



Oracle Enterprise Communications Broker &  
Oracle Enterprise Session Border Controller  
with Avaya's Aura 6.3 & Aura 7.0, Cisco's  
UCM 10.5 & UCM 11.0, Microsoft's Lync 2013  
& Skype for Business

Technical Application Note




## Disclaimer

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

## Table of Contents

<b>INTENDED AUDIENCE.....</b>	<b>6</b>
<b>DOCUMENT OVERVIEW .....</b>	<b>6</b>
<b>INTRODUCTION.....</b>	<b>7</b>
REQUIREMENTS.....	7
• ORACLE ENTERPRISE COMMUNICATIONS BROKER PCZ2.0.0 MR-2 PATCH 1 .....	7
• ORACLE ENTERPRISE SESSION BORDER CONTROLLER ECZ7.3.0 MR-1.....	7
• MICROSOFT LYNC 2013 AND/OR SKYPE FOR BUSINESS 2015 .....	7
• AVAYA AURA 6.3 AND/OR 7.0.....	7
• CISCO UNIFIED COMMUNICATIONS MANAGER 10.5 AND/OR 11.0 .....	7
LAB CONFIGURATION .....	8
<b>PHASE 1 – CONFIGURING THE ORACLE ECB.....</b>	<b>9</b>
RUNNING SETUP.....	10
LOGGING IN THE ECB.....	13
CONFIGURING THE ECB .....	14
System Settings.....	15
Configure SIP Interfaces.....	18
Configure Header Manipulation Rules (HMR).....	20
Configure Dial Plan.....	40
Configure Agents.....	47
Configure Users.....	56
Configure Routing.....	58
Configure LDAP Integration with Active Directory .....	61
Save and activate the configuration .....	67
<b>PHASE 2 – CONFIGURING THE ORACLE ENTERPRISE SBC.....</b>	<b>69</b>
IN SCOPE.....	69
OUT OF SCOPE .....	69
WHAT WILL YOU NEED.....	69
SBC- GETTING STARTED .....	69
Establish the serial connection and logging in the SBC.....	70
Initial Configuration – Assigning the management Interface an IP address .....	70
CONFIGURING THE SBC .....	71
High Availability .....	71
Local Policies.....	71
Media Manager.....	72
Network Interfaces.....	73
Physical Interfaces.....	76
Realm Configs .....	77
Redundancy Config (HA Pairs Only) .....	81
Session Agents.....	82
Session Translation .....	85
SIP Config.....	85
SIP Feature.....	86
SIP Interfaces .....	86
SIP Manipulations (Header Manipulation Rules – HMR) .....	90
SIP Monitoring.....	91
Steering Pools .....	91

System Config .....	91
Translation Rules .....	92
Web Server Config .....	93
Save, Activate, and Reboot .....	93
<b>PHASE 3 – CONFIGURING ACTIVE DIRECTORY FOR LDAP INTEGRATION WITH THE ECB .....</b>	<b>94</b>
ADDING A USER’S PHONE NUMBER(S) TO ACTIVE DIRECTORY .....	94
<b>PHASE 4 – CONFIGURING THE LYNC 2013 SERVER .....</b>	<b>99</b>
ADDING THE ECB AS A PSTN GATEWAY .....	99
CREATING A ROUTE WITHIN THE LYNC SERVER INFRASTRUCTURE .....	106
<b>PHASE 5 – CONFIGURING THE SKYPE FOR BUSINESS SERVER .....</b>	<b>115</b>
ADDING THE ECB AS A PSTN GATEWAY .....	115
CREATING A ROUTE WITHIN THE SKYPE FOR BUSINESS INFRASTRUCTURE.....	121
<b>PHASE 6 – CONFIGURING THE AVAYA SESSION MANAGER 6.3.....</b>	<b>132</b>
ADDING THE ECB AS A SIP ENTITY .....	132
CONFIGURING AN ENTITY LINK BETWEEN ECB AND SESSION MANAGER .....	134
CREATING A ROUTING POLICY TO ASSIGN THE APPROPRIATE ROUTING DESTINATION .....	135
<b>PHASE 7 – CONFIGURING THE AVAYA SESSION MANAGER 7.0.....</b>	<b>136</b>
ADDING THE ECB AS A SIP ENTITY .....	136
CONFIGURING AN ENTITY LINK BETWEEN ECB AND SESSION MANAGER .....	138
CREATING A ROUTING POLICY TO ASSIGN THE APPROPRIATE ROUTING DESTINATION .....	139
<b>PHASE 8 – CONFIGURING CISCO UNIFIED COMMUNICATIONS MANAGER 10.5 .....</b>	<b>140</b>
CONFIGURING THE SIP TRUNK SECURITY PROFILE.....	140
CONFIGURING THE SIP PROFILE .....	143
CONFIGURING THE TRUNK .....	146
CONFIGURING THE ROUTE PATTERN.....	149
<b>PHASE 9 – CONFIGURING CISCO UNIFIED COMMUNICATIONS MANAGER 11.0 .....</b>	<b>152</b>
CONFIGURING THE SIP TRUNK SECURITY PROFILE.....	152
CONFIGURING THE SIP PROFILE .....	155
CONFIGURING THE TRUNK .....	158
CONFIGURING THE ROUTE PATTERN.....	161
<b>TEST PLAN &amp; RESULTS.....</b>	<b>165</b>
TEST PLAN .....	165
<b>SOFTWARE VERSIONS USED .....</b>	<b>183</b>
<b>TROUBLESHOOTING TOOLS .....</b>	<b>184</b>
MICROSOFT NETWORK MONITOR (NETMON).....	184
WIRESHARK.....	184
EVENTVIEWER.....	184
ON THE ORACLE ECB AND E-SBC.....	184
Resetting the statistical counters, enabling logging and restarting the log files .....	184
Examining the log files.....	184
Through the Web GUI.....	185
TELNET .....	185
CISCO REAL-TIME MONITORING TOOL (RTMT).....	185
<b>APPENDIX A .....</b>	<b>186</b>
ACCESSING THE ACLI.....	186



ACLI BASICS .....	186
CONFIGURATION ELEMENTS .....	188
CREATING AN ELEMENT.....	188
EDITING AN ELEMENT.....	188
DELETING AN ELEMENT.....	189
CONFIGURATION VERSIONS.....	189
SAVING THE CONFIGURATION .....	189
ACTIVATING THE CONFIGURATION .....	190



## Intended Audience

This is a technical document intended for telecommunications engineers with the purpose of configuring the Oracle Communications Enterprise-SBC, Enterprise Communications Broker, Microsoft Lync and Skype for Business, Avaya Aura Session Manager and Cisco Unified Communications Manager. There will be steps that require navigating Microsoft Windows Server as well as the Acme Packet Command Line Interface (ACLI). Understanding the basic concepts of TCP/UDP, IP/Routing, and SIP/RTP are also necessary to complete the configuration and for troubleshooting, if necessary.

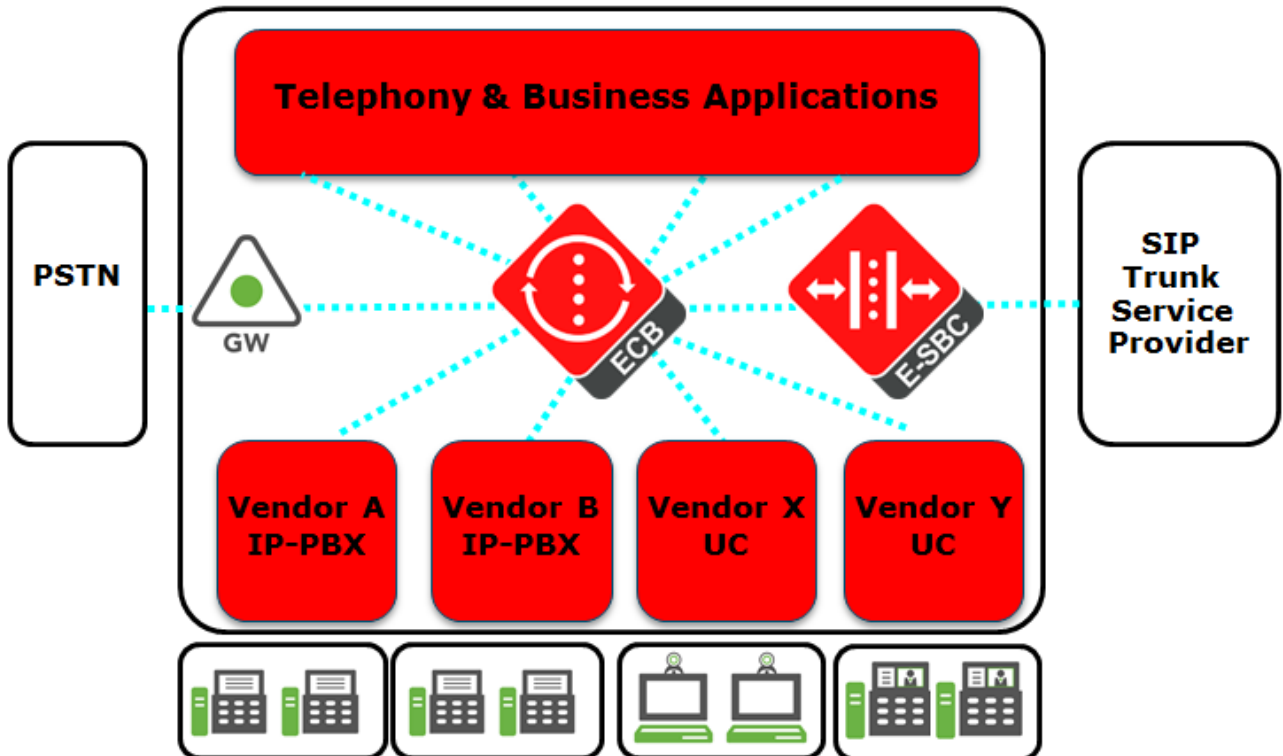
## Document Overview

This technical application note documents the implementation of the Oracle Enterprise Communications Broker (Oracle ECB) in an Enterprise network consisting of multi-vendor Unified Communications platforms - Microsoft Lync 2013, Microsoft Skype for Business 2015, Avaya Aura Session Manager and Cisco Unified Communications Manager - connecting to a SIP trunk through an Enterprise Session Border Controller.

## Introduction

### Enterprise Communications Broker Overview

The Oracle ECB is an enterprise-class, core signaling component designed to simplify communications networks. It combines innovative approaches toward dial plan management and SIP topology-aware routing with a purpose-built, intuitive GUI interface. While at its best in signaling environments comprised of products and solutions from multiple vendors, it is useful for consolidating policy enforcement decisions, integrating third-party applications, and managing a network-wide routing topology even in homogenous architectures.



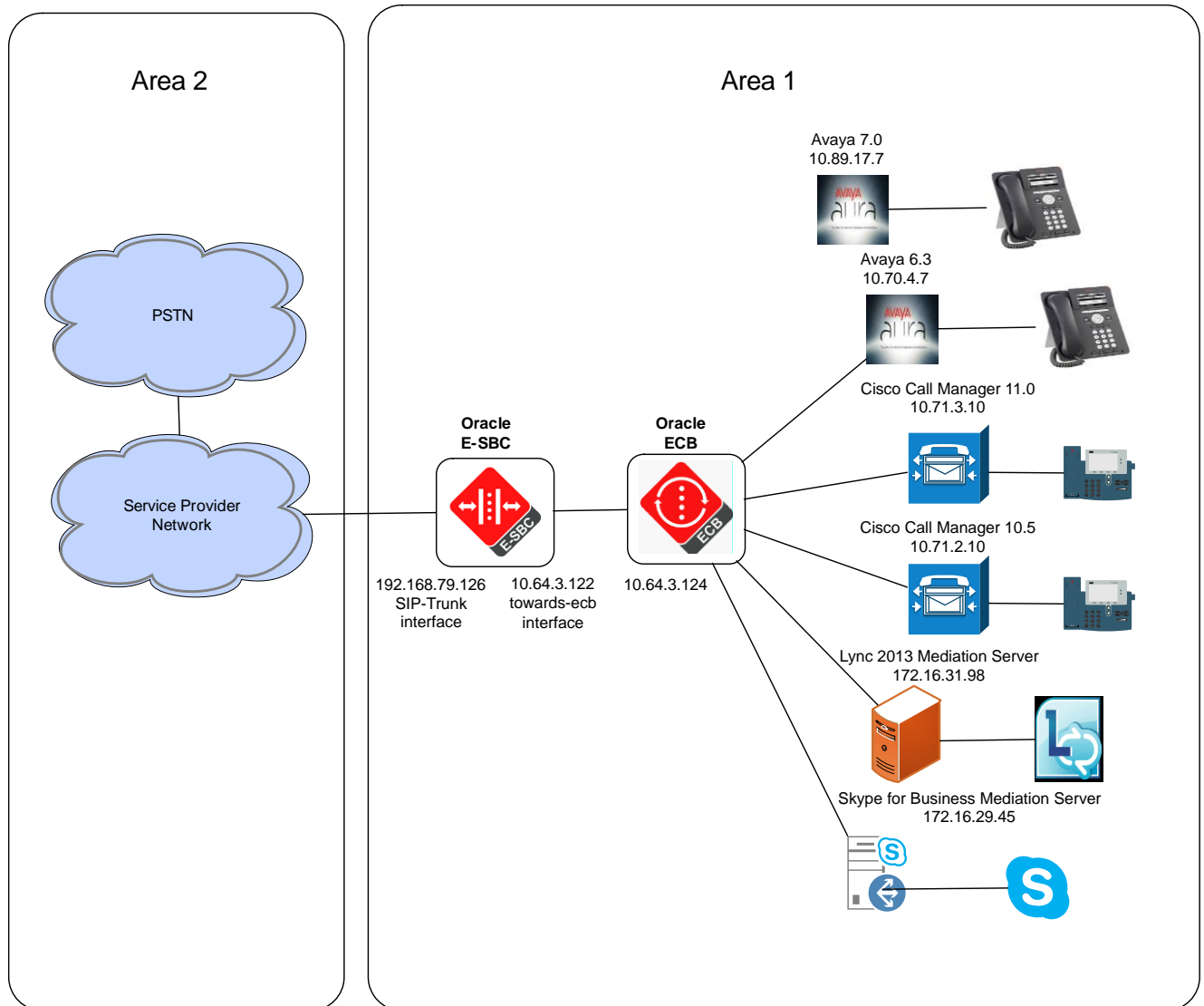
The Oracle ECB is typically deployed in the core of a multi-vendor communications network where multiple UC, PBX and service provider trunk interfaces must be interconnected. It normalizes communications between disparate premise-based systems and connects them to service provider networks and hosted applications through E-SBCs.

### Requirements

- Oracle Enterprise Communications Broker PCZ2.0.0 MR-2 Patch 1
- Oracle Enterprise Session Border Controller ECZ7.3.0 MR-1
- Microsoft Lync 2013 and/or Skype for Business 2015
- Avaya Aura 6.3 and/or 7.0
- Cisco Unified Communications Manager 10.5 and/or 11.0

## Lab Configuration

The following diagram illustrates the lab environment created by tekVizion to facilitate certification testing. tekVizion is a systems integrator specifically dedicated to the telecommunications industry. Their core services include consulting/solution design, interoperability/verification testing, integration, custom software development and solution support services.



The network architecture consists of two areas. Area 1 represents the Enterprise network and Area 2 is the service provide network. The Enterprise network has the ECB at its core connecting together multiple UC platforms. The ECB connects to the Enterprise SBC which provides the Enterprise network access to the PSTN through the service provider network.

The configuration, validation and troubleshooting of the Area 1 is the focus of this document and will be described in nine phases:

- Phase 1 – Configuring the Oracle ECB
- Phase 2 – Configuring the Oracle E-SBC
- Phase 3 – Configuring Active Directory for LDAP Integration with the ECB
- Phase 4 – Configuring the Lync 2013 server
- Phase 5 – Configuring the Skype for Business server



- Phase 6 – Configuring the Avaya Aura Session Manager 6.3
- Phase 7 – Configuring the Avaya Aura Session Manager 7.0
- Phase 8 – Configuring the Cisco Unified Communications Manager 10.5
- Phase 9 – Configuring the Cisco Unified Communications Manager 11.0

## Phase 1 – Configuring the Oracle ECB

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 setup via the CLI.

### Connecting to the ECB

The CLI can be accessed through the console connection. If the ECB is appliance based, you can connect to the ECB via a VGA monitor and USB keyboard.

Power the ECB on. Upon successful boot, the system prompts you to login. The default password for user mode is “acme” and super user mode is “packet”.

You can now use the installation wizard to setup your ECB. Using the wizard, you can enable the Web Server, set management access as well as configure high availability and service interface addressing.

```
Password: acme
ORACLE> enable
Password: packet
```

## Running Setup

The following steps detail the process of using the installation wizard to configure the base setup of the ECB

1. Start the installation wizard by entering the command `run setup` in super user mode.

```
ORACLE# run setup
```

The following displays

```
-----  
Thank you for purchasing the Oracle ECB. The following short wizard  
will guide you through the initial set-up.  
-----  
'?' = Help; '.' = Clear; 'q' = Exit  
CONFIGURATION  
WARNING: Proceeding with wizard will result in existing configuration  
being erased.  
Erase config and proceed (yes/no) [no] : yes
```

2. Type yes and press Enter

```
Configuration will be backed up as  
bkup_setup_wizard_Apr_8_13_25_49_632.gz  
'-' = Previous; '?' = Help; '.' = Clear; 'q' = Exit  
HIGH AVAILABILITY  
This ECB may be a standalone or part of a highly available redundant  
pair.  
Oracle ECB mode  
1 - standalone  
2 - high availability  
Enter choice [1 - standalone] : 1
```

3. Our setup consists of a standalone server. Type 1 and hit Enter
4. You will then be asked to configure a unique target name, the IP address, subnet mask and gateway of the management interface of the ECB. Please note at any time during configuration if you would like to keep the default values (values mentioned in [ ]), press Enter.

```
Unique target name of this ECB [primary] : ECB-Oracle  
IP address on management interface [172.30.200.111] : 172.18.255.82  
Subnet mask on management interface [255.255.0.0] :  
Gateway IP address on management interface [172.18.0.1] :
```

5. You will then see a prompt to configure your sip-interface. This step is required; the system does not allow you to proceed without making a setting. When prompted enter the IP address, subnet mask and gateway IP address of the sip-interface.

```
IP address on SIP interface : 10.64.3.124  
Subnet mask on SIP interface [255.255.255.0] : 255.255.0.0  
Gateway IP address on SIP interface : 10.64.1.1
```

6. The prompt to setup the system timezone will display

```
SETUP TIMEZONE Setup system timezone (yes/no) [yes] : yes
```

Type your response and press Enter.

7. You will then be asked to enter the number for sessions purchased for the ECB. Type your response and press Enter.

```
LICENSED SESSIONS
Number of licensed sessions           : 400
```

You will see the following message prompting to save the settings before proceeding to the timezone setup.

```
Enter 1-20 to modify, 'd' to display summary, 's' to save, 'q' to
exit.[s]:
Saving changes and quitting wizard. Are you sure? [y/n]?:
```

8. Type your response and press Enter.

```
SETUP TIMEZONE Setup system timezone (yes/no) [yes] : yes
```

The following message displays

```
Deleting configuration
Erase-Cache received, processing.
waiting 1200 for request to finish
Request to 'ERASE-CACHE' has Finished,
Erase-Cache: Completed
Running timezone setup application
Calling tzselect. Use ^D to cancel without save
Please identify a location so that time zone rules can be set
correctly.
Please select a continent or ocean.
1) Africa
2) Americas
3) Antarctica
4) Arctic Ocean
5) Asia
6) Atlantic Ocean
7) Australia
8) Europe
9) Indian Ocean
10) Pacific Ocean
11) none - I want to specify the time zone using the Posix TZ format.
#??
```

Type your response, for example, 2 for Americas and press Enter. The system lists applicable countries in the Americas. Make your selection and press Enter. The system displays applicable timezones. Make your selection. The following message appears

```
The following information has been given:
United States
Eastern Time
Therefore TZ='America/New_York' will be used.
Local time is now: Thu Apr 11 10:13:38 EDT 2014.
Universal Time is now: Thu Apr 11 14:13:38 UTC 2014.
```

Is the above information OK?

1) Yes

2) No

#?

9. Type 1 and then hit Enter. You will be then shown a summary of your settings.

```
Saved configuration. -----
HIGH AVAILABILITY
 2 : ECB mode                : standalone
 3 : ECB role                 : N/A

AUTOMATIC CONFIGURATION
 6 : Acquire config from the Primary (yes/no) : N/A

ECB SETTINGS
 7 : Unique target name of this ECB          : ECB-Oracle
 8 : Management interface IP address         : 172.18.255.82
 9 : Management interface subnet mask       : 255.255.0.0
10: Management interface gateway IP address : 172.18.0.1
11: SIP interface VLAN id                   : 0
12: SIP interface IP address                : 10.64.3.124
15: SIP interface subnet mask               : 255.255.0.0
16: SIP interface gateway IP address        : 10.64.1.1

PEER CONFIGURATION
18: Peer target name                       : N/A

SETUP TIMEZONE
19: Setup system timezone (yes/no)         : yes

LICENSED SESSIONS
20: Number of licensed sessions            : 400

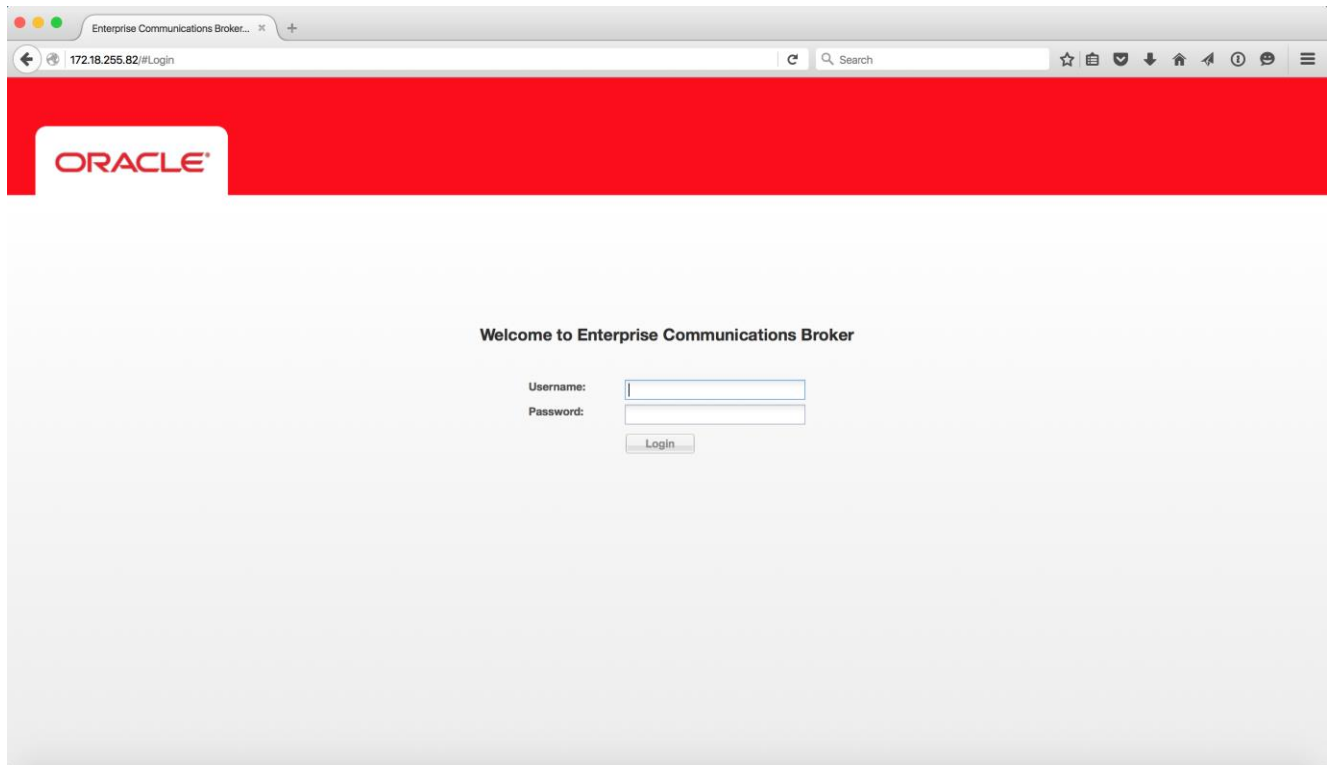
You may access the GUI via http://172.18.255.82:80/ or continue using
the acli after reboot.
```

## Logging in 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.



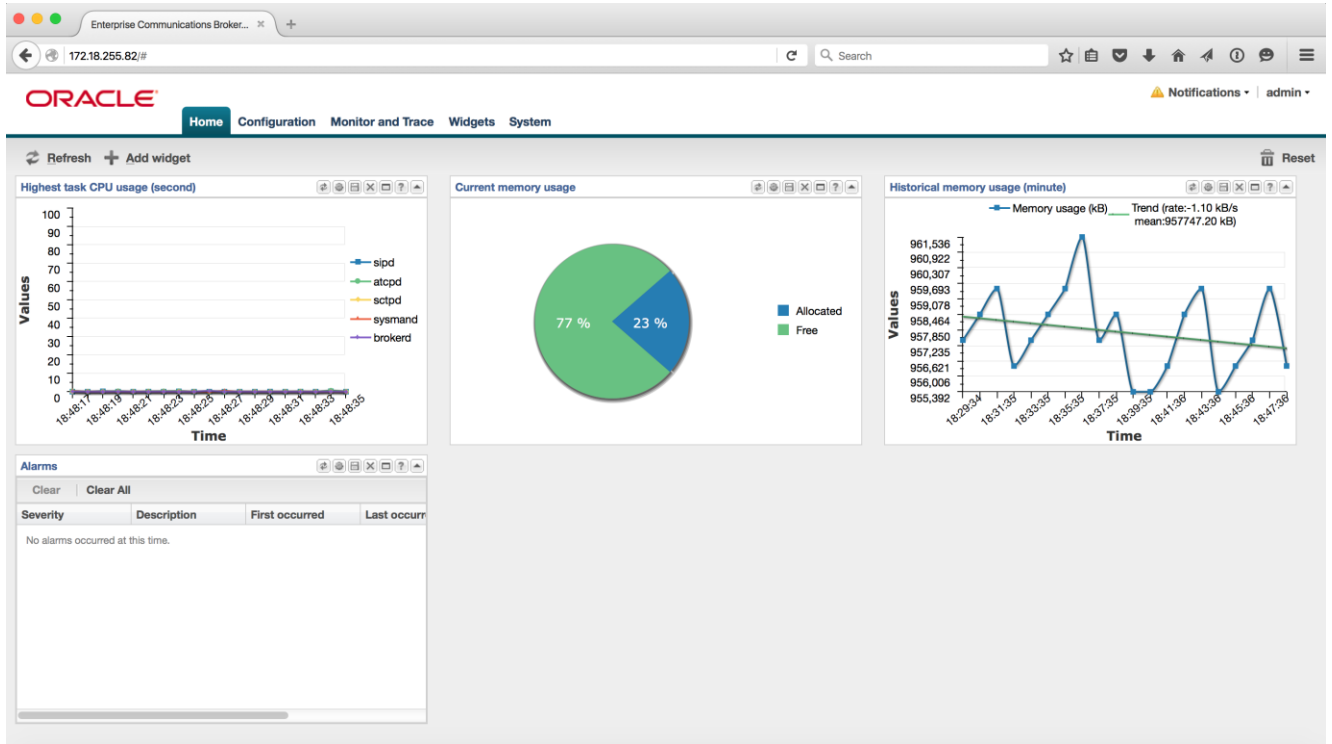
Enter your GUI username and password. The default username for the User level is "user" and the default password is "acme".

The default username for an Administrator level is "admin", and the default password is "packet".

## Configuring the ECB

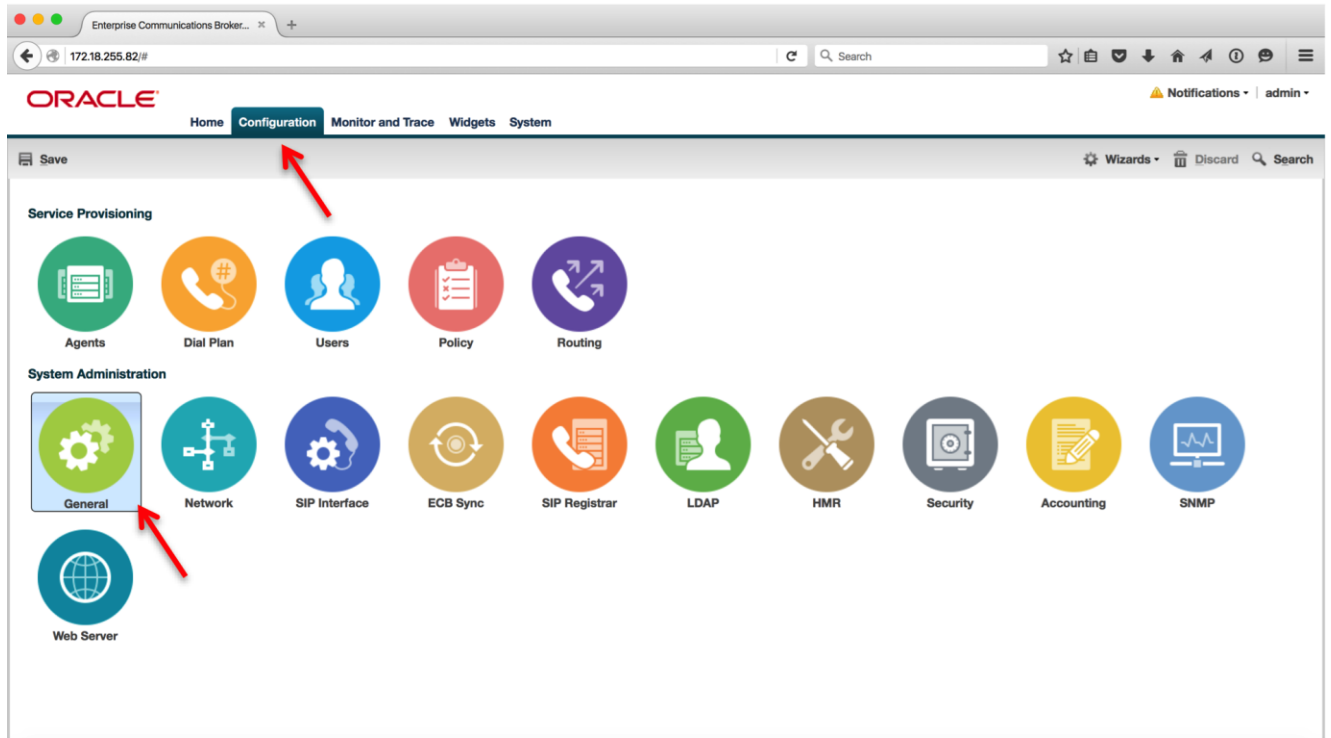
After logging into the ECB, the **Home** screen will be displayed. The Oracle ECB GUI has five tabs across the top – **Home**, **Configuration**, **Monitor and Trace**, **Widgets** and **System**.

The **Home** tab as shown below contains a configurable dashboard displaying the system statistics.



## System Settings

Select the **Configuration** tab. This tab displays the configurable elements in the ECB in two sections – **Service Provisioning** and **System Administration**. Click on the **General** icon under **System Administration**.



The Modify System Settings page is displayed.

**Modify System settings**

Hostname:

Description:

Location:

Default gateway IP address:

Enable restart on critical failure:

Console session timeout:  (Range: 0..65535)

Telnet session timeout:  (Range: 0..65535)

Enable SIP monitoring and tracing:

NTP servers: 

Add	Edit	Delete
-----	------	--------

Logging settings

SNMP settings

Denial of service settings

Communications monitoring probe settings

Expand the **Logging settings** section.

**Modify System settings**

Default gateway IP address:

Enable restart on critical failure:

Console session timeout:  (Range: 0..65535)

Telnet session timeout:  (Range: 0..65535)

Enable SIP monitoring and tracing:

NTP servers: 

Add	Edit	Delete
-----	------	--------

**Logging settings**

SysLog server IP address:

SysLog server port:  (Range: 0..65535)

SysLog facility:  (Range: 0..99999999)

Process log level:

SNMP settings



Process log level is set at **NOTICE**. Change the setting to **DEBUG** by selecting the option from the drop down menu and click **OK**. This should be changed back to **NOTICE** after testing is complete.

**Modify System settings**

Default gateway IP address:

Enable restart on critical failure:

Console session timeout:  (Range: 0..65535)

Telnet session timeout:  (Range: 0..65535)

Enable SIP monitoring and tracing:

NTP servers:

Add	Edit	Delete
-----	------	--------

Logging settings

SysLog server IP address:

SysLog server port:  (Range: 0..65535)

SysLog facility:  (Range: 0..99999999)

Process log level:

SNMP settings

Click the **Configuration** button at the top to go to the **Configuration** tab.

You can verify the network interface settings configured through the `run setup` command by clicking on the **Network** icon under **System Administration**

### Modify Network settings

VLAN id:  (Range: 0..4095)

Network IP address:

Network IP subnet mask:

Network IP gateway address:

Preferred DNS server IP address:

Alternate DNS server IP address:

Alternate DNS server IP address:

DNS domain:

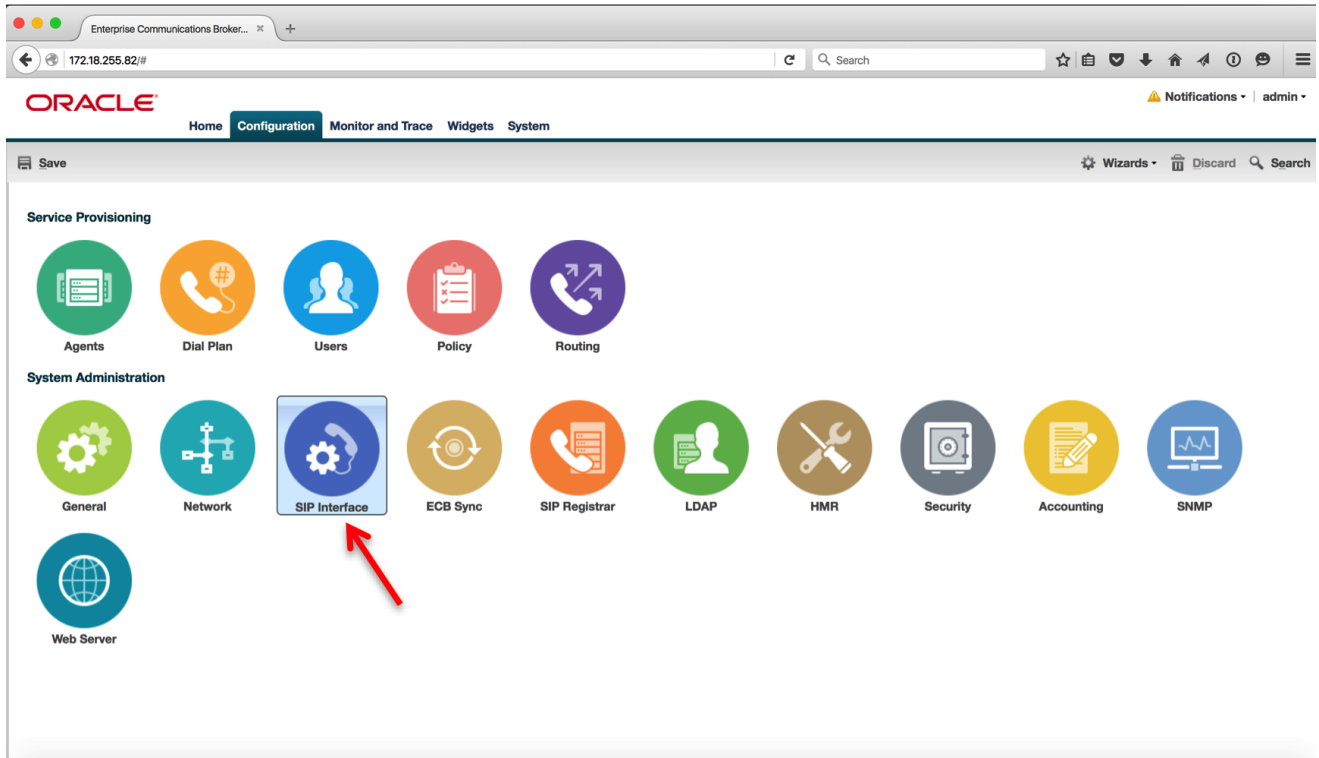
Enable ICMP:

Enable gateway heartbeat:

High availability settings

## Configure SIP Interfaces

Click **Configuration** button to go to the **Configuration** tab. Select the **SIP Interface** icon under **System Administration** to make changes to the SIP interface settings configured during initial setup.

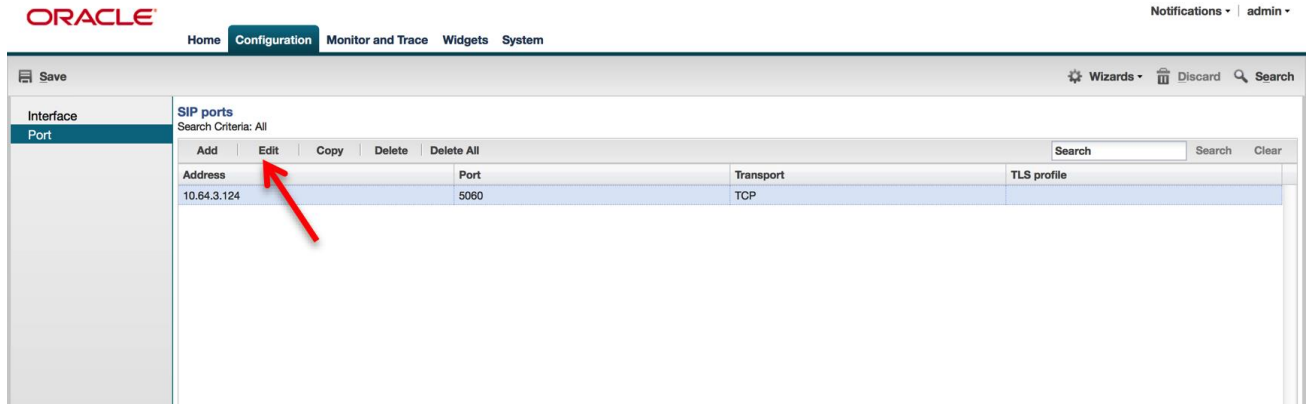


Click the “enable parallel forking” checkbox to enable parallel forking, i.e. calling a user on two devices at once, or leave it unchecked for serial forking. See the Configure LDAP Integration with Active Directory section of this document for more information.

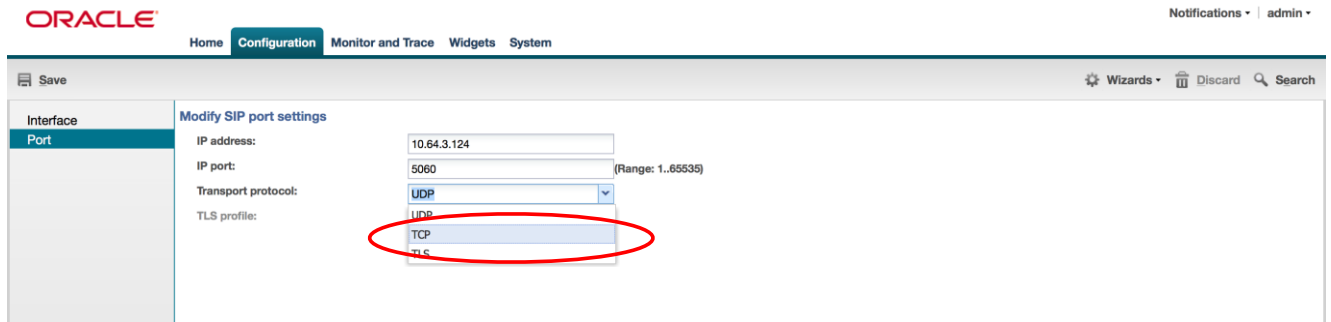
### Modify Interface settings

Maximum SIP message length:	<input type="text" value="4095"/>	(Range: 0..65535)
Enable parallel forking:	<input checked="" type="checkbox"/>	
Enable early media inhibit:	<input type="checkbox"/>	
Enable REFER termination:	<input type="checkbox"/>	
Send NOTIFY for REFER provisional responses:	<input type="text" value="none"/>	

Click on the **Port** tab on the left. You will see the sip port 10.64.3.124 with protocol UDP. Click **Edit** to change its protocol to TCP.



On the **Modify SIP port settings** page, select TCP as the transport protocol from the drop-down menu and click **OK**.

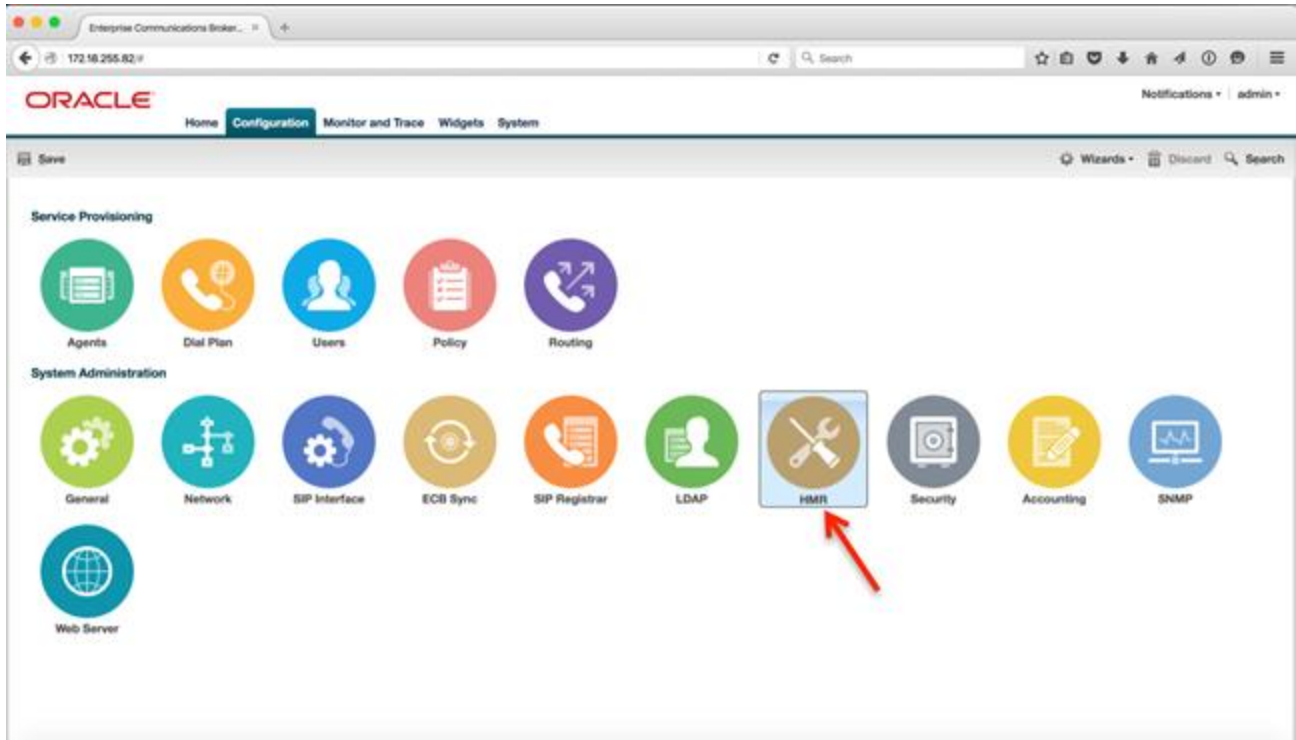


Click on the **Configuration** button to go back to the **Configuration** tab.

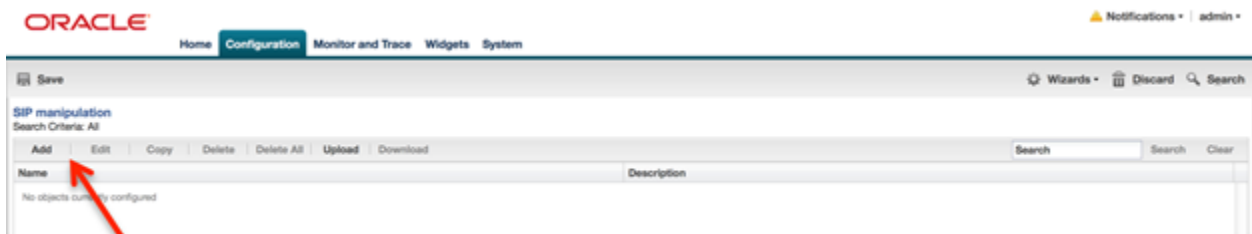
## Configure Header Manipulation Rules (HMR)

We will now configure header manipulation rules to hide network topology and ensure that the SIP messages sent to all agents cater to their specific signaling needs.

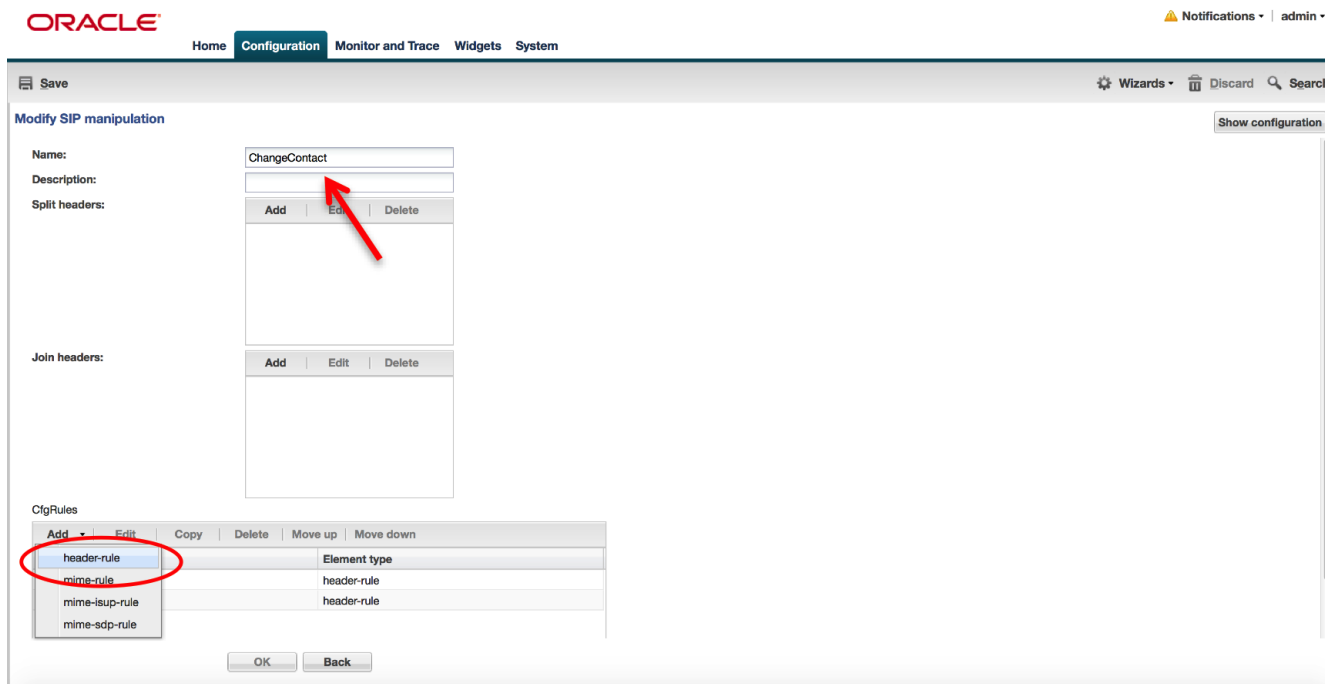
Click on the **HMR** icon under **System Administration** on the **Configuration** tab.



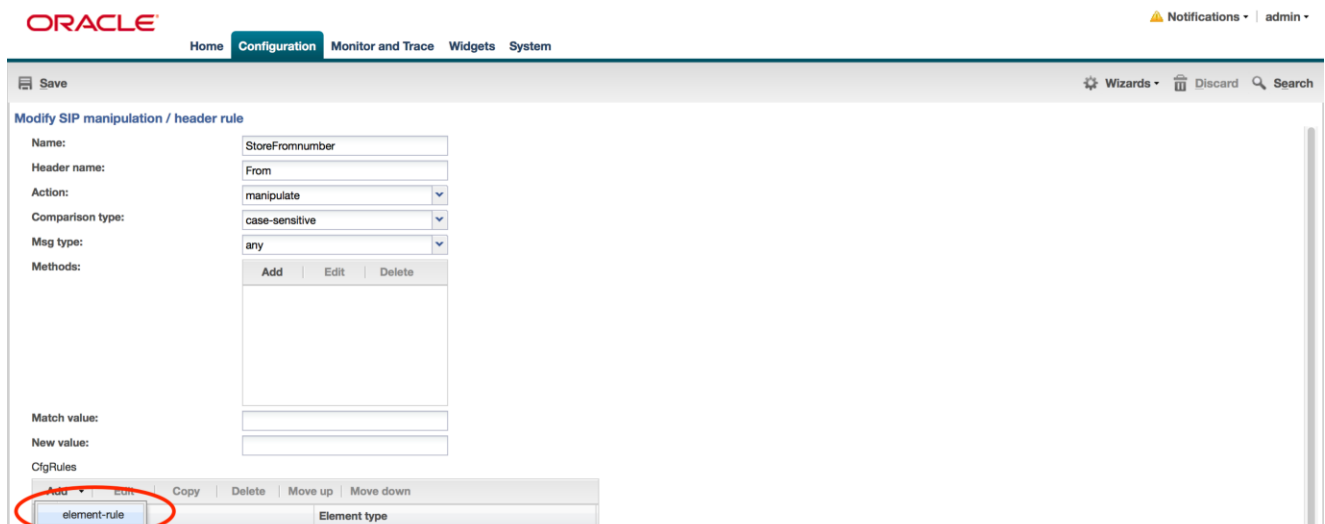
The **SIP manipulation** page is displayed. Click **Add** to add a SIP manipulation.



