

# Oracle® Enterprise Session Border Controller

## Web GUI User Guide



Release E-CZ7.3.0

February 2018

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Copyright © 2014, 2018, Oracle and/or its affiliates. All rights reserved.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

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.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

# Contents

## About This Guide

---

### 1 Getting Started

---

About This Software	1-1
Browser Support	1-2
Internet Protocol Version Support	1-2
Log On and Log Off	1-2
Log On to the Web GUI	1-2
Log Off the Web GUI	1-3
User and Administrator Access Rules	1-3
Simultaneous Logons	1-3
Change the Log On Password	1-4
Radius Server in the Network	1-4
Update the Configuration Schema	1-5
Web GUI Tools	1-6
Shortcut Keys	1-6
Tabs	1-6
Search	1-9
Help	1-10
Customize the Page Display	1-10
Save and Activate Network Configuration	1-11
Configuration Error Messages	1-11
Discard Changes	1-12

### 2 Home Tab

---

Add a Dashboard Widget	2-2
Configure Data Sampling Settings for a Dashboard Widget	2-3
View a Dashboard Widget in Full-Screen Mode	2-3
View Any Widget in Full-Screen Mode	2-3

## 3 Configuration Tab

---

Configuration States and Behavior	3-1
Configuration Error Messages	3-2
Configuration Copying Methods	3-2
Configuration Editing Methods	3-4
Configuration Deletion Methods	3-6
Configuration from the Web GUI	3-8
Wizards Button	3-9
Set Boot Parameters Wizard	3-10
Configurable Boot Loader Flags	3-11
Set Entitlements Wizard	3-11
Set Initial Configuration Wizard	3-11
Set License Wizard	3-13
Set Logon Banner Wizard	3-13
Set Time Zone Wizard	3-13
Upgrade Software Wizard	3-14
Basic Mode Configuration	3-15
Basic Mode Configuration Tools	3-16
Basic Mode Configuration Buttons and Dialogs	3-17
Device Icons Toolbar	3-18
Device Icon Connection Matrix	3-21
Network Configuration Using the Workspace Icons	3-27
Add a PBX	3-27
Add a Trunk	3-28
Add a One-Way Local Routing Policy	3-29
Add a Local Policy	3-30
Configure Advanced Routing	3-32
Configure LDAP	3-33
TDM Configuration	3-34
Settings Button	3-39
Configure System Settings Quick Reference	3-39
Logging Settings	3-41
Configure Logging Settings	3-41
Simple Network Management Protocol	3-42
Configure SNMP Settings	3-42
SIP Settings	3-42
Configure SIP Settings	3-43
Denial of Service Protection	3-44
Configure Denial of Service Settings	3-44
Communication Monitoring Probe Settings	3-45

Configure Communication Monitoring Probe Settings	3-45
High Availability Settings	3-46
High Availability on the Acme Packet 1100	3-47
Configure High Availability	3-47
Configure the Acme Packet 1100 Primary for HA	3-48
Configure the Acme Packet 1100 Secondary for HA	3-49
Packet Capture Settings	3-49
Configure Packet Capture Settings	3-50
Remote Site Survivability	3-50
Configure Remote Site Survivability	3-51
Network Button	3-52
Host Routes	3-52
Add a Host Route	3-52
Network Interface Configuration	3-53
Add a Network Interface	3-53
Security Button	3-55
Management Button	3-55
Configure Call Accounting	3-55
Configure SNMP Community	3-59
Configure an SNMP Trap Receiver	3-60
Web Server Configuration	3-61
Configure a Web Server	3-61
Other Button	3-62
Configure Media Profile	3-62
Configure Translation Rules	3-64
Configure SIP Features	3-65
Configure SIP Manipulations	3-66
Add an SPL	3-97
Expert Mode Configuration	3-98
Expert Mode Configuration tools	3-100
Function Buttons	3-101
Commands Button	3-101
Media Manager Configuration	3-102
Add a Codec Policy	3-102
Configure DNS	3-104
Configure Media Manager	3-105
Configure Media Policy	3-106
Configure Playback	3-107
Configure a Realm	3-108
Configure a Steering Pool	3-111
Security Configuration	3-111

Security Settings	3-112
TACACS+ Authentication	3-113
Certificate Configuration Process	3-114
SDES Configuration for a Media Stream	3-117
TLS Profile Configuration	3-117
Session Router Configuration	3-119
Configure Access Control	3-120
Accounting Configuration	3-122
Configure a Custom Monitor and Trace Filter	3-123
Dynamic ACL for the HTTP-ALG	3-124
Configure IWF	3-127
Configure LDAP	3-128
Configure Local Policy	3-129
Configure Local Routing	3-131
Configure a Session Agent	3-131
SIP hold-refer-reinvite	3-135
Enable hold-refer-reinvite	3-135
Configure a Session Group	3-136
Configure Session Recording Group	3-137
Configure SIP	3-138
Configure SIP Features	3-140
Configure SIP Interface	3-141
Configure SIP Manipulation	3-143
Configure SIP Monitoring	3-144
Remote Site Survivability Configuration	3-145
Configure Translation Rules	3-146
System Configuration	3-147
Configure a Host Route	3-148
Network Interface Configuration - Expert	3-148
Configure NTP	3-152
Physical Interface Configuration - Expert	3-153
High Availability	3-156
SNMP Trap Receiver	3-159
SNMP Community	3-161
Configure an SPL Plugin	3-162
Time Division Multiplexing (TDM)	3-163
Web Server Configuration	3-168

## 4 Monitor and Trace Tab

---

Configure SIP Monitoring	4-1
--------------------------	-----

Monitor and Trace SIP Messages	4-2
Sessions Report	4-3
Display a Sessions Report	4-5
Ladder Diagram	4-5
Display a Ladder Diagram	4-5
Session Summary	4-7
Display the Session Summary	4-7
SIP Message Details	4-8
SIPREC Call Data	4-9
Hairpin Call Data	4-10
SIP Monitor & Trace Ingress Egress Messages	4-11
Display SIP Message Details	4-11
QoS Statistics	4-12
Display QoS Statistics	4-12
Registrations Report	4-13
Display a Registrations Report	4-15
Subscriptions Report	4-15
Display a Subscriptions Report	4-17
Notable Events Report	4-17
Display a Notable Events Report	4-19
Search for a Record	4-19
Perform a Search	4-19
Specify Additional Identifiers	4-21
Specify Additional Search Options	4-22
Exporting Information to a Text File	4-22
Export Report Information to a Text File	4-23

## 5 Widgets Tab

---

Types of Widgets	5-1
Add a Widget to Favorites	5-2

## 6 System Tab

---

File Management	6-1
Manage Files	6-3
Group By Field	6-3
Upload a File	6-3
Download a File	6-5
Delete a File	6-5
Back up a File	6-6

Restore a File	6-7
Force an HA Switch Over	6-7
System Reboot	6-8
Obtain Support Information	6-8
Upgrade Software - Web GUI System Tab	6-8

## 7 Format of Exported Text Files

---

Introduction	7-1
Exporting Files	7-1
Session Summary Exported Text File	7-2
Example	7-2
Session Details Exported Text File	7-3
Example	7-3
Ladder Diagram Exported HTML File	7-8
Example	7-9



# About This Guide

This guide provides information about configuring and administering the Oracle Enterprise Session Border Controller from the Web GUI. The topics in this guide contain conceptual, procedural, and reference information.

## Documentation Set

The following table describes the documents included in the Oracle Enterprise Session Border Controller E-CZ7.3.0 documentation set.

Document Name	Document Description
ACLI Configuration Guide	Contains information about the installation, configuration, and administration of the Enterprise Oracle Enterprise Session Border Controller.
Acme Packet 1100 Hardware Installation Guide	Contains information related to the hardware components, features, installation, start-up, operation, and maintenance of the Acme Packet 1100.
Web GUI Users Guide	Contains information about using the tools and features of the Oracle Enterprise Session Border Controller Web GUI.
Release Notes	Contains information about this release, including platform support, new features, caveats, known issues, and limitations.

## Related Documentation

The following table describes related documentation for the Oracle Communications Session Border Controller.

Document Name	Document Description
Acme Packet 3820 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 3820.
Acme Packet 4500 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4500.
Acme Packet 4600 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4600.
Acme Packet 6300 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6300.

Document Name	Document Description
Release Notes	Contains information about the current documentation set release, including new features and management changes.
ACLI Configuration Guide	Contains information about the administration and software configuration of the Oracle Enterprise Session Border Controller.
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Maintenance and Troubleshooting Guide	Contains information about Oracle Enterprise Session Border Controller logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
MIB Reference Guide	Contains information about Management Information Base (MIBs), Acme Packet's enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Accounting Guide	Contains information about the Oracle Enterprise Session Border Controller's accounting support, including details about RADIUS accounting.
HDR Resource Guide	Contains information about the Oracle Enterprise Session Border Controller's Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Administrative Security Essentials	Contains information about the Oracle Enterprise Session Border Controller's support for its Administrative Security license.
Security Guide	Contains information about security considerations and best practices from a network and application security perspective for the Oracle Enterprise Session Border Controller family of products.

### Revision History

Date	Version	Description
March 2015	1.00	<ul style="list-style-type: none"> <li>Initial Release</li> </ul>

Date	Version	Description
March 2015	1.01	<ul style="list-style-type: none"> <li>• Removes the "Configuring a Service Tag for an IP Interface" and "Configuring Service Health" topics from the "Configuration Tab" section.</li> <li>• Modifies the "Configure Remote Site Survivability" procedure.</li> </ul>
March 2015	1.02	<ul style="list-style-type: none"> <li>• Removes KPML from the Events section of the table in the "Subscriptions Report" section.</li> <li>• Removes KPML from the Notable Event section of the table in the "Notable Events Report" section.</li> <li>• Reorganizes: "Configuration Tab" chapter.</li> </ul>
May 2015	1.03	<ul style="list-style-type: none"> <li>• Adds the "Internet Protocol Version Support" section.</li> <li>• Adds topics to the Basic Mode Configuration section.</li> </ul>
July 2015	1.04	<ul style="list-style-type: none"> <li>• Adds the note about HA pair behavior to the "Time Division Multiplexing" topic.</li> </ul>
September 2015	1.05	<ul style="list-style-type: none"> <li>• Replaces the "HA on VLAN" topic with the "HA on AP1100" topic.</li> <li>• Updates the " Home Tab" topic to clarify that the default widgets are also subject to the SIP configuration requirement for dashboard widget displays.</li> </ul>
October 2015	1.06	<ul style="list-style-type: none"> <li>• Updates the "High Availability on the Acme Packet 1100" topic to note that the Acme Packet 1100 supports only 1 VLAN tag.</li> </ul>

<b>Date</b>	<b>Version</b>	<b>Description</b>
January 2018	1.07	<ul style="list-style-type: none"><li>• Updates the Certificate Management and Import a Certificate topics with a reboot step.</li></ul>
February 2018	1.08	<ul style="list-style-type: none"><li>• Adds a statement to the "Monitor and Trace Tab" topic about the number of viewers allowed per session.</li></ul>

---

# 1

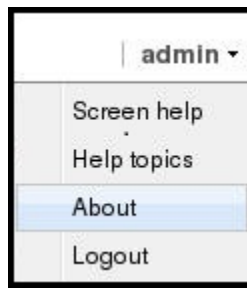
## Getting Started

Oracle® recommends that you review the topics in this section before working with the system to ensure successful use of the tools and functions provided.

### About This Software

You can display information about this software and corresponding licenses currently on the Oracle Enterprise Session Border Controller by clicking **About** on the **logged-on-user-name** menu.

In the following illustration, **Admin** is the name of the user who is logged on.



The About screen displays the following information about the Oracle Enterprise Session Border Controller that you are logged onto:

- Platform type
- Software version number
- Legal notices
- Copyright information
- Open source mailing address
- Trademark recognition
- Licensing information

## Browser Support

You can use the following Web browsers to access the Oracle Enterprise Session Border Controller (E-SBC) Web GUI:

- Internet Explorer versions 9.0 and higher
- Mozilla Firefox versions 12.0 and higher
- Google Chrome versions 19.0.1084.46m and higher



### Note:

After upgrading the software, clear the browser cache before using the E-SBC Web GUI.

## Internet Protocol Version Support

The Web GUI supports only IPv4.

## Log On and Log Off

This section provides the concepts and procedures for logging on to and logging off from the Web GUI.

### Log On to the Web GUI

You can log on to the Oracle Enterprise Session Border Controller (E-SBC) as a User or an Administrator, depending on your permissions.

The system defaults for user name and password follow:

- User. The username is **user** and the password is **acme**.
- Administrator. The user name is **admin** and the password is **packet**.

If you previously changed the default password, use that one to log on.

If your system Administrator configured the optional log on page message, the system displays the message after you enter your logon credentials. After reading the message, click **Close** and the system displays the GUI.

1. On a PC, open a supported Internet browser.
2. Start the GUI with either the HTTP or HTTPS logon.

```
http://<Server IP address>  
https://<Server IP address>
```

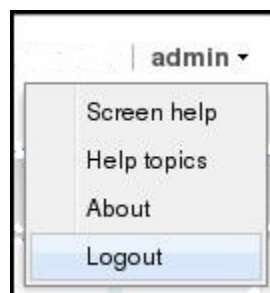
**Note:**

Whether you log on using HTTP or HTTPS depends on the settings for your deployment. Contact your system Administrator for more information.

3. Enter your Web GUI username and password.
4. Click **Login**.

## Log Off the Web GUI

To log off from the Web GUI, click **Logout** from the <logged-on-username> menu in the upper right corner of the Web GUI. In the following illustration, Admin is the name of the user who is logged on.



The system logs you off and displays the log on page.

## User and Administrator Access Rules

Users and Administrators can use the Oracle Enterprise Session Border Controller Web GUI according to the rules for their role.

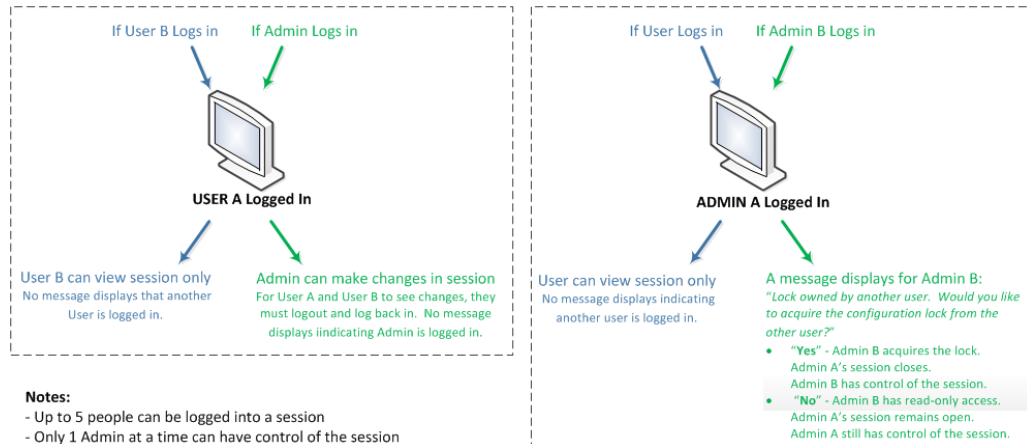
The following table describes the Web GUI access rules for the User and Administrator roles.

Role	Rule
User	User <ul style="list-style-type: none"> <li>• Read-only access only</li> <li>• View basic and advanced configuration information</li> <li>• Cannot save and activate a configuration</li> <li>• Cannot add a configuration</li> <li>• Cannot edit a configuration</li> </ul>
Administrator	Administrator <ul style="list-style-type: none"> <li>• Add, edit, and view configurations</li> <li>• Add, edit, and view advanced configurations</li> <li>• Save and activate a configuration</li> <li>• Switch between Basic mode and Expert mode</li> </ul>

## Simultaneous Logons

The Web GUI allows simultaneous logons for both the User and Administrator. Session availability to the User and Admin depends on which type of user is logged onto the session.

The following illustration shows a scenario of a User and an Administrator logged onto a Web GUI session.



Up to five users can log onto the same session at the same IP address at the same time. Only one Administrator at a time can have full control of a simultaneous session. If more than five users attempt to log on, the system displays the following error message:

User limit reached. Please try again later.

## Change the Log On Password

Use the Oracle Enterprise Session Border Controller ACLI to change a user or administrator logon password.

To change a password, use the `secret` command from the ACLI to change the logon password for a user and the `config password` for an Administrator. For more information about setting passwords, see the *Oracle Enterprise Session Border Controller ACLI Configuration Guide*

## Radius Server in the Network

The Web GUI supports authentication functionality similar to a user logging on by way of TELNET, Secure Shell (SSH), and SSH File Transfer Protocol (SFTP).

The Web GUI supports RADIUS authentication. The following table describes the functions available to the Administrator and User levels.

If	Then
RADIUS server is configured as <code>userclass=admin</code>	Administrator has full access to all features and functions after logging onto the GUI.



If	Then
RADIUS server is configured as userclass=user	User has the following limited access to the features and functions after logging onto the GUI: Full access to all SIP Monitor and Trace features and functions Can download the following files in System File Management: <ul style="list-style-type: none"><li>• Backup configuration</li><li>• Configuration CSV</li><li>• Local subscriber table (LST)</li><li>• Log</li><li>• Software image</li><li>• SPL Plug-in (SPL)</li></ul>

 **Note:**

A user with User privilege cannot upload files in System File Management.

## Update the Configuration Schema

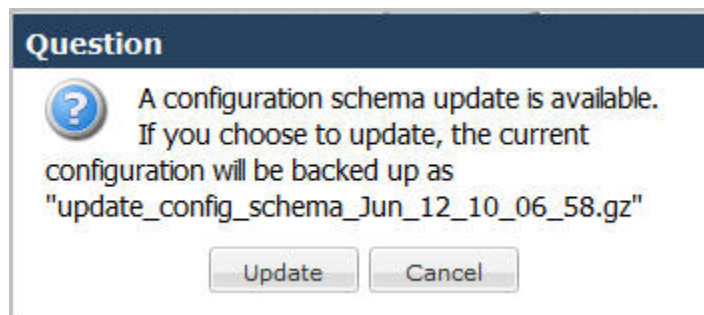
You can update the configuration parameters in your software with any new parameters included in a subsequent release by updating the schema.

Updating the schema adds any new parameters to each configuration screen in Basic Mode.

After updating your Web GUI software to a subsequent release, the system displays a schema update prompt after first log on to the GUI. If you click Cancel, the update is bypassed and no new parameters are added. The update prompt displays each time you log on to the Web GUI, until you choose to update the configuration schema.

### Procedure

1. Log into the Web GUI. The system displays the following prompt.



2. Click **Update**. The system backs up the current configuration and updates the configuration schema.

 **Note:**

If needed, you can reinstall the backed up configuration at a later time from the System tab in the Web GUI.

3. Click **OK**.
4. On the Configuration page toolbar, click **Save**.

## Web GUI Tools

The Web GUI provides some tools that apply to the entire GUI and other tools that apply to specific functions on a tab. For example, "Customizing the Page Display" applies to all pages and "Add widget" applies only to the Home page. Some tools are activated by icons and some are activated by links. The display of icons and links depends on whether the system displays Expert mode or Basic mode.

## Shortcut Keys

The following tables list the shortcut key commands for the Home page and the Configuration page.

Home Page	Shortcut Key Command
Add a Widget	Ctrl+Shift+a
Refresh	Ctrl+Shift+r

Configuration Page	Shortcut Key Command
Discard	Ctrl+Shift+d
Save	Ctrl+Shift+s
Search	Ctrl+Shift+e

## Tabs

The Web GUI displays tabs that you click to display information and where you can perform tasks.

The following table describes the behavior of each Web GUI tab in Basic Mode and in Expert Mode.

	Home Tab	Configuration Tab	Monitor and Trace Tab	Widgets Tab	System Tab
Basic Mode	<p>The Home tab displays the Web GUI Dashboard, where SIP statistics are displayed on configurable widgets. On the Home tab, you can:</p> <ul style="list-style-type: none"> <li>• Add a widget</li> <li>• Specify the widget sampling parameters</li> <li>• Reset the display to the default</li> <li>• Refresh the data displaying in the widgets</li> </ul>	<p>In Basic Mode the Configuration tab displays a workspace where you drag and drop icons to configure the border controller in the network. The toolbar on the Configuration Tab contains the following buttons that display task controls:</p> <ul style="list-style-type: none"> <li>• Settings. Configure system settings.</li> <li>• Network. Configure the Host Route and Network Interface.</li> <li>• Security. Configure a Certificate Record, the SDES profile, and the TLS profile.</li> <li>• Management. Configure Accounting, SNMP Community, Trap Receiver, and Web Server.</li> <li>• Other. Configure Media Profile, Translation Rules, SIP</li> </ul>	<p>The Monitor and Trace tab displays data that the system collects about:</p> <ul style="list-style-type: none"> <li>• Sessions</li> <li>• Registrations</li> <li>• Subscriptions</li> <li>• Notable Events</li> </ul> <p>The page displays a toolbar that you can configure to display particular data for each of the data collection types. For example, you can choose the sort order and column headings.</p> <p>When data is present, the following task controls are active:</p> <ul style="list-style-type: none"> <li>• Search. Configure a search filter.</li> <li>• Show all. Override the display filter and show all data.</li> <li>• Ladder diagram. Displays data in a ladder diagram.</li> <li>• Export session details. Save the detailed data to an</li> </ul>	<p>The Widgets tab is a portal to statistics about the system.</p> <ul style="list-style-type: none"> <li>• Displays a list of objects that provide Configuration, SIP, and System statistical data. Depending on the object selected, you can view the data in list, table, pie chart, bar graph, and line graph form.</li> <li>• Displays a list of Favorite widgets.</li> </ul>	<p>The System tab displays the following management controls:</p> <ul style="list-style-type: none"> <li>• File management. Displays a list of file types and a set of controls to Refresh, Upload, Download, Backup, Restore, and Delete files.</li> <li>• Force HA Switchover. Manually place the system in the standby state.</li> <li>• Reboot. Manually reboot the system at any time.</li> <li>• Support information. Generate a file that displays troubleshooting information that you can save and send to Oracle Customer Support.</li> <li>• Upgrade Software. Verify the health of the system software, for</li> </ul>

Home Tab	Configuration Tab	Monitor and Trace Tab	Widgets Tab	System Tab
	<p>Features, SIP Manipulations, and SPL.</p> <ul style="list-style-type: none"> <li>• Save. Save and activate the configuration.</li> <li>• Discard. Delete unsaved configuration changes.</li> <li>• Wizards. Set boot parameters, Set initial configuration, Set time zone, and Upgrade software.</li> <li>• Switch to Expert. Change from Basic mode to Expert mode.</li> <li>• Search. Search for objects and attributes.</li> </ul>	<p>external location.</p> <ul style="list-style-type: none"> <li>• Export summary. Save a summary of the data to an external location.</li> </ul>		<p>example, synchronization health, configuration version, and disk usage. Configure the upload method, browse to the software file to upload, and opt to automatically reboot the system after the upgrade.</p>

	Home Tab	Configuration Tab	Monitor and Trace Tab	Widgets Tab	System Tab
Expert Mode	Same as in Basic Mode	In Expert Mode the Configuration tab displays a list of configuration objects, grouped like those in the Acme Command Line Interface (ACLI). For example: <ul style="list-style-type: none"> <li>• Media Manager</li> <li>• Security</li> <li>• Session Router</li> <li>• System</li> </ul> Each group contains the same configuration objects as the ACLI. Each object displays the corresponding configuration dialog.	Same as in Basic Mode	Same as in Basic Mode	Same as in Basic Mode

## Search

From the Web GUI, you can search for a system object with the Search button located on the toolbar and you can search by the attributes of a system object with the Search field located on the page for a system object.

On the toolbar, click the Search button and the system displays the system objects in a drop down list. You can select an object from the list or type the object name in the text box. The system displays the search results in a list, where the object name is a link. Click the link to navigate to the object page.

On a system object page, enter an attribute or value for the object in the Search field and click Search. The system displays the results on the system object page.

### Note:

The system does not support searching or sorting on lists and sub-objects from the Search field on a system object page.

- For example, the realm-config system object page displays a list of Network Interfaces. You cannot search for one of the network interfaces on the list.
- For example, the realm-config system object displays the sub-objects "In realm", "In network", and "Same ip" under the "Mm" object. You cannot search for the sub-objects.

## Help

The logged on user button on the Web GUI displays the following information:

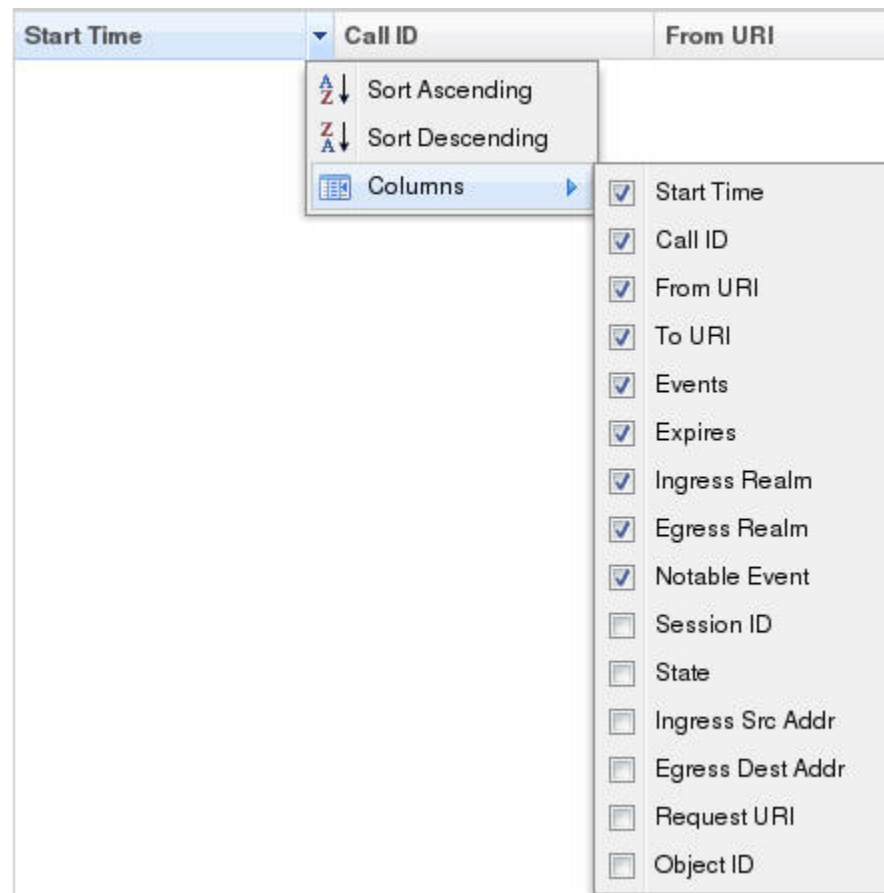
- **Screen Help.** Short descriptions of elements on the page.
- **Help Topics.** Online Help system containing topics about the tasks that you can perform on the Web GUI.
- **About.** Oracle notices and disclaimers, Oracle terms and restrictions, and third-party notices.

## Customize the Page Display

You can customize the display of the data on Web GUI pages by selecting which columns display, the information type, and the sort order.

### Procedure

1. Place the cursor on a column heading.  
The system displays a down arrow in the column heading.
2. Click the down arrow to display the customization menus. For example,



## Save and Activate Network Configuration

When you finish creating the network, you must save and activate the configuration on the Oracle Enterprise Session Border Controller.

1. In any configuration dialog, click **OK**.

The system verifies and saves the current configuration to the last-saved configuration, which is stored in flash memory. This allows you to queue multiple changes during a configuration session before you set them all on the device.

2. Optional. Perform additional configuration, and click **OK** each time.
3. Click **Save**.

The system displays the Confirmation dialog, with the **Activate** button.

4. Click **Activate**.

The system displays the success dialog.

5. Click **OK**.

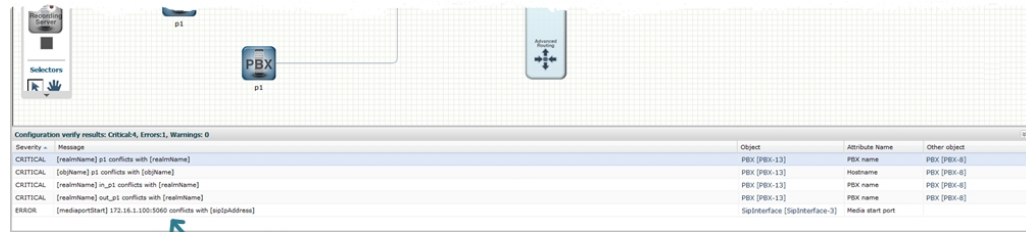
The system moves the changes from the flash memory to the running configuration.

## Configuration Error Messages

For both Basic and Expert Mode, if you save a configuration that contains errors, the errors display in a window at the bottom of the screen, and the following message displays:

There were errors! Are you sure you want to activate the configuration?

The following is an example of errors that display for a configuration in Basic Mode.



*Click on an error to go to the location in the configuration where you can fix it*

Click the error link in the Object column to go to the exact location in the configuration where the error exists, and then edit the configuration as applicable.

The following table identifies the columns in the error list.

Column	Description
Severity	Identifies the level of severity that the Oracle Enterprise Session Border Controller assigns to the error. Valid values are: ERROR - Indicates the issue identified in the "Message" column was not correctly configured or it does not exist. You can still verify, save, and activate the configuration if this severity exists. WARNING - Indicates the configuration contains invalid information for the element field identified in the "Message" column. You can still verify, save, and activate the configuration if this severity exists. CRITICAL - Indicates a critical error has occurred in the configuration and you cannot verify, save, or activate until the error is corrected. The "Message" column indicates the element field where the error has occurred.
Message	Identifies the element field(s) where the error, warning, or critical error has occurred, and identifies the reason for the error.
Object	Identifies the element and the field for that element where the error occurred.
Attribute	Identifies the attribute within the element where the error occurred.
Other Object	Identifies the other object when more than one object caused the error.

## Discard Changes

You can discard all changes made to a configuration object that have not been activated.

### Procedure

1. From the Web GUI toolbar, click **Discard**.  
The system displays a confirmation message.
2. Click **Discard**.



# 2

## Home Tab

The Oracle Enterprise Session Border Controller (E-SBC) provides a web-based dashboard on the Home tab that can display SIP data statistics to help you monitor and manage the system, for example, SIP Media Flows and Current Memory Usage. The E-SBC collects only SIP data for the dashboard widgets, including the default CPU and Memory widgets. For this reason, you must set up a valid SIP configuration before the E-SBC can display any data on a dashboard widget.

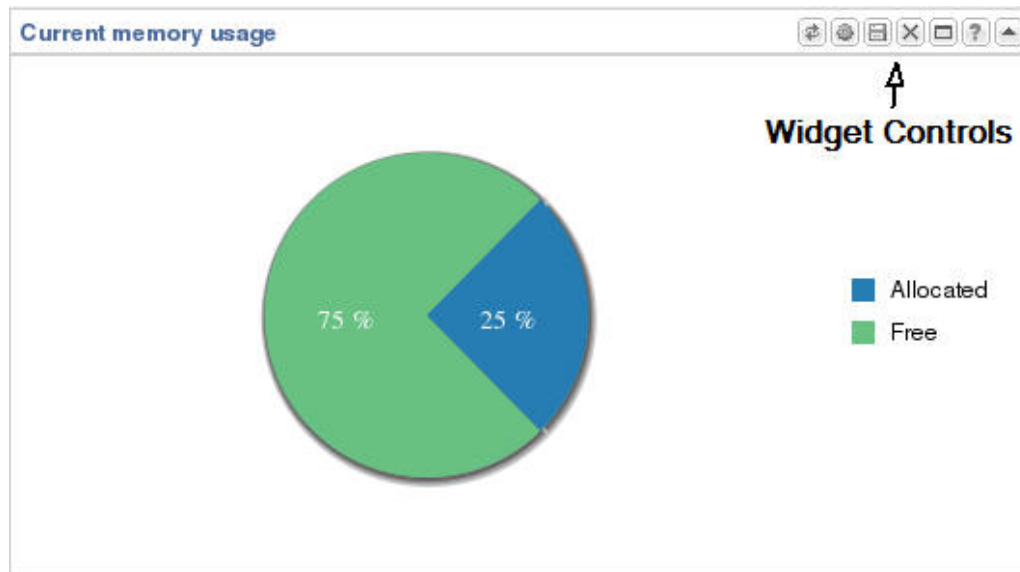
The Dashboard supports up to 18 widgets. Each widget can display up to 100 data samples in intervals of 1 hour, 1 minute, or 1 second. You can select a chart, a graph, a table, a web form, or text for the display. Customize the dashboard by adding, deleting, and moving the widgets. You can refresh the statistics displayed on the dashboard and you can reset the dashboard to its default display. The default display includes:

- Highest CPU Usage
- Current Memory Usage
- Historical Memory Usage

The following table describes the controls that you can use to customize the Home page display.

Button	Description
Refresh	Updates all of the widgets on the Dashboard.
Add widget	Displays a list of widgets that you can add to the Dashboard.
Reset	Resets the Dashboard to display the default widgets. All other widgets are removed from the Dashboard.

Use the icons in the upper right corner of the widget to perform specific tasks. Roll the mouse over the icon for a description of the function.



Note that the operation of widgets, such as those that require the SIP.Session module, may affect system performance. The system displays a warning when you add a widget that may affect performance. Oracle recommends adding such widgets at a time when the performance impact will not degrade service.

## Add a Dashboard Widget

Add a widget to the Web GUI Dashboard to display SIP and System statistics to help you monitor and manage the system.

You can add up to 18 widgets to the Dashboard with the **Add widget** control on the Web GUI Home page. The system does not require a reboot after adding a widget to the Dashboard.

### Note:

If the system displays a warning that adding this widget requires the SIP.Message module to be enabled, the system enables the SIP.Message module when you add the widget.

### Procedure

1. From the Home page, click **Add widget**.
2. From the list of **Widgets**, click the name of the widget to add.
3. Under the **Command** column header, click **Add** for the widget to add.  
The system displays a success message.
4. Click **OK**.
5. Click **Close**.

The system displays the Dashboard with the newly added widget.

See "Configure Data Sampling Settings for a Dashboard Widget."

## Configure Data Sampling Settings for a Dashboard Widget

Confirm that the widget that you want to configure is on the Dashboard. See *Add a Widget*.

To see SIP and System statistics displayed on a Dashboard widget, the system requires a setting for how often to refresh the display. You can use the default interval or select one from the Auto-refresh interval drop-down list on the widget. Some widgets also display the Table Name drop-down list, where you can set the data sampling frequency. For example, you might configure the widget to refresh the display every 40 seconds and to display the data samples in one minute increments.

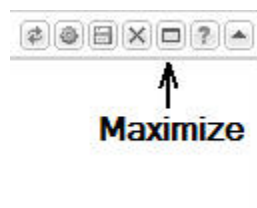
### Procedure

1. Click the **Home** tab.
2. On the widget, click the **Settings** icon.
3. Select a widget display refresh frequency from the **Auto-Refresh Interval (seconds)** drop down list.
4. If the widget displays the **Table Name** drop-down list, select a data sampling increment for the widget display.
5. Click **OK**.

## View a Dashboard Widget in Full-Screen Mode

Use the maximize icon located on the Dashboard widget for a full-screen view of the widget data.

Each Dashboard widget includes a maximize icon on its toolbar.



1. Click the maximize icon.  
The system displays a pop-up window of the selected widget.

### Note:

To view a widget that is not on the Dashboard in full-screen mode, see "View Any Widget in Full-Screen Mode."

## View Any Widget in Full-Screen Mode

Use the Widgets tab to display data from the SIP and System Dashboard widgets in full-screen mode.

Use the following procedure to view widgets that are not displayed on the Home page as Dashboard widgets, in full-screen mode.

**Procedure**

1. From the Web GUI, click the **Widgets** tab.
2. In the navigation pane, click a Dashboard Widget name.  
The system displays a list of the views available for the selected widget.
3. In the list of view types click the view that you want to see in full-screen.

# 3

## Configuration Tab

The Configuration tab on the Web GUI provides a graphical display of the same objects and elements that you can access from the command line to configure the Oracle Enterprise Session Border Controller (E-SBC).

The Web GUI provides the following configuration tools.

- **Basic Mode.** Displays a workspace where you drag-and-drop icons representing network objects and system elements, so that you can see a graphical representation as you build the network. When you click an icon on the workspace, the Web GUI displays the corresponding configuration dialog.
- **Expert Mode.** Displays a list of the network objects and system elements. When you click an element on the list, the Web GUI displays the corresponding configuration dialog. In Expert Mode, the system does not display the workspace and graphical representation of the network as it does in Basic Mode.
- **Wizards.** Displays a menu of select configuration wizards that lead you through setting boot parameters, setting entitlements, setting the initial configuration, setting the license, setting the logon banner text, setting the time zone, and upgrading the software.

## Configuration States and Behavior

After you finish creating or modifying a configuration, you must save and activate the configuration before the Oracle Enterprise Session Border Controller (E-SBC) saves the changes to the running configuration.

At any time, the following three versions of the configuration can exist on the E-SBC.

- **Editing.** The editing configuration is the version that you are making changes to from the Web GUI. The editing version is stored in the E-SBC volatile memory. The editing version cannot survive a system reboot.
- **Saved.** The saved configuration is the version of the editing configuration that the system copies into the non-volatile memory when you click **Save** on the Web GUI. Until you activate the saved configuration, the changes do not take effect on the E-SBC. The system does not load the saved, but not activated, configuration as the running configuration on reboot.
- **Running configuration.** The running configuration is the configuration that the system is using. When you activate the saved configuration it becomes the running configuration. Most configuration changes can take effect upon activation. Some configuration changes require a system reboot. On reboot, the system loads the running configuration.

The process for saving and activating a configuration, includes the following steps.

1. **OK.** All configuration dialogs display an **OK** button that saves changes to the editing memory. If you reboot before the next step, the E-SBC does not save the changes.
2. **Save.** The **Save** button on the Web GUI toolbar verifies the configuration, displays errors, saves the current configuration to the last-saved configuration, and stores it on the **E-SBC**. The system displays any errors at the bottom of the Configuration page. If you reboot after

saving the changes, the E-SBC retains the changes and moves the changes to the running configuration.

3. **Activate.** After you finish making one or more configuration changes, **OK** and **Save** from the last configuration dialog that you need to edit at this time. The system displays the Confirmation dialog containing the **Activate** button. When you click **Activate**, the E-SBC activates all of the saved configuration changes and saves the new configuration to the running configuration. If you cancel the activation function, the E-SBC saves the configuration in a file and does not change the running configuration. You can continue to make changes to the configuration.

## Configuration Error Messages

If you save a configuration that contains errors, the system displays the following error message: There were errors! Are you sure you want to activate the configuration?

The system displays a list of errors at the bottom the page. Click an error to go to the location in the configuration where the error occurred and edit the configuration as needed.

Column	Description
Severity	Identifies the level of severity that the Oracle Enterprise Session Border Controller assigns to the error. Valid values are: <ul style="list-style-type: none"> <li>• <b>ERROR.</b> Means that the issue identified in the Message column is not correctly configured or it does not exist. You can still verify, save, and activate the configuration if this severity exists.</li> <li>• <b>WARNING.</b> Means that the configuration contains invalid information for the element field identified in the Message column. You can still verify, save, and activate the configuration if this severity exists.</li> <li>• <b>CRITICAL.</b> Means that a critical error occurred in the configuration and you cannot verify, save, or activate until the error is corrected. The Message column indicates the element field where the error has occurred.</li> </ul>
Message	Identifies the element field where the error, warning, or critical error occurred, and the reason for the error.
Object	Identifies the element and the field for that element where the error occurred.
Attribute Name	Identifies the attribute within the element where the error occurred.
Other	Identifies any other pertinent information relating to the error.

