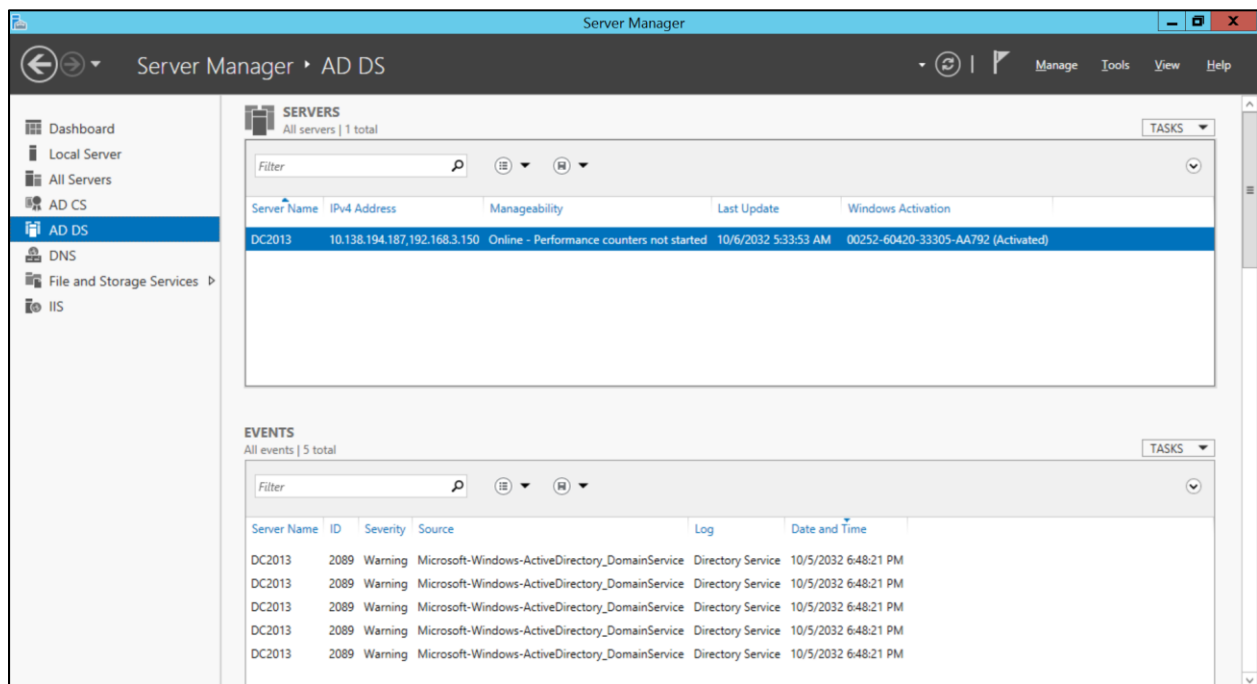
To test the Oracle ECB with LDAP authentication, we have used the Windows AD configuration with ECB. Regarding AD server, we need AD with Domain controller Service (AD DS) installed with which we can add Users to the AD which can be queried using LDAP protocol. If we configure windows AD with only LDS service (AD LDS), we will not be able to add Users in Active Directory and hence we cannot use AD server for LDAP configuration.

The Windows AD DS server is configured in the lab with 10.138.194.187 IP and Administrator/Abcd1234 credentials.

For more information on how to configure Windows Server with AD server and using ADSI and other option, please refer to below link

<https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/deploy/install-active-directory-domain-services--level-100->

The Screenshot from Windows AD side is given below: (High Level)



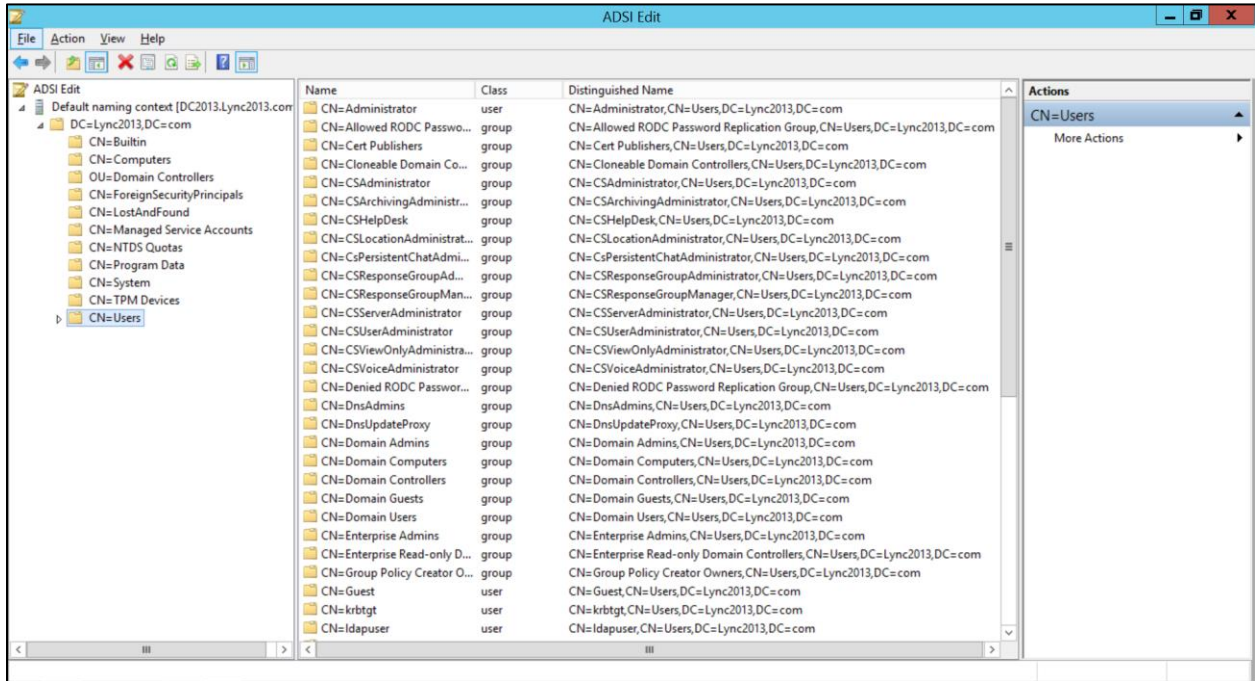
The screenshot displays the Windows Server Manager interface for an Active Directory Domain Services (AD DS) server. The left-hand navigation pane shows the hierarchy: Dashboard, Local Server, All Servers, AD CS, AD DS (selected), DNS, File and Storage Services, and IIS. The main area is titled 'SERVERS' and shows a list of servers. A single server, 'DC2013', is listed with the following details:

Server Name	IPv4 Address	Manageability	Last Update	Windows Activation
DC2013	10.138.194.187, 192.168.3.150	Online - Performance counters not started	10/6/2032 5:33:53 AM	00252-60420-33305-AA792 (Activated)

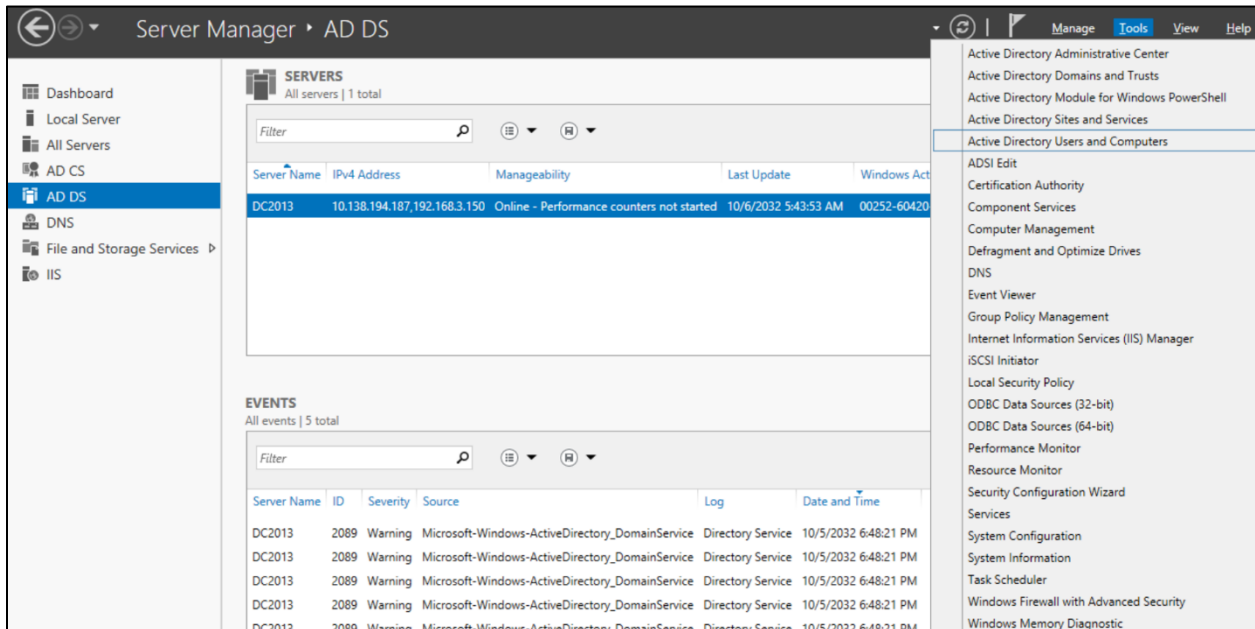
Below the servers list, the 'EVENTS' section shows a list of 5 events. All events are warnings from the Directory Service source, occurring on 10/5/2032 at 6:48:21 PM.

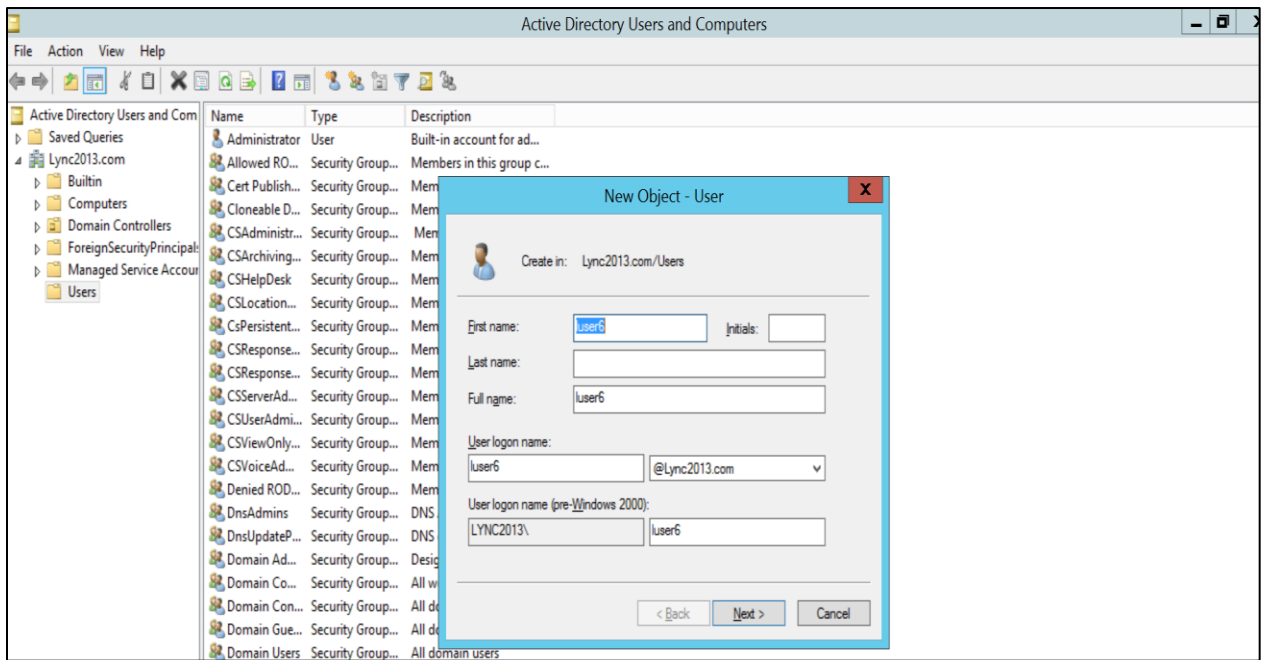
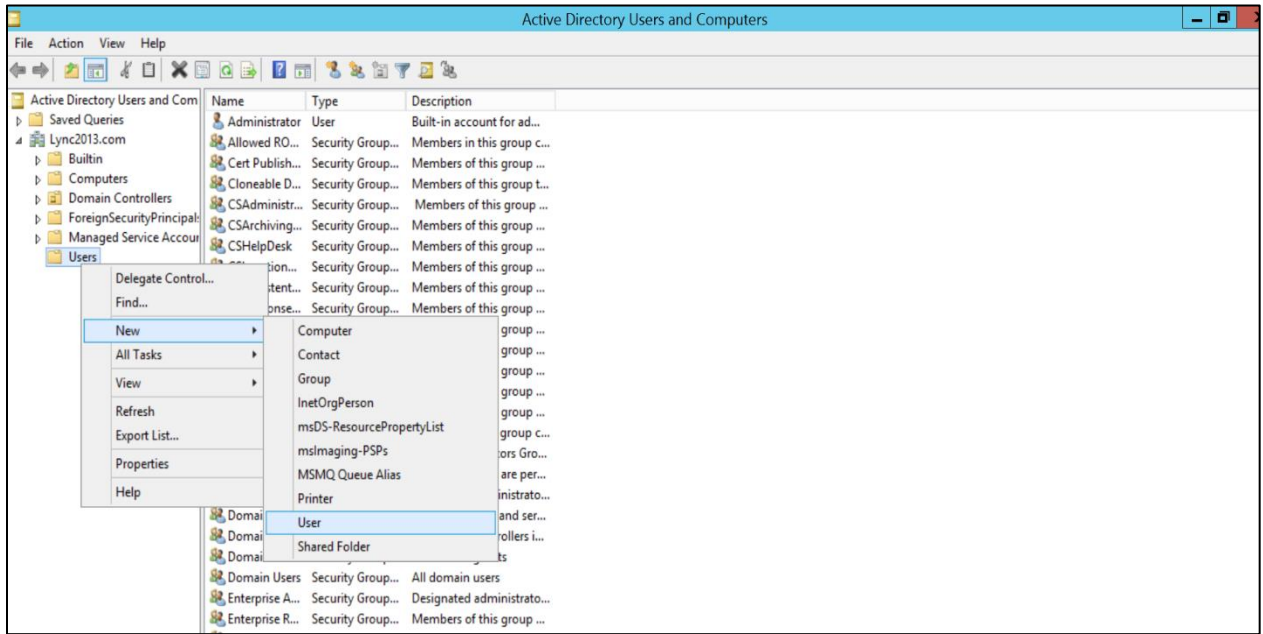
Server Name	ID	Severity	Source	Log	Date and Time
DC2013	2089	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory Service	10/5/2032 6:48:21 PM
DC2013	2089	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory Service	10/5/2032 6:48:21 PM
DC2013	2089	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory Service	10/5/2032 6:48:21 PM
DC2013	2089	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory Service	10/5/2032 6:48:21 PM
DC2013	2089	Warning	Microsoft-Windows-ActiveDirectory_DomainService	Directory Service	10/5/2032 6:48:21 PM