Type the name of the HMR rule, ChangeContact in this instance, and then click Add under CfgRules, then click header-rule. The manipulation consists of two header rules – StoreFromnumber and ChangeContact. The StoreFromnumber header rule stores the uri-user-only element in the From header which is then added as the uri-user in the Contact header in the ChangeContact header rule.



Enter the Name, Header name, and Action to match the following screenshot, then click on Add under CfgRules, then element-rule.



Then enter the following element-rule and click OK.

The screenshot shows the Oracle Configuration Wizard interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active. The main content area is titled 'Modify SIP manipulation / header rule / element rule'. It contains the following fields:

- Name: StoreFromnumber\_er
- Parameter name: (empty)
- Type: uri-user-only
- Action: store
- Match val type: any
- Comparison type: case-sensitive
- Match value: (empty)
- New value: (empty)

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

Add another header-rule:

The screenshot shows the Oracle Configuration Wizard interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The 'Configuration' tab is active. The main content area is titled 'Modify SIP manipulation'. It contains the following fields:

- Name: ChangeContact
- Description: (empty)
- Split headers: (empty table with 'Add', 'Edit', 'Delete' buttons)
- Join headers: (empty table with 'Add', 'Edit', 'Delete' buttons)

At the bottom, there is a 'CfgRules' table with the following data:

	Element type
header-rule	header-rule
mime-rule	header-rule
mime-isup-rule	header-rule
mime-sdp-rule	header-rule

The 'header-rule' row in the table is circled in red. At the bottom of the form, there are 'OK' and 'Back' buttons.

Add the following header-rule, then click on Add > element-rule.

The screenshot shows the Oracle Configuration interface for a SIP manipulation / header rule. The page title is "Modify SIP manipulation / header rule". The configuration fields are as follows:

- Name: ChangeContact
- Header name: contact
- Action: manipulate
- Comparison type: case-sensitive
- Msg type: any
- Methods: Add, Edit, Delete
- Match value: (empty)
- New value: (empty)

Below the configuration fields is a table with the following structure:

Element type
element-rule

The "element-rule" entry in the table is circled in red.

Add the following element-rule, then click OK. The New value displayed below is truncated and should be: \$StoreFromnumber.\$StoreFromnumber\_er.\$0

The screenshot shows the Oracle Configuration interface for a SIP manipulation / header rule / element rule. The page title is "Modify SIP manipulation / header rule / element rule". The configuration fields are as follows:

- Name: changeContact\_er
- Parameter name: (empty)
- Type: uri-user
- Action: add
- Match val type: any
- Comparison type: case-sensitive
- Match value: (empty)
- New value: \$StoreFromnumber.\$StoreFromnumber\_er.\$0

At the bottom of the page, there are two buttons: "OK" and "Back".

Here is a table of the HMR rules being configured on the ECB.

HMR Rule	Description
ChangeContact	Adds a user to the Contact header
HMRfromLync	Solves ringback issue and references ChangeContact rule
HMRtowardsAvaya	Changes From and To to 10 digits. Adds PAI to UPDATE requests.
HMRtowardsCUCM	Changes From and To to 10 digits. NATs IPs in those headers.
HMRtowardsLync	NAT, delete SDP b= lines, adds DTMF, changes to E.164, adds PAI to UPDATE
HMRtowardsSBC	Removes 9, removes +, removes PAI header
Modmline	Adds DTMF to SDP m= line
NATing	HMR for topology hiding
addPAItoUpdate	Adds P-Asserted-Identity to UPDATE requests
changeFromtoExt	Changes From and PAI to Extension only (optional)
changeTo10Digit	Changes From and To to 10 digits
changeToE164	Changes From and To to E.164
delblines	Deletes SDP b= lines from Avaya
fixSDP	Bypasses the 488 due to missing DTMF from CUCM during hold

For reference, here is the ChangeContact HMR rule in text format from the CLI. The text highlighted in **bold** are the non-default fields.

```

sip-manipulation
  name                               ChangeContact
  description
  split-headers
  join-headers
  header-rule
    name                               StoreFromnumber
    header-name                       From
    action                             manipulate
    comparison-type                   case-sensitive
    msg-type                           any
    methods
    match-value
    new-value
    element-rule
      name                               StoreFromnumber_er
      parameter-name
      type                               uri-user-only
      action                             store
      match-val-type                   any
      comparison-type                   case-sensitive
      match-value
      new-value
    header-rule
      name                               ChangeContact
      header-name                       Contact
      action                             manipulate
      comparison-type                   case-sensitive
      msg-type                           any
      methods
      match-value

```



```

new-value
element-rule
  name                ChangeContact_er
  parameter-name
  type
  action              add
  match-val-type     any
  comparison-type    case-sensitive
  match-value
  new-value          $StoreFromnumber.$StoreFromnumber_er.$0

```

The following HMR rule will be applied as an inbound manipulation from Lync and SFB. It changes “183 Session Progress” to “180 Ringing” to solve a ringback issue, and it references the ChangeContact rule as a nested HMR.

```

sip-manipulation
  name                HMRfromLync
  description
  split-headers
  join-headers
  header-rule
    name              change183to180
    header-name       @status-line
    action            manipulate
    comparison-type   case-sensitive
    msg-type          reply
    methods
    match-value
    new-value
    element-rule
      name            mod183to180
      parameter-name
      type            status-code
      action          replace
      match-val-type any
      comparison-type case-sensitive
      match-value     183
      new-value       180
    element-rule
      name            sessionProgressToRinging
      parameter-name
      type            reason-phrase
      action          replace
      match-val-type any
      comparison-type case-sensitive
      match-value     Session Progress
      new-value       Ringing
  header-rule
    name              ChangeContact
    header-name       To
    action            sip-manip
    comparison-type   case-sensitive
    msg-type          any
    methods
    match-value
    new-value         ChangeContact

```

The following HMR rule is applied as an outbound manipulation towards Avaya. It changes the From and To headers to 10 digits and adds a P-Asserted-Identity to UPDATE requests. **The last header-rule (changeFromtoExt) is optional and changes the From header to be a four digit extension. This can be used if internal Caller-ID needs to be extension based instead of 10 digits.** See the “changeFromtoExt” HMR rule later in this document for more details.

```

sip-manipulation
  name                               HMRtowardsAvaya
  description
  split-headers
  join-headers
  header-rule
    name                               changeTo10Digit
    header-name                         To
    action                               sip-manip
    comparison-type                     case-sensitive
    msg-type                             request
    methods
    match-value
    new-value                           changeTo10Digit
  header-rule
    name                               addPAItoUpdate
    header-name                         To
    action                               sip-manip
    comparison-type                     case-sensitive
    msg-type                             request
    methods                             UPDATE
    match-value
    new-value                           addPAItoUpdate
  header-rule (optional)
    name                               changeFromtoExt
    header-name                         To
    action                               sip-manip
    comparison-type                     case-sensitive
    msg-type                             request
    methods
    match-value
    new-value                           changeFromtoExt

```

The following HMR rule is applied as an outbound manipulation towards Cisco CUCM. It changes the From and To headers to 10 digits and NATs IPs in those headers as well. **The last header-rule (changeFromtoExt) is optional and changes the From header to be a four digit extension. This can be used if internal Caller-ID needs to be extension based instead of 10 digits.** See the "changeFromtoExt" HMR rule later in this document for more details.

```

sip-manipulation
  name HMRtowardsCUCM
  description
  split-headers
  join-headers
  header-rule
    name changeTo10Digit
    header-name To
    action sip-manip
    comparison-type case-sensitive
    msg-type request
    methods
    match-value
    new-value changeTo10Digit
  header-rule
    name NATing
    header-name To
    action sip-manip
    comparison-type case-sensitive
    msg-type request
    methods
    match-value
    new-value NATing
  header-rule (optional)
    name changeFromtoExt
    header-name To
    action sip-manip
    comparison-type case-sensitive
    msg-type request
    methods
    match-value
    new-value changeFromtoExt

```

The following HMR rule is applied as an outbound manipulation towards Microsoft Lync and SFB. It changes the From and To headers to E.164 format, NATs IPs in those headers, and modifies the SDP. **The last header-rule (changeFromtoExt) is optional and changes the From header to be a four digit extension. This can be used if internal Caller-ID needs to be extension based instead of 10 digits.** See the "changeFromtoExt" HMR rule later in this document for more details.

```

sip-manipulation
  name                                HMRtowardsLync
  description
  split-headers
  join-headers
  header-rule
    name                                doNAT
    header-name                          From
    action                                sip-manip
    comparison-type                       case-sensitive
    msg-type                              any
    methods
    match-value
    new-value                             NATing
  header-rule
    name                                deleteblines
    header-name                          From
    action                                sip-manip
    comparison-type                       case-sensitive
    msg-type                              any
    methods
    match-value
    new-value                             delblines
  header-rule
    name                                adddtmfines
    header-name                          From
    action                                sip-manip
    comparison-type                       case-sensitive
    msg-type                              any
    methods                              INVITE
    match-value
    new-value                             fixSDP
  header-rule
    name                                changeToE164
    header-name                          To
    action                                sip-manip
    comparison-type                       case-sensitive
    msg-type                              request
    methods
    match-value
    new-value                             changeToE164
  header-rule
    name                                addPAItoUpdate
    header-name                          To
    action                                sip-manip
    comparison-type                       case-sensitive
    msg-type                              any
    methods                              UPDATE
    match-value
    new-value                             addPAItoUpdate
  header-rule (optional)
    name                                changeFromtoExt
    header-name                          To
    action                                sip-manip
    comparison-type                       case-sensitive
    msg-type                              request
    methods
    match-value
    new-value                             changeFromtoExt

```

The following HMR rule is applied as an outbound manipulation towards the Oracle E-SBC. It removes 9 from the beginning of the Request- and To- URIs, NATs the From and To headers headers, removes the plus sign in the From header, and removes P-Asserted-Identity.

```

sip-manipulation
  name HMRtowardsSBC
  description
  split-headers
  join-headers
  header-rule
    name Remove9
    header-name request-uri
    action manipulate
    comparison-type pattern-rule
    msg-type request
    methods
    match-value
    new-value
    element-rule
      name remove9FromRuri
      parameter-name uri-user
      type replace
      action any
      comparison-type pattern-rule
      match-value 91(\d{10})
      new-value $1
  header-rule
    name NATing
    header-name To
    action sip-manip
    comparison-type case-sensitive
    msg-type request
    methods
    match-value
    new-value NATing
  header-rule
    name remove9fromTOURI
    header-name to
    action manipulate
    comparison-type pattern-rule
    msg-type request
    methods
    match-value
    new-value
    element-rule
      name remove9inTOuri
      parameter-name uri-user
      type replace
      action any
      comparison-type pattern-rule
      match-value 91(\d{10})
      new-value $1
  header-rule
    name reomvePlusInFrom
    header-name From
    action manipulate
    comparison-type pattern-rule
    msg-type request
    methods
    match-value
    new-value

```

```

element-rule
    name reomvePlus
    parameter-name
    type uri-user
    action replace
    match-val-type any
    comparison-type pattern-rule
    match-value ^\+([0-9]{10,11})$
    new-value $1

header-rule
    name removePAI
    header-name P-Asserted-Identity
    action delete
    comparison-type case-sensitive
    msg-type request
    methods
    match-value
    new-value

```

The following HMR rule is referenced in another HMR rule later in this document and adds DTMF to the m= line in SDP.

```

sip-manipulation
    name Modmline
    description Add DTMF to m line
    split-headers
    join-headers
    mime-sdp-rule
        name modmline
        msg-type any
        methods
        action manipulate
        comparison-type pattern-rule
        match-value
        new-value
    sdp-media-rule
        name modmline_m
        media-type audio
        action manipulate
        comparison-type pattern-rule
        match-value
        new-value
    sdp-line-rule
        name change_payload
        type m
        action find-replace-all
        comparison-type pattern-rule
        match-value ^(audio)( [0-9]{4,5})( RTP/AVP 0)$
        new-value audio+$2+" RTP/AVP 0 101"

```

The following HMR rule is referenced in other HMR rules in this document, and it NATs the IP addresses in the From and To headers.

```

sip-manipulation
  name                    NATing
  description             HMR for topology hiding
  split-headers
  join-headers
  header-rule
    name
    header-name          From
    action               From
                        manipulate
    comparison-type      case-sensitive
    msg-type             any
    methods
    match-value
    new-value
    element-rule
      name               From_header
      parameter-name
      type               uri-host
      action             replace
    match-val-type      any
    comparison-type      case-sensitive
    match-value
    new-value           $LOCAL_IP
  header-rule
    name
    header-name          To
    action               To
                        manipulate
    comparison-type      case-sensitive
    msg-type            request
    methods
    match-value
    new-value
    element-rule
      name               To
      parameter-name
      type               uri-host
      action             replace
    match-val-type      any
    comparison-type      case-sensitive
    match-value
    new-value           $REMOTE_IP

```

The following HMR rule is referenced in other HMR rules in this document, and it adds a P-Asserted-Identity header to UPDATE requests based on the user in the Contact-URI.

```

sip-manipulation
  name                addPAItoUpdate
  description
  split-headers
  join-headers
  header-rule
    name
    header-name
    action
    comparison-type
    msg-type
    methods
    match-value
    new-value
    element-rule
      name
      parameter-name
      type
      action
      match-val-type
      comparison-type
      match-value
      new-value
  header-rule
    name
    header-name
    action
    comparison-type
    msg-type
    methods
    match-value
    new-value
    element-rule
      name
      parameter-name
      type
      action
      match-val-type
      comparison-type
      match-value
      new-value " <sip:"+$storeContact.$storeContactUser.$0+"@"+$LOCAL_IP+>"

```



The following HMR rule is referenced in other HMR rules in this document, and it changes the From and P-Asserted-Identity headers to 4-digit extensions. **It is optional and may be used to ensure internal Caller-ID shows extensions only instead of 10-digits. In our lab config, it looks for 571293, 1571293, +571293, and +1571293, and strips these prefixes off if they are present. You will need to change this to be your network's prefix. It is looking for 4 digit extensions, which is why the {4} appears in the match-value. This may be changed to meet your extension length requirements. The match-value is a regular expression (regex) and it looks for an optional plus sign, an optional 1, and then 571293, followed by 4 digits. If you need it to look for a country code of +61 followed by 5712 followed by a 5 digit extension, for example, the regex would be: `^\+615712 ([0-9] {5}) $`**

```

sip-manipulation (optional)
  name                changeFromtoExt
  description         change From and PAI to Extension only
  split-headers
  join-headers
  header-rule
    name              removePlusandPrefix
    header-name       From
    action            manipulate
    comparison-type   pattern-rule
    msg-type          request
    methods
    match-value
    new-value
    element-rule
      name            changeFromUri
      parameter-name
      type            uri-user
      action          replace
      match-val-type any
      comparison-type pattern-rule
      match-value     ^\+?1?571293 ([0-9] {4}) $
      new-value       $1
  header-rule
    name              removePAIplusandPrefix
    header-name       P-Asserted-Identity
    action            manipulate
    comparison-type   pattern-rule
    msg-type          request
    methods
    match-value
    new-value
    element-rule
      name            modifyPaiUri
      parameter-name
      type            uri-user
      action          replace
      match-val-type any
      comparison-type pattern-rule
      match-value     ^\+?1?571293 ([0-9] {4}) $
      new-value       $1

```

The following HMR rule is referenced in other HMR rules in this document, and it converts the From and To headers to 10 digit dialing. **Change 571293 to match your prefix. {4} represents a 4 digit extension. Change the length of the extension if needed.**

```

sip-manipulation
  name changeTo10Digit
  description
  split-headers
  join-headers
  header-rule (do not use this header-rule if using the changeFromtoExt rule above)
    name changeFrom10Digit
    header-name From
    action manipulate
    comparison-type pattern-rule
    msg-type request
    methods
    match-value
    new-value
    element-rule
      name changeExtTo10Digit
      parameter-name
      type uri-user
      action replace
      match-val-type any
      comparison-type pattern-rule
      match-value ^([0-9]{4})$
      new-value 571293+$1
    element-rule
      name change11DigitTo10Digit
      parameter-name
      type uri-user
      action replace
      match-val-type any
      comparison-type pattern-rule
      match-value ^1([0-9]{10})$
      new-value $1
    element-rule
      name changeE164To10Digit
      parameter-name
      type uri-user
      action replace
      match-val-type any
      comparison-type pattern-rule
      match-value ^\+1([0-9]{10})$
      new-value $1
  header-rule
    name changeTo10Digit
    header-name To
    action manipulate
    comparison-type pattern-rule
    msg-type request
    methods
    match-value
    new-value
    element-rule
      name changeExtTo10Digit
      parameter-name
      type uri-user
      action replace
      match-val-type any
      comparison-type pattern-rule
      match-value ^([0-9]{4})$
      new-value 571293+$1
    element-rule

```

	<b>name</b>	<b>change11DigitTo10Digit</b>
	parameter-name	
	<b>type</b>	<b>uri-user</b>
	<b>action</b>	<b>replace</b>
	match-val-type	any
	<b>comparison-type</b>	<b>pattern-rule</b>
	<b>match-value</b>	<b>^1([0-9]{10})\$</b>
	<b>new-value</b>	<b>\$1</b>
element-rule		
	<b>name</b>	<b>changeE164to10Digit</b>
	parameter-name	
	<b>type</b>	<b>uri-user</b>
	<b>action</b>	<b>replace</b>
	match-val-type	any
	<b>comparison-type</b>	<b>pattern-rule</b>
	<b>match-value</b>	<b>^\+1([0-9]{10})\$</b>
	<b>new-value</b>	<b>\$1</b>

The following HMR rule is referenced in other HMR rules in this document, and it converts the From and To headers to E.164 dialing. **Change 571293 to match your prefix. {4} represents a 4 digit extension. Change the length of the extension if needed.**

```

sip-manipulation
  name                changeToE164
  description
  split-headers
  join-headers
  header-rule
    name              changeToE164
    header-name       To
    action            manipulate
    comparison-type   pattern-rule
    msg-type          request
    methods
    match-value
    new-value
    element-rule
      name            changeExtToE164
      parameter-name
      type            uri-user
      action          replace
      match-val-type any
      comparison-type pattern-rule
      match-value     ^([0-9]{4})$
      new-value       \+1571293+$1
    element-rule
      name            change11DigitToE164
      parameter-name
      type            uri-user
      action          replace
      match-val-type any
      comparison-type pattern-rule
      match-value     ^([0-9]{11})$
      new-value       \++$1
    element-rule
      name            change10DigitToE164
      parameter-name
      type            uri-user
      action          replace
      match-val-type any
      comparison-type pattern-rule
      match-value     ^([0-9]{10})$
      new-value       \+1+$1
  header-rule (do not use this header-rule if using the changeFromtoExt rule above)
    name              changeFromE164
    header-name       From
    action            manipulate
    comparison-type   pattern-rule
    msg-type          request
    methods
    match-value
    new-value
    element-rule
      name            changeExtToE164
      parameter-name
      type            uri-user
      action          replace
      match-val-type any
      comparison-type pattern-rule
      match-value     ^([0-9]{4})$
      new-value       \+1571293+$1
    element-rule

```

	<b>name</b> parameter-name <b>type</b> <b>action</b> match-val-type <b>comparison-type</b> <b>match-value</b> <b>new-value</b>	<b>change11DigitToE164</b>  uri-user <b>replace</b> any <b>pattern-rule</b> ^([0-9]{11})\$ \++\$1
element-rule	<b>name</b> parameter-name <b>type</b> <b>action</b> match-val-type <b>comparison-type</b> <b>match-value</b> <b>new-value</b>	<b>change10DigitToE164</b>  uri-user <b>replace</b> any <b>pattern-rule</b> ^([0-9]{10})\$ \+1+\$1

The following HMR rule is referenced in other HMR rules in this document, and it removes b= lines in the SDP coming from Avaya.

<pre> sip-manipulation   name   description   split-headers   join-headers   header-rule     name     header-name     action     comparison-type     msg-type     methods     match-value     new-value     element-rule       name       parameter-name       type       action       match-val-type       comparison-type       match-value       new-value     element-rule       name       parameter-name       type       action       match-val-type       comparison-type       match-value       new-value </pre>	<pre> delblines Deleting b-lines from Avaya  manipContentType Content-Type manipulate pattern-rule any  deleteB application/sdp mime find-replace-all any pattern-rule b=CT:.*(\n \r\n)  deleteLABEL application/sdp mime find-replace-all any pattern-rule b=TIAS:.*(\n \r\n) </pre>
--	---

The following HMR rule is referenced in other HMR rules in this document, and it adds DTMF to the SDP.

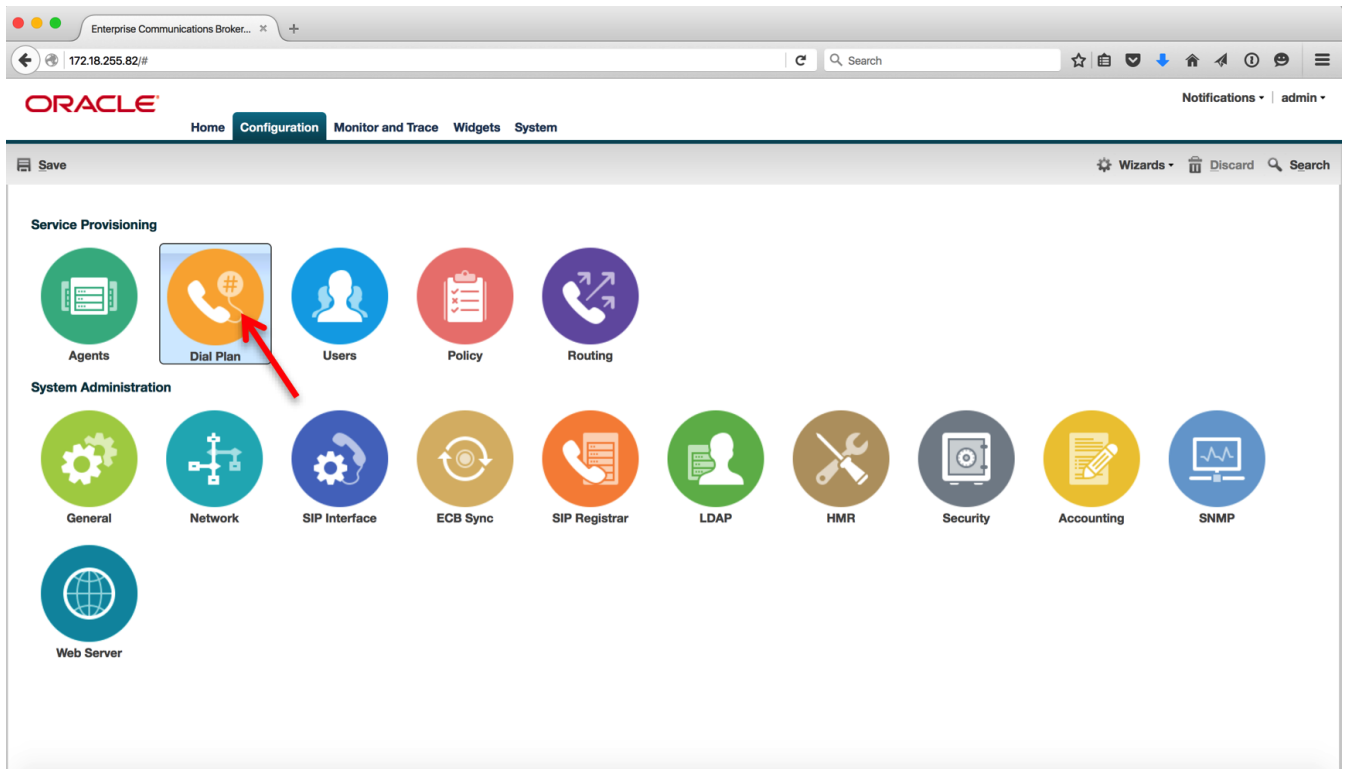
```

sip-manipulation
  name fixSDP
  description To bypass the 488 due to missing DTMF from
  CUCM during hold
  split-headers
  join-headers
  header-rule
    name Checkfordtmf
    header-name Content-type
    action store
    comparison-type case-sensitive
    msg-type any
    methods INVITE
    match-value
    new-value
    element-rule
      name Checkdtmfexists
      parameter-name application/sdp
      type mime
      action store
      match-val-type any
      comparison-type case-sensitive
      match-value (a=rtpmap:101 telephone-event/8000)
      new-value
    header-rule
      name AddPtime10
      header-name Content-Type
      action manipulate
      comparison-type boolean
      msg-type any
      methods INVITE
      match-value !$Checkfordtmf.$Checkdtmfexists
      new-value
      element-rule
        name Adddtmf
        parameter-name application/sdp
        type mime
        action find-replace-all
        match-val-type any
        comparison-type pattern-rule
        match-value (\,*)
        new-value $0+"a=rtpmap:101 telephone-event/8000"+$CRLF+"a=fmtp:101 0-15"+$CRLF
    header-rule
      name Modifymline
      header-name From
      action sip-manip
      comparison-type case-sensitive
      msg-type request
      methods
      match-value
      new-value Modmline

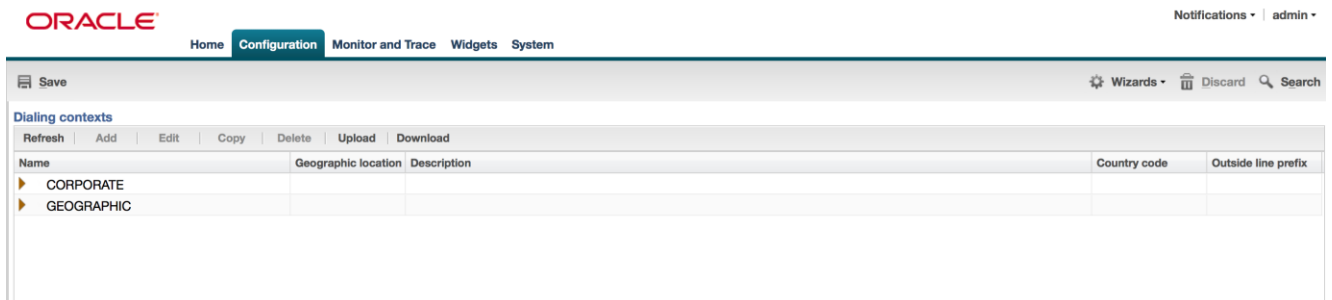
```

## Configure Dial Plan

We will now configure the dialing contexts and dial plans. Dialing-contexts define the system behavior for calls placed to and from either a corporate or geographic focus. Dialing-contexts include multiple dial-patterns, which define the normalization required to most effectively manage diverse signaling structures. Click on the **Dial Plan** icon under **Service Provisioning**.



The **Dialing Contexts** page shows the default dialing context parents – Corporate and Geographic.



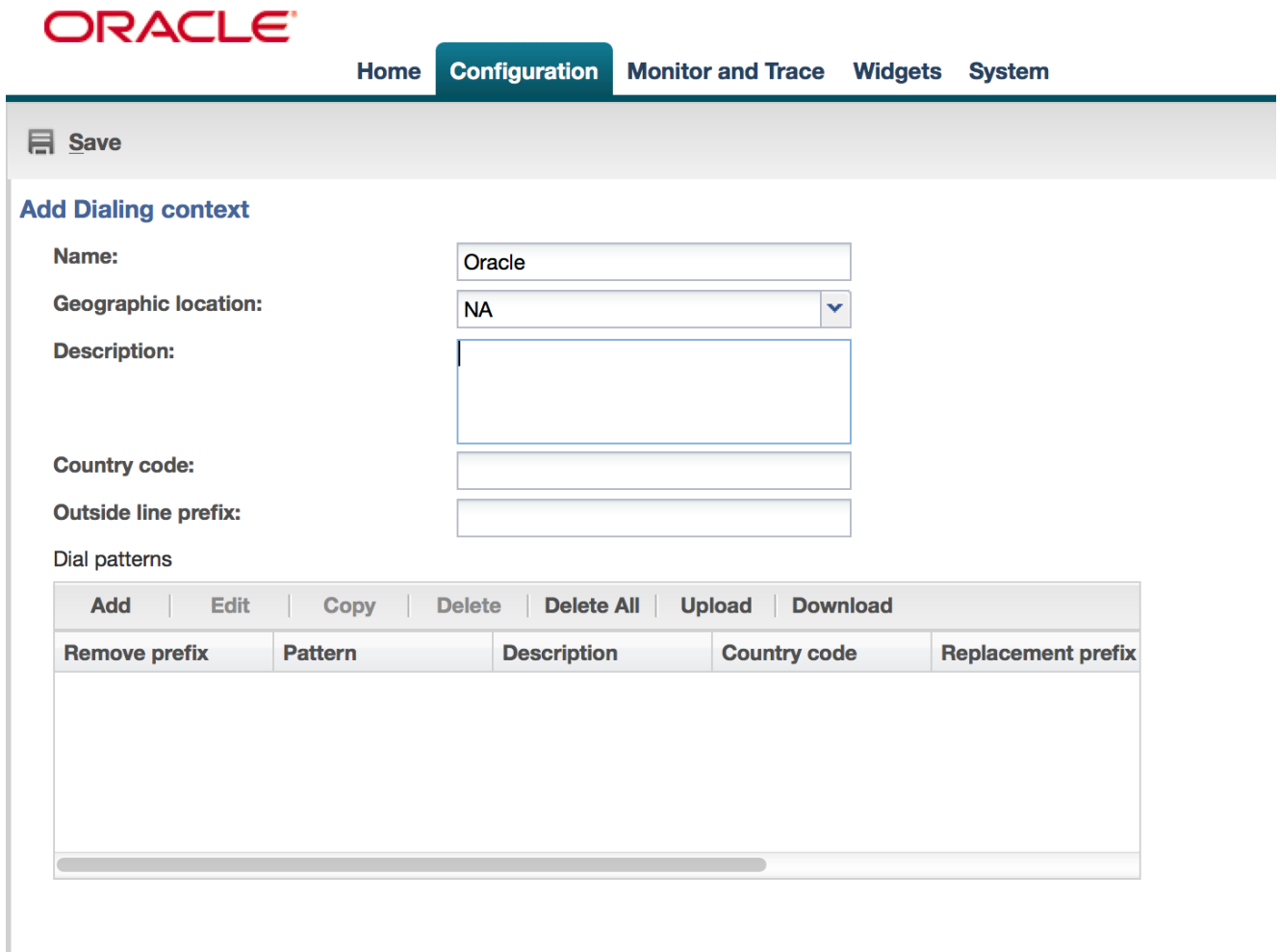


To configure a dialing context, select the Corporate context and click **Add**.



The screenshot shows the Oracle Configuration interface. At the top, there is a navigation bar with 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. Below this is a header area with 'Save', 'Wizards', 'Discard', and 'Search'. The main content area is titled 'Dialing contexts' and contains a table with columns: Name, Geographic location, Description, Country code, and Outside line prefix. The table has two rows: 'CORPORATE' and 'GEOGRAPHIC'. A red arrow points to the 'Add' button in the toolbar above the table.

In the **Add Dialing Context** page, configure a context with the following details and click **OK**.



The screenshot shows the 'Add Dialing context' form. The form has the following fields:

- Name:** Oracle
- Geographic location:** NA
- Description:** (empty text area)
- Country code:** (empty text field)
- Outside line prefix:** (empty text field)

Below the form is a section titled 'Dial patterns' with a table that has the following columns: Remove prefix, Pattern, Description, Country code, and Replacement prefix. The table is currently empty.

The Dialing Contexts page displays Oracle listed under Corporate contexts. We will now configure child contexts under Oracle for our Lync, SFB, Avaya and CUCM servers. These can be considered as contexts for the different branches an enterprise has.

Select Oracle under the Corporate context and click **Add**.

Dialing contexts

Name	Geographic location	Description	Country code	Outside line prefix
<ul style="list-style-type: none"> <li>▶ CORPORATE           <ul style="list-style-type: none"> <li>▶ Oracle</li> </ul> </li> <li>▶ GEOGRAPHIC</li> </ul>	NA			

In the **Add Dialing Context** window, configure a context named LYNC2013 and **Geographic location** as NA. To configure dial patterns, click **Add**.

**Add Dialing context**

Name:

Geographic location:

Description:

Country code:

Outside line prefix:

Dial patterns

Remove prefix	Pattern	Description	Country code	Replacement prefix

Add a dial pattern as shown below to enable 4 digit dialing and click **OK**. If the dialed digits match the pattern 53XX, the ECB transforms it to a 10 digit number by adding the prefix 571293.

**Add Dialing context / dial pattern**

Remove prefix:

Pattern:

Description:

Country code:

Replacement prefix:

Replacement uri:

Go to context:

The LYNC2013 dialing context displays the configured dial pattern.

**Modify Dialing context**

Name:

Geographic location:

Description:

Country code:

Outside line prefix:

Dial patterns

Add   Edit   Copy   Delete   Delete All   Upload   Download				
Remove prefix	Pattern	Description	Country code	Replacement prefix
	53XX			571293

Add another dialing context under Oracle named Avaya6\_3 with the following settings and click **OK**.

**Modify Dialing context**

Name:

Geographic location:

Description:

Country code:

Outside line prefix:

Dial patterns

Add   Edit   Copy   Delete   Delete All   Upload   Download				
Remove prefix	Pattern	Description	Country code	Replacement prefix
	53XX			571293

Add another dialing context under Oracle named Avaya7\_0\_dialing with the following settings and click **OK**.

**Modify Dialing context**

Name:

Geographic location:

Description:

Country code:

Outside line prefix:

Dial patterns

Add	Edit	Copy	Delete	Delete All	Upload	Download
Remove prefix	Pattern	Description	Country code	Replacement prefix		
	53XX			571293		

Add another dialing context under Oracle named CUCM11\_0 with the following settings and click **OK**.

**Modify Dialing context**

Name:

Geographic location:

Description:

Country code:

Outside line prefix:

Dial patterns

Add	Edit	Copy	Delete	Delete All	Upload	Download
Remove prefix	Pattern	Description	Country code	Replacement prefix		
	53XX			571293		

Add another dialing context under Oracle named Skype for Business with the following settings and click **OK**.

**Modify Dialing context**

**Name:**

**Geographic location:**

**Description:**

**Country code:**

**Outside line prefix:**

Dial patterns

Add	Edit	Copy	Delete	Delete All	Upload	Download
Remove prefix	Pattern	Description	Country code	Replacement prefix		
	53XX			571293		

Add another dialing context under Oracle named cucm10\_5 with the following settings and click **OK**.

**Modify Dialing context**

**Name:**

**Geographic location:**

**Description:**

**Country code:**

**Outside line prefix:**

Dial patterns

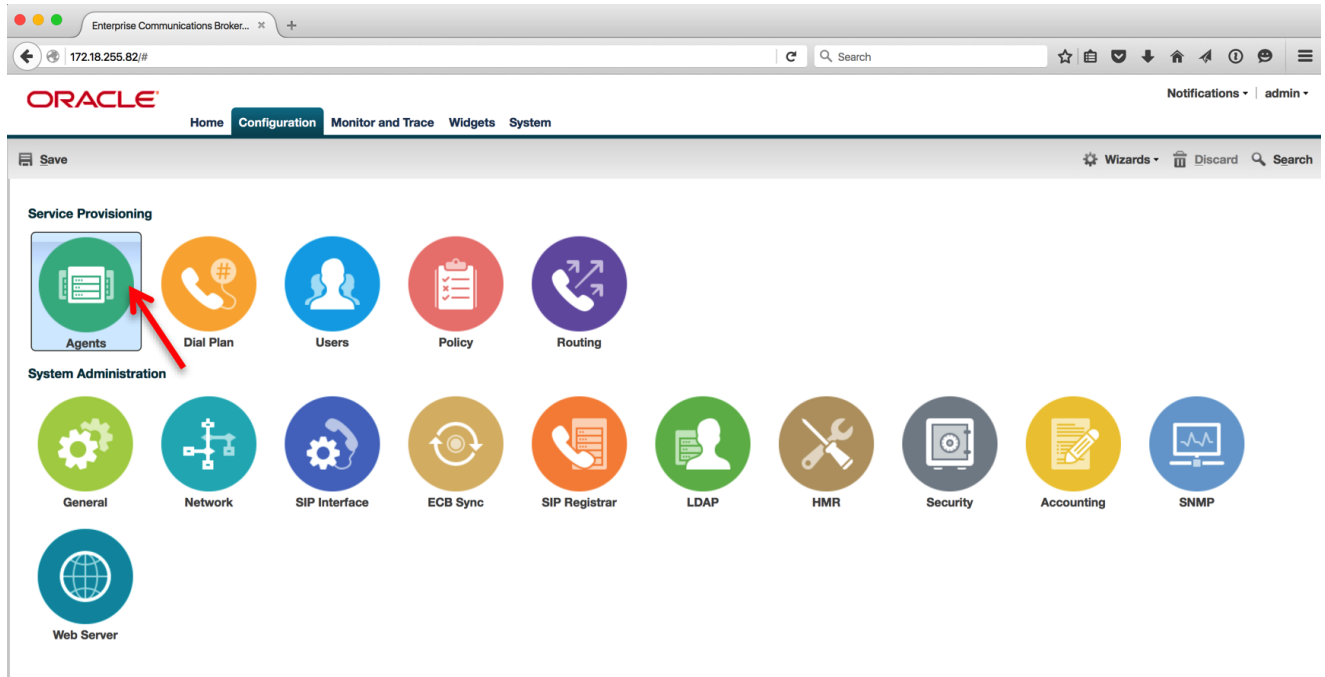
Add	Edit	Copy	Delete	Delete All	Upload	Download
Remove prefix	Pattern	Description	Country code	Replacement prefix		
	53XX			571293		

The **Dialing Contexts** page shows the parent context – Oracle and the child contexts.

Dialing contexts									
Refresh	Add	Edit	Copy	Delete	Upload	Download			
Name	Geographic location	Description	Country code	Outside line prefix					
▲ CORPORATE									
▲ Oracle	NA								
▶ Avaya6_3	NA								
▶ Avaya7_0_dialing	NA								
▲ CUCM11_0	NA								
▶ LYNC2013	NA								
▶ SFB	NA	Skype for business							
▶ cucm10_5	NA								
▶ GEOGRAPHIC									

## Configure Agents

We will now configure the next hops in our routing paths – the Agents – which in our setup are the Cisco CUCM, Lync and SFB Mediation Servers, Avaya SM and the SBC which connects the ECB to the SIP trunk. Click on **Agents** icon under **Service Provisioning**.



The Agents page will be displayed. Click on the **Add** button. The **Add Agent settings** page is displayed. Add the Oracle E-SBC by configuring the hostname, IP address, port, transport protocol, egress number translation mode, number of digits for n digit dialing, source context, and Header Manipulation Rule as shown below.

## Modify Agents

<b>Hostname:</b>	<input type="text" value="10.64.3.122"/>						
<b>IP address:</b>	<input type="text" value="10.64.3.122"/>						
<b>Port:</b>	<input type="text" value="5060"/> (Range: 0, 1025..65535)						
<b>State:</b>	<input checked="" type="checkbox"/>						
<b>Transport protocol:</b>	<input type="text" value="StaticTCP"/> ▼						
<b>TLS profile:</b>	<input type="text"/> ▼						
<b>Description:</b>	<input type="text" value="Oracle E-SBC"/>						
<b>Source context:</b>	<input type="text" value="NA"/> ▼						
<b>Egress number translation mode:</b>	<input type="text" value="n-digit-dialing"/> ▼						
<b>Number of digits for n digit dialing:</b>	<input type="text" value="10"/> (Range: 0..25)						
<b>Prepend prefix on egress:</b>	<input type="text"/>						
<b>Inbound header manipulation:</b>	<input type="text"/> ▼						
<b>Outbound header manipulation:</b>	<input type="text" value="HMRtowardsSBC"/> ▼						
<b>Apply outbound manipulation on:</b>	<input type="text" value="next-hop-only"/> ▼						
<b>Tags:</b>	<table border="1"><thead><tr><th>Add</th><th>Edit</th><th>Delete</th></tr></thead><tbody><tr><td colspan="3"> </td></tr></tbody></table>	Add	Edit	Delete			
Add	Edit	Delete					

OK

Back



Scroll down to enable SIP OPTIONS to monitor agent health locally. Check the Enable OPTIONS ping check box and configure the OPTIONS ping interval to 30. Click OK.

## Modify Agents

Inbound header manipulation:

Outbound header manipulation:

Apply outbound manipulation on:

Tags:

Add	Edit	Delete

Early media inhibit:

Enable OPTIONS ping:

OPTIONS ping interval:

(Range: 0..4294967295)

Ldap:

Additional target group:

Fork group:

(Range: 1..100)

Enable REFER termination:

Send NOTIFY for REFER provisional responses:

▾ Constraints

▾ Advanced

OK

Back

You will now see the Oracle E-SBC listed under **Agents**. Click **Add** to add the Cisco CUCM 10.5 server and also enable OPTIONS as shown in the previous step.

## Modify Agents

<b>Hostname:</b>	<input type="text" value="10.71.2.10"/>						
<b>IP address:</b>	<input type="text" value="10.71.2.10"/>						
<b>Port:</b>	<input type="text" value="5060"/> (Range: 0, 1025..65535)						
<b>State:</b>	<input checked="" type="checkbox"/>						
<b>Transport protocol:</b>	<input type="text" value="StaticTCP"/> ▼						
<b>TLS profile:</b>	<input type="text"/> ▼						
<b>Description:</b>	<input type="text"/>						
<b>Source context:</b>	<input type="text" value="Oracle.cucm10_5"/> ▼						
<b>Egress number translation mode:</b>	<input type="text" value="no-country-code"/> ▼						
<b>Number of digits for n digit dialing:</b>	<input type="text" value="4"/> (Range: 0..25)						
<b>Prepend prefix on egress:</b>	<input type="text"/>						
<b>Inbound header manipulation:</b>	<input type="text"/> ▼						
<b>Outbound header manipulation:</b>	<input type="text" value="HMRtowardsCUCM"/> ▼						
<b>Apply outbound manipulation on:</b>	<input type="text" value="next-hop-only"/> ▼						
<b>Tags:</b>	<table><tr><td><b>Add</b></td><td><b>Edit</b></td><td><b>Delete</b></td></tr><tr><td colspan="3"><input type="text"/></td></tr></table>	<b>Add</b>	<b>Edit</b>	<b>Delete</b>	<input type="text"/>		
<b>Add</b>	<b>Edit</b>	<b>Delete</b>					
<input type="text"/>							

OK

Back

Click **Add** to add the Cisco CUCM 11.0 server and also enable OPTIONS as shown in the previous step.

### Modify Agents

<b>Hostname:</b>	<input type="text" value="10.71.3.10"/>						
<b>IP address:</b>	<input type="text" value="10.71.3.10"/>						
<b>Port:</b>	<input type="text" value="5060"/> (Range: 0, 1025..65535)						
<b>State:</b>	<input checked="" type="checkbox"/>						
<b>Transport protocol:</b>	<input type="text" value="StaticTCP"/> ▼						
<b>TLS profile:</b>	<input type="text"/> ▼						
<b>Description:</b>	<input type="text"/>						
<b>Source context:</b>	<input type="text" value="Oracle.CUCM11_0"/> ▼						
<b>Egress number translation mode:</b>	<input type="text" value="no-country-code"/> ▼						
<b>Number of digits for n digit dialing:</b>	<input type="text" value="4"/> (Range: 0..25)						
<b>Prepend prefix on egress:</b>	<input type="text"/>						
<b>Inbound header manipulation:</b>	<input type="text"/> ▼						
<b>Outbound header manipulation:</b>	<input type="text" value="HMRtowardsCUCM"/> ▼						
<b>Apply outbound manipulation on:</b>	<input type="text" value="next-hop-only"/> ▼						
<b>Tags:</b>	<table border="1"><thead><tr><th>Add</th><th>Edit</th><th>Delete</th></tr></thead><tbody><tr><td colspan="3"> </td></tr></tbody></table>	Add	Edit	Delete			
Add	Edit	Delete					

Click **Add** to add Avaya 6.3 server and also enable OPTIONS as shown in the previous step.

### Modify Agents

<b>Hostname:</b>	<input type="text" value="avaya6dot3"/>						
<b>IP address:</b>	<input type="text" value="10.70.4.7"/>						
<b>Port:</b>	<input type="text" value="5060"/> (Range: 0, 1025..65535)						
<b>State:</b>	<input checked="" type="checkbox"/>						
<b>Transport protocol:</b>	<input type="text" value="StaticTCP"/> ▼						
<b>TLS profile:</b>	<input type="text"/> ▼						
<b>Description:</b>	<input type="text"/>						
<b>Source context:</b>	<input type="text" value="Oracle.Avaya6_3"/> ▼						
<b>Egress number translation mode:</b>	<input type="text" value="no-country-code"/> ▼						
<b>Number of digits for n digit dialing:</b>	<input type="text" value="4"/> (Range: 0..25)						
<b>Prepend prefix on egress:</b>	<input type="text"/>						
<b>Inbound header manipulation:</b>	<input type="text"/> ▼						
<b>Outbound header manipulation:</b>	<input type="text" value="HMRtowardsAvaya"/> ▼						
<b>Apply outbound manipulation on:</b>	<input type="text" value="next-hop-only"/> ▼						
<b>Tags:</b>	<table border="1"><thead><tr><th>Add</th><th>Edit</th><th>Delete</th></tr></thead><tbody><tr><td colspan="3"> </td></tr></tbody></table>	Add	Edit	Delete			
Add	Edit	Delete					

Click **Add** to add the Avaya 7.0 server and also enable OPTIONS as shown in the previous step.

## Modify Agents

<b>Hostname:</b>	<input type="text" value="avaya7"/>						
<b>IP address:</b>	<input type="text" value="10.89.17.7"/>						
<b>Port:</b>	<input type="text" value="5060"/> (Range: 0, 1025..65535)						
<b>State:</b>	<input checked="" type="checkbox"/>						
<b>Transport protocol:</b>	<input type="text" value="StaticTCP"/> ▼						
<b>TLS profile:</b>	<input type="text"/> ▼						
<b>Description:</b>	<input type="text"/>						
<b>Source context:</b>	<input type="text" value="Oracle.Avaya7_0_dialing"/> ▼						
<b>Egress number translation mode:</b>	<input type="text" value="no-country-code"/> ▼						
<b>Number of digits for n digit dialing:</b>	<input type="text" value="4"/> (Range: 0..25)						
<b>Prepend prefix on egress:</b>	<input type="text"/>						
<b>Inbound header manipulation:</b>	<input type="text"/> ▼						
<b>Outbound header manipulation:</b>	<input type="text" value="HMRtowardsAvaya"/> ▼						
<b>Apply outbound manipulation on:</b>	<input type="text" value="next-hop-only"/> ▼						
<b>Tags:</b>	<table border="1"><thead><tr><th>Add</th><th>Edit</th><th>Delete</th></tr></thead><tbody><tr><td colspan="3"> </td></tr></tbody></table>	Add	Edit	Delete			
Add	Edit	Delete					

OK

Back

Click **Add** to add the Lync 2013 mediation server and also enable OPTIONS as shown in the previous step.

### Modify Agents

<b>Hostname:</b>	<input type="text" value="med2.lynclabsram.local"/>						
<b>IP address:</b>	<input type="text" value="172.16.31.98"/>						
<b>Port:</b>	<input type="text" value="5060"/> (Range: 0, 1025..65535)						
<b>State:</b>	<input checked="" type="checkbox"/>						
<b>Transport protocol:</b>	<input type="text" value="StaticTCP"/> ▼						
<b>TLS profile:</b>	<input type="text"/> ▼						
<b>Description:</b>	<input type="text" value="LYNC 2013 Mediation server 2"/>						
<b>Source context:</b>	<input type="text" value="Oracle.LYNC2013"/> ▼						
<b>Egress number translation mode:</b>	<input type="text" value="E164"/> ▼						
<b>Number of digits for n digit dialing:</b>	<input type="text" value="4"/> (Range: 0..25)						
<b>Prepend prefix on egress:</b>	<input type="text"/>						
<b>Inbound header manipulation:</b>	<input type="text" value="HMRfromLync"/> ▼						
<b>Outbound header manipulation:</b>	<input type="text" value="HMRtowardsLync"/> ▼						
<b>Apply outbound manipulation on:</b>	<input type="text" value="next-hop-only"/> ▼						
<b>Tags:</b>	<table border="1"><tr><td><b>Add</b></td><td><b>Edit</b></td><td><b>Delete</b></td></tr><tr><td colspan="3"> </td></tr></table>	<b>Add</b>	<b>Edit</b>	<b>Delete</b>			
<b>Add</b>	<b>Edit</b>	<b>Delete</b>					

OK

Back

Click **Add** to add the Skype for Business mediation server and also enable OPTIONS as shown in the previous step.