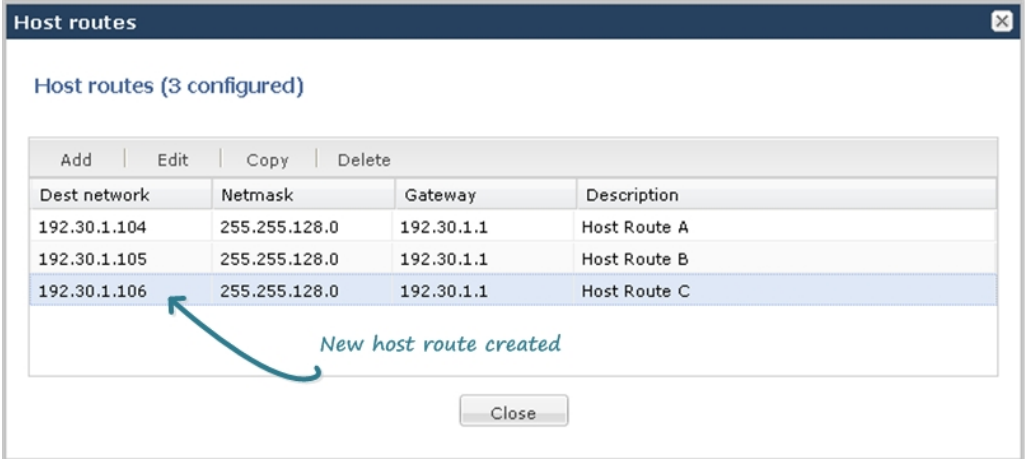
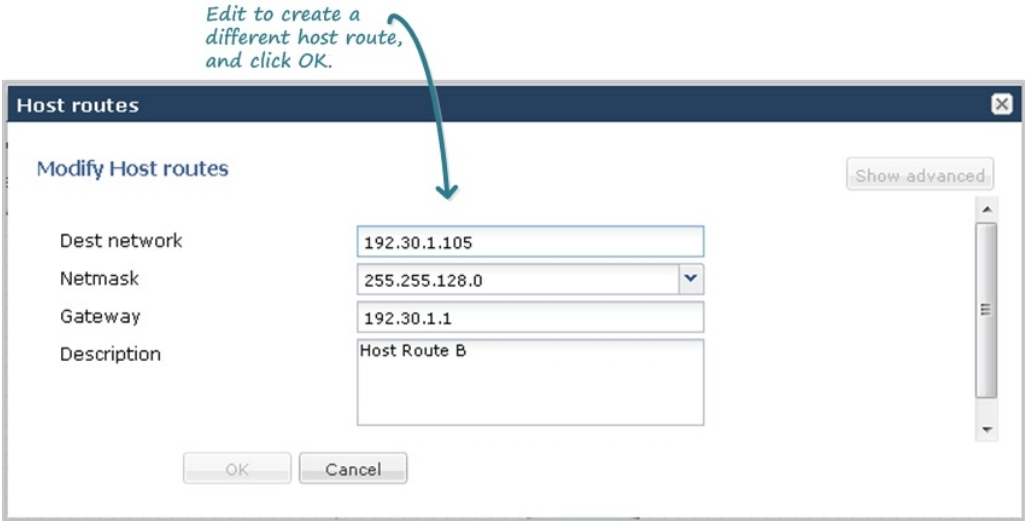
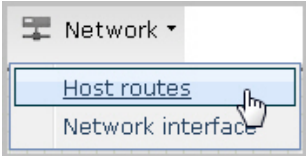
## Configuration Copying Methods

In Basic mode you can copy a configuration by way of the object menus on the toolbar, but not from the icons in the workspace.

To copy a configuration, use one of the following methods:

- Select an item on the list and click **Copy**.
- Select an item on the list, right click, and select **Copy** from the task menu.

The following illustrations show host route 192.30.1.105 copied and edited as a new host route of 192.30.1.106.



## Configuration Editing Methods

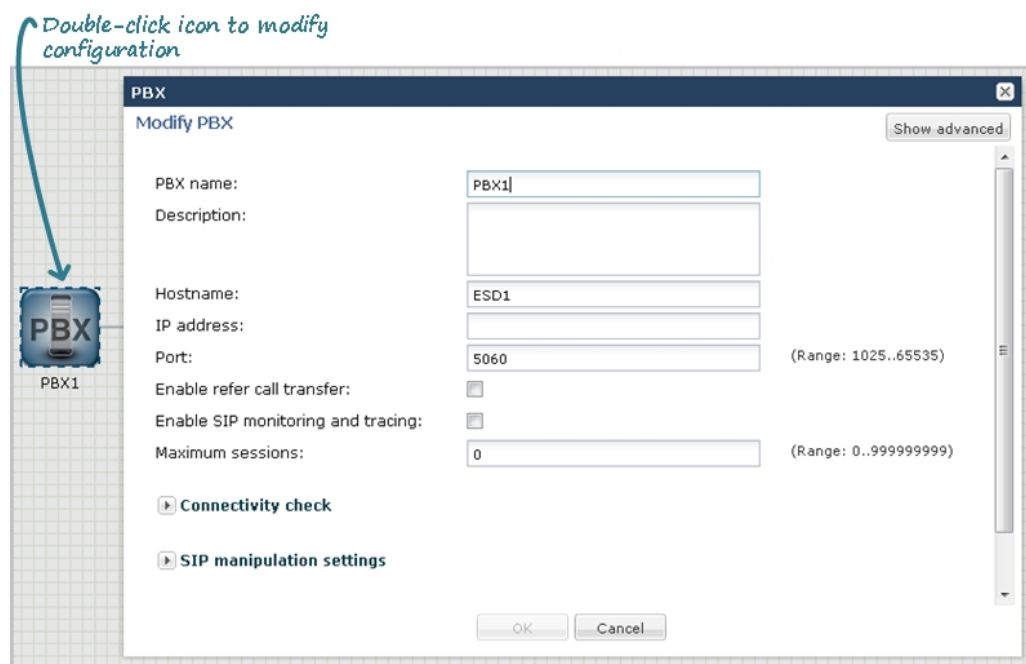
In Basic mode, you can edit a configuration by way of the following methods.

### Edit from an Icon

For any device or interface icon in the workspace, the system displays the configuration dialog when you:

- Double-click the icon.
- Right-click the icon and select Edit from the drop-down menu.

The following illustration shows an example of editing a configuration by way of the PBX icon.

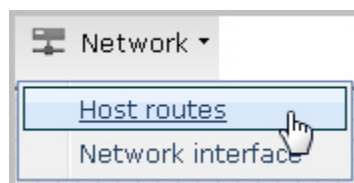


### Edit from a Configuration Dialog

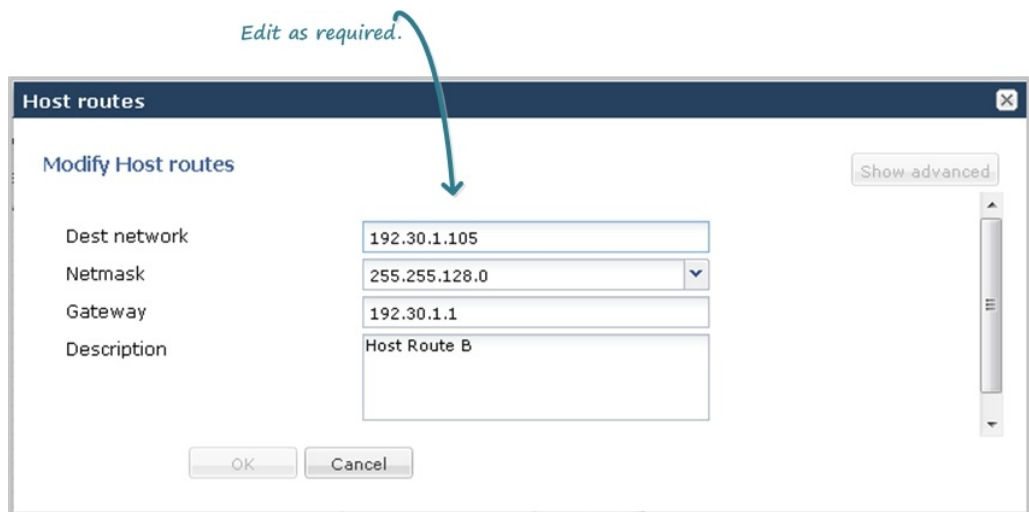
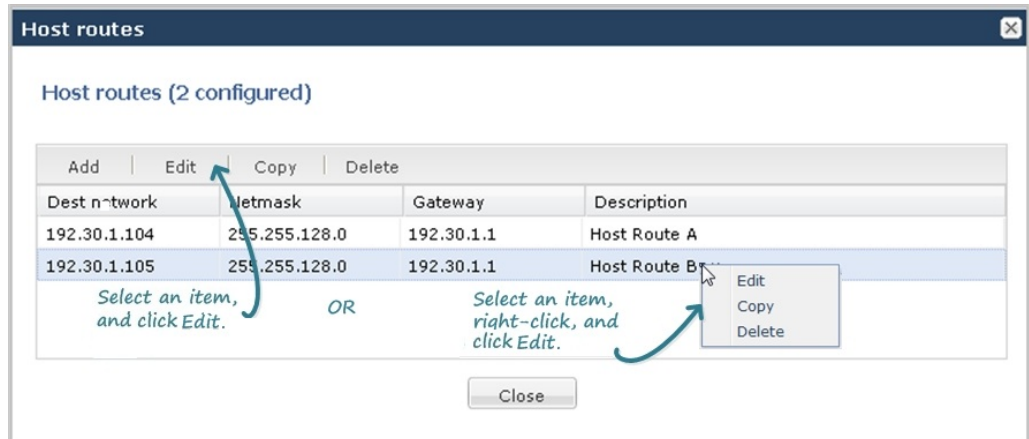
To edit a configuration from a toolbar menu, you click the configuration object that you want from the menu, and use one of the following methods to display the configuration dialog:

- Select an item on the list and click **Edit**.
- Select an item on the list, right click, and select **Edit** from the task menu.

The following illustrations show examples of editing a host route configuration by both methods.

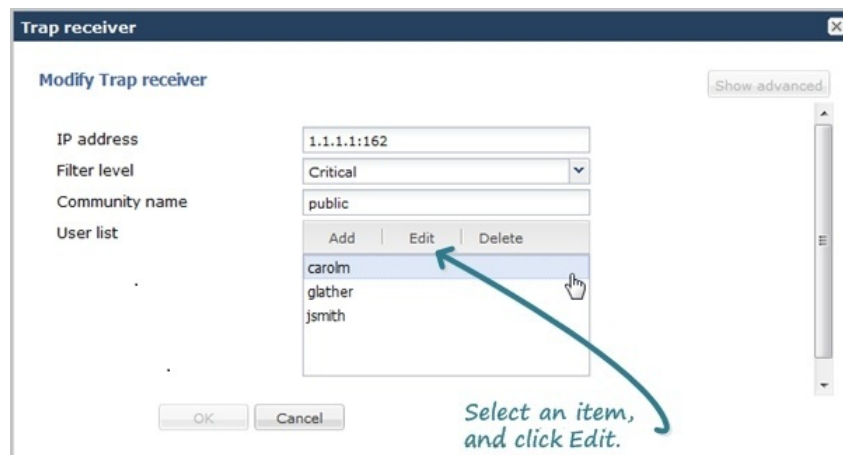






### Edit an Individual Parameter

Some configuration dialogs require additional configuration of a particular parameter. The following illustration shows an example of the editing dialog for the User List parameter within the trap-receiver configuration dialog.



 **Note:**

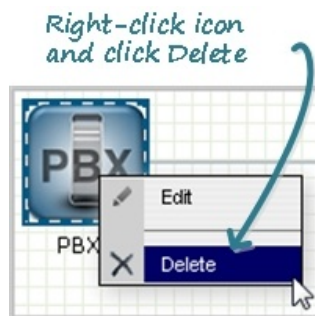
After editing a configuration, you must save and activate the configuration for the changes to take affect.

## Configuration Deletion Methods

In Basic mode, you can delete a configuration by way of the following methods.

### Delete from an Icon

For any device or interface in the workspace, right-click the icon and select Delete from the drop-down menu. The following illustration shows an example of deleting a configuration by way of the PBX icon.

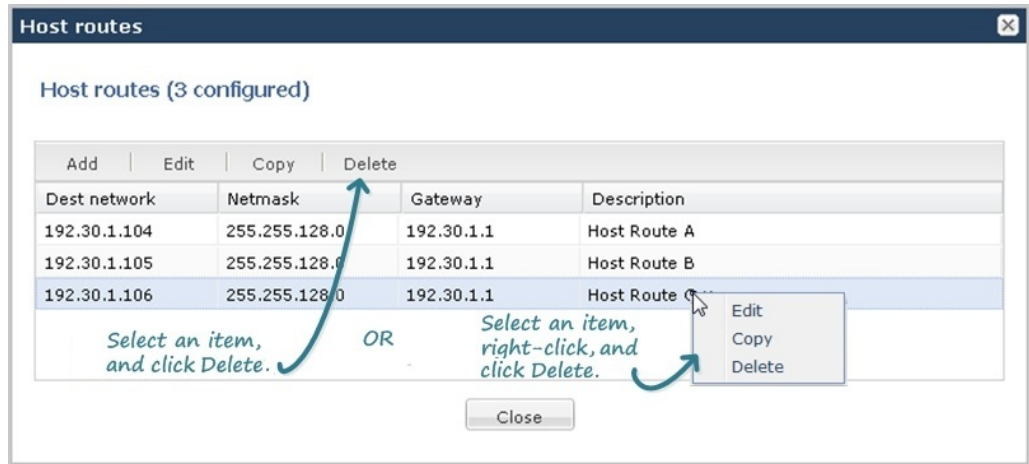


The system deletes the configuration from the workspace and from the Oracle Enterprise Session Border Controller.

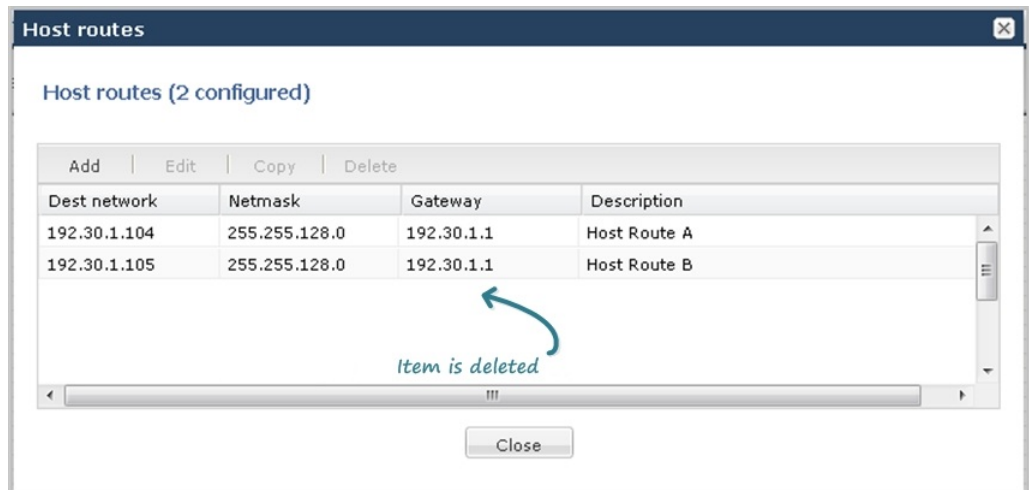
### Delete from a Configuration Dialog

To delete a configuration from a toolbar menu, you click the configuration object that you want from the menu, and use one of the following methods to delete the configuration:

- Select an item on the list and click **Delete**.
- Select an item on the list, right click, and select **Delete** from the task menu.

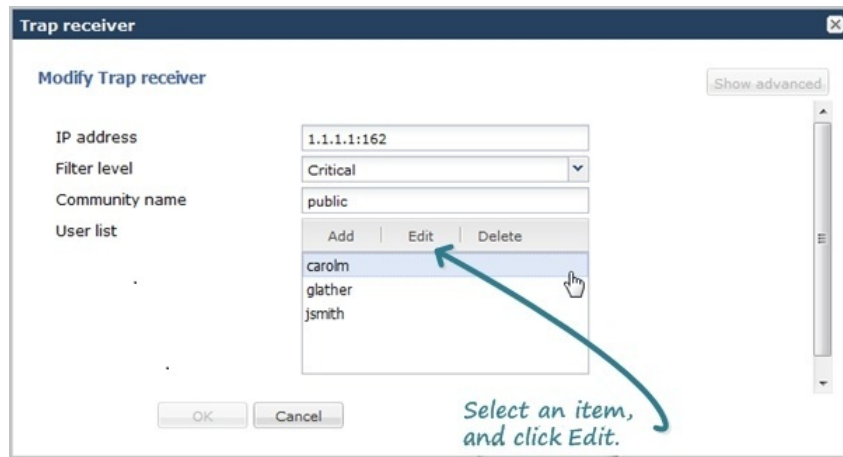


Click Yes to delete the item.  
Click No to cancel the delete function.



### Delete an Individual Parameter Configuration

Some configuration dialogs require additional configuration of a particular parameter. The following illustration shows an example of the deletion dialog for the User List parameter within the trap-receiver configuration dialog.



### Note:

After editing a configuration, you must save and activate the configuration for the changes to take affect.

## Configuration from the Web GUI

The procedures for configuring the Oracle Enterprise Session Border Controller from the Web GUI are consistent in how they begin and end. What varies are the steps in between, which are unique to each configuration procedure. Once you are familiar with the common steps for beginning and ending any configuration procedure, the unique information that you need is about the fields, selections, and options available within each procedure. The Web GUI Guide and the online Help system provide procedural, conceptual, and referential topics to help you with the steps in between. Procedural topics provide the "how" information, such as the prerequisites, the configuration steps, and the next steps. Conceptual topics provide the "why?" information, such as a description of the purpose and benefits of the configuration or feature. Reference topics provide the "what?" information, such as a list of the acceptable values for fields.

The following sections describe the common steps for beginning and ending configuration procedures from the Web GUI in Basic mode and in Expert mode.

### The common beginning in Basic mode

Each Basic mode configuration procedure begins, as follows:

1. From the Web GUI in Basic mode, click the **Configuration** tab.
2. On the Configuration page, you can do one or both of the following:
  - a. Drag an icon into the workspace. This gesture causes the system to display the corresponding configuration dialog.
  - b. Click Wizards, Settings, Network, Security, Management, or Other, and select a configuration option from the resulting drop down menu. The system displays the corresponding configuration dialog.

### The common ending in Basic mode

Each Basic mode configuration procedure ends, as follows:

1. When you finish configuring the fields, selections, and options in the configuration dialog, click **OK** or **Close**, depending on the dialog.
2. On the Web GUI toolbar, click **Save**.
3. Click **Activate**.
4. Click **OK**.

### The common beginning in Expert mode

Each Expert mode configuration procedure begins, as follows:

1. From the Web GUI in Expert mode, click the **Configuration** tab.
2. On the Configuration page, at the bottom of the **Objects** pane, click **Show advanced**.
3. Click the arrow by the object group name, for which you want to see the list of configuration elements.
4. Click the element that you want to configure, and the system displays the corresponding dialog.

### The common ending in Expert mode

Each Expert mode configuration procedure ends, as follows:

1. When you finish configuring the fields, selections, and options, and the system displays the page where you began the configuration, click **OK**.
2. On the Web GUI toolbar, click **Save**.
3. Click **Activate**.
4. Click **OK**.

#### Note:

Click **Show advanced** in the configuration dialogs to display all of the settings available within each function. Click **Hide advanced** to display only the minimum required settings.

## Wizards Button

The Wizards button displays a menu of configuration wizards from which you can perform, save, and activate selected configuration procedures for the Oracle Enterprise Session Border Controller. Configuration wizards are available in the Basic mode and in the Expert mode.

The Wizards button provides access to the following configuration wizards.

Configuration Wizard	Purpose
Set boot parameters	Specify the boot file and the boot parameters.
Set entitlements	Set the number of sessions that a license entitles, and enable advanced features.

Configuration Wizard	Purpose
Set initial configuration	Configure a new system and reconfigure an existing system. Includes configuring High Availability.
Set license	Enter the license number for a feature.
Set logon banner	Customize the text on the Web GUI logon banner.
Set time zone	Select the time zone for the deployment.
Upgrade Software	Upload a new version of the software.

## Set Boot Parameters Wizard

The Oracle Enterprise Session Border Controller (E-SBC) requires you to enter the necessary parameters to boot the system in your deployment.

You can set the E-SBC boot parameters from the Set Boot Parameters wizard on the Web GUI in either Basic mode or Expert mode.

### Procedure

1. From the Web GUI, click **Configuration > Wizards > Set Boot Parameters**.
2. In the Set Boot Parameters dialog, enter the following information:

Attributes	Instructions
Boot File	Name of the image file.
IP Address	Enter the IP address of the E-SBC.
VLAN	Range: 0-4095
Net Mask	Enter the net mask IP address in dot decimal format. For example, 255.255.0.0.
Gateway	Internet address of the boot host. Leave blank if the host is on the same network.
FTP Host IP	Enter the IP address of the FTP host.
FTP Username	Enter the FTP username for the FTP user on the boot host.
FTP Password	Enter the FTP password for the FTP user on the boot host.
Flags	Hexadecimal. Always starts with 0x. See "Configurable Boot Loader Flags."
Target Name	Name of the E-SBC, as displayed at the system prompt.
Console Device	Enter the type of console device. For example, VGA.
Console Baud Rate	Select a console baud rate from the drop-down list.

3. Click **Complete**.  
The system displays a success message.
4. Click **OK**.

## Configurable Boot Loader Flags

You may configure the following boot flags in the boot loader:

- 0x02 - enable kernel debug
- 0x04 - disable crashdumps
- 0x08 - changes autoboot countdown from 2 to 15 seconds
- 0x10 - enable debug login
- 0x40 - use DHCP for wancom0
- 0x80 - use TFTP instead of FTP

## Set Entitlements Wizard

Use the Set Entitlements wizard to enter the maximum number of sessions that your license allows.

### Before You Begin

- Note the session limit number from your license.

You can launch the Set Entitlements wizard on the Web GUI in either Basic mode or Expert mode.

### Procedure

1. From the Web GUI, click **Configuration > Wizards > Set Entitlements**.
2. In the Set Entitlements dialog, do the following:

Attributes	Instructions
Advanced	Select to add the Advanced license.
Session Capacity	Enter the session limit number from the license.

3. Click **Complete**.  
The system displays a success message.
4. Click **OK**.

## Set Initial Configuration Wizard

Use the Set Initial Configuration wizard to perform the initial configuration on an unconfigured system and to change the configuration on a configured system. During the configuration, you select the scope of configuration that you want to perform, define the boot parameters, opt to set a VLAN, and configure features such as High Availability (HA) and access to the Oracle Communications Session Delivery Manager (OC SDM). A valid license is required to run the Set Initial Configuration wizard.

Launch the Set Initial Configuration Wizard

- **Unconfigured system.** The system launches the Web GUI Set Initial Configuration wizard upon the first logon. When the initial configuration is complete, the system saves the configuration, activates the configuration, and reboots. The system does not backup the initial configuration of an unconfigured system.

- Configured system. From the Configuration tab on the Web GUI, click the Wizards button and click Set Initial Configuration. When the re-configuration is complete, the system saves a backup of the existing configuration, saves the new configuration, activates the new configuration, and reboots. The backup is stored in /code/bkups.

Before you can configure the E-SBC, the wizard requires you to make the following selections that determine which configuration parameters the wizard displays.

Selections	Behavior
Enable Web GUI: Yes/No	If you select <b>No</b> , you may continue using the wizard to set the initial configuration until you reboot. After you reboot, the system no longer displays the Web GUI. If you want to enable the Web GUI in the future, configure the <code>web-server-config</code> object from the ACLI.
Choose Web GUI Mode: Basic/Expert	<p>When selecting Basic mode or Expert mode, the decision is about how much control you want in the configuration process and whether or not you want to use one of more of the advanced features and settings provided in Expert mode.</p> <ul style="list-style-type: none"> <li>• In Basic mode, the system displays the minimum number of settings that you need to successfully deploy and operate the E-SBC. While you cannot configure the advanced settings and features in Basic mode, you can switch to Expert mode to do so. Note that when you switch to Expert mode and perform <b>Save</b>, you cannot switch back to Basic mode. The Web GUI will display the Expert mode from then on, including after a new log on.</li> <li>• In Expert mode, you can use the advanced settings and options to control the configuration with more granularity. The system does not require you to configure all advanced settings and features. You can choose what you need for your deployment.</li> </ul>
E-SBC Mode: Standalone/High Availability	<ul style="list-style-type: none"> <li>• If you select Standalone, you can begin configuring the parameters displayed.</li> <li>• If you select High Availability, the GUI adds E-SBC Role: Primary/Secondary to the display.</li> </ul>
E-SBC Role: Primary/Secondary	<p>If you selected High Availability for E-SBC Mode:</p> <ol style="list-style-type: none"> <li>1. Select Primary, and configure the displayed parameters.</li> <li>2. Select Secondary, and select <b>Yes</b> or <b>No</b> for Acquire Configuration from Primary. If you select <b>No</b>, the GUI adds a field where you enter the Peer Target Name.</li> </ol>



 **Note:**

Unlike other E-SBCs, which provide 2 management interfaces and 2 media interfaces, the Acme Packet 1100 provides 1 management interface and 2 media interfaces. When configuring HA, the configuration dialogs for the Acme Packet 1100 differ from the other E-SBCs because you must create a second, virtual management interface. For creating the second management interface, the HA dialogs on the Acme Packet 1100 contain more attributes than the dialogs for the other E-SBCs. Regardless of the E-SBC model, the path through the Set Initial Configuration wizard to the HA dialogs is the same as described in this topic.

## Set License Wizard

Use the Set License wizard to enter the serial number for your license.

### Before You Begin

- Obtain the license, which includes the serial number, for the feature that you want to add to the deployment. See "Obtain a License" in the ACLI Configuration Guide.

You can launch the Set License wizard on the Web GUI in either Basic mode or Expert mode.

### Procedure

1. From the Web GUI, click **Configuration > Wizards > Set License**.
2. In the Set License dialog, enter the license serial number in the Add license field.
3. Click **Complete**.  
The system displays a success message.
4. Click **OK**.

## Set Logon Banner Wizard

Use the Set Logon Banner wizard to add customized text to the logon page.

You can customize the logon page by adding text to help the user. For example, Welcome to <company name> <business unit> <location> session border controller <device name>.

### Procedure

1. From the Web GUI, click **Configuration > Wizards > Set Login Banner**.
2. In the Set Login Banner dialog, enter the text that you want to display on the log on page.
3. Click **Complete**.  
The system displays a success message.
4. Click **OK**.

## Set Time Zone Wizard

The system requires a setting for time zone.

You can set the system time from the Set Time Zone wizard on the Web GUI. You can select a time zone or Coordinated Universal Time (UTC). The wizard is available in Basic Mode and Expert Mode.

**Procedure**

1. From the Web GUI Home page, click **Configuration > Wizards > Set Time Zone**.
2. From the drop down list, select one of the following:
  - Time zone by locale
  - UTC
3. Click **Complete**.  
The system displays a success message.
4. Click **OK**.

## Upgrade Software Wizard

You can upgrade the system software with the Upgrade Software wizard on the Web GUI.

Use the Upgrade Software wizard to perform the following tasks:

- Check the system health before the upgrade
- Download new software
- Change boot parameters
- Reboot the system

The system requires a reboot after the upgrade for the changes to take effect.

**Procedure**

1. From the Web GUI tool bar, click **Wizards**.
2. On the Wizards drop down list, click **Upgrade Software**.
3. (Optional) In the Upgrade Software dialog, click **Verification**, and do the following:
  - Click **View Synchronization Health**, and confirm that the system components are synchronized.
  - Click **View Configuration Version**, and note the Current Version and Running Version.
  - Click **View Disk Usage**, and confirm that the system has enough free space.
4. In the Upgrade Software dialog, do the following:

Attributes	Instructions
Upload method	Select an upload method from the drop-down list.
Software file to upload	Browse to the file to upload.
Reboot after upload	Select to reboot the system after the upgrade.

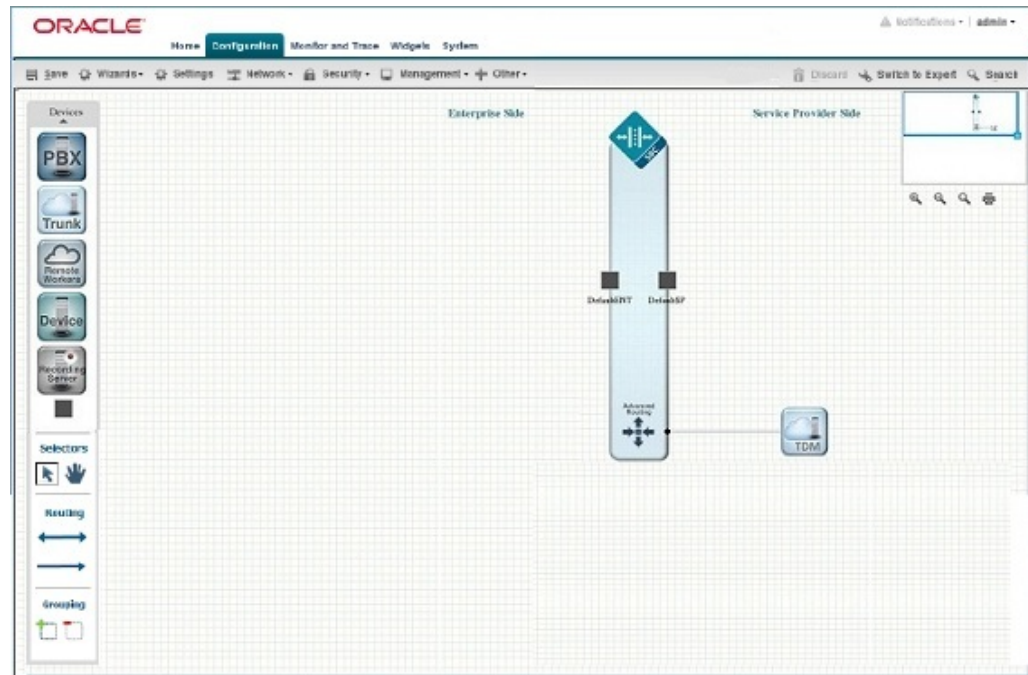
5. Click **Complete**.
  - If you did not select **Reboot After Upload**, the system displays a message stating that a reboot is required for the changes to take effect.
  - If you selected **Reboot After Upload**, the system displays a message stating that it is about to reboot.
6. Click **OK**.

The system performs the file transfer and any boot parameter changes. If you selected **Reboot After Update**, the system reboots.

## Basic Mode Configuration

Basic mode is a graphical method for deploying and configuring the Oracle Enterprise Session Border Controller (E-SBC) in the network.

The Basic mode workspace consists of a toolbar and a workspace onto which you can drag-and-drop icons to configure the E-SBC. The E-SBC is centered between the Enterprise network on the left and the Service Provider network on the right.







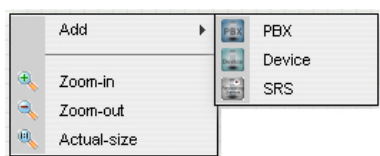
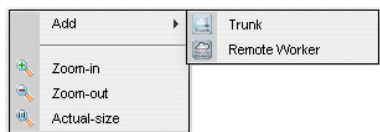
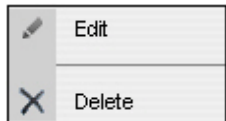
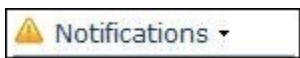
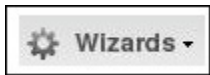
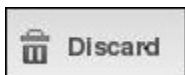
To populate the network, drag-and-drop elements from the Devices tool bar on the left of the page onto the workspace. As you drop an icon onto the workspace, the element connects to the E-SBC and a dialog displays where you configure that element. Elements in the toolbar are associated either with Enterprise or Service Provider. If you drag-and-drop an element to an incorrect location on the workspace, the system displays the following error message: "This icon cannot be placed here."



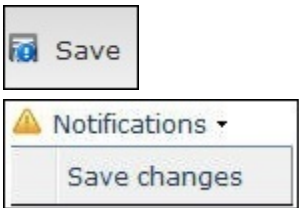
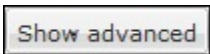
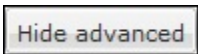
You can create local policies between the elements on the workspace, add new network interfaces to the E-SBC, and group like elements. No configuration parameters other than those available in Basic mode are required to deploy the E-SBC. If your deployment requires a more robust configuration, you can click Show Advanced in Basic mode dialogs that offer additional parameters or you can switch to Expert mode.

### Note:

The Web GUI does not indicate required fields and the system does not display an error message for a missing required parameter.

## Basic Mode Configuration Tools

Tool	Description
	Zoom-in - Used to increase the viewing size of the current window and all its contents.
	Zoom-out - Used to decrease the viewing size of the current window and all its contents.
	Actual size - Used to display the current window and all its contents on a one-on-one ratio (actual size).
	Print - Provides a view of the image that you can print from your browser.
<p>Enterprise Side Add Menu</p> 	<p>Add Menus - These menus can be accessed by right-clicking the mouse on the Enterprise side or the Service Provider side.</p> <p><b>Add &gt; PBX/Device/SRS-</b> Allows you to add a PBX, a Device, or a Session Recording Server (SRS) to your Enterprise configuration. You can use this menu in lieu of dragging and dropping these elements from the Device tools.</p>
<p>Service Provider Side Add Menu</p> 	<p><b>Add &gt; Trunk/Remote Worker</b> Allows you to add a Trunk or a Remote Worker, to your Service Provider configuration. You can use this menu in lieu of dragging and dropping these elements from the Device tools.</p>
	<p>You can use the following tools from either menu instead of from the workspace tools in the upper right corner of the screen, if required:</p> <p><b>Zoom-in</b> - Allows you to view a workspace and all of its elements in a closer proximity.</p> <p><b>Zoom-out</b> - Allows you to view a workspace and all of its elements in a more distant proximity.</p> <p><b>Actual Size</b> - Allows you to view a workspace and all of its elements in its actual size.</p> <p><b>Edit/Delete Menu</b> - This menu can be accessed by selecting an element on the screen and then right-clicking the mouse.</p> <p><b>Edit:</b> Allows you to edit the configuration of the element on which you right-clicked.</p> <p><b>Delete:</b> Allows you to remove the element from the workspace AND the configuration.</p>
	Displays system notifications and alarms.
	Wizards - Displays a list of configuration wizards and the Upgrade Software wizard.
	Discard - Allows you to discard all configuration changes made in the current session. Only the changes that have not yet been activated are discarded.

Tool	Description
	<p>Switch to Expert - Switches from Basic Mode to Expert Mode.</p> <p>Note: Before you can switch to Expert Mode, you must save and activate your configuration in Basic Mode.</p> <p>Caution: You can switch to Basic Mode from Expert Mode, if you do not save your changes. If you save your changes and you switch back to Basic Mode, you must run the Set Initial Configuration wizard again. You will lose all of the configuration changes you made in both modes.</p>
	<p>Search - Allows you to perform a search of any configuration element or sub-element on the Oracle Enterprise Session Border Controller. You perform the search by entering a keyword which is not case sensitive. Special characters are allowed.</p>
	<p>Save - Allows you to verify and save the current configuration in Basic Mode. A prompt also displays giving you a choice of whether or not to activate the configuration.</p> <p>Note: After clicking <b>Save</b>, a notification icon in the upper right corner of the screen indicates the configuration still needs to be activated. You can continue to make changes to the configuration as required. When finished, you can select <b>Notifications</b> &gt; <b>Save changes</b> to save and activate the configuration. The notification icon is inactive after saving and activating.</p>
	<p>Show advanced - The system displays this button in a configuration dialog that provides advanced parameters. When you click Show advanced, the system displays advanced parameters in the dialog in italics and the button toggles to Hide Advanced.</p>
	<p>Hide advanced - The system displays this button in a configuration dialog that provides advanced parameters. When you click Hide advanced, the system hides the advanced parameters from view, and the button toggles to a Show advanced button.</p>

## Basic Mode Configuration Buttons and Dialogs

In Basic mode, the Configuration tab toolbar displays the following buttons that lead to the corresponding sets of configuration dialogs.







Buttons	Configuration Dialogs
Wizards	<ul style="list-style-type: none"> <li>• Set boot parameters</li> <li>• Set entitlements</li> <li>• Set initial configuration</li> <li>• Set license</li> <li>• Set time zone</li> <li>• Upgrade software</li> </ul>
Settings	<ul style="list-style-type: none"> <li>• Hostname and default gateway</li> <li>• NTP IP address</li> <li>• Enable restart on critical failure</li> <li>• Logging settings</li> <li>• SNMP settings</li> <li>• SIP settings</li> <li>• Denial of Service settings</li> <li>• Communications monitoring probe settings</li> <li>• High availability settings</li> <li>• Packet capture settings</li> <li>• Survivability</li> </ul>
Network	<ul style="list-style-type: none"> <li>• Host route</li> <li>• Network interface</li> </ul>
Security	<ul style="list-style-type: none"> <li>• Certificate record</li> <li>• SDES profile</li> <li>• TLS profile</li> </ul>
Management	<ul style="list-style-type: none"> <li>• Accounting</li> <li>• SNMP community</li> <li>• Trap receiver</li> <li>• Web server</li> </ul>
Other	<ul style="list-style-type: none"> <li>• Media profile</li> <li>• Translation rules</li> <li>• SIP features</li> <li>• SIP manipulations</li> <li>• SPL</li> </ul>








## Device Icons Toolbar

The system displays drag-and-drop icons on the Devices tool bar in the Basic mode workspace for configuring the system in the network.



The following table describes each icon on the Devices toolbar.

Element	Description
Elements for Enterprise	When adding any of the Enterprise elements below, a dialog box displays for you to configure the device.

Element	Description
	<p>PBX - Drag-and-drop icon Adds a Private Branch Exchange (PBX) to your Enterprise network. A PBX is a privately owned telephone switching system for handling multiple telephone lines. Users of the PBX share a certain number of outside lines for making telephone calls external to the PBX.</p>
	<p>Device - Drag-and-drop icon Adds a network device (router, media device, phone, etc.) to your Enterprise network. A device can be any network device used to setup the Enterprise Local Area Network (LAN).</p>
	<p>Recording Server - Drag-and-drop icon Adds a session recording server (SRS) to your Enterprise network. An SRS is a 3rd party call recorder or the Net-Net ISR's Record and Store Server (RSS)). It controls the recording of media transmitted in the context of a communications session between multiple user agents.</p>
	<p>SIP Network Interface - Drag-and-drop icon Adds a Session Initiation Protocol (SIP) network interface to the Enterprise side of the Oracle Enterprise Session Border Controller. You can add up to five (5) SIP interfaces.</p>
<div style="border-left: 2px solid #0070C0; padding-left: 10px;"> <p> <b>Note:</b> You can associate a SIP interface to any configured network interface.</p> </div>	
<p>Elements for Service Provider</p>	<p>When adding any of the Service Provider elements below, a dialog box displays for you to configure the device.</p>
	<p>Trunk - Drag-and-drop icon Adds a SIP Trunk to the Service Provider network. A SIP trunk is a service offered to Enterprises by a Service Provider that permits the Enterprises with PBXs installed, to use IP communications (including Voice over IP (VoIP)) outside of their Enterprise network on an Internet connection.</p>

Element	Description
	<p>Remote Worker - Drag-and-drop icon Adds a Remote Worker to the Service Provider network.</p> <p>A Remote Worker is a device that is setup outside the network but is still connected to the Oracle Enterprise Session Border Controller from the remote location.</p>
	<p>SIP Network Interface - Drag-and-drop icon Adds a SIP network interface to the Service Provider side of the Oracle Enterprise Session Border Controller. You can add up to five (5) SIP interfaces.</p>
<p> <b>Note:</b> You can associate a SIP interface with any configured network interface.</p>	
<p>Elements for Both</p>	
	<p>Selection Tool - Select this then click on any element in your workspace. This tool allows you to select any element in your network.</p>
	<p>Image Mover - Select this then click on the image in your workspace. This tool allows you to move the entire image of your network around within the workspace.</p>
	<p>Two-Way Local Policy - Select this first then click on the center of an icon in your network. This tool allows you to create a two-way route (local policy) between devices within your local network, or between the devices on the Enterprise side and the Service Provider side. When adding a two-way route, a dialog box displays for you to configure the route.</p>
	<p>One-Way Local Policy - Select this first then click on the center of an icon in your network. This tool allows you to create a one-way route between devices within your local network, or between the devices on the Enterprise side and the Service Provider side. When adding a one-way route, a dialog box displays for you to configure the route.</p>



Element	Description
	<p>Grouping Tool - Select the devices in your network that you want to group, then select the grouping tool. This tool allows you to create a grouping around like devices in your network (i.e., multiple PBXs, multiple routers, etc.). When creating a group, a dialog box displays for you to configure the group.</p>
	<p>Ungrouping Tool - Select the group you want to ungroup first, then select the ungrouping tool to ungroup the devices. This tool allows you to remove a grouping from around like devices in your network (i.e., multiple PBXs, multiple routers, etc.). When removing a group, the group configuration information is removed (not the device configurations within the group).</p>

As you place an element in the workspace, the element connects to the SIP interface on the Oracle Enterprise Session Border Controller automatically, and a configuration dialog box displays allowing you to configure the element for your network.