Right Click the AD server and you will get various options and please select ADSIEdit option to open it and you will get the below tree structure if AD DS is configured properly.

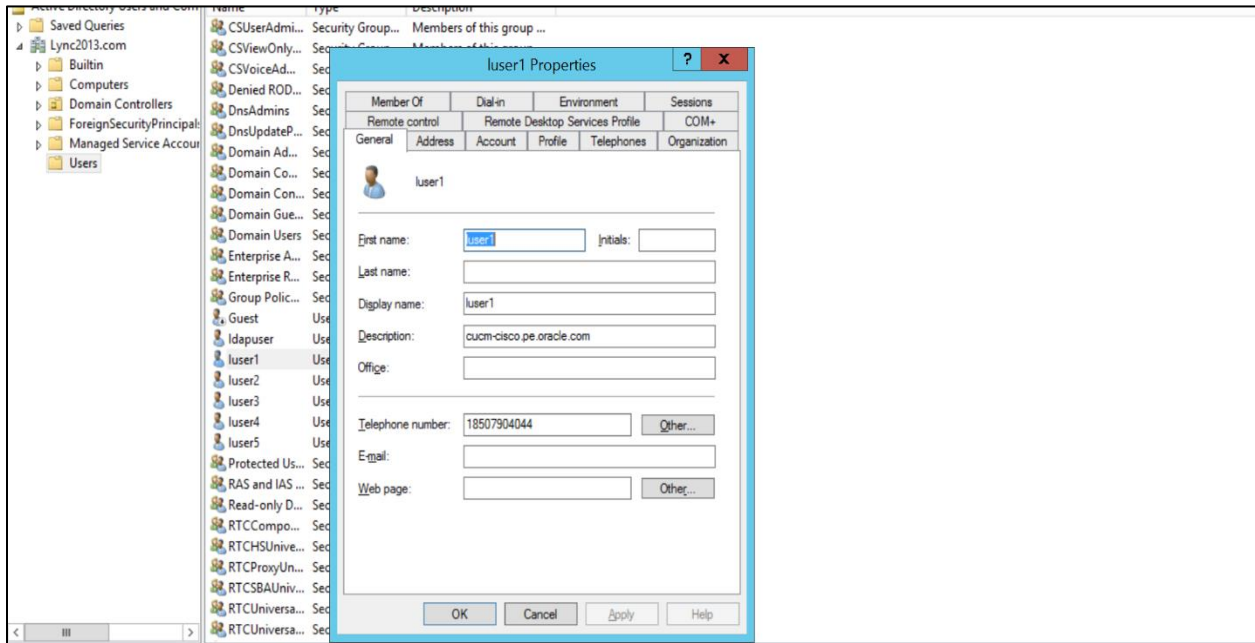


Please select AD server manager ---- tools and select users and computers tab and you can create the users that you will be querying using ECB LDAP configuration.





We can also add the **attributes “description” and “Telephone number”** to the users which will be used as search option in ECB LDAP config under routing/lookup query.



With the above steps, the user is created in the Windows AD DS server.

We can add more users using the above steps.

For our testing, we have created luser1 for Core side and luser2 for SBC side.

Once we have created the Users in AD DS server, we can proceed to ECB for LDAP configuration. The pre-requisite for this config to work is that we need to have Session Agents configured for both sides in the ECB.

Please go to ECB and Navigate to System Administration – LDAP --- LDAP Config and do the configuration as per the testing needs. In the below example, we have created configuration for LDAP to search for core side user and SBC side user. As the Call from ECB is routed to SBC side and vice versa, SBC interface IP configured for ECB side as Session Agent in ECB.

The config given below is to search core side user. (Avaya/CUCM/Genesys). Here in the below example, we used LDAP search for CUCM user.

The screenshot shows the 'Modify LDAP Config' page in the Oracle Enterprise Communications Broker. The configuration includes the following fields:

- Name: LDAP_Core
- State: enable
- LDAP Servers: 192.168.3.150:389
- Realm: ecb
- Username: CN=luser1,CN=Users,DC=Lync2013,DC
- Password: [Redacted]
- LDAP Search Base: DC=Lync2013,DC=com
- Timeout Limit: 15 (Range: 1..300)
- Max Request Timeouts: 3 (Range: 0..10)
- TCP Keepalive: enable

Buttons at the bottom include 'OK' and 'Back'.

The routing looks for attribute description and telephoneNumber added in the ldap user already.

The screenshot shows the 'Modify LDAP Config' page with the 'Routing' section expanded. The configuration includes:

- Max Request Timeouts: 3 (Range: 0..10)
- TCP Keepalive: enable
- LDAP Sec Type: None
- Routing State: enable
- Route Mode: match-only
- From Header Replacement: [Empty field]

The 'Lookup Queries' section contains a table with the following data:

Action	Select	Lookup Numb...	Lookup Numb...	Lookup Numb...	Lookup Numb...	Home Agent A...	Home Agent R...	Home Agent Regex Result	Default Hd
:	<input type="checkbox"/>	telephoneNum...	None	^\+?1?(\d{3})\(\s...	tel:+\$1\$2\$3	description			

Buttons at the bottom include 'OK' and 'Back'.

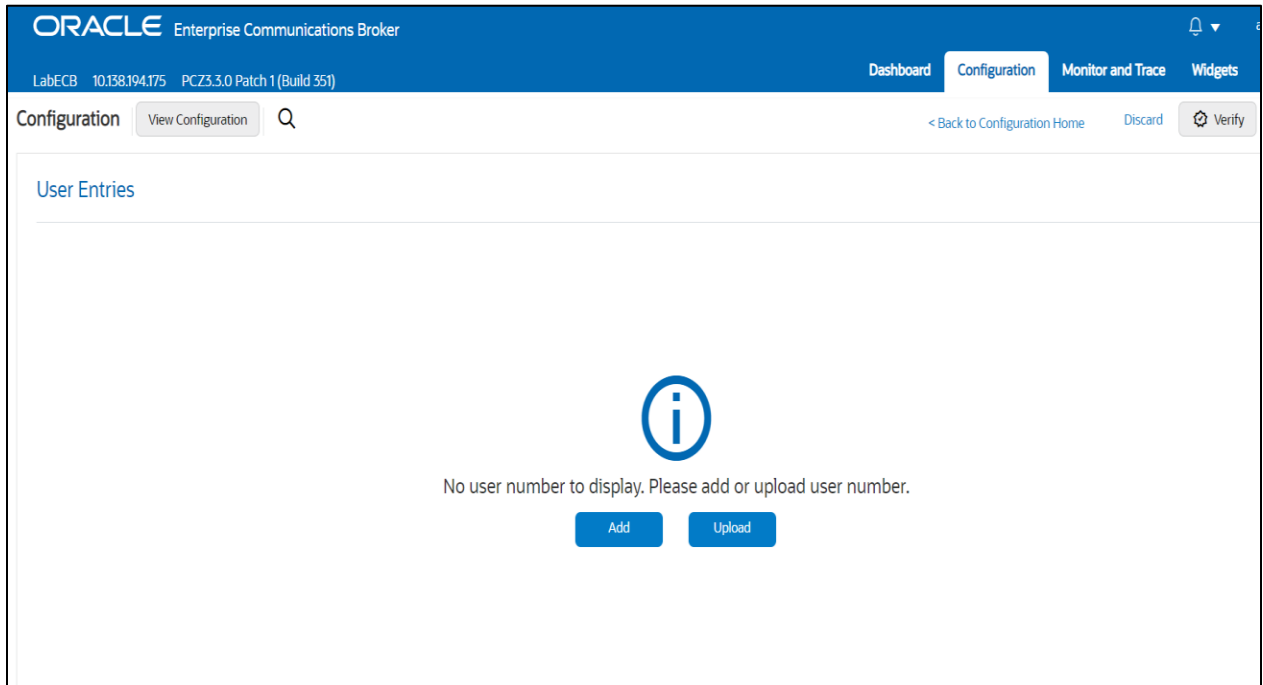
The screenshot shows the Oracle Enterprise Communications Broker interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The 'Configuration' tab is active. The main content area is titled 'Modify Ldap config / routing / lookup query'. On the left, there is a sidebar with 'LDAP config' and 'LDAP group' sections. The main form contains the following fields:

- Lookup Number Attribute: telephoneNumber
- Lookup Number Format Type: None
- Lookup Number Regex Pattern: ^\+?1?(\d{3})(\d{3})(\d{4})\$
- Lookup Number Regex Result: tel:+1\$1\$2\$5
- Home Agent Attribute: description
- Home Agent Regex Pattern: (empty)
- Home Agent Regex Result: (empty)
- Default Home Agent: (empty)
- Fork Group Attribute: (empty)

At the bottom of the form are 'OK' and 'Back' buttons.