## Modify Agents

<b>Hostname:</b>	<input type="text" value="med2.sfb labdm.local"/>						
<b>IP address:</b>	<input type="text" value="172.16.29.45"/>						
<b>Port:</b>	<input type="text" value="5060"/> (Range: 0, 1025..65535)						
<b>State:</b>	<input checked="" type="checkbox"/>						
<b>Transport protocol:</b>	<input type="text" value="StaticTCP"/> ▼						
<b>TLS profile:</b>	<input type="text"/> ▼						
<b>Description:</b>	<input type="text" value="skype for business- med 2"/>						
<b>Source context:</b>	<input type="text" value="Oracle.SFB"/> ▼						
<b>Egress number translation mode:</b>	<input type="text" value="E164"/> ▼						
<b>Number of digits for n digit dialing:</b>	<input type="text" value="4"/> (Range: 0..25)						
<b>Prepend prefix on egress:</b>	<input type="text"/>						
<b>Inbound header manipulation:</b>	<input type="text" value="HMRfromLync"/> ▼						
<b>Outbound header manipulation:</b>	<input type="text" value="HMRtowardsLync"/> ▼						
<b>Apply outbound manipulation on:</b>	<input type="text" value="next-hop-only"/> ▼						
<b>Tags:</b>	<table border="1"><thead><tr><th>Add</th><th>Edit</th><th>Delete</th></tr></thead><tbody><tr><td colspan="3"> </td></tr></tbody></table>	Add	Edit	Delete			
Add	Edit	Delete					

OK

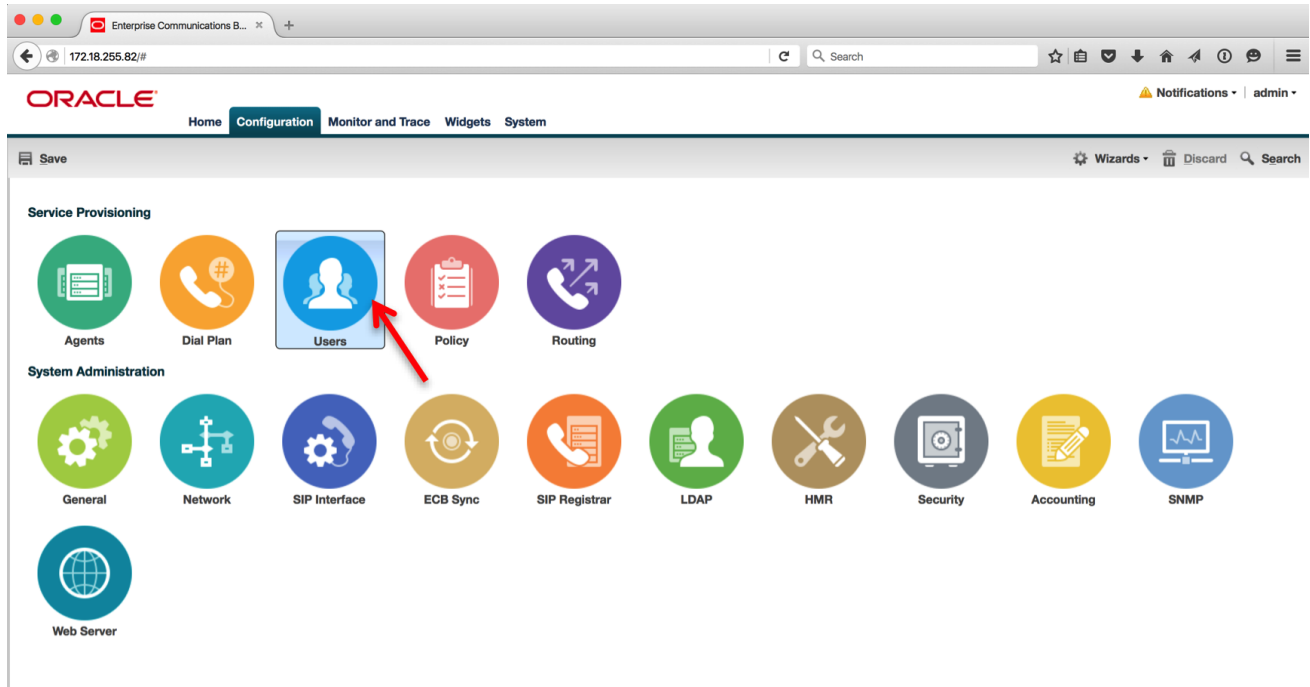
Back

## Configure Users

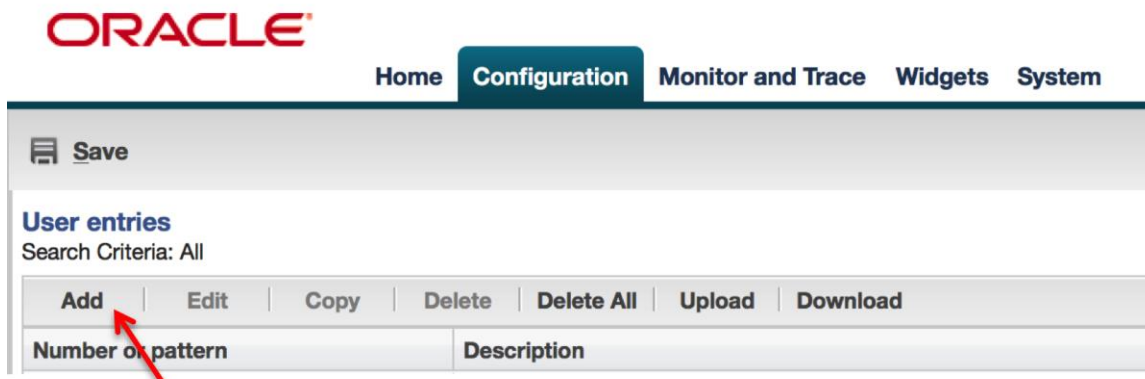
Next we will populate users in the User database. User entries can be added manually or uploaded in a format pre-configured to translate into a user database.

**If the ECB and Active Directory are configured for LDAP integration, then it is NOT necessary to define users in the User database on the ECB.**

Click on the **Users** icon under **Service Provisioning**.



The **User entries** page will be displayed. Click on **Add** to start adding users.





The **Add User entries** page will be displayed. You can enter the user numbers in E.164 format without the + (15712935327) or a number range (1571293[400-599]) in the **Number** field. Assign the appropriate **Agent** and **Dialing context** and click **OK**.

### Add User entries

**Number or pattern:**

15712935327

**Description:**

**Dialing context:**

Oracle.Avaya6\_3



**Agent:**

avaya6dot3



**Tags:**

Add

Edit

Delete

Add	Edit	Delete

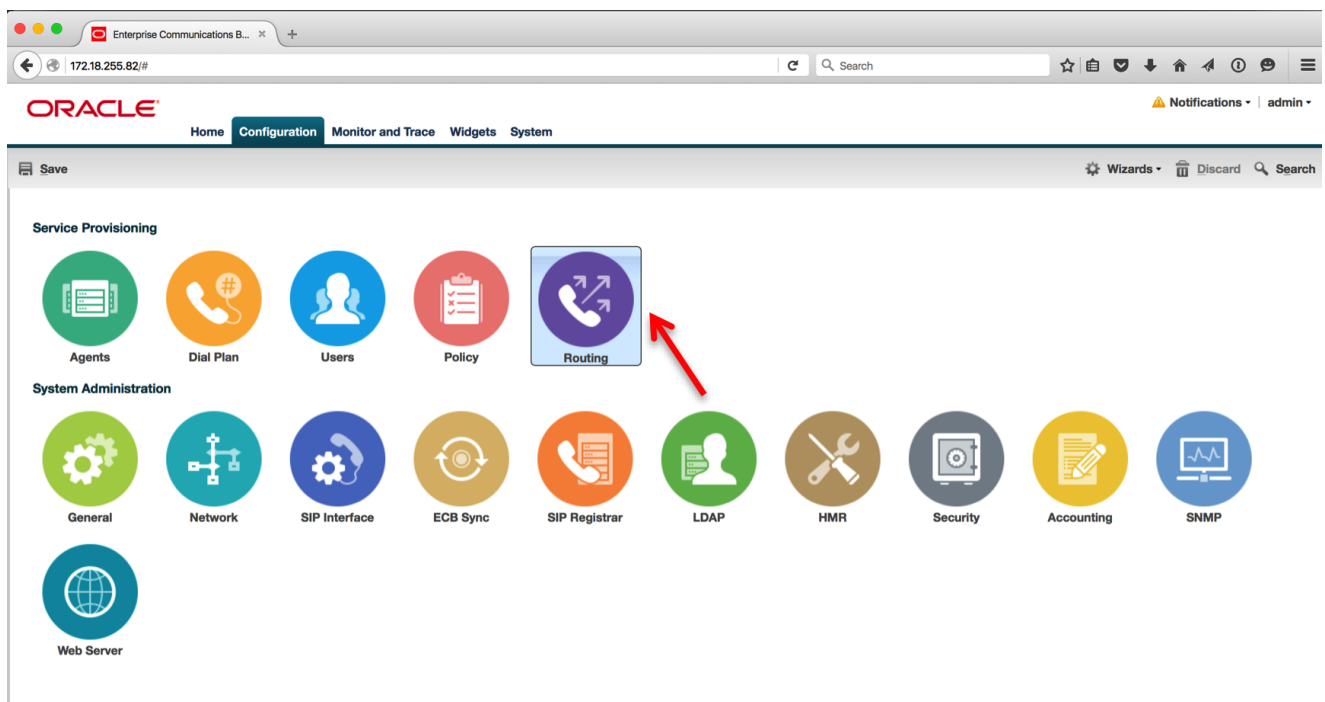
Continue adding users as shown above using the corresponding agents and dialing contexts.

## Configure Routing

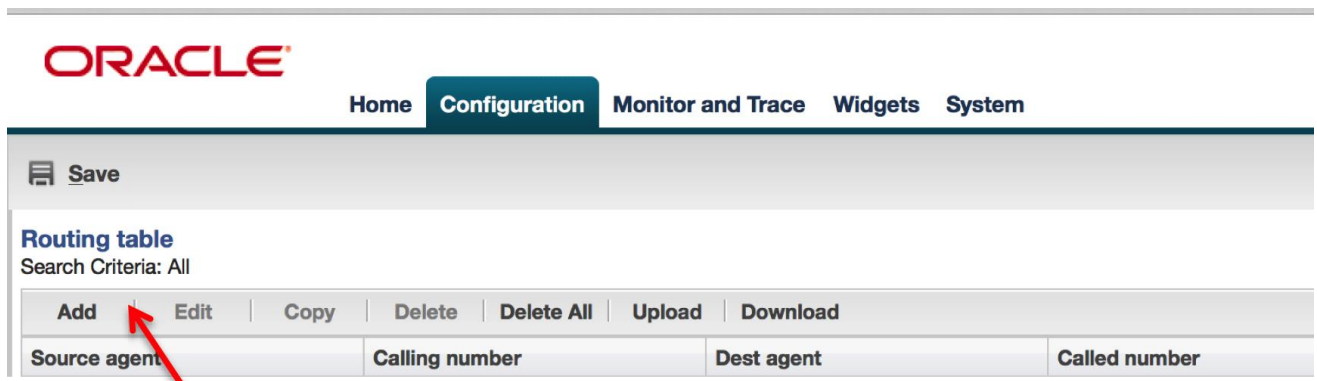
The ECB performs its session routing via the route configuration. The route configuration establishes hop-by-hop paths to signaling endpoints. Oracle ECB routing configuration allows the user to specify a route's cost to specify route preference. Cost may or may not be based on monetary considerations. But the reach of an enterprise's network often does allow the user to configure routes that keep session traffic within the enterprise infrastructure rather than incurring cost associated with a service provider.

The Oracle ECB allows for a range of route preference criteria to differentiate between routing paths. Criteria include source routing based on the agent or calling number. Target-oriented criteria are also available, allowing the enterprise to designate preferred paths for specific called numbers.

We need not configure a route for the users defined in the user database as the ECB will use their configured agents as next hop to route the calls. Since ECB does not support DNS load balancing as of now, the Lync users are assigned with one mediation server as their agent. To ensure the calls complete if the first mediation server in the pool goes down, we will configure a route to the second agent of the pool with a higher cost. On the **Configuration** tab click on the **Routing** icon under **Service Provisioning**.



On the **Routing table** page, click **Add** to add a route.



Add a routing entry for the Lync 2013 user – 15712935325 with the **Route** set to the second mediation server – med2.lyncclabsram.local with a cost of 20 and click **OK**.

### Modify Routing entry

<b>Source agent:</b>	<input type="text" value="*"/>							
<b>Calling number:</b>	<input type="text" value="*"/>							
<b>Dest agent:</b>	<input type="text" value="*"/>							
<b>Called number:</b>	<input type="text" value="15712935325"/>							
<b>Route:</b>	<input type="text" value="med2.lyncclabsram.local"/>							
<b>Cost:</b>	<input type="text" value="20"/>	(Range: 0..100)						
<b>Policy:</b>	<table border="1"><thead><tr><th>Add</th><th>Edit</th><th>Delete</th></tr></thead><tbody><tr><td colspan="3"> </td></tr></tbody></table>		Add	Edit	Delete			
Add	Edit	Delete						
<b>Description:</b>	<input type="text" value="failover route to lync 2013 mediation server 2"/>							

When the ECB receives a call for 15712935325, it looks up the user DB and finds that this user is associated to med1.lyncclabsram.local and routes the call to it. If this agent is down, ECB will find the above entry and route the call to the second agent of the pool – med2.lyncclabsram.local.

Configure a route for called number 91XXXXXXXXXX to point to the Oracle E-SBC. If a user dials an external number by dialing 9 and then 1 and the number, the ECB will route the call to the E-SBC to get to the service provider network.

### Modify Routing entry

**Source agent:** \*    
**Calling number:** \*   
**Dest agent:** \*    
**Called number:** 91XXXXXXXXXX   
**Route:** 10.64.3.122    
**Cost:** 5  (Range: 0..100)  
**Policy:**  |  |   
  
**Description:**

The **Routing Table** page will be displayed listing all the routes added. When you select a specific route, its **Route tree** is displayed at the bottom.

**Routing table**  
Search Criteria: All

Add	Edit	Copy	Delete	Delete All	Upload	Download	Search	Search	Clear
Source agent	Calling number	Dest agent	Called number	Route	Cost	Policy			
*	*	*	15712935320	10.71.2.10	0				
*	*	*	15712935325	med2.lynclabsram.local	20				
*	*	*	15712935326	med3.lynclabsram.local	0				
*	*	*	15712935327	avaya7	0				
*	*	*	15712935328	10.71.3.10	0				
*	*	*	91XXXXXXXXXXXX	10.64.3.122	5				

Displaying 1 - 6 of 6

---

**Route tree**

Cost	Hops
20	<div style="border: 1px solid black; padding: 2px; display: inline-block;">                     cost: 20                      called number: 15712935325                 </div> → med2.lynclabsram.local

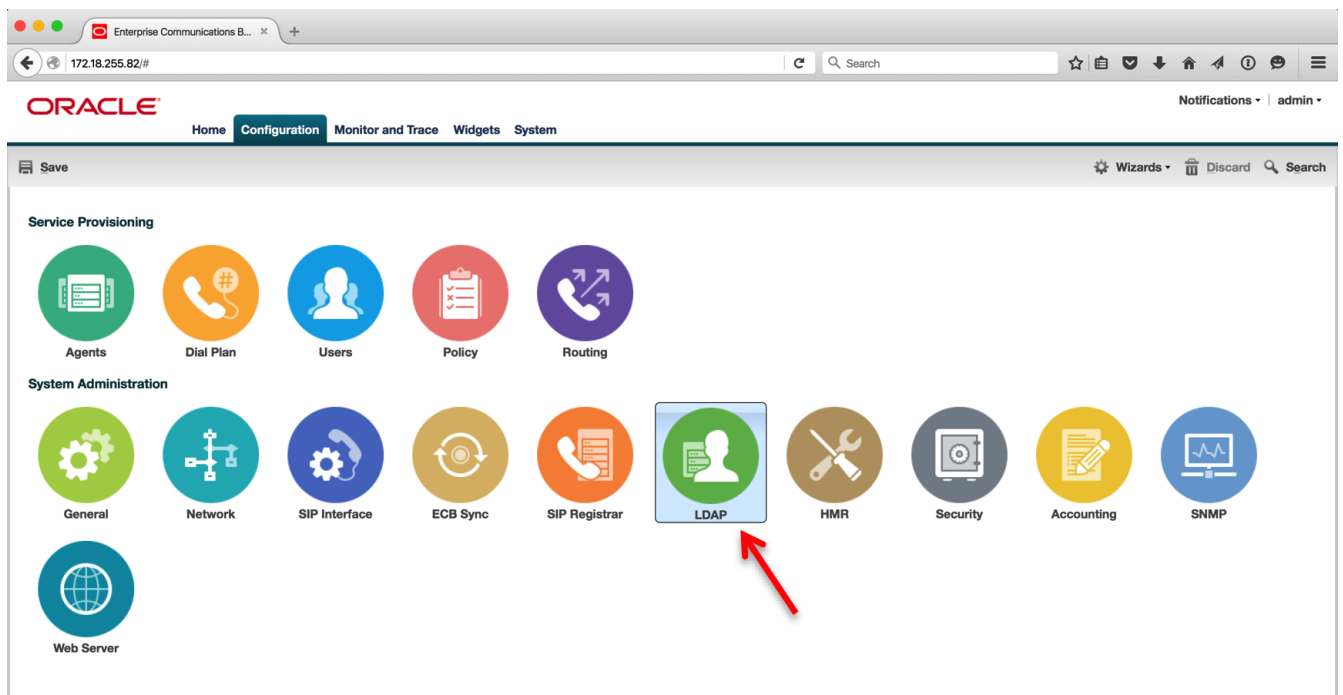
## Configure LDAP Integration with Active Directory

This is an optional step. If LDAP is used, then users do not need to be defined in the ECB's User database or in the Routing database. The Oracle ECB supports LDAP as a communications mechanism for interaction with an LDAP server. For many enterprises, this means utilizing Active Directory, a common LDAP-based service, to request information used in SIP session routing and authentication. The Oracle ECB's LDAP client requires configuration on the Oracle ECB and the LDAP server.

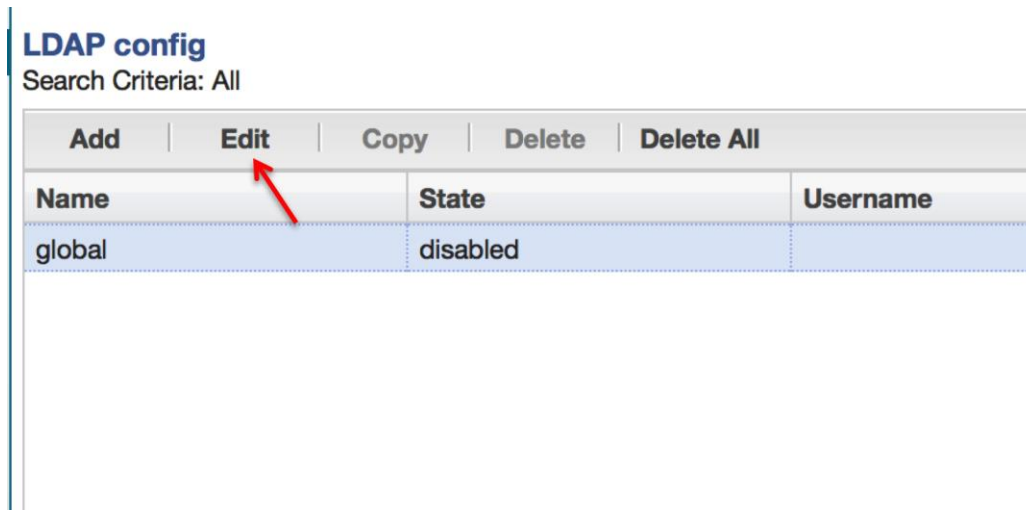
Configuration aspects of LDAP client configuration include:

- LDAP server access—The user specifies LDAP server location and access preferences.
- Routing queries—The user specifies the conditions wherein the Oracle ECB performs an LDAP dip to obtain location information (home agent) for FROM and REQUEST-URIs.
- AoR queries—Optionally searches for additional AoR matches in Active Directory so that it can create additional routes to target users that have contacts stored in separate records.

Click on the **LDAP** icon under **System Administration**.



Select the "global" LDAP config and click **Edit**.



Check the **State** checkbox to enable LDAP, then under **LDAP servers** click **Add**:

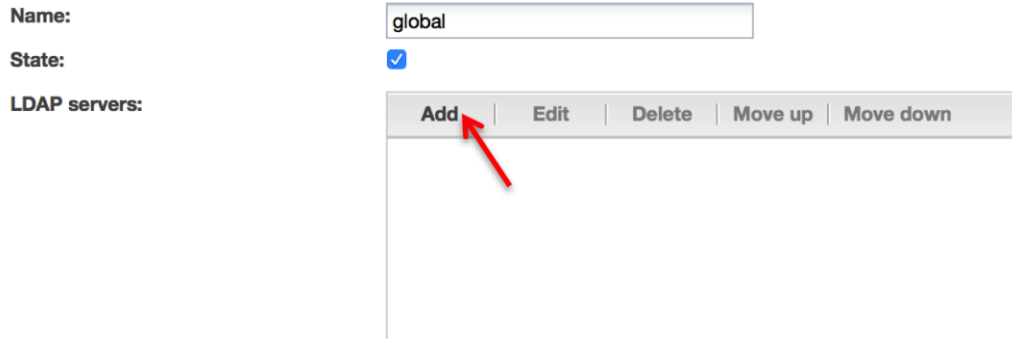
### Modify LDAP config

Name:

State:

LDAP servers:

<b>Add</b>	Edit	Delete	Move up	Move down
------------	------	--------	---------	-----------



Enter the LDAP server's IP address. If no port is specified, the ECB will use the default of 389.

Modify LDAP config

Name:

State:

LDAP servers:

<b>Add</b>	Edit	Delete	Move up	Move down
------------	------	--------	---------	-----------

**Add**

LDAP servers:

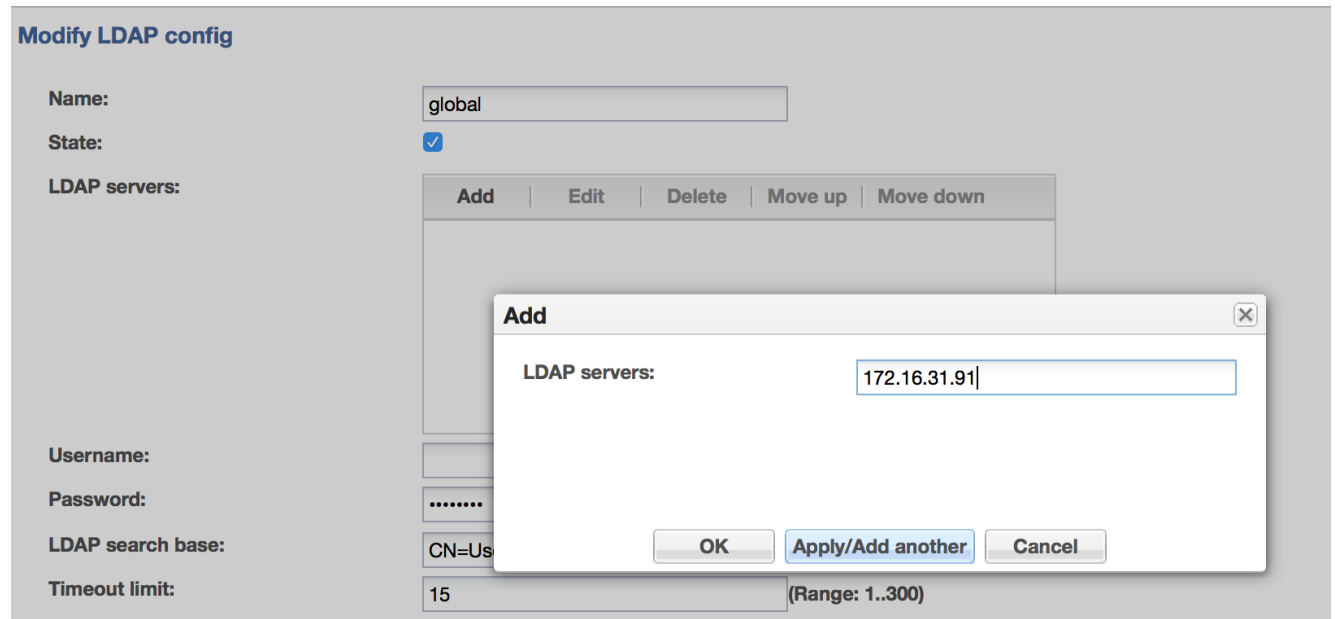
OK Apply/Add another Cancel

Username:

Password:

LDAP search base:

Timeout limit:  (Range: 1..300)



Click **Apply/Add another** to enter a secondary LDAP server IP, or click **OK** to use only one. If two are entered, the ECB will attempt to communicate with the first one, and if there is a failure, it will try the next server in the list on the next call.

Enter the LDAP sever username in the Username field, then click on Set next to the Password field to enter the LDAP server password.

### Modify LDAP config

**Name:**

**State:**

**LDAP servers:**

Add	Edit	Delete	Move up	Move down

**Username:**

**Password:**

Enter and re-enter the password, then click OK.

**Modify LDAP config**

**Name:**

**State:**

**LDAP servers:**

Add	Edit	Delete	Move up	Move down

**Username:**

**Password:**

**LDAP search base:**

**Timeout limit:**  (Range: 1..300)

**Max request timeouts:**  (Range: 0..10)

**Set Password**

**Password:**

**Confirm Password:**

Enter the **LDAP search base**. In the test lab, we used "CN=Users,DC=lynclabsram,DC=local" as shown in the following screenshot, where CN stands for Common Name and DC stands for Domain Component.

### Modify LDAP config

Name:

State:

LDAP servers:

Add	Edit	Delete	Move up	Move down

LDAP search base:

Username:

Password:

Timeout limit:  (Range: 1..300)

Max request timeouts:  (Range: 0..10)

Tcp keepalive:

Scroll down and select "attribute-order" under the **Route mode**.

### Modify LDAP config

LDAP search base:

Username:

Password:

Timeout limit:  (Range: 1..300)

Max request timeouts:  (Range: 0..10)

Tcp keepalive:

Security type:

TLS profile:

**Routing**

State:

Route mode:

From header replacement:

Lookup queries



Under the Lookup queries, click **Add**:

**Modify LDAP config**

Security type:

TLS profile:

Routing

State:

Route mode:

From header replacement:

Lookup queries

Add   Edit   Copy   Delete   Delete All   Move up   Move down				
Lookup number				
Attribute	Format type	Regex pattern	Regex result	Attribute

This is where attributes are referenced that determine the agent a user is assigned to. In the following example, msRTCSIP-Line is assigned to Lync 2013 and telephoneNumber is assigned to Cisco CUCM. When the ECB does an LDAP query, it will send these attributes. In the response, the server will return the attributes assigned to a particular user. Let's say the LDAP response returns both msRTCSIP-Line and telephoneNumber with value 15712935329, then the ECB knows to route the call to the same number on both Lync 2013 and CUCM. Whether it does this serially or in parallel depends on the SIP Interface "enable parallel forking" setting.

Add the following query and assign it to Lync 2013 (med3.lyncclabsram.local in our test lab). The Lookup number format type should be regular-expression, and the Home agent attribute can be anything. The Lookup number regex pattern and result are default values.

### Modify Lookup query

**Lookup number attribute:**

**Lookup number format type:**

**Lookup number regex pattern:**

**Lookup number regex result:**

**Home agent attribute:**

**Home agent regex pattern:**

**Home agent regex result:**

**Default home agent:**

**Fork group attribute:**

Add the following lookup query and assign it to Cisco CUCM:

### Modify Lookup query

Lookup number attribute:	telephoneNumber
Lookup number format type:	E164-no-plus
Lookup number regex pattern:	^\+?1?(d{3})(d{3})(d{4})\$
Lookup number regex result:	tel:+1\$1\$2\$3
Home agent attribute:	aaa
Home agent regex pattern:	
Home agent regex result:	
Default home agent:	10.71.2.10
Fork group attribute:	

Add other lookup queries as needed and determined by your Active Directory configuration.

When finished adding lookup queries, set the Lookup number format type to E164. Leave the Lookup number attribute at its default value of sAMAccountName.

### Modify LDAP config

Lookup queries

Add   Edit   Copy   Delete   Delete All   Move up   Move down				
Lookup number				
Attribute	Format type	Regex pattern	Regex result	Attribute
msRTCSIP-Line	regular-expression	^\+?1?(d{3})(d{3})...	tel:+1\$1\$2\$3	info
telephoneNumber	E164-no-plus	^\+?1?(d{3})(d{3})...	tel:+1\$1\$2\$3	aaa

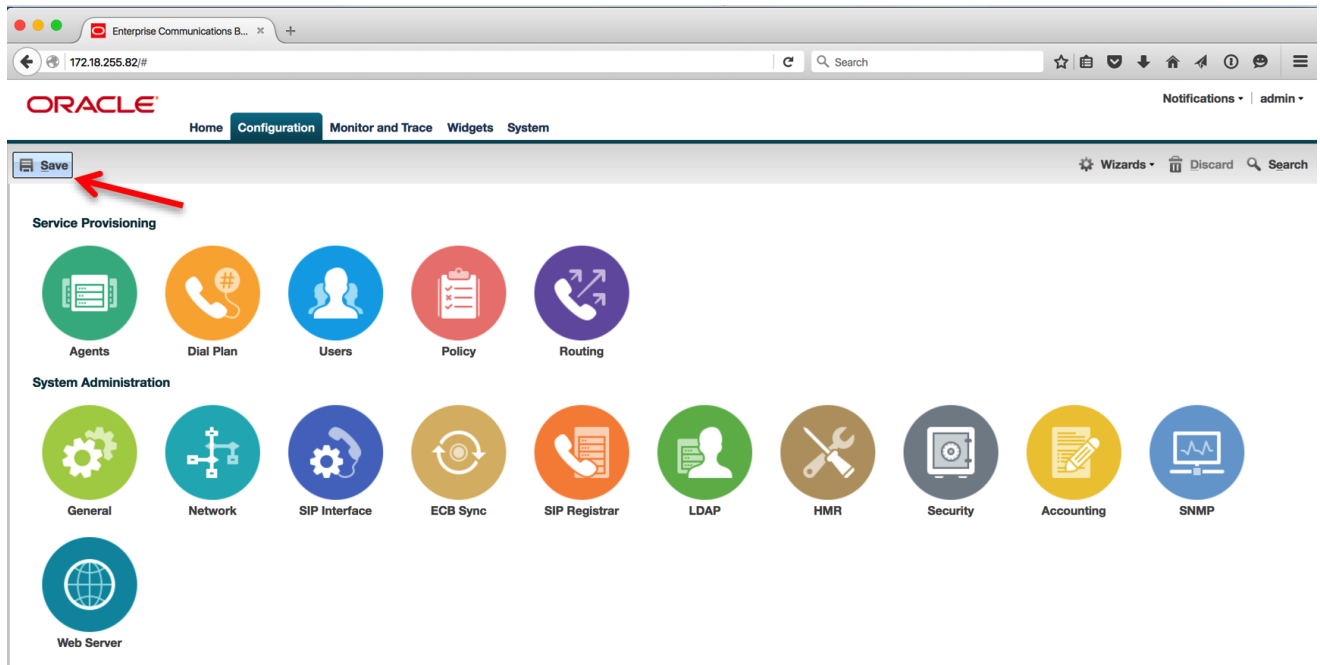
#### Address of record

Lookup number attribute:	sAMAccountName
Lookup number format type:	E164
Lookup number regex pattern:	

Click **OK** to finish the LDAP configuration.

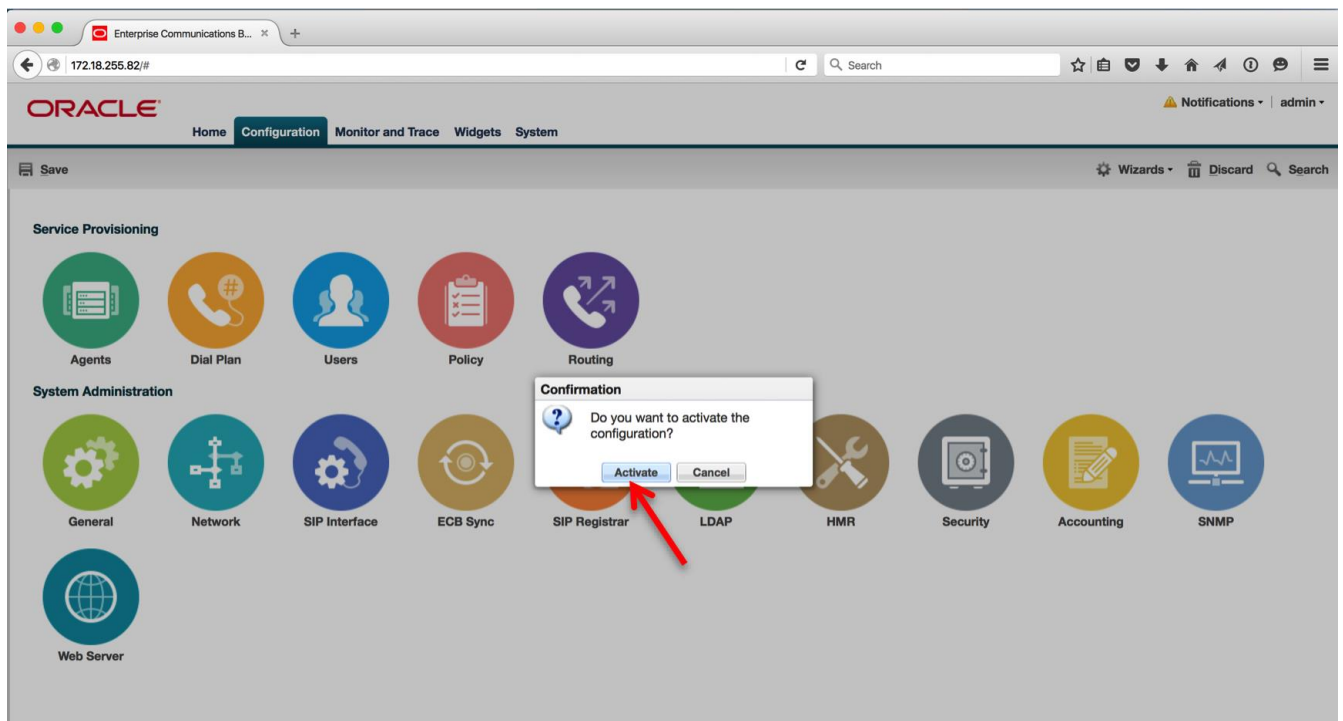
## Save and activate the configuration

We will now save and activate our ECB configuration. Click **Save** on the top left hand side of the **Configuration** tab.

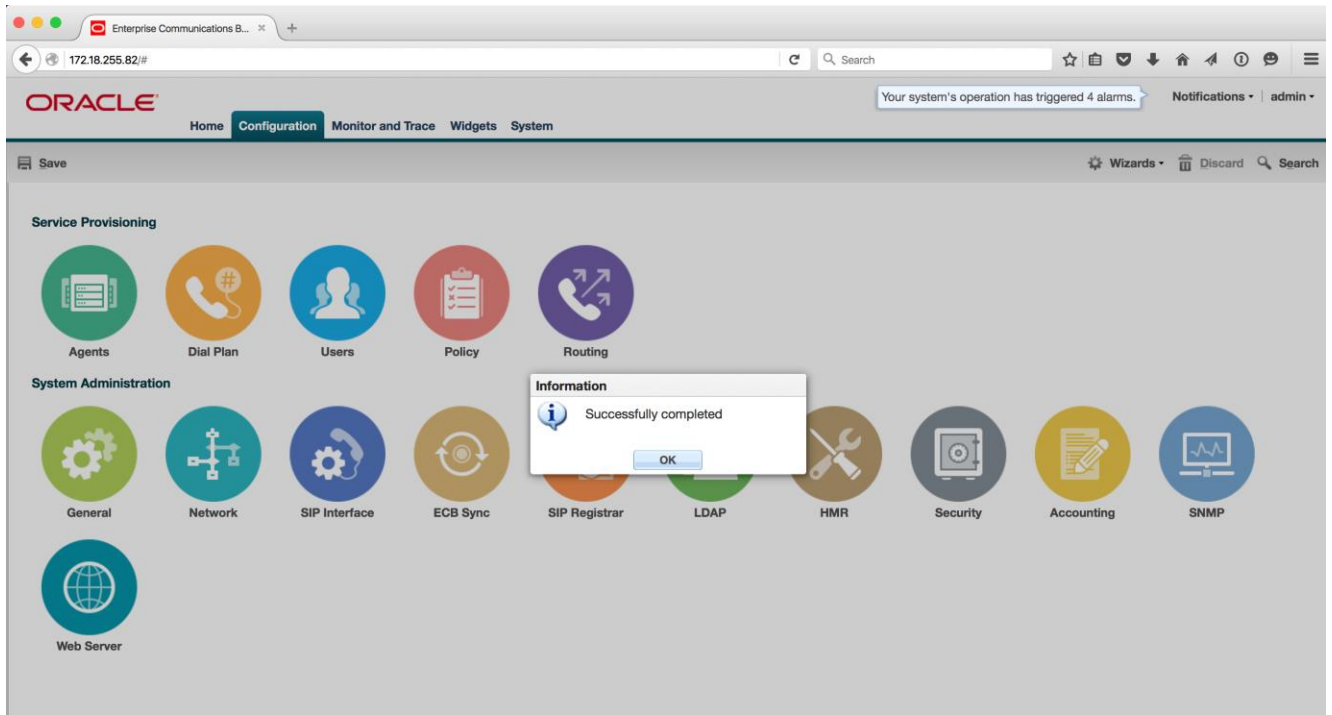


A progress dialog box will appear showing that the configuration is being saved.

You will be asked to confirm if you would like to activate the configuration. Click **Activate**.



After the activation is completed, you will see the screen below



Click OK and the ECB configuration is now complete.

## Phase 2 – Configuring the Oracle Enterprise SBC

In this section we describe the steps for configuring an Oracle Enterprise SBC (E-SBC) for use with the Oracle ECB, Microsoft Lync & Skype for Business, Cisco CUCM, and Avaya Aura. The E-SBC will connect the Enterprise network to the Service Provider network in a SIP trunking scenario.

### In Scope

The following guide for configuring the Oracle SBC assumes that this is a newly deployed device dedicated to a single customer. Please see the ACLI Configuration Guide on [http://docs.oracle.com/cd/E61547\\_01/index.html](http://docs.oracle.com/cd/E61547_01/index.html) for a better understanding of the Command Line Interface (CLI).

Note that Oracle offers several models of the SBC. This document covers the setup for the 1100, 3820, 4500, 4600, and 6300 platforms running OS ECZ7.3.0 MR-1 or later. If instructions are needed for other Oracle SBC models, please contact your Oracle representative.

### Out of Scope

- Configuration of Network management including SNMP and RADIUS
- Configuration of Distributed Denial of Service (DDoS) protection parameters as these are based on individual customer requirements.

### What will you need

- RJ45/DB9 serial adapter provided with the SBC, along with a straight-through Ethernet cable to go from the adapter to the SBC's console port (on the rear of the 1100, 4600, and 6300, and the front of the 3820 and 4500).
- Terminal emulation application such as PuTTY or HyperTerm
- Passwords for the User and Superuser modes on the Oracle SBC
- IP address to be assigned to the management interface (eth0, labeled Mgmt0 on the SBC chassis) of the SBC - the eth0 management interface must be connected and configured to a management network separate from the service interfaces. Otherwise the SBC is subject to ARP overlap issues, loss of system access when the network is down, and compromised DDoS protection. Oracle does not support SBC configurations with management and media/service interfaces on the same subnet.
- IP address of the Oracle ECB.
- IP addresses to be used for the SBC internal and external facing ports (Service Interfaces)

### SBC- Getting Started

Once the Oracle SBC is racked and the power cable connected, you are ready to set up physical network connectivity. **Note: use the console port on the front of the SBC, not the one on the back, on platforms such as the 3820 and 4500 that have two console ports.**

Plug the slot 0 port 0 (s0p0) interface into your outside (SIP Trunk-facing) network and the slot 1 port 0 (s1p0) interface into your inside (ECB-facing) network. Once connected, you are ready to power on and perform the following steps.

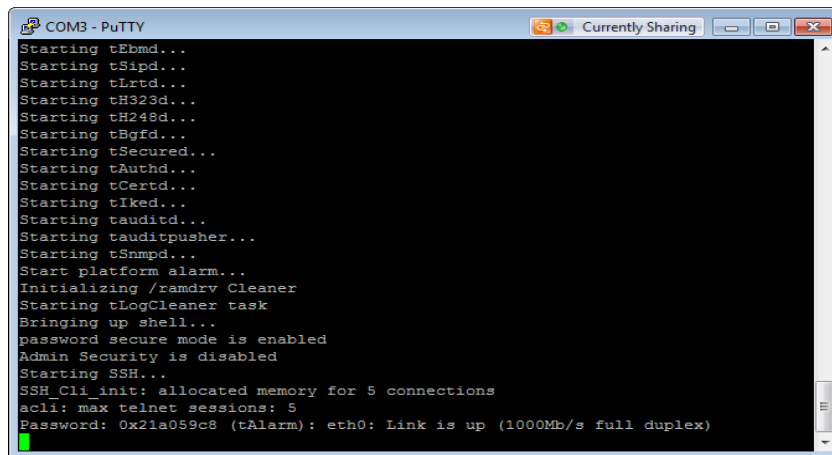
All commands are in bold, such as **configure terminal**; parameters in bold red such as **oraclesbc1** are parameters which are specific to an individual deployment. **Note:** The CLI is case sensitive.

## Establish the serial connection and logging in the SBC

Confirm the SBC is powered off and connect one end of a straight-through Ethernet cable to the console port on the SBC and the other end to console adapter that ships with the SBC, connect the console adapter (a DB9 adapter) to the DB9 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 bootup sequence.



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

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

```
Password: acme
oraclesbc1> enable
Password: packet
oraclesbc1# configure terminal
oraclesbc1(configuration)#
```

You are now in the global configuration mode.

### Initial Configuration – Assigning the management Interface an IP address

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

```
oraclesbc1# configure terminal --- >bootparams
```

- Once you type “bootparam” you have to use “carriage return” key to navigate down
- A reboot is required if changes are made to the existing bootparams. **Note these example boot parameters are specific to the 4600 platform. Other platforms will have different boot parameters. Use nnECZ730m1.64.bz for the 1100, 4500, 4600, and the 6300. Use nnECZ730m1.32.bz for the 3820.**

```
ORACLESBC1(configuration)# bootparam
'.' = clear field; '-' = go to previous field; a
= quit
```

```

Boot File           : /boot/nnECZ730m1.64.bz
IP Address          : 192.168.79.44
VLAN                :
Netmask             : 255.255.255.224
Gateway             : 192.168.79.33
IPv6 Address        :
IPv6 Gateway        :
Host IP             : 0.0.0.0
FTP username        : vxftp
FTP password        : vxftp123
Flags               :
Target Name         : oraclesbc1
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.

```

**Configuring the SBC**

The following section walks you through configuring the Oracle Enterprise SBC required to work with the Oracle Enterprise Communications Broker (ECB) in an environment with Microsoft Lync, Skype for Business, Cisco CUCM, and Avaya Aura.

It is outside the scope of this document to include all the interoperability working information as it will differ in every deployment.

**High Availability**

The Mgmt1 and Mgmt2 (labeled wancom1 and wancom2 in the configuration) ports which are on the rear panel of the SBC are used for the purpose of High Availability on the E-SBC. Crossover cables must be connected between these ports on the SBCs, i.e. Mgmt1 to Mgmt1 and Mgmt2 to Mgmt2. Please refer to the “High Availability Nodes” in the ACLI configuration guide for ECZ730 for more details.