You can use the workspace tools on the upper right corner of the screen to zoom in, zoom out, display actual size, or print the current screen.

 **Note:**

For more information about the workspace tools, see [Workspace Tools](#).

## Device Icon Connection Matrix

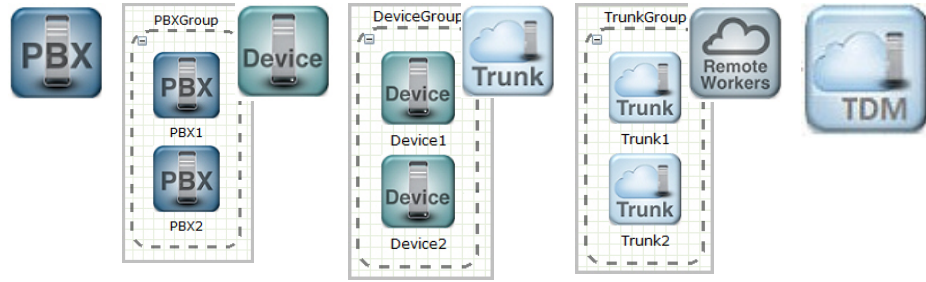
Before configuring the Oracle Enterprise Session Border Controller (E-SBC) from the Web GUI workspace, you need to know the types of connections that the system supports between device icons.

The Web GUI Basic mode workspace supports connections between Enterprise and Service Provider device icons in two ways. You can configure a one-way route or a two-way route between devices. The configured route is called a local policy. You can also connect certain device icons by way of the Advanced Routing icon located on the E-SBC graphic.

The following matrices show the device icons and their supported connections for a one-way policy, for a two-way policy, and for advanced routing. The Recording Server icon is not included here because you cannot route one by way of local policy.

### One-Way Routing Local Policy

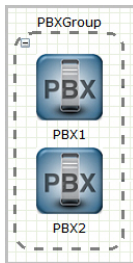
From	To



Yes Yes Yes Yes Yes Yes No Yes



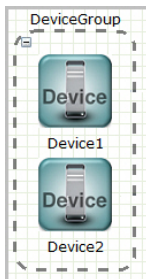
Yes Yes Yes Yes Yes Yes No Yes



Yes Yes Yes Yes Yes Yes No Yes



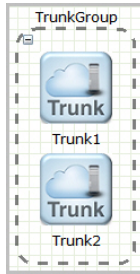
Yes Yes Yes Yes Yes Yes No Yes



Yes Yes Yes Yes No No No Yes



Yes Yes Yes Yes No No No Yes



Yes Yes Yes Yes No No No No

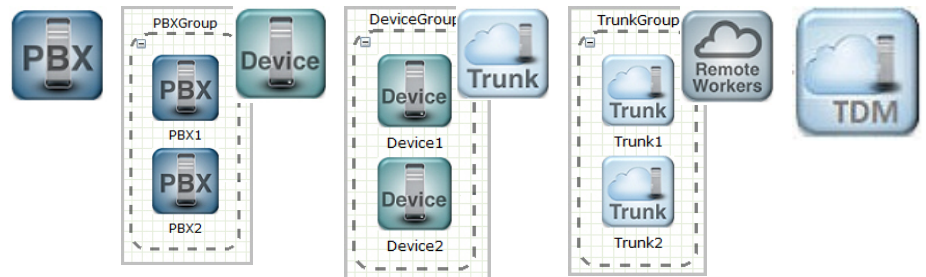


Yes Yes Yes Yes Yes Yes No Yes



**Two-Way Routing Local Policy**

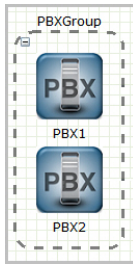
From To



Yes Yes Yes Yes Yes Yes No Yes



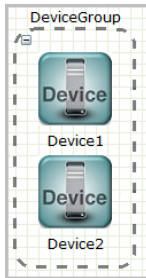
Yes Yes Yes Yes Yes Yes No Yes



Yes Yes Yes Yes Yes Yes No Yes



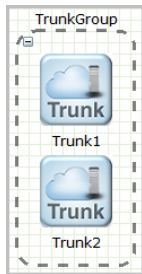
Yes Yes Yes Yes Yes Yes No Yes



Yes Yes Yes Yes No No No Yes



Yes Yes Yes Yes No No No Yes



No No No No No No No No



Yes Yes Yes Yes Yes Yes No Yes



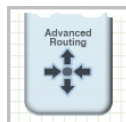

---

**Advanced Routing Local Policy**

---

From

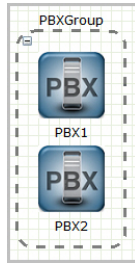
To



Yes



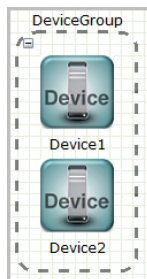
Yes



Yes



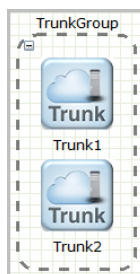
Yes



Yes



Yes



No



Yes



## Network Configuration Using the Workspace Icons

You can configure the network by dragging-and-dropping the icons from the Device tool bar onto the Basic mode workspace below the titles of Enterprise Side and Service Provider Side. After you drop the icon onto the workspace, click the icon to display the corresponding configuration dialog.

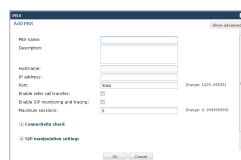
The following steps describe the process for configuring a typical network by way of the Web GUI in Basic mode.

1. Drag the PBX icon to the Enterprise Side, and complete the Add PBX dialog.
2. Drag the SIP Trunk icon to the Service Provider Side, and complete the Add SIP Trunk dialog.
3. Click the two-way Routing icon, click the center of the PBX icon, drag to the center of the SIP Trunk icon, and complete the Add Two-Way Route Information dialog.
4. Click the Network button, click Network Interface, and confirm that the Network Interface on the Oracle Enterprise Session Border Controller is correct on the Enterprise and Service Provider sides.
5. Save and Activate the configuration.

### Add a PBX

To add a PBX to the Enterprise side:

1. Click on the **PBX** icon in the device tool bar, and drag it to the Enterprise side in the workspace. The following dialog box displays.



2. In the **PBX name** field, enter the name to assign to this PBX in the Enterprise network. For example, PBX1. Valid values are alpha-numeric characters.

3. (optional) In the **Description** field, enter a description for this PBX. For example, PBX for Enterprise. Valid values are alpha-numeric characters.
4. In the **Hostname** field, enter the hostname of the Oracle Enterprise Session Border Controller to which this PBX is connected. For example, ESD1. Valid values are alpha-numeric characters.
5. (optional) In the **IP address** field, enter the IP address of this PBX. Enter the address in dotted decimal format. For example, 1.1.1.1. Default is 0.0.0.0.

#### Note:

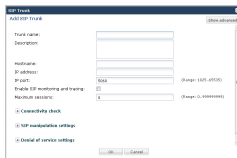
By default, the Port on the PBX is 5060. Also, setting all other parameters in this dialog box is optional. If you want to modify the values of the remaining parameters, or if you want to set more advanced parameters, see the *Net-Net® Enterprise Session Director Configuration Guide* for more information. Oracle recommends that only Administrators add or modify advanced parameters.

6. Click <OK> to save your settings. The PBX displays in your Enterprise workspace with the name of the PBX displayed beneath the icon. You can edit the PBX configuration anytime if required, by double-clicking the icon and modifying the configuration in the dialog box.

## Add a Trunk

To add a SIP Trunk to the Service Provider side:

1. Click on the **Trunk** icon in the device tool bar, and drag it to the Service Provider side in the workspace. The following dialog box displays.



2. In the **Trunk name** field, enter the name to assign to this SIP Trunk in the Service Provider network. For example, TrunkA. Valid values are alpha-numeric characters.
3. (optional) In the **Description** field, enter a description for this SIP Trunk. For example, Trunk between SP and Ent. Valid values are alpha-numeric characters.
4. In the **Hostname** field, enter the hostname of the Oracle Enterprise Session Border Controller to which this Trunk is connected. For example, ESD1. Valid values are alpha-numeric characters.
5. (optional) In the **IP address** field, enter the IP address of this SIP Trunk. Enter the address in dotted decimal format. For example, 2.2.2.2. Default is 0.0.0.0.



 **Note:**

By default, the IP Port on the SIP Trunk is 5060. Setting all other parameters in this dialog box is optional. If you want to modify the values of the remaining parameters, or if you want to set more advanced parameters, see the *Net-Net® Enterprise Session Director Configuration Guide* for more information. Oracle recommends that only Administrators add or modify advanced parameters.

6. Click <OK> to save your settings. The Trunk displays in your Enterprise workspace with the name of the Trunk displayed beneath the icon. You can edit the Trunk configuration anytime if required, by double-clicking the icon and modifying the configuration in the dialog box.

## Add a One-Way Local Routing Policy

You can perform the minimum configuration needed to add a one-way local routing policy to the Oracle Enterprise Session Border Controller (E-SBC) from the Configuration tab in Basic mode.

### Before You Begin

- Note the IP addresses of the devices that you want to affect with this policy.
- Confirm that the system displays the Basic mode.

This procedure provides an example of creating a one-way local route policy between two network devices, the PBX and the Trunk. You can perform this procedure between other elements of the network, such as other Devices and Remote Workers.

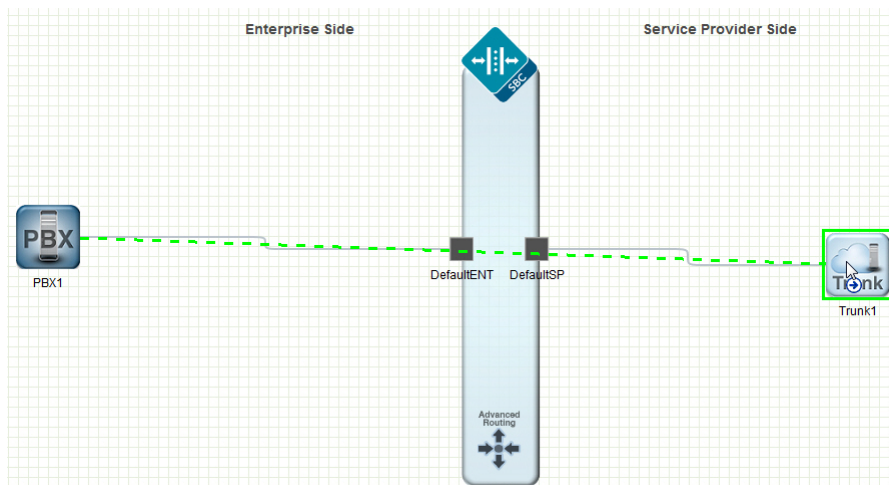
Drag and drop the one-way routing icon from the device toolbar onto the PBX icon and connect it to the Trunk icon. The system displays the Add One-Way Route Information dialog, where you enter the local routing policy parameters. After you perform the configuration and click **OK** in the Add One-Way Route Information dialog. The one-way route icon persists on the workspace. You can edit the local policy configuration any time by double-clicking the icon and modifying the configuration in the Modify One-Way Route Information dialog box. Save and activate the configuration after the initial configuration and after modifying the configuration.

### Procedure

1. From the Device toolbar, click the one-way arrow.  
The system frames the icon to indicate that it is ready to drag and drop.
2. Click center of the PBX icon on the Enterprise side of the E-SBC. The system displays a small arrow.



3. From the center of the PBX icon, hold down the left mouse button and drag to the center of the Trunk icon on the Service Provider side of the E-SBC. Release the left mouse button.



The system draws a one-way arrow between the PBX and the Trunk, displays a green border around the Trunk icon, and launches the Add One-Way Route Information dialog .

4. In the Add One-Way Route Information dialog, do the following:

Attributes	Instructions
Route name	Enter a name for this route. For example, Route A.
Route cost	Range: 999999999
From address	<ol style="list-style-type: none"> <li>a. Click <b>Add</b>, and enter the IP address of the PBX.</li> <li>b. Click <b>OK</b>.</li> </ol>
To address	<ol style="list-style-type: none"> <li>a. Click <b>Add</b>, and enter the IP address of the Trunk.</li> <li>b. Click <b>OK</b>.</li> </ol>

5. Click **OK**

The system displays the one-way route icon on the workspace with a connector line between the PBX and the Trunk icon.

6. Save and activate the configuration.

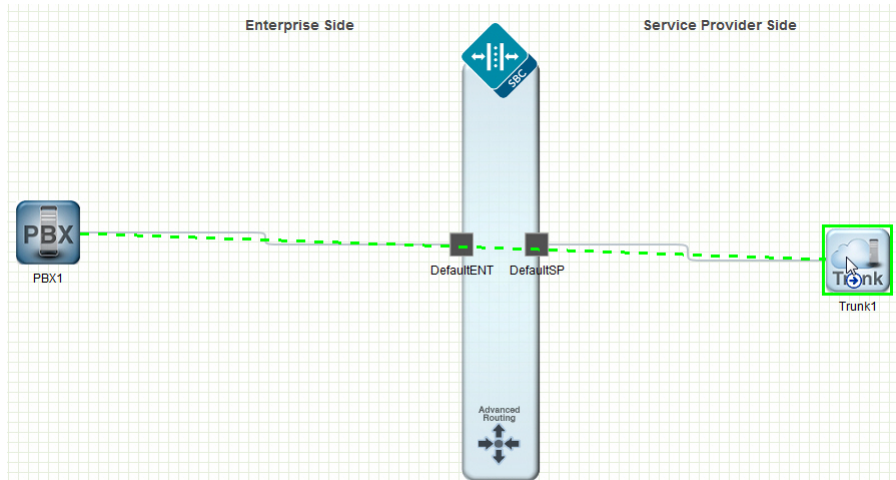
## Add a Local Policy

To add a Local Policy (2-way route) between the PBX and the SIP Trunk:

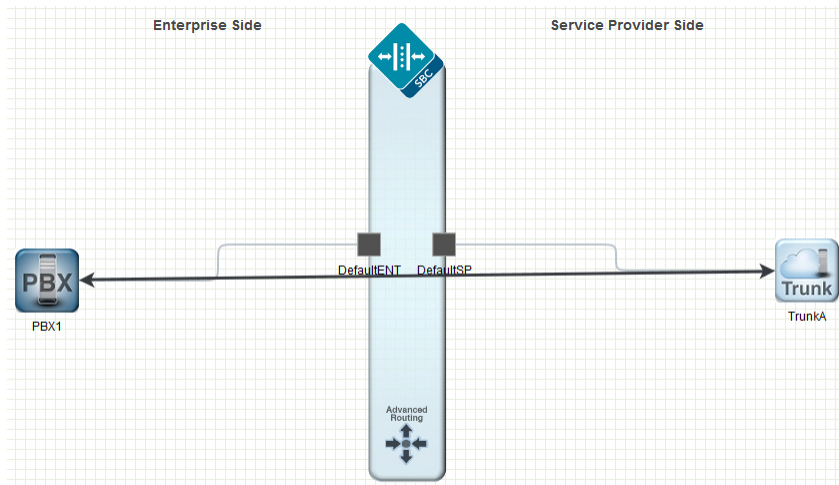
1. In the connectors section of the device tool bar, click on the 2-way arrow to select it.
2. Click in the center of the PBX icon in the Enterprise network. A small arrow displays.



3. Holding down the left mouse button, drag the mouse over to the Trunk icon, making sure a green border appears around the Trunk icon.



4. Release the left mouse button. This draws a 2-way arrow (local-policy) between the PBX and the Trunk. A dialog box displays.



5. In the **Route name** field, enter a name for this route. For example, RouteA.
6. Click **<OK>**. You can edit the local policy configuration anytime if required, by double-clicking the 2-way arrow and modifying the configuration in the dialog box.

 **Note:**

If you want to modify the values of the remaining parameters, or if you want to set more advanced parameters, see the ACLI Configuration Guide for more information.

## Configure Advanced Routing

After adding a one-way or two-way local policy route, you can configure the routes with more advanced parameters from the Web GUI.

In the Advanced Routing dialog, configure the advanced routing parameters that you want and add the corresponding LDAP configuration.

1. Click the Advanced Routing icon on the Oracle Enterprise Session Border Controller.
2. In the local-routing-config dialog, click **Add** and **Show Advanced**.
3. In the Add local routing config dialog, do the following:

- Name. Enter a unique name for the local route table. No spaces.
  - File name. Enter or select the name for the file from which the database corresponding to this local route table will be created. You should use the .gz format, and the file should be placed in the /code/lrt/ directory.
  - Prefix length. Enter a number from 0-999999999.
  - String lookup. Optional. Selection.
  - Re-target requests. Optional selection.
  - Match mode. Select a mode from the drop down list.
4. Click **OK**.
  5. Click **Close**.

Configure LDAP.

## Configure LDAP

The Oracle Enterprise Session Border Controller (E-SBC) uses Lightweight Directory Access Protocol (LDAP) for interaction between an LDAP client and an LDAP server. Use the ldap-config tab in the Advanced routing dialog in Basic mode to create and enable an LDAP configuration on the E-SBC.

### Before You Begin

- Confirm that one or more authentication modes exist.
- Confirm that one or more Transport Layer Security (TLS) profiles exist.
- Confirm that the system displays the Basic mode.

### Procedure

In the following procedure, you configure the LDAP server, filters, security, and local policy.

1. From the Web GUI, click **Configuration > Advanced Routing icon > ldap-config tab**.
2. On the LDAP config page, click **Add**.
3. On the Add LDAP config page, click **Show advanced**, and do the following:

Attributes	Instructions
Name	Enter a unique name to identify this configuration. Valid values are alpha-numeric characters.
State	Select State to enable this configuration. When not selected, the E-SBC does not attempt to establish a connection with any corresponding LDAP server.
LDAP servers	Click <b>Add</b> , enter the name of the LDAP server, and do one of the following: <ul style="list-style-type: none"> <li>• Click <b>OK</b>.</li> <li>• Click <b>Apply/Add another</b>, add another LDAP server, and click <b>OK</b>. Repeat, as needed.</li> </ul>
SIP interface	Select the SIP interface for this configuration.
Authentication mode	Select the authentication mode for the LDAP bind request from the drop-down list.

Attributes	Instructions
Username	Enter the username that the LDAP bind request uses for authentication before the LDAP server grants access.
Password	Click <b>Set</b> , enter and confirm the password to pair with the Username that the LDAP bind request uses for authentication before the LDAP server grants access. Click <b>OK</b> .
LDAP search base	Enter the base Directory Number for LDAP search requests.
Timeout limit	Enter a timeout limit in seconds. The range is from 1-300.
Max request timeouts	Enter the maximum number of timeouts allowed. The range is from 0-10.
TCP keepalive	Select TCP keepalive to enable Transmission Control Protocol (TCP) keepalive signalling.
LDAP sec type	Select None or LDAPS for the type of LDAP security from the drop down list.
LDAP TLS profile	Select a TLS profile for this LDAP configuration.
LDAP transactions	Click <b>Add</b> to add allowed LDAP transaction types to the list. The system displays the Add LDAP config / LDAP transactions configuration page, where you select the application transaction layer type, the route mode, operation type, and add LDAP configuration attributes.

4. Click **OK**.
5. Save and activate the configuration.

## TDM Configuration

Time Division Multiplexing (TDM) is an option that requires configuration. You must enable TDM on the device, specify the parameters for the TDM interface properties, and configure local policies for inbound and outbound TDM traffic. Two-way TDM call routing requires both inbound and outbound local policies. For inbound-only or outbound-only TDM call routing, the system requires a local policy only for the call direction that you want.

You can configure TDM from either the Acme Command Line Interface (ACLI) or the Web GUI.

- ACLI. Use the `tdm-config` object from the system group of elements.
- Web GUI - Basic mode. Double-click the TDM icon in the network diagram to display the TDM configuration dialog.
- Web GUI - Expert mode. Use the `tdm-config` object from the system group of objects.

In addition to configuring the TDM interface properties, you must configure an inbound local policy for traffic entering the TDM interface and an outbound local policy for traffic exiting the TDM interface. In the inbound local policy, you specify `tdmRealm` for the source realm. In the outbound local policy, you specify the next hop that you want for TDM traffic.

The TDM card always supports bidirectional calls, but TDM call routing can be unidirectional. For example, for inbound-only operations, configure the TDM interface and configure only the inbound TDM policy.

If you upgrade from a previous release in which you configured outbound TDM and you want to add inbound TDM, you need only to create the local TDM policy for inbound TDM calls.

You can configure TDM to support either the T1 line mode or the E1 line mode. You can configure all TDM properties, except for line mode, in realtime. For example, changing the default T1 line mode to the E1 line mode requires a system reboot.

After configuring TDM, you must save and activate the configuration. Activating the TDM configuration generates the tdm-config template, which you can view by way of the `show running-config generated` command. except for line mode

 **Note:**

The TDM configuration template includes the media-sec-policy object only when the SRTP license is activated. See "Licensing for Time Division Multiplexing (TDM)."

## Configure TDM - Basic

You can configure Time Division Multiplexing (TDM) from the Configuration page on the Web GUI in Basic Mode.

- You must have Superuser permissions.
- Confirm that the optional TDM card is present in the device.
- Confirm that logging is enabled for the system, if you want to enable TDM logging in this procedure.

To activate TDM, you must enable TDM and create a profile that specifies the TDM interface. The following procedure is provided as an example of a typical configuration. In this procedure, some profile parameters are specific to the selected line mode. For example, if you select the T1 line mode, you must select 1-23 for B channel. Configure the remaining settings according to the requirements of your deployment.

For signalling, use one of the following settings:

- `pri_net`, if you want the TDM card to use the internal clock as the source for timing.
- `pri_cpe`, if you want the TDM card to use an external clock as the source for timing.

1. From the Web GUI in Basic mode, and click the Configuration tab.

The system displays the TDM icon on the network diagram.

2. Double-click the TDM icon.

The system displays the TDM configuration dialog.

3. Select **State** to enable TDM.
4. (Optional) Select **Logging** to enable logging.
5. Click `tdm-profile` to display the property fields for the TDM profile.
6. Configure values for the following TDM profile parameters:
  - a. Name. Enter a name for this TDM profile.
  - b. Select T1 or E1.
  - c. Signaling. Select either `pri_net` or `pri-cpe`.
  - d. Switch type. Select a switch type for this configuration.

- e. B channel. For T1, select 1-23. For E1, select 1-15,17-31.
  - f. D channel. For T1, select 24. For T1, select 16.
  - g. Span number. Enter 0.
  - h. Line build out. Enter a number from 0 to133.
  - i. Framing value. For T1, select ESF. For E1, select CCS.
  - j. Coding value. For T1, select b8zs. For E1, select hdb3.
  - k. Tone zone. For T1, select US. For E1, select ES.
  - l. Rx gain. Optional—Set the TDM Receive channel volume in decibels. Maximum value is 9.9.
  - m. Tx gain. Optional—Set the TDM Transmit channel volume in decibels. Maximum value is 9.9.
  - n. Echo cancellation. Select to enable.
7. Click **OK**.
  8. Save and activate the configuration.

Configure the inbound and outbound TDM local policies.

## Configure Outbound Local Policy with TDM Backup - Basic

To complete the Time Division Multiplexing (TDM) configuration for redundancy, you must configure the outbound TDM local routing policy.

- Confirm that a TDM configuration exists.
- Confirm that the system displays the Basic mode.

In the following procedure, you must draw the outbound local routing policy arrow from the PBX icon to the Trunk icon because the system supports TDM operations only from the PBX to the Trunk. If you draw the outbound local routing policy arrow from the Trunk icon to the PBX icon, you cannot configure this policy for TDM.

1. From the Web GUI, click **Configuration**.
2. From the icon toolbar, under Routing, click the unidirectional arrow icon.
3. Click the center of the PBX icon.  
The system displays an arrow in the center of the PBX icon.
4. Drag from the arrow in the center of the PBX icon to the Trunk icon.  
The system displays the Add One-Way Route Information dialog.
5. In the Add One-Way Route Information dialog, do the following:
  - a. Route name – Enter a name for this policy. For example, TDM Policy.
  - b. Route cost – Optional. Enter a cost for this routing policy.
  - c. From address – Enter the PBX address.
  - d. To address – Enter the address of the Trunk.
  - e. TDM – Select TDM.
  - f. TDM profile name – Select the TDM configuration profile from the drop down list.
6. Click **OK**.



7. Save and activate the configuration.

## Configure Bidirectional Local Policy with TDM Backup

To complete the Time Division Multiplexing (TDM) configuration for redundancy, you must configure the TDM local routing policy.

### Before You Begin

- Confirm that a TDM configuration exists.
- Confirm that the system displays the Basic mode.

The following procedure assumes drawing the bidirectional local routing policy arrow from the PBX to the Trunk.

### Procedure

1. From the Web GUI, click **Configuration**.
2. From the icon toolbar, under Routing, click the bidirectional arrow icon.
3. Click the center of the PBX icon.

The system displays an arrow in the center of the PBX icon.

4. Drag from the arrow in the center of the PBX icon to the Trunk icon.

The system displays the Add Two-Way Route Information dialog.

5. In the Add Two-Way Route Information dialog, do the following:

Attributes	Instructions
Route name	Enter a name for this policy. For example, TDM Policy.
Route cost	Enter a cost for this routing policy.
Route from PBX to trunk - From address	Enter the PBX address.
Route from PBX to trunk - To address	Enter the address of the Trunk.
TDM	Select TDM.
TDM profile name	Select the TDM configuration profile from the drop down list.
Route from trunk to PBX - From address	Enter the address of the trunk.
Route from trunk to PBX - To address	Enter the address of the PBX.

6. Click **OK**.
7. Save and activate the configuration.

## Configure Outbound TDM Local Policy - Basic

To complete the configuration for outbound Time Division Multiplexing (TDM) operations, you must configure the TDM local routing policy.

### Before You Begin

- Confirm that a TDM configuration exists.
- Confirm that the system displays the Basic mode.

In the following procedure, you must draw the outbound local routing policy arrow from the TDM icon to the Trunk icon. If you draw the outbound local routing policy arrow from the Trunk icon to the TDM icon, you cannot configure this policy for TDM.

**Procedure**

1. From the Web GUI, click **Configuration**.
2. From the icon toolbar, under Routing, click the one-way arrow icon.
3. Click the center of the TDM icon.  
The system displays an arrow in the center of the TDM icon.
4. Drag from the arrow in the center of the TDM icon to the Trunk icon.  
The system displays the Add One-Way Route Information dialog.
5. In the Add One-Way Route Information dialog, do the following:

Attributes	Instructions
Route name	Enter a name for this policy. For example, TDM Policy.
Route cost	Enter a cost for this routing policy.
From address	Enter the TDM address.
To address	Enter the address of the Trunk.

6. Click **OK**.
7. Save and activate the configuration.

## Configure Bidirectional TDM Local Policy

To complete the configuration for inbound and outbound Time Division Multiplexing (TDM) operations, you must configure the TDM local routing policy.

**Before You Begin**

- Confirm that a TDM configuration exists.
- Confirm that the system displays the Basic mode.

The following procedure assumes drawing the bidirectional local routing policy arrow from the TDM to the Trunk.

**Procedure**

1. From the Web GUI, click **Configuration**.
2. From the icon toolbar, under Routing, click the bidirectional arrow icon.
3. Click the center of the TDM icon.  
The system displays an arrow in the center of the TDM icon.
4. Drag from the arrow in the center of the TDM icon to the Trunk icon.  
The system displays the Add Two-Way Route Information dialog.
5. In the Add Two-Way Route Information dialog, do the following:

Attributes	Instructions
Route name	Enter a name for this policy. For example, Two-Way TDM Policy.
Route cost	Enter a cost for this routing policy.
Route from TDM to trunk - From address	Enter the address of TDM.

Attributes	Instructions
Route from TDM to trunk - To address	Enter the address of the Trunk.
Route from trunk to TDM - From address	Enter the address of the Trunk.
Route from trunk to TDM - To address	Enter the address of TDM.

6. Click **OK**.
7. Save and activate the configuration.

## Settings Button

Use the Settings button to access the following configuration elements.

Configuration Element	Purpose
SBC Host Name	Name the session border controller host.
Description	Describe the session border controller host.
Location	Specify the location of the session border controller host.
Default Gateway IP Address	Specify the gateway IP address for the host.
NTP IP Address	Specify the IP address of the Network Time Protocol server.
Enable restart on critical failure	Enable automatic system restart after a critical failure.
Logging Settings	Specify the Syslog server and the process log level.
SNMP Settings	Enable SNMP traps and specify the MIB system.
SIP Settings	Configure SIP and add SIP options.
Denial of Service Settings	Specify packet rate settings for Denial of Service protection.
Communications Monitoring Probe Settings	Enable the Communications Monitoring Probe and specify the collector.
High Availability Settings	Enable High Availability and specify the peers.
Packet Capture Settings	Enable packet capture and specify the receiver.
Survivability	Enable remote site survivability and specify the triggering device.

## Configure System Settings Quick Reference

In Basic mode, use the Settings page to configure the following elements. Click **Show advanced** to display all available elements.

Attributes	Instructions
SBC Host Name	Enter the name of the session border controller host. Alphanumeric.
Description	Enter a description of the SBC host. Alphanumeric.
Location	Enter the location of the SBC host. Alphanumeric.
Default Gateway IP Address	Enter the default gateway IP address for the host. Dot-decimal.
NTP IP Address	Enter the IP address of the Network Time Protocol server. Dot-decimal.

Attributes	Instructions
Enable restart on critical failure	Select to enable an automatic system restart after a critical failure.
Logging Settings	<ul style="list-style-type: none"> <li>• Syslog server IP address. Enter the IP address of the Syslog server.</li> <li>• Process log level. Select the starting log level for all processes running on the system.</li> </ul>
SNMP Settings	<ul style="list-style-type: none"> <li>• MIB system contact. Enter the name of the contact person.</li> <li>• MIB system name. Enter the name of the MIB system.</li> <li>• MIB system location. Enter the MIB system location.</li> <li>• Enable event SNMP traps. Select to enable the E-SBC to report event SNMP traps.</li> </ul>
SIP Settings	<ul style="list-style-type: none"> <li>• Enable dialog transparency. Select to enable.</li> <li>• Allow SIP UDP fragmentation. Select to enable.</li> <li>• Set INVITE expires at 100 response. Select to enable.</li> <li>• Sip options. Click <b>Add</b>, enter one or more SIP options.</li> </ul>
Denial of Service Settings	<ul style="list-style-type: none"> <li>• Maximum trusted packet rate. Enter a number from 20-200000.</li> <li>• Maximum untrusted packet rate. Enter a number from 20-200000.</li> <li>• Maximum ARP packet rate. Enter a number from 20-10000.</li> </ul>
Communications Monitoring Probe Settings	<ul style="list-style-type: none"> <li>• Enable monitoring. Select to enable.</li> <li>• SBC group ID.</li> <li>• Network interface. Select an interface from the drop down list.</li> <li>• Collector IP address. Enter the IP address.</li> <li>• Collector port. Enter a number from 1025-65535.</li> </ul>
High Availability Settings	<ul style="list-style-type: none"> <li>• Enable high availability. Select to enable.</li> <li>• Name of primary peer. Enter a name for the primary.</li> <li>• Name of secondary peer. Enter a name for the secondary.</li> <li>• ENT phy interface virtual MAC. Enter the enterprise MAC address.</li> <li>• SP phy interface virtual MAC. Enter the MAC service provider address.</li> </ul>
Packet Capture Settings	<ul style="list-style-type: none"> <li>• Enable packet capture. Select to enable.</li> <li>• Capture receiver network Interface. Select an interface from the drop down list.</li> <li>• Capture receiver IP address. Enter the IP address.</li> </ul>

Attributes	Instructions
Survivability	<ul style="list-style-type: none"> <li>• State. Select to enable.</li> <li>• Registration expire time. Enter a number from 0-86400.</li> <li>• Extension length. Enter a number from 0-10.</li> <li>• Trigger on. Select a device from the drop down list.</li> </ul>

## Logging Settings

You can configure the Oracle Enterprise Session Border Controller (E-SBC) to generate Syslogs for system management and Process logs for debugging.

The E-SBC generates the following types of logs.

- Syslogs conform to the standard used for logging servers and processes as defined in RFC 3164. In configuration, you specify the Syslog server.
- Process logs are proprietary Oracle logs that the system generates on a per-task basis and are used mainly for debugging purposes. Because process logs are more data inclusive than Syslogs, their contents usually include Syslog log data. In configuration, you specify the log level.

Syslog and process log servers are both identified by an IPv4 address and port pair.

## Configure Logging Settings

The Oracle Enterprise Session Border Controller (E-SBC) generates SysLogs and process logs. You must configure the IP address for the SysLog server and the process log level for the process logs.

### Before You Begin

- Note the IP address of the Syslog server.
- Confirm that the system displays the Basic mode.

The Web GUI displays the logging configuration parameters on the Settings page. Use the following procedure to specify the Syslog server and to select a process log level.

### Procedure

1. From the Web GUI, click **Settings**.
2. In the Settings dialog, click **Logging settings**, and do the following:

Attributes	Instructions
SysLog server IP address	Enter the IPv4 address of the SysLog server.
Process log level	Select the starting log level of all processes running on the E-SBC.

3. Click **OK**.
4. Save and activate the configuration.

## Simple Network Management Protocol

Simple Network Management Protocol (SNMP) supports the monitoring of devices attached to the network for conditions that might need administrative attention.

On the Oracle Enterprise Session Border Controller (E-SBC), SNMP configuration is comprised of the following groups of system-wide settings.

- SNMP settings. Specifies the MIB contact information and enables event SNMP traps. See "Configure SNMP Settings."
- SNMP community. Specifies how certain E-SBC events are reported. See "Configure SNMP Community."
- Trap receiver. Specifies the trap receiver settings, including filters. See "Configure an SNMP Trap Receiver."

The system does not require you to configure these groups of settings for baseline E-SBC service. If you want to use network management systems to provide important monitoring and system health information, configure the settings.

## Configure SNMP Settings

Simple Network Management Protocol (SNMP) is used to support the monitoring of devices attached to the network, such as the Oracle Enterprise Session Border Controller (E-SBC), for conditions that warrant administrative attention.

### Before You Begin

- Confirm that the system displays the Basic mode.

The Web GUI displays the SNMP settings configuration parameters on the Settings page. Use the following procedure to configure MIB settings and to enable SNMP for the E-SBC.

### Procedure

1. From the Web GUI, click **Settings**.
2. In the Settings dialog, click **SNMP settings** > **Show advanced**, and do the following:

Attributes	Instructions
MIB system contact	Enter the contact information to use in the E-SBC MIB transactions.
MIB system name	Enter the identification of this E-SBC presented in MIB transactions.
MIB system location	Enter the physical location of this E-SBC that is reported within MIB transactions.
Enable event SNMP traps	Select to enable the E-SBC to report event SNMP traps.

3. Click **OK**.
4. Save and activate the configuration.

## SIP Settings

Session Initiation Protocol (SIP) is an IETF-defined signaling protocol widely used for controlling communication sessions such as voice and video calls over Internet Protocol (IP).

The protocol can be used for creating, modifying and terminating two-party (unicast) or multiparty (multicast) sessions. Sessions may consist of one or several media streams.

### Dialog Transparency

Dialog transparency prevents the Oracle Enterprise Session Border Controller (E-SBC) from generating a unique Call-ID and modifying dialog tags. With dialog transparency enabled, the E-SBC is prevented from generating a unique Call-ID and from modifying the dialog tags. The Oracle Enterprise Session Border Controller passes what it receives. When a call made on one E-SBC is transferred to another UA and crosses a second E-SBC, the second E-SBC does not note the context of the original dialog, and the original call identifiers are preserved end to end. The signalling presented to each endpoint remains in the appropriate context regardless of how many times a call crosses through a E-SBC or how many E-SBCs a call crosses.

Without dialog transparency enabled, the E-SBC SIP B2BUA rewrites the Call-ID header and inserted dialog cookies into the From and To tags of all messages it processes. These dialog cookies are in the following format: SDxxxxxNN-. Using these cookies, the E-SBC can recognize the direction of a dialog. However, this behavior makes call transfers problematic because the Call-ID of one E-SBC might not be properly decoded by another E-SBC. The result is asymmetric header manipulation and unsuccessful call transfers.

### IPv6 Reassembly and Fragmentation Support

As it does for IPv4, the E-SBC supports reassembly and fragmentation for large signaling packets when you enable IPV6 on the system.

The E-SBC takes incoming fragments and stores them until it receives the first fragment containing a Layer 4 header. With that header information, the E-SBC performs a look-up so it can forward the packets to its application layer. Then the packets are re-assembled at the applications layer. Media fragments, however, are not reassembled and are instead forwarded to the egress interface.

On the egress side, the E-SBC takes large signaling messages and encodes it into fragment datagrams before it transmits them.

Note that large SIP INVITE messages should be sent over TCP. If you want to modify that behavior, you can use the SIP interface's option parameter `max-udplength=xx` for each SIP interface where you expect to receive large INVITE packets.

Other than enabling IPv6 on your E-SBC, there is no configuration for IPv6 reassembly and fragmentation support. It is enabled automatically.

## Configure SIP Settings

Use the Settings button to access the SIP settings configuration section of the Settings page.

### Before You Begin

- Confirm that the system displays the Basic mode.

Use the following procedure to configure global SIP settings and options.

### Procedure

1. From the Web GUI, click **Settings**.
2. On the Settings page, click **SIP settings > Show advanced**, do the following.

Attributes	Instructions
Enable dialog transparency	Select to enable.
Maximum SIP message length	Enter the maximum SIP message length. Default: 4096. Range: 0-65535.
Allow SIP UDP fragmentation	Select to enable.
Set INVITE expires at 100 responses	Select to enable.
Options	Click <b>Add</b> , enter a SIP option, and do one of the following: <ul style="list-style-type: none"> <li>Click <b>OK</b>.</li> <li>Click <b>Apply/Add another</b>, add another media attribute, and click <b>OK</b>. Repeat, as needed.</li> </ul>

- Click **OK**.
- Save and activate the configuration.

#### Next Steps

- Configure SIP Features.

## Denial of Service Protection

The Oracle Enterprise Session Border Controller (E-SBC) Denial of Service (DoS) protection functionality protects soft switches and gateways with overload protection, dynamic and static access control, and trusted device classification and separation in layers 3-5.