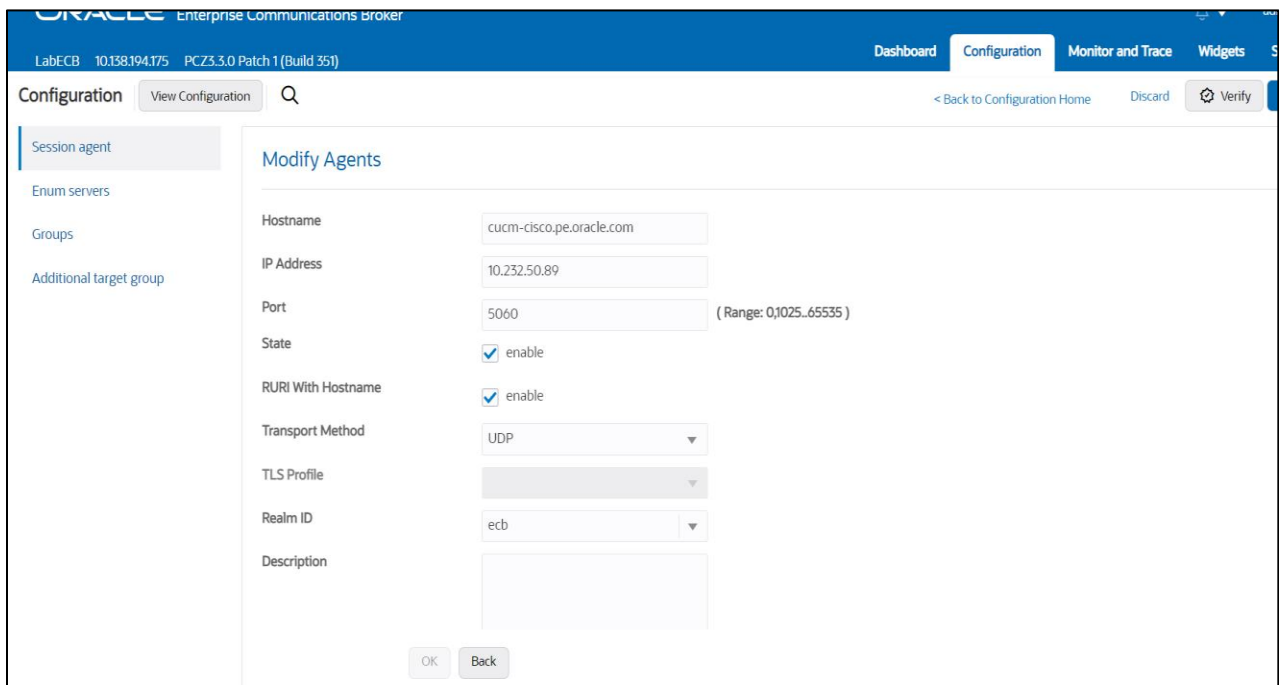
Similarly, create an LDAP config similar to above config for SBC side. Please check that there should not be any routing config or User Entry config in ECB when we are using LDAP config as the ECB need to search only LDAP to get the next step.

The screenshot shows the Oracle Enterprise Communications Broker interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active. The main content area is titled 'Routing Table'. Below the title, there is a large empty space with a central information icon (a lowercase 'i' inside a circle). Below the icon, the text reads: 'No routing entry to display. Please add or upload routing entry.' At the bottom of this section are two buttons: 'Add' and 'Upload'.



Once the config is done, please navigate to Session Agent, select the Source agent and add the LDAP config created under LDAP option as given below.

When Core side agent (Cisco CUCM) is the source side, add SBC side LDAP config under LDAP option. Save the config after making all the necessary steps.



The screenshot shows the 'Modify Agents' configuration page in the Oracle Enterprise Communications Broker. The 'LDAP' dropdown menu is highlighted with a red box, indicating that 'LDAP_SBC' is selected. Other configuration options include 'Apply Outbound Manipulation On' (next-hop-only), 'In Manipulationid', 'Out Manipulationid', 'Manipulation String', 'Early Media Inhibit' (enable), 'Additional Target Group', 'Fork Group' (1), 'Refer Call Transfer' (disabled), 'Refer Notify Provisional' (none), and 'Reuse Connections' (NONE).

Similarly, When SBC agent is source side, add Core side LDAP config under LDAP option. The LDAP config is ECB looks like below:

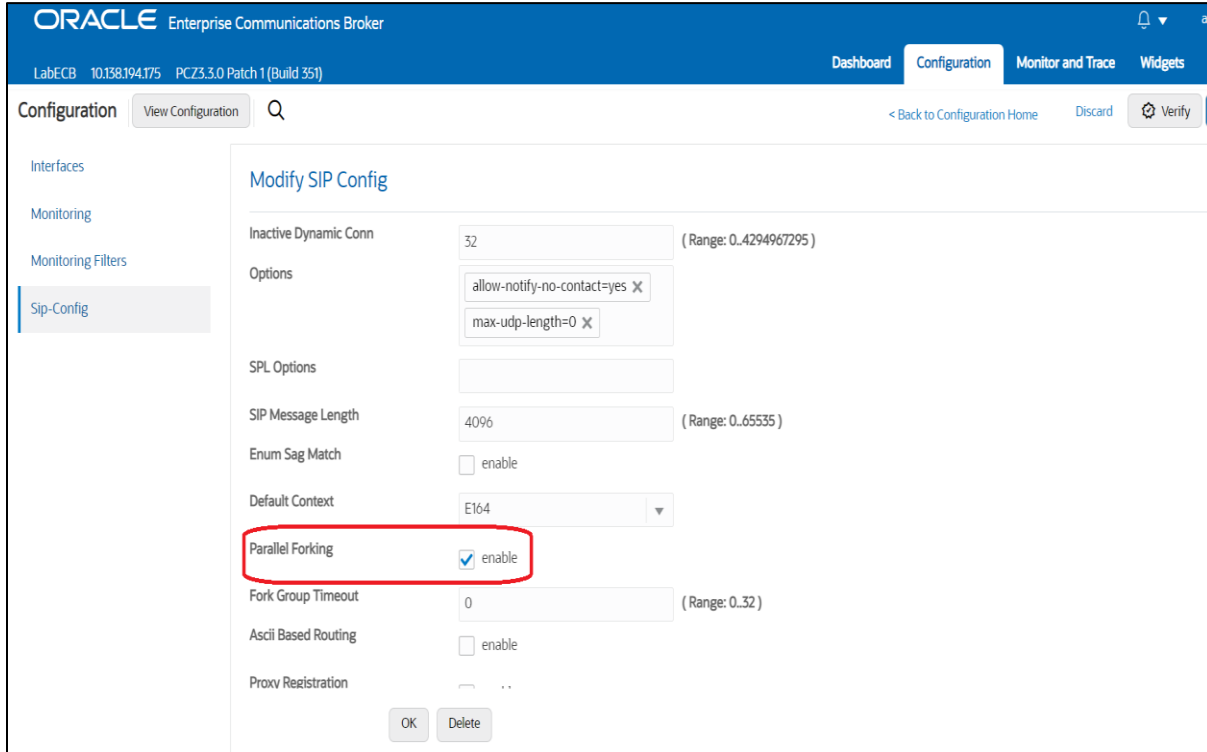
The screenshot shows the 'LDAP Config' table in the Oracle Enterprise Communications Broker. The table lists the following configurations:

Action	Select	Name	State	Realm	Username	Password	LDAP Search Base	Timeout Limit
:	<input type="checkbox"/>	LDAP_Core	enabled	ecb	CN=luser1,CN=Users,...	*****	DC=Lync2013,DC=com	15
:	<input type="checkbox"/>	LDAP_SBC	enabled	ecb	CN=luser2,CN=Users,...	*****	DC=Lync2013,DC=com	15
:	<input type="checkbox"/>	global	disabled	ecb			DC=WINGENCIC,DC...	15

4.7. ECB Parallel Forking with LDAP configuration

Oracle ECB can perform parallel forking, which directs the INVITE to all targets for an Address of Record (AOR) simultaneously. In other words, a single DID or directory number is configured in multiple Agents and an inbound call needs to be simultaneously alerted to those Agents. When any target responds, the Oracle ECB issues a CANCEL to the other targets and ignores any responses from them

We can enable parallel forking from SIP Interface ---- SIP Config configuration of the ECB as given below.



The screenshot shows the Oracle Enterprise Communications Broker configuration interface. The main heading is "Modify SIP Config". The "Parallel Forking" checkbox is checked and highlighted with a red box. Other configuration options include:

- Inactive Dynamic Conn: 32 (Range: 0.4294967295)
- Options: allow-notify-no-contact=yes X, max-udp-length=0 X
- SPL Options: (empty)
- SIP Message Length: 4096 (Range: 0.65535)
- Enum Sag Match: enable
- Default Context: E164
- Parallel Forking: enable
- Fork Group Timeout: 0 (Range: 0.32)
- Ascii Based Routing: enable
- Proxv Registration: (empty)

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

To test ECB parallel forking with LDAP config, we need to add additional attributes along with already added attributes in routing tab which is under LDAP config. The same attributes needs to be added under the LDAP user user1 in the AD server too.

For our testing, we have added the different attribute **“otherTelephone”** and **“info”** which corresponds to Avaya User so that ECB sends INVITE to both PBX at same time. Save the config after that.

The config is shown below for ECB parallel forking with LDAP.

The screenshot shows the 'Modify LDAP Config' page in the Oracle Enterprise Communications Broker. The configuration includes the following fields:

- Name: LDAP_Core
- State: enable
- LDAP Servers: 192.168.3.150:389
- Realm: ecb
- Username: CN=luser1,CN=Users,DC=Lync2013,DC=
- Password:
- LDAP Search Base: DC=Lync2013,DC=com
- Timeout Limit: 15 (Range: 1.300)
- Max Request Timeouts: 3 (Range: 0.10)
- TCP Keepalive: enable

Buttons at the bottom include 'OK' and 'Back'.

The screenshot shows the 'Modify LDAP Config' page in the Oracle Enterprise Communications Broker, focusing on routing and lookup queries. The configuration includes the following fields:

- LDAP Sec Type: None
- Routing:
 - State: enable
 - Route Mode: match-only
 - From Header Replacement:
- Lookup Queries:

Action	Select	Lookup Numb...	Lookup Numb...	Lookup Numb...	Lookup Numb...	Home Agent A...	Home Agent R...	Home Agent Regex Result	Default Hom...
:	<input type="checkbox"/>	telephoneNum...	None	^\+?1?(\d{3})\(...	tel:+1\$1\$2\$3	description			cucm-cisco.p
:	<input type="checkbox"/>	otherTelephone	None	^\+?1?(\d{3})\(...	tel:+1\$1\$2\$3	info			10.232.50.127

Buttons at the bottom include 'OK' and 'Back'.

ORACLE Enterprise Communications Broker

LabECB 10.138.194.175 PCZ3.3.0 Patch 1 (Build 351) Dashboard Configuration Monitor and Trace Widgets

Configuration View Configuration < Back to Configuration Home Discard Verify

LDAP config

LDAP group

Modify Ldap config / routing / lookup query

Lookup Number Attribute: otherTelephone

Lookup Number Format Type: None

Lookup Number Regex Pattern: ^\+?1?(\d{3})(\d{3})(\d{4})\$

Lookup Number Regex Result: tel:+1\$1\$2\$3

Home Agent Attribute: info

Home Agent Regex Pattern:

Home Agent Regex Result:

Default Home Agent: 10.232.50.127

Fork Group Attribute:

OK Back

The AD user luser1 additional attribute config is given below.

ADSI Edit

Default naming context [DC=2013.Lync2013.c

DC=Lync2013,DC=com

- CN=Builtin
- CN=Computers
- OU=Domain Controllers
- CN=ForeignSecurityPrincipals
- CN=LostAndFound
- CN=Managed Service Accounts
- CN=NTDS Quotas
- CN=Program Data
- CN=System
- CN=TPM Devices
- CN=Users
 - CN=Administrator
 - CN=Allowed RODC Password Re
 - CN=Cert Publishers
 - CN=Cloneable Domain Controlle
 - CN=CSAdministrator
 - CN=CSArchivingAdministrator
 - CN=CSHelpDesk
 - CN=CSLocationAdministrator
 - CN=CSPersistentChatAdministra
 - CN=CSResponseGroupAdministra
 - CN=CSResponseGroupManager
 - CN=CSServerAdministrator
 - CN=CSUserAdministrator
 - CN=CSViewOnlyAdministrator
 - CN=CSVoiceAdministrator
 - CN=Denied RODC Password Rep
 - CN=DnsAdmins

Name	Class	Distinguished Name
CN=luser1	Person	...