**Local Policies**

Path: **configure terminal > session-router > local-policy**

```

local-policy
  from-address      *
  to-address        *
  source-realm      SIP-Trunk
  description
  activate-time
  deactivate-time
  state              enabled
  policy-priority   none
  policy-attribute
    next-hop        10.64.3.124
    realm            towards-ecb
  action            none
  terminate-recursion disabled
  carrier
  start-time        0000
  end-time          2400

```

```

days-of-week          U-S
cost                   0
state                  enabled
app-protocol           SIP
methods
media-profiles
lookup                 single
next-key
eloc-str-lkup          disabled
eloc-str-match

local-policy
  from-address          *
  to-address            *
  source-realm         towards-ecb
description
activate-time
deactivate-time
state                  enabled
policy-priority        none
policy-attribute
  next-hop             192.168.147.48
  realm                SIP-Trunk
action                 none
terminate-recursion    disabled
carrier
start-time             0000
end-time               2400
days-of-week          U-S
cost                   0
state                  enabled
app-protocol           SIP
methods
media-profiles
lookup                 single
next-key
eloc-str-lkup          disabled
eloc-str-match

```

## Media Manager

Path: **configure terminal > media-manager > media-manager > select > done**

```

media-manager
state                  enabled
latching               enabled
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
tcp-number-of-ports-per-flow 2
hnt-rtcp               disabled
algd-log-level         NOTICE
mbcd-log-level         NOTICE

```



```

options
red-flow-port 1985
red-mgcp-port 1986
red-max-trans 10000
red-sync-start-time 5000
red-sync-comp-time 1000
media-policing enabled
max-signaling-bandwidth 10000000
max-untrusted-signaling 100
min-untrusted-signaling 30
tolerance-window 30
trap-on-demote-to-deny disabled
trap-on-demote-to-untrusted disabled
syslog-on-demote-to-deny disabled
syslog-on-demote-to-untrusted disabled
rtcp-rate-limit 0
anonymous-sdp disabled
arp-msg-bandwidth 32000
rfc2833-timestamp disabled
default-2833-duration 100
rfc2833-end-pkts-only-for-non-sig enabled
translate-non-rfc2833-event disabled
media-supervision-traps disabled
dnsalg-server-failover disabled
syslog-on-call-reject disabled

```

## Network Interfaces

Path: **configure terminal > system > network-interface**

```

network-interface
  name s0p0
  sub-port-id 0
  description For SIP-Trunk
  hostname
  ip-address 192.168.79.126 (virtual IP)
  pri-utility-addr 192.168.79.127 (for HA only)
  sec-utility-addr 192.168.79.128 (for HA only)
  netmask 255.255.255.224
  gateway 192.168.79.97
  sec-gateway
  gw-heartbeat
    state disabled
    heartbeat 0
    retry-count 0
    retry-timeout 1
    health-score 0
  dns-ip-primary
  dns-ip-backup1
  dns-ip-backup2
  dns-domain
  dns-timeout 11
  signaling-mtu 0
  hip-ip-list 192.168.79.126 (add-hip-ip command)
  ftp-address

```

```

icmp-address 192.168.79.126 (add-icmp-ip command)
snmp-address
telnet-address
ssh-address
network-interface
  name slp0
  sub-port-id 0
  description Facing Oracle ECB
  hostname
  ip-address 10.64.3.122 (virtual IP)
  pri-utility-addr 10.64.3.120 (for HA only)
  sec-utility-addr 10.64.3.121 (for HA only)
  netmask 255.255.0.0
  gateway 10.64.1.1
  sec-gateway
  gw-heartbeat
    state disabled
    heartbeat 0
    retry-count 0
    retry-timeout 1
    health-score 0
  dns-ip-primary
  dns-ip-backup1
  dns-ip-backup2
  dns-domain
  dns-timeout 11
  signaling-mtu 0
  hip-ip-list 10.64.3.122 (add-hip-ip command)
  ftp-address
  icmp-address 10.64.3.122 (add-icmp-ip command)
  snmp-address
  telnet-address
  ssh-address 10.64.3.122 (add-ssh-ip command)
network-interface
  name wancom1
  sub-port-id 0
  description
  hostname
  ip-address
  pri-utility-addr 169.254.1.1
  sec-utility-addr 169.254.1.2
  netmask 255.255.255.252
  gateway
  sec-gateway
  gw-heartbeat
    state disabled
    heartbeat 0
    retry-count 0
    retry-timeout 1
    health-score 0
  dns-ip-primary
  dns-ip-backup1
  dns-ip-backup2
  dns-domain
  dns-timeout 11
  signaling-mtu 0

```

```

hip-ip-list
ftp-address
icmp-address
snmp-address
telnet-address
ssh-address
network-interface
  name                    wancom2
  sub-port-id             0
  description
  hostname
  ip-address
  pri-utility-addr       169.254.2.1
  sec-utility-addr       169.254.2.2
  netmask                255.255.255.252
  gateway
  sec-gateway
  gw-heartbeat
    state                  disabled
    heartbeat              0
    retry-count            0
    retry-timeout          1
    health-score           0
  dns-ip-primary
  dns-ip-backup1
  dns-ip-backup2
  dns-domain
  dns-timeout             11
  signaling-mtu           0
hip-ip-list
ftp-address
icmp-address
snmp-address
telnet-address
ssh-address

```

## Physical Interfaces

Path: `configure terminal > system > phy-interface`

```
phy-interface
  name                s0p0
  operation-type      Media
  port                0
  slot                0
  virtual-mac         00:08:25:04:0d:1e <- determine by
issuing the "show prom-info main" command from the # prompt, noting the starting
MAC address, and replacing the last character with "e". For HA only.
  admin-state         enabled
  auto-negotiation    enabled
  duplex-mode         FULL
  speed               100
  wancom-health-score 50
  overload-protection disabled

phy-interface
  name                slp0
  operation-type      Media
  port                0
  slot                1
  virtual-mac         00:08:25:04:0d:1f <- determine by
issuing the "show prom-info main" command from the # prompt, noting the starting
MAC address, and replacing the last character with "f". For HA only.
  admin-state         enabled
  auto-negotiation    enabled
  duplex-mode         FULL
  speed               100
  wancom-health-score 50
  overload-protection disabled

phy-interface
  name                wancom1
  operation-type      Control
  port                1
  slot                0
  virtual-mac
  admin-state         enabled
  auto-negotiation    enabled
  duplex-mode
  speed
  wancom-health-score 8
  overload-protection disabled

phy-interface
  name                wancom2
  operation-type      Control
  port                2
  slot                0
  virtual-mac
  admin-state         enabled
  auto-negotiation    enabled
  duplex-mode
  speed
  wancom-health-score 9
  overload-protection disabled
```

## Realm Configs

Path: `configure terminal > media-manager > realm-config`

```
realm-config
```

<b>identifier</b>	<b>SIP-Trunk</b>
description	
addr-prefix	0.0.0.0
<b>network-interfaces</b>	<b>s0p0:0</b>
<b>mm-in-realm</b>	<b>enabled</b>
mm-in-network	enabled
mm-same-ip	enabled
mm-in-system	enabled
bw-cac-non-mm	disabled
msm-release	disabled
qos-enable	disabled
max-bandwidth	0
fallback-bandwidth	0
max-priority-bandwidth	0
max-latency	0
max-jitter	0
max-packet-loss	0
observ-window-size	0
parent-realm	
dns-realm	
media-policy	
media-sec-policy	
srtm-msm-passthrough	disabled
class-profile	
in-translationid	
out-translationid	
in-manipulationid	
out-manipulationid	
average-rate-limit	0
access-control-trust-level	none
invalid-signal-threshold	0
maximum-signal-threshold	0
untrusted-signal-threshold	0
nat-trust-threshold	0
max-endpoints-per-nat	0
nat-invalid-message-threshold	0
wait-time-for-invalid-register	0
deny-period	30
cac-failure-threshold	0
untrust-cac-failure-threshold	0
ext-policy-svr	
diam-e2-address-realm	
subscription-id-type	END_USER_NONE
symmetric-latching	disabled
pai-strip	disabled
trunk-context	
device-id	
early-media-allow	
enforcement-profile	

additional-prefixes	
restricted-latching	none
restriction-mask	32
user-cac-mode	none
user-cac-bandwidth	0
user-cac-sessions	0
icmp-detect-multiplier	0
icmp-advertisement-interval	0
icmp-target-ip	
monthly-minutes	0
options	
spl-options	
accounting-enable	enabled
net-management-control	disabled
delay-media-update	disabled
refer-call-transfer	disabled
hold-refer-reinvite	disabled
refer-notify-provisional	none
dyn-refer-term	disabled
codec-policy	to-trunk
codec-manip-in-realm	disabled
codec-manip-in-network	enabled
rtcp-policy	
constraint-name	
session-recording-server	
session-recording-required	disabled
manipulation-string	
manipulation-pattern	
stun-enable	disabled
stun-server-ip	0.0.0.0
stun-server-port	3478
stun-changed-ip	0.0.0.0
stun-changed-port	3479
sip-profile	
sip-isup-profile	
match-media-profiles	
qos-constraint	
block-rtcp	disabled
hide-egress-media-update	disabled
tcp-media-profile	
monitoring-filters	
node-functionality	
default-location-string	
alt-family-realm	
pref-addr-type	none
realm-config	
<b>identifier</b>	<b>towards-ecb</b>
description	
addr-prefix	0.0.0.0
<b>network-interfaces</b>	<b>slp0:0</b>
<b>mm-in-realm</b>	<b>enabled</b>
mm-in-network	enabled
mm-same-ip	enabled
mm-in-system	enabled
bw-cac-non-mm	disabled
msm-release	disabled

qos-enable	disabled
max-bandwidth	0
fallback-bandwidth	0
max-priority-bandwidth	0
max-latency	0
max-jitter	0
max-packet-loss	0
observ-window-size	0
parent-realm	
dns-realm	
media-policy	
media-sec-policy	
srtp-msm-passthrough	disabled
class-profile	
in-translationid	
out-translationid	
in-manipulationid	
out-manipulationid	
average-rate-limit	0
access-control-trust-level	none
invalid-signal-threshold	0
maximum-signal-threshold	0
untrusted-signal-threshold	0
nat-trust-threshold	0
max-endpoints-per-nat	0
nat-invalid-message-threshold	0
wait-time-for-invalid-register	0
deny-period	30
cac-failure-threshold	0
untrust-cac-failure-threshold	0
ext-policy-svr	
diam-e2-address-realm	
subscription-id-type	END_USER_NONE
symmetric-latching	disabled
pai-strip	disabled
trunk-context	
device-id	
early-media-allow	
enforcement-profile	
additional-prefixes	
restricted-latching	none
restriction-mask	32
user-cac-mode	none
user-cac-bandwidth	0
user-cac-sessions	0
icmp-detect-multiplier	0
icmp-advertisement-interval	0
icmp-target-ip	
monthly-minutes	0
options	
spl-options	
accounting-enable	enabled
net-management-control	disabled
delay-media-update	disabled
refer-call-transfer	enabled
hold-refer-reinvite	disabled

refer-notify-provisional	none
dyn-refer-term	disabled
codec-policy	
codec-manip-in-realm	disabled
codec-manip-in-network	enabled
rtcp-policy	
constraint-name	
session-recording-server	
session-recording-required	disabled
manipulation-string	
manipulation-pattern	
stun-enable	disabled
stun-server-ip	0.0.0.0
stun-server-port	3478
stun-changed-ip	0.0.0.0
stun-changed-port	3479
sip-profile	
sip-isup-profile	
match-media-profiles	
qos-constraint	
block-rtcp	disabled
hide-egress-media-update	disabled
tcp-media-profile	
monitoring-filters	
node-functionality	
default-location-string	
alt-family-realm	
pref-addr-type	none



## Redundancy Config (HA Pairs Only)

Path: `configure terminal > system > redundancy > select`

```
redundancy-config
  state                enabled
  log-level            INFO
  health-threshold     75
  emergency-threshold  50
  port                 9090
  advertisement-time   500
  percent-drift        210
  initial-time         1250
  becoming-standby-time 180000
  becoming-active-time 100
  cfg-port             1987
  cfg-max-trans        10000
  cfg-sync-start-time  5000
  cfg-sync-comp-time   1000
  gateway-heartbeat-interval 0
  gateway-heartbeat-retry 0
  gateway-heartbeat-timeout 1
  gateway-heartbeat-health 0
  media-if-peercheck-time 0
  peer
    name                oraclesbc1 <- must match
Primary SBC's target name in boot parameters
    state                enabled
    type                 Primary
    destination
      address            169.254.1.1:9090
      network-interface  wancom1:0
    destination
      address            169.254.2.1:9090
      network-interface  wancom2:0
  peer
    name                oraclesbc2 <- must match
Secondary SBC's target name in boot parameters
    state                enabled
    type                 Secondary
    destination
      address            169.254.1.2:9090
      network-interface  wancom1:0
    destination
      address            169.254.2.2:9090
      network-interface  wancom2:0
```

## Session Agents

Path: `configure terminal > session-router > session-agent`

```
session-agent
  hostname 10.64.3.124
  ip-address 10.64.3.124
  port 5060
  state enabled
  app-protocol SIP
  app-type
  transport-method StaticTCP
  realm-id towards-ecb
  egress-realm-id
  description
  carriers
  allow-next-hop-lp enabled
  constraints disabled
  max-sessions 0
  max-inbound-sessions 0
  max-outbound-sessions 0
  max-burst-rate 0
  max-inbound-burst-rate 0
  max-outbound-burst-rate 0
  max-sustain-rate 0
  max-inbound-sustain-rate 0
  max-outbound-sustain-rate 0
  min-seizures 5
  min-asr 0
  time-to-resume 0
  ttr-no-response 0
  in-service-period 0
  burst-rate-window 0
  sustain-rate-window 0
  req-uri-carrier-mode None
  proxy-mode
  redirect-action
  loose-routing enabled
  send-media-session enabled
  response-map
  ping-method OPTIONS;hops=0
  ping-interval 30
  ping-send-mode keep-alive
  ping-all-addresses disabled
  ping-in-service-response-codes
  out-service-response-codes
  load-balance-dns-query hunt
  options
  spl-options
  media-profiles
  in-translationid
  out-translationid
  trust-me disabled
  request-uri-headers
  stop-recurse
  local-response-map
```

ping-to-user-part	
ping-from-user-part	
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	
enforcement-profile	
refer-call-transfer	disabled
refer-notify-provisional	none
reuse-connections	NONE
tcp-keepalive	none
tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0
sip-profile	
sip-isup-profile	
kpml-interworking	inherit
monitoring-filters	
session-recording-server	
session-recording-required	disabled
hold-refer-reinvite	disabled
send-tcp-fin	disabled
session-agent	
<b>hostname</b>	<b>192.168.147.48</b>
<b>ip-address</b>	<b>192.168.147.48</b>
<b>port</b>	<b>5060</b>
state	enabled
app-protocol	SIP
app-type	
<b>transport-method</b>	<b>UDP</b>
<b>realm-id</b>	<b>SIP-Trunk</b>
egress-realm-id	
description	
carriers	
allow-next-hop-lp	enabled
constraints	disabled
max-sessions	0
max-inbound-sessions	0
max-outbound-sessions	0
max-burst-rate	0
max-inbound-burst-rate	0
max-outbound-burst-rate	0
max-sustain-rate	0
max-inbound-sustain-rate	0
max-outbound-sustain-rate	0
min-seizures	5
min-asr	0
time-to-resume	0

ttr-no-response	0
in-service-period	0
burst-rate-window	0
sustain-rate-window	0
req-uri-carrier-mode	None
proxy-mode	
redirect-action	
loose-routing	enabled
send-media-session	enabled
response-map	
<b>ping-method</b>	<b>OPTIONS</b>
<b>ping-interval</b>	<b>30</b>
ping-send-mode	keep-alive
ping-all-addresses	disabled
ping-in-service-response-codes	
out-service-response-codes	
load-balance-dns-query	hunt
options	
spl-options	
media-profiles	
in-translationid	
<b>out-translationid</b>	<b>stripplus1</b>
trust-me	disabled
request-uri-headers	
stop-recurse	
local-response-map	
ping-to-user-part	
ping-from-user-part	
in-manipulationid	
out-manipulationid	
manipulation-string	
manipulation-pattern	
p-asserted-id	
trunk-group	
max-register-sustain-rate	0
early-media-allow	
invalidate-registrations	disabled
rfc2833-mode	none
rfc2833-payload	0
codec-policy	
enforcement-profile	
refer-call-transfer	disabled
refer-notify-provisional	none
reuse-connections	NONE
tcp-keepalive	none
tcp-reconn-interval	0
max-register-burst-rate	0
register-burst-window	0
sip-profile	
sip-isup-profile	
kpml-interworking	inherit
monitoring-filters	
session-recording-server	
session-recording-required	disabled
hold-refer-reinvite	disabled
send-tcp-fin	disabled

## Session Translation

Path: `configure terminal > session-router > session-translation`

```
session-translation
  id                stripplus1
  rules-calling     stripplus1
  rules-called      stripplus1
```

## SIP Config

Path: `configure terminal > session-router > sip-config > select`

```
sip-config
  state                enabled
  operation-mode       dialog
  dialog-transparency  enabled
  home-realm-id       towards-ecb
  egress-realm-id
  auto-realm-id
  nat-mode             None
  registrar-domain   *
  registrar-host    *
  registrar-port       0
  register-service-route always
  init-timer           500
  max-timer            4000
  trans-expire         32
  initial-inv-trans-expire 0
  invite-expire        180
  inactive-dynamic-conn 32
  enforcement-profile
  pac-method
  pac-interval         10
  pac-strategy         PropDist
  pac-load-weight      1
  pac-session-weight   1
  pac-route-weight     1
  pac-callid-lifetime  600
  pac-user-lifetime    3600
  red-sip-port         1988
  red-max-trans        10000
  red-sync-start-time  5000
  red-sync-comp-time   1000
  options            max-udp-length=0
  add-reason-header    disabled
  sip-message-len      4096
  enum-sag-match       disabled
  extra-method-stats   disabled
  extra-enum-stats     disabled
  rph-feature          disabled
  nsep-user-sessions-rate 0
  nsep-sa-sessions-rate 0
  registration-cache-limit 0
  register-use-to-for-lp disabled
  refer-src-routing    disabled
```

add-ucid-header	disabled
proxy-sub-events	
allow-pani-for-trusted-only	disabled
atcf-stn-sr	
atcf-psi-dn	
atcf-route-to-sccas	disabled
eatf-stn-sr	
pass-gruu-contact	disabled
sag-lookup-on-redirect	disabled
set-disconnect-time-on-bye	disabled
msrp-delayed-bye-timer	15
transcoding-realm	
transcoding-agents	
create-dynamic-sa	disabled
node-functionality	P-CSCF
match-sip-instance	disabled
sa-routes-stats	disabled
sa-routes-traps	disabled
rx-sip-reason-mapping	disabled
add-ue-location-in-pani	disabled
hold-emergency-calls-for-loc-info	0

### SIP Feature

Path: **configure terminal > session-router > sip-feature**

sip-feature	
<b>name</b>	<b>100rel</b>
<b>realm</b>	<b>SIP-Trunk</b>
support-mode-inbound	Pass
<b>require-mode-inbound</b>	<b>Pass</b>
proxy-require-mode-inbound	Pass
support-mode-outbound	Pass
<b>require-mode-outbound</b>	<b>Pass</b>
proxy-require-mode-outbound	Pass

### SIP Interfaces

Path: **configure terminal > session-router > sip-interface**

sip-interface	
state	enabled
<b>realm-id</b>	<b>SIP-Trunk</b>
description	
sip-port	
<b>address</b>	<b>192.168.79.126</b>
port	5060
<b>transport-protocol</b>	<b>UDP</b>
tls-profile	
allow-anonymous	all
multi-home-addr	
ims-aka-profile	
carriers	
trans-expire	0

```

initial-inv-trans-expire      0
invite-expire                 0
max-redirect-contacts        0
proxy-mode
redirect-action
contact-mode                  none
nat-traversal                 none
nat-interval                  30
tcp-nat-interval             90
registration-caching          disabled
min-reg-expire                300
registration-interval        3600
route-to-registrar            disabled
secured-network               disabled
teluri-scheme                 disabled
uri-fqdn-domain
options
spl-options
trust-mode                    all
max-nat-interval              3600
nat-int-increment             10
nat-test-increment            30
sip-dynamic-hnt               disabled
stop-recurse                  401,407
port-map-start                0
port-map-end                  0
in-manipulationid
out-manipulationid          NAT_IP
sip-ims-feature               disabled
sip-atcf-feature              disabled
subscribe-reg-event           disabled
operator-identifier
anonymous-priority            none
max-incoming-conns            0
per-src-ip-max-incoming-conns 0
inactive-conn-timeout         0
untrusted-conn-timeout        0
network-id
ext-policy-server
ldap-policy-server
default-location-string
term-tgrp-mode                none
charging-vector-mode           pass
charging-function-address-mode pass
ccf-address
ecf-address
implicit-service-route        disabled
rfc2833-payload               101
rfc2833-mode                   transparent
constraint-name
response-map
local-response-map
sec-agree-feature              disabled
sec-agree-pref                 ipsec3gpp
enforcement-profile
route-unauthorized-calls

```

tcp-keepalive	none
add-sdp-invite	disabled
p-early-media-header	disabled
p-early-media-direction	
add-sdp-profiles	
manipulation-string	
manipulation-pattern	
sip-profile	
sip-isup-profile	
tcp-conn-dereg	0
tunnel-name	
register-keep-alive	none
kpml-interworking	disabled
msrp-delay-egress-bye	disabled
send-380-response	
pcscf-restoration	
session-timer-profile	
session-recording-server	
session-recording-required	disabled
service-tag	
reg-cache-route	disabled
sip-interface	
state	enabled
<b>realm-id</b>	<b>towards-ecb</b>
description	
sip-port	
<b>address</b>	<b>10.64.3.122</b>
port	5060
<b>transport-protocol</b>	<b>TCP</b>
tls-profile	
allow-anonymous	all
multi-home-addr	
ims-aka-profile	
carriers	
trans-expire	0
initial-inv-trans-expire	0
invite-expire	0
max-redirect-contacts	0
proxy-mode	
redirect-action	
contact-mode	none
nat-traversal	none
nat-interval	30
tcp-nat-interval	90
registration-caching	disabled
min-reg-expire	300
registration-interval	3600
route-to-registrar	disabled
secured-network	disabled
teluri-scheme	disabled
uri-fqdn-domain	
<b>options</b>	<b>100rel-interworking</b>
spl-options	
trust-mode	all
max-nat-interval	3600
nat-int-increment	10



nat-test-increment	30
sip-dynamic-hnt	disabled
stop-recurse	401,407
port-map-start	0
port-map-end	0
in-manipulationid	
<b>out-manipulationid</b>	<b>NAT_IP</b>
sip-ims-feature	disabled
sip-atcf-feature	disabled
subscribe-reg-event	disabled
operator-identifier	
anonymous-priority	none
max-incoming-conns	0
per-src-ip-max-incoming-conns	0
inactive-conn-timeout	0
untrusted-conn-timeout	0
network-id	
ext-policy-server	
ldap-policy-server	
default-location-string	
term-tgrp-mode	none
charging-vector-mode	pass
charging-function-address-mode	pass
ccf-address	
ecf-address	
implicit-service-route	disabled
rfc2833-payload	101
rfc2833-mode	transparent
constraint-name	
response-map	
local-response-map	
sec-agree-feature	disabled
sec-agree-pref	ipsec3gpp
enforcement-profile	
route-unauthorized-calls	
tcp-keepalive	none
add-sdp-invite	disabled
p-early-media-header	disabled
p-early-media-direction	
add-sdp-profiles	
manipulation-string	
manipulation-pattern	
sip-profile	
sip-isup-profile	
tcp-conn-dereg	0
tunnel-name	
register-keep-alive	none
kpml-interworking	disabled
msrp-delay-egress-bye	disabled
send-380-response	
pcscf-restoration	
session-timer-profile	
session-recording-server	
session-recording-required	disabled
service-tag	
reg-cache-route	disabled

## SIP Manipulations (Header Manipulation Rules – HMR)

Path: `configure terminal > session-router > sip-manipulation`

```
sip-manipulation
  name NAT_IP
  description
  split-headers
  join-headers
  header-rule
    name
    header-name natFrom
    action From
    comparison-type manipulate
    msg-type case-sensitive
    methods request
    match-value
    new-value
    element-rule
      name natFromHost
      parameter-name
      type uri-host
      action replace
      match-val-type any
      comparison-type case-sensitive
      match-value
      new-value $LOCAL_IP
  header-rule
    name
    header-name natTo
    action To
    comparison-type manipulate
    msg-type case-sensitive
    methods request
    match-value
    new-value
    element-rule
      name natToHost
      parameter-name
      type uri-host
      action replace
      match-val-type any
      comparison-type case-sensitive
      match-value
      new-value $REMOTE_IP
```

## SIP Monitoring

Path: `configure terminal > session-router > sip-monitoring > select`

sip-monitoring	
match-any-filter	disabled
<b>state</b>	<b>enabled</b>
short-session-duration	0
<b>monitoring-filters</b>	<b>*</b>
trigger-window	30

## Steering Pools

Path: `configure terminal > media-manager > steering-pool`

steering-pool	
<b>ip-address</b>	<b>10.64.3.122</b>
<b>start-port</b>	<b>49152</b>
<b>end-port</b>	<b>65535</b>
<b>realm-id</b>	<b>towards-ecb</b>
network-interface	
steering-pool	
<b>ip-address</b>	<b>192.168.79.126</b>
<b>start-port</b>	<b>49152</b>
<b>end-port</b>	<b>65535</b>
<b>realm-id</b>	<b>SIP-Trunk</b>
network-interface	

## System Config

Path: `configure terminal > system > system-config > select`

system-config	
<b>hostname</b>	<b>ORACLESB</b>
<b>description</b>	<b>4600 for ECB Testing</b>
location	
mib-system-contact	
mib-system-name	
mib-system-location	
snmp-enabled	enabled
enable-snmp-auth-traps	disabled
enable-snmp-syslog-notify	disabled
enable-snmp-monitor-traps	disabled
enable-env-monitor-traps	disabled
enable-mblk_tracking	disabled
snmp-syslog-his-table-length	1
snmp-syslog-level	WARNING
system-log-level	WARNING
<b>process-log-level</b>	<b>DEBUG (change to NOTICE after testing is complete)</b>
process-log-ip-address	0.0.0.0
process-log-port	0
collect	
sample-interval	5
push-interval	15

boot-state	disabled
start-time	now
end-time	never
red-collect-state	disabled
red-max-trans	1000
red-sync-start-time	5000
red-sync-comp-time	1000
push-success-trap-state	disabled
comm-monitor	
state	disabled
sbc-grp-id	0
tls-profile	
qos-enable	enabled
interim-qos-update	disabled
call-trace	disabled
internal-trace	disabled
log-filter	all
<b>default-gateway</b>	<b>192.168.79.33</b>
restart	enabled
exceptions	
telnet-timeout	0
console-timeout	0
remote-control	enabled
cli-audit-trail	enabled
link-redundancy-state	disabled
<b>source-routing</b>	<b>enabled</b>
cli-more	disabled
terminal-height	24
debug-timeout	0
trap-event-lifetime	0
ids-syslog-facility	-1
options	
default-v6-gateway	::
ipv6-signaling-mtu	1500
ipv4-signaling-mtu	1500
cleanup-time-of-day	00:00
snmp-engine-id-suffix	
snmp-agent-mode	v1v2

### Translation Rules

Path: **configure terminal > session-router > translation-rule**

translation-rules	
<b>id</b>	<b>stripplus1</b>
<b>type</b>	<b>delete</b>
add-string	
add-index	0
<b>delete-string</b>	<b>+1</b>
<b>delete-index</b>	<b>0</b>

## Web Server Config

Path: `configure terminal > system > web-server-config > select`

web-server-config	
state	enabled
inactivity-timeout	5
http-state	enabled
http-port	80
https-state	disabled
https-port	443
tls-profile	

## Save, Activate, and Reboot

You will now save your configuration with the `save-config` command. This will make it persistent through reboots, but it will not take effect until after you issue the `activate-config` command. Some config elements are not Real-Time Configuration (RTC) supported, so a reboot is required after the initial configuration.

```
oraclesbcl# save-config
checking configuration
Save-Config received, processing.
waiting for request to finish
Request to 'SAVE-CONFIG' has Finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
oraclesbcl# activate-config
Activate-Config received, processing.
waiting for request to finish
Setting phy0 on Slot=0, Port=0, MAC=00:08:25:03:FC:43,
VMAC=00:08:25:03:FC:43
Setting phy1 on Slot=1, Port=0, MAC=00:08:25:03:FC:45,
VMAC=00:08:25:03:FC:45
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
oraclesbcl# reboot force
```

The E-SBC configuration is now complete.

## Phase 3 – Configuring Active Directory for LDAP Integration with the ECB

In this section we describe the steps for configuring Active Directory (AD) for LDAP integration with the ECB. **This step is optional.** It allows the ECB to receive routing information from AD for users on a per-call basis and can be used for parallel or serial call forking, such as having a user with the same number ring on both Skype for Business and Cisco CUCM. If a user is already defined on the Lync or Skype for Business server, then the user will already exist with the “msRTCSIP-Line” parameter in AD.

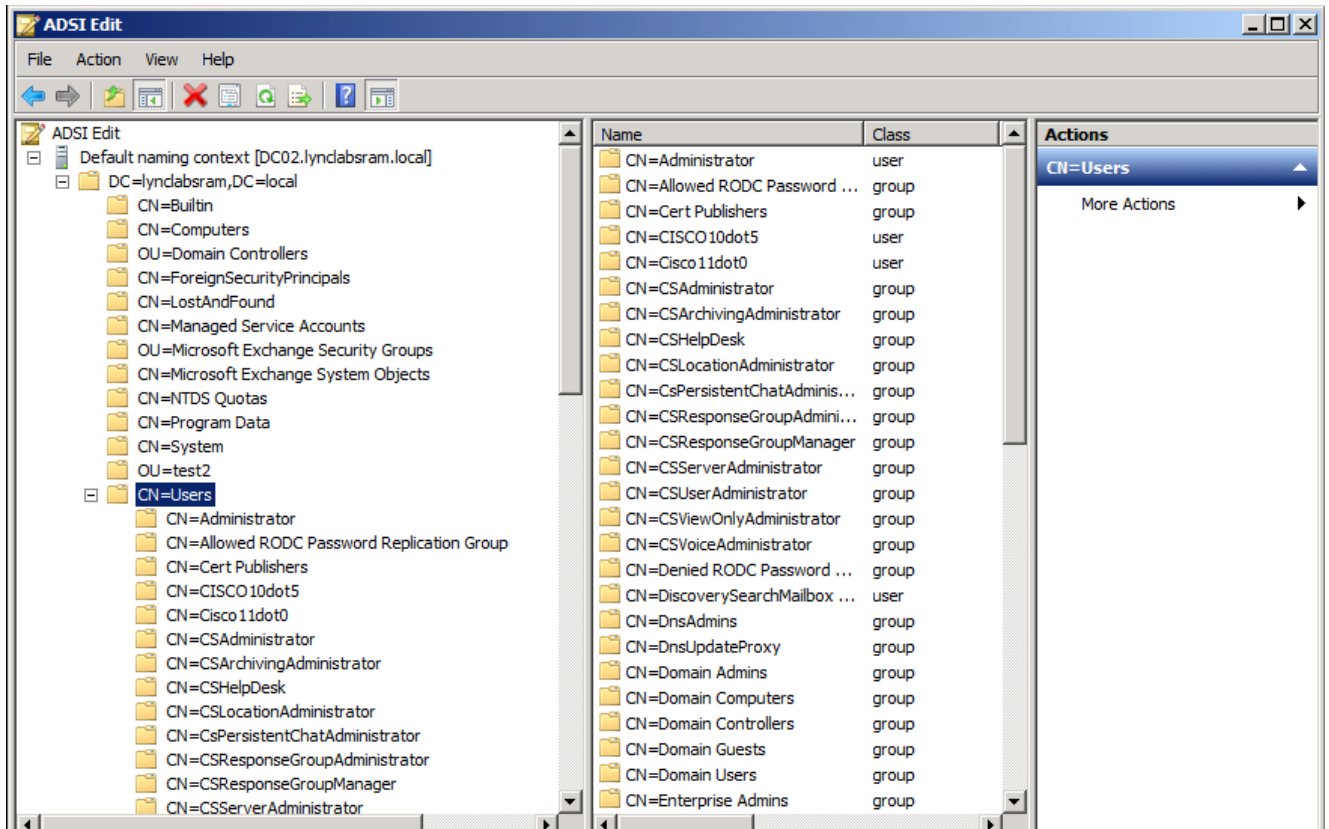
**If the ECB and AD are configured for LDAP integration, then it is NOT necessary to define users in the User database on the ECB.**

### Adding a User’s Phone Number(s) to Active Directory

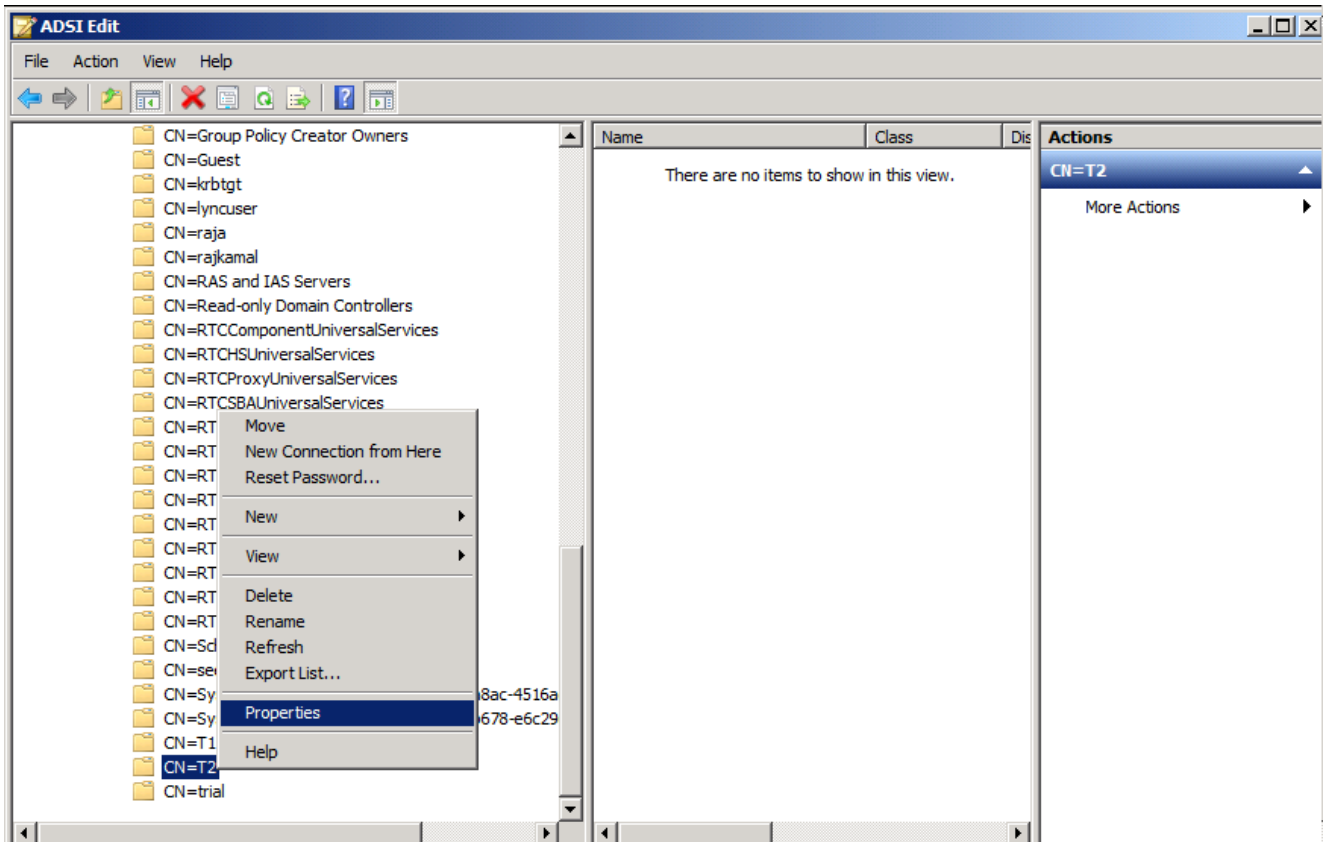
1. On the Active Directory (AD) server, click the **Start** menu, then click on **ADSI Edit**.



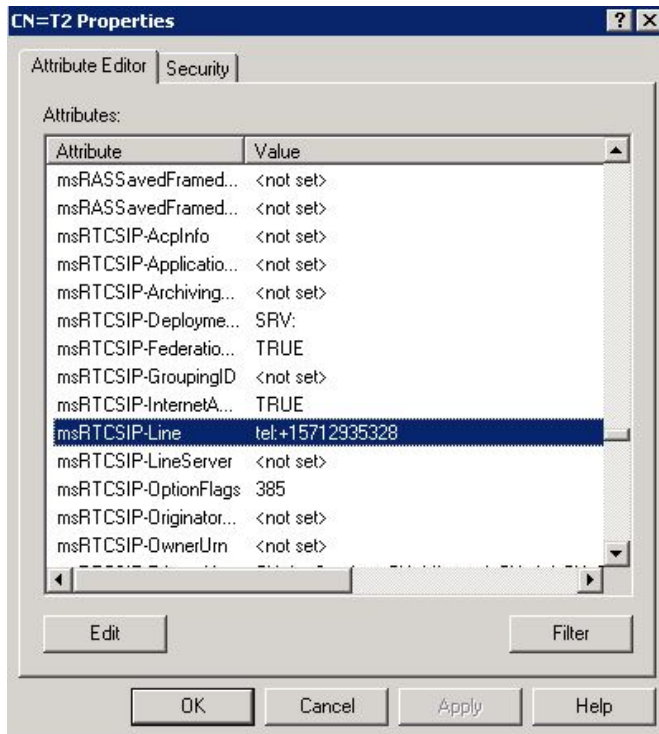
- Expand the **Default running context** (DC02.lynclabsram.local in our example), expand **DC=lynclabsram,DC=local**, then expand **CN=Users**.



3. Select the user to be modified (T2 in the this example). Right click on the user and select **Properties**.

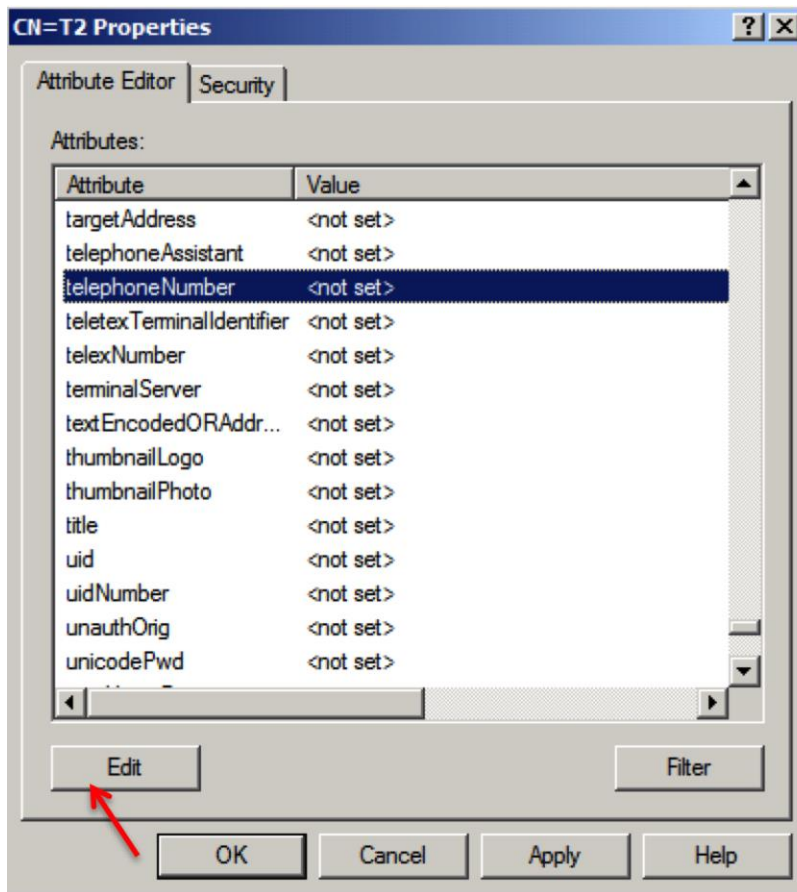


4. If a user is already defined on the Lync or Skype for Business server, then the user will already exist with the "msRTCSIP-Line" parameter in AD. Scroll down to msRTCSIP-Line and verify the telephone number is the correct value.

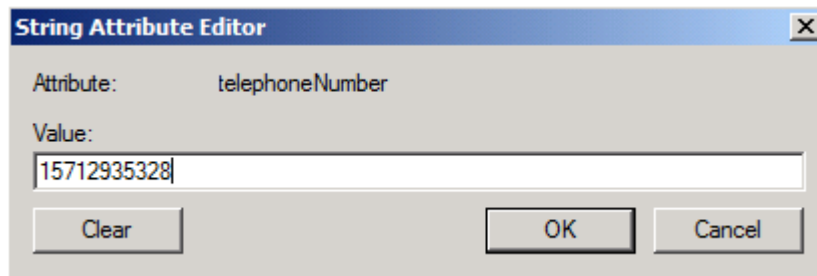




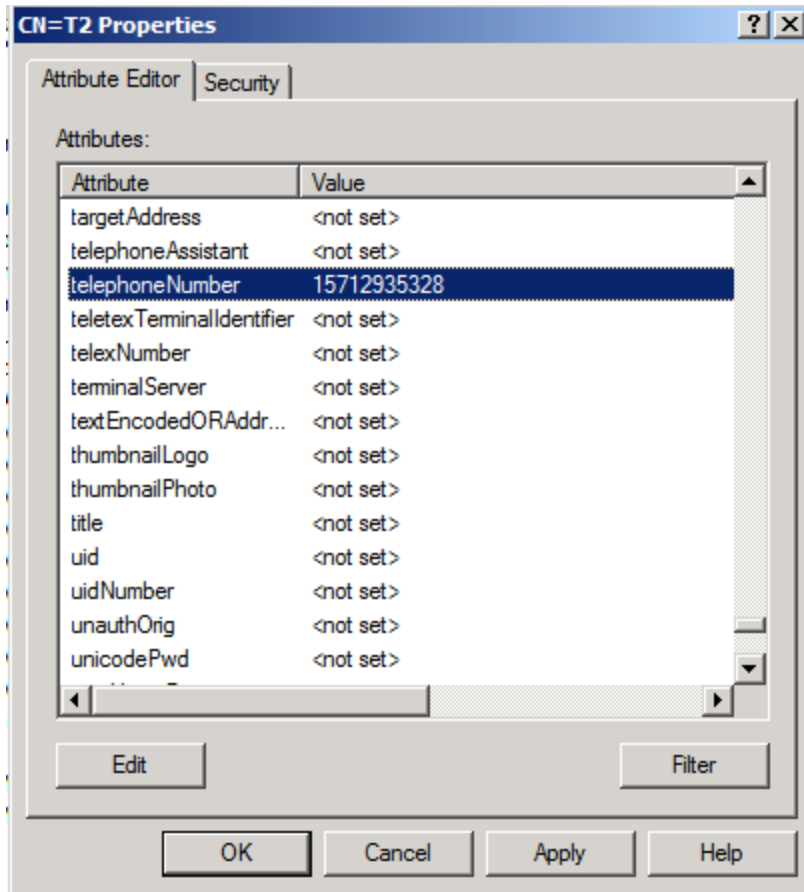
5. Scroll down to telephoneNumber and click Edit.



6. Enter the user's telephone number and click OK.



- Click OK. You can also scroll to other attributes to define the user's telephone number on other systems, such as Avaya Aura. **Ensure that these attributes match those defined on the ECB under LDAP integration.** In the examples in this document, msRTCSIP-Line represents a Lync 2013 user, and telephoneNumber represents a CUCM user.



The Active Directory configuration is now complete.

## Phase 4 – Configuring the Lync 2013 server

The enterprise will have a fully functioning Lync Server infrastructure with Enterprise Voice deployed and a Mediation Server dedicated to this installation. If there is no Mediation Server present for this purpose, one will have to be deployed.

There are two parts for configuring Lync Server to operate with the Oracle ECB:

- Adding the ECB as a PSTN gateway to the Lync Server infrastructure
- Creating a route within the Lync Server infrastructure to utilize the SIP trunk connected through the ECB.

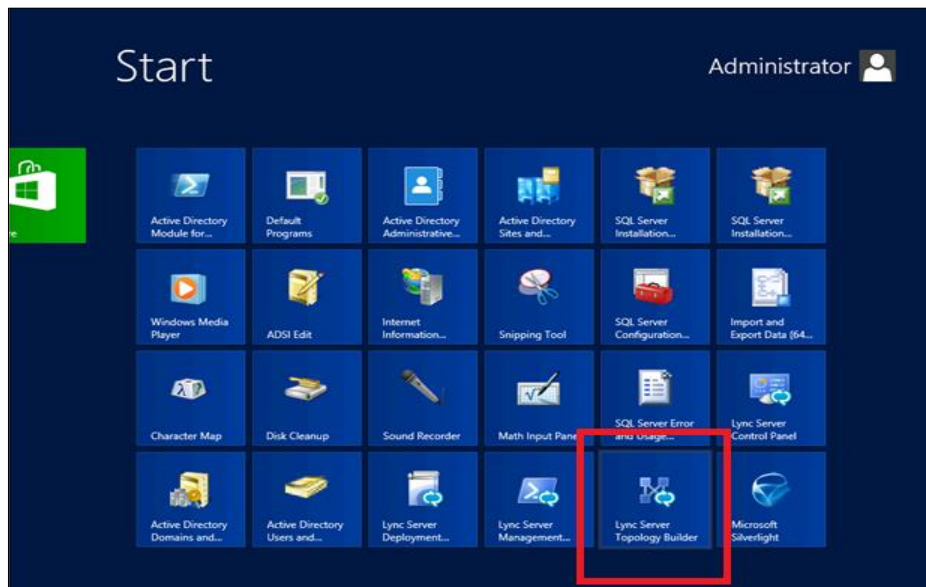
To add the PSTN gateway, we will need:

- IP addresses of the external facing NICs of the Mediation Servers
- IP address of the SIP interface of the ECB
- Rights to administer Lync Server Topology Builder
- Access to the Lync Server Topology Builder

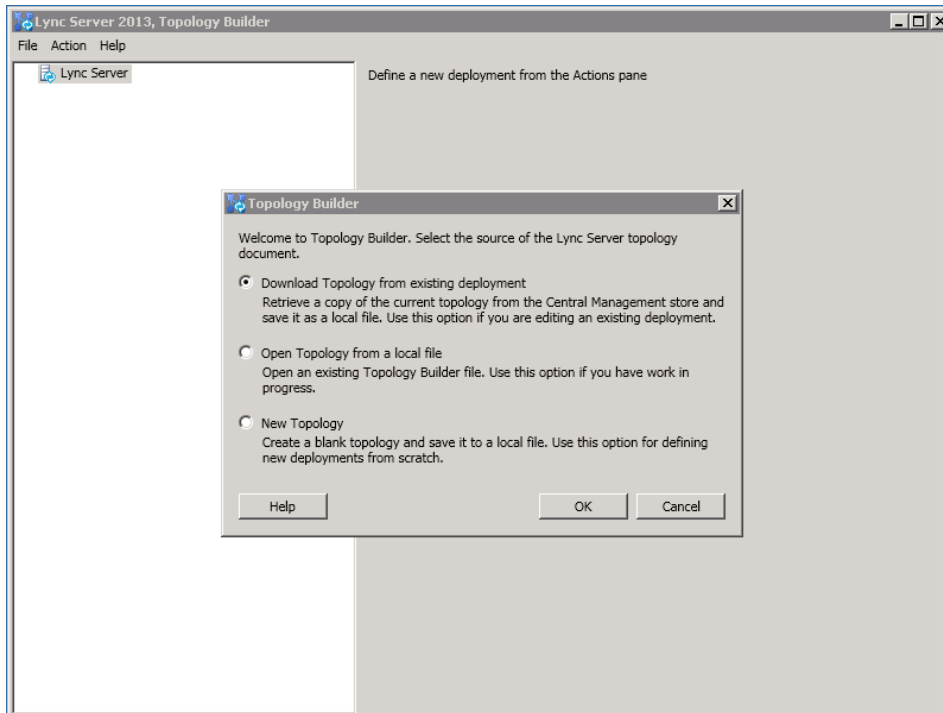
### Adding the ECB as a PSTN gateway

The following process details the steps to add the ECB as the PSTN gateway

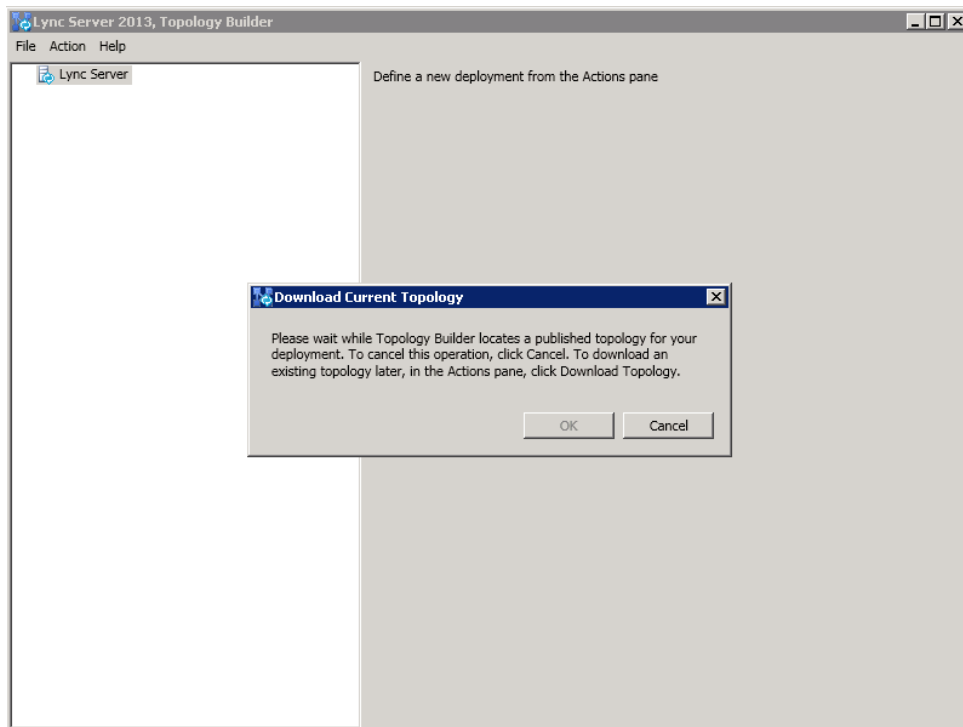
1. On the server where the Topology Builder is located start the console.
2. From the Start bar, select Lync Server Topology Builder.



3. The Topology Builder window will now be displayed. Select **Download Topology from existing deployment**.

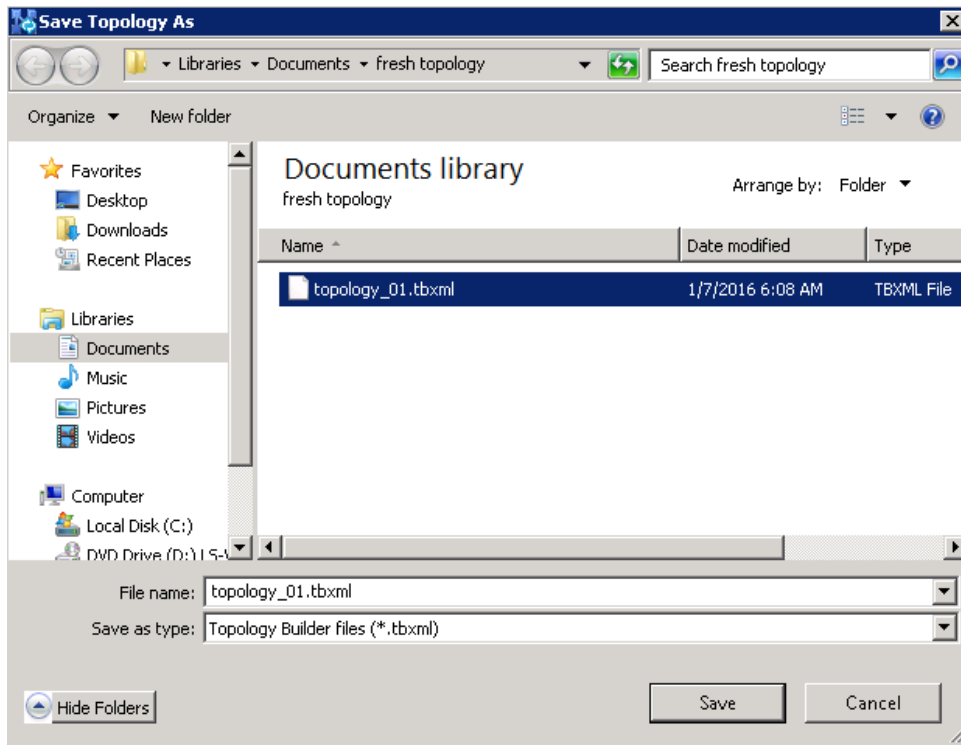


4. You will then see a screen showing that the current topology is being downloaded. Click the **OK** button.



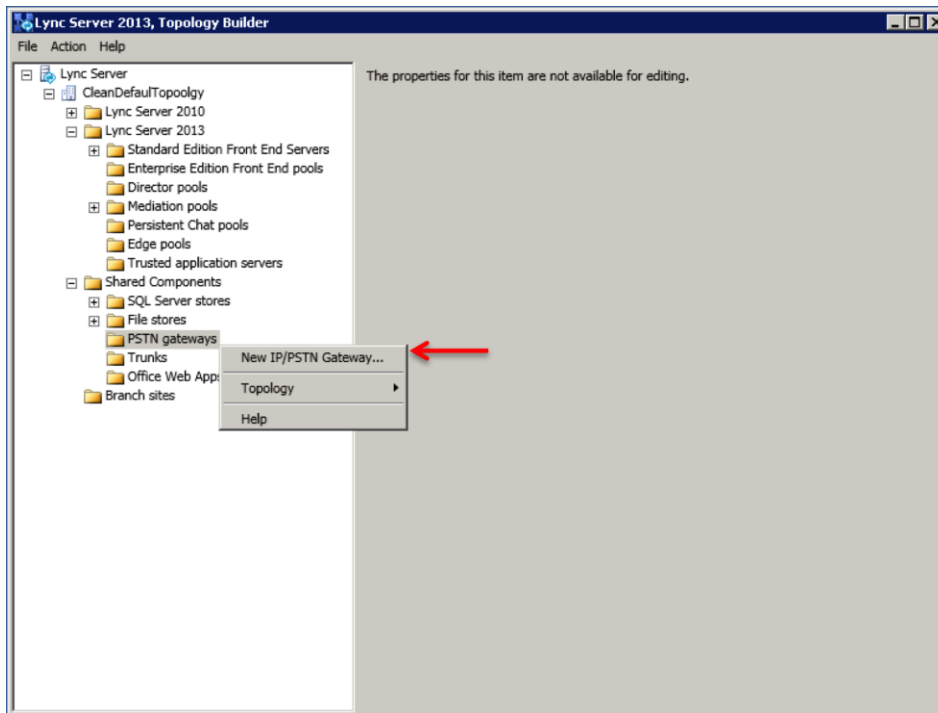
- Next you will be prompted to save the topology which you have imported. You should revision the name or number of the topology according to the standards used within the enterprise. Click the **Save** button

Note: This keeps track of topology changes and, if desired, will allow you to fall back from any changes you make during this installation

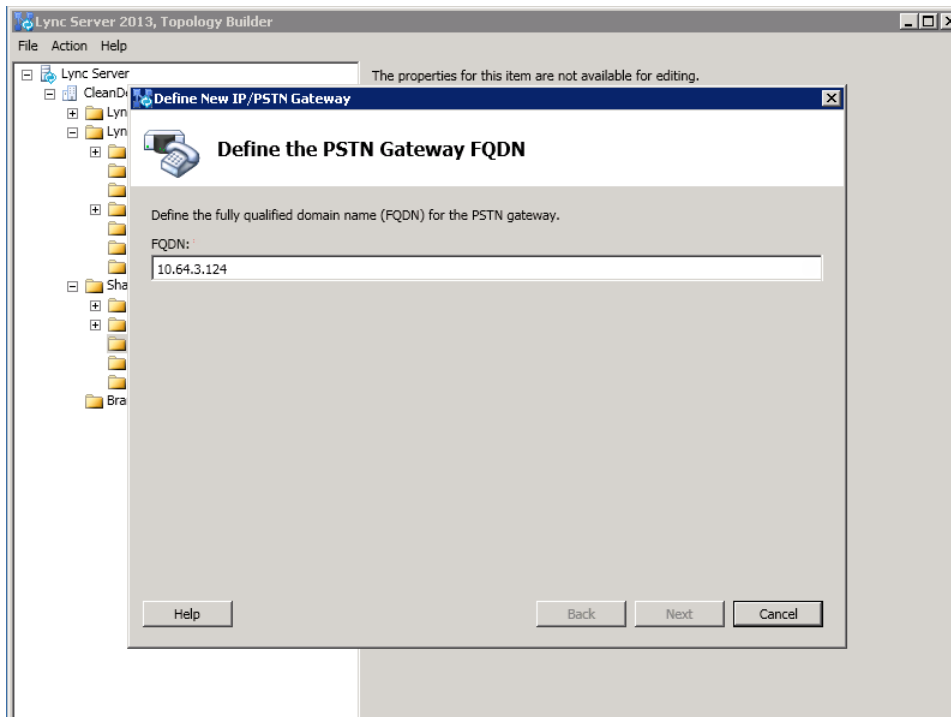


- You will now see the topology builder screen with the enterprise's topology imported.