DoS protection prevents the E-SBC host processor from being overwhelmed by a targeted DoS attack from the following:

- IP packets from an untrusted source, as defined by provisioned and dynamic ACLs
- IP packets for unsupported and disabled protocols
- Nonconforming and malformed packets to signaling ports
- Volume-based attack of valid and invalid call requests, signaling messages, and so on.

The Server Edition and VM Edition support of DoS protection differs from the Oracle Hardware Platforms Edition due to the absence of Oracle network interface hardware. Consequently, DoS protection is implemented in software and consumes CPU cycles when responding to attacks.

The Server Edition and VM Edition handle media packet fragments differently, processing them in the data path rather than in the host application code. Protection against fragment attacks occurs because the system never keeps fragments for more than 5 milliseconds.

## Configure Denial of Service Settings

Configure Denial of Service (DoS) settings to protect the Oracle Enterprise Session Border Controller (E-SBC) from signal and media overload, while allowing legitimate, trusted devices to continue receiving service during an attack.

#### Before You Begin

- Plan the maximum number of packets per second that you want for trusted packets, untrusted packets, and ARP packets.
- Confirm that the system displays the Basic mode.



The Web GUI displays the denial of service configuration parameters on the Settings page. Use the following procedure to specify the settings that the system uses to calculate the trusted, untrusted, and ARP packets per second. Note that the configured rate is specified in packets per second, but the system measures the rate in packets per millisecond. For example, when the configured rate is 3200 packets per second, the actual measured rate is 3 packets per millisecond.

#### Procedure

1. From the Web GUI, click **Configuration > Settings**.
2. On the settings page, click **Denial of Service settings > Show advanced**, and do the following.

Attributes	Instructions
Maximum trusted packet rate	Maximum bandwidth for trusted hosts. Packets per second. Default 50000. Range: 20-200000.
Maximum untrusted packet rate	Maximum bandwidth for un-trusted hosts. Packets per second. Default 50000. Range: 20-200000.
Maximum ARP packet rate	Maximum bandwidth for ARP. Packets per second. Default 1000. Range: 20-10000.

3. Click **OK**.
4. Save and activate the configuration.

## Communication Monitoring Probe Settings

Palladion is the Oracle Communication Experience Manager.

The manager is powered by the Palladion Mediation Engine, a platform that collects SIP, DNS, ENUM, and protocol message traffic received from Palladion Probes. The mediation engine stores the traffic in an internal database, and analyzes aggregated data to provide comprehensive multi-level monitoring, troubleshooting, and interoperability information.

Palladion simplifies the operation of software-based Palladion probes by enabling the transmission of Internet Protocol Flow Information Export (IPFIX) data to one or more Palladion Mediation Engines, possibly on different sub-nets.

#### Note:

The Palladion Communications Monitor Probe communicates over the media interface for signaling and Quality of Service (QoS) statistics using IPFIX. QoS reporting is done by way of Call Detail Records (CDR) accounting.

## Configure Communication Monitoring Probe Settings

Use the following procedure to establish a connection between the Oracle Enterprise Session Border Controller (E-SBC) and the Palladion Mediation Engine. The E-SBC is the exporter of protocol message traffic and data and the Palladion Mediation Engine is the information collector.

#### Before You Begin

- Confirm that the network interface that you want to monitor is configured.
- Confirm that the system displays the Basic mode.

The Web GUI displays the communication monitoring probe settings configuration parameters on the Settings page. Use the following procedure to enable this function, and to specify the connection parameters.

#### Procedure

1. From the Web GUI, click **Configuration > Settings**.
2. On the Settings page, click **Communications Monitoring Probe Settings > Show advanced**, and do the following:

Attributes	Instructions
Enable monitoring	Select to enable.
SBC group ID	Enter a number to assign to the E-SBC in its role as an information exporter. Range: 0-999999999.
Network interface	Select a network interface from the drop down list that supports the TCP connection between the E-SBC and the Palladion Mediation Engine.
Collector IP address	Enter the IP address of the Palladion Mediation Engine collector. Default: 0.0.0.0.
Collector port	Enter the number of the Palladion Mediation Engine collector port from 1025-65535. Default: 4739. Range: 1025-65535.

3. Click **OK**.
4. Save and activate the configuration.

## High Availability Settings

You can deploy the Oracle Enterprise Session Border Controller (E-SBC) in pairs to deliver High Availability (HA). Two E-SBCs operating in this way are called an HA node. Over the HA node, call state is shared, keeping sessions and calls from dropping in the event of a service disruption.

Two E-SBCs work together in an HA node, one in active mode and one in standby mode.

- The active E-SBC checks itself for internal process and IP connectivity issues. If it detects that it is experiencing certain faults, it hands over its role as the active system to the standby E-SBC in the node.
- The standby E-SBC is the backup system, fully synchronized with the active E-SBC session status. The standby E-SBC monitors the status of the active system so that, if needed, it can assume the active role without the active system having to instruct it to do so. If the standby system takes over the active role, it notifies network management using an SNMP trap.

To produce seamless switch overs from one E-SBC to the other, the HA node uses shared virtual MAC and virtual IP addresses for the media interfaces in a way that is similar to Virtual Router Redundancy Protocol (VRRP). Sharing addresses eliminates the possibility that the MAC and IPv4 address set on one E-SBC in an HA node will be a single point of failure. The standby E-SBC sends ARP requests using a utility IPv4 address and its hard-coded MAC addresses to obtain Layer 2 bindings.

When there is a switch over, the standby E-SBC issues gratuitous ARP messages using the virtual MAC address, establishing that MAC on another physical port within the Ethernet switch. To the upstream router, the MAC and IP are still alive, meaning that existing sessions continue uninterrupted.

Within the HA node, the E-SBCs advertise their current state and health to one another in checkpointing messages; each system is apprised of the other's status. Using Oracle's HA protocol, the E-SBCs communicate with UDP messages sent out and received on the interfaces carrying "heartbeat" traffic between the active and standby devices.

The standby E-SBC assumes the active role when:

- It has not received a checkpoint message from the active E-SBC for a certain period of time.
- It determines that the active E-SBC's health score has decreased to an unacceptable level.
- The active E-SBC relinquishes the active role.

## High Availability on the Acme Packet 1100

The Acme Packet 1100 supports High Availability (HA), but the configuration differs from other Oracle Enterprise Session Border Controllers (E-SBC) because there is only one management interface on this device.

Unlike other E-SBCs, which provide two management interfaces and two media interfaces, the Acme Packet 1100 provides 1 management interface and 2 media interfaces. For HA, you must create a second management interface object on the Acme Packet 1100 with `wancom0` for the **name** and VLAN for the **sub-port-id**. You can configure only one management interface in an HA pair with these settings and the system does not support more than one HA interface with a VLAN tag.

### Note:

The Acme Packet 1100 E-SBC does not support High Availability (HA) for any call using the Time Division Multiplexing (TDM) interface.

## Configure High Availability

To create a High Availability (HA) pair of Oracle Enterprise Session Border Controllers (E-SBC), you must configure one E-SBC as the primary and the other E-SBC as the secondary.

### Before You Begin

- Confirm that the system displays the Basic mode.

The Web GUI displays the HA configuration parameters on the Settings page. Use the following procedure to create an HA pair and to establish communication between the devices.

### Procedure

1. From the Web GUI, click **Configuration > Settings**.
2. On the Settings page, click **High availability settings**, and do the following:

Attributes	Instructions
Enable high availability	Select to enable HA.
Name of primary peer	Enter the name of the primary E-SBC peer.
Name of secondary peer	Enter the name of the secondary E-SBC that you want to use for HA purposes to peer with the primary.
ENT phy interface virtual MAC	Enter the MAC address of the Enterprise physical interface on the E-SBC.
SP phy interface virtual MAC	Enter the MAC address of the Service Provider physical interface on the E-SBC.

3. Click **OK**.
4. Save and activate the configuration.

## Configure the Acme Packet 1100 Primary for HA

You can configure the Acme Packet 1100 primary for High Availability (HA) operations from the Web GUI by using the configuration tools in Basic mode.

### Before You Begin

- Confirm that the Oracle Enterprise Session Border Controller software is installed on two separate systems.

You must perform the following procedure on the primary system before configuring the secondary system for HA operations.

### Procedure

1. On the Web GUI, click **Configuration > Wizards > Set initial configuration > Run Setup**.

The system displays the Set initial configuration dialog.

2. In the Set initial configuration dialog, do the following:

Attributes	Instructions
Enable Web GUI	Select <b>Yes</b> to enable the Web GUI.
Choose Web GUI mode	Select <b>Basic Web GUI</b> mode.
SBC mode	<ul style="list-style-type: none"> <li>• Select <b>high availability</b> SBC mode.</li> <li>• Select primary.</li> </ul>
IP address on management interface	Enter the IP address of the management interface on the primary.
Unique target name	Enter a unique target name for the primary.
Subnet mask	Enter the subnet mask.
Management interface VLAN	Enter the number of the management interface VLAN. Range: 0-4095.
Gateway IP address	Enter the gateway IP address.
Peer target name	Enter the name of the secondary.

3. Click **Complete**.  
The system reboots.

### Next Steps

Configure the secondary for High Availability. See "Configure the Acme Packet 1100 Secondary for High Availability (HA) - GUI Basic."

## Configure the Acme Packet 1100 Secondary for HA

You can configure the Acme Packet 1100 secondary for High Availability (HA) operations from the Web GUI by using the configuration tools in Basic mode.

### Before You Begin

- Confirm that the Oracle Enterprise Session Border Controller primary is configured for HA operations.

When configuring the secondary system, enter the same management interface VLAN that you entered for the primary system.

### Procedure

1. On the Web GUI, click **Configuration > Wizards > Set initial configuration > Run Setup**.

The system displays the Set initial configuration dialog.

2. In the Set initial configuration dialog, do the following:

Attributes	Instructions
Enable Web GUI	Select <b>Yes</b> to enable the Web GUI.
Choose Web GUI mode	Select <b>Basic Web GUI</b> mode.
SBC mode	<ul style="list-style-type: none"> <li>• Select <b>high availability</b> SBC mode.</li> <li>• Select primary.</li> </ul>
IP address on management interface	Enter the IP address of the management interface on the primary.
Unique target name	Enter a unique target name for the primary.
Subnet mask	Enter the subnet mask.
Management interface VLAN	Enter the number of the management interface VLAN. Range: 0-4095.
Gateway IP address	Enter the gateway IP address.
Acquire configuration from primary	Select <b>Yes</b> .

3. Click **Complete**

The system reboots.

## Packet Capture Settings

You can configure the packet capture function on the Oracle Enterprise Session Border Controller (E-SBC) to view packet traffic on your network. For example, you might want to confirm the network configuration or to perform troubleshooting.

During a packet capture session, the system creates a set of .pcap files in the /opt/traces directory. If the /opt/traces directory contains files when you run the packet-trace command, the system prompts you to either remove or keep the existing files before running the command. The following table describes the system behavior for both options.

Option	Result	Packet Trace Command Behavior
Yes	Removes all existing files.	The system captures up to 25 new .pcap files. During the session, the system rotates the files in the /opt/traces directory by size. For example, the system keeps the last 25 files and rotates them when they reach 100 MB
No	Keeps all existing files.	<ul style="list-style-type: none"> <li>• If the /opt/traces directory contains 25 .pcap files, the system cannot add more files to the directory or overwrite the existing files.</li> <li>• If the /opt/traces directory contains fewer than 25 .pcap files, the system can add new files to the directory up to the 25 file limit. For example, if the /opt/traces directory contains 10 existing files, the system can add up to 15 new files.</li> </ul>

## Configure Packet Capture Settings

You can configure the Oracle Enterprise Session Border Controller (E-SBC) to send packet captures to a designated receiver.

### Before You Begin

- Note the IP address and network interface of the device to which the E-SBC will send captured packets.
- Confirm that the system displays the Basic mode.

Use the following procedure to enable the packet capture function and to specify where the E-SBC sends the captured packets.

### Procedure

1. From the Web GUI, click **Configuration > Settings > Show advanced > Packet capture settings**.
2. Under Packet capture settings, do the following:

Attributes	Instructions
Enable packet capture	Select to enable.
Capture receiver network interface	Select the network interface that you want for the packet capture receiver from the drop-down list.
Capture receiver IP address	Enter the IP address of the packet capture receiver.

3. Click **OK**.
4. Save and activate the configuration.

## Remote Site Survivability

The remote site survivability feature enables an Oracle Enterprise Session Border Controller (E-SBC) that is deployed in a Remote Office/Branch Office (ROBO) site to detect the loss of communication over SIP-based telephony to the Enterprise's core call processing Data Center.

When loss of communication is detected over the SIP service, the ROBO E-SBC dynamically switches into Survivable Mode, handling call processing locally and providing limited additional server functionality.

 **Note:**

Remote Site Survivability supports SIP only. It does not support H.323 call signalling.

Remote Site Survivability:

- Works with or without High Availability (HA).
- Is configurable in real-time, with no reboot required to enable this feature.
- Allows configuration by way of the E-SBC Web GUI.
- Maintains Historical Recording (HDR) statistics about being in survivability mode, such as:
  - Whether or not the E-SBC is in survivable mode using the ACLI command, show health.
  - Length of time the E-SBC was in survivable mode (records the number of times and the amount of time in survivability mode).
  - Number of SIP messages handled in survivable mode.
  - Number of SIP users registered locally in survivable mode (both existing based on cache, and separately - new registrations).

## Configure Remote Site Survivability

You must enable remote site survivability on the Oracle Enterprise Session Border Controller (E-SBC) and set the parameters before the system can enter and exit survival mode.

### Before You Begin

- Confirm that at least one session is configured.
- Confirm that the system displays the Basic mode.

The Web GUI displays the Survivability configuration parameters on the Settings page, after you click **Show advanced**. Use the following procedure to enable this function, specify a triggering device, and optionally change the default settings.

### Procedure

1. From the Web GUI, click **Configuration > Settings > Show advanced > Survivability**.
2. Under Survivability, do the following:

Attributes	Instructions
State	Select to enable.
Registration expire time	Enter the time, in seconds, that the E-SBC waits before entering survival mode. Default: 30. Range: 086400.
Extension length	Enter the maximum length allowed for a phone extension. Default: 4. Range :0-10

Attributes	Instructions
Trigger on	Select a PBX, Trunk, device, or group from the drop-down list that triggers survivability mode when it goes out of service.

## Network Button

Use the Network button to access the following configuration elements.

Configuration Element	Purpose
Host route	Specify where to direct management traffic.
Network interface	Specify a logical network interface over which you can configure one or more SIP interfaces.

## Host Routes

Host routes let you insert entries into the Oracle Enterprise Session Border Controller (E-SBC) routing table. These routes affect traffic that originates at the E-SBC host process. Host routes are used primarily for steering management traffic to the correct network.

When traffic is destined for a network that is not explicitly defined on an E-SBC, the default gateway is used. If you try to route traffic to a specific destination that is not accessible through the default gateway, you need to add a host route. Host routes can be thought of as a default gateway override.

Certain SIP configurations require that the default gateway is located on a front media interface. In this scenario, if management applications are located on a network connected to a rear-interface network, you need to add a host route for management connectivity.

When source-based routing is used, the default gateway must exist on a front media interface. Host routes might be needed to reach management applications connected to a wancom port in this kind of situation.

## Add a Host Route

You can configure the Oracle Enterprise Session Border Controller (E-SBC) to steer management traffic to the correct network by inserting an entry in the routing table.

Use the following procedure to insert an entry into the E-SBC routing table.

### Procedure

1. From the Main Menu, click **Network > Host routes**.
2. On the Host Route page, click **Add**.
3. In the Add Host Route dialog, do the following.

Attributes	Instructions
Dest network	Enter the IPv4 address of the destination network that this host route points to. Dotted decimal format. For example, 192.30.1.104. No two host-route elements can use the same destination network address.



Attributes	Instructions
Netmask	Select the netmask from the drop-down list associated with the destination network that you entered for the Dest network parameter.
Gateway	Enter the gateway which traffic destined for the address defined in the Dest network parameter should use as its first hop when forwarding a packet out of the originator's LAN. Dotted decimal format. For example, 192.30.1.1.
Description	Enter a description for this host route. Valid values are alpha-numeric characters. For example, Host Route A.

- Click **OK** to save the host route.  
The host route that you created displays in the Host Routes table.
- Click **Close**.
- Save and activate the configuration.

## Network Interface Configuration

The network interface element specifies a logical network interface. In order to use a network port on a network interface, you must configure both the physical interface and the corresponding network interface configuration elements.

### Add a Network Interface

Use the network interface element to create and configure a logical network interface.

You can add a network interface from the Web GUI in either Basic mode or Expert mode. If the network interface does not use VLANs tagging, ensure that the subport ID field is set to 0, the default value. When VLAN tags are used on a network interface, the valid subport ID value can range from 1-4096. Network interface is a multiple instance configuration element. The combination of the name field and the subport ID field must be unique in order to identify a discrete network interface. Except where noted, you can use an IPv6 IP address in any parameter in the following procedure.

#### Procedure

- From the Web GUI, select **Configuration > Network > Network interface**.
- In the Network interface dialog, click **Add**.
- In the Add Network interface dialog, click **Show advanced**, and do the following:

Attributes	Instructions
Name	Enter the name of the physical interface with which this network-interface element is linked. For example Enterprise. Network-interface elements that correspond to phy-interface elements with an operation type of Control or Maintenance must start with "wancom."

Attributes	Instructions
Sub port ID	Required only for a VLAN, where the operation type is Media. Enter the identification number from 1-4095 of a specific virtual interface in a physical interface. Otherwise, leave the default 0, which means this element is not using a virtual interface.
Description	Enter a description of this interface for easier identification.
Hostname	(Optional) Enter the hostname of this network interface in FQDN or IP Address format.
IP Address	Enter the IP address of this network interface in IP Address format.
Pri utility address	Enter the utility IP address for the primary High Availability (HA) peer in an HA architecture.
Sec utility address	Enter the utility IP address for the secondary Oracle Communications Session Border Controller in an HA architecture.
Netmask	Enter the netmask portion of the IP address for this network interface entered in IP address format.
Gateway	Enter the gateway this network interface uses to forward packets in IP Address format.
Sec gateway	Enter the gateway to use on the secondary Oracle Enterprise Session Border Controller (E-SBC) in an HA pair in IP Address format.
Gw heartbeat State	Click to display the configuration fields. Select to enable the front interface link detection and polling functionality on the E-SBC.
Heartbeat	Enter the time interval in seconds between heartbeats for the front interface gateway.
Retry count	Enter the number of front interface gateway heartbeat retries before a gateway is considered unreachable.
Retry timeout	Enter the heartbeat retry timeout value in seconds.
Health score	Enter the amount to subtract from the health score if the front interface gateway heartbeat stops responding.
DNS IP primary	Enter the IP address of the primary DNS to be used for this interface.
DNS IP backup 1	Enter the IP address of the first backup DNS to be used for this interface.
DNS IP backup 2	Enter the IP address of the second backup DNS to use for this interface.
DNS domain	Set the default domain name used to populate incomplete hostnames that do not include a domain in Name format.
DNS timeout	Enter the total time in seconds to elapse before a query (and its retransmission) is sent to a DNS server timeout.
Signalling MTU	Enter the size of the Maximum Transmission Unit for packets leaving this interface. Default-inherits system-wide MTU. IPv4-0, 576-4096. IPv6-0, 1280-4096.

Attributes	Instructions
HIP IP list	Add all IPv4 Host Identity Protocol lists for which you want the E-SBC to accept administrative traffic.
FTP address	Enter a list of IP addresses from which FTP traffic can be received and acted upon by a front media interface.
ICMP address	Enter the IP address to pass standard ping packets to the host.
Telnet address	Enter the IP address where port 23 is open for Telnet access.
SSH address	Enter a list of IP addresses from which SSH traffic can be received and acted upon by a front media interface. Requires a valid IPv4 network address.

4. Click **OK**.
5. Save and activate the configuration

## Security Button

Use the Security button to access the following configuration elements.

Configuration Element	Purpose
Certificate record	Create the certificate record for adding a digital certificate for the Oracle Enterprise Session Border Controller (E-SBC).
SDES profile	Add one or more Session Description Protocol Security Descriptions (SDES) profiles for media streams to the E-SBC.
TLS profile	Add one or more Transport Layer Security (TLS) profiles for communications security to the E-SBC.

See *Security Configuration* under "Expert Mode Configuration" for more information. The instructions are the same for the Basic mode and the Expert mode.

## Management Button

Use the Management button to access the following configuration elements.

Configuration Element	Purpose
Accounting	Specify call accounting strategy, protocol, receivers, servers, parameters, and options.
SNMP community	Add and specify one or more Simple Network Management Protocol (SNMP) communities.
Trap receiver	Add and specify one or more SNMP trap receivers.
Web server	Specify the web server.

## Configure Call Accounting

### Before You Begin

- Confirm that the system displays the Basic mode.

**Procedure**


1. From the Web GUI, click **Configuration > Management > Accounting**.
2. In the Account config dialog, click **Show Advanced**, and do the following:



Attributes	Instructions
Strategy	Select the lookup algorithm from the drop-down list for the accounting server.
Protocol	Select a protocol from the drop-down list.
State	Select to enable call accounting.
Generate start	Select an event trigger from the drop-down list for session accounting recording .
Generate interim	Click <b>Add</b> , select an event to collect in a session, and do one of the following: <ul style="list-style-type: none"> <li>• Click <b>OK</b>.</li> <li>• Click <b>Apply/Add another</b>, add another media attribute, and click <b>OK</b>. Repeat, as needed.</li> </ul> Default: Reinvite-Response.
Generate event	Click <b>Add</b> , select a Diameter event to collect in a session, and do one of the following: <ul style="list-style-type: none"> <li>• Click <b>OK</b>.</li> <li>• Click <b>Apply/Add another</b>, add another media attribute, and click <b>OK</b>. Repeat, as needed.</li> </ul> Leave blank to disable.
File output	Select to enable active writing of comma delimited records.
File path	Enter the local, comma delimited CDR output storage directory. <ul style="list-style-type: none"> <li>• Do not use /boot or /code file systems.</li> <li>• Default: /opt/logs/.</li> </ul>
File rotate time	Enter a number for the time, in minutes, for the file rotation interval. Range: 0-2147483647.
Options. Add optional parameters.	Click <b>Add</b> , enter an option, and do one of the following: <ul style="list-style-type: none"> <li>• Click <b>OK</b>.</li> <li>• Click <b>Apply/Add another</b>, add another media attribute, and click <b>OK</b>. Repeat, as needed.</li> </ul>
FTP push	Select to push files to an FTP server.
FTP address	Enter the IPv4 address of the FTP server.
FTP user	Enter the FTP server User Name.
FTP password	Enter the FTP server Password.
FTP remote path	Enter the remote FTP server path for comma delimited CDR files.

---

Attributes	Instructions
Push receiver	<p>Click <b>Add</b> &gt; <b>Show advanced</b>, and do the following:</p> <ol style="list-style-type: none"><li>a. Server. Enter the server IP address.</li><li>b. Port. Enter the server port. Range: 1-65535.</li><li>c. Admin state. Select to enable.</li><li>d. Remote path. Enter the remote path name.</li><li>e. File name prefix. Enter the prefix for file names pushed to the server.</li><li>f. Priority. Enter the priority of the push receiver. Range 0 (highest)-4 (lowest).</li><li>g. Protocol. Select a protocol from the drop-down list for pushing to the server.</li><li>h. Enter the server User Name.</li><li>i. Enter the server Password, and click <b>Set</b>.</li><li>j. Public key. Enter the public key.</li><li>k. Click <b>OK</b>.</li></ol>
CDR output redundancy	Select to enable.
Interim state ID type	<p>Click <b>Add</b>, select an interim state ID type, and do one of the following:</p> <ul style="list-style-type: none"><li>• Click <b>OK</b>.</li><li>• Click <b>Apply/Add another</b>, add another media attribute, and click <b>OK</b>. Repeat, as needed.</li></ul>

---

Attributes	Instructions
Account servers	<p>Click <b>Add &gt; Show advanced</b>, and do the following:</p> <ol style="list-style-type: none"> <li><b>a.</b> Hostname. Enter the hostname of the remote server.</li> <li><b>b.</b> Min round trip. Enter the minimum time allowed to and from the remote server in milliseconds. Range: 10-5000.</li> <li><b>c.</b> Max inactivity. Enter the maximum time allowed for remote server inactivity in seconds. Range: 1-300.</li> <li><b>d.</b> Restart delay. Enter the delay time before retrying an inactive remote server in seconds. Range: 1-300.</li> <li><b>e.</b> Bundle vsa. Select to enable.</li> <li><b>f.</b> Secret. Enter the authentication secret.</li> <li><b>g.</b> NAS ID. Enter the remote network accounting server ID.</li> <li><b>h.</b> Domain name suffix. Enter the suffix to use for all domain names.</li> <li><b>i.</b> Watchdog ka timer. Enter the time interval for keep alive messages in seconds. Range: 0, 6-65535.</li> <li><b>j.</b> Diameter in manip. Enter the inbound Diameter manipulation to apply.</li> <li><b>k.</b> Diameter out manip. Enter the outbound Diameter manipulation to apply.</li> <li><b>l.</b> Click <b>OK</b>.</li> </ol>
Prevent duplicate attr	Select to enable preventing duplicate accounting attributes.
VSA ID range	Enter a comma delimited range of accounting attributes to include in CDRs.
<p> <b>Note:</b></p> <p>Blank means that all attributes are included.</p>	
CDR output inclusive	Select to enable the inclusion of all empty fields.

Attributes	Instructions
Diam attr ID range	Enter a comma delimited range of accounting attributes to include in Diameter Rf accounting records.
	<div style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> <b>Note:</b> Blank means that all attributes are included.</p> </div>
Msg queue size	Enter the maximum number of accounting records to store in memory. Default: 5000. Range: 5000-150000.
Diam send throttle	Enter the maximum number of accounting records to send to the Diameter server without yielding to other tasks. Default 20. Range: 2-20.
Diam srv ctx rel	Enter the 3GPP release number of the service specific document.
Diam srvc ctx mnc mcc	Enter the Mobile Country Code / Mobile Network Code tuple. Format: MNC.MCC.
Diam srvc ctx ext	Enter the operator-specific extension information.
Diam srvc attr ID range	Enter a comma delimited range of Acme accounting attributes to include in Diameter Rf accounting records.
	<div style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> <b>Note:</b> Blank means that all attributes are included.</p> </div>
Max acr retries	Enter the maximum number of ACR retries. Range: 0-4.
ACR retry interval	Enter the interval time between ACR retries in seconds. Default: 10. Range: 5-20.

3. Click **OK**.
4. Save and activate the configuration.

## Configure SNMP Community

Configure a Simple Network Management Protocol (SNMP) community to support the monitoring of devices, such as the Oracle Enterprise Session Border Controller (E-SBC), attached to the network for conditions that warrant administrative attention.

### Before You Begin

- Confirm that SNMP is configured.
- Note the IP addresses that you want for this community.
- Confirm that the system displays Basic mode.

Use this procedure to group network devices and management stations, and to set the access rights for the community.



#### Note:

Only devices that support SNMPv1 and SNMPv2c protocol can use SNMP community strings. SNMPv3 uses username and password authentication, along with an encryption key.

#### Procedure

1. From the Web GUI, click **Configuration > Management > SNMP community**.
2. On the SNMP community page, click **Add**, and do the following:

Attributes	Instructions
Community name	Enter an SNMP community name of an active community where this E-SBC can send and receive SNMP information.
Access mode	Select the access level for all Network Management Systems (NMS) defined within this SNMP community.
IP address	Click <b>Add</b> , enter an IPv4 address that is valid within this SNMP community, and do one of the following: <ul style="list-style-type: none"> <li>• Click <b>OK</b>.</li> <li>• Click <b>Apply/Add another</b>, add another media attribute, and click <b>OK</b>. Repeat, as needed.</li> </ul>

3. Click **Close**.
4. Save and activate the configuration.

## Configure an SNMP Trap Receiver

You can define one or more SNMP trap receivers on an Oracle Enterprise Session Border Controller (E-SBC) for redundancy or to segregate alarms with different severity levels to individual trap receivers.

#### Before You Begin

- Confirm that SNMP is configured.
- Note the names of users who are allowed to receive secure traps.
- Confirm that the system displays Expert mode.

Oracle recommends that you configure each server with an NMS installed as a trap receiver on each ESBC managed by an NMS. When configuring the trap-receiver element for use with Network Management Systems, Oracle recommends setting the filter-level parameter to All.

#### Procedure

1. From the Web GUI, click **Configuration > Management > trap-receiver**.
2. On the Trap receiver page, click **Add**.



- On the Add trap receiver page, do the following.

Attributes	Instructions
IP address	Enter the IPv4 address and port number of an authorized NMS in dotted decimal format. Default: 0.0.0.0:162.
Filter level	Select the filter level threshold from the drop-down list that indicates the severity level at which a trap is sent to the trap receiver.
Community name	Enter the SNMP community name to which this trap receiver belongs.
User list	Click <b>Add</b> , enter the name of a user allowed to receive secure traps, and do one of the following: <ul style="list-style-type: none"> <li>Click <b>OK</b>.</li> <li>Click <b>Apply/Add another</b>, add another media attribute, and click <b>OK</b>. Repeat, as needed.</li> </ul>

 **Note:**

If SNMPv3 is enabled on the E-SBC, and no users are listed for this field, the system displays a warning message during a verify-config execution.

- Click **Close**.
- Save and activate the configuration.

## Web Server Configuration

The Web server is a software application that helps to deliver Web content that you can access through the Internet. The Web server runs the Enterprise application called the Web GUI.

Every Web server has an IP address and sometimes a domain name. For example, if you enter the URL `http://www.acmepacket.com/index.html` in your browser, the browser sends a request to the Web server with domain name is `acmepacket.com`. The server fetches the page named `index.html` and sends it to the browser.

If you enter `http://132.45.6.5`, and this address has been configured by your Administrator to access the Web GUI, the server fetches the page and displays the Web GUI logon page to your browser.

This section provides a procedure for configuring the Web server in your network.

## Configure a Web Server

You can configure Transport Layer Security (TLS) on the Web Server to enhance security.

### Before You Begin

- Confirm that at least one TLS profile exists.
- Confirm that the system displays the Basic mode.

Enable the Web server, specify connection to the Oracle Enterprise Session Border Controller, and select a TLS profile.

#### Procedure

1. From the Web GUI, click **Management > Web server**.
2. On the Web server config page, click **Show advanced**, and do the following.

Attributes	Instructions
State	Select to enable Web server.
Inactivity timeout	Enter the number of minutes you want the Web server to wait before timing out. Range: 0-20.
HTTP state	Select to enable HTTP connection to the Web server.
HTTP port	Enter the HTTP port number. Default: 80. Range: 1-65535.
HTTPS state	Select to enable HTTPS connection to the Web server.
HTTPS port	Enter the HTTPS port number. Default: 443. Range: 1-65535.
TLS profile	Select a TLS profile to use for HTTPS from the drop-down list.

3. Click **OK**.
4. Save and activate the configuration.

## Other Button

Use the Other button to access the following configuration elements.

Configuration Element	Purpose
Media profile	Adds one or more media profiles.
Translations rules	Adds one or more translation rules.
SIP features	Adds one or more SIP features.
SIP manipulations	Specifies how to handle SIP headers and configuration rules.
SPL	Adds one or more SPL plugins.

## Configure Media Profile

You can configure one or more media profiles for the Oracle Enterprise Session Border Controller to use as a rules for sending and receiving media over the network.



In the following procedure, you can configure:

- One media profile for a particular SIP SDP encoding, such as G729, by providing a unique name to identify the profile for the particular encoding type.
- Multiple media profiles for the same SIP SDP encoding by adding a subname to the configuration. The system uses the subname plus the profile name as the unique identifier.

#### Procedure

1. From the Web GUI, click **Other > Media profile**.

2. On the Media profile page, click **Add > Show advanced**, and to the following.

Attributes	Instructions
Name	Enter the name for this media profile. For example, PCMU, G723, G729. Valid values are alpha-numeric characters.
Subname	Enter the encoding subname used for the Codec variation. Valid values are alpha-numeric characters. You must use a combination of alpha and numeric characters.
Media type	Enter the media type to use in SDP m lines. For example, audio, video, data.
Payload type	Enter the payload type to use in SDP media lines. Valid values are alpha-numeric characters.
	<div data-bbox="1019 716 1138 751"> <b>Note:</b></div> <div data-bbox="1055 772 1390 861">The Payload type value must be numeric if you use the RTP/AVP transport method.</div>
Transport	Enter the transport protocol to use in the SDP RTPMAP attribute. Default: RTP/AVP. Valid values are: <ul style="list-style-type: none"><li>• RTP/AVP</li><li>• UDP</li></ul>
Clock rate	Enter the clock rate to use in the SDP RTPMAP attribute in Hz. For example, 8000 in narrowband Codecs and 16000 in wideband Codecs. Range: 0=4294967295.
	<div data-bbox="1019 1268 1138 1304"> <b>Note:</b></div> <div data-bbox="1055 1325 1471 1411">When configured with 0, the default, the system uses the clock rate for the Codec.</div>
Res bandwidth	Enter the amount of bandwidth required in Kilobits. Range: 0-999999999.
Frames per packet	Enter the maximum number of frames per packet. Range: 0-256.

Attributes	Instructions
Parameters	Click <b>Add</b> , enter the parameter, and do one of the following: <ul style="list-style-type: none"> <li>Click <b>OK</b>.</li> <li>Click <b>Apply/Add another</b>, add another media attribute, and click <b>OK</b>. Repeat, as needed.</li> </ul>

 **Note:**

For each parameter, use the + character to add and the - character to remove. For example, +silenceSuppression=0.

- Click **OK**.
- Save and activate the configuration.

## Configure Translation Rules

You can configure the Oracle Enterprise Session Border Controller (E-SBC) to use number translation to change a layer 5 endpoint name according to prescribed rules. For example, to add or to remove a 1 or a + from a phone number sent from or addressed to a device. Use the translation-rules element to create unique sets of translation rules to apply to calling and called party numbers.

### Before You Begin


- Confirm that the system displays the Basic mode.

In the following procedure, you set the translation type, define the string to add or delete, and set the character position (index) where the add, delete, or replace occurs in the string. The index starts at 0, immediately before the leftmost character, and increases by 1 for every position to the right. Use the \$ character to specify the last position in a string.

### Procedure

- From the Web GUI, click **Other > Translation rules**.
- On the Translation rules page, click **Add > Show advanced**.
- In the Add Translation rules dialog, do the following.

Attributes	Instructions
ID	Enter a descriptive ID name for this translation rule. Valid values are alpha-numeric characters.

Attributes	Instructions
Type	Select the one of the following translation rules that you want to configure from the drop-down list. <ul style="list-style-type: none"> <li>• Add. Adds a character or string of characters to the address.</li> <li>• Delete. Deletes a character or string of characters from the address.</li> <li>• None: Disables the translation rule function.</li> <li>• Replace. Replaces a character or string of characters within the address.</li> </ul>
Add string	Enter the index for the Add string. Use the \$ character to append the string at the end of the address. Valid values are alpha-numeric characters.
Add index	Enter the index for the Add string. Use the \$ character to append the string at the end of the address. Valid values are alpha-numeric characters.
Delete string	Enter the string to be deleted from the original address during address translation. Unspecified characters are denoted by the @ character. Valid values are alpha-numeric characters.
	<div style="border: 1px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> <b>Note:</b></p> <p>The @ character only works if the type parameter is set to delete. This parameter supports wildcard characters or digits only. For example, valid entries are: delete-string=@@@@@, or delete-string=123456. An invalid entry is delete-string=123@@@.</p> </div>
	When the type is set to <b>replace</b> , this value is used in conjunction with the add-string value. The value specified in the delete-string field is deleted and the value specified in the add-string field is inserted. If no value is specified in the delete-string parameter and the type field is set to replace, then nothing is inserted into the address.
Delete index	Enter the index for the Delete string.

4. Click **OK**.
5. Save and activate the configuration.

## Configure SIP Features

Use the sip-feature dialog to define how the Oracle Enterprise Session Border Controller (E-SBC) handles option tags in the SIP Supported header, Require header, and the Proxy-Require header.

### Before You Begin

- Confirm that the system displays the Basic mode.

You can specify whether a SIP feature is applied to a specific realm or globally across all realms. You can also specify the treatment for an option based upon whether it appears in an inbound or outbound packet. You need to configure option tag handling in the SIP feature element only when you want a treatment other than the default.

### Procedure

1. From the Web GUI, click **Configuration > Other > Sip Features**.
2. On the Sip feature page, click **Add**, and do the following:

Attributes	Instructions
Name	Enter the action tag name to display in the Require, Supported, and Proxy-Require headers of SIP messages.
SIP interface	Do one of the following: <ul style="list-style-type: none"> <li>• Select the SIP interface with which to associate this configuration.</li> <li>• Leave this parameter blank to make this configuration global.</li> </ul>
Support mode inbound	Select the action tag in the Supported header in an inbound packet from the drop-down list.
Require mode inbound	Select the action tag in the Require header for an inbound packet from the drop-down list. Default is reject.
Proxy require mode inbound	Select the action tag in the Proxy-Require header in an inbound packet from the drop-down list.
Support mode outbound	Select the action tag in the Supported header in an outbound packet from the drop-down list.
Require mode outbound	Select the action tag in the Require header for an outbound packet from the drop-down list.
Proxy require mode outbound	Select the action tag in the Proxy-Require header for an outbound packet from the drop-down list.

3. Click **OK**.
4. Save and activate the configuration.

Enter the tasks the user should do after finishing this task (optional).

## Configure SIP Manipulations

SIP Header Manipulation provides the flexibility to add, remove, or modify any attribute in a SIP message on the Oracle Enterprise Session Border Controller (E-SBC). The most common reason for doing this is to fix an incompatibility problem between two SIP endpoints. This could range from anything such as Softswitch/PSTN incompatibility or an issue between two different IP PBX platforms in a multi-site Enterprise where calls between them fail due to issues in the SIP messaging.

The SIP header and parameter manipulation feature allows you to add, modify, and delete SIP headers and parts of SIP headers called SIP header elements. SIP header elements are the different subparts of the header, such as the header value, header parameter, URI parameter and so on (excluding the header name).

To enable the SIP header and parameter manipulation functionality, you create header manipulation rule sets in which you specify header manipulation rules, as well as optional

header element rules that operate on specified header elements. You then apply the header manipulation ruleset as inbound or outbound for a session agent or SIP interface.

Header manipulation rules operate on the header you specify when you configure the rule. A header manipulation rule can also be configured with a list of element rules, each of which would specify the actions you want performed for a given element of this header.

Header element rules perform operations on the elements of a header. Header elements include all subparts of a header; excluding the header name. For example, header value, header parameter, URI parameter, and so on.

1. From the Main Menu, click **Other > SIP manipulation**.

The SIP manipulation table displays the default header manipulation rules for the E-SBC. You can select a rule to edit or add a new rule as required.

2. To add a new rule, click **<Add>**. The following dialog box displays.
3. In the **Name** field, enter the name of the header to which this rule applies. The name you enter here must match a header name. This is a case-insensitive string that is compared to the header name for matching. You need to create a rule using the long form of the header name and a rule using the compact form of the header name. Valid values are alpha-numeric characters. Default is blank.

 **Note:**

The Request-URI header is identified as request-uri.

4. In the **Description** field, enter a description for this header manipulation rule. Valid values are alpha-numeric characters. Default is blank.

## Specify Split Headers

1. In the **Split headers** field, enter the elements of the message header that you want the Oracle Enterprise Session Border Controller to split.

Click **<Add>**.

In the Split headers field, enter the header element you want to split. For example, \$LOCAL\_IP.