CN=luser1 Properties

Attribute	Value
homePhone	<not set>
homePostalAddress	<not set>
houseIdentifier	<not set>
info	10.232.50.127
initials	<not set>
instanceType	0x4 = (WRITE)
internationalISDNNu...	<not set>
ipPhone	<not set>
isCriticalSystemObject	<not set>
isDeleted	<not set>
isRecycled	<not set>
jpegPhoto	<not set>
I	<not set>
labeledURI	<not set>

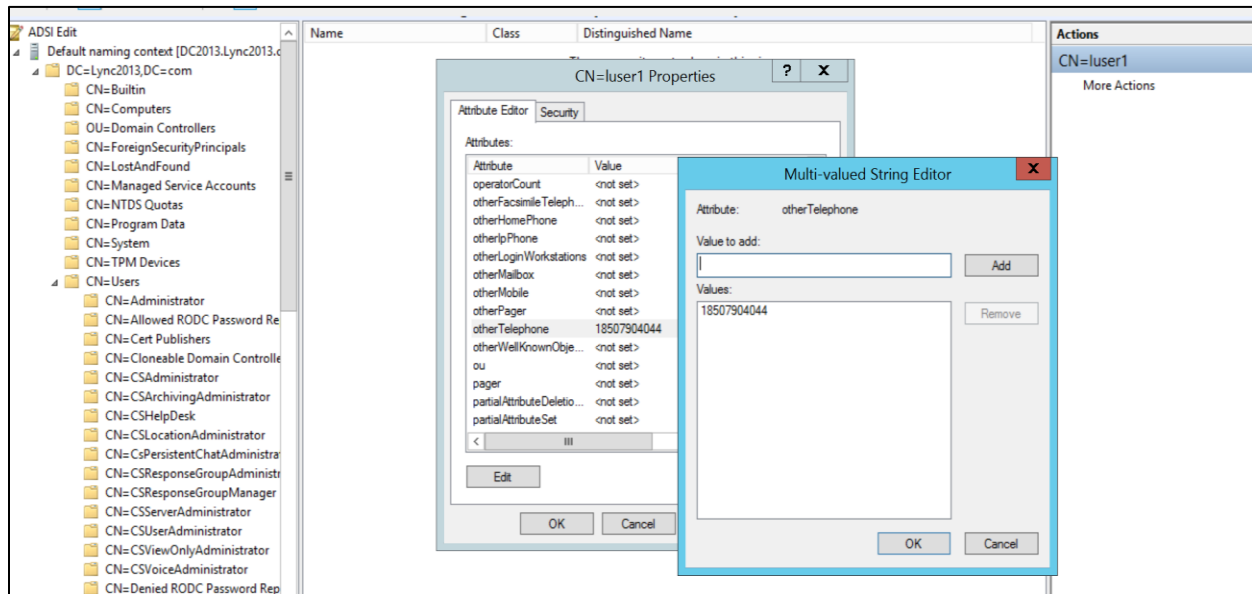
String Attribute Editor

Attribute: info

Value: 10.232.50.127

Clear OK Cancel

The same directory number 18507904044 is given to Avaya User as well for ECB parallel forking.

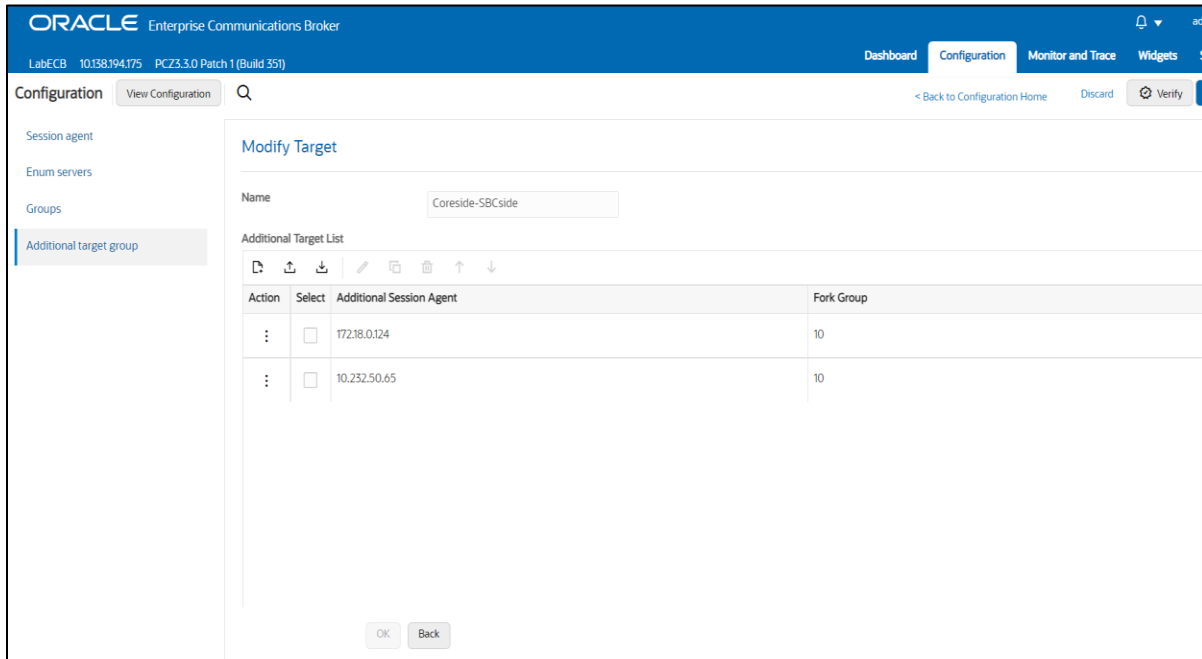


4.8. ECB Parallel Forking with Additional Target Group (ATG) configuration

Similar to LDAP parallel forking, ECB can also perform parallel forking using Additional Target Group (ATG) configuration. An Additional Target Group (ATG) is a list of agents or end stations that ECB uses as candidates for either parallel or serial forking. You can configure these ATGs with fork group numbers, which the system then uses to do forking (For our testing, we do parallel forking). The configuration for ECB ATG parallel forking is performed in different way and is given below.

Please go to ECB and Navigate to Service Provisioning – Agents --- Additional Target Group --- Add, To add a new ATG for parallel forking by giving Name – Any desired Name.

After that, select the Agents that you want to do parallel forking.
For this testing, we have selected Agents from both core side and SBC side.
Give Fork Group as equal for both Agents (10 in our case for both agents).



Go to: Service Provisioning ----- Agents ----- Session Agent.
 Create a dummy agent with the following config for ATG parallel forking.

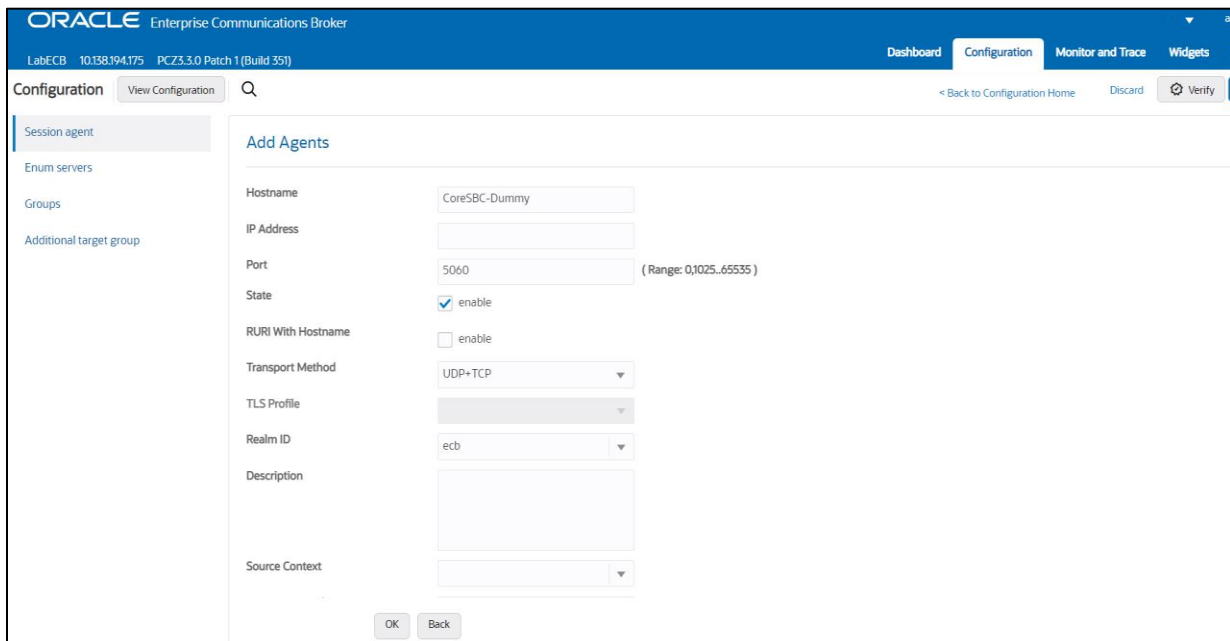
Hostname: Create a new agent (Dummy Agent) for the desired targets that require parallel forking.

IP Address: Leave blank for the Dummy Agent.

Enable OPTIONS ping: Should be disabled for dummy agent.

Additional target group: Assign the created ATG group

Fork group: The fork group number (90) must be higher than the values assigned to the Agents (10) within the ATG.



The screenshot shows the 'Add Agents' configuration page in the Oracle Enterprise Communications Broker. The page is titled 'Configuration' and includes a search bar and navigation links. The main content area contains several configuration fields:

- Sustain Rate Window:** 0 (Range: 0.999999999)
- Enable OPTIONS Ping:** enable (highlighted with a red box)
- Ping Interval:** 0 (Range: 0.4294907295)
- Ping All Addresses:** enable
- Ping Method:** (dropdown menu)
- Ping In Service Response Codes:** (text input)
- Load Balance DNS Query:** hunt (dropdown menu)
- SPL Options:** (text input)
- Apply Outbound Manipulation On:** next-hop-only (dropdown menu)
- In Manipulationid:** (dropdown menu)
- Out Manipulationid:** (dropdown menu)
- Manipulation String:** (text input)
- Early Media Inhibit:** enable
- LDAP:** (dropdown menu)
- Additional Target Group:** Coreside-SBCside (dropdown menu, highlighted with a red box)
- Fork Group:** 90 (Range: 1,100)

At the bottom of the form, there are 'OK' and 'Back' buttons.

Go to: Service Provisioning ----- User Entries ----- Session Agent and Add a new entry as shown below.

Number or Pattern: Enter the DID of the Agents
Agent: Select the Dummy Agent created.

The screenshot shows the 'Add User Entries' configuration page in the Oracle Enterprise Communications Broker. The page is titled 'Configuration' and includes a search bar and navigation links. The main content area contains several configuration fields:

- AoR:** (text input)
- Number Or Pattern:** 17814437248
- Description:** (text input)
- Dialling Context:** (dropdown menu)
- Agent:** CoreSBC-Dummy (dropdown menu)
- Policy:** (text input)
- Tags:** (text input)

At the bottom of the form, there are 'OK' and 'Back' buttons.

This DID will ring both Core side PBX (Genesys) and SBC side (Teams) due to parallel forking.

Finally, Go to: Service Provisioning ----- Agents ----- Session Agent.

The standard agent selected for Core and SBC side also need to be set to Fork group (10) to match the ATG fork group to make ATG parallel forking work properly. The config is shown below for reference. Save the config after that.

The screenshot shows the Oracle Enterprise Communications Broker configuration interface. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The 'Configuration' tab is active. On the left, a sidebar lists 'Session agent', 'Enum servers', 'Groups', and 'Additional target group'. The main area is titled 'Modify Agents' and contains the following fields:

Hostname	10.232.50.65
IP Address	10.232.50.65
Port	5060 (Range: 0,1025..65535)
State	<input checked="" type="checkbox"/> enable
RURI With Hostname	<input checked="" type="checkbox"/> enable
Transport Method	UDP+TCP
TLS Profile	
Realm ID	ecb
Description	
Source Context	

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

This screenshot shows the same 'Modify Agents' configuration page, but with additional fields visible. The 'Fork Group' field is highlighted with a red rectangle and is set to the value '10'. The range for this field is indicated as '(Range: 1,100)'. Other fields include:

In Manipulationid	rejectOPTIONS
Out Manipulationid	
Manipulation String	
Early Media Inhibit	<input type="checkbox"/> enable
LDAP	
Additional Target Group	
Fork Group	10 (Range: 1,100)
Refer Call Transfer	disabled
Refer Notify Provisional	none
Reuse Connections	NONE
TCP Keepalive	none
TCP Reconn Interval	0 (Range: 0,2..300)

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

ORACLE Enterprise Communications Broker

LabECB 10.138.194.175 PCZ3.3.0 Patch 1 (Build 351) Dashboard Configuration Monitor and Trace Widgets

Configuration View Configuration Q < Back to Configuration Home Discard Verify

Session agent

Enum servers

Groups

Additional target group

Add Agents

Hostname: 172.18.0.124

IP Address: 172.18.0.124

Port: 4080 (Range: 0,1025..65535)

State: enable

RURI With Hostname: enable

Transport Method: UDP+TCP

TLS Profile:

Realm ID: ecb

Description:

Source Context:

OK Back

ORACLE Enterprise Communications Broker

LabECB 10.138.194.175 PCZ3.3.0 Patch 1 (Build 351) Dashboard Configuration Monitor and Trace Widgets

Configuration View Configuration Q < Back to Configuration Home Discard Verify

Session agent

Enum servers

Groups

Additional target group

Modify Agents

In Manipulationid: rejectOPTIONS

Out Manipulationid:

Manipulation String:

Early Media Inhibit: enable

LDAP:

Additional Target Group:

Fork Group: 10 (Range: 1,100)

Refer Call Transfer: disabled

Refer Notify Provisional: none

Reuse Connections: NONE

TCP Keepalive: none

TCP Reconn Interval: 0 (Range: 0,2..300)

OK Back

With this, ECB feature specific configuration are complete.