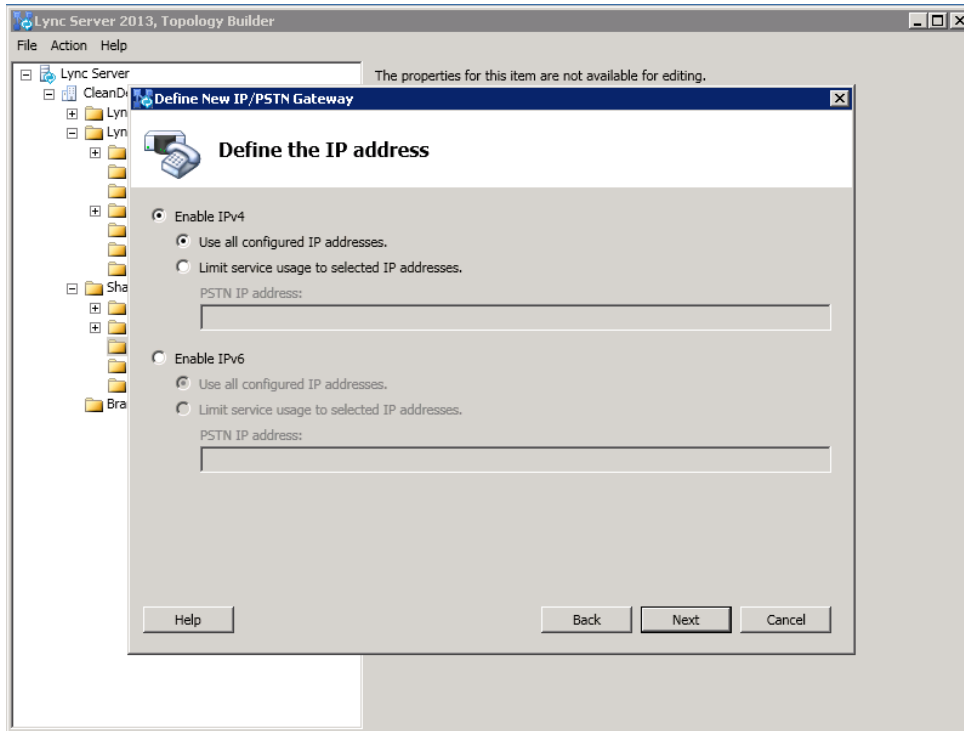
7. In the upper left hand corner, expand the site in which the PSTN gateway will be added. In our case, the site is labeled **CleanDefaultTopology**. Expand **Shared Components**. Then click on the **PSTN Gateways**. Right click on **PSTN gateways** and select **New IP/PSTN Gateway**.



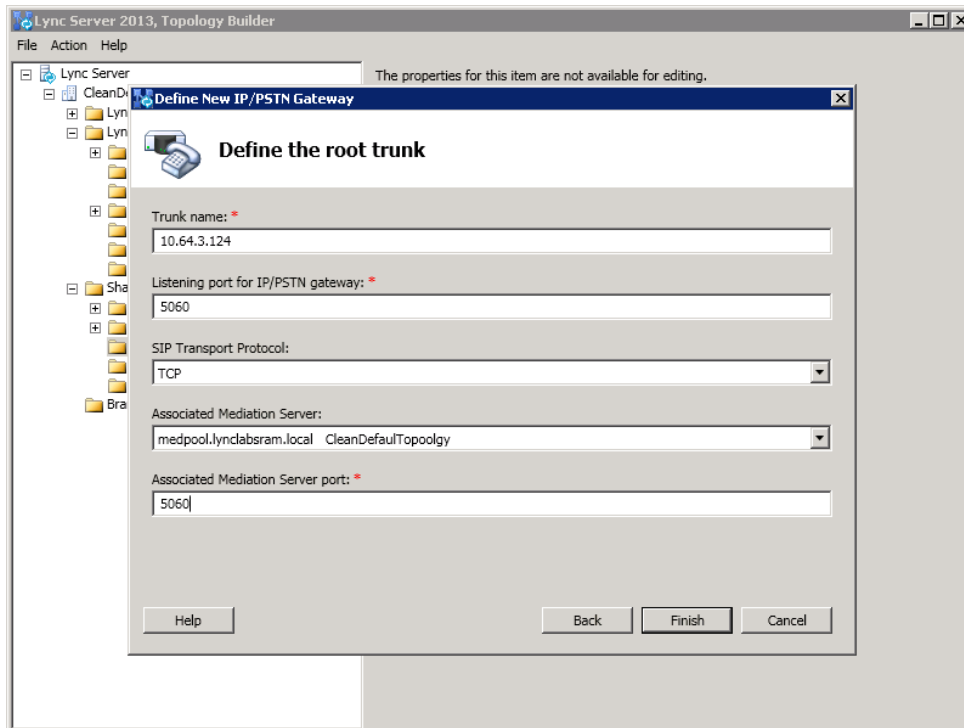
8. In the **Define New IP/PSTN Gateway** window, enter the IP address of the SIP interface of the ECB in the **FQDN** text box and click **Next**.



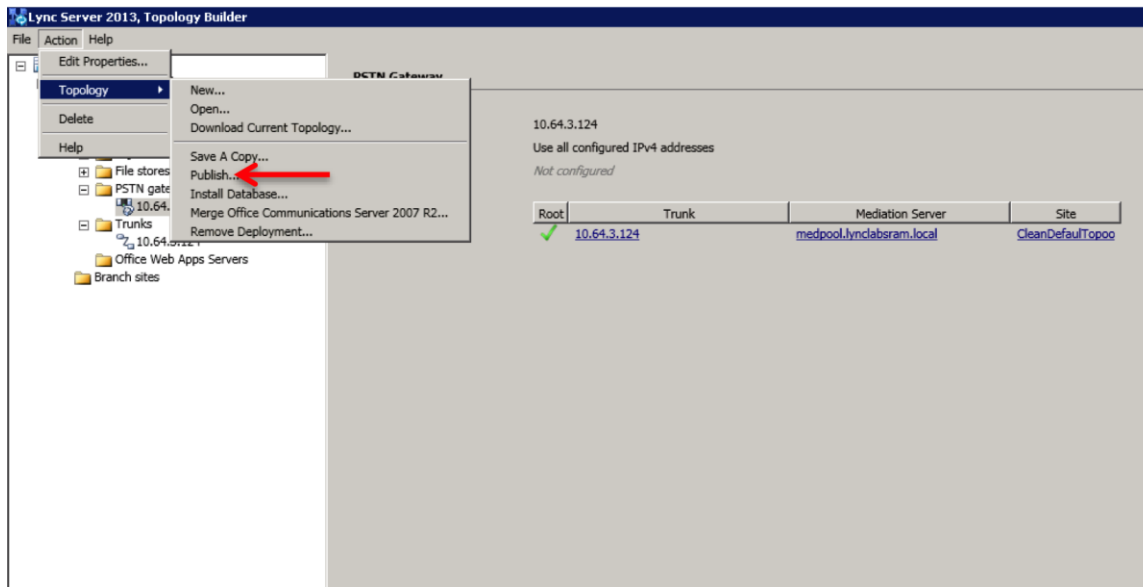
9. Select **Enable IPv4** in the **Define the IP address** section and click **Next**.



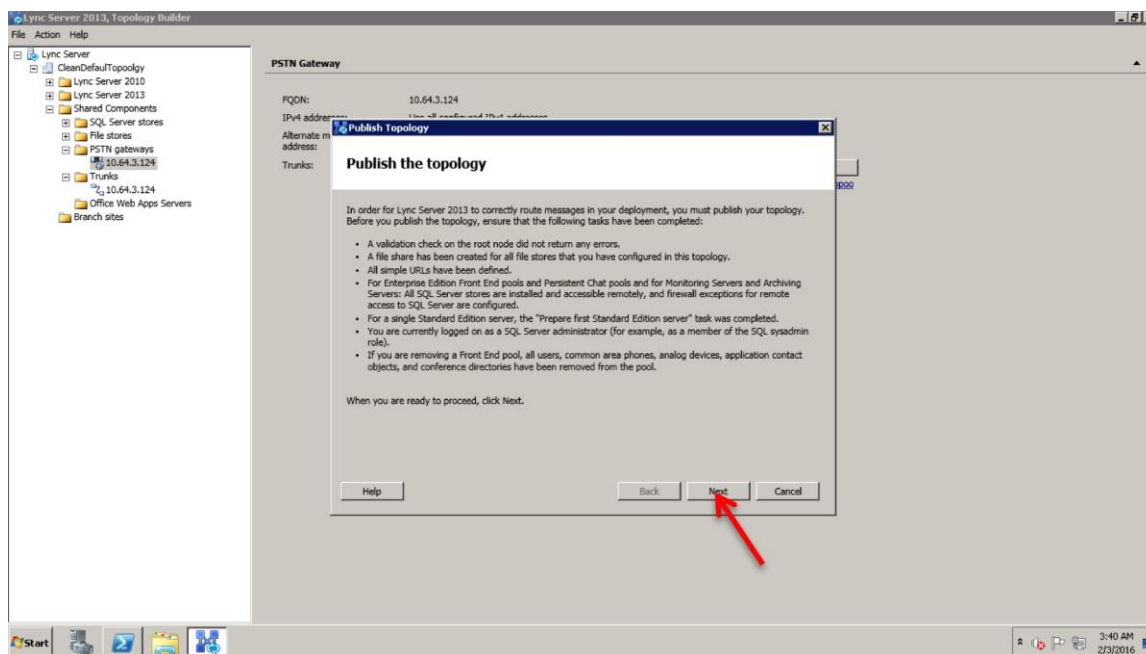
10. In the next section, enter the IP address of the ECB's SIP interface under **Trunk name**. Configure the **Listening port for IP/PSTN gateway** as 5060, TCP as the **SIP Transport Protocol**, and 5060 as the **Associated Mediation Server port**, and click **Finish**.



11. In the upper right hand corner of your screen under **Actions** select **Topology** then select **Publish**.

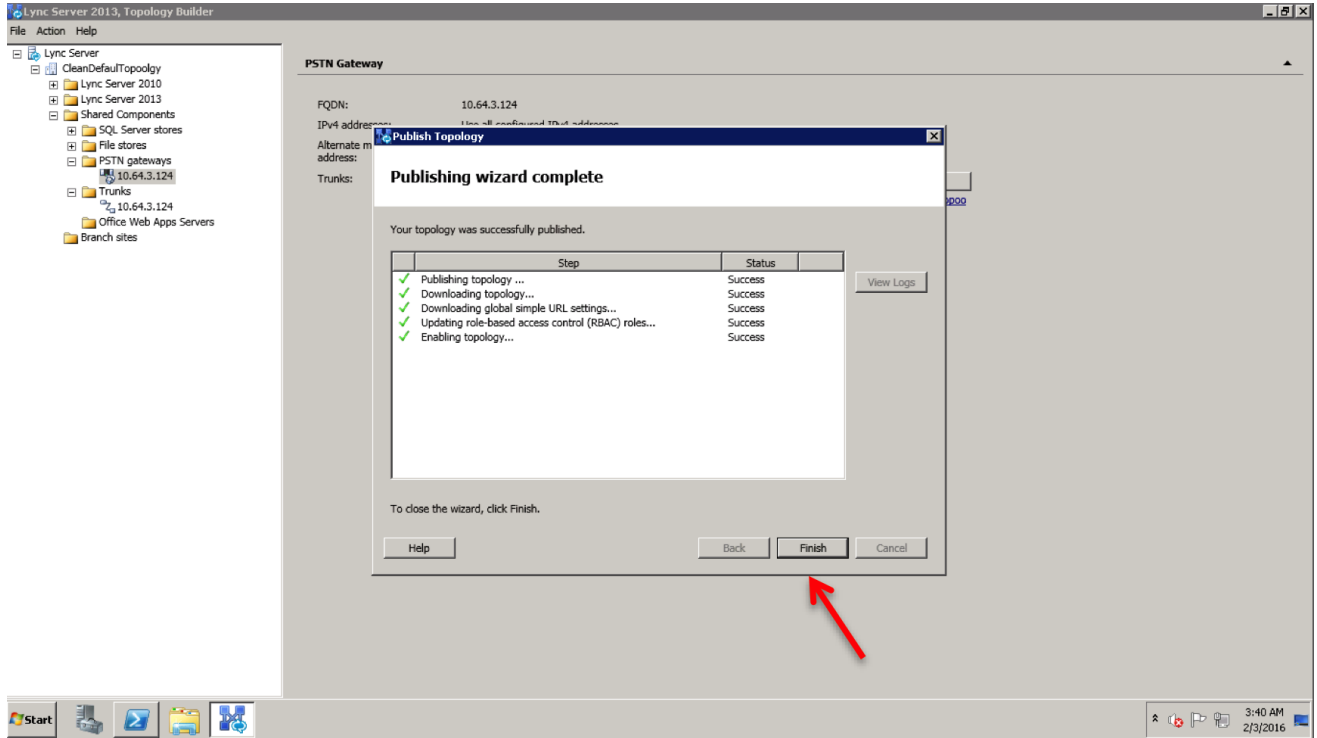


12. You will now see the **Publish Topology** window. Click on the **Next** button





13. When complete you should see a window from Topology Builder stating that your topology was successfully published. Click the **Finish** button.



14. You will be at the Topology Builder main window, expand your site and double check that your PSTN entries are correct and that the appropriate Mediation Server has the PSTN gateway associated.

## Creating a route within the Lync Server infrastructure

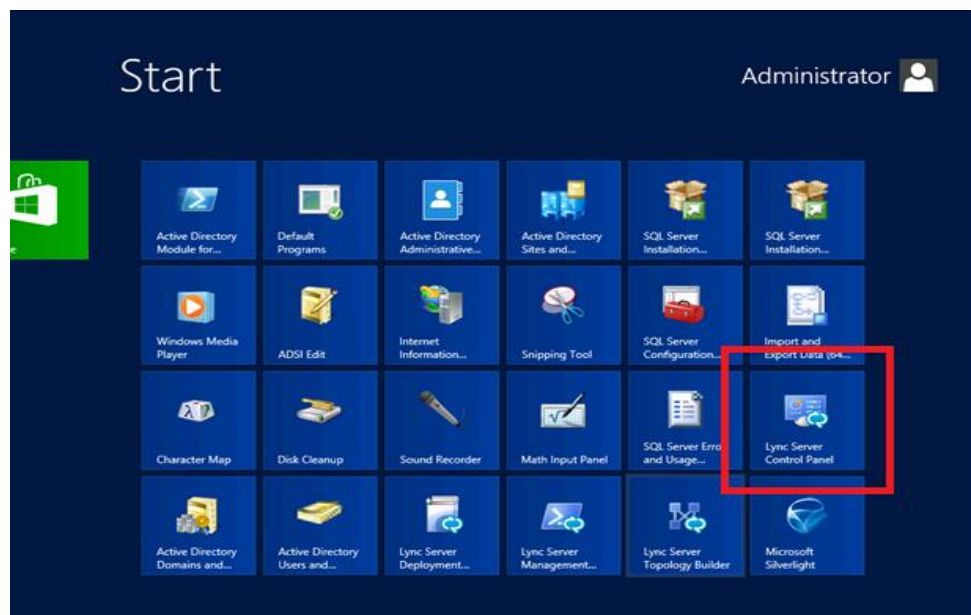
In order for the Lync Server Enterprise Voice clients to utilize the SIP trunking infrastructure that has been put in place, a route will need to be created to allow direction to this egress. Routes specify how Lync Server handles calls placed by enterprise voice users. When a user places a call, the server, if necessary, normalizes the phone number to the E.164 format and then attempts to match that phone number to a SIP Uniform Resource Identifier (URI). If the server is unable to make a match, it applies outgoing call routing logic based on the number. That logic is defined in the form of a separate voice route for each set of target phone numbers listed in the location profile for a locale. For this document we are only describing how to set up a route. Other aspects which apply to Lync Server Enterprise Voice deployments such as dial plans, voice policies, and PSTN usages are not covered.

To add the route we will need:

- Rights to administer Lync Server Control Panel
  - Membership in the CS Administrator Active Directory Group
- Access to the Lync Server Control Panel

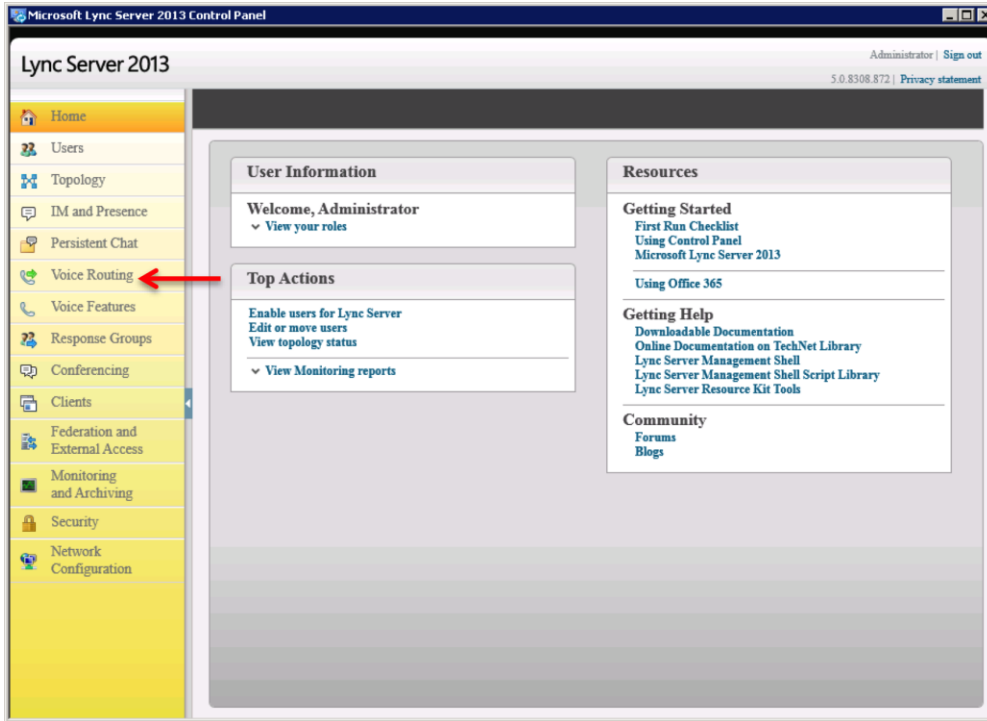
The following process details the steps to create the route:

1. From the Start bar, select Lync Server Control Panel.

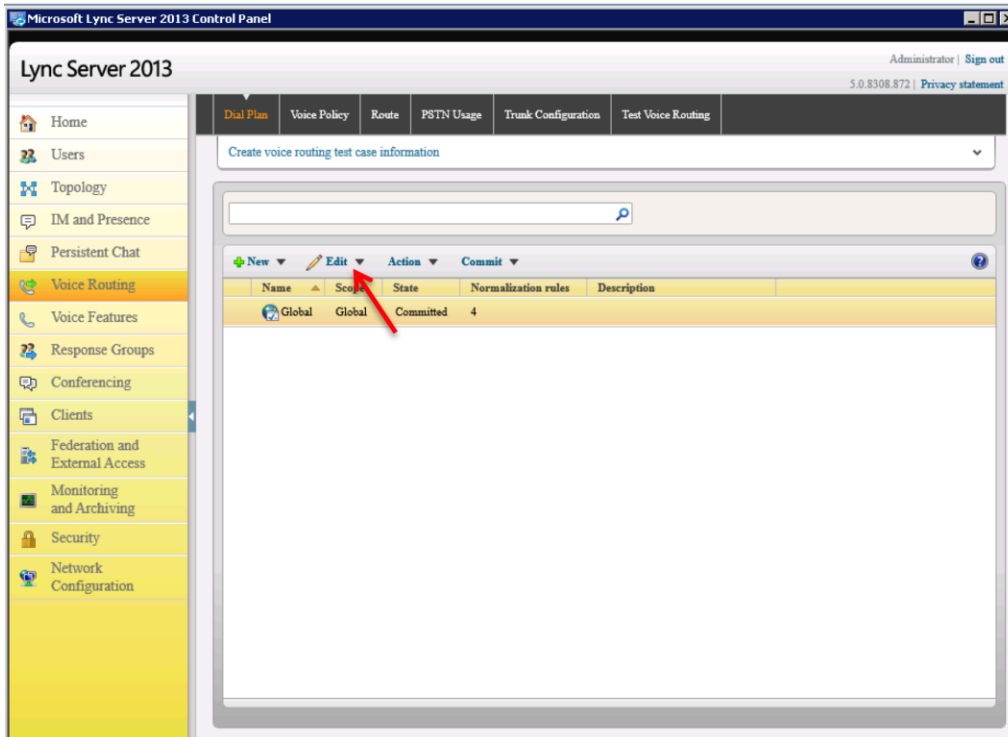


You will be prompted for credentials, enter your domain username and password.

2. Once logged in, you will now be at the "Welcome Screen". On the left hand side of the window, click on **Voice Routing**.



3. The Dial Plan tab in the Voice Routing section will be displayed. Select the Global dial plan. On the content area toolbar, click **Edit**



4. Next you build a Dial Plan and a translation rule for the phone numbers you want this route to handle.

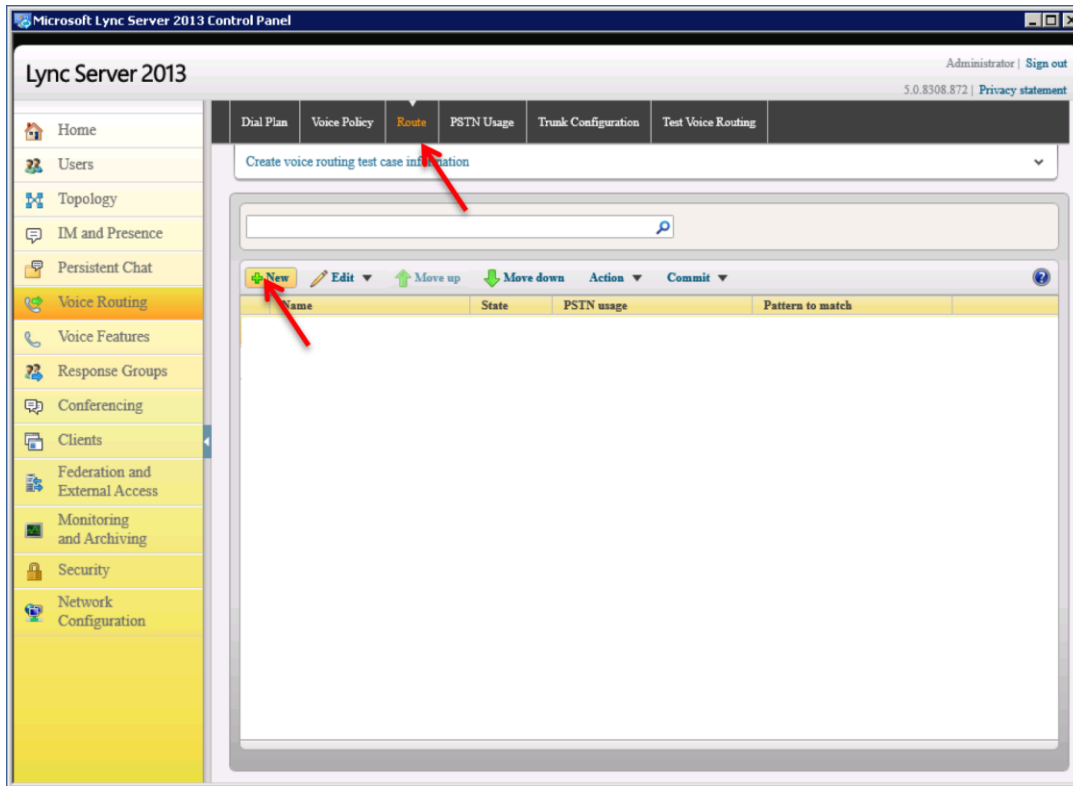
The screenshot displays the Microsoft Lync Server 2013 Control Panel interface. The main window is titled "Lync Server 2013" and shows the "Voice Routing" configuration area. The "Edit Dial Plan - Global" dialog box is open, showing the following configuration options:

- OK** (checked) and **Cancel** buttons.
- Dial-in conferencing region:** An empty text input field.
- External access prefix:** An empty text input field.
- Associated Normalization Rules:** A table with the following data:

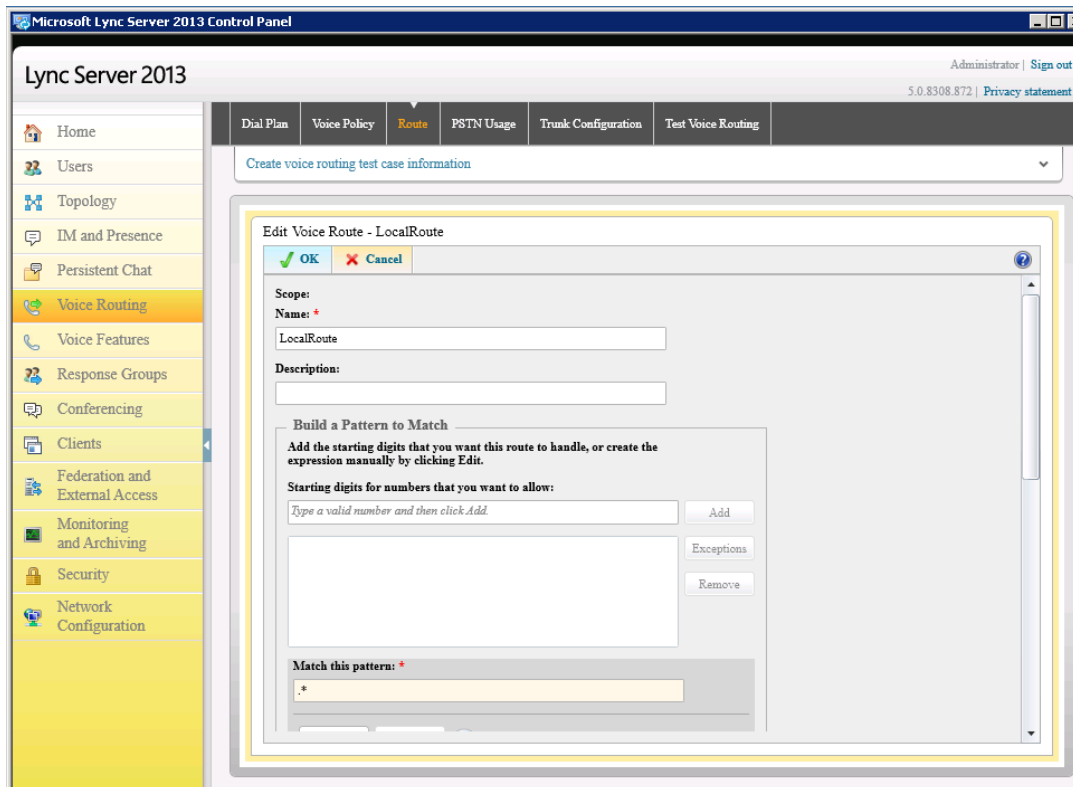
Normalization rule	State	Pattern to match	Translation pattern
4 digit	Committed	^(d{4})\$	\$1
10 digit	Committed	^(d{10})\$	+1\$1
Keep All	Committed	^(d{3}d+)\$	\$1

- Dial number to test:** An empty text input field with a **Go** button and a help icon.

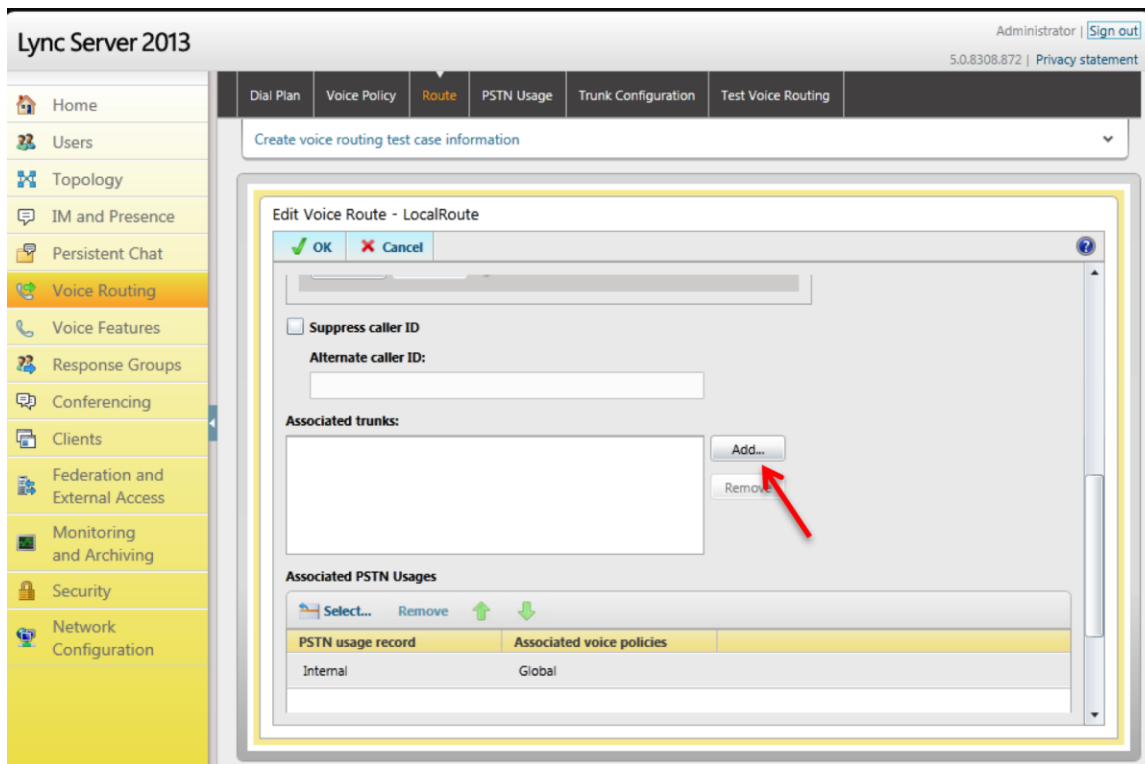
5. On the top row of the tabs, select **Route**. On the content area toolbar, click **+New**.



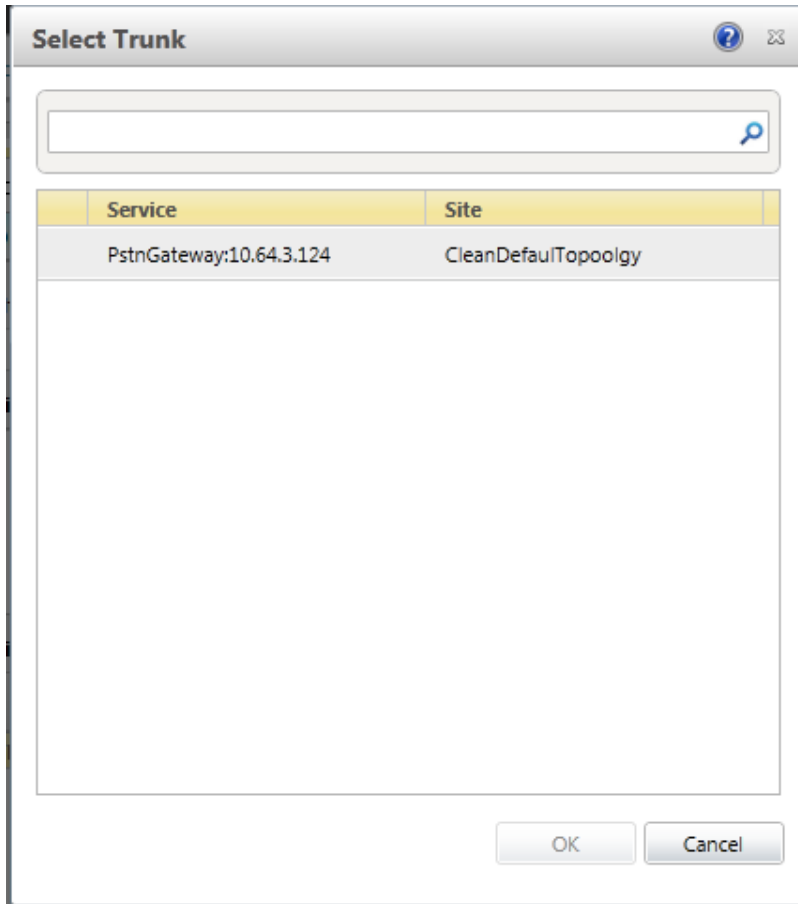
6. On the **New Voice Route** page, in the **Name** field, enter the name you have selected for the Route. In our example, it is labeled “LocalRoute”. Leave the **Match this pattern** field as .\* so all numbers will be matched.



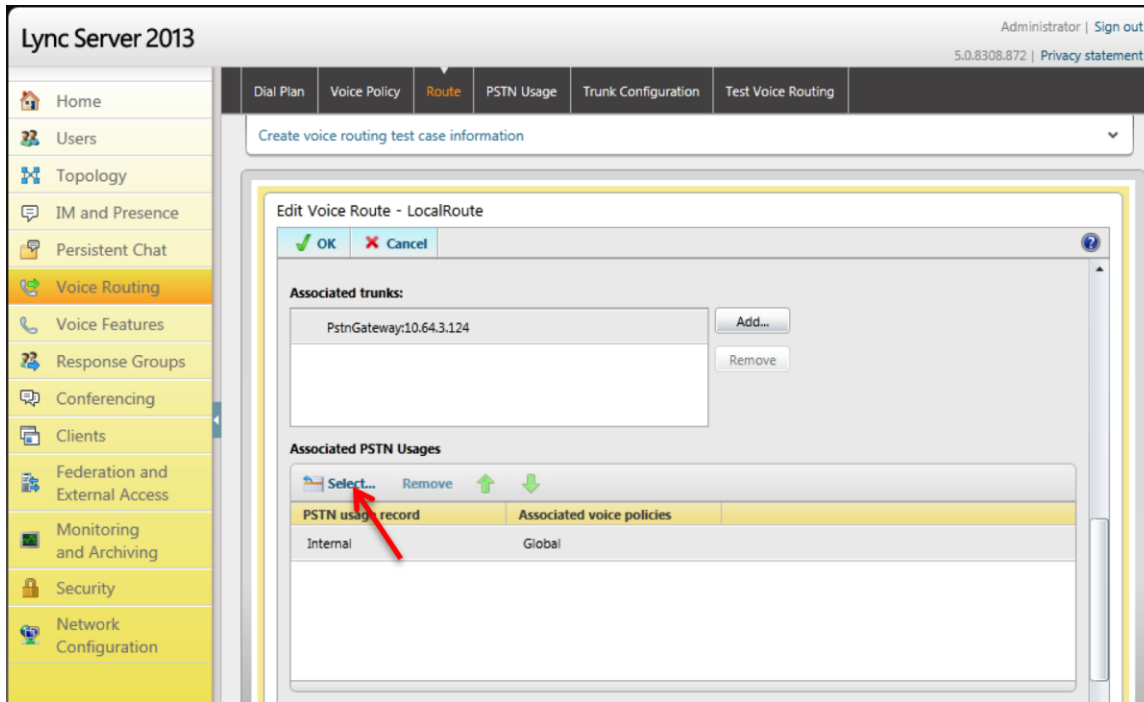
- Next you want to associate the Voice Route with the **Trunk** you have just created. Scroll down to **Associated Trunks**, click on the **Add** button.



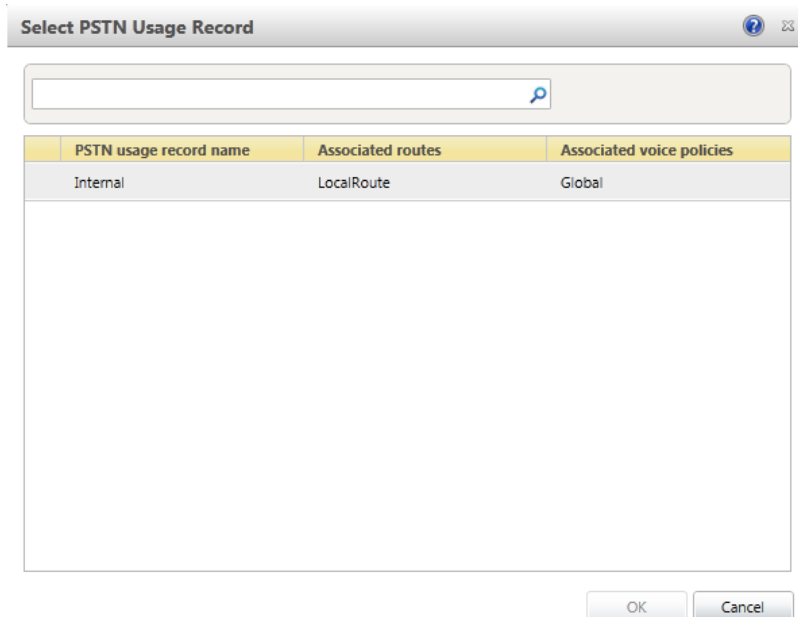
8. You will now be at a window showing available Trunks to associate your Voice Route. Click on the PSTN gateway that you just created and then click the **OK** button.



- You can now see that you have associated your trunk with the route you created. An appropriate PSTN usage record will need to be assigned as well. In our example, we use one that was already created in the enterprise. Click on the **Select** button under **Associated PSTN Usages**



- In the **Select PSTN Usage Record** window displayed, select the appropriate PSTN Usage Record and click **OK**.





11. You will now see the Associated PSTN Usages which you have added. Click the **OK** button at the top of the **New Voice Route** screen.

The screenshot shows the Lync Server 2013 administration console. The left-hand navigation pane is visible, with 'Voice Routing' selected. The top navigation bar includes 'Dial Plan', 'Voice Policy', 'Route', 'PSTN Usage', 'Trunk Configuration', and 'Test Voice Routing'. The 'Route' tab is active, and a search bar contains 'Create voice routing test case information'. The main content area displays the 'Edit Voice Route - LocalRoute' dialog box. At the top of the dialog are 'OK' and 'Cancel' buttons. Below this, the 'Associated trunks' section shows a list with one entry: 'PstnGateway:10.64.3.124'. To the right of this list are 'Add...' and 'Remove' buttons. The 'Associated PSTN Usages' section features a 'Select...' button, 'Remove' text, and up/down arrow icons. Below these is a table with two columns: 'PSTN usage record' and 'Associated voice policies'. The table contains one row with 'Internal' under the first column and 'Global' under the second column.

PSTN usage record	Associated voice policies
Internal	Global

12. You will now be at the Routes page showing the LocalRoute. Click the **Commit** drop-down menu, and then **Commit All**.

The screenshot shows the Lync Server 2013 administration console. The top navigation bar includes 'Dial Plan', 'Voice Policy', 'Route', 'PSTN Usage', 'Trunk Configuration', and 'Test Voice Routing'. The 'Route' tab is active. Below the navigation bar, there is a search bar and a toolbar with 'New', 'Edit', 'Move up', 'Move down', 'Action', and 'Commit' buttons. The 'Commit' dropdown menu is open, showing options: 'Review uncommitted changes', 'Commit all', 'Cancel selected changes', and 'Cancel all uncommitted changes'. A red arrow points to the 'Commit all' option. Below the toolbar is a table with columns: Name, State, PSTN usage, and Match. The table contains one row: 'LocalRoute', 'Uncommitted', 'Internal', and an empty cell.

Name	State	PSTN usage	Match
LocalRoute	Uncommitted	Internal	

## Phase 5 – Configuring the Skype for Business Server

The enterprise will have a fully functioning Skype for Business (SFB) Server infrastructure with Enterprise Voice deployed and a Mediation Server dedicated to this installation. If there is no Mediation Server present for this purpose, one will have to be deployed.

There are two parts for configuring SFB Server to operate with the Oracle ECB:

- Adding the ECB as a PSTN gateway to the SFB Server infrastructure
- Creating a route within the SFB Server infrastructure to utilize the SIP trunk connected through the ECB.

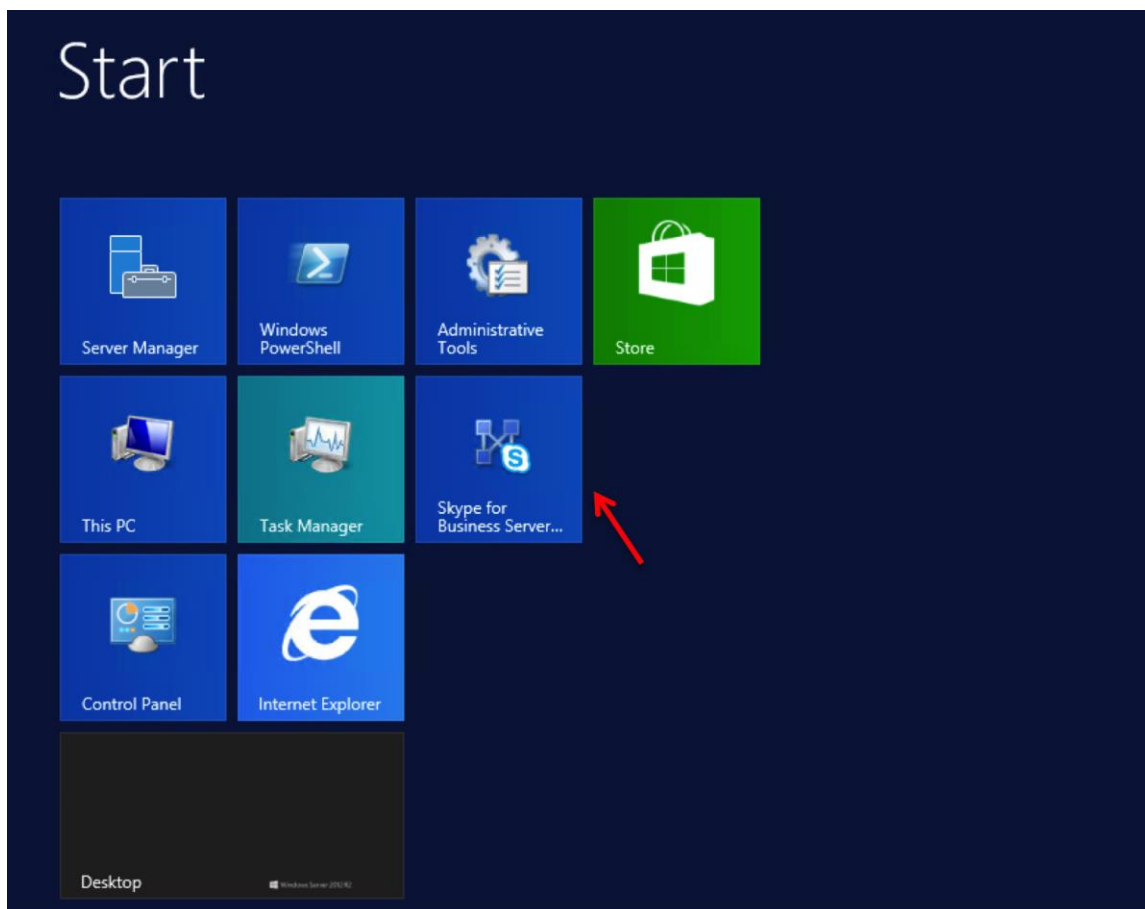
To add the PSTN gateway, we will need:

- IP addresses of the external facing NICs of the Mediation Servers
- IP address of the SIP interface of the ECB
- Rights to administer SFB Server Topology Builder
- Access to the SFB Server Topology Builder

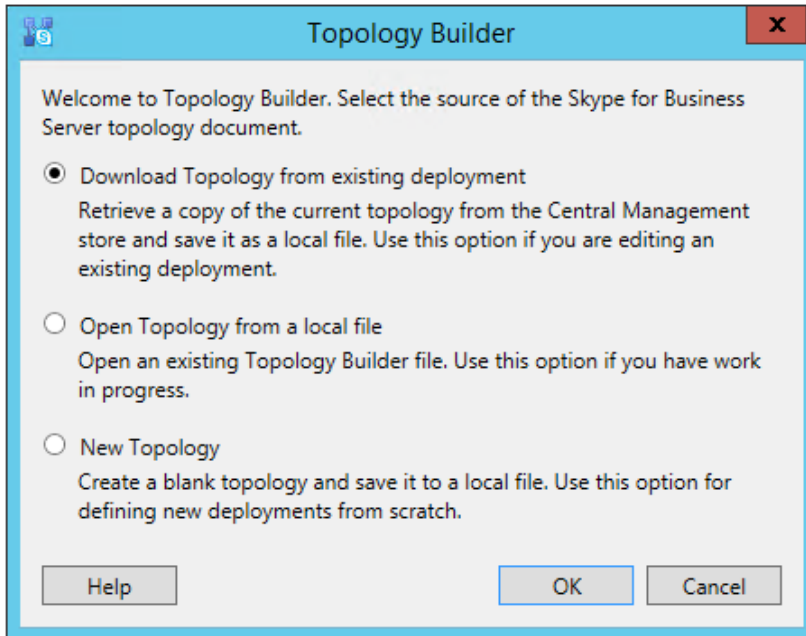
### Adding the ECB as a PSTN gateway

The following process details the steps to add the ECB as the PSTN gateway

1. On the server where the Topology Builder is located start the console.
2. From the Start bar, select SFB Server Topology Builder.

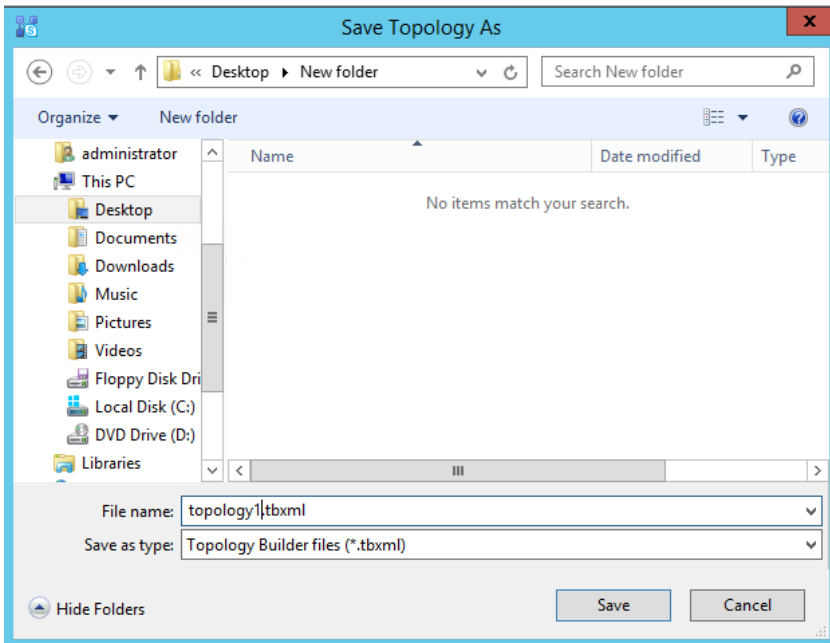


1. The Topology Builder window will now be displayed. Select **Download Topology from existing deployment**.

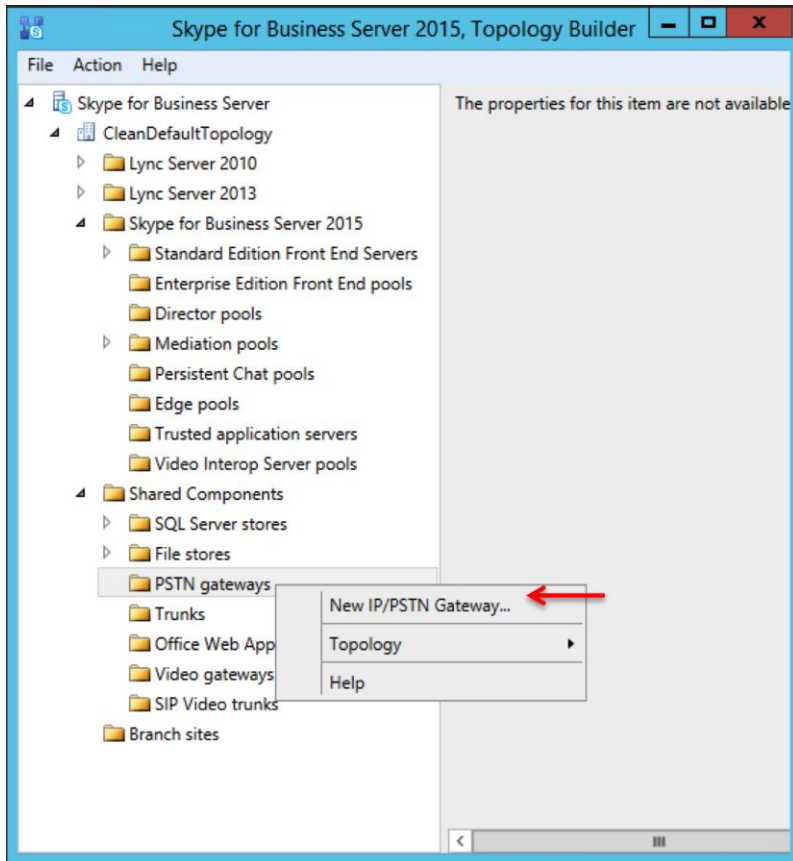


2. You will then see a screen showing that the current topology is being downloaded. Click the **OK** button.
3. Next you will be prompted to save the topology which you have imported. You should revision the name or number of the topology according to the standards used within the enterprise. Click the **Save** button

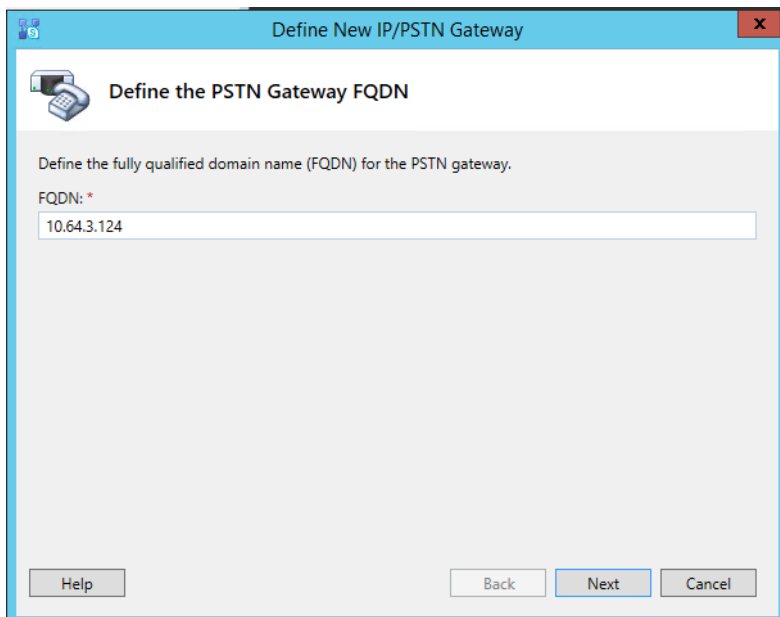
Note: This keeps track of topology changes and, if desired, will allow you to fall back from any changes you make during this installation



- In the upper left hand corner, expand the site in which the PSTN gateway will be added. In our case, the site is labeled **CleanDefaultTopology**. Expand **Shared Components**. Then click on the **PSTN Gateways**. Right click on **PSTN gateways** and select **New IP/PSTN Gateway**.