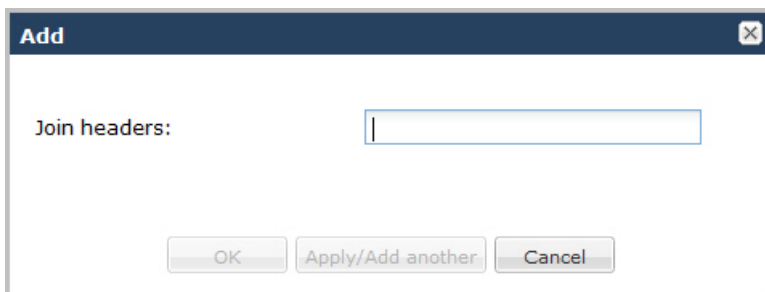
To add the element to the list and apply another one, click **<Apply/Add Another>**.

When you have completed adding header elements to the Split header list, click **<OK>**.

## Specify Join Headers

1. In the **Join headers** field, enter the header element you want the Oracle Enterprise Session Border Controller to join.

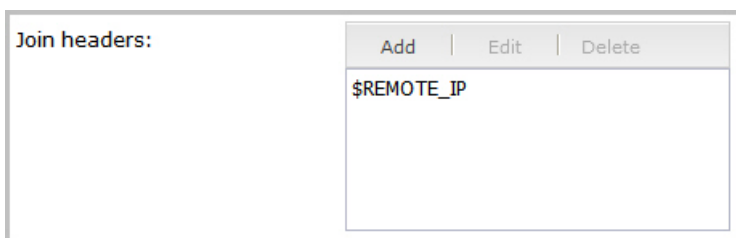
Click **<Add>**. The following displays.



In the Join headers field, enter the header element you want to join. For example, \$REMOTE\_IP.

To add the element to the list and apply another one, click <Apply/Add Another>.

When you have completed adding header elements to the Join header list, click <OK>. The following displays.



## Specify Configuration Rule

1. In the **cfgRules** field, enter the rule to use in the Oracle Enterprise Session Border Controller configuration. These rules use the “Split” and Join headers you specified above.
2. Click <Add>, and select **header-rule** from the drop-down list. The following displays.





3. In the **Name** field, enter a name you want to use for this rule set. Valid values are alpha-numeric characters. Default is blank.
4. In the **Header name** field, enter the name of the header to which this rule applies. The name you enter here must match a header name. This is a case-insensitive string that is compared to the header name for matching. You need to create a rule using the long form of the header name and a rule using the compact form of the header name. Valid values are alpha-numeric characters. Default is blank.

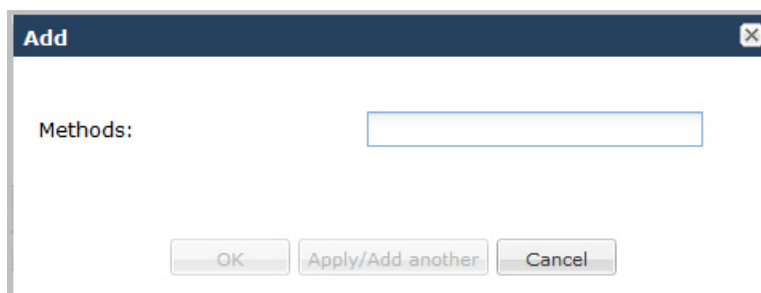
 **Note:**

The Request-URI header is identified as request-uri.

5. In the **Action** field, select an action you want applied to the header specified in the Name parameter. Default is **none**. Valid values are:
  - add—Adds a new header, if that header does not already exist.
  - delete—Deletes the header, if it exists.
  - find-replace-all—Finds all matching headers and replaces it with the header you specified for “Split” and Join.
  - log—Logs the header.
  - manipulate—Manipulates the elements of this header to the element rules configured.
  - monitor—Monitors the header.
  - store—Stores the header.

- none—(default) No action is taken.
  - reject—Rejects the header.
  - sip-manip—Manipulates the SIP elements of this header to the element rules configured.
  - store—Stores the header.
6. In the **Comparison type** field, select the way that you want SIP headers to be compared. This choice dictates how the Oracle Enterprise Session Border Controller processes the match rules against the SIP header. Default is **case-sensitive**. Valid values are:
- boolean—Header is compared to header rule and must match exactly or it is rejected.
  - case-insensitive—Header is compared to header rule regardless of the case of the header.
  - case-sensitive—(default) Header is compared to the header rule and case must be exactly the same or it is rejected.
  - pattern-rule—Header is compared to the header rule and the pattern must be exactly the same or it is rejected.
  - refer-case-insensitive—Header is compared to the header rule regardless of the case in a REFER message.
  - refer-case-sensitive—Header is compared to the header rule and the case must be exactly the same as in the REFER message or it is rejected.
7. In the **Msg type** field, select the message type to which this header rule applies. Default is **any**. Valid values are:
- any—(default) Requests, replies, and out-of-dialog messages
  - out-of-dialog—Out of dialog messages only.
  - reply—Reply messages only
  - request—Request messages only
8. In the **Methods** field, specify the SIP method names to which you want to apply this header rule.

Click <Add>. The following displays.



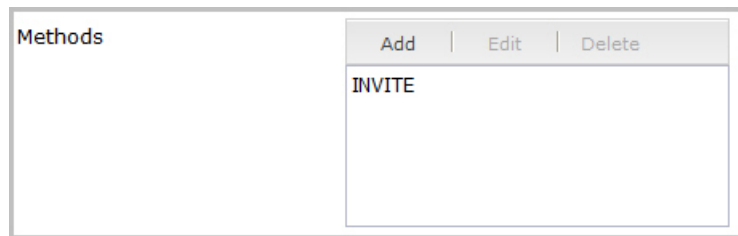
In the Methods field, enter SIP method names to which you want to apply this header rule. For example, INVITE, ACK, BYE.

**Note:**

This field is empty by default. If you leave the method field empty, the header rule applies to all methods.

To add the method to the list and apply another one, click <Apply/Add Another>.

When you have completed adding methods, click <OK>. The following displays.



9. In the **Match value** field, enter the value you want to match against the element value for an action to be performed.
10. In the **New value** field, enter the value for a new element or to replace a value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.

- Absolute values - use double quotes for clarity. You must escape all double quotes and back slashes that are part of an absolute value, and enclose the absolute value in double quotes.

For example:

```
sip:?"+$STRUNK_GROUP+".$STRUNK_GROUP_CONTEXT
```

- Pre-defined parameters always start with a \$. The following table describes the pre-defined parameters.

Pre-defined Parameters Table

Parameter	Description
\$ORIGINAL	Original value of the element is used.
\$LOCAL_IP	IP address of the SIP interface on which the message was received for inbound manipulation; or sent on for outbound manipulation.
\$REMOTE_IP	IP address the message was received from for inbound manipulation; or being sent to for outbound manipulation.
\$REMOTE_VIA_HOST	Host from the top Via header of the message is used.
\$STRUNK_GROUP	Trunk group is used.
\$STRUNK_GROUP_CONTEXT	Trunk group context is used.

The following table describes the Operators.

Operators Table

Operator	Description
+	Append the value to the end. For example: acme"+"packet generates acmepacket
+^	Prepends the value. For example: acme"+"^"packet generates packetacme
-	Subtract at the end. For example: 112311"-^"11 generates 1123
-.^	Subtract at the beginning. For example: 112311"-^"11 generates 2311

Examples of entries for the **new-value** field.

```
$ORIGINAL+acme
$ORIGINAL+"my name is john"
$ORIGINAL+"my name is \"john\" "
$ORIGINAL-^781+^617
```

## Specify Element Rule

Header element rules perform operations on the elements of a header. Header elements include all subparts of a header, excluding the header name. For example, header value, header parameter, URI parameter, and so on.

1. In the **cfgRules** field, click **<Add>**, and then select **element-rule** from the drop-down list. This allows you to define the element rules you want to use to be performed on the elements of the header specified by the header rule. The following dialog box displays.



2. In the **Name** field, enter the name of the element to which this rule applies. Valid values are alpha-numeric characters. Default is blank.
3. In the **Parameter name** field, enter the parameter name to which this rule applies. The parameter name depends on the element name you entered in step 2. For uri-param, uri-user-param, and header-param it is the parameter name to be added, replaced, or deleted. For all other types, it serves to identify the element rule and any name can be used. Valid values are alpha-numeric characters. Default is blank.
4. In the **Type** field, select the type of element on which to perform the action. Default is blank. Valid values are:
  - header-param—Perform the action on the parameter portion of the header.
  - header-param-name—Perform the action on the header parameter name.
  - header-value—Perform the action on the header value.
  - mime—Perform the action on Multipurpose Internet Mail Extensions (MIME).
  - reason-phrase—Perform the action on reason phrases.
  - status-code—Perform the action on status codes.
  - teluri-param—Perform the action on a SIP telephone Uniform Resource Identifier (URI).
  - uri-display—Perform the action on the display of the SIP URI.
  - uri-header—Perform the action on a header included in a request constructed from the URI.
  - uri-header-name—Perform the action on a SIP URI header name.
  - uri-host—Perform the action on a Host portion of the SIP URI.
  - uri-param—Perform the action on the parameter included in the SIP URI.
  - uri-param-name—Perform the action on the name parameter of the SIP URI.
  - uri-phone-number-only—Perform the action on a SIP URI phone number only.
  - uri-port—Perform the action on the port number portion of the SIP URI.
  - uri-user—Perform the action on the user portion of the SIP URI.
  - uri-user-only—Perform the action on the user portion only of the SIP URI.
  - uri-user-param—Perform the action on the user parameter of the SIP URI.
5. In the **Action** field, enter the action you want applied to the element specified in the Name parameter, if there is a match value. Default is **none**. Valid values are:
  - add—Adds a new element, if that element does not already exist.
  - delete-element—Deletes the element, if it exists.
  - delete-header—Delete the header where this element exists.
  - find-replace-all—Finds all matching elements and replaces it with the element you specified in this procedure.
  - log—Logs the element.
  - none—(default) No action is taken.
  - reject—Rejects the element.
  - replace—Replaces the element

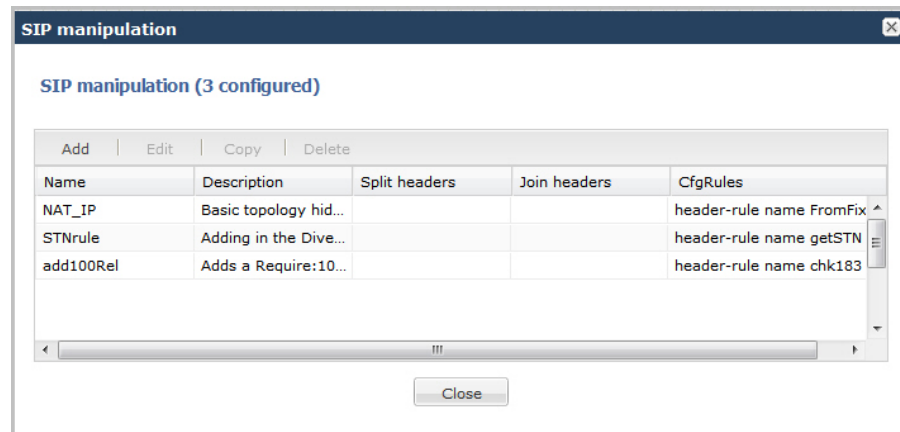
- sip-manip—Manipulates the SIP elements of this header to the element rules configured.
  - store—Stores the element.
6. In the **Match val type** field, select the type of value that needs to be matched to the match-field entry for the action to be performed. Default is **any**. Valid values are:
    - any—(default) Element value in the SIP message is compared with the match-value field entry. If the match-value field is empty, all values are considered a match.
    - fqdn—Element value in the SIP message must be a valid FQDN to be compared to the match-value field entry. If the match-value field is empty, any valid FQDN is considered a match. If the element value is not a valid FQDN, it is not considered a match.
    - ip—Element value in the SIP message must be a valid IP address to be compared to the match-value field entry. If the match-value field is empty, any valid IP address is considered a match. If the element value is not a valid IP address, it is not considered a match.
  7. In the **Comparison type** field, select the way that you want SIP elements to be compared. This choice dictates how the Oracle Enterprise Session Border Controller processes the match rules against the SIP header. Default is **case-sensitive**. Valid values are:
    - boolean—Header is compared to header rule and must match exactly or it is rejected.
    - case-insensitive—Header is compared to header rule regardless of the case of the header.
    - case-sensitive—(default) Header is compared to the header rule and case must be exactly the same or it is rejected.
    - pattern-rule—Header is compared to the header rule and the pattern must be exactly the same or it is rejected.
    - refer-case-insensitive—Header is compared to the header rule regardless of the case in a REFER message.
    - refer-case-sensitive—Header is compared to the header rule and the case must be exactly the same as in the REFER message or it is rejected.
  8. In the **Match value** field, enter the value you want to match against the element value for an action to be performed.
  9. In the **New value** field, enter the value for a new element or to replace a value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.
    - Absolute values - use double quotes for clarity. You must escape all double quotes and back slashes that are part of an absolute value, and enclose the absolute value in double quotes.  
For example:  
sip:”+\$STRUNK\_GROUP+”.\$STRUNK\_GROUP\_CONTEXT
    - Pre-defined parameters always start with a \$. For valid values, see the Pre-defined Parameters Table.
    - Operators parameters - For valid values, see the Operators Table.Examples of entries for the **new-value** field.  
\$ORIGINAL+acme  
\$ORIGINAL+”my name is john”

```

$ORIGINAL+"my name is \"john\"
$ORIGINAL-^781+^617

```

10. Click **<OK>**. The Header Rule dialog box displays.



11. Click **<Close>**.

## Configuring MIME Rules

Using the SIP Head Manipulation Rule (HMR) feature set, you can manipulate Multipurpose Internet Mail Extensions (MIME) types in SIP message bodies. While you can manipulate the body of SIP messages or a specific content type using other iterations of SIP HMR, this version gives you the power to change the MIME attachment of a specific type within the body by using regular expressions.

To achieve this, you use the find-replace-all action type, which enables the search for a particular string and the replacement of all matches for that type. Although you use find-replace-all to manipulate MIME attachments, it can also be used to achieve other goals in SIP HMR. Note that using find-replace-all might consume more system resources than other HMR types. Therefore this powerful action type should only be used when another type cannot perform the type of manipulation you require.

For more information about configuring MIME rules, see the section, MIME Support in the *Net-Net® Enterprise Session Director Configuration Guide*.

To configure MIME rules:

1. After adding a new SIP manipulation rule, go to the SIP Manipulation dialog box.

SIP manipulation
✕

### Modify SIP manipulation

Name:

Description:

Split headers:  |  |

Join headers:  |  |

**cfgRules**

Add | Edit | Copy | Delete | Move up | Move down

Name	Element type
FromFix	header-rule
ToFix	header-rule
PAIFix	header-rule
HeaderRule1	header-rule

2. In the **cfgRules** field, click **<Add>** and select **mime-rules from the drop-down list**. This allows you to specify mime rules for the header rules you configured. The following dialog box displays.





3. In the **Name** field, enter a name you want to use for this MIME rule. Valid values are alpha-numeric characters. Default is blank.
4. In the **Content type** field, enter the content type of the MIME. For example, application/sipfrag or application/sdp. This value is the content type that the Oracle Enterprise Session Border Controller looks for in the MIME. Valid values are alpha-numeric characters. Default is blank.
5. In the **Msg type** field, specify the type of message to which this MIME rule applies. Default is **any**. Valid values are:
  - any—Both Requests and Reply messages
  - out-of-dialog—Out of dialog messages only.
  - reply—Reply messages only
  - request—Request messages only
6. In the **Methods** field, specify the SIP method names to which you want to apply this MIME rule.

Click <Add>. The following displays.

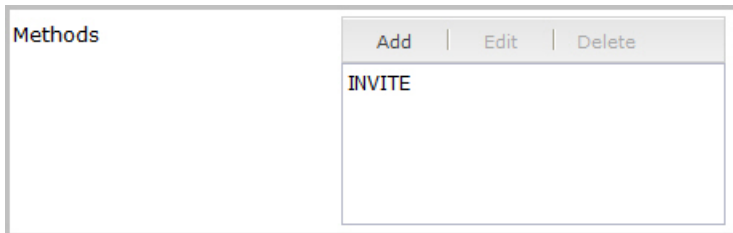
In the **Methods** field, enter SIP method names to which you want to apply this MIME rule. For example, INVITE, ACK, BYE.

 **Note:**

This field is empty by default. If you leave the method field empty, the MIME rule applies to all methods.

To add the method to the list and apply another one, click <Apply/Add Another>.

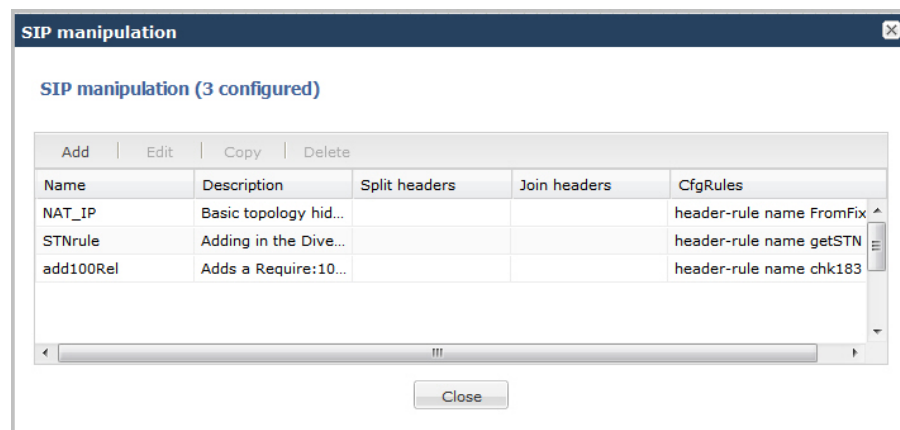
When you have completed adding methods, click <OK>. The following displays.



The screenshot shows a window titled "Methods" with a list containing the text "INVITE". Above the list are three buttons: "Add", "Edit", and "Delete".

7. In the **Format** field, select the format to apply to this MIME rule. Default is **ascii-string**. Valid values are:
  - **ascii-string** - a character-encoding scheme that represents text (128 ASCII codes, 7 bits)
  - **binary-ascii** - encoding scheme where each byte of an ASCII character is used; can use up to 256 bit patterns
  - **hex-ascii** - encoding scheme that uses a string of numbers (no spaces) to represent each ASCII character.
8. In the **Action** field, enter the action you want applied to the MIME rule specified in the Name parameter, if there is a match value. Default is **none**. Valid values are:
  - **add**—Adds a new element, if that element does not already exist.
  - **delete**—Deletes the element, if it exists.
  - **find-replace-all**—Finds all matching elements and replaces it with the element you specified in this procedure.
  - **log**—Logs the element.
  - **manipulate**—Manipulates the elements of this header to the element rules configured.
  - **monitor**—Monitors the header for this element.
  - **none**—(default) No action is taken.
  - **reject**—Rejects the element.
  - **sip-manip**—Manipulates the SIP elements of this header to the element rules configured.
  - **store**—Stores the element.
9. In the **Comparison type** field, select the way that you want the MIME to be compared with this MIME rule. This choice dictates how the Oracle Enterprise Session Border Controller processes the match rules against the MIME. Default is **case-sensitive**. Valid values are:

- boolean—Header is compared to MIME rule and must match exactly or it is rejected.
  - case-insensitive—Header is compared to MIME rule regardless of the case of the header.
  - case-sensitive—(default) Header is compared to the MIME rule and case must be exactly the same or it is rejected.
  - pattern-rule—Header is compared to the MIME rule and the pattern must be exactly the same or it is rejected.
  - refer-case-insensitive—Header is compared to the header rule regardless of the case in a REFER message.
  - refer-case-sensitive—Header is compared to the header rule and the case must be exactly the same as in the REFER message or it is rejected.
10. In the **Match value** field, enter the value you want to match against the element value for an action to be performed.
11. In the **New value** field, enter the value for a new element or to replace a value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.
- Absolute values - use double quotes for clarity. You must escape all double quotes and back slashes that are part of an absolute value, and enclose the absolute value in double quotes.
- For example:
- ```
sip:~+$STRUNK_GROUP+~.$STRUNK_GROUP_CONTEXT
```
- Pre-defined parameters always start with a \$. For valid values, see the Pre-defined Parameters Table.
  - Operators parameters - For valid values, see the Operators Table.
- Examples of entries for the **new-value** field.
- ```
$ORIGINAL+acme
$ORIGINAL+"my name is john"
$ORIGINAL+"my name is \"john\""
$ORIGINAL-^781+^617
```
12. Click **<OK>**. The MIME Rule dialog box displays.
13. Click **<OK>**. The SIP Manipulation dialog box displays.



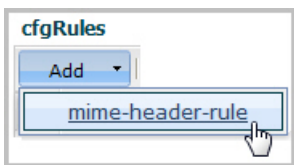

14. Click <Close>.

## Configuring MIME Header Rule

You can configure MIME header rules within a MIME rule. Use the following procedure to configure a MIME header rule.

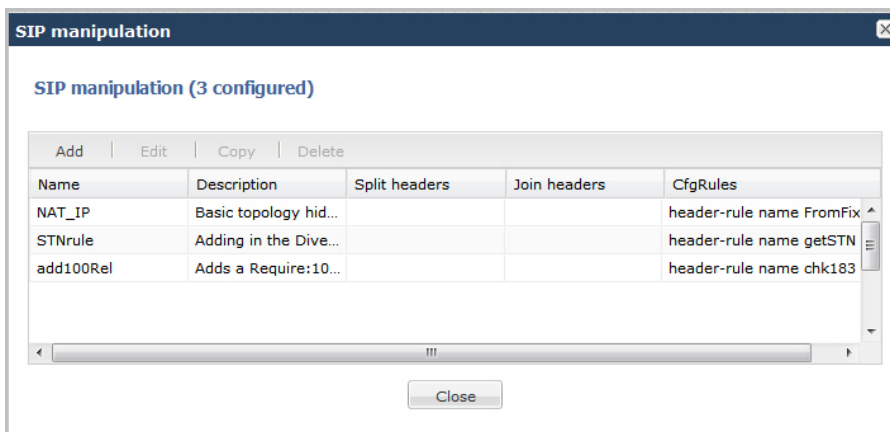
To configure a MIME header rule:

1. In the MIME rules dialog box, in the **cfgRules** field, click <Add>, and then select **mime-header-rule** from the drop-down list. This allows you to define the MIME rules you want to use to be performed on the elements of the header specified by the MIME rule. The following dialog box displays.

2. In the **Name** field, enter the name of the element to which this rule applies. Valid values are alpha-numeric characters. Default is blank.
3. In the **Mime header name** field, enter the parameter name to which this rule applies. The parameter name depends on the element name you entered in step 2. For uri-param, uri-user-param, and header-param it is the parameter name to be added, replaced, or deleted. For all other types, it serves to identify the element rule and any name can be used. Valid values are alpha-numeric characters. Default is blank.
4. In the **Action** field, enter the action you want applied to the MIME rule specified in the Name parameter, if there is a match value. Default is **none**. Valid values are:
  - add—Adds a new element, if that element does not already exist.
  - delete—Deletes the element, if it exists.
  - find-replace-all—Finds all matching elements and replaces it with the element you specified in this procedure.
  - log—Logs the element.
  - monitor—Monitors the header for this element.

- none—(default) No action is taken.
  - reject—Rejects the element.
  - replace—Replaces the element.
  - sip-manip—Manipulates the SIP elements of this header to the element rules configured.
  - store—Stores the element.
5. In the **Comparison type** field, select the way that you want the MIME to be compared with this MIME rule. This choice dictates how the Oracle Enterprise Session Border Controller processes the match rules against the MIME. Default is **case-sensitive**. Valid values are:
- boolean—Header is compared to MIME rule and must match exactly or it is rejected.
  - case-insensitive—Header is compared to MIME rule regardless of the case of the header.
  - case-sensitive—(default) Header is compared to the MIME rule and case must be exactly the same or it is rejected.
  - pattern-rule—Header is compared to the MIME rule and the pattern must be exactly the same or it is rejected.
  - refer-case-insensitive—Header is compared to the header rule regardless of the case in a REFER message.
  - refer-case-sensitive—Header is compared to the header rule and the case must be exactly the same as in the REFER message or it is rejected.
6. In the **Match value** field, enter the value you want to match against the element value for an action to be performed.
7. In the **New value** field, enter the value for a new element or to replace a value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.
- Absolute values - use double quotes for clarity. You must escape all double quotes and back slashes that are part of an absolute value, and enclose the absolute value in double quotes.
- For example:
- ```
sip:"+$STRUNK_GROUP+".$STRUNK_GROUP_CONTEXT
```
- Pre-defined parameters always start with a \$. For valid values, see the Pre-defined Parameters Table.
  - Operators parameters - For valid values, see the Operators Table.
- Examples of entries for the **new-value** field.
- ```
$ORIGINAL+acme  
$ORIGINAL+"my name is john"  
$ORIGINAL+"my name is \"john\""  
$ORIGINAL-^781+^617
```
8. Click **<OK>**. The MIME Rule dialog box displays.
9. Click **<OK>**. The SIP Manipulation dialog box displays.



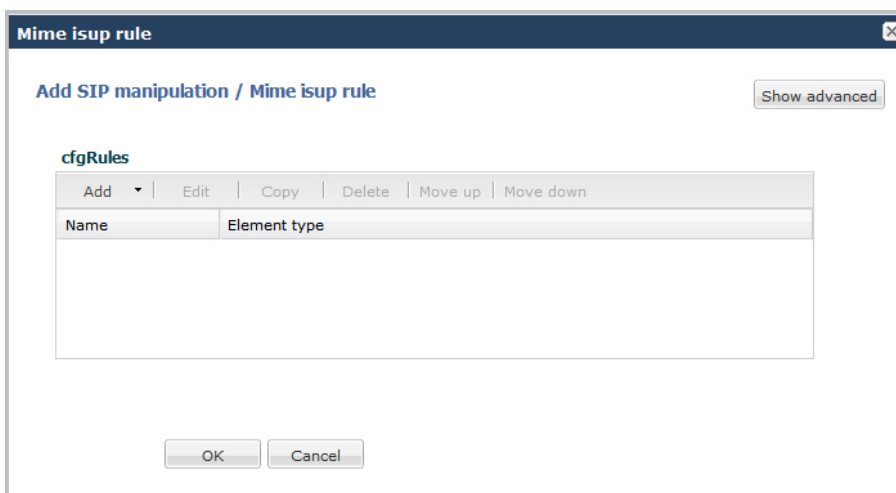
10. Click <Close>.

## Configuring MIME ISUP Rule

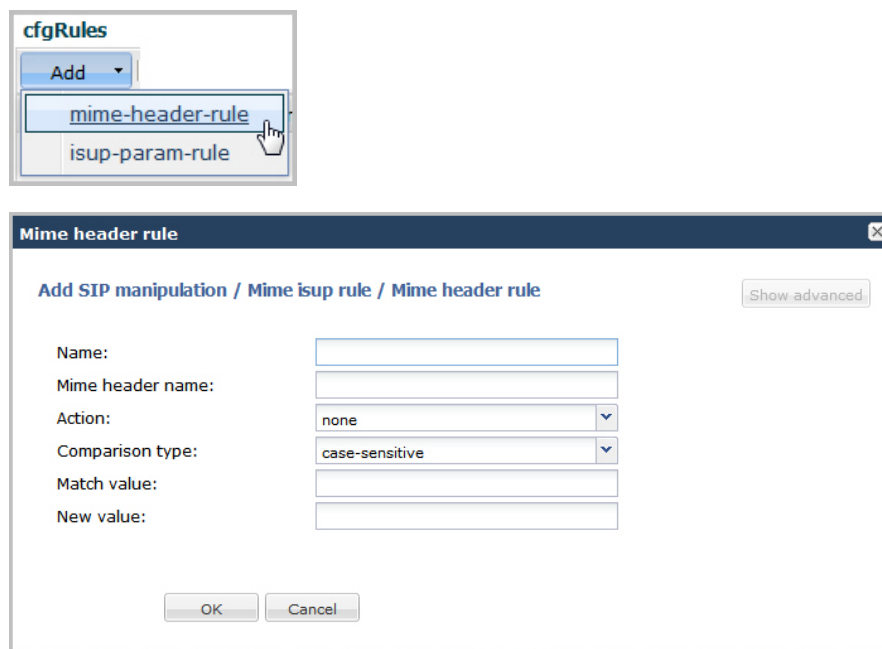
You can configure a MIME ISDN User Part (ISUP) rule for a SIP manipulation rule. Use the following procedure to configure a MIME ISUP rule.

To configure a MIME ISUP rule:

1. In the SIP Manipulation dialog box, in the **cfgRules** field, click <Add>, and then select **mime-isup-rule** from the drop-down list. This allows you to define the MIME ISUP rules you want to use to be performed on the elements of the header specified by the MIME rule. The following dialog box displays.



2. In the **cfgRules** field, click <Add>, and then select **mime-header-rule** from the drop-down list. The following dialog box displays.



3. In the **Name** field, enter the name of the element to which this rule applies. Valid values are alpha-numeric characters. Default is blank.
4. In the **Mime header name** field, enter the parameter name to which this rule applies. The parameter name depends on the element name you entered in step 3. For uri-param, uri-user-param, and header-param it is the parameter name to be added, replaced, or deleted. For all other types, it serves to identify the element rule and any name can be used. Valid values are alpha-numeric characters. Default is blank.
5. In the **Action** field, enter the action you want applied to the MIME rule specified in the Name parameter, if there is a match value. Default is **none**. Valid values are:
  - add—Adds a new element, if that element does not already exist.
  - delete—Deletes the element, if it exists.
  - find-replace-all—Finds all matching elements and replaces it with the element you specified in this procedure.
  - log—Logs the element.
  - monitor—Monitors the header for this element.
  - none—(default) No action is taken.
  - reject—Rejects the element.
  - replace—Replaces the element.
  - sip-manip—Manipulates the SIP elements of this header to the element rules configured.
  - store—Stores the element.
6. In the **Comparison type** field, select the way that you want the MIME to be compared with this MIME rule. This choice dictates how the Oracle Enterprise Session Border Controller processes the match rules against the MIME. Default is **case-sensitive**. Valid values are:
  - boolean—Header is compared to MIME rule and must match exactly or it is rejected.

- case-insensitive—Header is compared to MIME rule regardless of the case of the header.
  - case-sensitive—(default) Header is compared to the MIME rule and case must be exactly the same or it is rejected.
  - pattern-rule—Header is compared to the MIME rule and the pattern must be exactly the same or it is rejected.
  - refer-case-insensitive—Header is compared to the header rule regardless of the case in a REFER message.
  - refer-case-sensitive—Header is compared to the header rule and the case must be exactly the same as in the REFER message or it is rejected.
7. In the **Match value** field, enter the value you want to match against the element value for an action to be performed.
  8. In the **New value** field, enter the value for a new element or to replace a value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.
    - Absolute values - use double quotes for clarity. You must escape all double quotes and back slashes that are part of an absolute value, and enclose the absolute value in double quotes.

For example:

```

sip:~+$STRUNK_GROUP+~$.STRUNK_GROUP_CONTEXT

```

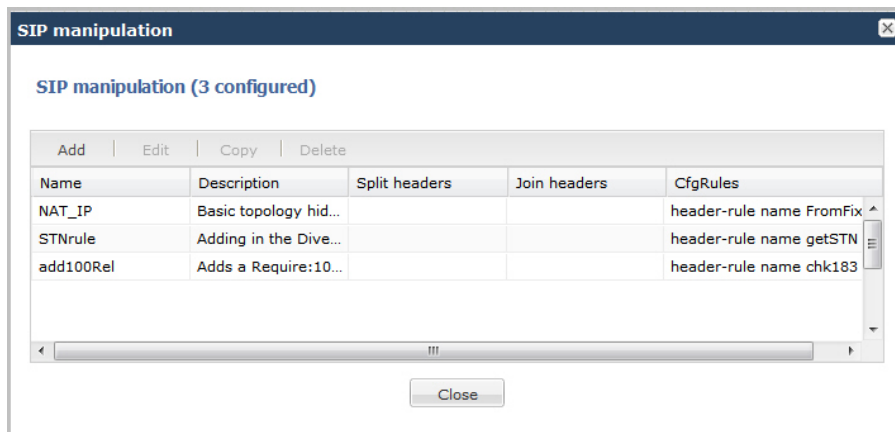
    - Pre-defined parameters always start with a \$. For valid values, see the Pre-defined Parameters Table.
    - Operators parameters - For valid values, see the Operators Table.

Examples of entries for the **new-value** field.

```

$ORIGINAL+acme
$ORIGINAL+"my name is john"
$ORIGINAL+"my name is \"john\""
$ORIGINAL-^781+^617

```
  9. Click **<OK>**. The MIME ISUP Rule dialog box displays.
  10. Click **<OK>**. The SIP Manipulation dialog box displays.



11. Click **<Close>**.



## Configuring ISUP Param Rules

The ISUP param rules are for advanced users only. This feature configures the following for the ISUP param rules:

- Name
- Type
- Format
- Action
- Comparison Type
- Match Value
- New Value

For more information about configuring ISUP Param Rules, see the section, Regular Expressions and Boolean Expressions in the *Net-Net® Enterprise Session Director Configuration Guide*.

## Configuring MIME SDP Rules

You can configure MIME Session Description Protocol (SDP) rules for SIP Manipulation on the Oracle Enterprise Session Border Controller if required. Use the following procedure to configure MIME SDP rules.

To configuration MIME SDP rules:

1. From the SIP Manipulation dialog box, in the **cfgRules** field, click <Add>, and then select **mime-sdp-rule** from the drop-down list. The following dialog box displays.



2. In the **Name** field, enter a name you want to use for this MIME SDP rule. Valid values are alpha-numeric characters. Default is blank.
3. In the **Msg type** field, specify the type of message to which this MIME SDP rule applies. Default is **any**. Valid values are:
  - any—Both Requests and Reply messages
  - out-of-dialog—Out of dialog messages only.
  - reply—Reply messages only
  - request—Request messages only
4. In the **Methods** field, specify the SIP method names to which you want to apply this MIME SDP rule.

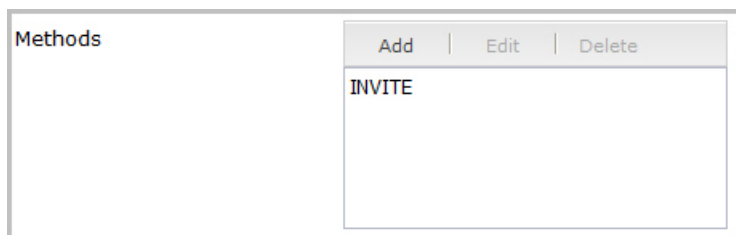
Click <Add>. The following displays.

In the Methods field, enter SIP method names to which you want to apply this MIME SDP rule. For example, INVITE, ACK, BYE.

 **Note:**

This field is empty by default. If you leave the method field empty, the MIME rule applies to all methods.

To add the method to the list and apply another one, click <Apply/Add Another>. When you have completed adding methods, click <OK>. The following displays.



5. In the **Action** field, enter the action you want applied to the MIME SDP rule specified in the Name parameter, if there is a match value. Default is **none**. Valid values are:
  - add—Adds a new element, if that element does not already exist.
  - delete—Deletes the element, if it exists.
  - find-replace-all—Finds all matching elements and replaces it with the element you specified in this procedure.
  - log—Logs the element.
  - manipulate—Manipulates the elements of this header to the element rules configured.
  - monitor—Monitors the header for this element.
  - none—(default) No action is taken.
  - reject—Rejects the element.
  - sip-manip—Manipulates the SIP elements of this header to the element rules configured.
  - store—Stores the element.
6. In the **Comparison type** field, select the way that you want the MIME to be compared with this MIME SDP rule. This choice dictates how the Oracle Enterprise Session Border Controller processes the match rules against the MIME. Default is **case-sensitive**. Valid values are:
  - boolean—Header is compared to MIME rule and must match exactly or it is rejected.
  - case-insensitive—Header is compared to MIME rule regardless of the case of the header.
  - case-sensitive—(default) Header is compared to the MIME rule and case must be exactly the same or it is rejected.
  - pattern-rule—Header is compared to the MIME rule and the pattern must be exactly the same or it is rejected.
  - refer-case-insensitive—Header is compared to the header rule regardless of the case in a REFER message.
  - refer-case-sensitive—Header is compared to the header rule and the case must be exactly the same as in the REFER message or it is rejected.
7. In the **Match value** field, enter the value you want to match against the element value for an action to be performed.
8. In the **New value** field, enter the value for a new element or to replace a value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.

- Absolute values - use double quotes for clarity. You must escape all double quotes and back slashes that are part of an absolute value, and enclose the absolute value in double quotes.

For example:

```
sip:~+$STRUNK_GROUP+~.$STRUNK_GROUP_CONTEXT
```

- Pre-defined parameters always start with a \$. For valid values, see the Pre-defined Parameters Table.
- Operators parameters - For valid values, see the Operators Table.

Examples of entries for the **new-value** field.

```
$ORIGINAL+acme  
$ORIGINAL+"my name is john"  
$ORIGINAL+"my name is \"john\""  
$ORIGINAL-^781+^617
```

## Configuring MIME Header Rule for SDP

You can configure the MIME header rule for the MIME SDP rule if required. Use the procedures in Configuring MIME Header Rule to configure the MIME header rule fo SDP.

## Configuring SDP Session Rule

You can configure the SDP session rules for the MIME SDP rules if required. Use the following procedure to configure SDP Session rules.

To configure SDP session rules:

1. In the MIME SDP Rules dialog box, in the **cfgRules** field, click **<Add>**, and then select **sdp-session-rule** from the drop-down list. This allows you to define the SDP session rules you want to use to be performed on the elements of the header specified by the MIME rule. The following dialog box displays.



2. In the **Name** field, enter the name of the element to which this rule applies. Valid values are alpha-numeric characters. Default is blank.
3. In the **Action** field, enter the action you want applied to the SDP session rule specified in the Name parameter, if there is a match value. Default is **none**. Valid values are:
  - add—Adds a new element, if that element does not already exist.
  - delete—Deletes the element, if it exists.
  - find-replace-all—Finds all matching elements and replaces it with the element you specified in this procedure.
  - log—Logs the element.
  - monitor—Monitors the header for this element.
  - none—(default) No action is taken.
  - reject—Rejects the element.
  - replace—Replaces the element.
  - sip-manip—Manipulates the SIP elements of this header to the element rules configured.
  - store—Stores the element.
4. In the **Comparison type** field, select the way that you want the MIME to be compared with this SDP session rule. This choice dictates how the Oracle Enterprise Session Border Controller processes the match rules against the MIME. Default is **case-sensitive**. Valid values are:
  - boolean—Header is compared to MIME rule and must match exactly or it is rejected.
  - case-insensitive—Header is compared to MIME rule regardless of the case of the header.
  - case-sensitive—(default) Header is compared to the MIME rule and case must be exactly the same or it is rejected.
  - pattern-rule—Header is compared to the MIME rule and the pattern must be exactly the same or it is rejected.

- refer-case-insensitive—Header is compared to the header rule regardless of the case in a REFER message.
  - refer-case-sensitive—Header is compared to the header rule and the case must be exactly the same as in the REFER message or it is rejected.
5. In the **Match value** field, enter the value you want to match against the element value for an action to be performed.
  6. In the **New value** field, enter the value for a new element or to replace a value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.
    - Absolute values - use double quotes for clarity. You must escape all double quotes and back slashes that are part of an absolute value, and enclose the absolute value in double quotes.

For example:

```
sip:~+$STRUNK_GROUP+~.$STRUNK_GROUP_CONTEXT
```

- Pre-defined parameters always start with a \$. For valid values, see the Pre-defined Parameters Table.
- Operators parameters - For valid values, see the Operators Table.