5. Configuring the SBC

This chapter strictly provides step-by-step guidance on how to configure Oracle SBC to route calls to Oracle ECB and ECB features related testing using Teams configuration as an example.

Note: This document will not cover SBC config for Teams and those config can be referred using any other Teams with SBC app notes.

5.1. Validated Oracle SBC version

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

- AP 1100
- AP 3900
- AP 4600
- AP 6350
- AP 6300
- 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

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 tIPTd...
Starting tSecured...
Starting tAuthd...
Starting tCertd...
Starting tIked...
Starting tTscfd...
Starting tAppWeb...
Starting tauditd...
Starting tauditpusher...
Starting tSnmpd...
Starting tIFMIBd...
Start platform alarm...
Starting display manager...
Initializing /opt/ Cleaner
Starting tLogCleaner task
Bringing up shell...
password secure mode is enabled
Admin Security is disabled
Starting SSH...
SSH Cli init: allocated memory for 5 connections
```

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.

```
Starting acmeboot...
ACME bootloader Acme Packet SCZ9.0.0 GA (Build 54) 202105121954
Press the space bar to stop auto-boot...
0
auto-booting...

Boot File           : /boot/nnSCZ840p7.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        : vxftp
Flags               : 0x00000000
Target Name         : NN4600-139
Console Device      : COM1
Console Baudrate    : 115200
Other               :

Booting image version Acme Packet SCZ8.4.0 Patch 7 (Build 436) 202108231854
```

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

```
NN4600-139#
NN4600-139# setup product

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

Last Modified 2020-04-30 22:38:15

-----
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.