- In the **Define New IP/PSTN Gateway** window, enter the IP address of the SIP interface of the ECB in the **FQDN** text box and click **Next**.



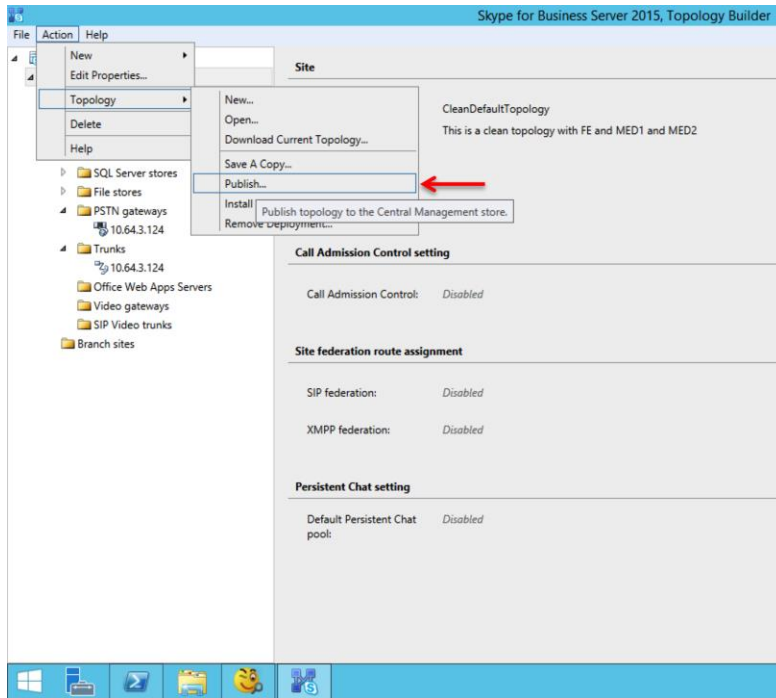
6. Select **Enable IPv4** in the **Define the IP address** section and click **Next**.

The screenshot shows a dialog box titled "Define New IP/PSTN Gateway" with a sub-section "Define the IP address". It contains two radio button options: "Enable IPv4" (selected) and "Enable IPv6". Under each, there are sub-options: "Use all configured IP addresses." (selected) and "Limit service usage to selected IP addresses." Below these are two text input fields labeled "PSTN IP address:". At the bottom, there are buttons for "Help", "Back", "Next" (highlighted), and "Cancel".

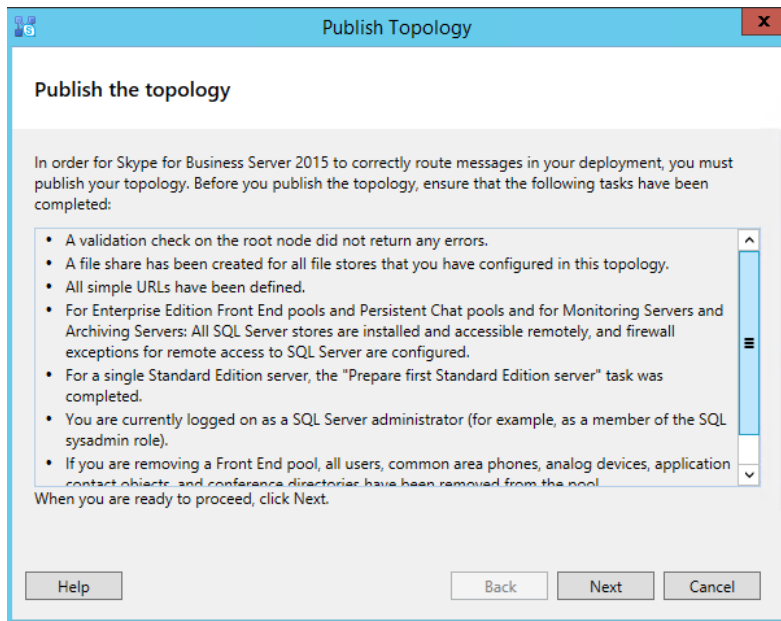
7. In the next section, enter the IP address of the ECB's SIP interface under **Trunk name**. Configure the **Listening port for IP/PSTN gateway** as 5060, TCP as the **SIP Transport Protocol**, and 5060 as the **Associated Mediation Server port**, and click **Finish**.

The screenshot shows the same dialog box, now in the "Define the root trunk" section. It contains several fields: "Trunk name:" with the value "10.64.3.124"; "Listening port for IP/PSTN gateway:" with the value "5060"; "SIP Transport Protocol:" with a dropdown menu set to "TCP"; "Associated Mediation Server:" with a dropdown menu set to "medpool.sflabdm.local CleanDefaultTopology"; and "Associated Mediation Server port:" with the value "5060". At the bottom, there are buttons for "Help", "Back", "Finish" (highlighted), and "Cancel".

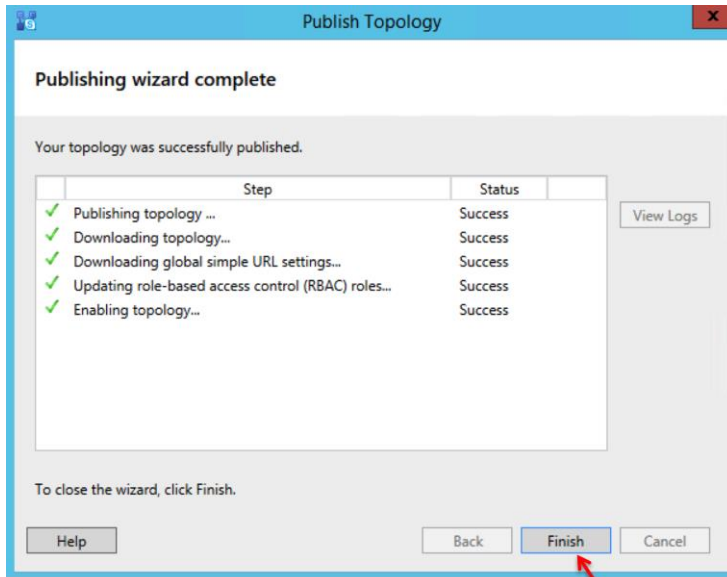
8. In the upper right hand corner of your screen under **Actions** select **Topology** then select **Publish**.



9. You will now see the **Publish Topology** window. Click on the **Next** button.



10. When complete you should see a window from Topology Builder stating that your topology was successfully published. Click the **Finish** button.





## Creating a route within the Skype for Business infrastructure

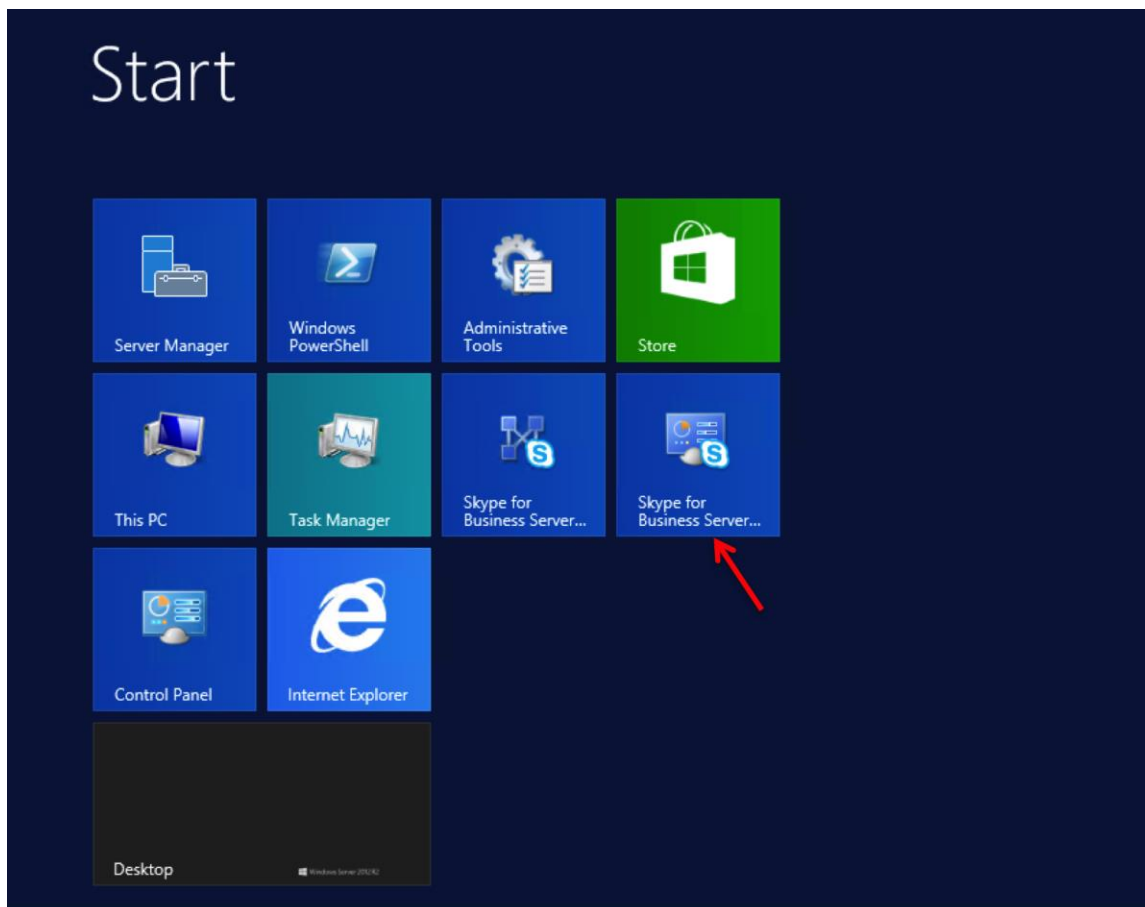
In order for the Skype for Business (SFB) clients to utilize the SIP trunking infrastructure that has been put in place, a route will need to be created to allow direction to this egress. Routes specify how SFB handles calls placed by enterprise voice users. When a user places a call, the server, if necessary, normalizes the phone number to the E.164 format and then attempts to match that phone number to a SIP Uniform Resource Identifier (URI). If the server is unable to make a match, it applies outgoing call routing logic based on the number. That logic is defined in the form of a separate voice route for each set of target phone numbers listed in the location profile for a locale. For this document we are only describing how to set up a route. Other aspects which apply to SFB deployments such as dial plans, voice policies, and PSTN usages are not covered.

To add the route we will need:

- Rights to administer the SFB Control Panel
  - Membership in the CS Administrator Active Directory Group
- Access to the SFB Control Panel

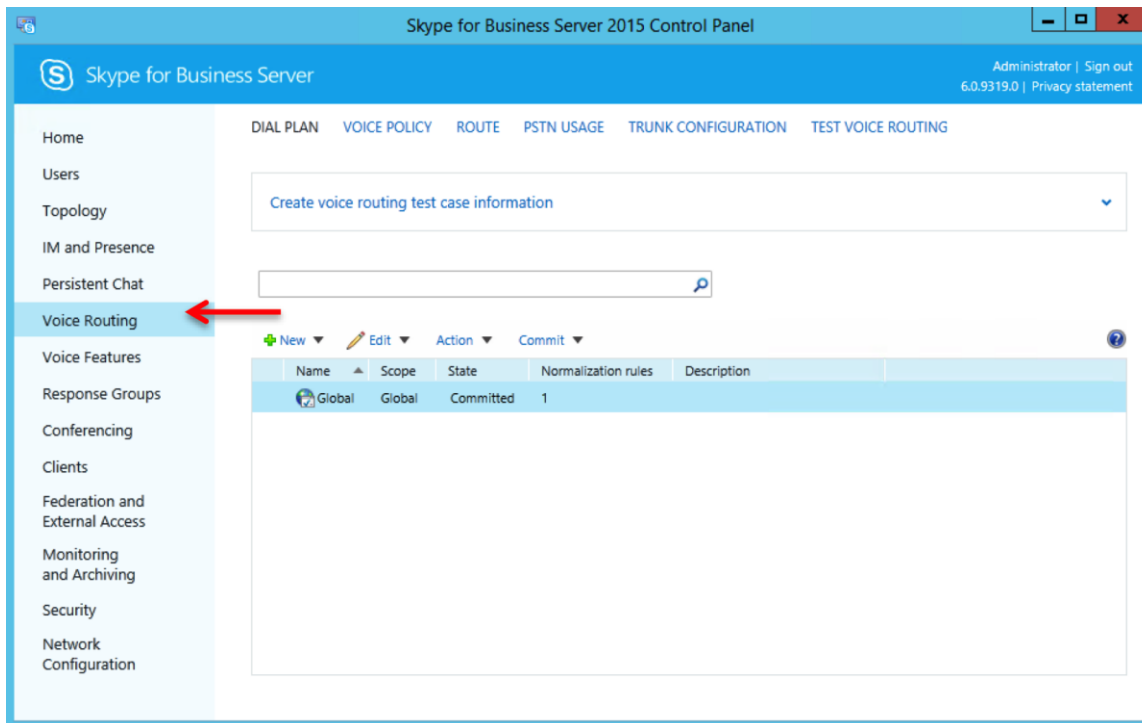
The following process details the steps to create the route:

1. From the Start bar, select SFB Control Panel.

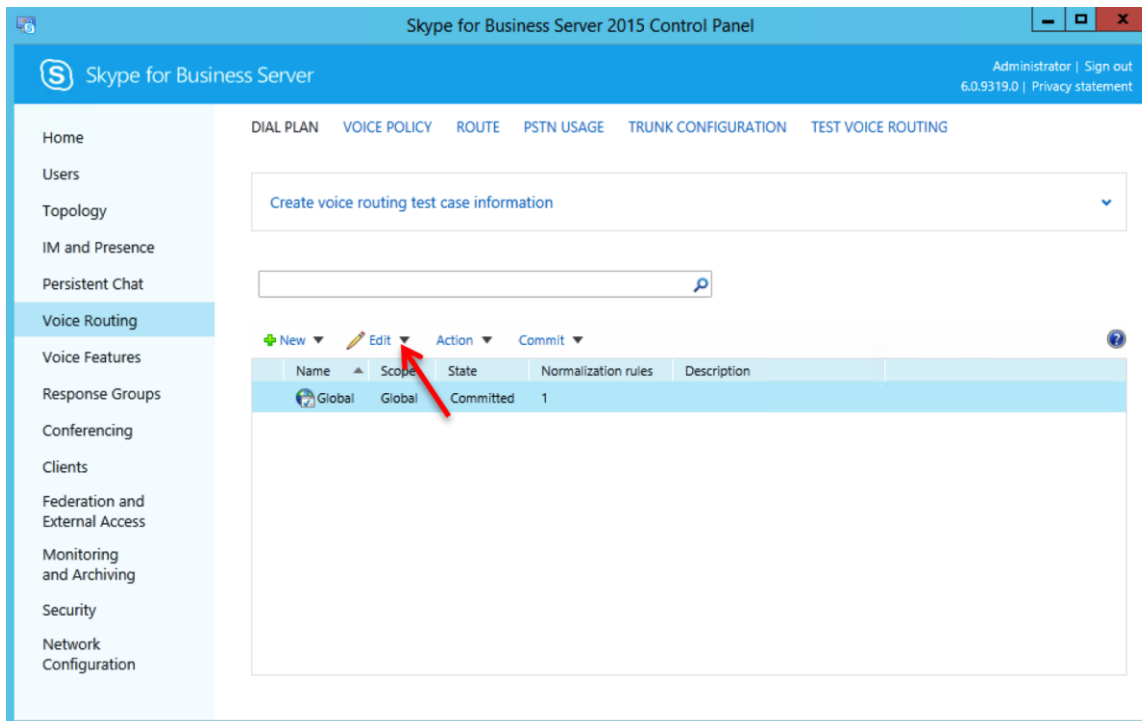


You will be prompted for credentials, enter your domain username and password.

- Once logged in, you will now be at the "Welcome Screen". On the left hand side of the window, click on **Voice Routing**.



- The Dial Plan tab in the Voice Routing section will be displayed. Select the Global dial plan. On the content area toolbar, click **Edit**



4. Next you build a Dial Plan and a translation rule for the phone numbers you want this route to handle.

Skype for Business Server

DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING

Create voice routing test case information

Edit Dial Plan - Global

OK Cancel

Description:

Dial-in conferencing region: Dallas

External access prefix:

Associated Normalization Rules

Normalization rule	State	Pattern to match	Translation pattern
4 digit	Committed	^\d{4}\$	\$1
10 digit	Committed	^\d{10}\$	\$1
Keep All	Committed	^\d*\$	\$1

Dialed number to test: Go

5. On the top row of the tabs, select **Route**. On the content area toolbar, click **+New**.

Skype for Business Server

DIAL PLAN VOICE POLICY **ROUTE** PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING

Create voice routing test case information

+New Edit Move up Move down Action Commit

Name	State	PSTN usage	Pattern to match
------	-------	------------	------------------

6. On the **New Voice Route** page, in the **Name** field, enter the name you have selected for the Route. In our example, it is labeled "route1". Leave the **Match this pattern** field as .\* so all numbers will be matched.

Skype for Business Server

Home  
Users  
Topology  
IM and Presence  
Persistent Chat  
**Voice Routing**  
Voice Features  
Response Groups  
Conferencing  
Clients  
Federation and External Access  
Monitoring and Archiving  
Security  
Network Configuration

DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING

Create voice routing test case information

New Voice Route

✓ OK ✗ Cancel

**Scope:**  
**Name: \***  
route1

**Description:**

**Build a Pattern to Match**  
Add the starting digits that you want this route to handle, or create the expression manually by clicking Edit.

**Starting digits for numbers that you want to allow:**  
Type a valid number and then click Add. Add

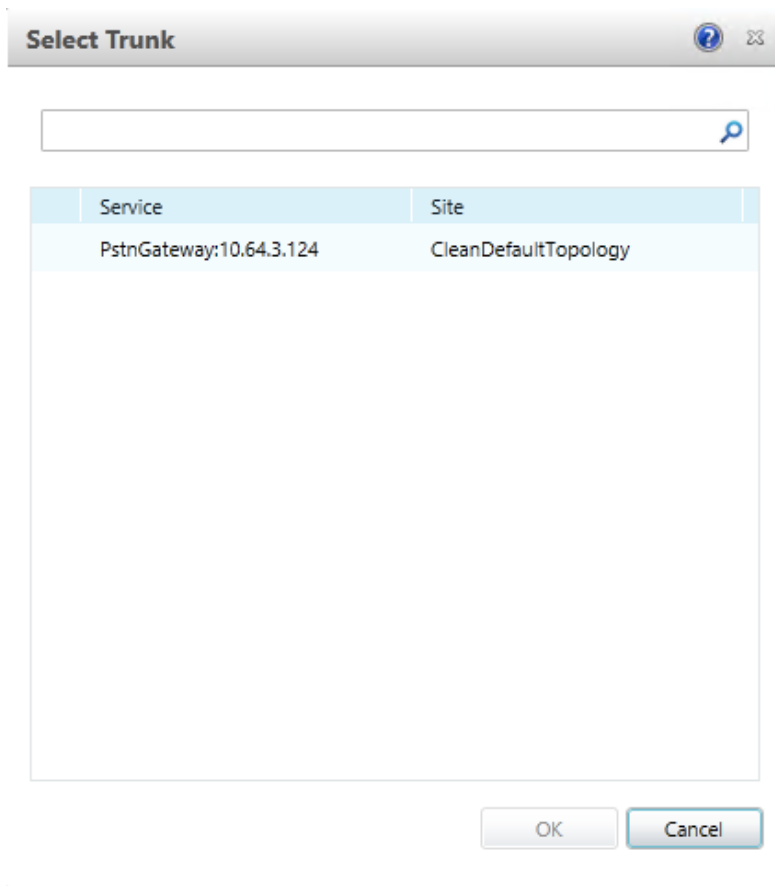
Exceptions  
Remove

**Match this pattern: \***  
.\*

- Next you want to associate the Voice Route with the **Trunk** you have just created. Scroll down to **Associated Trunks**, click on the **Add** button.

The screenshot shows the Skype for Business Server administration console. The top navigation bar includes 'DIAL PLAN', 'VOICE POLICY', 'ROUTE', 'PSTN USAGE', 'TRUNK CONFIGURATION', and 'TEST VOICE ROUTING'. The left sidebar lists various configuration areas, with 'Voice Routing' selected. The main content area is titled 'New Voice Route' and includes a search bar, 'OK' and 'Cancel' buttons, and a 'Suppress caller ID' checkbox. Below this is an 'Alternate caller ID' field. The 'Associated trunks' section contains an empty list and 'Add' and 'Remove' buttons. A red arrow points to the 'Add' button. At the bottom, there is an 'Associated PSTN Usages' section with a 'Select...' button and 'Remove', 'Up', and 'Down' arrows, and a table with two columns: 'PSTN usage record' and 'Associated voice policies'.

8. You will now be at a window showing available Trunks to associate your Voice Route. Click on the PSTN gateway that you just created and then click the **OK** button.



9. You can now see that you have associated your trunk with the route you created. An appropriate PSTN usage record will need to be assigned as well. In our example, we use one that was already created in the enterprise. Click on the **Select** button under **Associated PSTN Usages**

The screenshot displays the Skype for Business Server administration interface. The left-hand navigation pane includes options such as Home, Users, Topology, IM and Presence, Persistent Chat, Voice Routing (which is currently selected), Voice Features, Response Groups, Conferencing, Clients, Federation and External Access, Monitoring and Archiving, Security, and Network Configuration. The main content area is titled 'New Voice Route' and includes tabs for DIAL PLAN, VOICE POLICY, ROUTE, PSTN USAGE, TRUNK CONFIGURATION, and TEST VOICE ROUTING. A 'Create voice routing test case information' link is visible at the top. Below this, there are 'OK' and 'Cancel' buttons. The configuration area includes an 'Edit' button, a 'Reset' button, and a 'Suppress caller ID' checkbox. An 'Alternate caller ID' field is present. Under 'Associated trunks', a list shows 'PstnGateway:10.64.3.124' with 'Add...' and 'Remove' buttons. The 'Associated PSTN Usages' section is highlighted in blue and contains a 'Select...' button with a red arrow pointing to it, along with a 'Remove' button and up/down arrow icons. Below this is a table with columns for 'PSTN usage record' and 'Associated voice policies'.



10. In the **Select PSTN Usage Record** window displayed, select the appropriate PSTN Usage Record and click **OK**.

PSTN usage record name	Associated routes	Associated voice policies
PSTN_1		Global

11. You will now see the Associated PSTN Usages which you have added. Click the **OK** button at the top of the **New Voice Route** screen.

The screenshot displays the Skype for Business Server administration interface. The left sidebar contains navigation options: Home, Users, Topology, IM and Presence, Persistent Chat, Voice Routing (highlighted), Voice Features, Response Groups, Conferencing, Clients, Federation and External Access, Monitoring and Archiving, Security, and Network Configuration. The main content area is titled 'Edit Voice Route - route1' and includes a 'Create voice routing test case information' section. Below this, there are 'OK' and 'Cancel' buttons. The 'Associated trunks' section shows a table with one entry: 'PstnGateway:10.64.3.124', with 'Add...' and 'Remove' buttons. The 'Associated PSTN Usages' section features a 'Select...' button, a 'Remove' button, and up/down arrow icons. Below these is a table with two columns: 'PSTN usage record' and 'Associated voice policies'. The table contains one row: 'PSTN\_1' and 'Global'. At the bottom, there is a 'Translated number to test:' section with an input field and a 'Go' button.

Skype for Business Server

DIAL PLAN VOICE POLICY ROUTE PSTN USAGE TRUNK CONFIGURATION TEST VOICE ROUTING

Create voice routing test case information

Edit Voice Route - route1

OK Cancel

Associated trunks:

PstnGateway:10.64.3.124	Add...
	Remove

Associated PSTN Usages

Select... Remove ↑ ↓

PSTN usage record	Associated voice policies
PSTN_1	Global

Translated number to test:

Go

12. You will now be at the Routes page showing route1. Click the **Commit** drop-down menu, and then **Commit All**.

The screenshot shows the Skype for Business Server 2015 Control Panel interface. The top navigation bar includes 'DIAL PLAN', 'VOICE POLICY', 'ROUTE', 'PSTN USAGE', 'TRUNK CONFIGURATION', and 'TEST VOICE ROUTING'. The left sidebar lists various configuration areas, with 'Voice Routing' selected. The main content area displays a table of routes. The first row is 'route1', which is in an 'Uncommitted' state. A 'Commit' dropdown menu is open over the 'route1' row, showing options: 'Review uncommitted changes', 'Commit all', 'Cancel selected changes', and 'Cancel all uncommitted changes'. A red arrow points to the 'Commit all' option.

Name	State	PSTN usage	match
route1	Uncommitted	PSTN_1	

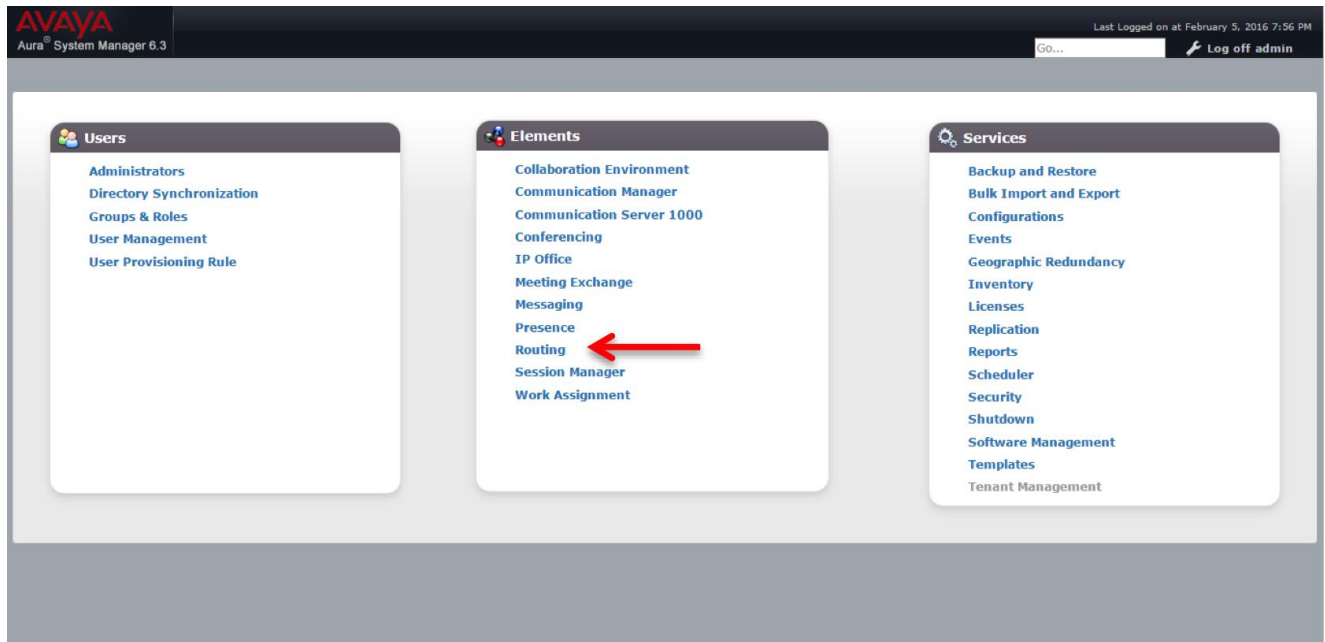
## Phase 6 – Configuring the Avaya Session Manager 6.3

The enterprise has a fully functional Avaya Aura System Manager. Configuring the System Manager to operate with ECB consists of three steps –

- Adding the ECB as a SIP Entity
- Configuring an Entity link between ECB and Session Manager
- Creating a Routing policy to assign the appropriate routing destination.

### Adding the ECB as a SIP Entity

Log in to the Aura System Manager. Click on **Routing** under the **Elements** section.



On the **Routing** tab, select **SIP Entities** from the menu on the left side of the screen. Click **New** to add ECB as a SIP entity as shown below and click **Commit**.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar is expanded to 'Routing' > 'SIP Entities'. The main area displays the 'SIP Entity Details' form for a new entity named 'To ECB'. The form includes fields for Name, FQDN or IP Address, Type, Notes, Adaptation, Location, Time Zone, SIP Timer B/F, Credential name, Call Detail Recording, Loop Detection Mode, Loop Count Threshold, Loop Detection Interval, SIP Link Monitoring, and Entity Links.

**SIP Entity Details** Commit Cancel

**General**

\* Name: To ECB

\* FQDN or IP Address: 10.64.3.124

Type: SIP Trunk

Notes:

Adaptation:

Location: TekV Communications Manager

Time Zone: America/Fortaleza

\* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: egress

**Loop Detection**

Loop Detection Mode: On

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

**SIP Link Monitoring**

SIP Link Monitoring: Link Monitoring Enabled

\* Proactive Monitoring Interval (in seconds): 900

\* Reactive Monitoring Interval (in seconds): 120

\* Number of Retries: 1

Supports Call Admission Control:

Shared Bandwidth Manager:

Primary Session Manager Bandwidth Association:

Backup Session Manager Bandwidth Association:

**Entity Links**

Override Port & Transport with DNS SRV:

Add Remove

1 Item <span style="float: right;">Filter: Enable</span>								
<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* tekaasm to ECB	tekaasm	TCP	* 5060	To ECB	* 5060	trusted	<input type="checkbox"/>

Select : All, None

## Configuring an Entity link between ECB and Session Manager

Select **Entity Links** from the menu and click on **New** to add an Entity Link between ECB and SM with the following settings and click **Commit**.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The top navigation bar includes the Avaya logo, the text "Aura System Manager 6.3", a search box, and a "Log off admin" button. The breadcrumb trail is "Home / Elements / Routing / Entity Links". The left sidebar menu is expanded to "Entity Links". The main content area shows the "Entity Links" configuration page with "Commit" and "Cancel" buttons. Below the buttons is a table with one item:

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	* tekaasm to ECB	* tekaasm	TCP	* 5060	* To ECB	<input type="checkbox"/>	* 5060	trusted	<input type="checkbox"/>	

Below the table, there is a "Select : All, None" option.

## Creating a Routing policy to assign the appropriate routing destination

Select **Routing policies** from the menu and click on **New** to add a routing policy between ECB and SM with the following settings and click **Commit**.

The screenshot shows the Avaya System Manager 6.3 interface. The left sidebar has a menu with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and includes the following sections:

- General:**
  - \* Name: To ECB
  - Disabled:
  - \* Retries: 0
  - Notes: (empty field)
- SIP Entity as Destination:**
  - Select: (dropdown menu)
  - Table with 4 columns: Name, FQDN or IP Address, Type, Notes. One row is visible: Name: To ECB, FQDN or IP Address: 10.64.3.124, Type: SIP Trunk, Notes: (empty).
- Time of Day:**
  - Buttons: Add, Remove, View Gaps/Overlaps
  - 1 Item table with 12 columns: Ranking, Name, Mon, Tue, Wed, Thu, Fri, Sat, Sun, Start Time, End Time, Notes. One row is visible: Ranking: 0, Name: 24/7, Mon: checked, Tue: checked, Wed: checked, Thu: checked, Fri: checked, Sat: checked, Sun: checked, Start Time: 00:00, End Time: 23:59, Notes: Time Range 24/7.
- Dial Patterns:**
  - Buttons: Add, Remove
  - 4 Items table with 8 columns: Pattern, Min, Max, Emergency Call, SIP Domain, Originating Location, Notes. Four rows are visible:
 

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
5327	4	4	<input type="checkbox"/>	lab.tekvizion.com	TekV Communications Manager	
53xx	4	4	<input type="checkbox"/>	lab.tekvizion.com	TekV Communications Manager	
57129353xx	10	10	<input type="checkbox"/>	lab.tekvizion.com	TekV Communications Manager	
9157129353xx	12	12	<input type="checkbox"/>	lab.tekvizion.com	TekV Communications Manager	
- Regular Expressions:**
  - Buttons: Add, Remove
  - 0 Items table with 4 columns: Pattern, Rank Order, Deny, Notes.

At the bottom of the 'Routing Policy Details' section, there are 'Commit' and 'Cancel' buttons.

The Avaya System Manager 6.3 is now configured to operate with the ECB.

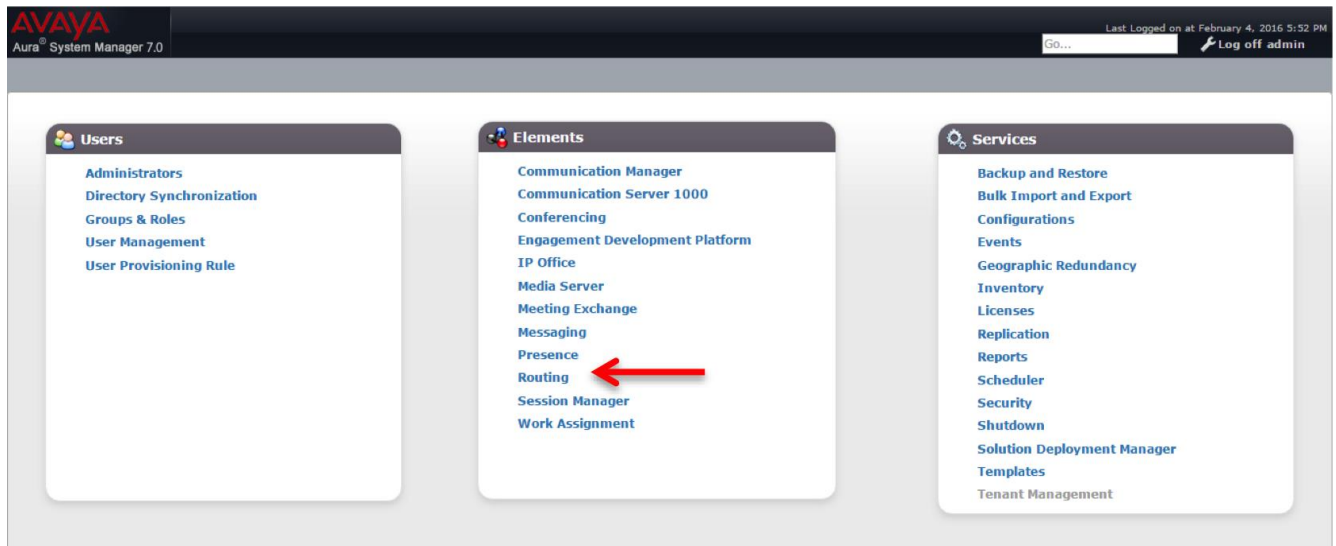
## Phase 7 – Configuring the Avaya Session Manager 7.0

The enterprise has a fully functional Avaya Aura System Manager. Configuring the System Manager to operate with ECB consists of three steps –

- Adding the ECB as a SIP Entity
- Configuring an Entity link between ECB and Session Manager
- Creating a Routing policy to assign the appropriate routing destination.

### Adding the ECB as a SIP Entity

Log in to the Aura System Manager. Click on **Routing** under the **Elements** section.





On the **Routing** tab, select **SIP Entities** from the menu on the left side of the screen. Click **New** to add ECB as a SIP entity as shown below and click **Commit**.

The screenshot shows the 'SIP Entity Details' configuration page. The left sidebar contains a navigation menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and includes a 'Commit' button and a 'Cancel' button. The 'General' section contains the following fields:

- Name:** ECB
- \* FQDN or IP Address:** 10.64.3.124
- Type:** SIP Trunk
- Notes:** Oracle-ECB
- Adaptation:** (empty dropdown)
- Location:** Plano
- Time Zone:** America/Fortaleza
- \* SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Securable:**
- Call Detail Recording:** egress

#### Loop Detection

**Loop Detection Mode:** On

**Loop Count Threshold:** 5

**Loop Detection Interval (in msec):** 200

#### SIP Link Monitoring

**SIP Link Monitoring:** Link Monitoring Enabled

**\* Proactive Monitoring Interval (in seconds):** 30

**\* Reactive Monitoring Interval (in seconds):** 10

**\* Number of Retries:** 1

**Supports Call Admission Control:**

**Shared Bandwidth Manager:**

**Primary Session Manager Bandwidth Association:** (empty dropdown)

**Backup Session Manager Bandwidth Association:** (empty dropdown)


## Configuring an Entity link between ECB and Session Manager

Select **Entity Links** from the menu and click on **New** to add an Entity Link between ECB and SM with the following settings and click **Commit**.

**Entity Links**

Override Port & Transport with DNS SRV:

Add Remove


1 Item  Filter: Enable

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	* AASM7.0 to ECB TCP	AA SM7.0	TCP	* 5060	ECB	* 5060	trusted	<input type="checkbox"/>

Select : All, None

**SIP Responses to an OPTIONS Request**

Add Remove

0 Items  Filter: Enable

<input type="checkbox"/>	Response Code & Reason Phrase	Mark Entity Up/Down	Notes
--------------------------	-------------------------------	---------------------	-------

Commit Cancel

## Creating a Routing policy to assign the appropriate routing destination

Select **Routing policies** from the menu and click on **New** to add a routing policy between ECB and SM with the following settings and click **Commit**.

Home
Routing

Home / Elements / Routing / Routing Policies
Help ?

- Routing
- Domains
- Locations
- Adaptations
- SIP Entities
- Entity Links
- Time Ranges
- Routing Policies
- Dial Patterns
- Regular Expressions
- Defaults

### Routing Policy Details

**General**

\* Name:

Disabled:

\* Retries:

Notes:

**SIP Entity as Destination**

Name	FQDN or IP Address	Type	Notes
ECB	10.64.3.124	SIP Trunk	

**Time of Day**

1 Item Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
<input type="checkbox"/>	0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Select : All, None

**Dial Patterns**

3 Items Filter: Enable

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
<input type="checkbox"/> 532x	4	4	<input type="checkbox"/>	lab.tekvizion.com	Plano	
<input type="checkbox"/> 571293532x	10	10	<input type="checkbox"/>	lab.tekvizion.com	Plano	
<input type="checkbox"/> 9157129353xx	12	12	<input type="checkbox"/>	lab.tekvizion.com	Plano	

Select : All, None

**Regular Expressions**

0 Items Filter: Enable

Pattern	Rank Order	Deny	Notes
---------	------------	------	-------

The Avaya System Manager 7.0 is now configured to operate with the ECB.

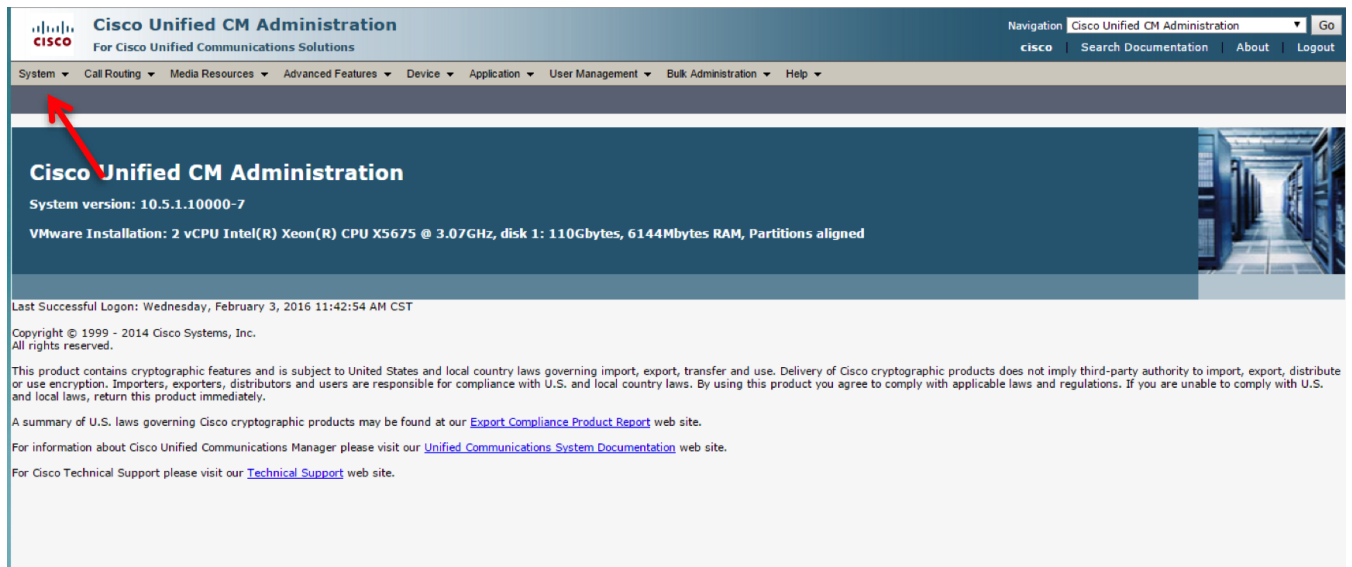
## Phase 8 – Configuring Cisco Unified Communications Manager 10.5

The enterprise will have a fully functioning Cisco Unified Communications Manager deployed. We will now configure it to operate with the ECB. This consists of the following steps

- Configuring the SIP Trunk Security profile
- Configuring the SIP profile
- Configure the Trunk
- Configuring the Route Pattern

### Configuring the SIP Trunk Security Profile

1. Log into the Cisco Unified CM administration page using <https://server-ip/> and then click on **Cisco Unified Communications Manager** under **Installed Applications**.
2. To go to the **SIP trunk security profile** page, expand the **System** drop down menu, select **SIP Trunk Security Profile** under **Security**



**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

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

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

**Cisco Unified CM Administration**  
System version: 10.5.1.10000-7  
VMware Installation: 2 vCPU Intel(R) Xeon(R) CPU X5675 @ 3.07GHz, disk 1: 110Gbytes, 6144Mbytes RAM, Partitions aligned

Last Successful Logon: Wednesday, February 3, 2016 11:42:54 AM CST  
Copyright © 1999 - 2014 Cisco Systems, Inc.  
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our [Export Compliance Product Report](#) web site.

For information about Cisco Unified Communications Manager please visit our [Unified Communications System Documentation](#) web site.

For Cisco Technical Support please visit our [Technical Support](#) web site.

The screenshot displays the Cisco Unified CM Administration web interface. On the left, a navigation menu is open, listing various configuration categories. The 'Security' category is highlighted, and its sub-menu is also open, showing options like Certificate, Phone Security Profile, SIP Trunk Security Profile, and CUMA Server Security Profile. Two red arrows point to the 'Security' and 'SIP Trunk Security Profile' items. The main content area shows system information, including the server name '7', hardware details like 'Intel(R) Xeon(R) CPU X5675 @ 3.07GHz', and a timestamp 'February 3, 2016 11:42:54 AM CST'. There are also links to 'Export Compliance Product Report' and 'Unified Communications System Documentation'.

- Server
  - Cisco Unified CM
  - Cisco Unified CM Group
  - Presence Redundancy Groups
  - Phone NTP Reference
  - Date/Time Group
  - BLF Presence Group
  - Region Information
  - Device Pool
  - Device Mobility
  - DHCP
  - LDAP
  - SAML Single Sign-On
  - Cross-Origin Resource Sharing (CORS)
  - Location Info
  - MLPP
  - Physical Location
  - SRST
  - Enterprise Parameters
  - Enterprise Phone Configuration
  - Service Parameters
  - Security**
    - Certificate
    - Phone Security Profile
    - SIP Trunk Security Profile**
    - CUMA Server Security Profile
  - Application Server
  - Licensing
  - Geolocation Configuration
  - Geolocation Filter
  - E911 Messages

3. A Non Secure SIP Trunk security profile should be present, if not create one as shown below

The screenshot shows the Cisco Unified CM Administration interface for configuring a SIP Trunk Security Profile. The page title is "SIP Trunk Security Profile Configuration". The navigation menu includes System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The configuration page includes a toolbar with Save, Delete, Copy, Reset, Apply Config, and Add New buttons. The Status section shows "Status: Ready". The SIP Trunk Security Profile Information section contains the following fields and options:

Name*	Non Secure SIP Trunk Profile_ for oracle ECB
Description	for ECB testing
Device Security Mode	Non Secure
Incoming Transport Type*	TCP+UDP
Outgoing Transport Type	TCP
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	
Incoming Port*	5060
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input type="checkbox"/> Accept out-of-dialog refer**	
<input type="checkbox"/> Accept unsolicited notification	
<input type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

## Configuring the SIP Profile

1. To go to the SIP Profile page, expand the **Device** drop down menu and select **SIP Profile** from **Device Settings**.

The screenshot shows the Cisco Unified CM Administration web interface. The top navigation bar includes menus for System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The 'Device' menu is expanded, showing options like CTI Route Point, Gatekeeper, Gateway, Phone, Trunk, Remote Destination, and Device Settings. The 'Device Settings' sub-menu is also expanded, listing various configuration options such as Device Defaults, Firmware Load Information, Default Device Profile, Device Profile, Phone Button Template, Softkey Template, Phone Services, SIP Profile, Common Device Configuration, Common Phone Profile, Remote Destination Profile, Feature Control Policy, Recording Profile, SIP Normalization Script, SDP Transparency Profile, Network Access Profile, Wireless LAN Profile, Wireless LAN Profile Group, and Wi-Fi Hotspot Profile. Red arrows point to the 'Device Settings' and 'SIP Profile' options.

Cisco Unified CM Administration  
System version: 10.5.1.10000-7  
VMware Installation: 2 vCPU Intel(R) Xeon(R) CPU X56

Last Successful Logon: Thursday, February 4, 2016 7:18:42 AM CST  
Copyright © 1999 - 2014 Cisco Systems, Inc. All rights reserved.  
This product contains cryptographic features and is subject to United States and local country laws governing importation or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local laws, return this product immediately.  
A summary of U.S. laws governing Cisco cryptographic products may be found at our [Export Compliance Product](#)  
For information about Cisco Unified Communications Manager please visit our [Unified Communications System Doc](#)  
For Cisco Technical Support please visit our [Technical Support](#) web site.

2. The **Find and List SIP Profiles** page will display the default SIP profile. Click on the **Copy** button to create a new SIP profile.







The screenshot shows the 'Find and List SIP Profiles' page. At the top, there are buttons for '+ Add New', 'Select All', 'Clear All', and 'Delete Selected'. Below this, a status bar indicates '1 records found'. The main table displays the following information:

	Name ^	Description	Copy
<input type="checkbox"/>	<a href="#">Standard SIP Profile</a>	Default SIP Profile	

Below the table, there are buttons for '+ Add New', 'Select All', 'Clear All', and 'Delete Selected'. A search bar at the top of the table area contains the text 'Find SIP Profile where Name begins with' and buttons for 'Find', 'Clear Filter', '+', and '-'.


3. Add a new SIP profile with the following settings. It is same as the default profile but includes PRACK support. Click **Save** when finished.


**SIP Profile Configuration**

 Save
  Delete
  Copy
  Reset
  Apply Config
  Add New

---

**Status**

 Status: Ready

 All SIP devices using this profile must be restarted before any changes will take affect.