Examples of entries for the **new-value** field.

```
$ORIGINAL+acme
$ORIGINAL+"my name is john"
$ORIGINAL+"my name is \"john\""
$ORIGINAL-^781+^617
```

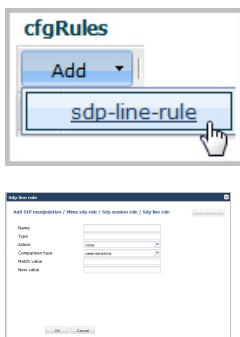
## Configuring SDP Line Rules for Sessions

When configuring the SDP session rules, you can also configure the SDP line rules. For more information about configuring SDP line rules, see the section, `sdp-line-rule` in the *Net-Net® Enterprise Session Director Configuration Guide*.

Use the following procedure to configure the SDP line rules.

To configure SDP line rules:

1. From the SDP Session Rule dialog box, in the **cfgRules** field, click <Add>, and then select **sdp-line-rules** from the drop-down list. This allows you to define the SDP line rules you want to use to be performed on the elements of the header specified by the SDP session rule. The following dialog box displays.



2. In the **Name** field, enter the name of the element to which this rule applies. Valid values are alpha-numeric characters. Default is blank.

3. In the **Type** field, enter the applicable SDP descriptor for the SDP line rule. SDP descriptors are added to the SDP, adhering to the definitions in RFC 4566. Default is blank. Valid values are:

---

Session Description	
v	Protocol version
o	Originator and session identifier
s	Session name
i	Session information*
u	URI of description*
e	Email address*
p	Phone number*
c	Connection information - not required if included in all media*
b	Zero or more bandwidth information lines* One or more time descriptions (“t=” and r= lines; see below)
z	Time zone adjustments*
k	Encryption key*
a	Zero or more session attribute lines* Zero or more media descriptions (see below)
Time Description	
t	Time the session is active
r	Zero or more repeat times*

---

\*Indicates an optional descriptor

4. In the **Action** field, enter the action you want applied to the SDP line rule specified in the Name parameter, if there is a match value. Default is **none**. Valid values are:
- add—Adds a new element, if that element does not already exist.
  - delete—Deletes the element, if it exists.
  - find-replace-all—Finds all matching elements and replaces it with the element you specified in this procedure.
  - log—Logs the element.
  - monitor—Monitors the header for this element.
  - none—(default) No action is taken.
  - reject—Rejects the element.
  - replace—Replaces the element.
  - sip-manip—Manipulates the SIP elements of this header to the element rules configured.
  - store—Stores the element.
5. In the **Comparison type** field, select the way that you want the MIME to be compared with this SDP line rule. This choice dictates how the Oracle Enterprise Session Border Controller processes the match rules against the MIME. Default is **case-sensitive**. Valid values are:
- boolean—Header is compared to MIME rule and must match exactly or it is rejected.
  - case-insensitive—Header is compared to MIME rule regardless of the case of the header.

- case-sensitive—(default) Header is compared to the MIME rule and case must be exactly the same or it is rejected.
  - pattern-rule—Header is compared to the MIME rule and the pattern must be exactly the same or it is rejected.
  - refer-case-insensitive—Header is compared to the header rule regardless of the case in a REFER message.
  - refer-case-sensitive—Header is compared to the header rule and the case must be exactly the same as in the REFER message or it is rejected.
6. In the **Match value** field, enter the value you want to match against the element value for an action to be performed.
  7. In the **New value** field, enter the value for a new element or to replace a value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.

- Absolute values - use double quotes for clarity. You must escape all double quotes and back slashes that are part of an absolute value, and enclose the absolute value in double quotes.

For example:

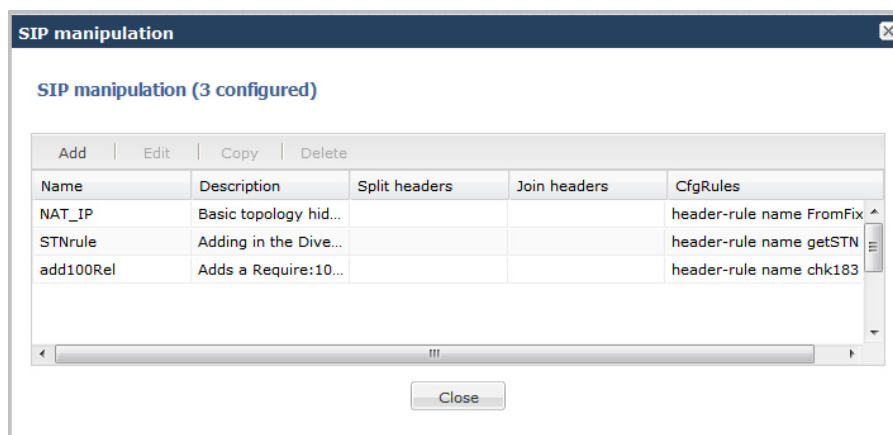
```
sip:~+$STRUNK_GROUP+~.$STRUNK_GROUP_CONTEXT
```

- Pre-defined parameters always start with a \$. For valid values, see the Pre-defined Parameters Table.
- Operators parameters - For valid values, see the Operators Table.

Examples of entries for the **new-value** field.

```
$ORIGINAL+acme
$ORIGINAL+"my name is john"
$ORIGINAL+"my name is \"john\""
$ORIGINAL-^781+^617
```

8. Click **<OK>**. The SDP Session Rule dialog box displays.
9. Click **<OK>**. The SIP Manipulation dialog box displays.



10. Click **<Close>**.

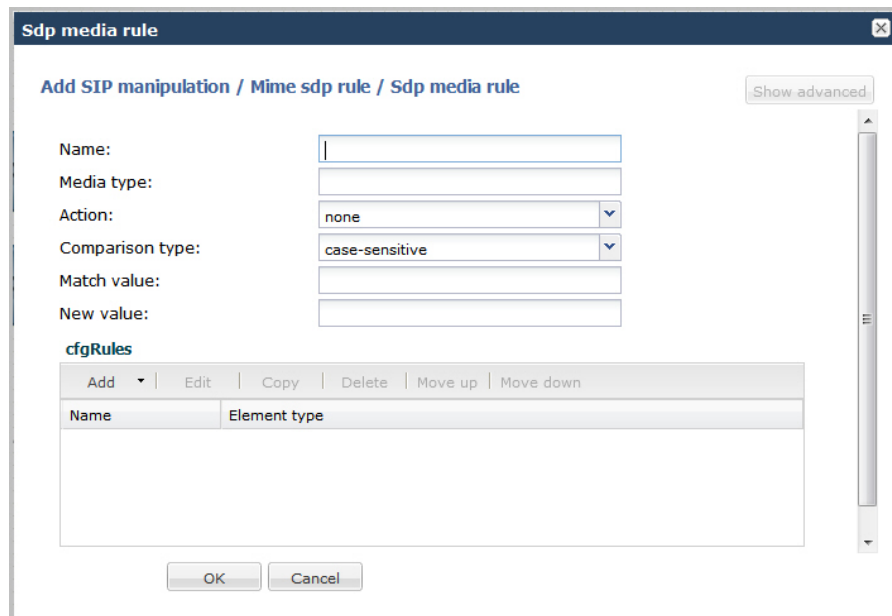


## Configuring SDP Media Rules

When configuring the SDP session rules, you can also configure the SDP media rules. Use the following procedure to configure the SDP media rules.

To configure SDP media rules:

1. From the SDP Session Rule dialog box, in the **cfgRules** field, click <Add>, and then select **sdp-media-rule** from the drop-down list. This allows you to define the SDP media rules you want to use to be performed on the elements of the header specified by the SDP session rule. The following dialog box displays.



2. In the **Name** field, enter the name of the element to which this rule applies. Valid values are alpha-numeric characters. Default is blank.
3. In the **Media Type** field, enter the applicable SDP descriptor for the SDP media rule. SDP descriptors are added to the SDP, adhering to the definitions in RFC 4566. Default is blank. Valid values are:

Media Description (if present)

- |   |   |
|---|---|
| m | Media name and transport address                                |
| i | Media title*  |
| c | Connection information - optional if included at session level* |
| b | Zero or more bandwidth information lines*                       |
| k | Encryption key*   |

---

a	Zero or more media attribute lines*
Time	Description
t	Time the session is active
r	Zero or more repeat times*

---

\*Indicates an optional descriptor

4. In the **Action** field, enter the action you want applied to the SDP media rule specified in the Name parameter, if there is a match value. Default is **none**. Valid values are:
  - add—Adds a new element, if that element does not already exist.
  - delete—Deletes the element, if it exists.
  - find-replace-all—Finds all matching elements and replaces it with the element you specified in this procedure.
  - log—Logs the element.
  - monitor—Monitors the header for this element.
  - none—(default) No action is taken.
  - reject—Rejects the element.
  - replace—Replaces the element.
  - sip-manip—Manipulates the SIP elements of this header to the element rules configured.
  - store—Stores the element.
5. In the **Comparison type** field, select the way that you want the MIME to be compared with this SDP media rule. This choice dictates how the Oracle Enterprise Session Border Controller processes the match rules against the MIME. Default is **case-sensitive**. Valid values are:
  - boolean—Header is compared to MIME rule and must match exactly or it is rejected.
  - case-insensitive—Header is compared to MIME rule regardless of the case of the header.
  - case-sensitive—(default) Header is compared to the MIME rule and case must be exactly the same or it is rejected.
  - pattern-rule—Header is compared to the MIME rule and the pattern must be exactly the same or it is rejected.
  - refer-case-insensitive—Header is compared to the header rule regardless of the case in a REFER message.
  - refer-case-sensitive—Header is compared to the header rule and the case must be exactly the same as in the REFER message or it is rejected.
6. In the **Match value** field, enter the value you want to match against the element value for an action to be performed.
7. In the **New value** field, enter the value for a new element or to replace a value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.
  - Absolute values - use double quotes for clarity. You must escape all double quotes and back slashes that are part of an absolute value, and enclose the absolute value in double quotes.  
For example:

sip:”+\$STRUNK\_GROUP+”.\$STRUNK\_GROUP\_CONTEXT

- Pre-defined parameters always start with a \$. For valid values, see the Pre-defined Parameters Table.
- Operators parameters - For valid values, see the Operators Table.

Examples of entries for the **new-value** field.

```
$ORIGINAL+acme
$ORIGINAL+"my name is john"
$ORIGINAL+"my name is \"john\" "
$ORIGINAL-^781+^617
```

## Configuring SDP Line Rules for Media

You can configure SDP Line Rules for Media if required. For more information about configuring SDP line rules, see the section, sdp-line-rule in the *Net-Net® Enterprise Session Director Configuration Guide*.

Use the following procedure to configure SDP line rules for media.

To configure SDP line rules for media:

1. From the SDP Media Rule dialog box, in the **cfgRules** field, click <Add>, and then select **sdp-line-rule** from the drop-down list. This allows you to define the SDP line rules you want to use to be performed on the elements of the header specified by the SDP media rule. The following dialog box displays.



2. In the **Name** field, enter the name of the element to which this rule applies. Valid values are alpha-numeric characters. Default is blank.
3. In the **Type** field, enter the applicable SDP descriptor for the SDP line rule. SDP descriptors are added to the SDP, adhering to the definitions in RFC 4566. Default is blank. Valid values are:

---

Session Description	
v	Protocol version
o	Originator and session identifier
s	Session name
i	Session information*
u	URI of description*
e	Email address*
p	Phone number*
c	Connection information - not required if included in all media*
b	Zero or more bandwidth information lines* One or more time descriptions (“t=” and r= lines; see below)
z	Time zone adjustments*
k	Encryption key*
a	Zero or more session attribute lines* Zero or more media descriptions (see below)
Time Description	
t	Time the session is active
r	Zero or more repeat times*

---

\*Indicates an optional descriptor

- In the **Action** field, enter the action you want applied to the SDP line rule specified in the Name parameter, if there is a match value. Default is **none**. Valid values are:
  - add—Adds a new element, if that element does not already exist.
  - delete—Deletes the element, if it exists.
  - find-replace-all—Finds all matching elements and replaces it with the element you specified in this procedure.
  - log—Logs the element.
  - monitor—Monitors the header for this element.
  - none—(default) No action is taken.
  - reject—Rejects the element.
  - replace—Replaces the element.
  - sip-manip—Manipulates the SIP elements of this header to the element rules configured.
  - store—Stores the element.
- In the **Comparison type** field, select the way that you want the MIME to be compared with this SDP line rule. This choice dictates how the Oracle Enterprise Session Border Controller processes the match rules against the MIME. Default is **case-sensitive**. Valid values are:
  - boolean—Header is compared to MIME rule and must match exactly or it is rejected.
  - case-insensitive—Header is compared to MIME rule regardless of the case of the header.
  - case-sensitive—(default) Header is compared to the MIME rule and case must be exactly the same or it is rejected.
  - pattern-rule—Header is compared to the MIME rule and the pattern must be exactly the same or it is rejected.

- refer-case-insensitive—Header is compared to the header rule regardless of the case in a REFER message.
  - refer-case-sensitive—Header is compared to the header rule and the case must be exactly the same as in the REFER message or it is rejected.
6. In the **Match value** field, enter the value you want to match against the element value for an action to be performed.
  7. In the **New value** field, enter the value for a new element or to replace a value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.

- Absolute values - use double quotes for clarity. You must escape all double quotes and back slashes that are part of an absolute value, and enclose the absolute value in double quotes.

For example:

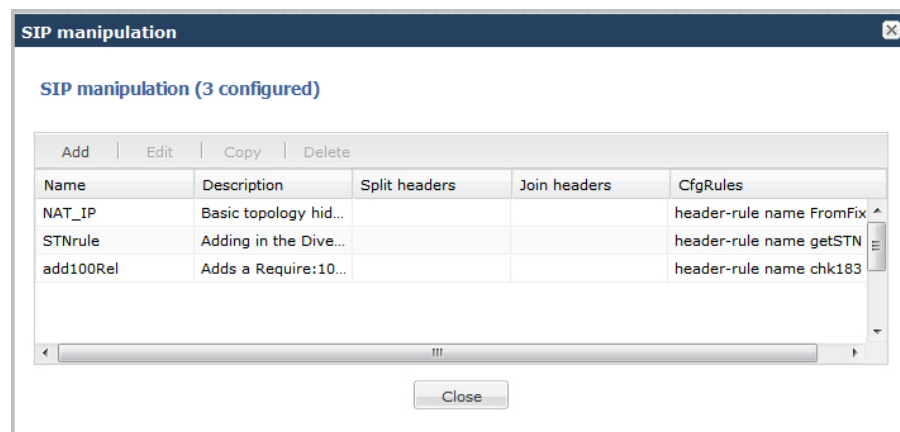
```
sip:”+$STRUNK_GROUP+”.$STRUNK_GROUP_CONTEXT
```

- Pre-defined parameters always start with a \$. For valid values, see the Pre-defined Parameters Table.
- Operators parameters - For valid values, see the Operators Table.

Examples of entries for the **new-value** field.

```
$ORIGINAL+acme
$ORIGINAL+"my name is john"
$ORIGINAL+"my name is \"john\" "
$ORIGINAL-^781+^617
```

8. Click **<OK>**. The SDP Media Rule dialog box displays.
9. Click **<OK>**. The MIME SDP Rule dialog box displays.
10. Click **<OK>**. The Modify SIP manipulation dialog box displays.
11. Click **<OK>**. The SIP Manipulation dialog box displays.



12. Click **<Close>**.

## Add an SPL

Add an SPL plugin, which is a customized script, to quickly implement a feature on the Oracle Enterprise Session Border Controller (E-SBC). The SPL plugin augments running the software

image on the E-SBC, and provides new features when you need them without having to upgrade the software.

### Before You Begin

- Confirm the name and location of the SPL plugin that you want to add.

Use the following procedure to integrate an Oracle-signed plug-in with the E-SBC operating system. Note that the E-SBC) does not load an unsigned SPL or one with invalid signatures.

### Procedure

1. From the Web GUI, click **Other** > **SPL**.
2. In the **Spl config** dialog, do the following:

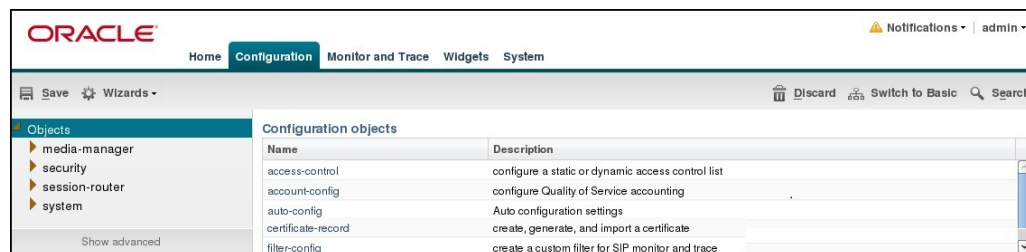
Attributes	Instructions
Spl options	Enter the name of SPL option.
Plugins	Click <b>Add</b> , and do the following: <ul style="list-style-type: none"> <li>• Select State to enable the plugin.</li> <li>• Enter the name of plugin to load.</li> <li>• Click <b>OK</b>.</li> </ul> The system displays the SPI config page.

3. Click **OK**.
4. Save and activate the configuration.

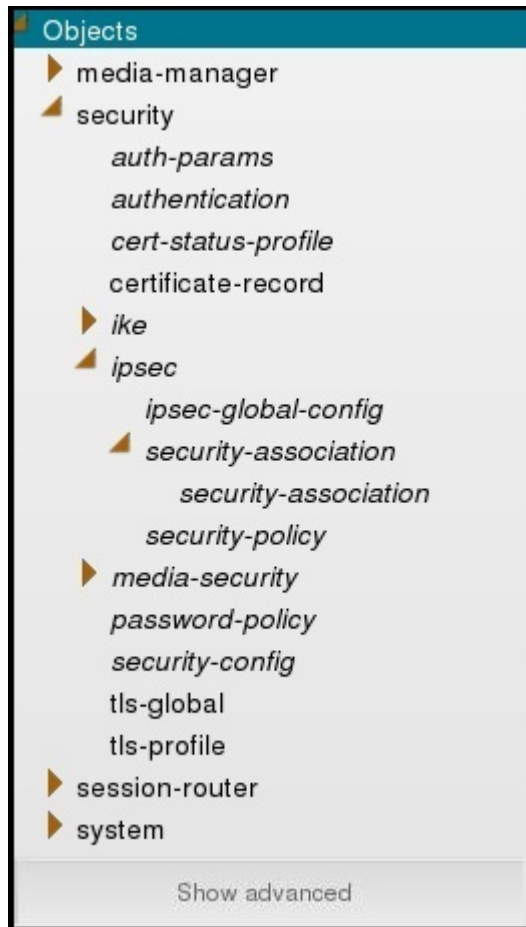
## Expert Mode Configuration

Expert mode is a method of configuring the Oracle Enterprise Session Border Controller using the ACLI configuration tree by way of the Web GUI.

The Expert mode workspace displays a list of configuration objects and elements in the left pane of the configuration page, grouped like the ACLI configuration tree and displayed in command line format. The Configuration page also lists all of the configuration objects and elements in alphabetical order in the center pane.



Click the arrow by the Objects group name in the left pane to display the basic elements in the group. For example, under security, certificate-record, tls-global, and tls-profile are basic elements.



- Click Show Advanced to display the advanced elements in the group. The system displays the advanced elements in italics. For example, under security, auth-params and authentication are some of the advanced elements displayed in italics.
- Click the arrow by an advanced element to display sub-elements. For example, under security, ipsec-global-config is a sub-element of ipsec.
- Click the object, element, or sub-element to display the corresponding configuration dialog.

In the alphabetical list of Configuration Objects, click the Name of the object or element to display the corresponding configuration dialog.

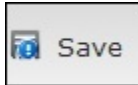
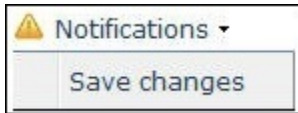
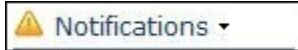
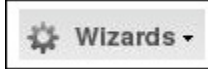



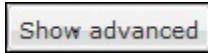
Configuration objects	
Name	
access-control	
account-config	
auto-config	
certificate-record	
filter-config	

 **Note:**

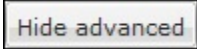

The Web GUI does not indicate required fields. You may be able to save the configuration without a required value because the E-SBC ignores the element in the configuration. The system does not display an error message for a missing required parameter.

## Expert Mode Configuration tools

Use the following tools to create the configuration in Expert Mode.

Button	Description
	Use to verify and save the current configuration in Expert Mode. A prompt also displays giving you a choice of whether or not to activate the configuration. Note: After clicking Save, a notification icon in the upper right corner of the screen indicates the configuration still needs to be activated. You can continue to make changes to the configuration as required. When finished, you can select Notifications->Save changes to save and activate the configuration. The notification icon dims after saving and activating.
	
	The system displays notifications and alarms.
	Use to a list of configuration wizards and the Update Software wizard.
	Use to perform a search of any configuration element or sub-element on the Oracle Enterprise Session Border Controller. You perform the search by entering a keyword which is not case sensitive. Special characters are allowed.
	Allows you to discard all configuration changes made in the current session. Only the changes that have not yet been activated are discarded.
	Use to switch from Expert Mode to Basic Mode. Note: If you save your configuration in Expert Mode, you cannot switch to Basic Mode. Caution: You can switch to Basic Mode from Expert Mode, if you do not save your changes. If you save your changes and you switch back to Basic Mode, you must run the Set Initial Configuration wizard again. You will lose all of the configuration changes you made in both modes.
	Use to display advanced parameters, which the system displays in italics. Is active only in configuration dialogs that contain advanced parameters.



Button	Description
	Use to hide advanced parameters from view. Is active only in configuration dialogs that contain advanced parameters.
	Use to display the sub-objects related to a configuration element in Expert mode. A configuration element that contains sub-objects displays the <b>Show configuration</b> button on the corresponding Edit configuration dialog.

## Function Buttons

Expert Mode displays function buttons on each configuration page to perform tasks such as add, edit, copy, and delete. The system activates the buttons depending on your selection on a page. Some sub-element tables also display these buttons. The following table describes each button.

Button	Description
Add	Use to add configuration information to the Oracle Enterprise Session Border Controller.
Edit	Use to edit existing configuration information. Note: Select an item in a list to enable the Edit button.
Copy	Use to copy existing configuration information, and edit the information to create a new configuration. Note: Select an item in a list to enable the Copy button.
Delete	Use to delete existing configuration information. Note: Select an item in a list to enable the Delete button.
Search	Use to search for configured objects.
Clear	Use to clear the Search field.

## Commands Button

The Commands button on the Configuration tab displays a limited menu of widgets that provide information about the state of the configuration on the Oracle Enterprise Session Border Controller (E-SBC). For example, you might want to know about objects that are already configured or which version of the configuration is running.

You can find the following configuration-related widgets in the alphabetical list on the Widgets tab, but they are grouped under the Commands button on the Configuration page for convenience.

Command	Description	Widget Controls
Show Inventory	Displays all of the configured objects.	<ul style="list-style-type: none"> <li>Refresh: Refresh the display.</li> <li>Settings: Set the auto refresh interval and opt to show only differences in the configuration in the display.</li> <li>Export: Download the inventory to a location to save.</li> </ul>

Command	Description	Widget Controls
Show Editing Configuration Short	Displays the version of the configuration that you are editing.	<ul style="list-style-type: none"> <li>Refresh: Refresh the display.</li> <li>Settings: Set the auto refresh interval.</li> </ul>
Show Running Configuration Short	Displays the version of the configuration that the E-SBC is using.	<ul style="list-style-type: none"> <li>Refresh: Refresh the display.</li> <li>Settings: Set the auto refresh interval.</li> </ul>
Show Configuration Version	Displays the current version and the running version of the configuration.	<ul style="list-style-type: none"> <li>Refresh: Refresh the display.</li> </ul>
Show Realm Specifics	Displays the name of the realm and how often the widget refreshes. You can configure both items in the dialog that displays.	<ul style="list-style-type: none"> <li>Refresh: Refresh the display.</li> <li>Settings: Select a realm and set the auto refresh interval.</li> </ul>

## Media Manager Configuration

You can configure the following media-manager objects from the Configuration tab on the Web GUI:

Object	Purpose
codec-policy	Create a codec policy to specify allowed codecs, the order of codecs, and codecs to add on egress.
dns-alg-constraints	Configure and enable DNS ALG constraints.
dns-config	Configure the DNS ALG service.
media-manager	Configure media steering functions.
media-policy	Configure a media policy and ToS settings.
msrp-config	Configure and enable MSRP.
playback-config	Configure media use for playback.
realm-config	Configure a realm for media management.
realm-group	Configure realm groups for local media playback.
rtcp-policy	Configure an RTCP policy.
static-flow	Configure static network traffic flows.
steering-pool	Specify one or more ports for steering media flows.
tcp-media-profile	Configure the TCP media profile and profile entries.

### Note:

Click **Show Advanced** in the navigation pane to display all of the Media Manager objects in the preceding list.

## Add a Codec Policy

You can create policies to specify how the Oracle Enterprise Session Border Controller (E-SBC) manipulates SDP offers before passing the INVITE to the end point. For example, you might want to strip or re-order codecs when the originating device sends a particular codec that

the end point does not support or prefer. To simplify SIP end point management, the E-SBC can apply global codec policy enforcement to all end points.

### Before You Begin

- Confirm that the system displays the Expert mode.

### Procedure

Use the codec-policy configuration element to specify how the E-SBC handles codecs.

1. From the Web GUI, click **Configuration > media-manager > codec-policy**.
2. On the Add Codec policy page, do the following:

Attributes	Instructions
Name	Enter a unique name for this policy.
Allow codecs	<p>Create a list of one or more codecs that this policy allows. Use the asterisk (*) as a wildcard, the force attribute, and the no attribute, as needed. Enclose entries containing multiple values in parentheses ( ). Each codec that you add to this list requires a corresponding media profile configuration.</p> <ul style="list-style-type: none"> <li>• Use the :no tag to specify exceptions. The system allows the video:no and audio:no exceptions. For example, to allow all codecs except iLBC and video, enter *iLBC:no video:no.</li> <li>• If a codec is given a :force tag, the tag means that when the specified codec is present in the incoming offer, all non-force codes are stripped out.</li> </ul>
Add codecs on egress	Create a list of one or more codecs to add on egress. Add the codecs that you want the E-SBC to add to an egress SDP offer, when they are not present in the offer. Each codec that you add to this list requires a corresponding media profile configuration.
Order codecs	Create an ordered list of codecs. Create the list in the order in which you want the codecs to appear in the outbound SDP offer. Use the asterisk (*) as a wildcard in different positions in the offer to reflect your configuration. Enclose entries containing multiple values in parentheses ( ).
Packetization time	<p>Enter the preferred time for an outgoing SDP offer, when Force Ptime is enabled. The following times are valid:</p> <ul style="list-style-type: none"> <li>• PCMU 10, 20, 30, 40, 50, 60</li> <li>• PCMA 10, 20, 30, 40, 50, 60</li> <li>• G729 10, 20, 30, 40, 50, 60</li> <li>• G729A 10, 20, 30, 40, 50, 60</li> </ul>
Force ptime	Select to enable.

3. Save and activate the configuration.

## Configure DNS

Use the dns-config element to configure the DNS ALG service.

### Before You Begin

- Configure a DNS ALG constraint, if you want to apply one to this DNS configuration.
- Configure a server realm, if you want to add server DNS attributes.
- Confirm that the system displays the Expert mode.

### Procedure

Configure DNS for Application Gateway Service (ALG) per client, per realm.

1. From the Web GUI, click **Configuration > media-manager > Show advanced > dns-config**.
2. On the Add DNS Config page, to the following:

Attributes	Instructions
Client realm	Select the realm from the drop-down list from which the system receives DNS queries.
Description	Enter a description of this configuration.
Constraint name	Select a DNS-ALG constraint from the drop-down list to apply to this configuration.
Trap on status change	Select to enable.
Extra dnsmg stats	Select to enable.
Client address list	Click <b>Add</b> to add one or more client address lists, and do one of the following: <ul style="list-style-type: none"><li>• Click <b>OK</b>.</li><li>• Click <b>Apply/Add another</b>, add another client address list, and click</li><li>• Click <b>OK</b>. Repeat as needed.</li></ul>

Attributes	Instructions
Server DNS attributes	<p>Click <b>Add</b> to add server DNS attributes, and do the following:</p> <ul style="list-style-type: none"> <li>• Server realm. Select the server realm from the drop-down list.</li> <li>• Domain suffix. Click <b>Add</b>, add a domain suffix list and click <b>OK</b>, or add another domain suffix list, click <b>OK</b>, and repeat as needed.</li> <li>• Server address list. Click <b>Add</b>, add a server address list and click <b>OK</b>, or add another server list, click <b>OK</b>, and repeat as needed.</li> <li>• Source address. Enter the source IPv4 address.</li> <li>• Source port. Enter the source port. Range: 1025-65535.</li> <li>• Transaction timeout. Enter the time in seconds for the DNS transaction timeout. Range: 0-999999999. 0 = unlimited.</li> <li>• Address translation. Click <b>Add</b>, enter the Server Prefix and Client Prefix, and click <b>OK</b>. Repeat as needed.</li> </ul> <p>Click <b>Back</b>.</p> <p>Click <b>Back</b>.</p>

3. Save and activate the configuration.

## Configure Media Manager

Use the media-manager element to define parameters used in the media steering functions performed by the Oracle Enterprise Session Border Controller, including the flow timers.

### Before You Begin

- Confirm that the system displays the Expert mode.

### Procedure

1. From the Web GUI, click **Configuration > media-manager > media-manager**.
2. On the Media manager page, click **Show advanced**, and do the following:

Attributes	Instructions
State	Select to enable Media Manager.
Flow time limit	Enter the time limit, in seconds, for a media flow. Range: 0-4294967295.
Initial guard timer	Enter the time limit, in seconds, for a media flow guard timer. Range: 0-4294967295.
Subsq guard timer	Enter the time limit, in seconds, for a subsequent media flow guard timer. Range: 0-4294967295.
TCP flow time limit	Enter the time limit, in seconds, for a TCP flow. Range: 0-4294967295.
TCP initial guard timer	Enter the time limit, in seconds, for the initial TCP flow. Range: 0-4294967295.
TCP subsq guard timer	Enter the time limit, in seconds, for a subsequent TCP flow. Range: 0-4294967295.

Attributes	Instructions
Hnt rtcp	Select to enable RTCP for hosted NAT traversal.
Algd log level	Select an ALGD log level from the drop-down list.
Mbcd log level	Select an MBCD log level from the drop-down list.
Options	Add any optional parameters.
Red max trans	Enter the number of redundancy sync transactions to keep. Range: 0-50000.
Red sync start time	Range: 0-4294967295.
Red synch comp time	Range: 0-4294967295.
Media policing	Select to enable per session traffic rate policing in a media gateway.
Max untrusted packet rate	Enter the maximum untrusted signaling bandwidth allowed to the host path in bytes per second. Range: 20-200000.
Max trusted packet rate	Enter the maximum trusted signaling bandwidth allowed to the host path in bytes per second. Range 20 to 200000.
Max arp packet rate	Enter the maximum bandwidth that can be used by an ARP message. Range: 20 to 10000.
Tolerance window	Range: 0-4294967295.
Trap on demote to deny	Select to generate a trap when the endpoint is demoted from untrusted to deny.
Trap on demote to untrusted	Select to generate a trap when the endpoint is demoted from trusted to untrusted.
Syslog on demote to deny	Select to generate Syslog when the endpoint is demoted from untrusted to deny.
Syslog on demote to untrusted	Select to generate Syslog when the endpoint is demoted from trusted to untrusted.
Anonymous sdp	Select to enable the Use Name and Session Name fields in Session Description Protocol (SDP).
Translate non rfc283 event	Select to accept UII/INFO events for Interworking Function (IWF), although RFC2833 is preferred.
Syslog on call reject	Select to enable Syslog on SIP call rejection.

3. Click **OK**.
4. Save and activate the configuration.

## Configure Media Policy

Use the media-policy element to configure the Type of Service (TOS) and Differentiated Services (DiffServ) values that define a type or class of service. Apply the media policy to one or more realms.

### Before You Begin

- Confirm the system displays the Expert mode.

In the following procedure, you can enter any of the media types defined by the Internet Assigned Numbers Authority (IANA). For example, audio, example, image, message, model, multi-part, text, and video. You can enter any of the sub-media types defined by the IANA for a

specific media type. For example, for the Image media type, you can use the sub-type jpeg. (image/jpeg)

#### Procedure

1. From the Web GUI, click **Configuration > media-manager > media-policy**.
2. On the media policy page, click **Add**.
3. On the Add media policy page, do the following:

Attributes	Instructions
Name	Enter a name for this media policy.
TOS settings	Click <b>Add</b> .
Add media policy / tos settings	<ul style="list-style-type: none"> <li>• Media type. Enter any IANA-defined media type to use for this group of TOS settings. Range: 1-255 characters. Not case-sensitive.</li> <li>• Media sub-type. Enter any IANA-defined media sub-type for the media type. Range: 1-255 characters. Not case-sensitive.</li> <li>• Tos value. Enter a list of TOS values for this policy. You can specify one or more audio media types and one or more video media types. Use decimal (0.0) or hexadecimal number (0x00) format. Default is hexadecimal.</li> <li>• Media attributes. Click <b>Add</b>, and enter a list of one or more media attributes to match in the Session Description Protocol (SDP). Range: 1-255 characters. Case-sensitive. When entering more than one media attribute value, enclose the entry in quotation marks, for example, "&lt;attribute&gt;". Do one of the following: <ul style="list-style-type: none"> <li>– Click <b>OK</b>.</li> <li>– Click <b>Apply/Add another</b>, add another media attribute, and click <b>OK</b>. Repeat, as needed.</li> </ul> </li> </ul>

4. Click **OK**.
5. Save and activate the configuration.

## Configure Playback

The playback configuration defines the media files that you want to play, listed by codec. Each codec encoding that you want to support requires a separate file that is defined by the playback entry sub-element.

#### Before You Begin

- Confirm that the system displays the Expert mode.

#### Procedure

In the following procedure, you specify a type of media that you want the Oracle Enterprise Session Border Controller (E-SBC) to play and you give the configuration a name. The name that you give to this playback configuration is used with the playback trigger that you specify in the spl-options parameter in the realm-config and sip-interface configurations. There, the name effectively specifies the media that the Oracle Enterprise Session Border Controller (E-SBC)

plays back because it uses the settings in this configuration. For more information about playback triggers, see Local Media Playback in the *ALCI Configuration Guide*.

1. From the Web GUI, click **Configuration** > **media-manager** > **Show advanced** > **playback-config**.
2. On the Playback Config page, click **Add**.
3. On the Add Playback Config page, enter a name for this playback configuration, click **Add**, and do the following:

Attributes	Instructions
Encoding	Enter the codec name for this media file entry. This value must match the encoding name negotiated on the E-SBC.
File name	Enter the file name of the raw binary media file stored in code/media directory on the E-SBC.
Bytes per sec	Enter the playback rate for the media file in bytes per second. Default: 8000. Range: 100-99999.

4. Click **OK**.
5. (Optional). Repeat steps 3 and 4 to add more playback configurations.  
The system adds each additional configuration to the table on the Add Playback Config page.
6. Click **Back**.  
The system displays the Playback Config page.
7. Save and activate the configuration.

#### Next Steps

- Configure local media playback.

## Configure a Realm

Use the realm-config element to configure a realm for the Oracle Enterprise Session Border Controller (E-SBC).

#### Before You Begin

- Configure a physical interface.
- Configure a network interface.
- If you use Quality of Service (QoS), confirm that QoS is enabled on the E-SBC.
- Confirm that the system displays the Expert mode.

#### Note:

In Expert mode, in a table that contains the Realm ID column, you can click a cell in the column to view the realm configuration.

#### Procedure



1. From the Web GUI, click **Configuration > media-manager > realm-config > Add**.
2. On the Add Realm Config page, click **Show advanced** and do the following:

Attributes	Instructions
Identifier	Enter the name of the realm.
Description	Enter a description of this realm.
Addr prefix	Enter the IPv4 or IPv6 address and subnet mask combination to set the criteria the E-SBC uses to match packets sent or received on the network interface associated with this realm.
Network interfaces	Enter the physical and network interfaces through which this realm can be reached for ingress and egress traffic. Entries in this parameter take the form: (network-interface-ID): (subport). Only one network interface is allowed per realm-config object.
Mm in realm	Select to enable steering media through the E-SBC, when the communicating endpoints are located in the same realm.
Mm in network	Select to enable the E-SBC to trust media within realms with the same subnet mask as the E-SBC.
Mm same ip	Select to enable media managing for endpoints behind the same IP address.
QoS enable	Select to enable the use of QoS in this realm.
Max bandwidth	Enter the maximum bandwidth for dynamic flows to and from this realm in kilobits per second.
Max priority bandwidths	Enter the maximum priority bandwidth for dynamic flows to and from this realm in kilobits per second.
Parent realm	Enter the parent realm, if this is a nested realm.
DNS realm	Enter the name of the DNS realm for this realm.
Media policy	Select a default media-policy on a per-realm basis. This parameter must correspond to a valid name entry in a media policy element.
Media sec policy	Enter the name of the default media security policy.
Srtp msm passthrough	Select to enable the inclusion of information for multi-system SRTP passthrough.
Class profile	Enter the name of class-profile to use for this realm for ToS marking.
In translationid	Enter the name of a session-translation element. Only one is allowed.
Out translationid	Enter the name of a session-translation element. Only one is allowed.
Average rate limit	Enter the average data rate limit in bytes per second.
Access control trust level	Select a trust level for the host within the realm.
Invalid signal threshold	Enter the allowed invalid signalling message rate within the tolerance time period.
Maximum signal threshold	Enter the allowed signalling message rate within the tolerance time period.

Attributes	Instructions
Untrusted signal threshold	Enter the maximum number of untrusted signalling messages within the tolerance time period.
NAT trust threshold	Enter the number of endpoints behind the NAT device that must be denied.
Max endpoints per NAT	Enter the maximum number of endpoints allowed behind a NAT device.
NAT invalid message threshold	Enter the allowed number of invalid messages from behind a NAT device.
Wait time for invalid register	Enter the time period, in seconds, for the E-SBC to wait before counting the absence of the REGISTER message as an invalid message.
Deny period	Enter the number, in seconds, for the time period to block denied dynamic entries.
Untrust cac failure threshold	Enter the maximum number of untrusted CAC failures in the time period.
Subscription id type	Select a subscription ID type from the drop down list.
Early media allow	Select the early media handling policy from the drop down list.
Enforcement profile	Select the enforcement profile from the drop down list.
Additional prefixes	Select or add an additional address prefix to use. Omit the number of bits for an exact match.
Restricted latching Options	Select a restricted latching mode. Enter optional features and parameters. Click <b>Add</b> , and enter an option. Do one of the following: <ul style="list-style-type: none"> <li>Click <b>OK</b>.</li> <li>Click <b>Apply/Add another</b>, add another media attribute, and click <b>OK</b>. Repeat, as needed.</li> </ul>
SPL options.	Enter SPL options. Click <b>Add</b> , and enter an SPL option. Do one of the following: <ul style="list-style-type: none"> <li>Click <b>OK</b>.</li> <li>Click <b>Apply/Add another</b>, add another media attribute, and click <b>OK</b>. Repeat, as needed.</li> </ul>
Delay media update	Select to enable media update delay support for this realm.
Refer call transfer	Select the refer call transfer mode for this realm.
Hold refer reinvoke	Select to enable the hold-refer-reinvoite option.
Refer notify provisional	Select provisional mode for sending a NOTIFY message from the drop down list.
Dyn refer term	Select to enable terminating refer call transfer for this realm.
Codec policy	Select the codec policy mode for this realm from the drop down list.
Codec manIP in realm	Select to enable codec manipulation support for this realm.
Codec manIP in network	Select to enable codec policy in this network.
RTCP policy	Select the RTCP policy for this realm.