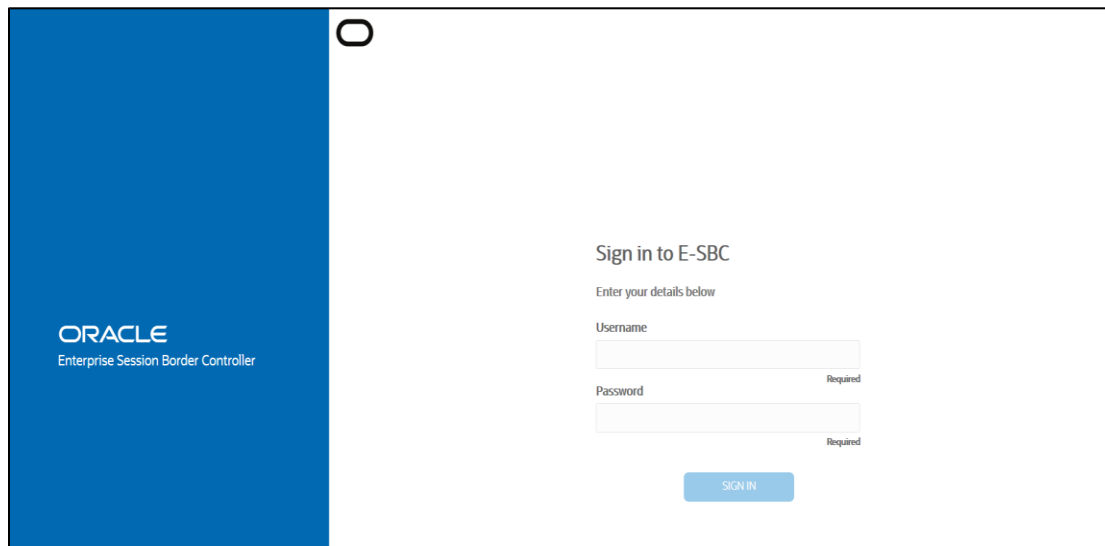
Enable the http-server-config to access the SBC using Web GUI. Save and activate the config.

```
NN4600-139(http-server)#
NN4600-139(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  REST, GUI
  http-file-upload-size 0
  tls-profile
  auth-profile
  last-modified-by     @
  last-modified-date   2021-01-25 00:16:28
NN4600-139(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>.



ORACLE
Enterprise Session Border Controller

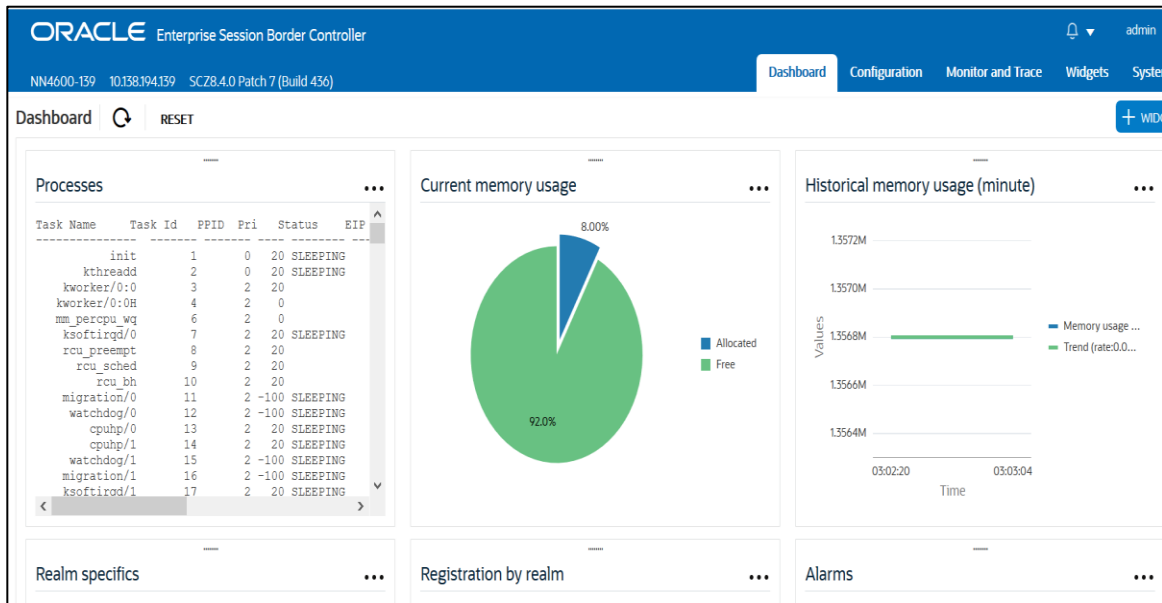
Sign in to E-SBC

Enter your details below

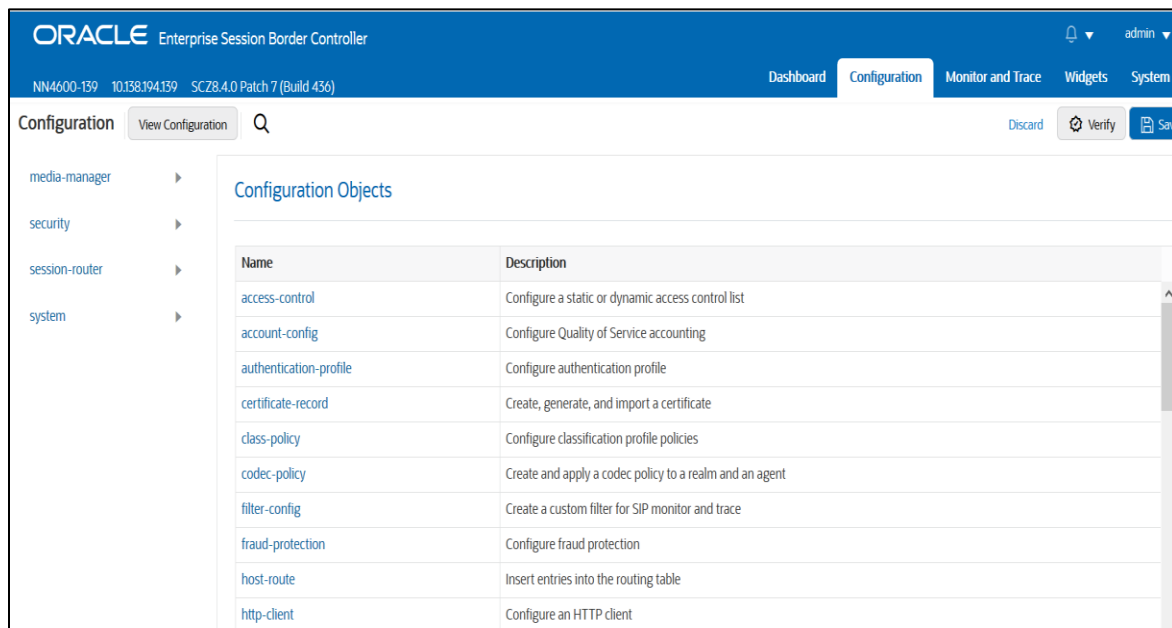
Username

Password Required

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



Go to Configuration as shown below, to configure the SBC



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

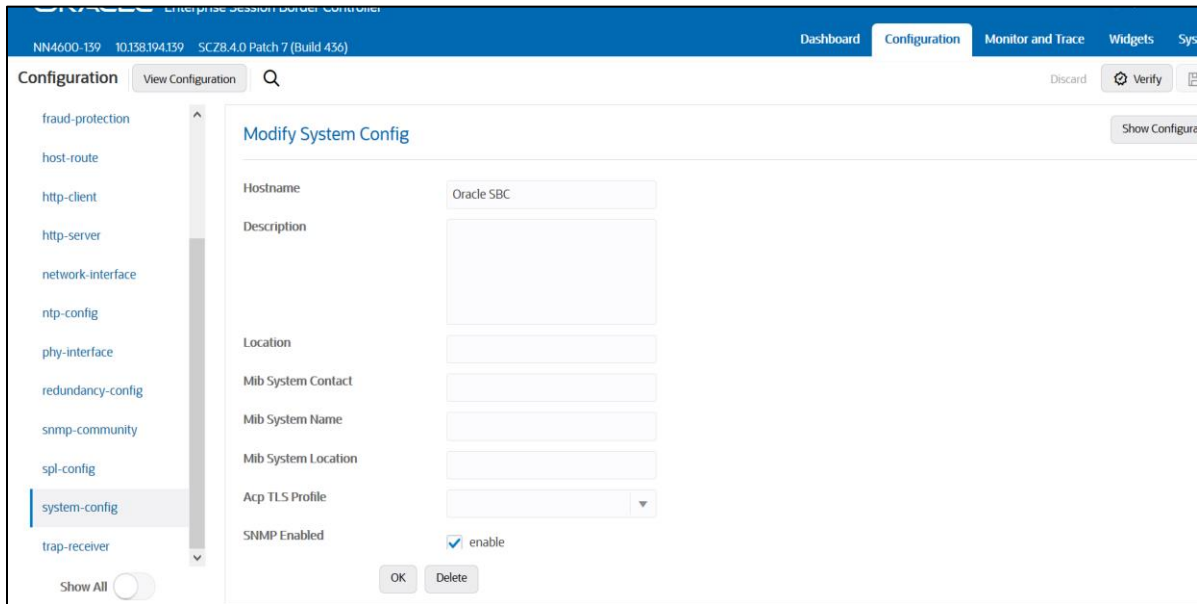
https://docs.oracle.com/en/industries/communications/enterprise-session-border-controller/8.4.0/webgui/esbc_scz840_webgui.pdf

The expert mode is used for configuration.

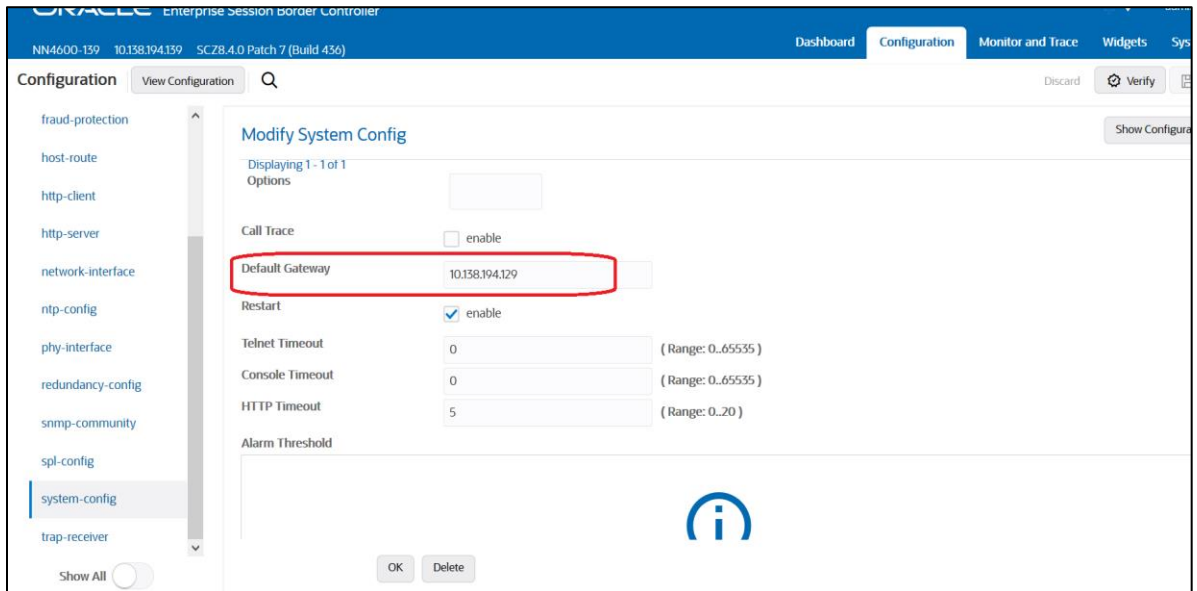
Tip: To make this configuration simpler, one can directly search the element to be configured, from the Objects tab available.

6.3. Configure system-config

Go to system->system-config



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



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/8.4.0/releasenotes/esbc_scz840_releasenotes.pdf

The above step is needed only if any transcoding is used in the configuration. If there is no transcoding involved, then the above step is not needed.

6.4. Configure Physical Interface values

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

You will first configure the slot 0, port 0 interface designated with the name M00.
This will be the port plugged into your public interface. (For Teams and Verizon side)
Avaya side is configured on the slot 0 port 1

Parameter Name	Public Interface(M00)	ECB Side (M10)
Slot	0	0
Port	0	1
Operation Mode	Media	Media

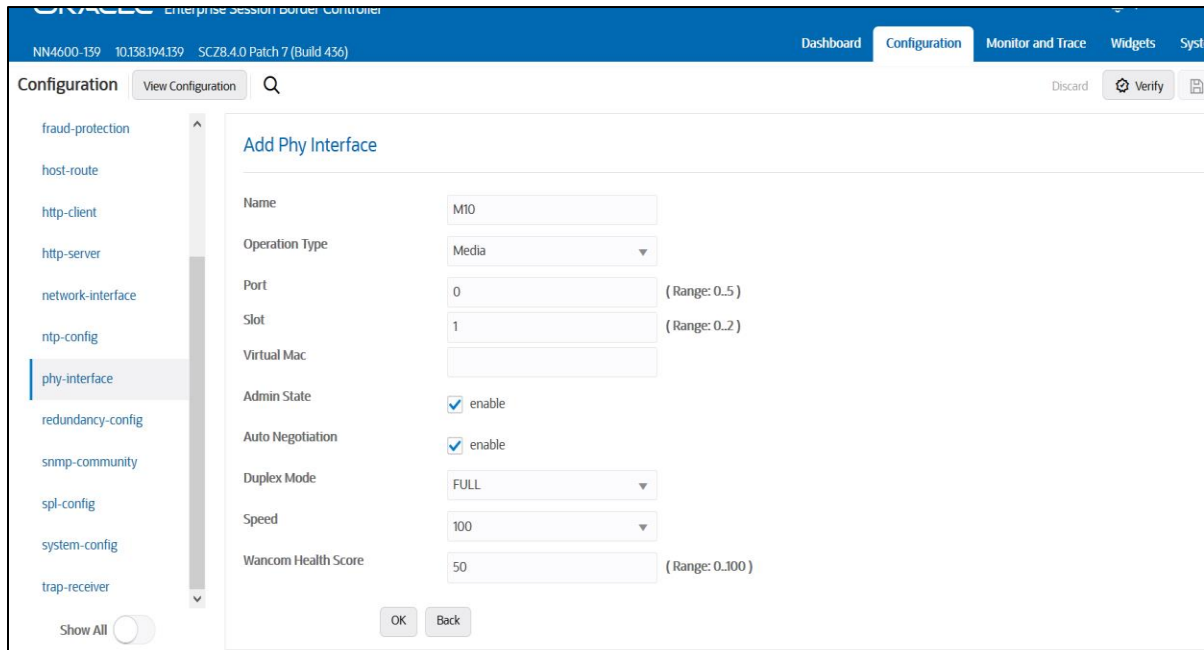
Please configure M00 interface as below.

The screenshot shows the 'Add Phy Interface' configuration page in the Oracle Enterprise Session Border Controller. The interface includes a navigation menu on the left with 'phy-interface' selected. The main configuration area contains the following fields and values:

- 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
- Speed: 100
- Wancom Health Score: 50 (Range: 0.100)

Buttons for 'OK' and 'Back' are located at the bottom of the configuration area. The top navigation bar includes 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'.

Similarly, configure M10 interface as below.



6.5. Configure Network Interface values

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

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

Parameter Name	Public Interface (For Teams)	ECB side Network interface
Name	M00	M10
Host Name	customers.telechat.o-test06161977.com	
IP address	<input type="text"/>	10.232.50.65
Netmask	255.255.255.192	255.255.255.0
Gateway	<input type="text"/>	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 'Widget'. The 'Configuration' tab is active. On the left, a sidebar lists various configuration categories, with 'network-interface' selected. The main area is titled 'Add Network Interface' and contains the following fields:

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

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

Please configure network interface M10 as below

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface, similar to the previous one. The 'network-interface' category is selected in the sidebar. The 'Add Network Interface' form is filled with the following values:

Name	M10
Sub Port Id	0 (Range: 0..4095)
Description	
Hostname	
IP Address	10.252.50.65
Pri Utility Addr	
Sec Utility Addr	
Netmask	

'OK' and 'Back' buttons are at the bottom. The 'Show All' toggle is at the bottom left of the sidebar.

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 Oracle Enterprise Session Border Controller configuration interface. The 'Configuration' tab is active, and the 'media-manager' section is selected in the left sidebar. The main area displays the 'Modify Media Manager' configuration page. The 'State' is set to 'enable'. The 'Flow Time Limit' is 86400, 'Initial Guard Timer' is 300, 'Subsq Guard Timer' is 300, 'TCP Flow Time Limit' is 86400, 'TCP Initial Guard Timer' is 300, and 'TCP Subsq Guard Timer' is 300. The 'Hint Rtcp' is set to 'enable'. The 'Algd Log Level' and 'Mbcd Log Level' are both set to 'NOTICE'. The 'Options' field is empty. There are 'OK' and 'Delete' buttons at the bottom.

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)
Hint Rtcp	<input type="checkbox"/> enable	
Algd Log Level	NOTICE	
Mbcd Log Level	NOTICE	
Options		

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The 'Configuration' tab is active, and the 'media-manager' section is selected in the left sidebar. The main area displays the 'Modify Media Manager' configuration page. The 'Media Policing' is set to 'enable'. The 'Max Signaling Bandwidth' is 100000000. The 'Max Untrusted Signaling' is 1, and the 'Min Untrusted Signaling' is 1, both with red arrows pointing to the input fields. The 'Tolerance Window' is 30, 'Untrusted Drop Threshold' is 0, 'Trusted Drop Threshold' is 0, and 'Acl Monitor Window' is 30. The 'Trap On Demote To Deny', 'Trap On Demote To Untrusted', and 'Syslog On Demote To Deny' are all set to 'enable'. There are 'OK' and 'Delete' buttons at the bottom.

Parameter	Value	Range
Media Policing	<input checked="" type="checkbox"/> enable	
Max Signaling Bandwidth	100000000	(Range: 71000..100000000)
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	
Trap On Demote To Untrusted	<input type="checkbox"/> enable	
Syslog On Demote To Deny	<input type="checkbox"/> enable	

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 three realms used in this configuration:

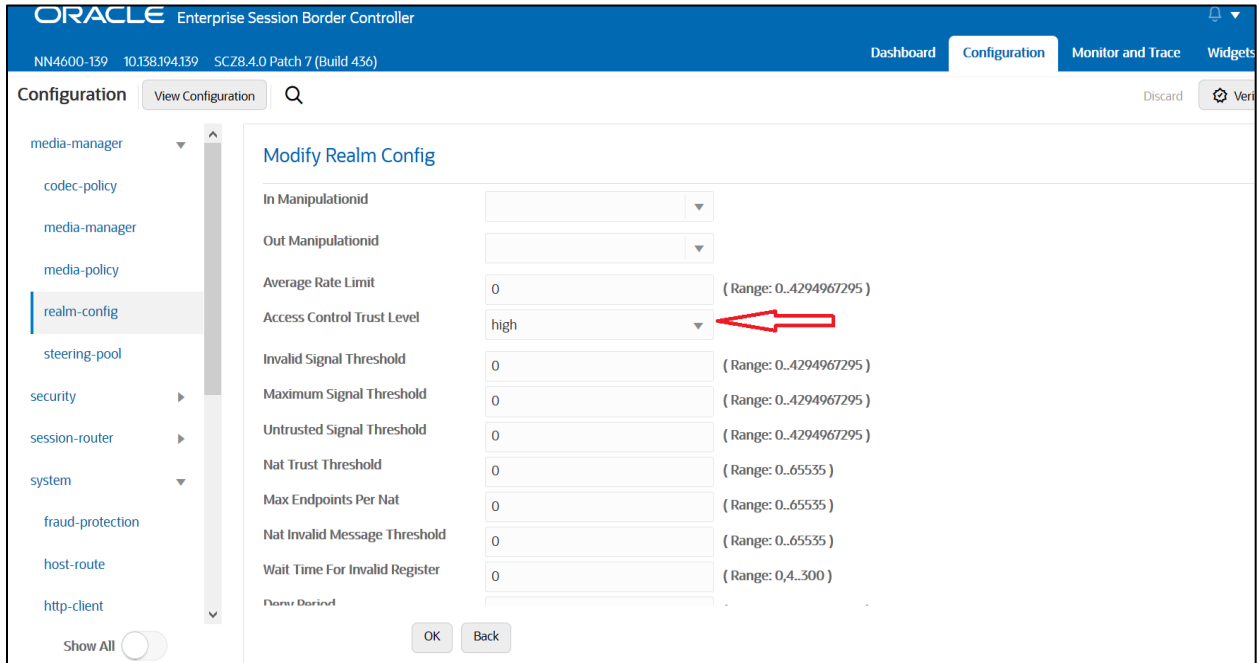
Config Parameter	Teams Realm	ECB Realm
Identifier	Teams	Avaya Realm
Network Interface	M00	M10
Mm in realm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Teams-FQDN	Telechat.o-test06161977.com	
Teams fqdn in uri	<input checked="" type="checkbox"/>	
Sdp inactive only	<input checked="" type="checkbox"/>	
Media Sec policy	sdesppolicy	RTP
RTCP mux	<input checked="" type="checkbox"/>	
ice profile	ice	
Codec policy	addCN	OptimizeCodecs
RTCP policy	rtcpGen	
Access Control Trust Level	High	High
Pai-strip	Enabled	enabled
Refer Call Transfer	Enabled	

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

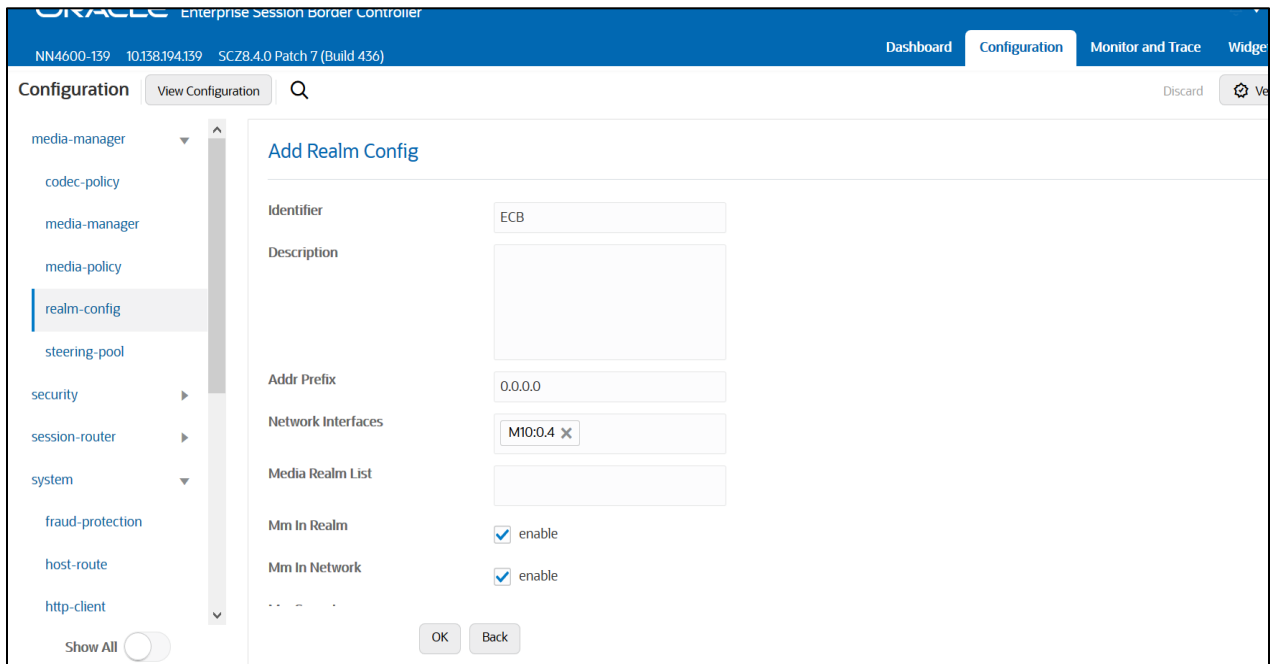
The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', system information (NN4600-139, 10.138.194.139, SC28.4.0 Patch 7 (Build 436)), and tabs for 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The 'Configuration' tab is active, and the 'realm-config' option is selected in the left-hand navigation menu. The main content area displays the 'Modify Realm Config' page for the 'Teams' realm. The configuration fields are as follows:

- Identifier: Teams
- Description: (empty text area)
- Addr Prefix: 0.0.0.0
- Network Interfaces: M00:0.4
- Media Realm List: (empty text area)
- Mm In Realm: enable
- Mm In Network: enable

At the bottom of the configuration area, there are 'OK' and 'Back' buttons.



Finally, Realm name is given as ECB for ECB Side.
Please set the Access Control Trust Level to high for this realm



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

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

6.8. 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
- inmanip-before-validate

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The left sidebar lists various configuration categories, with 'sip-config' selected. The main area is titled 'Modify SIP Config' and contains the following fields:

State	<input checked="" type="checkbox"/>	enable
Dialog Transparency	<input checked="" type="checkbox"/>	enable
Home Realm ID		Teams
Egress Realm ID		
Nat Mode		None
Registrar Domain		*
Registrar Host		*
Registrar Port		5060 (Range: 0,1025..65535)
Init Timer		500 (Range: 0..4294967295)
Max Timer		4000 (Range: 0..4294967295)

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

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface, specifically the 'Options' section of the 'Modify SIP Config' page. The left sidebar is the same as in the previous screenshot. The main area contains the following fields:

Invite Expire		180 (Range: 0..4294967295)
Session Max Life Limit		0
Enforcement Profile		
Red Max Trans		10000 (Range: 0..50000)
Options		inmanip-before-validate ✕ max-udp-length=0 ✕
SPL Options		