---

**SIP Profile Information**

Name\*

Description

Default MTP Telephony Event Payload Type\*

Early Offer for G.Clear Calls\*

User-Agent and Server header information\*

Version in User Agent and Server Header\*

Dial String Interpretation\*

Confidential Access Level Headers\*

Redirect by Application

Disable Early Media on 180

Outgoing T.38 INVITE include audio mline

Use Fully Qualified Domain Name in SIP Requests

Assured Services SIP conformance

---

**SDP Information**

SDP Session-level Bandwidth Modifier for Early Offer and Re-invites\*

SDP Transparency Profile

Accept Audio Codec Preferences in Received Offer\*

Require SDP Inactive Exchange for Mid-Call Media Change

Allow RR/RS bandwidth modifier (RFC 3556)

---

**Parameters used in Phone**

Timer Invite Expires (seconds)*	<input type="text" value="180"/>
Timer Register Delta (seconds)*	<input type="text" value="5"/>
Timer Register Expires (seconds)*	<input type="text" value="3600"/>
Timer T1 (msec)*	<input type="text" value="500"/>
Timer T2 (msec)*	<input type="text" value="4000"/>
Retry INVITE*	<input type="text" value="6"/>
Retry Non-INVITE*	<input type="text" value="10"/>
Start Media Port*	<input type="text" value="16384"/>
Stop Media Port*	<input type="text" value="32766"/>
Call Pickup URI*	<input type="text" value="x-cisco-serviceuri-pickup"/>
Call Pickup Group Other URI*	<input type="text" value="x-cisco-serviceuri-opickup"/>
Call Pickup Group URI*	<input type="text" value="x-cisco-serviceuri-gpickup"/>
Meet Me Service URI*	<input type="text" value="x-cisco-serviceuri-meetme"/>



User Info\*

DTMF DB Level\*

Call Hold Ring Back\*

Anonymous Call Block\*

Caller ID Blocking\*

Do Not Disturb Control\*

Telnet Level for 7940 and 7960\*

Resource Priority Namespace

Timer Keep Alive Expires (seconds)\*

Timer Subscribe Expires (seconds)\*

Timer Subscribe Delta (seconds)\*

Maximum Redirections\*

Off Hook To First Digit Timer (milliseconds)\*

Call Forward URI\*

Speed Dial (Abbreviated Dial) URI\*

Conference Join Enabled

RFC 2543 Hold

Semi Attended Transfer

Enable VAD

Stutter Message Waiting

MLPP User Authorization

**Normalization Script**

Normalization Script

Enable Trace

	Parameter Name	Parameter Value		
1	<input type="text"/>	<input type="text"/>	<input type="button" value="+"/>	<input type="button" value="-"/>

**Incoming Requests FROM URI Settings**

Caller ID DN

Caller Name

**Trunk Specific Configuration**

Reroute Incoming Request to new Trunk based on\*

RSVP Over SIP\*

Resource Priority Namespace List

Fall back to local RSVP

SIP Rel1XX Options\*

Video Call Traffic Class\*

Calling Line Identification Presentation\*

Session Refresh Method\*

Early Offer support for voice and video calls\*



- Enable ANAT
- Deliver Conference Bridge Identifier
- Allow Passthrough of Configured Line Device Caller Information
- Reject Anonymous Incoming Calls
- Reject Anonymous Outgoing Calls
- Send ILS Learned Destination Route String

**SIP OPTIONS Ping**

Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"

Ping Interval for In-service and Partially In-service Trunks (seconds)\*

Ping Interval for Out-of-service Trunks (seconds)\*

Ping Retry Timer (milliseconds)\*

Ping Retry Count\*

**SDP Information**

- Send send-receive SDP in mid-call INVITE
- Allow Presentation Sharing using BFCP
- Allow iX Application Media
- Allow multiple codecs in answer SDP

## Configuring the Trunk

- To go to the Trunks page, select **Trunk** from the **Device** drop down menu.

The screenshot shows the Cisco Unified CM Administration web interface. At the top, there is a navigation bar with several dropdown menus: System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The 'Device' dropdown menu is open, showing a list of options: CTI Route Point, Gatekeeper, Gateway, Phone, Trunk (highlighted with a red arrow), Remote Destination, and Device Settings. The main content area displays 'Cisco Unified CM Administration' and 'System version: 10.5.1.10000-7'. At the bottom, there is a footer with copyright information and links to external resources.

2. Add a trunk with the following settings and click **Save**.

**Trunk Configuration**

Save  Delete  Reset  Add New

**Status**

**i** Status: Ready

**SIP Trunk Status**

**Service Status:** Full Service  
**Duration:** Time In Full Service: 0 day 19 hours 44 minutes

**Device Information**

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	Oracle_SIP_trunk
Description	to ECB oracle
Device Pool*	Default
Common Device Configuration	< None >
Call Classification*	Use System Default
Media Resource Group List	AllCMsMediaResGrpList
Location*	Hub_None
AAR Group	< None >
Tunneled Protocol*	None
QSIG Variant*	No Changes
ASN.1 ROSE OID Encoding*	No Changes
Packet Capture Mode*	Batch Processing Mode
Packet Capture Duration	0

Media Termination Point Required

Retry Video Call as Audio

Path Replacement Support

Transmit UTF-8 for Calling Party Name

Transmit UTF-8 Names in QSIG APDU

Unattended Port

SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information.

Consider Traffic on This Trunk Secure\*  When using both sRTP and TLS

Route Class Signaling Enabled\*  Default

Use Trusted Relay Point\*  Default

PSTN Access

Run On All Active Unified CM Nodes

**Intercompany Media Engine (IME)**

E.164 Transformation Profile  < None >

**MLPP and Confidential Access Level Information**

MLPP Domain

Confidential Access Mode

Confidential Access Level

**Call Routing Information**

Remote-Party-Id

Asserted-Identity

Asserted-Type\*

SIP Privacy\*

**Inbound Calls**

Significant Digits\*

Connected Line ID Presentation\*

Connected Name Presentation\*

Calling Search Space

AAR Calling Search Space

Prefix DN

Redirecting Diversion Header Delivery - Inbound

**Incoming Calling Party Settings**

If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.

Number Type	Prefix	Strip Digits	Calling Search Space	Use Device Pool CSS
Incoming Number	<input style="width: 100px;" type="text" value=" Default "/>	<input style="width: 50px;" type="text" value=" 0 "/>	<input style="width: 150px;" type="text" value=" &lt; None &gt; "/>	<input checked="" type="checkbox"/>

**Incoming Called Party Settings**

If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.

Number Type	Prefix	Strip Digits	Calling Search Space	Use Device Pool CSS
Incoming Number	<input style="width: 100px;" type="text" value=" Default "/>	<input style="width: 50px;" type="text" value=" 0 "/>	<input style="width: 150px;" type="text" value=" &lt; None &gt; "/>	<input checked="" type="checkbox"/>

**Connected Party Settings**

Connected Party Transformation CSS

Use Device Pool Connected Party Transformation CSS

**Outbound Calls**

Called Party Transformation CSS

Use Device Pool Called Party Transformation CSS

Calling Party Transformation CSS

Use Device Pool Calling Party Transformation CSS

Calling Party Selection\*

Calling Line ID Presentation\*

Calling Name Presentation\*

Calling and Connected Party Info Format\*

Redirecting Diversion Header Delivery - Outbound

Redirecting Party Transformation CSS

Use Device Pool Redirecting Party Transformation CSS

**Caller Information**

Caller ID DN

Caller Name

Maintain Original Caller ID DN and Caller Name in Identity Headers

**SIP Information**

**Destination**

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port	Status	Status Reason	Duration
1 *	10.64.3.124		5060	up		Time Up: 0 day 44 minu

MTP Preferred Originating Codec\*

BLF Presence Group\*

SIP Trunk Security Profile\*

Rerouting Calling Search Space

Out-Of-Dialog Refer Calling Search Space

SUBSCRIBE Calling Search Space

SIP Profile\*  [View Details](#)

DTMF Signaling Method\*

**Normalization Script**

Normalization Script

Enable Trace

	Parameter Name	Parameter Value
1		

**Recording Information**

None

This trunk connects to a recording-enabled gateway

This trunk connects to other clusters with recording-enabled gateways

**Geolocation Configuration**

Geolocation

Geolocation Filter

Send Geolocation Information

**i** \* - indicates required item.

**i** \*\* - Device reset is not required for changes to Packet Capture Mode and Packet Capture Duration.

## Configuring the Route Pattern

- To go to the Route pattern page, click on **Call Routing** and select **Route Pattern** from the **Route/Hunt** drop down menu.

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration

cisco | Search Documentation | About | Logout

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

**Cisco Unified CM Administration**

System version: 10.5.1.10000-7

VMware Installation: 2 vCPU Intel(R) Xeon(R) CPU X5675 @ 3.07GHz, disk 1: 110Gbytes, 6144Mbytes RAM, Partitions aligned

Last Successful Logon: Thursday, February 4, 2016 7:18:42 AM CST

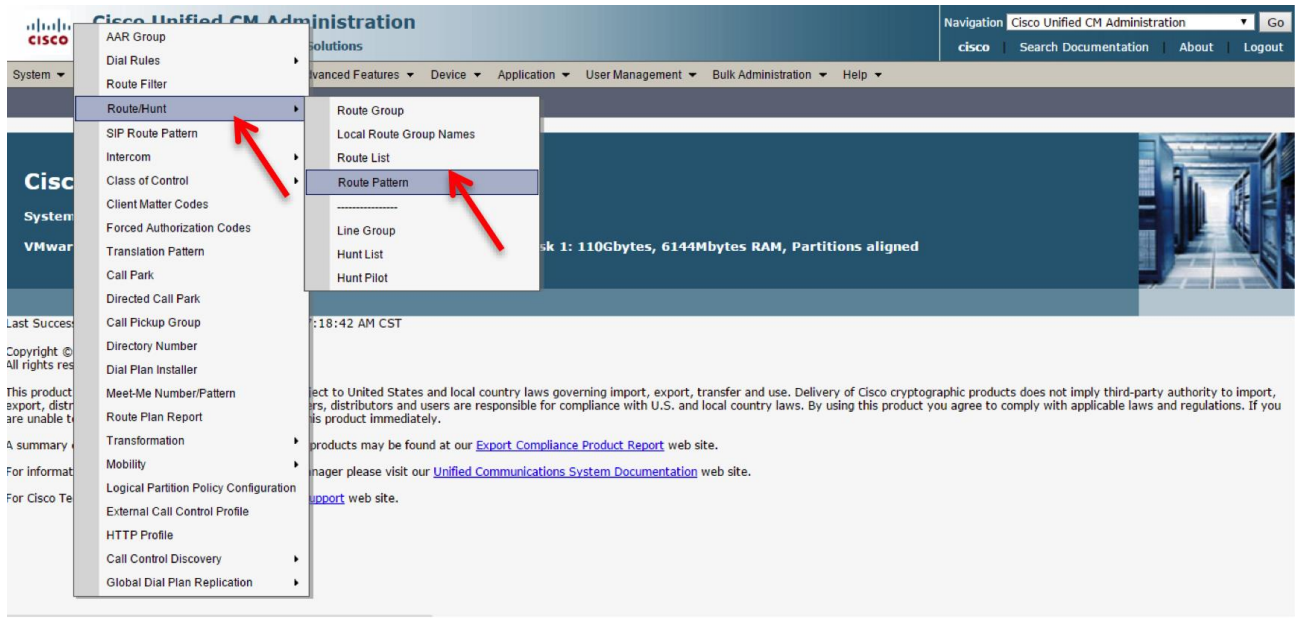
Copyright © 1999 - 2014 Cisco Systems, Inc.  
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our [Export Compliance Product Report](#) web site.

For information about Cisco Unified Communications Manager please visit our [Unified Communications System Documentation](#) web site.

For Cisco Technical Support please visit our [Technical Support](#) web site.



- In our setup, users dial 6 to dial out. Add a route pattern with the following settings and associate it with the trunk configured in the previous step, then click **Save**.

**Route Pattern Configuration**

Save Delete Copy Add New

**Status**  
 Status: Ready

**Pattern Definition**

Route Pattern\* 6.@

Route Partition < None >

Description towards ECB

Numbering Plan\* NANP

Route Filter < None >

MLPP Precedence\* Default

Apply Call Blocking Percentage

Resource Priority Namespace Network Domain < None >

Route Class\* Default

Gateway/Route List\* Oracle\_SIP\_trunk (Edit)

Route Option  
 Route this pattern  
 Block this pattern No Error

Call Classification\* OffNet

External Call Control Profile < None >

Allow Device Override  Provide Outside Dial Tone  Allow Overlap Sending  Urgent Priority

Require Forced Authorization Code

Authorization Level\*

Require Client Matter Code

---

**Calling Party Transformations**

Use Calling Party's External Phone Number Mask

Calling Party Transform Mask

Prefix Digits (Outgoing Calls)

Calling Line ID Presentation\*

Calling Name Presentation\*

Calling Party Number Type\*

Calling Party Numbering Plan\*

---

**Connected Party Transformations**

Connected Line ID Presentation\*

Connected Name Presentation\*

---

**Called Party Transformations**

Discard Digits

Called Party Transform Mask

Prefix Digits (Outgoing Calls)

Called Party Number Type\*

Called Party Numbering Plan\*

---

**ISDN Network-Specific Facilities Information Element**

Network Service Protocol

Carrier Identification Code

Network Service	Service Parameter Name	Service Parameter Value
<input type="text" value="-- Not Selected --"/>	<input type="text" value="&lt; Not Exist &gt;"/>	<input type="text"/>

The CUCM 10.5 configuration is now complete.


## Phase 9 – Configuring Cisco Unified Communications Manager 11.0

The enterprise will have a fully functioning Cisco Unified Communications Manager deployed. We will now configure it to operate with the ECB. This consists of the following steps

- Configuring the SIP Trunk Security profile
- Configuring the SIP profile
- Configure the Trunk
- Configuring the Route Pattern

### Configuring the SIP Trunk Security Profile

1. Log into the Cisco Unified CM administration page using [https://server\\_ip/](https://server_ip/) and then click on Cisco Unified **Communications Manager** under **Installed Applications**.
2. To go to the **SIP trunk security profile** page, expand the **System** drop down menu, select **SIP Trunk Security Profile** under **Security**



The screenshot displays the Cisco Unified CM Administration web interface. At the top, there is a navigation bar with the Cisco logo and the text 'Cisco Unified CM Administration For Cisco Unified Communications Solutions'. Below this is a navigation menu with items like 'System', 'Call Routing', 'Media Resources', 'Advanced Features', 'Device', 'Application', 'User Management', 'Bulk Administration', and 'Help'. The 'System' menu is expanded, showing a warning icon and the text 'WARNING: No backup device is configured. This is required to recover your system in case of failure.' Below the warning, the main content area shows 'Cisco Unified CM Administration' with system version '11.0.1.10000-10' and VMware installation details: 'VMware Installation: 2 vCPU Intel(R) Xeon(R) CPU X5675 @ 3.07GHZ, disk 1: 110Gbytes, 6144Mbytes RAM, Partitions aligned'. A red arrow points to the 'System' menu item.

User cisco last logged in to this cluster on Wednesday, February 3, 2016 6:39:31 AM CST, to node 10.71.3.10, from 172.16.31.200 using HTTPS

Copyright © 1999 - 2015 Cisco Systems, Inc.  
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our [Export Compliance Product Report](#) web site.

For information about Cisco Unified Communications Manager please visit our [Unified Communications System Documentation](#) web site.

For Cisco Technical Support please visit our [Technical Support](#) web site.



Cisco Unified CM Administration

Communications Solutions

Resources ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

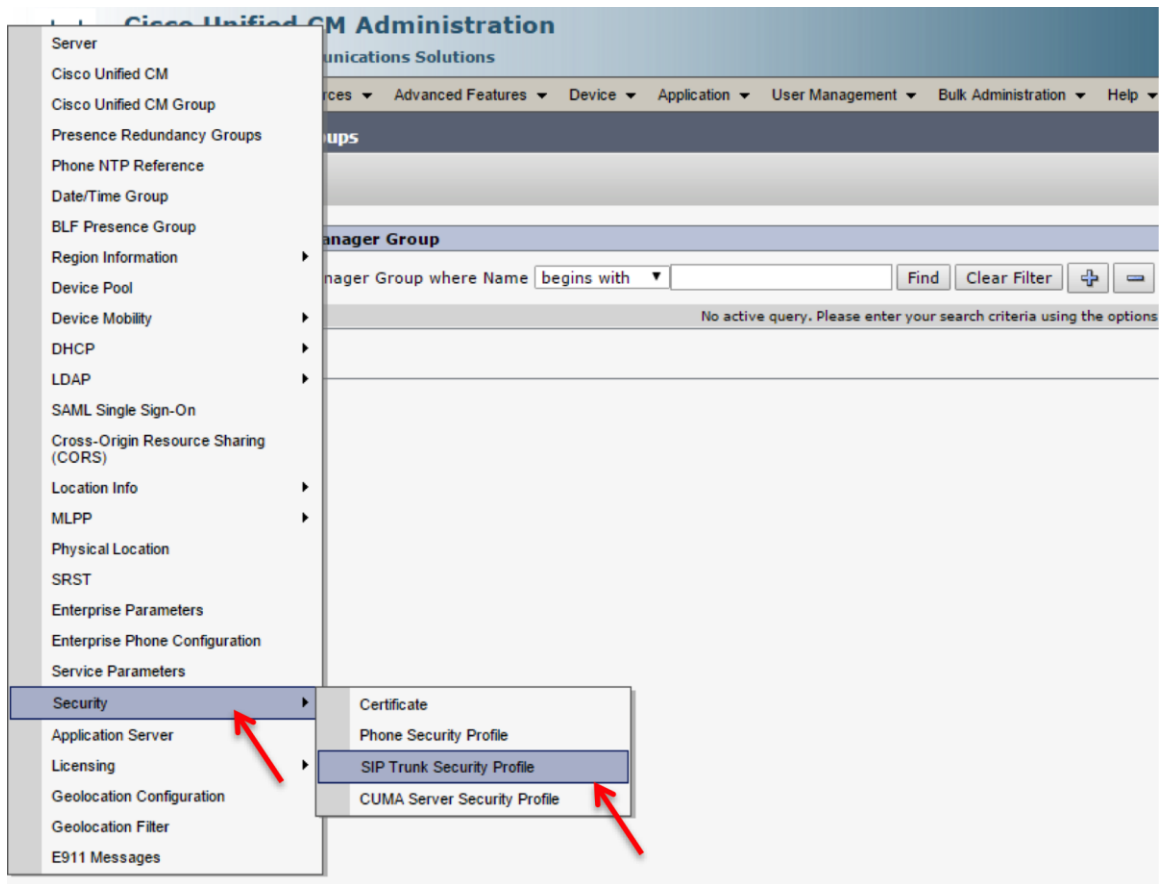
### Groups

#### Manager Group

Manager Group where Name

No active query. Please enter your search criteria using the options

- Server
  - Cisco Unified CM
  - Cisco Unified CM Group
  - Presence Redundancy Groups
  - Phone NTP Reference
  - Date/Time Group
  - BLF Presence Group
  - Region Information ▶
  - Device Pool
  - Device Mobility ▶
  - DHCP ▶
  - LDAP ▶
  - SAML Single Sign-On
  - Cross-Origin Resource Sharing (CORS)
  - Location Info ▶
  - MLPP ▶
  - Physical Location
  - SRST
  - Enterprise Parameters
  - Enterprise Phone Configuration
  - Service Parameters
  - Security ▶**
    - Certificate
    - Phone Security Profile
    - SIP Trunk Security Profile**
    - CUMA Server Security Profile
  - Application Server
  - Licensing ▶
  - Geolocation Configuration
  - Geolocation Filter
  - E911 Messages



3. A Non Secure SIP Trunk security profile should be present, if not create one as shown below

### SIP Trunk Security Profile Configuration

Save Delete Copy Reset Apply Config Add New

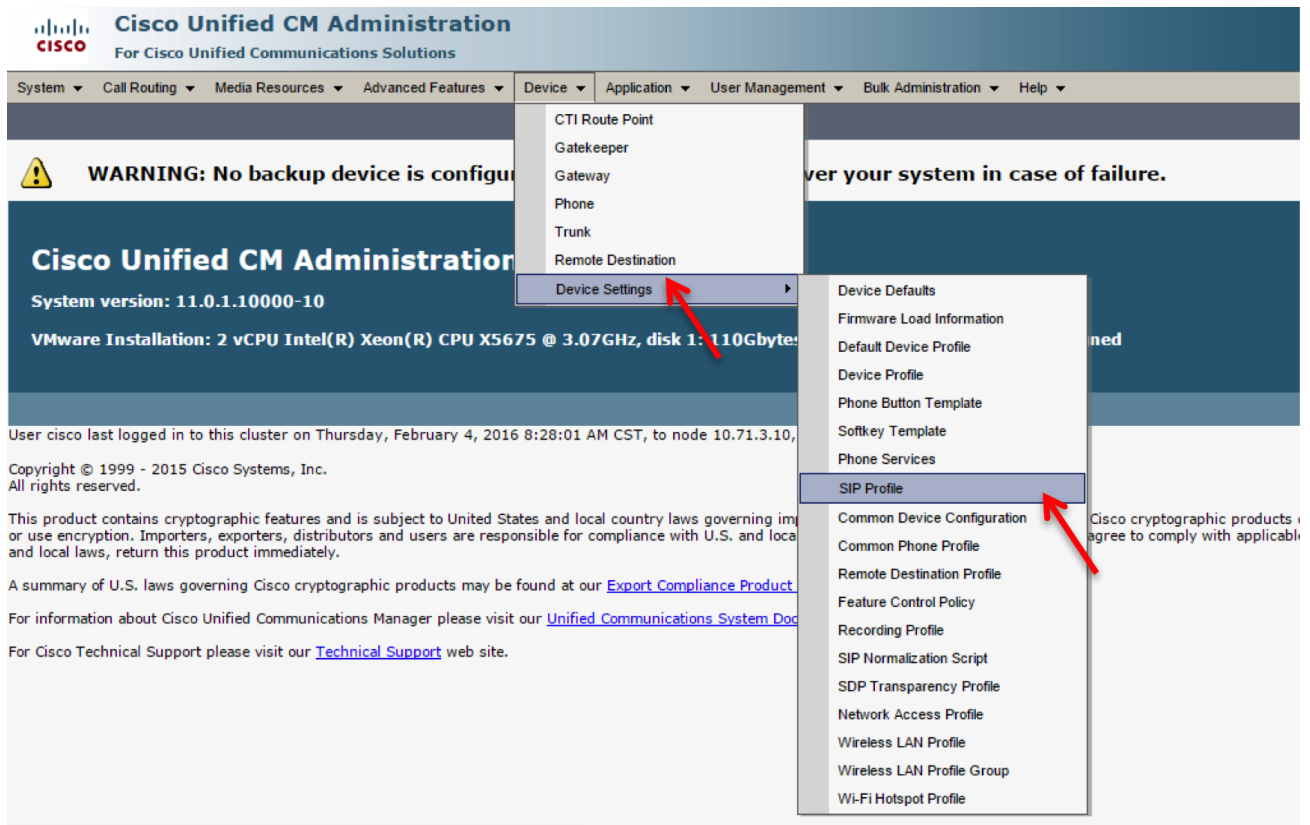
**Status**  
Status: Ready

**SIP Trunk Security Profile Information**

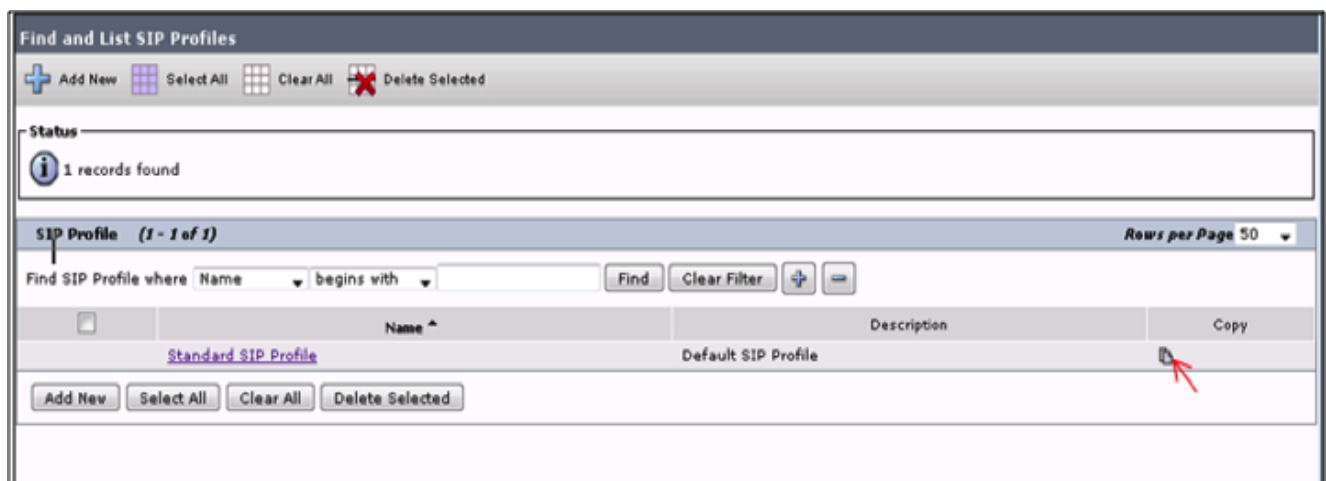
Name*	Non Secure SIP Trunk Profile_ for oracle ECB
Description	for ECB testing- Rajkamal
Device Security Mode	Non Secure
Incoming Transport Type*	TCP+UDP
Outgoing Transport Type	TCP
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	
Incoming Port*	5060
<input type="checkbox"/> Enable Application level authorization	
<input type="checkbox"/> Accept presence subscription	
<input type="checkbox"/> Accept out-of-dialog refer**	
<input type="checkbox"/> Accept unsolicited notification	
<input type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Use Default Filter

## Configuring the SIP Profile

1. To go to the SIP Profile page, expand the **Device** drop down menu and select **SIP Profile** from **Device Settings**.



2. The **Find and List SIP Profiles** page will display the default SIP profile. Click on the **Copy** button to create a new SIP profile.



3. Add a new SIP profile with the following settings. It is same as the default profile but includes PRACK support. Click **Save** when finished.

**SIP Profile Configuration**

Save ✖ Delete 📄 Copy 🔄 Reset 🔧 Apply Config ➕ Add New

---

**Status**

- 📘 Status: Ready
- 📘 All SIP devices using this profile must be restarted before any changes will take affect.

---

**SIP Profile Information**

Name*	<input type="text" value="oracle_ECB_sip_profile"/>
Description	<input type="text" value="Profile with prack"/>
Default MTP Telephony Event Payload Type*	<input type="text" value="101"/>
Early Offer for G.Clear Calls*	<input type="text" value="Disabled"/>
User-Agent and Server header information*	<input type="text" value="Send Unified CM Version Information as User-Ager"/>
Version in User Agent and Server Header*	<input type="text" value="Major And Minor"/>
Dial String Interpretation*	<input type="text" value="Phone number consists of characters 0-9, *, #, an"/>
Confidential Access Level Headers*	<input type="text" value="Disabled"/>

Redirect by Application  
 Disable Early Media on 180  
 Outgoing T.38 INVITE include audio mline  
 Use Fully Qualified Domain Name in SIP Requests  
 Assured Services SIP conformance

---

**SDP Information**

SDP Session-level Bandwidth Modifier for Early Offer and Re-invites*	<input type="text" value="TIAS and AS"/>
SDP Transparency Profile	<input type="text" value="&lt; None &gt;"/>
Accept Audio Codec Preferences in Received Offer*	<input type="text" value="Default"/>

Require SDP Inactive Exchange for Mid-Call Media Change  
 Allow RR/RS bandwidth modifier (RFC 3556)

---

**Parameters used in Phone**

Timer Invite Expires (seconds)*	<input type="text" value="180"/>
Timer Register Delta (seconds)*	<input type="text" value="5"/>
Timer Register Expires (seconds)*	<input type="text" value="3600"/>
Timer T1 (msec)*	<input type="text" value="500"/>
Timer T2 (msec)*	<input type="text" value="4000"/>
Retry INVITE*	<input type="text" value="6"/>
Retry Non-INVITE*	<input type="text" value="10"/>
Media Port Ranges	<input checked="" type="radio"/> Common Port Range for Audio and Video <input type="radio"/> Separate Port Ranges for Audio and Video
Start Media Port*	<input type="text" value="16384"/>
Stop Media Port*	<input type="text" value="32766"/>
DSCP for Audio Calls	<input type="text" value="Use System Default"/>
DSCP for Video Calls	<input type="text" value="Use System Default"/>
DSCP for Audio Portion of Video Calls	<input type="text" value="Use System Default"/>

DSCP for TelePresence Calls	Use System Default
DSCP for Audio Portion of TelePresence Calls	Use System Default
Call Pickup URI*	x-cisco-serviceuri-pickup
Call Pickup Group Other URI*	x-cisco-serviceuri-opickup
Call Pickup Group URI*	x-cisco-serviceuri-gpickup
Meet Me Service URI*	x-cisco-serviceuri-meetme
User Info*	None
DTMF DB Level*	Nominal
Call Hold Ring Back*	Off
Anonymous Call Block*	Off
Caller ID Blocking*	Off
Do Not Disturb Control*	User
Telnet Level for 7940 and 7960*	Disabled
Resource Priority Namespace	< None >
Timer Keep Alive Expires (seconds)*	120
Timer Subscribe Expires (seconds)*	120
Timer Subscribe Delta (seconds)*	5
Maximum Redirections*	70
Off Hook To First Digit Timer (milliseconds)*	15000
Call Forward URI*	x-cisco-serviceuri-cfwdall
Speed Dial (Abbreviated Dial) URI*	x-cisco-serviceuri-abbrdial

- Conference Join Enabled
- RFC 2543 Hold
- Semi Attended Transfer
- Enable VAD
- Stutter Message Waiting
- MLPP User Authorization

#### Normalization Script

Normalization Script < None >

Enable Trace

	Parameter Name	Parameter Value	
1	<input type="text"/>	<input type="text"/>	<input type="button" value="+"/> <input type="button" value="-"/>

#### Incoming Requests FROM URI Settings

Caller ID DN

Caller Name

#### Trunk Specific Configuration

Reroute Incoming Request to new Trunk based on\*

Resource Priority Namespace List

SIP Rel1XX Options\*

Video Call Traffic Class\*

Calling Line Identification Presentation\*

Session Refresh Method\*



Early Offer support for voice and video calls\* Disabled (Default value) ▼

- Enable ANAT
- Deliver Conference Bridge Identifier
- Allow Passthrough of Configured Line Device Caller Information
- Reject Anonymous Incoming Calls
- Reject Anonymous Outgoing Calls
- Send ILS Learned Destination Route String

#### SIP OPTIONS Ping

Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"

Ping Interval for In-service and Partially In-service Trunks (seconds)\*

Ping Interval for Out-of-service Trunks (seconds)\*

Ping Retry Timer (milliseconds)\*

Ping Retry Count\*

#### SDP Information

- Send send-receive SDP in mid-call INVITE
- Allow Presentation Sharing using BFCP
- Allow iX Application Media
- Allow multiple codecs in answer SDP

## Configuring the Trunk

1. To go to the Trunks page, select **Trunk** from the **Device** drop down menu.

The screenshot shows the Cisco Unified CM Administration web interface. At the top, there is a navigation bar with the Cisco logo and the text "Cisco Unified CM Administration For Cisco Unified Communications Solutions". Below this is a navigation menu with items like System, Call Routing, Media Resources, Advanced Features, Device, Application, User Management, Bulk Administration, and Help. The "Device" dropdown menu is open, showing options: CTI Route Point, Gatekeeper, Gateway, Phone, Trunk (highlighted with a blue bar and a red arrow), Remote Destination, and Device Settings. A warning banner is visible in the background, stating "WARNING: No backup device is configured. Back up your system in case of failure." Below the navigation menu, there is a main content area with the text "Cisco Unified CM Administration" and "System version: 11.0.1.10000-10". At the bottom of the page, there is a footer with copyright information and links to compliance reports, documentation, and technical support.

2. Add a trunk with the following settings and click **Save**.

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

### Trunk Configuration

Save 
 Delete 
 Reset 
 Add New

---

**Status**

Status: Ready

---

**SIP Trunk Status**

**Service Status:** Full Service  
**Duration:** Time In Full Service: 2 days 23 hours 37 minutes

---

**Device Information**

Product:	SIP Trunk
Device Protocol:	SIP
Trunk Service Type	None(Default)
Device Name*	<input type="text" value="Oracle_SIP_trunk"/>
Description	<input type="text" value="to ECB oracle"/>
Device Pool*	<input type="text" value="Default"/>
Common Device Configuration	<input type="text" value="Common Device Config"/>
Call Classification*	<input type="text" value="Use System Default"/>
Media Resource Group List	<input type="text" value="MRGL1"/>
Location*	<input type="text" value="Hub_None"/>
AAR Group	<input type="text" value="&lt; None &gt;"/>
Tunneled Protocol*	<input type="text" value="None"/>
QSIG Variant*	<input type="text" value="No Changes"/>
ASN.1 ROSE OID Encoding*	<input type="text" value="No Changes"/>
Packet Capture Mode*	<input type="text" value="Batch Processing Mode"/>

---

Packet Capture Mode\*

Packet Capture Duration

Media Termination Point Required  
 Retry Video Call as Audio  
 Path Replacement Support  
 Transmit UTF-8 for Calling Party Name  
 Transmit UTF-8 Names in QSIG APDU  
 Unattended Port  
 SRTP Allowed - When this flag is checked, Encrypted TLS needs to be configured in the network to provide end to end security. Failure to do so will expose keys and other information. Consider Traffic on This Trunk Secure\*

Route Class Signaling Enabled\*

Use Trusted Relay Point\*

PSTN Access  
 Run On All Active Unified CM Nodes

---

**-Intercompany Media Engine (IME)-**

E.164 Transformation Profile

---

**-MLPP and Confidential Access Level Information-**

MLPP Domain

Confidential Access Mode

Confidential Access Level

**Call Routing Information**

Remote-Party-Id  
 Asserted-Identity  
 Asserted-Type\* [PAI]  
 SIP Privacy\* [Default]

**Inbound Calls**

Significant Digits\* [4]  
 Connected Line ID Presentation\* [Default]  
 Connected Name Presentation\* [Default]  
 Calling Search Space [< None >]  
 AAR Calling Search Space [< None >]  
 Prefix DN [ ]  
 Redirecting Diversion Header Delivery - Inbound

**Incoming Calling Party Settings**

If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.

[Clear Prefix Settings] [Default Prefix Settings]

Number Type	Prefix	Strip Digits	Calling Search Space	Use Device Pool CSS
Incoming Number	[Default]	[0]	[< None >]	<input checked="" type="checkbox"/>

**Incoming Called Party Settings**

If the administrator sets the prefix to Default this indicates call processing will use prefix at the next level setting (DevicePool/Service Parameter). Otherwise, the value configured is used as the prefix unless the field is empty in which case there is no prefix assigned.

[Clear Prefix Settings] [Default Prefix Settings]

Number Type	Prefix	Strip Digits	Calling Search Space	Use Device Pool CSS
Incoming Number	[Default]	[0]	[< None >]	<input checked="" type="checkbox"/>

**Connected Party Settings**

Connected Party Transformation CSS [< None >]  
 Use Device Pool Connected Party Transformation CSS

**Outbound Calls**

Called Party Transformation CSS [< None >]  
 Use Device Pool Called Party Transformation CSS  
 Calling Party Transformation CSS [< None >]  
 Use Device Pool Calling Party Transformation CSS  
 Calling Party Selection\* [Originator]  
 Calling Line ID Presentation\* [Default]  
 Calling Name Presentation\* [Default]  
 Calling and Connected Party Info Format\* [Deliver DN only in connected party]  
 Redirecting Diversion Header Delivery - Outbound  
 Redirecting Party Transformation CSS [< None >]  
 Use Device Pool Redirecting Party Transformation CSS

**Caller Information**

Caller ID DN [ ]  
 Caller Name [ ]  
 Maintain Original Caller ID DN and Caller Name in Identity Headers

**SIP Information**

**Destination**

Destination Address is an SRV

1*	Destination Address	Destination Address IPv6	Destination Port	Status	Status Reason	Duration
	[10.64.3.124]	[ ]	[5060]	up		Time Up: 0 day 23 hour 37 minutes

MTP Preferred Originating Codec\* [711ulaw]  
 BLF Presence Group\* [Standard Presence group]  
 SIP Trunk Security Profile\* [Non Secure SIP Trunk Profile\_ for oracle ECB]  
 Rerouting Calling Search Space [< None >]  
 Out-Of-Dialog Refer Calling Search Space [< None >]  
 SUBSCRIBE Calling Search Space [< None >]  
 SIP Profile\* [oracle\_ECB\_sip\_profile] [View Details](#)  
 DTMF Signaling Method\* [No Preference]



**Normalization Script**

Normalization Script < None >

Enable Trace

	Parameter Name	Parameter Value		
1			<input type="button" value="+"/>	<input type="button" value="-"/>

---

**Recording Information**

None

This trunk connects to a recording-enabled gateway

This trunk connects to other clusters with recording-enabled gateways

---

**Geolocation Configuration**

Geolocation < None >

Geolocation Filter < None >

Send Geolocation Information

## Configuring the Route Pattern

- To go to the Route pattern page, click on **Call Routing** and select **Route Pattern** from the **Route/Hunt** drop down menu.

**Cisco Unified CM Administration**  
For Cisco Unified Communications Solutions

Navigation: Cisco Unified CM Administration

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

**WARNING:** No backup device is configured. This is required to recover your system in case of failure.

**Cisco Unified CM Administration**

System version: 11.0.1.10000-10

VMware Installation: 2 vCPU Intel(R) Xeon(R) CPU X5675 @ 3.07GHz, disk 1: 110Gbytes, 6144Mbytes RAM, Partitions aligned

User cisco last logged in to this cluster on Wednesday, February 3, 2016 6:39:31 AM CST, to node 10.71.3.10, from 172.16.31.200 using HTTPS

Copyright © 1999 - 2015 Cisco Systems, Inc.  
All rights reserved.

This product contains cryptographic features and is subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco cryptographic products does not imply third-party authority to import, export, distribute or use encryption. Importers, exporters, distributors and users are responsible for compliance with U.S. and local country laws. By using this product you agree to comply with applicable laws and regulations. If you are unable to comply with U.S. and local laws, return this product immediately.

A summary of U.S. laws governing Cisco cryptographic products may be found at our [Export Compliance Product Report](#) web site.

For information about Cisco Unified Communications Manager please visit our [Unified Communications System Documentation](#) web site.

For Cisco Technical Support please visit our [Technical Support](#) web site.



# Cisco Unified CM Administration

For Cisco Unified Communications Solutions

System ▾ Advanced Features ▾ Device ▾ Application ▾ User Management ▾ Bulk Administration ▾ Help ▾

- System ▾
  - AAR Group
  - Dial Rules ▶
  - Route Filter
  - Route/Hunt ▶**
    - Route Group
    - Local Route Group Names
    - Route List
    - Route Pattern ▶**
      - 
      - Line Group
      - Hunt List
      - Hunt Pilot
  - SIP Route Pattern
  - Class of Control ▶
  - Intercom ▶
  - Client Matter Codes
  - Forced Authorization Codes
  - Emergency Location ▶
  - Translation Pattern
  - Call Park
  - Directed Call Park
  - Call Pickup Group
  - Directory Number
  - Meet-Me Number/Pattern
  - Conference Now
  - Dial Plan Installer
  - Route Plan Report
  - Transformation ▶
  - Mobility ▶
  - Logical Partition Policy Configuration
  - External Call Control Profile
  - HTTP Profile
  - Call Control Discovery ▶
  - Global Dial Plan Replication ▶

Required to recover your system in case of failure.

Link 1: 110Gbytes, 6144Mbytes RAM, Partitions aligned

February 4, 2016 8:28:01 AM CST, to node 10.71.3.10, from 172.16.29.51 using HTTPS

subject to United States and local country laws governing import, export, transfer and use. Delivery of Cisco crypt... and users are responsible for compliance with U.S. and local country laws. By using this product you agree to con...

c products may be found at our [Export Compliance Product Report](#) web site.

anager please visit our [Unified Communications System Documentation](#) web site.

[Support](#) web site.

User cisco l  
Copyright ©  
All rights res  
This produc  
or use encry  
and local lav  
A summary  
For informat  
For Cisco Te

- In our setup, users dial 6 to dial out. Add a route pattern with the following settings and associate it with the trunk configured in the previous step, then click **Save**.

### Route Pattern Configuration

Save Delete Copy Add New

---

#### Status

Status: Ready

---

#### Pattern Definition

Route Pattern*	<input type="text" value="6.@"/>
Route Partition	< None >
Description	<input type="text" value="From CUCM to ECB for Oracle"/>
Numbering Plan*	NANP
Route Filter	< None >
MLPP Precedence*	Default
<input type="checkbox"/> Apply Call Blocking Percentage	
Resource Priority Namespace Network Domain	< None >
Route Class*	Default
Gateway/Route List*	Oracle_SIP_trunk <a href="#">(Edit)</a>
Route Option	<input checked="" type="radio"/> Route this pattern <input type="radio"/> Block this pattern <input type="text" value="No Error"/>
Call Classification*	OffNet
External Call Control Profile	< None >
<input type="checkbox"/> Allow Device Override <input checked="" type="checkbox"/> Provide Outside Dial Tone <input type="checkbox"/> Allow Overlap Sending <input type="checkbox"/> Urgent Priority	
<input type="checkbox"/> Require Forced Authorization Code	
Authorization Level*	<input type="text" value="0"/>
<input type="checkbox"/> Require Client Matter Code	

### Calling Party Transformations

Use Calling Party's External Phone Number Mask

Calling Party Transform Mask	<input type="text"/>
Prefix Digits (Outgoing Calls)	<input type="text" value="571293"/>
Calling Line ID Presentation*	<input type="text" value="Default"/>
Calling Name Presentation*	<input type="text" value="Default"/>
Calling Party Number Type*	<input type="text" value="Cisco CallManager"/>
Calling Party Numbering Plan*	<input type="text" value="Cisco CallManager"/>

### Connected Party Transformations

Connected Line ID Presentation*	<input type="text" value="Default"/>
Connected Name Presentation*	<input type="text" value="Default"/>

### Called Party Transformations

Discard Digits	<input type="text" value="PreDot"/>
Called Party Transform Mask	<input type="text"/>
Prefix Digits (Outgoing Calls)	<input type="text"/>
Called Party Number Type*	<input type="text" value="Cisco CallManager"/>
Called Party Numbering Plan*	<input type="text" value="Cisco CallManager"/>

### ISDN Network-Specific Facilities Information Element

Network Service Protocol	<input type="text" value="-- Not Selected --"/>	
Carrier Identification Code	<input type="text"/>	
Network Service	Service Parameter Name	Service Parameter Value
<input type="text" value="-- Not Selected --"/>	<input type="text" value="&lt; Not Exist &gt;"/>	<input type="text"/>

The CUCM 11.0 configuration is now complete.

## Test Plan & Results

### Test Plan

The testing was done with SIP/TCP and RTP and was performed by tekVizion.

The test plan consisted of the following test cases. All tests passed.