Attributes	Instructions
Constraint name	Select the name of a constraint for this realm from the drop down list.
Call recording server ID	Enter the name of the call recording server.
Session recording server	Select a recording server or recording server group.
Session recording required	Select to enable session recording for this realm.
QoS constraint	Enter the name of a QoS constraint.
TCP media profile	Select a TCP media profile for this realm.
Monitoring filters	Add a comma-separated list of monitoring filters for this realm.
Node functionality	Select a node function from the drop down list.

3. Click **OK**.
4. Save and activate the configuration.

## Configure a Steering Pool

Use the steering-pool element to define sets of ports used to steer media flows through the Oracle Enterprise Session Border Controller to provide packet steering to ensure a level of quality or a routing path.

### Before You Begin

- Confirm that network interface that you want to steer media to is configured and named.
- Confirm that the system displays the Expert mode.

In the following procedure, the combination of IP address, start port, and realm ID, must be unique.

### Procedure

1. From the Web GUI, click **Configuration > media-manager > steering-pool**.
2. On the Steering pool page, do the following:

Attributes	Instructions
IP address	Enter the IP address of the generated pool.
Start port	Enter the port number that begins the range of ports available to this steering pool. Range: 1-65535.
End port	Enter the port number that ends the range of ports available to this steering pool. Range: 1-65535.
Realm id	Select the realm from the drop-down list from which media flows are allowed for this steering pool.
Network interface	Select the network interface from the drop-down list to which this steering pool directs media.

## Security Configuration

The Oracle Enterprise Session Border Controller (E-SBC) can provide security for VoIP and other multi-media services. E-SBC security includes access control, DoS attack, and overload

protection, which help to secure service and protect the network infrastructure. E-SBC security lets legitimate users place a call during attack conditions, while protecting the service itself.

E-SBC security includes the Net-SAFE framework's numerous features and architecture designs. Net-SAFE is a requirements framework for the components required to provide protection for the E-SBC, the service provider's infrastructure equipment (proxies, gateways, call agents, application servers, and so on), and the service itself. You can configure the following security objects from the Configuration tab on the Web GUI.

Object	Purpose
auth-params	Configure authentication protocol, strategy, and servers.
authentication	Configure RADIUS and TACACS authentication.
cert-status-profile	Configure the information needed to contact an Online Certificate Status Protocol (OCSP) responder for certificate status.
certificate-record	Create a certificate record for either a CA or end entity.
dpd-params	Configure parameters to re-establish connections with unreachable Internet Key Exchange (IKE) peers.
ipsec-global-config	Configure global IPsec for authenticating and encrypting packets in communication sessions.
media-sec-policy	Create a media security policy.
password-policy	Create a password policy.
sdes-profile	Create a Session Description Protocol Security Descriptions (SDES) profile for media streams.
security-association	Configure a manual security association.
security-config	Configure security for VoIP and other multi-media services.
security-policy	Create a security policy.
sipura-profile	Create a SIPURA/Linksys profile.
tls-global	Configure session caching to allow a previously authenticated client to re-connect with the unique session identifier from the previous session.
tls-profile	Create a profile to define communications security for running SIP over TLS.



#### Note:

Click **Show Advanced** in the navigation pane to display all of the Security objects in the preceding list.

## Security Settings

Security configuration from the web GUI consists of creating the building blocks used to establish TLS-secured paths for signaling traffic.

The process includes the following steps.

1. Configure Certificate Records.

2. Configure TLS Profiles, which utilize your certificate records.
3. Apply TLS Profiles to SIP Interfaces.

The dialogs available from the Security button allow you to perform the first two steps. You apply TLS profiles to SIP interfaces using controls within the SIP Interface dialog.

## TACACS+ Authentication

The Web GUI supports TACACS+ authentication.

TACACS+ provides access control for routers, network access servers, and other networked computing devices by way of one or more centralized servers. The Oracle Enterprise Session Border Controller (E-SBC), supports TACACS+ authentication and limited accounting services. For accounting services support, the E-SBC supports only authentication success and failure. The E-SBC does not support TACACS+ authentication.

## Add TACACS+ Authentication

Use the authentication element to add Terminal Access Controller Access-Control System+ (TACACS+) authentication to the Oracle Enterprise Session Border Controller (E-SBC) for Web GUI users.

### Before You Begin

- Confirm that the TACACS+ server is configured.
- Confirm that the system displays the Expert mode.

You must enable and configure the TACACS+ authentication method before Web GUI users can log on to the E-SBC with TACACS+ credentials.

### Procedure

1. From the Web GUI, click **Configuration > Show advanced > security > authentication**.
2. On the Add Authentication page, click **Show advanced**, and do the following:

Attributes	Instructions
Source port	Enter 1812.
Type	Select tacacs from the drop down list.
Protocol	Select ascii from the drop down list.
TACACS authorization	Select to enable.
TACACS accounting	Select to enable.
Server assigned privilege	Select to enable.
Allow local authorization	Select to enable.
Logon as Admin	Select to enable.
Management strategy	Select hunt from the drop-down list.
Management servers	Click <b>Add</b> , add a management server, and do one of the following: <ul style="list-style-type: none"> <li>• Click <b>OK</b>.</li> <li>• Click <b>Apply/Add another</b>, add another management server, and click <b>OK</b>. Repeat, as needed.</li> </ul>

3. TACACS servers. Click **Add > Show Advanced**, and do the following:

Attributes	Instructions
Address	Enter the IP address of the management server.
Port	Enter the TACACS+ port number. Range: 0-65535.
State	Select to enable.
Secret	Click <b>Set</b> , and do the following: <ol style="list-style-type: none"> <li>a. Enter the secret.</li> <li>b. Confirm the secret.</li> <li>c. Click <b>OK</b>.</li> </ol>
Realm ID.	Not needed.
Dead time.	Enter the dead timer value in seconds. Range: 0-10000.
Authentication methods.	Click <b>Add</b> , select <b>All</b> from the drop-down list, and click <b>OK</b> .

4. Do one of the following:
  - Repeat Step 3 to add another TACACS+ server.
  - Click **OK**.

After you click **OK**, the system displays the Add authentication page.

5. Click **OK**.
6. Save and activate the configuration.

## Certificate Configuration Process

You can perform the following certificate management tasks from the Web GUI in either Basic Mode or Expert Mode. The process for configuring certificates on the Oracle Enterprise Session Border Controller (E-SBC) includes the following steps:

1. Configure a Certificate Record on the E-SBC. See *Add a Certificate Record*.
2. Generate a Certificate request by the E-SBC. See *Generate a Certificate Request*.
3. Import a Certificate into the E-SBC. See *Import a Certificate*.
4. Reboot the system.

### Add a Certificate Record

Use the certificate-record element to add certificate records to the Oracle Enterprise Session Border Controller (E-SBC).

- Confirm that the system displays the Expert mode.

A certificate record represents either the end-entity or the Certificate Authority (CA) certificate on the E-SBC. When you configure a certificate for the E-SBC, the name that you enter must be the same as the name that you use to generate a certificate request. If configuring for an end stations CA certificate for mutual authentication, the certificate name must be the same name used during the import procedure.

- If this certificate record is used to present an end-entity certificate, associate a private key with this certificate record by using a certificate request.

- If this certificate record is created to hold a CA certificate or certificate in pkcs12 format, a private key is not required.
1. From the Web GUI, click **Configuration > Security > Certificate record**.
  2. On the Certificate record page, click **Add**.
  3. On the Add certificate record page, click **Show advanced**, and do the following:

Attributes	Instructions
Name	Enter the name of the certificate record.
Country	Enter a two character country name abbreviation. For example, US for the United States.
State	Enter a two character state or province name abbreviation. For example, NE for Nebraska.
Locality	Enter the name of the locality in the state or province. For example, a city, a township, or a parish. Range: 1-128 characters.
Organization	Enter the name of the organization holding the certificate. For example, a company name. Range: 1-64 characters.
Unit	Name of the unit within the organization holding the certificate. For example, a business unit or a department. Range: 1-64 characters.
Common name	Common name for the certificate record. For example, your name. Range: 1-64 characters.
Key size	Size of the key for the certificate. Supported values: 512   1024   2048. Default: .
Alternate name	Alternate name of the certificate holder.
Trusted	Select to trust this certificate record.
Key usage list	<p>Click <b>Add</b> and select a key that you want to use with this certificate record from the drop-down list, and do one of the following:</p> <ul style="list-style-type: none"> <li>• Click <b>OK</b>.</li> <li>• Click <b>Apply/Add Another</b>, add another key , and click <b>OK</b>. Repeat as needed.</li> </ul> <p>This parameter defaults to the combination of digitalSignature and keyEncipherment. For a list of other valid values and their descriptions, see the section “Key Usage Control” in the <i>ACLI Configuration Guide</i>.</p>
Extended key usage list	<p>Click <b>Add</b>, select an extended key that you want to use with this certificate record from the drop-down list, and do one of the following:</p> <ul style="list-style-type: none"> <li>• Click <b>OK</b>.</li> <li>• Click <b>Apply/Add Another</b>, add another extended key, and click <b>OK</b>. Repeat as needed.</li> </ul> <p>This parameter defaults to serverAuth. For a list of other valid values and their descriptions, see the section “Key Usage Control” in the <i>ACLI Configuration Guide</i>.</p>
Options	

4. Click **OK**.

5. Save the configuration.
  - Create TLS profiles, using the certificate records to further define the encryption behavior and to provide an entity that you can apply to a SIP interface.

## Generate a Certificate Request from the GUI

Use the certificate-record element to select a certificate record and generate a certificate request.

- Confirm that the certificate record exists.

To get a certificate authorized by a Certificate Authority (CA), you must generate a certificate request from the certificate record on the device and send it to the CA.

1. From the Web GUI, click **Configuration** > **security** > **certificate-record**.

The system displays a list of certificate records.

2. Select the certificate record for the device.

3. Click **Generate**.

The system creates the request and displays it in a dialog.

4. Copy the information from the dialog and send it to your CA as a text file.

- When the CA replies with the certificate, import the certificate to the device with the corresponding certificate record.

## Import a Certificate

Use the certificate-record element to import a certificate into the Oracle Enterprise Session Border Controller (E-SBC).

Use this procedure to import either a device certificate or an end-station CA certificate for a mutual authentication deployment. You must import the certificate to the corresponding certificate record for the E-SBC. End-station CA certificates may or may not need to be imported against a pre-configured certificate record.

1. From the Web GUI, click **Configuration** > **security** > **certificate record** .

2. Select the certificate record for the device.

3. Click **Import**.

The system displays a dialog from which you can import the certificate.

4. Select one of the following format types from the **Format** drop down list:

- pkcs7
- x509
- Try-all. The system tries all possible formats until it can import the certificate.

5. Browse to the certificate file, and select the certificate to import.

6. Click **Import**.

The E-SBC imports the certificate.

7. Reboot the system.

- Apply the corresponding certificate record to the intended SIP interface.



## SDES Configuration for a Media Stream

Configuring a Session Description Protocol Security Descriptions (SDES) profile for a media stream is a way to negotiate the key for Secure Real-time Transport Protocol (SRTP). The SDES profile provides confidentiality, message authentication, and replay protection for RTP media and control traffic. SDES profile configuration on the Oracle Enterprise Session Border Controller (E-SBC) includes the following steps.

1. Create at least one SDES profile that specifies the parameter values to negotiate during the offer-answer exchange.
2. Create at least one Media Security Policy that specifies the key exchange protocols and protocol specific profiles.
3. Assign the appropriate Media Security Policy to the appropriate realm.
4. Create an interface-specific security policy that enables the E-SBC to identify inbound and outbound media streams treated as SRTP and SRTCP.

## TLS Profile Configuration

The Transport Layer Security (TLS) profile specifies the information required to run SIP over TLS.

TLS is a cryptographic protocol that provides communication security over the Internet. TLS encrypts the segments of network connections at the Application layer for the Transport layer, using asymmetric cryptography for key exchange, symmetric encryption for confidentiality and message authentication codes for message integrity.

Create a TLS profile, using your certificate records, to further define the encryption behavior and create the configuration element that you apply to the SIP interface. You can configure an end entity certificate and a trusted Certification Authority (CA) certificate for a TLS policy. CA certificates are issued by a CA to itself or to a second CA for the purpose of creating a defined relationship between the two entities. A certificate that is issued by a CA to itself is referred to as a trusted root certificate, because it is intended to establish a point of ultimate trust for a CA hierarchy. Once the trusted root has been established, it can be used to authorize subordinate CAs to issue certificates on its behalf.

## TLS Session Caching

Transport Layer Security (TLS) session caching allows the Oracle Enterprise Session Border Controller to cache key information for TLS connections, and to set the length of time that the information is cached.

When TLS session caching is not enabled, the Oracle Enterprise Session Border Controller and a TLS client perform the handshake portion of the authentication sequence in which they exchange a shared secret and encryption keys are generated. One result of the successful handshake is the creation of a unique session identifier. When an established TLS connection is torn down and the client wants to reinstate it, this entire process is repeated. Because the process is resource-intensive, you can enable TLS session caching to avoid repeating the handshake process for previously authenticated clients to preserve valuable Oracle Enterprise Session Border Controller resources.

When TLS session caching is enabled on the Oracle Enterprise Session Border Controller, a previously authenticated client can request re-connection using the unique session identifier from the previous session. The Oracle Enterprise Session Border Controller checks its cache,

finds the session identifier, and reinstates the client. This process reduces the handshake to three messages, which preserves system resources.

If the client offers an invalid session identifier, for example, one that the Oracle Enterprise Session Border Controller has never seen or one that has been deleted from its cache, the system does not allow the re-connection. The system negotiates the connection as a new connection.

## Configure TLS-Global Session Caching

Use the `tls-global` element to enable `tls-global` session caching to allow the Oracle Enterprise Session Border Controller (E-SBC) to cache the session identifier for possible re-connection with a former client.

### Before You Begin

- Confirm that a TLS profile is configured.
- Confirm that the system displays the Expert mode.

Session caching is a global setting for all TLS operations on the E-SBC. You must enable session caching and set the session cache timeout. Note that the number 0 disables session cache timeout. When the session cache timeout is disabled, cache entries never age and they remain until you delete them. RFC 2246, The TLS Protocol Version 1.0, recommends setting session cache timeout to the maximum of 24 hours.

### Procedure

1. From the Web GUI, click **Configuration > security > tls-global**.
2. On the Add TLS global page, do the following:

Attributes	Instructions
Session caching	Select to enable.
Session cache timeout	Enter the number of hours to cache TLS sessions for re-connection. Range: 0-24.

3. Click **OK**.
4. Save and activate the configuration.

## Add a TLS Profile

Use the `tls-profile` element to specify the parameters for running SIP over Transport Layer Security (TLS).

### Before You Begin

- Add one or more certificate records to the Oracle Enterprise Session Border Controller that you need for this profile.

### Procedure

Create a TLS profile, using your certificate records, to further define encryption behavior and create the configuration element that you apply to the SIP interface. You can configure an end-entity certificate and a trusted Certification Authority (CA) certificate for a TLS profile.

1. From Web GUI, click **Configuration > security > tls-profile**.
2. On the TLS profile page, click **Add**.
3. On the Add TLS profile page, click **Show advanced**, and do the following:

Attributes	Instructions
Name	Enter a name for the TLS profile, for example, TLS1.
End entity certificate	Enter the name of the end-entity certificate record for the TLS session.
Trusted ca certificates	Add the names of the trusted CA certificate records.
Cipher list	Add cipher lists.
Verify depth	Enter the verify depth for mutual authentications.
Mutual authenticate	Select to enable mutual authentication.
TLS version	Select a TLS version for this profile from the drop down list.
Options	Add optional features and parameters.
Cert status check	Select to enable checking the status of the certificate.
Cert status profile list	Add one or more lists of certificate status profiles for status requests.
Ignore dead responder	Select to ignore a dead certificate status responder.
Allow self signed cert	Select to allow a self-signed certificate.

4. Click **OK**.
5. Save and activate the configuration.

## Session Router Configuration

You can configure the following session-router objects from the Configuration tab on the Web GUI:

Object	Purpose
access-control	Configure a static or dynamic access control list.
account-config	Configure and enable Quality of Service (QoS) accounting.
allowed-elements-profile	Configure an allowed elements profile.
call-recording-server	Configure a call recording server.
class-policy	Configure a classification profile policy.
diameter-manipulation	Configure diameter manipulation rules.
enforcement-profile	Configure an enforcement profile.
enum-config	Configure an ENUM server.
filter-config	Configure a custom filter for SIP monitor and trace.
h323-config	Configure and enable an H.323 protocol.
h323-stack	Configure an H.323 stack.
home-subscriber-server	Configure a home subscriber server.
http-alg	Configure an HTTP proxy.
iwf-config	Configure and enable Inter-Working Function (IWF).
ldap-config	Configure and enable an LDAP server.
local-policy	Configure a session request routing policy.
local-response-map	Configure a local SIP response map.

Object	Purpose
local-routing-config	Configure the parameters for the local routing table.
media-profile	Configure a media profile and apply it to a media type.
net-management-control	Configure and enable network management controls.
qos-constraints	Configure Quality of Service (QoS) constraints.
response-map	Configure a SIP response map.
service-health	Configure a service tag list.
session-agent	Configure and enable a session agent.
session-constraints	Configure and enable session constraints.
session-group	Configure a session agent group.
session-recording-group	Configure a session recording server group.
session-recording-server	Configure and enable a session recording server.
session-timer-profile	Configure a session timer profile.
session-translation	Configure the translation rules for calling and called numbers.
sip-advanced-logging	Configure logging of specific SIP requests by criteria.
sip-config	Configure and enable signaling and session management.
sip-feature	Configure SIP option tag parameters.
sip-interface	Configure and enable a SIP interface.
sip-manipulation	Configure SIP manipulation.
sip-monitoring	Configure and enable SIP monitor and trace features.
surrogate-agent	Configure a surrogate agent.
survivability	Configure and enable survivability.
translation-rules	Configure and apply session translation rules to an agent and a realm.

 **Note:**

Click **Show Advanced** in the navigation pane to display all of the Session Router objects in the preceding list.

## Configure Access Control

Use the access-control configuration element to manually create an Access Control List (ACL) for the host path in the Oracle Enterprise Session Border Controller.

### Before You Begin

- Confirm that the system displays the Expert mode.

### Procedure

1. From the Web GUI, click **Configuration > session-router > access-control**.
2. In the Add Access Control dialog, click **Show advanced**, and do the following:

Attributes	Instructions
Realm ID	Enter the ingress realm of traffic destined to the host to apply this ACL.
Description	Type a brief description of this access-control configuration element.
Source address	Enter the source address, net mask, port number, and port mask to specify traffic matching for this ACL.
Destination address	Enter the destination address, net mask, port number, and port mask to specify traffic matching for this ACL in the following format: (ip-address)/[(num-bits)][::(port)]/[(port-bits)]. Not specifying a port mask implies an exact source port. Not specifying an address mask implies an exact IP address.
Application protocol	Select the application-layer protocol configured for this ACL entry from the drop down list.
Transport protocol	Select the transport-layer protocol configured for this ACL entry from the drop down list.
Access	Select the access control type from the drop down list.
Average rate limit	Enter the average data in bytes per second. Range is 0-4294967295.
Trust level	Select the trust level for the host from the drop down list.
Minimum reserved bandwidth	Enter the minimum reserved bandwidth in bytes per second. Range is 0-4294967295.
Invalid signal threshold	Enter the acceptable invalid signaling message rate allowed within the tolerance window. Range is 0-4294967295.
Maximum signal threshold	Enter the maximum number of signalling messages allowed within the tolerance window. Range is 0-4294967295.
Untrusted signal threshold	Enter the maximum number of untrusted signalling messages allowed within the tolerance window. Range is 0-4294967295.
Deny period	Enter the number for the blocked period for dynamic denied entries. Range is 0-4294967295.
NAT trust threshold	Enter the number of endpoints behind NAT to deny. Range is 0-65535.
Max endpoints per NAT	Enter the maximum number of endpoints behind a NAT device. Range is 0-65535.
NAT invalid message threshold	Enter the acceptable number of invalid messages from behind a NAT device. Range is 0-65535.
CAC failure threshold	Enter the maximum number of admission failures allowed within the tolerance window. Range is 0-4294967295.
Untrust CAC failure threshold	Enter the maximum number of untrusted admission failures allowed within the tolerance window. Range is 0-4294967295.

3. Click **OK**.
4. Save and activate the configuration.

## Accounting Configuration

The Oracle Enterprise Session Border Controller (E-SBC) supports RADIUS, an accounting, authentication, and authorization (AAA) system. RADIUS servers are responsible for receiving user connection requests, authenticating users, and returning all configuration information necessary for the client to deliver service to the user.

You can configure the E-SBC to send call accounting information to one or more RADIUS servers. This information can help you to see usage and Quality of Service (QoS) metrics, monitor traffic, and even troubleshoot your system.

For information about how to configure the E-SBC for RADIUS accounting, refer to the *Oracle Communications Session Border Controller Accounting Guide*. The Accounting Guide contains all RADIUS information, as well as information about:

- Accounting for SIP and H.323
- Local CDR storage on the E-SBC, including CSV file format settings
- Ability to send CDRs via FTP to a RADIUS sever (the FTP push feature)
- Per-realm accounting control
- Configurable intermediate period
- RADIUS CDR redundancy
- RADIUS CDR content control

## Configure Call Accounting

Use the account-config element to set the destination parameters for accounting messages.

### Before You Begin

- Confirm that the system displays the Expert Mode.

### Procedure

1. From the Web GUI, click **Configuration > account-config > Show Advanced**.
2. On the Add account-config dialog, do the following:

Attributes	Instructions
Strategy	Select the lookup algorithm for the accounting server.
Protocol	Select RADIUS or Diameter.
State	Select to enable call accounting.
File output	Select to enable active writing comma delimited records.
File rotate time	Enter a number from 0-2147483647.
Options	Add optional parameters.
FTP push	Select to push files to an FTP server.
Push receiver	Add push file receiver.
Account-servers	Add accounting servers.

3. Save and activate the configuration.

## Configure RADIUS Call Accounting

You can configure the Oracle Enterprise Session Border Controller to send call accounting information to one or more RADIUS servers. This information can help you to see usage and Quality of Service (QoS) metrics, to monitor traffic, and to troubleshoot the system.

### Procedure

To set the RADIUS call accounting parameters, use the account-config element to specify where and when you want the system to send accounting messages, and the strategy for selecting account servers. Use the following procedure to configure the minimum settings required for RADIUS call accounting.

### Procedure

1. From the Web GUI, click **Configuration** > **session-router** > **account-config**.
2. In the Add Account Config dialog do the following:

Attributes	Instructions
Strategy	Select the strategy from the drop down list to use for selecting the server to which the E-SBC sends accounting messages.
Protocol	Select RADIUS from the drop down list.
State	Select to enable the call accounting configuration.
File output	Select to enable the system to store the .csv file locally.
File rotate time	Enter the number of minutes from 1-2147483647.
Options	(Optional) Click <b>Add</b> to add options.
FTP push	(Optional) Select to enable.
Push receiver	(Optional) Click <b>Add</b> to add a push receiver to the list.
Account servers	Click <b>Add</b> to add a RADIUS server to the list.

3. Click **OK**.
4. Save and activate the configuration.

## Configure a Custom Monitor and Trace Filter

In the following procedure, you can specify filtering on an IP address alone or on an IP address and its netmask. Depending on the value you specify for User, the system can filter the phone number string or the user-part with the following information when present:

- From URI
- To URI
- Request URI
- P-Called Party URI

1. From the Web GUI, click **Configuration** > **session-router** > **filter-config**.
2. On the filter config page, click **Add**.

- On the Add filter config page, do the following:

Fields	Values
Name	Enter a name for this filter.
Address	Enter the IP address or IP address and Netmask on which to filter.
User	Enter the phone number or user-part to filter.

- Click **OK**.
- Save and activate the configuration.

## Dynamic ACL for the HTTP-ALG

The dynamic Access Control List (ACL) option for HTTP-Application Layer Gateway (ALG) provides Distributed Denial of Service (DDoS) attack protection for the HTTP port.

When the dynamic ACL option is enabled, the static flow for the public listening socket defined in **http-alg > public** is created with a trust level set to **untrusted**. Each listening socket creates and manages its ACL list, which allows the listening socket to keep track of the number of received and invalid messages, the number of connections per endpoint, and so on. You can configure a different setting for each **http-alg** object.

Dynamic ACL for each endpoint is triggered by Session Initialization Protocol (SIP) registration messages. Upon receiving a SIP registration message, the SIP agent creates a dynamic ACL entry for the endpoint. If the 200 OK response is received, the ACL is promoted, allowing the HTTP message to go through the security domain. If SIP registration is unsuccessful, the ACL entry is removed and HTTP ingress messages are blocked from the endpoint. The ACL entry is removed upon incomplete registration renewal or telephone disconnect.

The following example describes the criteria and associated configuration item that result in a denied or allowed connection for both low and medium control levels.

Criteria	Associated Configuration Item	Action
Exceed total number of connections for allowed	http-alg > max-incoming-conns	Connection denied
Exceed total connections per peer	http-alg > per-src-ip-mas-incoming-conns	Connection denied
ACL not promoted	Dynamically set on SIP registration	Connection denied
Exceed maximum number of packets/sec	realm-config > maximum-signal-threshold	Connection denied and peer is demoted
Exceed maximum number of error packets	Realm-config > invalid-signal-threshold	Connection denied and peer is demoted

Oracle recommends setting **realm-config > access-control-level** to **medium**.

If a peer is promoted to **trusted**, the system performs DDoS checks on **max number of packets/sec** and **max number of error packets** allowed.

Demotions depend on the realm's **ream-config > access-control-trust-level** setting. For more information on **realm-config** settings, see the ACLI Configuration Guide.



If you want to configure different ACL settings for SIP traffic and for HTTP-ALG traffic, you must configure a realm for each type of traffic.

## Enable Dynamic ACL for the HTTP ALG

The Dynamic Access Control List (ACL) for HTTP Application Layer Gateway (ALG) option, which provides Distributed Denial of Service (DDoS) attack protection for the HTTP port, is an option that you must enable.

### Before You Begin

- Confirm that the session manager is mapped to the Oracle Enterprise Session Border Controller.
- Confirm that the system displays the Expert mode.

Two ACL entries are required for each registered telephone, where one entry is used for SIP traffic and one is used for HTTP-ALG traffic.

### Note:

Enabling dynamic access control for HTTP-ALG traffic reduces the number of available dynamic ACL entries on the session border controller, which may reduce the number of concurrent trusted endpoints that the system can support.

### Procedure

1. On the Web GUI, on the Configuration tab, click **Objects** --> **session-router** --> **http-alg**.
2. Click **Add**.  
The system displays the Add http-alg page.
3. On the Add http-alg page, click **Show advanced**.
4. In the Add http-alg dialog, do the following:

Attributes	Instructions
Name	Enter a name for this ACL.
State	Select State to enable this ACL.
Description	Enter a description of this ACL.
Realm id	Select the private realm to which to apply this ACL from the drop down list.
Address	Enter the IP address of the selected private realm.
Destination address	Enter the destination IP address.
Destination port	Enter the destination port. Range:1-65535. Default: 80.
TLS profile	Enter TLS profile to apply from the drop-down list.
Realm id	Select the public realm identifier from the drop down list.
Address	Enter the IP address of the selected public realm.
Port	Enter the listening port number. Range:1-65535. Default: 80.

Attributes	Instructions
TLS profile	Select a TLS profile to apply from the drop-down list.
Session-manager-mapping	Not applicable to this procedure.
Dynamic ACL	Select to enable dynamic ACL creation on SIP messages.
Max incoming conns	Enter a number for the maximum allowed incoming HTTP connections. Range: 0-4294967295.
Per src IP max incoming conns	Enter a number for the maximum allowed incoming connections per registered IP address. Range: 0-4294967295.

5. Click **OK**.
6. Save and activate the configuration.

## Dynamic Access Control List (ACL) Settings for the HTTP Application Layer Gateway (ALG)

You can set the following parameters for the realm specified in **http-alg > public > realm-id**.

- access-control-trust-level
- invalid-signal-threshold
- maximum-signal-threshold
- untrusted-signal-threshold
- deny-period

For more information on **realm-config** settings, see the ACLI Configuration Guide.

## Session Manager Mapping

The Oracle Enterprise Session Border Controller (SBC) supports mapping between multiple session managers and multiple SBCs. Such mapping allows the SBC to work in a redundant network configuration where you can map:

- The primary session manager to the primary SBC IP address
- One or more redundant session managers to one or more redundant SBCs

To map a redundant session manager to a redundant SBC, map the private IP address of the redundant session manager to the public SIP IP address configured in HTTP-ALG > Public on the SBC. For instructions, see "Map a Session Manager to a Session Border Controller."

## Map a Session Manager to a Session Border Controller

You can map one or more session managers to an Oracle Enterprise Session Border Controller (E-SBC) to provide redundancy and load balancing.

### Before You Begin

- Note the private IP address of the session manager and the public SIP interface IP address of the session border controller that you want to map.
- Confirm that the system displays the Expert mode.

Map the private IP address of the session manager to the public SIP interface IP address of the E-SBC.

#### Procedure

1. From the Web GUI, go to **Configuration > session-router > http-alg**.
2. On the http-alg page, click **Show advanced > Add**.
3. In the Add http-alg dialog, enter the information in the fields and make the selections for the deployment.
4. Click **OK**.  
The system lists the new map on the http-alg page.
5. Save and activate the configuration.

## Configure IWF

You must enable and configure the Oracle Enterprise Session Border Controller to perform Inter-Working Function (IWF) operations.

#### Before You Begin

- A complete SIP configuration, including SIP interfaces, SIP ports, SIP NAT if needed, and SIP features
- A complete H.323 configuration, including H.323 global and H.323 interface configurations
- Local policy and local policy attributes
- Media profiles
- Session agents and, if needed, session groups
- Confirm that the system displays the Expert mode

In the following procedure, the system provides dialogs where you can either select existing media profiles and options or add new ones.

#### Procedure

1. From the Web GUI, click **Configuration > Show advanced > session-router > iwf-config**.
2. On the Add iwf config page, click **Show Advanced**, and do the following:

Attributes	Instructions
State	Select to enable IWF.
Media profiles	Select the media profiles that you want to use for IWF translations.
Logging	Select to enable logging SIP messages related to the IWF.
Add reason hdr	Select to enable SIP-H323 Add Reason header for SIP.
Slow start no sdp in invite	Select to enable no offer SDP in INVITE for slow start H.323.

Attributes	Instructions
Options	Click <b>Add</b> , and enter an optional feature or parameter. Do one of the following: <ul style="list-style-type: none"> <li>Click <b>OK</b>.</li> <li>Click <b>Apply/Add another</b>, add another feature or parameter, and click <b>OK</b>. Repeat, as needed.</li> </ul>
Forward source call address	Select to enable adding the h225SourceCallSignalAddress IP for IWF to outgoing SIP INVITEs.

- Click **OK**.
- Save and activate the configuration.

## Configure LDAP

The Oracle Enterprise Session Border Controller (E-SBC) uses Lightweight Directory Access Protocol (LDAP) for interaction between an LDAP client and an LDAP server. Use the ldap-config object in Expert mode to create and enable an LDAP configuration on the E-SBC.

### Before You Begin

- Confirm that one or more authentication modes exist.
- Confirm that one or more Transport Layer Security (TLS) profiles exist.
- Confirm that the system displays the Expert mode.

In the following procedure, you configure the LDAP server, filters, security, and local policy.

### Procedure

- From the Web GUI, click **Configuration > session-router > ldap-config**.
- On the LDAP config page, click **Add**.
- On the Add LDAP config page, click **Show advanced**, and do the following:

Attributes	Instructions
Name	Enter a unique name to identify this configuration. Valid values are alpha-numeric characters.
State	Select State to enable this configuration. When not selected, the E-SBC does not attempt to establish a connection with any corresponding LDAP server.
LDAP servers	Add one or more LDAP servers to the list that you want to include in this configuration. The IP address is required. Enter the default IP Address in dotted decimal format, for example, 0.0.0.0. When adding more than one server, separate each server address with a space and enclose the list within parentheses. The port number is optional. The E-SBC uses port 389 for LDAP over TCP and port 636 for LDAP over TLS.
Realm	Select the realm for this configuration.

Attributes	Instructions
Authentication mode	Select the authentication mode for the LDAP bind request. The default is Simple, where no specific password encryption is performed when the sending the bind request. To maintain security, configure <code>LDAP sec type</code> on this page.
Username	Enter the username that the LDAP bind request uses for authentication before the LDAP server grants access.
Password	Click <b>Set</b> , enter and confirm the password to pair with the Username that the LDAP bind request uses for authentication before the LDAP server grants access. Click <b>OK</b> .
LDAP search base	Enter the base Directory Number for LDAP search requests.
Timeout limit	Enter a timeout limit in seconds. The range is from 1-300.
Max request timeouts	Enter the maximum number of timeouts allowed. The range is from 0-10.
TCP keepalive	Select TCP keepalive to enable Transmission Control Protocol (TCP) keepalive signalling.
LDAP sec type	Select <b>None</b> or <b>LDAPS</b> for the type of LDAP security from the drop down list.
LDAP TLS profile	Select a TLS profile for this LDAP configuration.
LDAP transactions	Click <b>Add</b> to add allowed LDAP transaction types to the list. The system displays the Add LDAP config / LDAP transactions configuration page, where you select the application transaction layer type, the route mode, and add LDAP configuration attributes.

4. Click **OK**.
5. Save and activate the configuration.

## Configure Local Policy

Configure local policy and local policy attributes for session routing based on the next hop parameter. The local policy specifies the protocol the

### Before You Begin

- Confirm that the system displays the Expert mode.

Use the local-policy element to configure where signalling messages are routed and forwarded.

### Procedure

1. From the Web GUI, click **Configuration > session-router > local-policy**.
2. On the Add local-policy page, click **Show advanced**, and do the following:

Attributes	Instructions
From address	<p>Click <b>Add</b>, and enter the source IP address, the POTS number, the E.164 number, or the hostname for the local-policy element.</p> <ul style="list-style-type: none"> <li>• This list requires at least one address.</li> <li>• You can add as many addresses as necessary.</li> <li>• You can use a wildcard or a DS:prefix (dialed string) for this parameter.</li> </ul>
To address	<p>Click <b>Add</b>, and enter the destination IP address, the POTS number, the E.164 number, or the hostname for the local-policy element.</p> <ul style="list-style-type: none"> <li>• This list requires at least one address.</li> <li>• You can add as many addresses as necessary.</li> <li>• You can use a wildcard for this parameter.</li> </ul>
Source realm	<p>Click <b>Add</b>, and enter one or more valid realms for identifying coming into a realm. The default is *.</p>
Description	<p>Enter a description of this local-policy.</p>
State	<p>Select to enable this policy.</p>
Policy priority	<p>Select the policy priority for this local policy from the drop-down list. The default is none.</p>
Policy attributes	<p>Click <b>Add &gt; Show advanced</b>, and do the following:</p> <ul style="list-style-type: none"> <li>• Next hop. Select the signaling host IP address, SAG, hostname, or ENUM config from the drop-down list.</li> <li>• Realm. Select the realm for the next hop from the drop-down list. Not required when the realm is the same as the realm configured for the Session Agent that is the next hop.</li> <li>• Action. Select an action for the next hop from the drop-down list.</li> <li>• Terminate recursion. Select to terminate route recursion with the next hop. Deselect to include next hops after this one.</li> <li>• Cost. Enter the cost configured for local policy to rank policy attributes, representing the cost of a route relative to other routes reaching the same destination address. Enter a number from 0-9999999.</li> <li>• State. Select to enable.</li> <li>• App protocol. Select the application protocol for signalling the session agent from the drop-down list.</li> <li>• Lookup. Select an additional local policy lookup from the drop-down list.</li> <li>• Next key. Enter the next stage key for multi-stage local policy lookups.</li> </ul>

3. Click **OK**.
4. Save and activate the configuration.

## Configure Local Routing

Use the local-routing-config element to specify route tables that the Oracle Enterprise Session Border Controller (E-SBC) uses to direct calls to the next hop and to map an E.164 telephone number to a SIP URI, locally.

### Before You Begin

- Confirm that the system displays the Expert mode.

### Procedure

1. From the Web GUI, click **Configuration** > **session-router** > **local-routing-config**.
2. On the local routing config page, click **Add**.
3. On the Add local routing config page, do the following:

Attributes	Instructions
Name	Enter a unique name to use to refer to this local route table when you configure policy attributes. Required.
File name	Enter the name for the file from which the database corresponding to this local route table is created. Use the .gz format, and place the file in the /code/lrt/ directory. Required.
Prefix length	Enter the number of digits to use for lookup and cache storage. Range: 0-999999999.
String lookup	Select to enable lookup by string instead of E.164 phone numbers, when lookup tables contain range entries with alphanumeric prefixes.
Retarget requests	Select to replace Request-URI in forwarded requests.
Match mode	Select a lookup matching mode from the drop-down list. Note that this setting has no effect when table entries are ranges.

4. Click **OK**.
5. Save and activate the configuration.

## Configure a Session Agent

You can enable and configure constraints that the Oracle Enterprise Session Border Controller (E-SBC) applies to regulate session activity with the session agent.

### Before You Begin

- Confirm that the system displays the Expert mode, and that a least one of each of the following parameters is configured:
  - Media profile
  - Out Translation ID
  - Local Response Maps
  - Codec Policy
  - Session Recording Server

In the following procedure, some constraints affect session agent groups and SIP proxies outside of, and at the edge of the network. For example, the maximum sessions and maximum outbound sessions constraints do not apply to core routing proxies because they are transaction statefull, rather than session statefull. Other constraints, such as maximum burst rate, burst rate window, maximum sustained rate, and sustained rate apply to core routing proxies.

### Procedure

1. From the Web GUI, click **Configuration** > **session-router** > **session-agent**.
2. On the session-agent page, click **Add**, do the following:

Attributes	Instructions
Host name	Enter the name of the host associated with the agent in host name, FQDN, or IP address format. This field is required and the name cannot include blank spaces. The value entered here must be unique to this agent because no two agents can use the same host name. <ul style="list-style-type: none"> <li>• If you enter the host name as an IP address, you do not have to enter an IP address in the optional IP address parameter.</li> <li>• If you enter the host name in FQDN format, and you want to specify an IP address, enter it in the optional IP address parameter.</li> </ul>
IP address	(Optional) Enter the IP address for the host name that you entered in FQDN format if you want to specify the IP address. Otherwise, you can leave this parameter blank to allow a DNS query to resolve the host name.
Port	Enter the number of the port associated with this agent. <ul style="list-style-type: none"> <li>• 0. If you enter zero, the E-SBC cannot initiate communication with this agent (although it will accept calls).</li> <li>• 1025-65535.</li> <li>• The default value is 5060.</li> </ul> If the transport method value is TCP, the E-SBC will initiate communication on the TCP port of the agent.
State	Select State to enable this agent.
App protocol	Select the protocol to use to signal the session agent.
Transport method	Select the transport mode for connections to this agent. <ul style="list-style-type: none"> <li>• UDP - Default</li> <li>• UDP+TCP</li> <li>• Dynamic TCP</li> <li>• Static TCP</li> <li>• Dynamic TLS</li> <li>• Static TLS</li> <li>• DTLS</li> <li>• TLS+DTLS</li> <li>• Static SCTP</li> </ul>
Realm ID	Select the name of the realm where this agent is located.