SIP Message Len		0 (Range: 0..65535)
Enum Sag Match	<input type="checkbox"/>	enable
Extra Method Stats	<input checked="" type="checkbox"/>	enable
Extra Enum Stats		

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.

- Tls-profile needs to match the name of the tls-profile created (Not covered in this app note)
- Set allow-anonymous to agents-only to ensure traffic to this sip-interface only comes from the particular Session agents added to the SBC.

Below is the sip-interface Configured for Teams side.

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

- State: enable
- Realm ID: Teams
- Description: (empty text area)
- SIP Ports table:

Action	Select	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addr
⋮	<input type="checkbox"/>	[highlighted]	5061	TLS	TLSTeamsCarrier	agents-only	

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

Similarly, configure sip-interface for ECB side as below

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

- State: enable
- Realm ID: ECB
- Description: (empty text area)
- SIP Ports table:

Action	Select	Address	Port	Transport Protocol	TLS Profile	Allow Anonymous	Multi Home Addr
⋮	<input type="checkbox"/>	10.232.50.65	5060	UDP		agents-only	
⋮	<input type="checkbox"/>	10.232.50.65	5060	TCP		agents-only	

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

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.

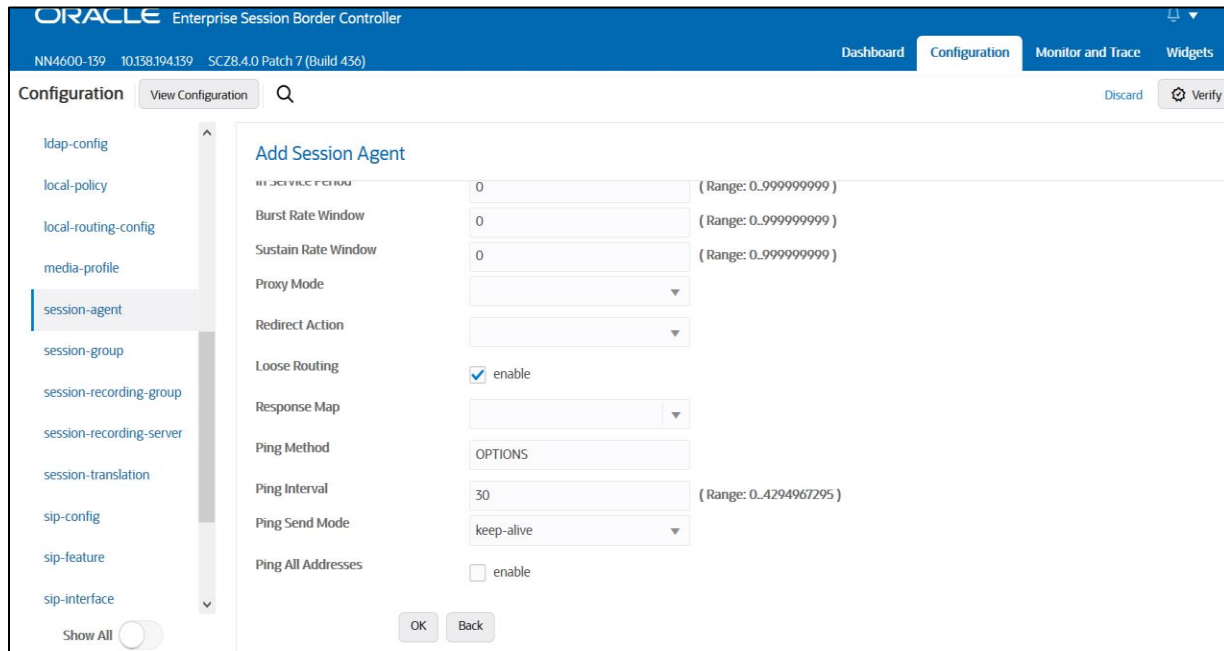
Configure the session-agent for Teams with the following parameters.
Go to session-router->Session-Agent.

- hostname to “sip.pstnhub.microsoft.com”
- port 5061
- realm-id – needs to match the realm created for Teams
- transport set to “StaticTLS”
- refer-call-transfer set to enabled
- ping-method – send OPTIONS message to Microsoft to check health
- ping-interval to 30 secs
- Refer Call Transfer set to Enabled

The screenshot shows the Oracle Enterprise Session Border Controller configuration page. The top navigation bar includes 'ORACLE Enterprise Session Border Controller', system information (NN4600-139, 10.138.194.139, SCZ8.4.0 Patch 7 (Build 436)), and tabs for 'Dashboard', 'Configuration', 'Monitor and Trace', and 'Widgets'. The 'Configuration' tab is active, and the 'session-agent' option is selected in the left-hand navigation menu. The main content area is titled 'Add Session Agent' and contains the following configuration fields:

Hostname	<input type="text" value="sip.pstnhub.microsoft.com"/>
IP Address	<input type="text"/>
Port	<input type="text" value="5061"/> (Range: 0,1025..65535)
State	<input checked="" type="checkbox"/> enable
App Protocol	<input type="text" value="SIP"/>
App Type	<input type="text"/>
Transport Method	<input type="text" value="StaticTLS"/>
Realm ID	<input type="text" value="Teams"/>
Egress Realm ID	<input type="text"/>
Description	<input type="text"/>

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



Follow above steps to create 2 more sessions for:

- sip2.pstnhub.microsoft.com
- sip3.pstnhub.microsoft.com

We also need to create Session Agent Group and sip-manipulations for Teams side which is not covered in this document.

Finally, Configure the session-agent for ECB Side which is Oracle ECB where SBC should route the calls. Go to session-router->Session-Agent.

- **Host name and IP address to 10.232.50.70 which is the ECB IP.**
- port 5060
- realm-id – needs to match the realm created for ECB Side.
- transport set to “UDP+TCP”

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-agent' selected. The main content area is titled 'Add Session Agent' and contains the following fields:

- Hostname: 10.232.50.70
- IP Address: 10.232.50.70
- Port: 5060 (Range: 0,1025..65535)
- State: enable
- App Protocol: SIP
- App Type: (empty dropdown)
- Transport Method: UDP+TCP
- Realm ID: ECB
- Egress Realm ID: (empty dropdown)
- Description: (empty text area)

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

6.11. 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 Teams to ECB Realm, use the below local -policy
Please note that the next hop is ECB IP which is 10.232.50.70

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

- From Address: * X
- To Address: * X
- Source Realm: Teams X |
- Description: (empty text area)
- State: enable
- Policy Priority: none
- Policy Attributes: (empty text area)

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

ORACLE Enterprise Session Border Controller

NN4600-139 10.138.194.139 SCZ8.4.0 Patch 7 (Build 436)

Dashboard Configuration Monitor and Trace Widgets Sys

Configuration View Configuration Q Discard Verify

local-policy

Modify Local Policy

Source Realm: Teams X

Description:

State: enable

Policy Priority: none

Policy Attributes

Action	Select	Next Hop	Realm	Action	Terminate Re...	Cost	State	App Protocol	Lookup	Ne
:	<input type="checkbox"/>	10.232.50.70	ECB	none	disabled	0	enabled		single	

OK Back

To route the calls from ECB to Teams Realm, use the below local –policy

ORACLE Enterprise Session Border Controller

NN4600-139 10.138.194.139 SCZ8.4.0 Patch 7 (Build 436)

Dashboard Configuration Monitor and Trace Widgets

Configuration View Configuration Q Discard Verify

local-policy

Add Local Policy

From Address: * X

To Address: * X

Source Realm: ECB X

Description:

State: enable

Policy Priority: none

Policy Attributes

OK Back

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 'local-policy' selected. The main content area is titled 'Modify Local Policy' and contains the following fields:

- Source Realm: ECB
- Description: (empty text area)
- State: enable
- Policy Priority: none
- Policy Attributes: A table with columns for Action, Select, Next Hop, Realm, Action, Terminate Re..., Cost, State, App Protocol, and Lookup.

Action	Select	Next Hop	Realm	Action	Terminate Re...	Cost	State	App Protocol	Lookup
:	<input type="checkbox"/>	sag:TeamsGrp	Teams	none	disabled	0	enabled		single

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

6.12. Configure steering-pool

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

Teams side steering pool.

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

- IP Address: (empty text input)
- Start Port: 10000 (Range: 0,1.65535)
- End Port: 20000 (Range: 0,1.65535)
- Realm ID: Teams
- Network Interface: (empty dropdown)

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

ECB side steering pool.

The screenshot shows the Oracle Enterprise Session Border Controller configuration interface. The top navigation bar includes the Oracle logo, the product name 'Enterprise Session Border Controller', and the version 'SC78.4.0 Patch 7 (Build 436)'. The main menu has 'Dashboard', 'Configuration', and 'Monitor and Trace'. The 'Configuration' section is active, and the 'steering-pool' option is selected in the left-hand navigation pane. The main content area displays the 'Add Steering Pool' form with the following fields:

IP Address	10.232.50.65
Start Port	30000 (Range: 0,1.65535)
End Port	40000 (Range: 0,1.65535)
Realm ID	ECB
Network Interface	

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

With this, SBC configuration is complete

7. 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](#)
- [New steering-pools](#)
- [New local-policy](#)

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

8. Verification of Sample Call flows

Once the configuration is complete, we can try making sample calls and can check the signaling path and the call trace details as below:

1. Make Call from Teams User to IP-PBX user (CUCM user) using ECB LDAP config and check the call flow. The Call from Teams reaches SBC and then routed to ECB IP in below trace.

Monitor and Trace

Sessions

Registrations

Subscriptions

Notable Events

Session List [b581b25f4bf25aa5bd232ef47f01da84](#) ✕

[*] Session Summary			
52.114.148.0		10.232.50.65	10.232.50.70
2021-09-17 03:55:11.120	→	INVITE (1)	→
2021-09-17 03:55:11.120	←	Status:100 (1)	←
2021-09-17 03:55:11.122		MEDIA FLOW ADD, ID=134217731, DIRECTION=CALLING	
2021-09-17 03:55:11.122		MEDIA FLOW ADD, ID=134217732, DIRECTION=CALLED	
2021-09-17 03:55:11.123		EGRESS ROUTE, TYPE=local-policy, NEXT HOP=<sip:+18507904044@10.232.50.70:5060;user=phone>	
2021-09-17 03:55:11.123			→ INVITE (1)
2021-09-17 03:55:11.134			← Status:100 (1)
2021-09-17 03:55:11.241			← Status:180 (1)
2021-09-17 03:55:11.242	←	Status:180 (1)	←
2021-09-17 03:55:13.409			← Status:200 (1)
2021-09-17 03:55:13.411		MEDIA FLOW MODIFY, ID=134217732, DIRECTION=CALLED	
2021-09-17 03:55:13.411		MEDIA FLOW MODIFY, ID=134217731, DIRECTION=CALLING	
2021-09-17 03:55:13.411	←	Status:200 (1)	←
2021-09-17 03:55:13.524	→	ACK (1)	→
2021-09-17 03:55:13.524			→ ACK (1)