External ID	Title	Status	Comments
		(Pass or Fail)	
<b>Inbound / Outbound / Extension Dialing</b>			
1	Avaya 6.3 calls Avaya 7.0 using extension dialing	Pass	
2	Avaya 6.3 calls Avaya 7.0 using 10 digit dialing	Pass	
3	Avaya 6.3 calls Avaya 7.0 using PSTN dialing	Pass	
4	Avaya 6.3 calls Cisco 10.5 using extension dialing	Pass	
5	Avaya 6.3 calls Cisco 10.5 using 10 digit dialing	Pass	
6	Avaya 6.3 calls Cisco 10.5 using PSTN dialing	Pass	
7	Avaya 6.3 calls Cisco 11.0 using extension dialing	Pass	
8	Avaya 6.3 calls Cisco 11.0 using 10 digit dialing	Pass	
9	Avaya 6.3 calls Cisco 11.0 using PSTN dialing	Pass	
10	Avaya 6.3 calls Microsoft Lync 2013 using extension dialing	Pass	
11	Avaya 6.3 calls Microsoft Lync 2013 using 10 digit dialing	Pass	
12	Avaya 6.3 calls Microsoft Lync 2013 using PSTN dialing	Pass	
13	Avaya 6.3 calls Skype for Business using extension dialing	Pass	
14	Avaya 6.3 calls Skype for Business using 10 digit dialing	Pass	
15	Avaya 6.3 calls Skype for Business using PSTN dialing	Pass	
16	Avaya 7.0 calls Avaya 6.3 using extension dialing	Pass	
17	Avaya 7.0 calls Avaya 6.3 using 10 digit dialing	Pass	
18	Avaya 7.0 calls Avaya 6.3 using PSTN dialing	Pass	
19	Avaya 7.0 calls Cisco 10.5 using extension dialing	Pass	
20	Avaya 7.0 calls Cisco 10.5 using 10 digit dialing	Pass	

21	Avaya 7.0 calls Cisco 10.5 using PSTN dialing	Pass	
22	Avaya 7.0 calls Cisco 11.0 using extension dialing	Pass	
23	Avaya 7.0 calls Cisco 11.0 using 10 digit dialing	Pass	
24	Avaya 7.0 calls Cisco 11.0 using PSTN dialing	Pass	
25	Avaya 7.0 calls Microsoft Lync 2013 using extension dialing	Pass	
26	Avaya 7.0 calls Microsoft Lync 2013 using 10 digit dialing	Pass	
27	Avaya 7.0 calls Microsoft Lync 2013 using PSTN dialing	Pass	
28	Avaya 7.0 calls Skype for Business using extension dialing	Pass	
29	Avaya 7.0 calls Skype for Business using 10 digit dialing	Pass	
30	Avaya 7.0 calls Skype for Business using PSTN dialing	Pass	
31	Cisco 10.5 calls Avaya 6.3 using extension dialing	Pass	
32	Cisco 10.5 calls Avaya 6.3 using 10 digit dialing	Pass	
33	Cisco 10.5 calls Avaya 6.3 using PSTN dialing	Pass	
34	Cisco 10.5 calls Avaya 7.0 using extension dialing	Pass	
35	Cisco 10.5 calls Avaya 7.0 using 10 digit dialing	Pass	
36	Cisco 10.5 calls Avaya 7.0 using PSTN dialing	Pass	
37	Cisco 10.5 calls Cisco 11.0 using extension dialing	Pass	
38	Cisco 10.5 calls Cisco 11.0 using 10 digit dialing	Pass	
39	Cisco 10.5 calls Cisco 11.0 using PSTN dialing	Pass	
40	Cisco 10.5 calls Microsoft Lync 2013 using extension	Pass	
41	Cisco 10.5 calls Microsoft Lync 2013 using 10 digit dialing	Pass	
42	Cisco 10.5 calls Microsoft Lync 2013 using PSTN dialing	Pass	
43	Cisco 10.5 calls Skype for Business using extension dialing	Pass	
44	Cisco 10.5 calls Skype for Business using 10 digit dialing	Pass	
45	Cisco 10.5 calls Skype for Business using PSTN dialing	Pass	
46	Cisco 11.0 calls Avaya 6.3 using extension dialing	Pass	
47	Cisco 11.0 calls Avaya 6.3 using 10 digit dialing	Pass	
48	Cisco 11.0 calls Avaya 6.3 using	Pass	

	PSTN dialing		
49	Cisco 11.0 calls Avaya 7.0 using extension dialing	Pass	
50	Cisco 11.0 calls Avaya 7.0 using 10 digit dialing	Pass	
51	Cisco 11.0 calls Avaya 7.0 using PSTN dialing	Pass	
52	Cisco 11.0 calls Cisco 10.5 using extension dialing	Pass	
53	Cisco 11.0 calls Cisco 10.5 using 10 digit dialing	Pass	
54	Cisco 11.0 calls Cisco 10.5 using PSTN dialing	Pass	
55	Cisco 11.0 calls Microsoft Lync 2013 using extension dialing	Pass	
56	Cisco 11.0 calls Microsoft Lync 2013 using 10 digit dialing	Pass	
57	Cisco 11.0 calls Microsoft Lync 2013 using PSTN dialing	Pass	
58	Cisco 11.0 calls Skype for Business using extension dialing	Pass	
59	Cisco 11.0 calls Skype for Business using 10 digit dialing	Pass	
60	Cisco 11.0 calls Skype for Business using PSTN dialing	Pass	
61	Microsoft Lync 2013 calls Avaya 6.3 using extension dialing	Pass	
62	Microsoft Lync 2013 calls Avaya 6.3 using 10 digit dialing	Pass	
63	Microsoft Lync 2013 calls Avaya 6.3 using PSTN dialing	Pass	
64	Microsoft Lync 2013 calls Avaya 7.0 using extension dialing	Pass	
65	Microsoft Lync 2013 calls Avaya 7.0 using 10 digit dialing	Pass	
66	Microsoft Lync 2013 calls Avaya 7.0 using PSTN dialing	Pass	
67	Microsoft Lync 2013 calls Cisco 10.5 using extension dialing	Pass	
68	Microsoft Lync 2013 calls Cisco 10.5 using 10 digit dialing	Pass	
69	Microsoft Lync 2013 calls Cisco 10.5 using PSTN dialing	Pass	
70	Microsoft Lync 2013 calls Cisco 11.0 using extension dialing	Pass	
71	Microsoft Lync 2013 calls Cisco 11.0 using 10 digit dialing	Pass	
72	Microsoft Lync 2013 calls Cisco 11.0 using PSTN dialing	Pass	
73	Microsoft Lync 2013 calls Skype for Business using extension dialing	Pass	
74	Microsoft Lync 2013 calls Skype for Business using 10 digit dialing	Pass	

75	Microsoft Lync 2013 calls Skype for Business using PSTN dialing	Pass	
76	Skype for Business calls Avaya 6.3 using extension dialing	Pass	
77	Skype for Business calls Avaya 6.3 using 10 digit dialing	Pass	
78	Skype for Business calls Avaya 6.3 using PSTN dialing	Pass	
79	Skype for Business calls Avaya 7.0 using extension dialing	Pass	
80	Skype for Business calls Avaya 7.0 using 10 digit dialing	Pass	
81	Skype for Business calls Avaya 7.0 using PSTN dialing	Pass	
82	Skype for Business calls Cisco 10.5 using extension dialing	Pass	
83	Skype for Business calls Cisco 10.5 using 10 digit dialing	Pass	
84	Skype for Business calls Cisco 10.5 using PSTN dialing	Pass	
85	Skype for Business calls Cisco 11.0 using extension dialing	Pass	
86	Skype for Business calls Cisco 11.0 using 10 digit dialing	Pass	
87	Skype for Business calls Cisco 11.0 using PSTN dialing	Pass	
88	Skype for Business calls Microsoft Lync 2013 using extension dialing	Pass	
89	Skype for Business calls Microsoft Lync 2013 using 10 digit dialing	Pass	
90	Skype for Business calls Microsoft Lync 2013 using PSTN dialing	Pass	
<b>Transfer Functionality</b>			
91	PSTN calls into Avaya 6.3 and transfers to Avaya 7.0 using 10 digit dialing	Pass	
92	PSTN calls into Avaya 6.3 and transfers to Avaya 7.0 using extension dialing	Pass	
93	PSTN calls into Avaya 6.3 and transfers to Cisco 10.5 using 10 digit dialing	Pass	
94	PSTN calls into Avaya 6.3 and transfers to Cisco 10.5 using extension dialing	Pass	
95	PSTN calls into Avaya 6.3 and transfers to Cisco 11.0 using 10 digit dialing	Pass	
96	PSTN calls into Avaya 6.3 and transfers to Cisco 11.0 using extension dialing	Pass	
97	PSTN calls into Avaya 6.3 and transfers to Microsoft Lync 2013 using 10 digit dialing	Pass	The transfer was successful but the calling number displayed on Lync client is of Avaya phone and not the original PSTN party



98	PSTN calls into Avaya 6.3 and transfers to Microsoft Lync 2013 using extension dialing	Pass	The transfer was successful but the calling number displayed on Lync client is of Avaya phone and not the original PSTN party
99	PSTN calls into Avaya 6.3 and transfers to Skype for Business using 10 digit dialing	Pass	The transfer was successful but the calling number displayed on Skype for Business client is of Avaya phone and not the Original PSTN party
100	PSTN calls into Avaya 6.3 and transfers to Skype for Business using extension dialing	Pass	The transfer was successful but the calling number displayed on Skype for Business client is of Avaya phone and not the original PSTN party
101	PSTN calls into Avaya 7.0 and transfers to Avaya 6.3 using 10 digit dialing	Pass	
102	PSTN calls into Avaya 7.0 and transfers to Avaya 6.3 using extension dialing	Pass	
103	PSTN calls into Avaya 7.0 and transfers to Cisco 10.5 using 10 digit dialing	Pass	
104	PSTN calls into Avaya 7.0 and transfers to Cisco 10.5 using extension dialing	Pass	
105	PSTN calls into Avaya 7.0 and transfers to Cisco 11.0 using 10 digit dialing	Pass	
106	PSTN calls into Avaya 7.0 and transfers to Cisco 11.0 using extension dialing	Pass	
107	PSTN calls into Avaya 7.0 and transfers to Microsoft Lync 2013 using 10 digit dialing	Pass	The transfer was successful but the calling number displayed on Lync client is of Avaya phone and not the original PSTN party
108	PSTN calls into Avaya 7.0 and transfers to Microsoft Lync 2013 using extension dialing	Pass	The transfer was successful but the calling number displayed on Lync Client is of Avaya phone and not the Original PSTN party
109	PSTN calls into Avaya 7.0 and transfers to Skype for Business using 10 digit dialing	Pass	The transfer was successful but the calling number displayed on Skype for Business client is of Avaya phone and not the original PSTN party
110	PSTN calls into Avaya 7.0 and transfers to Skype for Business using extension dialing	Pass	The transfer was successful but the calling number displayed on Skype for Business client is of Avaya phone and not the original PSTN party
111	PSTN calls into Cisco 10.5 and transfers to Avaya 6.3 using 10 digit dialing	Pass	
112	PSTN calls into Cisco 10.5 and transfers to Avaya 6.3 using extension dialing	Pass	
113	PSTN calls into Cisco 10.5 and transfers to Avaya 7.0 using 10 digit dialing	Pass	The transfer was successful but the calling number displayed on Avaya phone is of Cisco phone and not the original PSTN party. To resolve this HMR is added in ECB to add PAI to the UPDATE header

114	PSTN calls into Cisco 10.5 and transfers to Avaya 7.0 using extension dialing	Pass	The transfer was successful but the calling number displayed on Avaya phone is of Cisco phone and not the original PSTN party. To resolve this HMR is added in ECB to add PAI to the UPDATE header
115	PSTN calls into Cisco 10.5 and transfers to Cisco 11.0 using 10 digit dialing	Pass	The transfer was successful but the calling number displayed on the second PSTN party is of Cisco 10.5 phone and not the original PSTN party
116	PSTN calls into Cisco 10.5 and transfers to Cisco 11.0 using extension dialing	Pass	The transfer was successful but the calling number displayed on the second PSTN party is of Cisco 10.5 phone and not the original PSTN party
117	PSTN calls into Cisco 10.5 and transfers to Microsoft Lync 2013 using 10 digit dialing	Pass	The transfer was successful but the calling number displayed on Lync client is of Cisco phone and not the original PSTN party
118	PSTN calls into Cisco 10.5 and transfers to Microsoft Lync 2013 using extension dialing	Pass	The transfer was successful but the calling number displayed on Lync client is of Cisco phone and not the original PSTN party
119	PSTN calls into Cisco 10.5 and transfers to Skype for Business using 10 digit dialing	Pass	The transfer was successful but the calling number displayed on Skype for Business client is of Cisco phone and not the original PSTN party
120	PSTN calls into Cisco 10.5 and transfers to Skype for Business using extension dialing	Pass	The transfer was successful but the calling number displayed on Skype for Business client is of Cisco phone and not the original PSTN party
121	PSTN calls into Cisco 11.0 and transfers to Avaya 6.3 using 10 digit dialing	Pass	
122	PSTN calls into Cisco 11.0 and transfers to Avaya 6.3 using extension dialing	Pass	
123	PSTN calls into Cisco 11.0 and transfers to Avaya 7.0 using 10 digit dialing	Pass	The transfer was successful but the calling number displayed on Avaya phone is of Cisco phone and not the original PSTN party. To resolve this HMR is added in ECB to add PAI to the UPDATE header
124	PSTN calls into Cisco 11.0 and transfers to Avaya 7.0 using extension dialing	Pass	The transfer was successful but the calling number displayed on Avaya phone is of Cisco phone and not the original PSTN party. To resolve this HMR is added in ECB to add PAI to the UPDATE header
125	PSTN calls into Cisco 11.0 and transfers to Cisco 10.5 using 10 digit dialing	Pass	The transfer was successful but the calling number displayed on the second PSTN party is of Cisco 11.0 phone and not the original PSTN party
126	PSTN calls into Cisco 11.0 and transfers to Cisco 10.5 using extension dialing	Pass	The transfer was successful but the calling number displayed on the second PSTN party is of Cisco 11.0 phone and not the original PSTN party
127	PSTN calls into Cisco 11.0 and transfers to Microsoft Lync 2013 using 10 digit dialing	Pass	The transfer was successful but the calling number displayed on Lync client is of Cisco phone and not the original PSTN party

128	PSTN calls into Cisco 11.0 and transfers to Microsoft Lync 2013 using extension dialing	Pass	The transfer was successful but the calling number displayed on Lync client is of Cisco phone and not the original PSTN party
129	PSTN calls into Cisco 11.0 and transfers to Skype for Business using 10 digit dialing	Pass	The transfer was successful but the calling number displayed on Skype for Business client is of Cisco phone and not the original PSTN party
130	PSTN calls into Cisco 11.0 and transfers to Skype for Business using extension dialing	Pass	The transfer was successful but the calling number displayed on Skype for Business client is of Cisco phone and not the original PSTN party
131	PSTN calls into Microsoft Lync 2013 and transfers to Avaya 6.3 using 10 digit dialing	Pass	
132	PSTN calls into Microsoft Lync 2013 and transfers to Avaya 6.3 using extension dialing	Pass	
133	PSTN calls into Microsoft Lync 2013 and transfers to Avaya 7.0 using 10 digit dialing	Pass	
134	PSTN calls into Microsoft Lync 2013 and transfers to Avaya 7.0 using extension dialing	Pass	
135	PSTN calls into Microsoft Lync 2013 and transfers to Cisco 10.5 using 10 digit dialing	Pass	
136	PSTN calls into Microsoft Lync 2013 and transfers to Cisco 10.5 using extension dialing	Pass	
137	PSTN calls into Microsoft Lync 2013 and transfers to Cisco 11.0 using 10 digit dialing	Pass	
138	PSTN calls into Microsoft Lync 2013 and transfers to Cisco 11.0 using extension dialing	Pass	
139	PSTN calls into Microsoft Lync 2013 and transfers to Skype for Business using 10 digit dialing	Pass	
140	PSTN calls into Microsoft Lync 2013 and transfers to Skype for Business using extension	Pass	
141	PSTN calls into Skype for Business and transfers to Avaya 6.3 using 10 digit dialing	Pass	
142	PSTN calls into Skype for Business and transfers to Avaya 6.3 using extension dialing	Pass	
143	PSTN calls into Skype for Business and transfers to Avaya 7.0 using 10 digit dialing	Pass	
144	PSTN calls into Skype for Business and transfers to Avaya 7.0 using extension dialing	Pass	
145	PSTN calls into Skype for Business and transfers to Cisco 10.5 using 10 digit dialing	Pass	

146	PSTN calls into Skype for Business and transfers to Cisco 10.5 using extension dialing	Pass	
147	PSTN calls into Skype for Business and transfers to Cisco 11.0 using 10 digit dialing	Pass	
148	PSTN calls into Skype for Business and transfers to Cisco 11.0 using extension dialing	Pass	
149	PSTN calls into Skype for Business and transfers to Microsoft Lync 2013 using 10 digit dialing	Pass	
150	PSTN calls into Skype for Business and transfers to Microsoft Lync 2013 using extension dialing	Pass	
<b>Call Hold / Resume</b>			
151	Avaya 6.3 calls Avaya 7.0 using PSTN dialing and places the call on hold & reconnects	Pass	
152	Avaya 6.3 calls Avaya 7.0 using extension dialing and places the call on hold & reconnects	Pass	
153	Avaya 6.3 calls Cisco 10.5 using PSTN dialing and places the call on hold & reconnects	Pass	
154	Avaya 6.3 calls Cisco 10.5 using extension dialing and places the call on hold & reconnects	Pass	
155	Avaya 6.3 calls Cisco 11.0 using PSTN dialing and places the call on hold & reconnects	Pass	
156	Avaya 6.3 calls Cisco 11.0 using extension dialing and places the call on hold & reconnects	Pass	
157	Avaya 6.3 calls Microsoft Lync 2013 using PSTN dialing and places the call on hold & reconnects	Pass	
158	Avaya 6.3 calls Microsoft Lync 2013 using extension dialing and places the call on hold & reconnects	Pass	
159	Avaya 6.3 calls Skype for Business using PSTN dialing and places the call on hold & reconnects	Pass	
160	Avaya 6.3 calls Skype for Business using extension dialing and places the call on hold & reconnects	Pass	
161	Avaya 7.0 calls Avaya 6.3 using PSTN dialing and places the call on hold & reconnects	Pass	
162	Avaya 7.0 calls Avaya 6.3 using extension dialing and places the call on hold & reconnects	Pass	
163	Avaya 7.0 calls Cisco 10.5 using PSTN dialing and places the call on hold & reconnects	Pass	

164	Avaya 7.0 calls Cisco 10.5 using extension dialing and places the call on hold & reconnects	Pass	
165	Avaya 7.0 calls Cisco 11.0 using PSTN dialing and places the call on hold & reconnects	Pass	
166	Avaya 7.0 calls Cisco 11.0 using extension dialing and places the call on hold & reconnects	Pass	
167	Avaya 7.0 calls Microsoft Lync 2013 using PSTN dialing and places the call on hold & reconnects	Pass	
168	Avaya 7.0 calls Microsoft Lync 2013 using extension dialing and places the call on hold & reconnects	Pass	
169	Avaya 7.0 calls Skype for Business using PSTN dialing and places the call on hold & reconnects	Pass	
170	Avaya 7.0 calls Skype for Business using extension dialing and places the call on hold & reconnects	Pass	
171	Cisco 10.5 calls Avaya 6.3 using PSTN dialing and places the call on hold & reconnects	Pass	
172	Cisco 10.5 calls Avaya 6.3 using extension dialing and places the call on hold & reconnects	Pass	
173	Cisco 10.5 calls Avaya 7.0 using PSTN dialing and places the call on hold & reconnects	Pass	
174	Cisco 10.5 calls Avaya 7.0 using extension dialing and places the call on hold & reconnects	Pass	
175	Cisco 10.5 calls Cisco 11.0 using PSTN dialing and places the call on hold & reconnects	Pass	
176	Cisco 10.5 calls Cisco 11.0 using extension dialing and places the call on hold & reconnects	Pass	
177	Cisco 10.5 calls Microsoft Lync 2013 using PSTN dialing and places the call on hold & reconnects	Pass	The re-invite with SDP sent from the CUCM to resume the call on hold does not support DTMF. Due to this Lync responds with a "488 DTMF not supported" and call is dropped. Issue resolved by adding a HMR in ECB towards Lync to add the DTMF event 101 when the re-invite does not offer it.
178	Cisco 10.5 calls Microsoft Lync 2013 using extension dialing and places the call on hold & reconnects	Pass	The re-invite with SDP sent from the CUCM to resume the call on hold does not support DTMF. Due to this Lync responds with a "488 DTMF not supported" and call is dropped. Issue resolved by adding a HMR in ECB towards Lync to add the DTMF event 101 when the re-invite does not offer it.

179	Cisco 10.5 calls Skype for Business using PSTN dialing and places the call on hold & reconnects	Pass	The re-invite with SDP sent from the CUCM to resume the call on hold does not support DTMF. Due to this Skype for Business responds with a 488 DTMF not supported and call is dropped. Issue resolved by adding a HMR in ECB towards Skype for Business to add the DTMF event 101 when the re-invite does not offer it.
180	Cisco 10.5 calls Skype for Business using extension dialing and places the call on hold & reconnects	Pass	The re-invite with SDP sent from the CUCM to resume the call on hold does not support DTMF. Due to this Skype for Business responds with a 488 DTMF not supported and call is dropped. Issue resolved by adding a HMR in ECB towards Skype for Business to add the DTMF event when the re-invite does not offer it.
181	Cisco 11.0 calls Avaya 6.3 using PSTN dialing and places the call on hold & reconnects	Pass	
182	Cisco 11.0 calls Avaya 6.3 using extension dialing and places the call on hold & reconnects	Pass	
183	Cisco 11.0 calls Avaya 7.0 using PSTN dialing and places the call on hold & reconnects	Pass	
184	Cisco 11.0 calls Avaya 7.0 using extension dialing and places the call on hold & reconnects	Pass	
185	Cisco 11.0 calls Cisco 10.5 using PSTN dialing and places the call on hold & reconnects	Pass	
186	Cisco 11.0 calls Cisco 10.5 using extension dialing and places the call on hold & reconnects	Pass	
187	Cisco 11.0 calls Microsoft Lync 2013 using PSTN dialing and places the call on hold & reconnects	Pass	The re-invite with SDP sent from the CUCM to resume the call on hold does not support DTMF. Due to this Lync responds with a "488 DTMF not supported" and call is dropped. Issue resolved by adding a HMR in ECB towards Lync to add the DTMF event 101 when the re-invite does not offer it.
188	Cisco 11.0 calls Microsoft Lync 2013 using extension and places the call on hold & reconnects	Pass	The re-invite with SDP sent from the CUCM to resume the call on hold does not support DTMF. Due to this Lync responds with a "488 DTMF not supported" and call is dropped. Issue resolved by adding a HMR in ECB towards Lync to add the DTMF event 101 when the re-invite does not offer it.

189	Cisco 11.0 calls Skype for Business using PSTN dialing and places the call on hold & reconnects	Pass	The re-invite with SDP sent from the CUCM to resume the call on hold does not support DTMF. Due to this Skype for Business responds with a “488 DTMF not supported” and call is dropped. Issue resolved by adding a HMR in ECB towards Skype for Business to add the DTMF event 101 when the re-invite does not offer it.
190	Cisco 11.0 calls Skype for Business using extension dialing and places the call on hold & reconnects	Pass	The re-invite with SDP sent from the CUCM to resume the call on hold does not support DTMF. Due to this Skype for Business responds with a “488 DTMF not supported” and call is dropped. Issue resolved by adding a HMR in ECB towards Skype for Business to add the DTMF event 101 when the re-invite does not offer it.
191	Microsoft Lync 2013 calls Avaya 6.3 using PSTN dialing and places the call on hold & reconnects	Pass	
192	Microsoft Lync 2013 calls Avaya 6.3 using extension dialing and places the call on hold & reconnects	Pass	
193	Microsoft Lync 2013 calls Avaya 7.0 using PSTN dialing and places the call on hold & reconnects	Pass	
194	Microsoft Lync 2013 calls Avaya 7.0 using extension dialing and places the call on hold & reconnects	Pass	
195	Microsoft Lync 2013 calls Cisco 10.5 using PSTN dialing and places the call on hold & reconnects	Pass	
196	Microsoft Lync 2013 calls Cisco 10.5 using extension dialing and places the call on hold & reconnects	Pass	
197	Microsoft Lync 2013 calls Cisco 11.0 using PSTN dialing and places the call on hold & reconnects	Pass	
198	Microsoft Lync 2013 calls Cisco 11.0 using extension dialing and places the call on hold & reconnects	Pass	
199	Microsoft Lync 2013 calls Skype for Business using PSTN dialing and places the call on hold & reconnects	Pass	
200	Microsoft Lync 2013 calls Skype for Business using extension dialing and places the call on hold & reconnects	Pass	
201	Skype for Business calls Avaya 6.3 using PSTN dialing and places the call on hold & reconnects	Pass	
202	Skype for Business calls Avaya 6.3 using extension dialing and places the call on hold & reconnects	Pass	
203	Skype for Business calls Avaya 7.0 using PSTN dialing and places the call on hold & reconnects	Pass	

204	Skype for Business calls Avaya 7.0 using extension dialing and places the call on hold & reconnects	Pass	
205	Skype for Business calls Cisco 10.5 using PSTN dialing and places the call on hold & reconnects	Pass	
206	Skype for Business calls Cisco 10.5 using extension dialing and places the call on hold & reconnects	Pass	
207	Skype for Business calls Cisco 11.0 using PSTN dialing and places the call on hold & reconnects	Pass	
208	Skype for Business calls Cisco 11.0 using extension dialing and places the call on hold & reconnects	Pass	
209	Skype for Business calls Microsoft Lync 2013 using PSTN dialing and places the call on hold & reconnects	Pass	
210	Skype for Business calls Microsoft Lync 2013 using extension dialing and places the call on hold & reconnects	Pass	



<b>Parallel Forking w/ LDAP Integration</b>			
211	Avaya 6.3 calls a user (via 10-digit dial) which is configured on both Cisco 10.5 and Lync 2013. Both Cisco 10.5 and Lync 2013 instances should ring in parallel and either can be answered.	Pass	Ring back is not heard on Avaya during this test case execution. Added a HMR in ECB to convert "183 with SDP" from Lync to "180 RINGING with SDP" to produce the ring back.
212	Avaya 6.3 calls a user (via extension dial) which is configured on both Cisco 10.5 and Lync 2013. Both Cisco 10.5 and Lync 2013 instances should ring in parallel and either can be answered.	Pass	Ring back is not heard on Avaya during this test case execution. Added a HMR in ECB to convert "183 with SDP" from Lync to "180 RINGING with SDP" to produce the ring back.
213	Avaya 6.3 calls a user (via 10 digit dial) which is configured on both Cisco 10.5 and Lync 2013. Both Cisco 10.5 and Lync 2013 instances should ring in parallel and either can be answered.	Pass	Ring back is not heard on Avaya during this test case execution. Added a HMR in ECB to convert "183 with SDP" from Lync to "180 RINGING with SDP" to produce the ring back.
214	Avaya 6.3 calls a user (via extension dial) which is configured on both Cisco 10.5 and Lync 2013. Both Cisco 10.5 and Lync 2013 instances should ring in parallel and either can be answered.	Pass	Ring back is not heard on Avaya during this test case execution. Added a HMR in ECB to convert "183 with SDP" from Lync to "180 RINGING with SDP" to produce the ring back.
215	Avaya 7.0 calls a user (via 10-digit dial) which is configured on both Cisco 11.0 and Skype for Business. Both Cisco 11.0 and Skype for Business instances should ring in parallel and either can be answered.	Pass	
216	Avaya 7.0 calls a user (via extension dial) which is configured on both Cisco 11.0 and Skype for Business. Both Cisco 11.0 and Skype for Business instances should ring in parallel and either can be answered.	Pass	
217	Avaya 7.0 calls a user (via 10 digit dial) which is configured on both Cisco 11.0 and Skype for Business. Both Cisco 11.0 and Skype for Business instances should ring in parallel and the call is unanswered and forwarded to voice mail	Pass	
218	Avaya 7.0 calls a user (via extension dial) which is configured on both Cisco 11.0 and Skype for Business. Both Cisco 11.0 and Skype for Business instances should ring in parallel and either can be answered.	Pass	
<b>Serial Forking w/ LDAP Integration</b>			
219	Avaya 6.3 calls a user (via 10 digit dial) which is configured on both	Pass	

	Cisco 10.5 and Lync 2013. Both Cisco 10.5 and Lync 2013 instances should ring in Serially and either can be answered.		
220	Avaya 6.3 calls a user (via extension dial) which is configured on both Cisco 10.5 and Lync 2013. Both Cisco 10.5 and Lync 2013 instances should ring in serially .This call is unanswered and forwarded to Voice Mail	Pass	
221	Avaya 6.3 calls a user (via 10 digit dial) which is configured on both Cisco 10.5 and Lync 2013. Both Cisco 10.5 and Lync 2013 instances should ring in serially and either can be answered.	Pass	
222	Avaya 6.3 calls a user (via extension dial) which is configured on both Cisco 10.5 and Lync 2013. Both Cisco 10.5 and Lync 2013 instances should ring in serially and either can be answered.	Pass	
223	Avaya 7.0 calls a user (via 10 digit dial) which is configured on both Cisco 11.0 and Skype for Business. Both Cisco 11.0 and Skype for Business instances should ring in serially and either can be answered.	Pass	
224	Avaya 7.0 calls a user (via extension dial) which is configured on both Cisco 11.0 and Skype for Business. Both Cisco 11.0 and Skype for Business instances should ring in serially and either can be answered.	Pass	
225	Avaya 7.0 calls a user (via 10 digit dial) which is configured on both Cisco 11.0 and Skype for Business. Both Cisco 11.0 and Skype for Business instances should ring in serially and either can be answered.	Pass	
226	Avaya 7.0 calls a user (via extension dial) which is configured on both Cisco 11.0 and Skype for Business. Both Cisco 11.0 and Skype for Business instances should ring in serially and either can be answered.	Pass	
<b>From Header Replacement w/ Active Directory</b>			
227	User A (x4444) configured in ECB for endpoints on cisco 10.5 and Lync 2013. Call is initiated from Avaya 6.3 system to x4444. Result = both endpoints ring and display CID on cisco 10.5 and Lync 2013 end points.	Pass	

228	Call initiated by Avaya 6.3 and calls User A (x4444) with full 10 digit number (312-777-4444). User A configured in ECB for endpoints on Cisco 10.5 and Lync 2013. Result = Both endpoints ring and display CID on Cisco 10.5 and Lync 2013 endpoints.	Pass	
229	User A (x4444) configured in ECB for endpoints on Cisco 10.5 and Lync 2013. Call is initiated from Avaya 6.3 system to x4444. Result = both endpoints ring and display CID on Cisco 10.5 and Lync 2013 end points.	Pass	
230	Call initiated by Avaya 6.3 and calls User A (x4444) with full 10 digit number (312-777-4444). User A configured in ECB for endpoints on Cisco 10.5 and Lync 2013. Result = Both endpoints ring and display CID on Cisco 10.5 and Lync 2013 endpoints.	Pass	
231	User A (x5555) configured in ECB for endpoints on Cisco 11.0 and Skype for Business. Call is initiated from Avaya 7.0 system to x5555. Result = both endpoints ring and display CID on Cisco 11.0 and Skype for Business end points.	Pass	
232	Call initiated by Avaya 7.0 and calls User A (x5555) with full 10 digit number (312-777-5555). Both endpoints ring and display CID on Cisco 11.0 and Skype for Business endpoints.	Pass	
233	User A (x5555) configured in ECB for endpoints on Cisco 11.0 and Skype for Business. Call is initiated from Avaya 7.0 system to x5555. Result = both endpoints ring and display CID on Cisco 11.0 and Skype for Business end points.	Pass	
234	Call initiated by Avaya 7.0 and calls User A (x5555) with full 10 digit number (312-777-5555). Both endpoints ring and display CID on Cisco 11.0 and Skype for Business endpoints.	Pass	
235	User A (x4444) configured in ECB for endpoints on Cisco 10.5 and Lync 2013. Call is initiated from Cisco 10.5 system to x4444. Result = both endpoints ring and display CID on Cisco 10.5 and Lync 2013	Pass	Call does not reach the ECB since the extension dialed belongs to the PBX from which the call is originated. To route the call towards ECB a separate route pattern in CUCM is required (ex: 9.XXXX)

	endpoints.		
236	Call initiated by Cisco 10.5 and calls User A (x4444) with full 10 digit number (312-777-4444). User A configured in ECB for endpoints on Cisco 10.5 and Lync 2013. Result = Both endpoints ring and display CID on Cisco 10.5 and Lync 2013 endpoints.	Pass	Call does not reach the ECB since the extension dialed belongs to the PBX from which the call is originated. To route the call towards ECB a separate route pattern in CUCM is required (ex: 9.312777XXXX).
237	User A (x4444) configured in ECB for endpoints on Cisco 10.5 and Lync 2013. Call is initiated from Cisco 10.5 system to x4444. Result = both endpoints ring and display CID on Cisco 10.5 and Lync 2013 endpoints.	Pass	Call does not reach the ECB since the extension dialed belongs to the PBX from which the call is originated. To route the call towards ECB a separate route pattern in CUCM is required (ex: 9.XXXX)
238	Call initiated by Cisco 10.5 and calls User A (x4444) with full 10 digit number (312-777-4444). User A configured in ECB for endpoints on Cisco 10.5 and Lync 2013. Result = Both endpoints ring and display CID on Cisco 10.5 and Lync 2013 endpoints.	Pass	Call does not reach the ECB since the extension dialed belongs to the PBX from which the call is originated. To route the call towards ECB a separate route pattern in CUCM is required (ex: 9.312777XXXX).
239	User A (x5555) configured in ECB for endpoints on Cisco 11.0 and Skype for Business. Call is initiated from Cisco 11.0 system to x5555. Result = both endpoints ring and display CID on Cisco 11.0 and Skype for Business end points.	Pass	Call does not reach the ECB since the extension dialed belongs to the PBX from which the call is originated. To route the call towards ECB a separate route pattern in CUCM is required (ex: 9.XXXX)
240	Call initiated by Cisco 11.0 and calls User A (x5555) with full 10 digit number (312-777-5555). Both endpoints ring and display CID on Cisco 11.0 and Skype for Business endpoints.	Pass	Call does not reach the ECB since the extension dialed belongs to the PBX from which the call is originated. To route the call towards ECB a separate route pattern in CUCM is required (ex: 9.312777XXXX).
241	User A (x5555) configured in ECB for endpoints on Cisco 11.0 and Skype for Business. Call is initiated from Cisco 11.0 system to x5555. Result = both endpoints ring and display CID on Cisco 11.0 and Skype for Business end points.	Pass	Call does not reach the ECB since the extension dialed belongs to the PBX from which the call is originated. To route the call towards ECB a separate route pattern in CUCM is required (ex: 9.XXXX)
242	Call initiated by Cisco 11.0 and calls User A (x5555) with full 10 digit number (312-777-5555). Both endpoints ring and display CID on Cisco 11.0 and Skype for Business endpoints.	Pass	Call does not reach the ECB since the extension dialed belongs to the PBX from which the call is originated. To route the call towards ECB a separate route pattern in CUCM is required (ex: 9.312777XXXX).

243	User A (x4444) configured in ECB for endpoints on Cisco 10.5 and Lync 2013. Call is initiated from Lync 2013 system to x4444. Result = both endpoints ring and display CID on Cisco 10.5 and Lync 2013 endpoints.	Pass	
244	Call initiated by Lync 2013 and calls User A (x4444) with full 10 digit number (312-777-4444). User A configured in ECB for endpoints on Cisco 10.5 and Lync 2013. Result = Both endpoints ring and display CID on Cisco 10.5 and Lync 2013 endpoints.	Pass	Call does not reach the ECB since the extension dialed belongs to the PBX from which the call is originated. To route the call towards ECB a separate route in Lync is required (ex: 9.312777XXXX).
245	User A (x4444) configured in ECB for endpoints on Cisco 10.5 and Lync 2013. Call is initiated from Lync 2013 system to x4444. Result = both endpoints ring and display CID on Cisco 10.5 and Lync 2013 endpoints.	Pass	
246	Call initiated by Lync 2013 and calls User A (x4444) with full 10 digit number (312-777-4444). User A configured in ECB for endpoints on Cisco 10.5 and Lync 2013. Result = Both endpoints ring and display CID on Cisco 10.5 and Lync 2013 endpoints.	Pass	Call does not reach the ECB since the extension dialed belongs to the PBX from which the call is originated. To route the call towards ECB a separate route in Lync is required (ex: 9.312777XXXX).
247	User A (x4444) configured in ECB for endpoints on Cisco 11.0 and Skype for Business. Call is initiated from Skype for Business system to x4444. Result = both endpoints ring and display CID on Cisco 11.0 and Skype for Business endpoints.	Pass	
248	Call initiated by Skype for Business and calls User A (x4444) with full 10 digit number (312-777-4444). User A configured in ECB for endpoints on Cisco 11.0 and Skype for Business. Result = Both endpoints ring and display CID on Cisco 11.0 and Skype for Business endpoints.	Pass	Call does not reach the ECB since the extension dialed belongs to the PBX from which the call is originated. To route the call towards ECB a separate route in Skype for Business is required (ex: 9.312777XXXX).
249	User A (x4444) configured in ECB for endpoints on Cisco 11.0 and Skype for Business. Call is initiated from Skype for Business system to x4444. Result = both endpoints ring and display CID on Cisco 11.0 and Skype for Business endpoints.	Pass	

250	Call initiated by Skype for Business and calls User A (x4444) with full 10 digit number (312-777-4444). User A configured in ECB for endpoints on Cisco 11.0 and Skype for Business. Result = Both endpoints ring and display CID on Cisco 11.0 and Skype for Business endpoints.	Pass	Call does not reach the ECB since the extension dialed belongs to the PBX from which the call is originated. To route the call towards ECB a separate route in Skype for Business is required (ex: 9.312777XXXX).
-----	---	------	---

**Active Directory Failover**

(Test querying LDAP and the query failing / falling back to backup LDAP / User DB / Default mode)

251	Cisco 10.5 calls Avaya 6.3	Pass	
252	Cisco 10.5 calls Avaya 7.0	Pass	
253	Cisco 10.5 calls cisco 11.0	Pass	
254	Cisco 10.5 calls Lync 2013	Pass	
255	Cisco 10.5 calls Skype for Business	Pass	
256	Lync 2013 calls Avaya 6.3	Pass	
257	Lync 2013 calls Avaya 7.0	Pass	
258	Lync 2013 calls Cisco 10.5	Pass	
259	Lync 2013 calls Cisco 11.0	Pass	
260	Lync 2013 calls Skype for Business	Pass	

## Software Versions Used

The following are the software versions used in this testing by tekVizion.

Component	Version
ECB	PCZ2.0.0 MR-2 Patch 1 (Build 209)
E-SBC	ECZ7.3.0 MR-1 GA (Build 104)
Microsoft Lync 2013 Server	5.0.8308.0
Microsoft Skype for Business Server 2015	6.0.9319.0
Cisco Unified Communication Manager	10.5.1 & 11.0.1
Avaya Aura	6.3.14 & 7.0.0.1

## Troubleshooting Tools

If you find that you are not able to complete calls or have problems with the test cases, there are a few tools available for Windows Server, Lync/SFB Server, and the Oracle ECB and SBC like logging and tracing which may be of assistance. In this section we will provide a list of tools which you can use to aid in troubleshooting any issues you may encounter.

### Microsoft Network Monitor (NetMon)

NetMon is a network protocol analyzer which is freely downloadable from Microsoft. It can be found at [www.microsoft.com/downloads](http://www.microsoft.com/downloads). NetMon could be installed on the Lync Server mediation server, the Lync Server Standard Edition server, or Enterprise Edition front end server.

### Wireshark

Wireshark is also a network protocol analyzer which is freely downloadable from [www.wireshark.org](http://www.wireshark.org). Wireshark could be installed on the Lync/SFB Server mediation server, the Lync/SFB Server Standard Edition server, or MCS Enterprise Edition front end server.

### Eventviewer

There are several locations in the event viewer where you can find valuable information to aid in troubleshooting issues with your deployment.

With the requirement that there is a completely functioning Lync and/or SFB Server with Enterprise Voice deployment in place, there are only a few areas in which one would use the Event Viewer for troubleshooting:

- The Enterprise Voice client;
- The Lync/SFB Server Front End server;
- A Lync/SFB Server Standard Edition Server; and
- A Lync/SFB Server Mediation Server.

### On the Oracle ECB and E-SBC

The Oracle SBC and ECB provide a rich set of statistical counters available from the CLI, as well as log file output with configurable detail. The follow sections detail enabling, adjusting and accessing those interfaces.

#### Resetting the statistical counters, enabling logging and restarting the log files.

At the console:

```
oraclesbc1# reset sipd
oraclesbc1# notify sipd debug
oraclesbc1#
enabled SIP Debugging
oraclesbc1# notify all rotate-logs
```

#### Examining the log files

**Note:** You will FTP to the management interface of the ECB or SBC with the username user and user mode password (the default is “acme”).

```
C:\Documents and Settings\user>ftp 192.168.5.24
Connected to 192.168.85.55.
220 oraclesbc1FTP server (VxWorks 6.4) ready.
User (192.168.85.55:(none)): user
```



```
331 Password required for user.
Password: acme
230 User user logged in.
ftp> cd /ramdrv/logs
250 CWD command successful.
ftp> get sipmsg.log
200 PORT command successful.
150 Opening ASCII mode data connection for '/ramdrv/logs/sipmsg.log' (3353
bytes).
226 Transfer complete.
ftp: 3447 bytes received in 0.00Seconds 3447000.00Kbytes/sec.
ftp> get log.sipd
200 PORT command successful.
150 Opening ASCII mode data connection for '/ramdrv/logs/log.sipd' (204681
bytes).
226 Transfer complete.
ftp: 206823 bytes received in 0.11Seconds 1897.46Kbytes/sec.
ftp> bye
221 Goodbye.
```

You may now examine the log files with the text editor of your choice.

#### Through the Web GUI

You can also check the display results of filtered SIP session data from the Oracle E-SBC and ECB, and provide traces in a common log format for local viewing or for exporting to your PC. Please check the “Monitor and Trace SIP Messages” section (page 140) of the E-SBC Web GUI User Guide available at [http://docs.oracle.com/cd/E56581\\_01/index.htm](http://docs.oracle.com/cd/E56581_01/index.htm). For the ECB, see the “Monitor and Trace” section (page 95) of the User’s Guide available at [http://docs.oracle.com/cd/E55725\\_01/index.htm](http://docs.oracle.com/cd/E55725_01/index.htm).

#### Telnet

Since we are working within an architecture which uses bound TCP listening ports for functionality, the simplest form of troubleshooting can be seeing if the devices are listening on a particular port, as well as confirming that there is nothing blocking them such as firewalls. Ensure that you have a TELNET client available on a workstation.

All devices tested in this document will listen on TCP port 5060 for SIP signaling. In our example we are listening on 5060 on the PSTN facing NIC. Tests may include:

- Client to pool server: `telnet <servername> 5060`
- Pool server to Mediation Server: `telnet <servername> 5060`

#### Cisco Real-Time Monitoring Tool (RTMT)

The Cisco Real-Time Monitoring Tool (RTMT) is a tool that can be downloaded from CUCM to a Windows or Linux computer. See <https://supportforums.cisco.com/document/93281/using-rtmt-monitor-cisco-unity-connection-and-cucm> for details.

# Appendix A

## Accessing the ACLI

Access to the ACLI is provided by:

- The serial console connection;
- TELNET, which is enabled by default but may be disabled; and
- SSH.

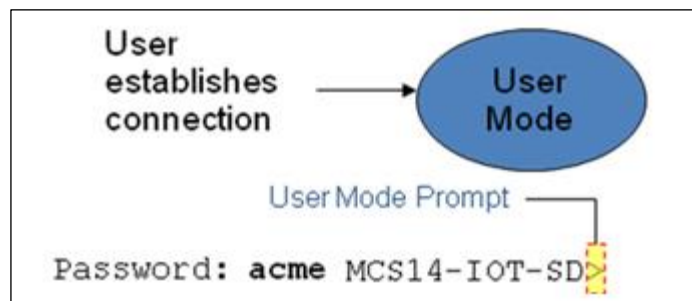
Initial connectivity will be through the serial console port. At a minimum, this is how to configure the management (eth0) interface on the SBC.

## ACLI Basics

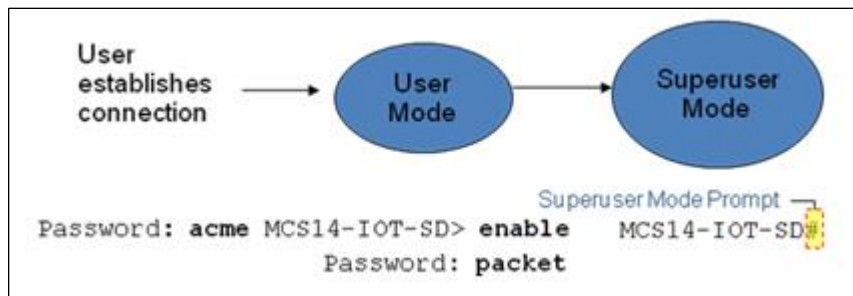
There are two password protected modes of operation within the ACLI, User mode and Superuser mode.

When you establish a connection to the SBC, the prompt for the User mode password appears. The default password is acme.

User mode consists of a restricted set of basic monitoring commands and is identified by the greater than sign (>) in the system prompt after the target name. You cannot perform configuration and maintenance from this mode.



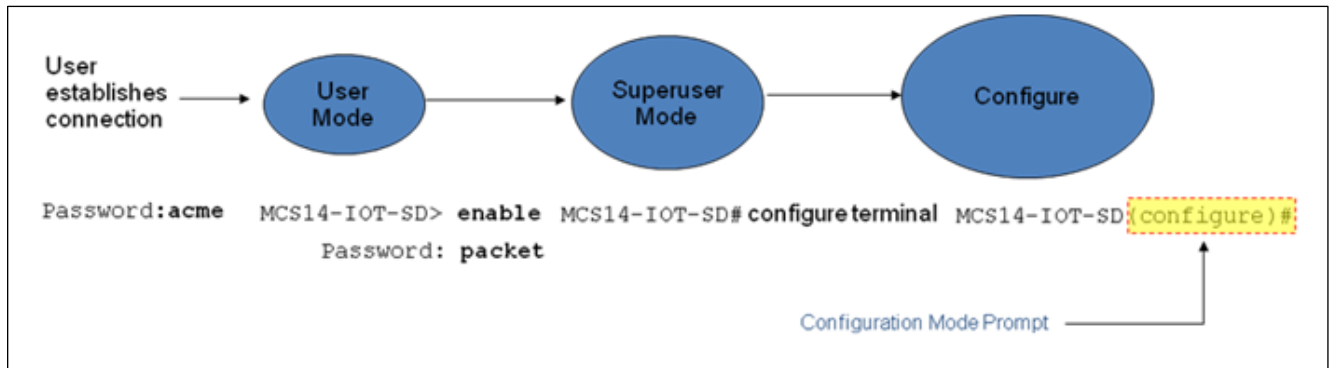
The Superuser mode allows for access to all system commands for operation, maintenance, and administration. This mode is identified by the pound sign (#) in the prompt after the target name. To enter the Superuser mode, issue the enable command in the User mode.



From the Superuser mode, you can perform monitoring and administrative tasks; however you cannot configure any elements. To return to User mode, issue the exit command.

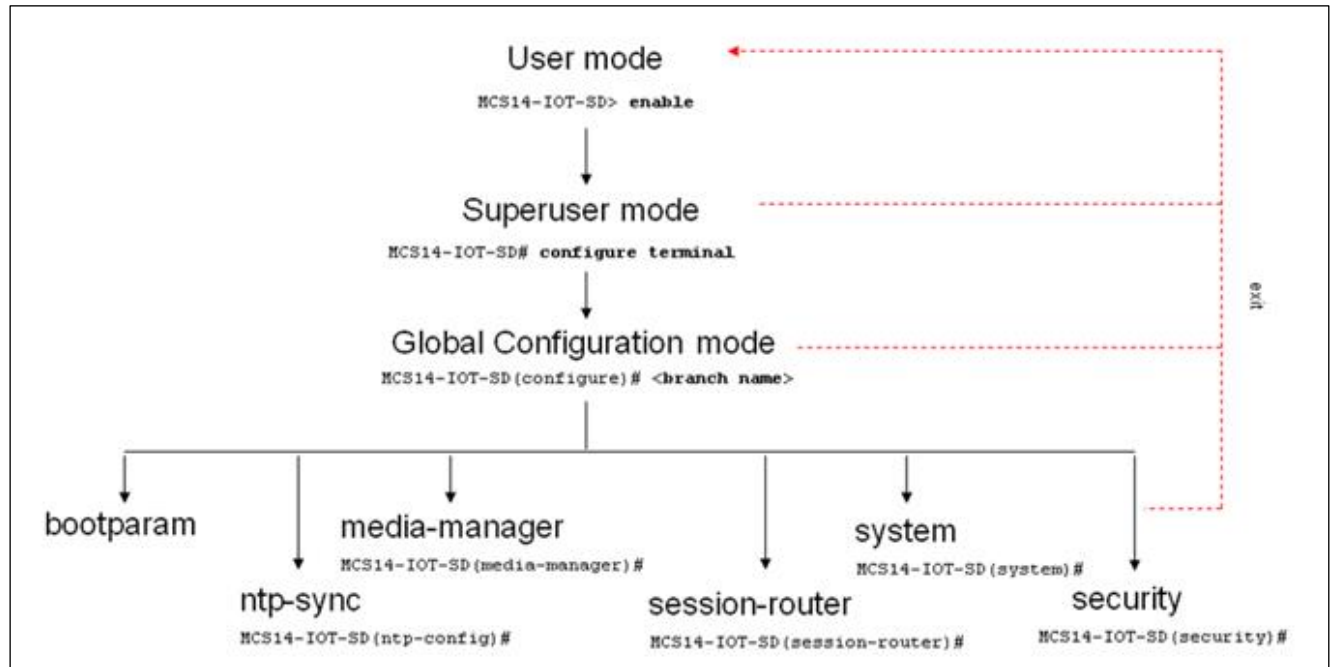
You must enter the Configuration mode to configure elements. For example, you can access the configuration branches and configuration elements for signaling and media configurations. To enter the Configuration mode, issue the `configure terminal` command in the Superuser mode.

Configuration mode is identified by the word configure in parenthesis followed by the pound sign (#) in the prompt after the target name, for example, `oraclesbc1(configure)#`. To return to the Superuser mode, issue the `exit` command.



In the configuration mode, there are six configuration branches:

- bootparam;
- ntp-sync;
- media-manager;
- session-router;
- system; and
- security.



The ntp-sync and bootparams branches are flat branches (i.e., they do not have elements inside the branches). The rest of the branches have several elements under each of the branches.

The bootparam branch provides access to SBC boot parameters.

The ntp-sync branch provides access to ntp server configuration commands for synchronizing the SBC time and date.

The security branch provides access to security configuration.

The system branch provides access to basic configuration elements as system-config, snmp-community, redundancy, physical interfaces, network interfaces, etc.

The session-router branch provides access to signaling and routing related elements, including H323-config, sip-config, ivf-config, local-policy, sip-manipulation, session-agent, etc.

The media-manager branch provides access to media-related elements, including realms, steering pools, dns-config, media-manager, and so forth.

You will use media-manager, session-router, and system branches for most of your working configuration.

## Configuration Elements

The configuration branches contain the configuration elements. Each configurable object is referred to as an element. Each element consists of a number of configurable parameters.

Some elements are single-instance elements, meaning that there is only one of that type of the element - for example, the global system configuration and redundancy configuration.

Some elements are multiple-instance elements. There may be one or more of the elements of any given type. For example, physical and network interfaces.

Some elements (both single and multiple instance) have sub-elements. For example:

- SIP-ports - are children of the sip-interface element
- peers – are children of the redundancy element
- destinations – are children of the peer element

## Creating an Element

1. To create a single-instance element, you go to the appropriate level in the ACLI path and enter its parameters. There is no need to specify a unique identifier property because a single-instance element is a global element and there is only one instance of this element.
2. When creating a multiple-instance element, you must specify a unique identifier for each instance of the element.
3. It is important to check the parameters of the element you are configuring before committing the changes. You do this by issuing the **show** command before issuing the **done** command. The parameters that you did not configure are filled with either default values or left empty.
4. On completion, you must issue the **done** command. The done command causes the configuration to be echoed to the screen and commits the changes to the volatile memory. It is a good idea to review this output to ensure that your configurations are correct.
5. Issue the **exit** command to exit the selected element.

Note that the configurations at this point are not permanently saved yet. If the SBC reboots, your configurations will be lost.

## Editing an Element

The procedure of editing an element is similar to creating an element, except that you must select the element that you will edit before editing it.

1. Enter the element that you will edit at the correct level of the ACLI path.
2. Select the element that you will edit, and view it before editing it.  
The **select** command loads the element to the volatile memory for editing. The **show** command allows you to view the element to ensure that it is the right one that you want to edit.
3. Once you are sure that the element you selected is the right one for editing, edit the parameter one by one. The new value you provide will overwrite the old value.

4. It is important to check the properties of the element you are configuring before committing it to the volatile memory. You do this by issuing the `show` command before issuing the `done` command.
5. On completion, you must issue the `done` command.
6. Issue the `exit` command to exit the selected element.

Note that the configurations at this point are not permanently saved yet. If the SBC reboots, your configurations will be lost.

## Deleting an Element

The `no` command deletes an element from the configuration in editing.

To delete a single-instance element,

1. Enter the `no` command from within the path for that specific element
2. Issue the `exit` command.

To delete a multiple-instance element,

1. Enter the `no` command from within the path for that particular element.  
The key field prompt, such as <name>:<sub-port-id>, appears.
2. Use the <Enter> key to display a list of the existing configured elements.
3. Enter the number corresponding to the element you wish to delete.
4. Issue the `select` command to view the list of elements to confirm that the element was removed.

Note that the configuration changes at this point are not permanently saved yet. If the SBC reboots, your configurations will be lost.

## Configuration Versions

At any time, three versions of the configuration can exist on the SBC: the edited configuration, the saved configuration, and the running configuration.

- The **edited configuration** – this is the version that you are making changes to. This version of the configuration is stored in the SBC's volatile memory and will be lost on a reboot.  
To view the editing configuration, issue the `show configuration` command.
- The **saved configuration** – on issuing the `save-config` command, the edited configuration is copied into the non-volatile memory on the SBC and becomes the saved configuration. Because the saved configuration has not been activated yet, the changes in the configuration will not take effect. On reboot, the last activated configuration (i.e., the last running configuration) will be loaded, not the saved configuration.
- The **running configuration** is the saved then activated configuration. On issuing the `activate-config` command, the saved configuration is copied from the non-volatile memory to the volatile memory. The saved configuration is activated and becomes the running configuration. Although most of the configurations can take effect once being activated without reboot, some configurations require a reboot for the changes to take effect.  
To view the running configuration, issue command `show running-config`.

## Saving the Configuration

The `save-config` command stores the edited configuration persistently.

Because the saved configuration has not been activated yet, changes in configuration will not take effect. On reboot, the last activated configuration (i.e., the last running configuration) will be loaded. At this stage, the saved configuration is different from the running configuration.

Because the saved configuration is stored in non-volatile memory, it can be accessed and activated at later time.

Upon issuing the `save-config` command, the SBC displays a reminder on screen stating that you must use the `activate-config` command if you want the configurations to be updated.

```
oraclesbcl # save-config
Save-Config received, processing.
waiting 1200 for request to finish
Request to 'SAVE-CONFIG' has Finished,
Save complete
Currently active and saved configurations do not match!
To sync & activate, run 'activate-config' or 'reboot activate'.
oraclesbcl #
```

## Activating the Configuration





On issuing the **activate-config** command, the saved configuration is copied from the non-volatile memory to the volatile memory. The saved configuration is activated and becomes the running configuration.

Some configuration changes are service affecting when activated. For these configurations, the SBC warns that the change could have an impact on service with the configuration elements that will potentially be service affecting. You may decide whether or not to continue with applying these changes immediately or to apply them at a later time.

```
oraclesbcl# activate-config
Activate-Config received, processing.
waiting 120000 for request to finish
Request to 'ACTIVATE-CONFIG' has Finished,
Activate Complete
oraclesbcl#
```



### CONNECT WITH US

-  [blogs.oracle.com/oracle](https://blogs.oracle.com/oracle)
-  [facebook.com/oracle](https://facebook.com/oracle)
-  [twitter.com/oracle](https://twitter.com/oracle)
-  [oracle.com](https://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 © 2016, 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