Refresh Export diagram Export session details

The call reaches ECB IP and then ECB does LDAP search and then routes the call to CUCM IP. Then the call reaches CUCM and then the call is established as in below trace.

Monitor and Trace

Sessions

Registrations

Subscriptions

Notable Events

Session List [b581b25f4bf25aa5bd232ef47f01da84](#) ✕

[*] Session Summary			
10.232.50.65		10.232.50.70	10.232.50.89
2021-09-17 00:06:27.752	→	INVITE (1)	→
2021-09-17 00:06:27.754	←	Status:100 (1)	←
2021-09-17 00:06:27.809		EGRESS ROUTE, TYPE=ecb, NEXT HOP=10.232.50.89:5060/UDP	
2021-09-17 00:06:27.809			→ INVITE (1)
2021-09-17 00:06:27.818			← Status:100 (1)
2021-09-17 00:06:27.851			← Status:180 (1)
2021-09-17 00:06:27.860	←	Status:180 (1)	←
2021-09-17 00:06:30.018			← Status:200 (1)
2021-09-17 00:06:30.028	←	Status:200 (1)	←
2021-09-17 00:06:30.153	→	ACK (1)	→
2021-09-17 00:06:30.158			→ ACK (1)
2021-09-17 00:06:38.233			← BYE (101)
2021-09-17 00:06:38.243	←	BYE (101)	←
2021-09-17 00:06:42.690	→	BYE (2)	→
2021-09-17 00:06:42.696			→ BYE (2)

Refresh Export diagram Export session details

2. Make Call from CUCM user to Teams User using ECB LDAP config and check the call flow. The Call from CUCM user reaches ECB first and ECB does LDAP query and sends call to SBC interface IP as given below.

Monitor and Trace

Sessions

Registrations

Subscriptions

Notable Events

Session List [7c4c5880-14415a7e-c9fb-5932e80a@10.232.50.89](#) x

[+] Session Summary		
10.232.50.89	10.232.50.70	10.232.50.65
2021-09-17 02:33:41.983	→ INVITE (101)	→
2021-09-17 02:33:41.984	← Status:100 (101)	←
2021-09-17 02:33:42.029	EGRESS ROUTE, TYPE=ecb, NEXT HOP=10.232.50.65:5060/UDP	
2021-09-17 02:33:42.029	→ INVITE (101)	→
2021-09-17 02:33:42.037	← Status:100 (101)	←
2021-09-17 02:33:42.370	← Status:180 (101)	←
2021-09-17 02:33:42.377	← Status:180 (101)	←
2021-09-17 02:33:43.349	← Status:180 (101)	←
2021-09-17 02:33:43.357	← Status:180 (101)	←
2021-09-17 02:33:43.711	← Status:180 (101)	←
2021-09-17 02:33:43.719	← Status:180 (101)	←
2021-09-17 02:33:45.807	← Status:180 (101)	←
2021-09-17 02:33:45.815	← Status:180 (101)	←
2021-09-17 02:33:51.055	← Status:200 (101)	←
2021-09-17 02:33:51.067	← Status:200 (101)	←

Refresh Export diagram Export session details

When Call reaches SBC IP, Call is then routed to Teams User and the call gets established as shown in the below trace.

Monitor and Trace

Sessions

Registrations

Subscriptions

Notable Events

Session List [2f688200-144159fd-c9fb0-5932e80a@10.232.50.89](#) x

[+] Session Summary		
10.232.50.70	10.232.50.65	52.114.132.46
2021-09-17 06:20:17.154	→ INVITE (101)	→
2021-09-17 06:20:17.154	← Status:100 (101)	←
2021-09-17 06:20:17.156	MEDIA FLOW ADD, ID=167772167, DIRECTION=CALLING	
2021-09-17 06:20:17.156	MEDIA FLOW ADD, ID=167772168, DIRECTION=CALLED	
2021-09-17 06:20:17.156	EGRESS ROUTE, TYPE=local-policy, NEXT HOP=<sip:17814437248@sip.pstnhub.microsoft.com:5061;transport=tls>	
2021-09-17 06:20:17.156	→ INVITE (101)	→
2021-09-17 06:20:17.249	← Status:100 (101)	←
2021-09-17 06:20:17.628	← Status:180 (101)	←
2021-09-17 06:20:17.628	← Status:180 (101)	←
2021-09-17 06:20:20.204	← Status:180 (101)	←
2021-09-17 06:20:20.204	← Status:180 (101)	←
2021-09-17 06:20:20.218	← Status:180 (101)	←
2021-09-17 06:20:20.218	← Status:180 (101)	←
2021-09-17 06:20:20.218	← Status:180 (101)	←
2021-09-17 06:20:20.218	← Status:180 (101)	←
2021-09-17 06:20:24.766	← Status:180 (101)	←
2021-09-17 06:20:24.766	← Status:180 (101)	←
2021-09-17 06:20:31.247	← Status:200 (101)	←
2021-09-17 06:20:31.248	MEDIA FLOW MODIFY, ID=167772168, DIRECTION=CALLED	

Refresh Export diagram Export session details

- Make Call from Teams User to On premise IP-PBX user and check the ECB LDAP parallel forking call flow as shown below. The Call from Teams User reaches SBC and then routed to ECB as shown below.

Monitor and Trace

Sessions

Registrations

Subscriptions

Notable Events

Session List: [fcc8d0f393985fcda1473e2e110aafc9](#)

[+] Session Summary

Time	IP 1	IP 2	IP 3	IP 4
2021-09-17 05:47:10.663	→	INVITE (1)	→	
2021-09-17 05:47:10.664	←	Status:100 (1)	←	
2021-09-17 05:47:10.666		MEDIA FLOW ADD, ID=50331655, DIRECTION=CALLING		
2021-09-17 05:47:10.666		MEDIA FLOW ADD, ID=50331656, DIRECTION=CALLED		
2021-09-17 05:47:10.666		EGRESS ROUTE, TYPE=local-policy, NEXT HOP=<sip:+18507904044@10.232.50.70:5060;user=phone>		
2021-09-17 05:47:10.666			→	INVITE (1)
2021-09-17 05:47:10.680			←	Status:100 (1)
2021-09-17 05:47:10.764			←	Status:180 (1)
2021-09-17 05:47:10.764	←	Status:180 (1)		
2021-09-17 05:47:10.793			←	Status:180 (1)
2021-09-17 05:47:10.794	←	Status:180 (1)		
2021-09-17 05:47:16.085			←	Status:200 (1)
2021-09-17 05:47:16.086		MEDIA FLOW MODIFY, ID=50331656, DIRECTION=CALLED		
2021-09-17 05:47:16.086		MEDIA FLOW MODIFY, ID=50331655, DIRECTION=CALLING		
2021-09-17 05:47:16.087	←	Status:200 (1)		

Refresh Export diagram Export session details

The Call now reaches ECB and it does LDAP parallel forking and sends calls to both Avaya and CUCM User and when Avaya User attends the call, ECB sends CANCEL to CUCM user as shown below.

Monitor and Trace

Sessions

Registrations

Subscriptions

Notable Events

Session List: [fcc8d0f393985fcda1473e2e110aafc9](#)

[+] Session Summary

Time	IP 1	IP 2	IP 3	IP 4
2021-09-17 01:58:26.485	→	INVITE (1)	→	
2021-09-17 01:58:26.487	←	Status:100 (1)	←	
2021-09-17 01:58:26.534		EGRESS ROUTE, TYPE=ecb, NEXT HOP=10.232.50.89:5060/UDP		
2021-09-17 01:58:26.534			→	INVITE (1)
2021-09-17 01:58:26.547		EGRESS ROUTE, TYPE=ecb, NEXT HOP=10.232.50.127:5060/UDP		
2021-09-17 01:58:26.547			→	INVITE (1)
2021-09-17 01:58:26.558			←	Status:100 (1)
2021-09-17 01:58:26.561			←	Status:180 (1)
2021-09-17 01:58:26.569	←	Status:180 (1)		
2021-09-17 01:58:26.572			←	Status:100 (1)
2021-09-17 01:58:26.587			←	Status:180 (1)
2021-09-17 01:58:26.598	←	Status:180 (1)		
2021-09-17 01:58:31.864			←	Status:200 (1)
2021-09-17 01:58:31.872			→	CANCEL (1)
2021-09-17 01:58:31.888	←	Status:200 (1)		

Refresh Export diagram Export session details

Monitor and Trace

Sessions

Registrations

Subscriptions

Notable Events

Session List [fcc8d0f393985fcd1473e2e110aafc9](#) x

2021-09-17 01:58:26.534		→ INVITE (1) →	
2021-09-17 01:58:26.547	EGRESS ROUTE, TYPE=ecb, NEXT HOP=10.232.50.127:5060/UDP		
2021-09-17 01:58:26.547		→ INVITE (1) →	
2021-09-17 01:58:26.558		← Status:100 (1) ←	
2021-09-17 01:58:26.561		← Status:180 (1) ←	
2021-09-17 01:58:26.569	← Status:180 (1) ←		
2021-09-17 01:58:26.572		← Status:100 (1) ←	
2021-09-17 01:58:26.587		← Status:180 (1) ←	
2021-09-17 01:58:26.598	← Status:180 (1) ←		
2021-09-17 01:58:31.864		← Status:200 (1) ←	
2021-09-17 01:58:31.872		→ CANCEL (1) →	
2021-09-17 01:58:31.888	← Status:200 (1) ←		
2021-09-17 01:58:31.893		← Status:200 (1) ←	
2021-09-17 01:58:31.895	CALL FAILURE!! STATUS=487, REASON=Request Terminated		
2021-09-17 01:58:31.895		← Status:487 (1) ←	
2021-09-17 01:58:31.897		→ ACK (1) →	
2021-09-17 01:58:32.015	→ ACK (1) →		
2021-09-17 01:58:32.020		→ ACK (1) →	

Refresh Export diagram Export session details

We can also make calls using ECB ATG config parallel forking using the configuration given in this document. The call trace looks similar to the above call trace from SBC and ECB point of view and so we did not add the call trace for the ECB ATG config scenario.

We can also make calls to auto-attendant (Either to Teams – towards SBC side or to On Premise IP-PBX - Core side) as one of the DIDs along with other normal Phone number DIDs using the ECB ATG parallel forking configuration. We need to add auto-attendant DID in the User Entry of the ECB config. Only thing to remember here is we need to assign the same number assigned to auto-attendant to other PBX users involved in ECB ATG parallel forking configuration.

Appendix A

Following are the test cases that are executed as part of Oracle ECB and SBC integration interworking with on premise IP-PBX and MS Teams

Serial Number	Test Cases Executed	Result
1	Teams User calling On premise IP-PBX user (Avaya/CUCM/Genesys) using ECB LDAP feature	Pass
2	On premise IP-PBX user (Avaya/CUCM/Genesys) calling Teams User using ECB LDAP feature	Pass
3	Teams User calling On premise IP-PBX user (Avaya/CUCM/Genesys) using ECB LDAP parallel forking feature	Pass
4	Testing Oracle ECB ATG parallel forking by making calls to Core side User (On Premise IP-PBX User) and SBC side user (Teams User)	Pass
5	Testing Oracle ECB ATG parallel forking by making calls to Core side User (On Premise IP-PBX User) and Teams side auto attendant	Pass
6	Testing Oracle ECB ATG parallel forking by making calls to Core side User and voice mail profile (On Premise IP-PBX User)	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