Attributes	Instructions
Egress realm ID	Select the default egress realm to use for session agent pings and for when multiple egress realms are possible. For example, "realm-id is empty, or..."
Description	Enter descriptive text to identify this agent.
Constraints	Select to enable the use of constraints on this agent.
Max sessions	Enter the maximum number of sessions allowed for this constraint. 0-999999999.
Max inbound sessions	Enter the maximum number of inbound sessions allowed from this session agent. 0-999999999.
Max outbound sessions	Enter the maximum number of outbound sessions allowed for this constraint. 0-999999999.
Max burst rate	Enter the maximum number of invites allowed in a burst time period. 0-999999999.
Max inbound burst rate	Enter the maximum inbound burst rate in INVITEs per second from this session agent. 0-999999999.
Max outbound burst rate	Enter the maximum outbound burst rate in INVITEs per second from this session agent. 0-999999999.
Max sustain rate	Enter the maximum rate of session invitations allowed within the current time period for this constraint. 0-999999999.
Max inbound sustain rate	Enter the maximum inbound sustain rate of session invitations allowed within the current time period for this constraint. 0-999999999.
Max outbound sustain rate	Enter the maximum outbound sustain rate of session invitations allowed within the current time period for this constraint. 0-999999999.
Time to resume	Enter the number of seconds that this session agent is out of service after reaching the constraint limit before attempting to re-initialize.
In service period	Enter the number of seconds that this session agent is allowed to re-initialize before returning to in-service status.
Burst rate window	Enter the time period, in seconds, used to measure the burst rate. 0-999999999.
Sustain rate window	Enter the time period, in seconds, used to measure the sustained rate. 0-999999999.
Proxy mode	Select a proxy mode for the E-SBC to use when a SIP request arrives from this agent.
Redirect action	Select a method for the redirect response from this agent. <ul style="list-style-type: none"> <li>• Proxy. Send the response back to the previous hop.</li> <li>• Recurse. Recurse on the contacts in the response.</li> <li>• Recurse 305, only. Recurse on the contacts in the 305 response, only.</li> </ul>
Loose routing	Select to enable.
Response map	Select the name of the response map.

Attributes	Instructions
Ping method	Enter the SIP ping method.
Ping interval	Enter the time, in seconds, to ping this session agent.
Ping send mode	Select the mode for pinging this session agent. <ul style="list-style-type: none"> <li>• Continuous</li> <li>• Keep alive</li> </ul>
Ping all addresses	Select to ping all addresses.
Ping in service response codes	Enter one or more response codes that keep the session agent in service.
Options	Add one or more options.
SPL solutions	Use to add, edit or delete an SPL against this agent.
Media profiles	Add the name of one or more media profiles.
In translationid	Select the inbound translation ID.
Out translationid	Select the outbound translation ID.
Manipulation string	Enter the string to use in header manipulation rules.
Manipulation pattern	Enter a regular expression to use in header manipulation rules.
Trunk group	Specify the name of the trunk group that you must use to reach this agent.
Max register sustain rate	Enter the maximum register sustain rate.
Invalidate registrations	Select to invalidate all registrations going to this session agent.
RFC2833 mode	Select the preferred mode for RFC2833.
RFC2833 payload	Enter a number for the RFC2833 payload type.
Codec policy	Select the codec policy to apply to this session agent.
Refer call transfer	Select the refer method for call transfer.
Refer notify provisional	Select the provisional mode for sending a NOTIFY message. <ul style="list-style-type: none"> <li>• None. The system sends no intermediate NOTIFY message.</li> <li>• Initial. The system sends an intermediate 100 Trying NOTIFY message.</li> <li>• All. The system sends an intermediate 100 Trying NOTIFY message, plus a NOTIFY for each non-100 provisional received by the E-SBC.</li> </ul>
Reuse connections	Select the protocol for SIP reuse connection.
TCP keepalive	Select an option for the TCP keepalive function.
TCP reconn interval	Enter the re-connection interval for TCP re-connection.
Max register burst rate	Enter the number of seconds allowed for the maximum register burst rate.
KPML interworking	Select a status for KPML Interworking.
Monitoring filters	Add one or more monitoring filters.
Auth attribute	Add one or more authentication attributes.
Session recording server	Select a session recording server.
Session recording required	Select to enable.
Hold refer reinvite	Select to enable.

3. Click **OK**.
4. Save and activate the configuration.

## SIP hold-refer-reinvite

When SIP hold-refer-reinvite is enabled for REFER with Replaces, the system queues the outgoing Invite populated from the received REFER based on the dialog state.

In a deployment where a call goes through the Oracle Enterprise Session Border Controller (E-SBC) before going to an Interactive Voice Response (IVR) server, the E-SBC proxies the intermediate reinvite that the IVR sends to the transfer target. If the intermediate reinvite is in either the pending state or the established state when the IVR initiates the transfer to the transfer target, the E-SBC terminates the call prematurely. The hold-refer-reinvite option allows the E-SBC to queue the Out Going INVITE from the received REFER request when the previously proxied reinvite request is in either the pending state or the established state. The result is a successful call.

Enable the SIP hold-refer-reinvite option from the CLI command line or the Web GUI in Expert mode.

## Enable hold-refer-reinvite

The SIP hold-refer-reinvite parameter for REFER with Replaces is a parameter that you enable to prevent premature call termination in a deployment where calls are proxied by the Oracle Enterprise Session Border Controller.

### Before You Begin

- Confirm that refer-reinvite is added to realm/SA/SipInterface options.
- Confirm that refer-call-transfer is enabled on realm/SA/SipInterface
- Confirm that the session agent on which you want to enable hold-refer-reinvite is configured.
- Confirm that the system displays the Expert mode.

To enable hold-refer-reinvite, select a configured session agent and enable the parameter on the selected agent.

### Procedure

1. From the Web GUI, click **Configuration > session-router > session-agent**.
2. On the Session Agent page, select the agent and click **Edit**.
3. On the Modify Session Agent page, select Hold refer invite.
4. Click **OK**.
5. Save and activate the configuration.

### Next Steps

- Enable the refer-hold-reinvite parameter in the realm configuration.
- Enable the refer-hold-reinvite parameter in the session agent configuration.

## Configure a Session Group

Use the session-group element to define a signalling endpoint configured to apply traffic shaping attributes and information about next hops and previous hops.

### Before You Begin

- Confirm that the system displays the Expert mode.

### Procedure

1. From the Web GUI, click **Configuration** > **session-router** > **session-group**.
2. On the session group page, click **Add** > **Show advanced**.
3. On the Add session group page, do the following:

Attributes	Instructions
Group name	Enter the unique name of the session agent group element in the name format.
Description	Enter a description of this session group.
State	Select to enable.
App protocol	Select an application protocol from the drop-down list.
Strategy	Select a strategy from the drop-down list. <ul style="list-style-type: none"> <li>• Hunt. System selects the session agent in list order.</li> <li>• Least Busy. System selects the session agent with the fewest number of sessions relative to the max-outbound-sessions constraint of the session-agent element.</li> <li>• Low Sus Rate. System selects the session agent with the lowest sustained rate of session initiations and incitations.</li> <li>• Prop Dist. System uses the proportional distribution strategy to distribute traffic among all available session agent elements, based on session constraint limits.</li> <li>• Round Robin. System selects each session agent, one per session, in the order in which it is listed in the destination list. After all each session agents on the list is used, the system begins at the top of the list and repeats the cycle.</li> </ul>
Dest	Add one or more destinations to the list for this session agent group. The destination must correspond to a valid group name in another session agent group or to a valid hostname. Do one of the following, after adding a destination. <ul style="list-style-type: none"> <li>• Click <b>OK</b>.</li> <li>• Click <b>Apply/Add another</b>, add another destination, and click <b>OK</b>. Repeat, as needed.</li> </ul>

Attributes	Instructions
Trunk group	Add one or more trunk groups and context to the list for this session agent group. To use the default context case, omit : and the context. Preface with the + character to add, the - character to remove, and exclude and to remove and replace. Do one of the following, after adding a trunk group. <ul style="list-style-type: none"> <li>Click <b>OK</b>.</li> <li>Click <b>Apply/Add another</b>, add another trunk group, and click <b>OK</b>. Repeat, as needed.</li> </ul>
Sag recursion	Select to enable session agent group recursion for this session agent group.
Stop sag recursion	Enter the list of SIP response codes that terminate recursion in the session agent group. You can enter the response codes in a comma-separated list or as a range. Default is 401, 407.

- Click **OK**.
- Save and activate the configuration.

## Configure Session Recording Group

Use the **session-recording-group** element to define the collection of session recording servers in the HA group.

### Before You Begin

- Confirm that the system displays the Expert mode.

The session-recording-group configuration element is for High Availability (HA) only.

### Procedure

- From the Web GUI, click **Configuration** > **session-router** > **session-recording-group**.
- On the session recording group page, click **Add**.
- In the Add session recording group dialog, do the following:

Attributes	Instructions
Name	Enter a unique name for the session recording group.
Description	Enter a description for the session recording group.
Session recording servers	Click <b>Add</b> , enter the name of the session recording server, and do one of the following: <ul style="list-style-type: none"> <li>Click <b>OK</b>.</li> <li>Click <b>Apply/Add another</b>, add another session recording server, and click <b>OK</b>. Repeat, as needed.</li> </ul>

- Click **OK**.
- Save and activate the configuration.

## Configure SIP

Use the sip-config element to define parameters for communications between the Session Initiation Protocol (SIP) and the Oracle Enterprise Session Border Controller (E-SBC).

### Before You Begin

- Configure at least one home realm, egress realm, and transcoding realm.
- Confirm that the system displays the Expert mode.

### Procedure

1. From the Web GUI, click **Configuration** > **session-router** > **sip-config**.
2. On the SIP config page, do the following:

Attributes	Instructions
State	Select to enable SIP operations.
Dialog transparency	Select to preserve call IDs and tags.
Home realm id	Select the home realm to connect to the E-SBC from the drop-down list.
Egress realm	Select the default egress realm from the drop-down list.
Nat mode	Select a Network Address Translation (NAT) mode from the drop-down list. <ul style="list-style-type: none"> <li>• None. No SIP-NAT function.</li> <li>• Public. Means the home realm is public address space. Encrypt any URI from an external realm.</li> <li>• Private. Means the home realm is private address space. Encrypt any URI from the home realm.</li> </ul>
Registrar domain	Enter the domain name of the SIP registrar server.
Register host	Enter the hostname for the SIP registrar server.
Registrar port	Enter the port number of the SIP registrar server. Range: 1024-65535.
Init timer	Enter the time, in milliseconds, for the initial request retransmission timer. Range: 0-4294967295.
Max timer	Enter the maximum time, in milliseconds, for the request retransmission timer. Range: 0-4294967295.
Trans expire	Enter the time, in seconds, for the transaction expiration timer. Range: 0-4294967295.
Initial invite trans expire	Enter the transaction expiration time for the initial INVITE. Range: 0-999999999. If you enter 0, the system uses the sip-config-inv-trans expiration time. Default is 0.
Invite expire	Enter the INVITE transaction expiration time. Range: 0-4294967295.
Enforcement profile	Enter the name of the enforcement profile.

Attributes	Instructions
Red max trans	Enter the maximum number of redundancy synchronization transactions to keep on active. Range: 0-50000.
Options	Add any optional parameters and features.
SIP message len	Enter the maximum SIP message length. Range: 0-65535.
Enum sag match	Select to enable matching the name of this Session Agent Group to the hostname portions of ENUM NAPTR and LRT replacement URIs.
Extra method stats	Select to enable tracking method statistics for more entities.
Extra enum stats	Select to enable tracking ENUM statistics per server address.
Registration cache limit	Enter the maximum allowed number of registration cache entries.
Register use to for lp	Select to enable To header routing for REGISTER.
Refer src routing	Select to enable refer source realm routing.
Atcf stn sr	Enter the Session Transfer Number (STN-SR) allocated by Access Transfer Control Function (ACTF) in the REGISTER message.
Atcf psi dn	Enter the PSI-DN allocated by Access Transfer Control Function (ATCF) in the REGISTER message.
Atcf route to sccas	Select to enable routing the Access Transfer Control Function (ATCF) handover rate to SCCAS.
Eatf stn sr	Enter the E-TN-SR allocated by EATF in the INVITE handover message.
Sag lookup on redirect	Select to enable lookup of the Session Agent Group name on a redirect.
Set disconnect time on bye	Select to enable, if the disconnect time is set on receiving the BYE request.
Msrp delayed bye	Enter the maximum time, in seconds, to delay forwarding a BYE for an MSRP session. 0 = no delay. Range: 1-60.
Transcoding realm	Enter the name of the realm where transcoding agents reside.
Transcoding agents	Create a list of transcoding agents. Click <b>Add</b> , enter the name of a transcoding agent, and do one of the following: <ul style="list-style-type: none"> <li>Click <b>OK</b>.</li> <li>Click <b>Apply/Add another</b>, add another calling translation rule, and click <b>OK</b>. Repeat, as needed.</li> </ul>
Create dynamic sa	Select to enable the creation of dynamic session agents for service route.
Node functionality	Select a node functionality from the drop-down list.
Match SIP instance	Select to enable matching registration cache entries using the SIP instance parameter.
Sa routes stats	Select to enable tracking session agent statistics for routes resolved by DNS.

Attributes	Instructions
Sa routes traps	Select to enable generating traps when session agent routes change state.
Rx SIP reason mapping	Select to enable mapping RX disconnect events to the SIP Reason header.
Add ue location in pani	Select to enable adding the UE location string in the PANI header, when available.
Hold emergency calls for loc info	Enter a time to hold emergency calls until the E-SBC receives location information from PCRF over the RX interface. Range: 0-4294967295.

3. Click **OK**.
4. Save and activate the configuration.

## Configure SIP Features

Use the sip-feature element to define how the Oracle Enterprise Session Border Controller (E-SBC) handles option tags in the SIP Supported header, Require header, and the Proxy-Require header.

### Before You Begin

- Confirm that the system displays the Expert mode.

You can specify whether a SIP feature is applied to a specific realm or globally across all realms. You can also specify the treatment for an option based upon whether it appears in an inbound or outbound packet. You need to configure option tag handling in the SIP feature element only when you want a treatment other than the default.

### Procedure

1. From the Web GUI, click **Configuration > session-router > sip-feature**.
2. On the Sip feature page, do the following:

Attributes	Instructions
Name	Enter the action tag name to display in the Require, Supported, and Proxy-Require headers of SIP messages.
Realm	Do one of the following: <ul style="list-style-type: none"> <li>• Select the realm with which to associate this configuration.</li> <li>• Leave this parameter blank to make this configuration global.</li> </ul>
Support mode inbound	Select the action tag in the Supported header in an inbound packet from the drop-down list.
Require mode inbound	Select the action tag in the Require header for an inbound packet from the drop-down list. Default is reject.
Proxy require mode inbound	Select the action tag in the Proxy-Require header in an inbound packet from the drop-down list.
Support mode outbound	Select the action tag in the Supported header in an outbound packet from the drop-down list.
Require mode outbound	Select the action tag in the Require header for an outbound packet from the drop-down list.



Attributes	Instructions
Proxy require mode outbound	Select the action tag in the Proxy-Require header for an outbound packet from the drop-down list.

3. Click **OK**.
4. Save and activate the configuration.

## Configure SIP Interface

Use the sip-interface element to define SIP signaling.

### Before You Begin

- Confirm that a TLS profile exists.
- Confirm that rules exist for inbound and outbound SIP manipulation.
- Confirm that the system displays the Expert mode.

Configure a SIP interface for each network or realm to which you want to connect the Oracle Enterprise Session Border Controller.

### Procedure

1. From the Web GUI, click **Configuration > session-router > isp-interface**.
2. On the SIP Interface page, click Add.
3. On the Add SIP Interface page, do the following:

Attributes	Instructions
State	Select to enable this SIP interface.
Realm id	Select the realm in which to apply this SIP interface from the drop-down list.
Description	Enter a description of this SIP interface.

Attributes	Instructions												
SIP ports	<p>Specify the following parameters for the ports that the SIP proxy or B2BUA uses for connections.</p> <ul style="list-style-type: none"> <li>Address. Enter the IP address of the host associated with the sip-port entry.</li> <li>Port. Enter the port number for this sip-port. Default is 5060. Range 1025-65535.</li> <li>Transport protocol. Select the transport protocol associated with this SIP port. Default is UDP. Valid values are: DTLS, SCTP, TCP, TLS, and UDP.</li> <li>TLS profile. Enter the TLS profile name.</li> <li>Allow anonymous. Select the type of anonymous connection to allow from agents. Default is All. Valid values include:</li> </ul> <table border="1"> <thead> <tr> <th>Selection</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>All</td> <td>Allow all anonymous connections.</td> </tr> <tr> <td>Agents-only</td> <td>Allow requests from agents, only.</td> </tr> <tr> <td>Realm-prefix</td> <td>Allow session agent and address matching the realm prefix.</td> </tr> <tr> <td>Registered</td> <td>Allow session agent and registered endpoints, where REGISTER is allowed from any endpoint.</td> </tr> <tr> <td>Register-prefix</td> <td>Allow all connections from a session agent that match agents-only, realm-prefix, and registered agents.</td> </tr> </tbody> </table>	Selection	Description	All	Allow all anonymous connections.	Agents-only	Allow requests from agents, only.	Realm-prefix	Allow session agent and address matching the realm prefix.	Registered	Allow session agent and registered endpoints, where REGISTER is allowed from any endpoint.	Register-prefix	Allow all connections from a session agent that match agents-only, realm-prefix, and registered agents.
Selection	Description												
All	Allow all anonymous connections.												
Agents-only	Allow requests from agents, only.												
Realm-prefix	Allow session agent and address matching the realm prefix.												
Registered	Allow session agent and registered endpoints, where REGISTER is allowed from any endpoint.												
Register-prefix	Allow all connections from a session agent that match agents-only, realm-prefix, and registered agents.												
Nat traversal	<p>Select a Network Address Translation (NAT) traversal mode for SIP from the drop-down list.</p> <ul style="list-style-type: none"> <li>None. NAT traversal is disabled.</li> <li>Always. The system performs Hosted NAT Traversal (HNT), when the SIP-Via and the transport address do not match.</li> <li>Rport. The system performs HNT, when the VIA rport parameter is present and the SIP-Via and transport addresses do not match.</li> </ul>												
Registration caching	Select to enable non-HNT registration caching.												
Route to registrar	Select to enable routing requests to the registrar.												
In manipulationid	Select an inbound SIP manipulation rule from the drop-down list.												
Out manipulationid	Select an outbound SIP manipulation rule from the drop-down list.												
Service tag	Enter the service tag for this interface.												

- Click **OK**.
- Save and activate the configuration.

## Configure SIP Manipulation

When you need to modify specific components of a SIP message, configure a SIP manipulation rule. For example, you might need to resolve protocol differences between vendors. You can configure rules for SIP headers and for the sub-elements within the headers.

### Before You Begin

- Confirm that the system displays the Expert mode.

Use the **sip-manipulation** element to add, modify, delete, split, and join SIP headers and to specify SIP header rules. To begin, configure the Name, Description, (Optional) Split Headers, and (Optional) Join Headers attributes. When you reach the "Cfg Rules" section, click **Add** and select the header rule that you want to create. For further instructions, refer to the topics noted in the Cfg rules "Instructions" cell in the following table.

### Procedure

1. From the Web GUI, click **Configuration > session-router > sip-manipulation > Show advanced**.
2. In the SIP manipulation dialog, click **Add** and do the following:

Attributes	Instructions
Name	Enter the exact name of the header to which this rule applies. Alpha-numeric. No spaces. Case-sensitive.
Description	Enter a description of the purpose of this set of rules. Alpha-numeric.
Split headers	Create a list of headers that you want the system to split and treat separately before executing any manipulation rules. Click <b>Add</b> , enter the header, and do one of the following: <ul style="list-style-type: none"> <li>• Click <b>OK</b>.</li> <li>• Click <b>Apply/Add another</b>, add another header, and click <b>OK</b>. Repeat, as needed.</li> </ul>
Join headers	Create a list of headers that you want the system to join and treat as one header after executing any manipulation rules. Click <b>Add</b> , enter the header that you want the system to join, and do one of the following: <ul style="list-style-type: none"> <li>• Click <b>OK</b>.</li> <li>• Click <b>Apply/Add another</b>, add another header, and click <b>OK</b>. Repeat, as needed.</li> </ul>
cfg rules	Click <b>Add</b> , select one of the following header rules from the menu, and see the corresponding documentation for further instructions. <ul style="list-style-type: none"> <li>• header rule—"Configure Header Rule"</li> <li>• mime rule—"Configure MIME Rule"</li> <li>• mime isup rule—"Configure MIME ISUP Rule"</li> <li>• mime sdp rule—"Configure MIME SDP Rule"</li> </ul>

3. When you finish configuring SIP manipulations, and the system returns you to the SIP manipulation page, save and activate the configuration.

**Next Steps**

- Apply the rules to a session agent or SIP interface as "inbound" or "outbound."

## Configure SIP Monitoring

Use the sip-monitoring element to configure SIP Monitor and Trace features and to set filters for SIP monitoring.

**Before You Begin**

- Confirm that a session agent, a realm, or both are configured, or you must set filtering on a global basis for Monitor and Trace to occur.
- Confirm that the system is displaying Expert mode.

You must configure the sip-monitoring object to enable filtering. The only required setting is State, which enables sip-monitoring. You can optionally monitor all filters or you can specify one or more filters to monitor. You can specify a time for short session duration monitoring and you can select interesting events to monitor.

**Note:**

Interesting Events are always enabled on a global-basis on the Oracle Enterprise Session Border Controller.

**Procedure**

1. From the Web GUI, click **Configuration > session-router > sip-monitoring**.
2. On the SIP monitoring page, click **Show advanced**, and do the following:

Attributes	Instructions
Match any filter	Select to enable.
State	Select to enable the sip-monitoring configuration.
Short session duration	Enter a number of minutes from 0-999999999.
Monitoring filters	Click <b>Add</b> to add one or more custom monitoring filters to the list to use when monitoring on a global-basis. Enter the name of the filter, and do one of the following: <ul style="list-style-type: none"> <li>• Click <b>OK</b>.</li> <li>• Click <b>Apply/Add another</b>, add another media attribute, and click <b>OK</b>. Repeat, as needed.</li> </ul>
Interesting events	Click <b>Add</b> , and select either short-session or local-rejection.
Trigger window	Enter a number from 0-999999999.

3. Click **OK**.
4. Save and activate the configuration.

## Remote Site Survivability Configuration

You must enable remote site survivability on the Oracle Enterprise Session Border Controller (E-SBC) and set the ping method for the session agent before the E-SBC can perform remote site survivability operations.

The process for configuring remote site survivability includes the following procedures.

1. Enable remote site survivability mode on the E-SBC.
2. Configure a ping method for the session agent to use to determine when the E-SBC is not responding.

### Note:

The system does not require a reboot after activating or modifying remote site survivability.

## Configure Remote Site Survivability

You must enable remote site survivability on the Oracle Enterprise Session Border Controller (E-SBC) and set the parameters before the system can enter and exit survival mode.

### Before You Begin

- Confirm that at least one session agent is configured.
- Confirm that the system displays the Expert mode.

### Procedure

1. From the Web GUI, click **Configuration > session-router > survivability**.
2. At the bottom of the left pane, click **Show advanced**.
3. On the Add survivability page, do the following:

Attributes	Instructions
State	Select to enable Survivability.
Reg expires	Enter the number of seconds that the Oracle Enterprise Session Border Controller waits before entering the remote site survivability mode when the registration expires.
Prefix length	Enter the maximum number of digits allowed for a phone extension. Range: 0-10.
Session agent hostname	Select the agent hostname or the session agent group name from the drop down list.

4. Click **OK**.
5. Save and activate the configuration.

### Next Steps

- Configure a ping method on the session agent. See "Configure a Session Agent."

## Configure the Ping Method for a Session Agent

Configure a ping method to confirm that the session agent is in service.

Use the session-agent object to configure the ping-method for a session-agent.

1. Click **Configuration > session-router > session-agent**.
2. On the Modify Session Agent page, select the session-agent for which you want to configure the ping-method, and click **OK**.
3. In the **Ping method** field, enter the SIP message/method to use to ping a session agent. Oracle recommends setting this value to **OPTIONS**.
4. In the **Ping interval** field, enter the number of seconds between pings.
5. Click **OK**.
6. Save and activate the configuration.

## Configure Translation Rules

You can configure the Oracle Enterprise Session Border Controller (E-SBC) to use number translation to change a layer 5 endpoint name according to prescribed rules. For example, to add or to remove a 1 or a + from a phone number sent from or addressed to a device. Use the translation-rules element to create unique sets of translation rules to apply to calling and called party numbers.

### Before You Begin

- Confirm that the system displays the Expert mode.

In the following procedure, you set the translation type, define the string to add or delete, and set the character position (index) where the add, delete, or replace occurs in the string. The index starts at 0, immediately before the leftmost character, and increases by 1 for every position to the right. Use the \$ character to specify the last position in a string.

### Procedure

1. From the Web GUI, click **Configuration > session-router > translation-rules**.
2. On the Translation rules page, click **Show advanced**, and do the following:

Attributes	Instructions
Id	Enter the identifier or name for this rule.
Type	Select the address translation type from the drop-down list. <ul style="list-style-type: none"> <li>• Add. Add one or more characters to the address.</li> <li>• Delete. Delete one or more characters from the address.</li> <li>• None. Disable the translation rule.</li> <li>• Replace. Replace one or more characters in the address.</li> </ul>
Add string	Enter the string to add to the original address during address translation. For example, do not use characters such as @ and \$. Valid values are alpha-numeric characters.

Attributes	Instructions
Add index	Enter the index for the Add string. Use the \$ character to append the string at the end of the address. Valid values are alpha-numeric characters.
Delete string	Enter the string to be deleted from the original address during address translation. Unspecified characters are denoted by the @ character. Valid values are alpha-numeric characters.
Delete index	Enter the index for the string to delete.

 **Note:**

The @ character only works if the type parameter is set to delete. This parameter supports wildcard characters or digits only. For example, valid entries are: delete-string=@@@@, or delete-string=123456. An invalid entry is delete-string=123@@@.

When the type is set to **replace**, this value is used in conjunction with the add-string value. The value specified in the delete-string field is deleted and the value specified in the add-string field is inserted. If no value is specified in the delete-string parameter and the type field is set to replace, then nothing is inserted into the address.

3. Click **OK**.
4. Save and activate the configuration.

## System Configuration

You can configure the following system objects from the Configuration tab on the Web GUI:

Object	Purpose
auto-config	Enable automatic configuration.
capture-receiver	Configure and enable a capture receiver.
fraud-protection	Configure and enable fraud protection.
host-route	Configure a host route.
network-interface	Configure a network interface.
network-parameters	Configure TCP and SCTP parameters for the network.
ntp-config	Configure an NTP server and an authentication server.
phy-interface	Configure a physical interface.
redundancy-config	Enable redundancy and add a peer.
snmp-community	Configure an SNMP community.
spl-config	Enable an SPL plug-in.
system-access-list	Configure a system access list.

Object	Purpose
system-config	Configure the system.
tdm-config	Configure and enable TDM.
trap-reciever	Configure a trap receiver.
web-server-config	Configure and enable a web server.

 **Note:**

Click **Show Advanced** in the navigation pane to display all of the System objects in the preceding list.

## Configure a Host Route

Use the host-routes element to insert entries into the Oracle Enterprise Session Border Controller routing table to steer management traffic to the correct network.

### Before You Begin

- Confirm that the gateway for this host route is defined as a gateway for an existing network interface.
- Confirm that the system displays the Expert mode.

In the following procedure, note that no two host-route elements can use the same "dest network" address.

### Procedure

1. From the Web GUI, click **Configuration > system > host-route**.
2. On the Host Route page, click **Add**.
3. On the Add host route page, do the following:

Attributes	Instructions
Dest network	Enter the IPv4 address of the destination network for this host route.
Netmask	Select the netmask associated with the destination network from the drop-down list.
Gateway	Enter the gateway address for traffic going to the Dest network parameter to use as the first hop when forwarding a packet out of the originator's LAN.
Description	Enter a description for this host route. Alpha-numeric characters.

4. Click
5. Save and activate the configuration.

## Network Interface Configuration - Expert

In Expert mode, use the network-interface object to configure the parameters for the network interface.



The network interface element specifies a logical network interface over which you can configure one or more application (SIP) interfaces. The Oracle Enterprise Session Border Controller (E-SBC) supports only one network interface.

The following table describes the parameters that you can configure on the network interface. For configuration instructions, see "Configure the Network Interface."

Configuration Element	Description
Name	The name of the physical interface with which this network-interface element is linked. The name for network-interface elements that correspond to the phy-interface Control and Maintenance operation types must start with "wancom."
Sub port ID	The identification of a specific virtual interface in a physical interface (e.g., a VLAN tag). A value of 0 indicates that this element is not using a virtual interface. The sub-port-id field value is required only if the operation type is Media. Default is zero (0). Valid values are 0- 4095.
Description	A description of this network interface.
Hostname	Optional. The hostname of this network interface in Fully Qualified Domain Name (FQDN) format or IP address format.
IP address	Required. The IP address of this network interface in the IP address format.
Pri utility addr	The utility IP address for the primary peer in an HA pair.
Sec utility addr	The utility IP address for the secondary peer in an HA pair.
Netmask	The netmask portion of the IP address for this network interface entered in IP address format. The network-interface element will not function properly unless this field value is valid.
Gateway	A description for this host route. Valid values are alpha-numeric characters.

Configuration Element	Description
gw heartbeat	<ul style="list-style-type: none"> <li>State. Enable or disable front interface link detection and polling functionality on the E-SBC for this network-interface element. Default is enabled.</li> <li>Heartbeat. The time interval in seconds between heartbeats for the front interface gateway. Default is zero (0). Valid values are 0-65535.</li> <li>Retry count. Enter the number of front interface gateway heartbeat retries before a gateway is considered unreachable. Default is zero (0). Valid values are 0- 65535.</li> <li>Retry timeout. The heartbeat retry timeout value in seconds. Default is 1. Valid values are 1-65535.</li> <li>Health score. The amount to subtract from the health score if the front interface gateway heartbeat stops responding. (i.e. expires) The health score will be decremented by the amount set in this field if the timeout value set in the gw-heartbeat: retry timeout. Valid values are 0 -100.</li> </ul>
DNS IP primary	The IP address of the primary DNS to be used for this interface.
DNS IP backup1	The IP address of the first backup DNS to be used for this interface.
DNS domain	The default domain name used to populate incomplete hostnames that do not include a domain. Entries must follow the name format.
HIP IP list	A list of IP addresses allowed to access signaling and maintenance protocol stacks by way of this front interface using the HIP feature.

## Configure the Network Interface

You must configure the network interface of the Oracle Enterprise Session Border Controller (E-SBC) to communicate with the physical interface and the network.

### Before You Begin

- Confirm that the physical interface is configured. For more information, see "Physical Interface Configuration."
- Confirm that the system displays the Expert mode.

Use the network-interface object to configure the parameters for the network interface, which specifies a logical network interface over which you can configure one or more application SIP interfaces. Note that the E-SBC supports only one network interface.

### Procedure

- From the Web GUI, click **Configuration > Objects > System > network-interface**.
- On the network-interface page, click **Add**.
- On the Add network-interface page, click **Show Advanced**.
- In the Add network-interface dialog, do the following:

Attributes	Instructions
Name	Enter the name of the physical interface linked to this network interface. Control and Maintenance operation types must start with “wancom.”
Sub port ID	Enter the sub port ID to identify a specific virtual interface in a physical interface (e.g., a VLAN tag). A value of 0 indicates that this element is not using a virtual interface. The sub-port-id field value is required only if the operation type is Media. Default: 0. Range: 0-4095.
Description	Enter a description of this network interface.
Hostname	Enter the hostname of this network interface in Fully Qualified Domain Name (FQDN) format or IP address format.
IP address	The IP address of this network interface in the IP address format.
Pri utility addr	Enter the utility IP address of the primary peer in an HA pair.
Sec utility addr	Enter the utility IP address of the secondary peer in an HA pair.
Netmask	Enter the netmask portion of the IP address for this network interface in IP address format.
Gateway	Enter a description for this host route. Alpha-numeric characters.
Gw heartbeat	<ul style="list-style-type: none"><li>• State. Select to enable front interface link detection and polling functionality on the E-SBC for this network-interface element. Default: enabled.</li><li>• Heartbeat. Enter the time interval in seconds between heartbeats for the front interface gateway. Default: 0. Range: 0-65535.</li><li>• Retry count. Enter the number of front interface gateway heartbeat retries before a gateway is considered unreachable. Default: 0. Range: 0- 65535.</li><li>• Retry timeout. Enter the heartbeat retry timeout value in seconds. Default: 1. Range: 1-65535.</li><li>• Health score. Enter the amount to subtract from the health score if the front interface gateway heartbeat expires. Range: 0 -100.</li></ul>
DNS IP primary	Enter the IP address of the primary DNS to use for this interface.
DNS IP backup1	Enter the IP address of the first backup DNS to use for this interface.
DNS IP backup 2	Enter the IP address of the second backup DNS to use for this interface.
DNS domain	Enter the default domain name associated with this interface. Entries must follow the name format.
DNS timeout	Enter the maximum waiting time for a DNS response in seconds. Range: 0-4294967295.

Attributes	Instructions
Signalling mtu	Enter the Maximum Transmission Unit (MTU) size for signalling packets. Default: 0. Range: 576-4096.
HIP IP list	Create a list of IP addresses allowed to access signaling and maintenance protocol stacks by way of this front interface using the Hosted IP (HIP) feature. Click <b>Add</b> , enter the HIP IP address, and do one of the following: <ul style="list-style-type: none"> <li>• Click <b>OK</b>.</li> <li>• Click <b>Apply/Add another</b>, add another HIP IP address, and click <b>OK</b>. Repeat, as needed.</li> </ul>
Ftp address	Enter the FTP address.
ICMP address	Create a list of Internet Control Message Protocol (ICMP) addresses. Click <b>Add</b> , enter the ICMP address, and do one of the following: <ul style="list-style-type: none"> <li>• Click <b>OK</b>.</li> <li>• Click <b>Apply/Add another</b>, add another ICMP address, and click <b>OK</b>. Repeat, as needed.</li> </ul>
Telnet address	Enter the Telnet address.
Ssh address	Enter the SSH IP address. The gateway address of this interface must be default gateway.

5. Click **OK**.
6. Save and Activate the configuration.

#### Next Steps

- For High Availability (HA), configure redundancy. See "Redundancy Configuration" and "Configure Redundancy."

## Configure NTP

Use the `ntp-config` element to associate the Network Time Protocol (NTP) server with the Oracle Enterprise Session Border Controller (E-SBC).

#### Before You Begin

- Confirm that the system displays the Expert mode.

Use the following procedure to configure synchronization of the NTP server with the E-SBC.

#### Procedure

1. From the Web GUI, click **Configuration** > **system** > **ntp-config**
2. On the `ntp-config` page, do the following:

Attributes	Instructions
Server	Click <b>Add</b> , enter the name or IP address of the NTP server in your network that you want to use for the E-SBC, and do one of the following: <ul style="list-style-type: none"> <li>Click <b>OK</b>.</li> <li>Click <b>Apply/Add another</b>, add another NTP server, and click <b>OK</b>. Repeat, as needed.</li> </ul>
Auth servers	<ol style="list-style-type: none"> <li>Click <b>Add</b>.</li> <li>IP address. Enter the IPv4 address of the NTP server.</li> <li>Keyid. Enter the Key ID. Range: 1-999999.</li> <li>Key. Enter the authentication key in bytes. Range: 1-28.</li> <li>Click <b>OK</b>.</li> </ol>

- Click **OK**.
- Save and activate the configuration.

## Physical Interface Configuration - Expert

In Expert mode, use the phy-interface object to configure the type of physical interface and the parameters for its operation.

The following table describes the parameters that you can configure on the physical interface. For configuration instructions, see "Configure the Physical Interface for Control - Expert" and "Configure the Physical Interface for Media - Expert."

Field	Description
Name	Enter a unique name for this physical interface, using the name format. The name for Control and Maintenance physical interfaces must begin with "wancom."
Operation type	The physical interface performs the following types of operations. You must perform the phy-interface configuration procedure for each type of operation. Default is Control. <ul style="list-style-type: none"> <li>Media. Front-panel interfaces only. Port: 0-3. Slot: 0 or 1.</li> <li>Control. Rear-panel interfaces only. Port 0, 1, or 2 Slot: 0.</li> <li>Maintenance. Rear-panel interfaces only. Port 0, 1, or 2 Slot: 0.</li> </ul>
Port	The physical port number on an interface of the phy-interface being configured. Default is zero (0). Valid values are: <ul style="list-style-type: none"> <li>0-2 for rear-panel interfaces</li> <li>0-1 for two possible GigE ports on front of Oracle Enterprise Session Border Controller (E-SBC)chassis</li> <li>0-3 for four possible FastE ports on front of E-SBC chassis</li> </ul>

Field	Description
Slot	The physical slot number on the Oracle Enterprise Session Border Controller chassis. Default is zero. Valid values are: <ul style="list-style-type: none"> <li>0 is the motherboard (rear-panel interface) if the name begins with "wancom." 0 is the left Phy media slot on front of Oracle Enterprise Session Border Controller chassis.</li> <li>1 is the right Phy media slot on front of Oracle Enterprise Session Border Controller chassis.</li> </ul>
Virtual mac	Required for High Availability (HA) configuration. Enter the MAC address identifying a front-panel interface when the E-SBC is in the Active state. Generate this field value from the unused MAC addresses assigned to a E-SBC.
Admin state	Media interface, only.
Auto negotiation	Media interface, only.
Duplex mode	The 10/100 Phy card interfaces located on the front panel of the E-SBC can operate in full-duplex mode or half-duplex mode. Default is full.
Speed	Media interface, only. The speed in Mbps of the front-panel 10/100 Phy interfaces. This field is used only if the auto-negotiation field is set to disabled for 10/100 Phy cards. Default is 100.
Wancom health score	The amount to subtract from the E-SBC health score if a rear interface link goes down. Default is 50. Valid values are 0-100.

## Configure the Physical Interface for Control - Expert

You must configure the physical interface of the Oracle Enterprise Session Border Controller to connect to the network for control operations.

Note the settings that you want for this interface. For information about the configuration settings, see "Physical Interface Configuration."

In Expert mode, use the phy-interface object to configure the physical interface for the operation type Control.

1. From the Web GUI, go to **Configuration > Objects > System > phy-interface**.
2. On the phy-interface page, click **Add**.
3. On the Add phy-interface page, click **Show Advanced**.
4. In the Add phy-interface dialog, do the following:
  - Name. Enter "wancom0."
  - Operation type. Select Control from the operation type drop down list.
  - Port. Enter 0.
  - Slot. Enter 0.
5. Click **OK**.
6. **Save** and **Activate** the configuration.

Configure the Media Interface. See "Media Interface Configuration" and "Configure the Physical Interface for Media - GUI Expert."

## Configure the Physical Interface

You must configure the physical interface of the Oracle Enterprise Session Border Controller to connect to the network.

### Before You Begin

- Confirm that the system displays the Expert mode.

Use the phy-interface object to configure the physical interface for control, media, and maintenance operations. Perform this procedure for each operation type, which you will select in step 4.

### Procedure

1. From the Web GUI, click **Configuration > Objects > System > phy-interface**.
2. On the phy-interface page, click **Add**.
3. On the Add phy-interface page, click **Show Advanced**.
4. In the Add phy-interface dialog, do the following:

Field	Description
Name	Enter a unique name for this physical interface, using the name format. For Control and Maintenance physical interfaces, the name must begin with "wancom."
Operation type	Select the type of operation for this physical interface configuration. You must perform the phy-interface configuration procedure for each type of operation. Default: Control. <ul style="list-style-type: none"> <li>• Media</li> <li>• Control</li> <li>• Maintenance</li> </ul>
Port	Enter the physical port number for the operation type. <ul style="list-style-type: none"> <li>• Media. Front-panel interfaces only. Port: 0-3.</li> <li>• Control. Rear-panel interfaces only. Port 0-2.</li> <li>• Maintenance. Rear-panel interfaces only. Port 0-2.</li> </ul>
Slot	Enter the physical slot number for the operation type. <ul style="list-style-type: none"> <li>• Media. Front-panel interfaces only. Slot: 0 or 1.</li> <li>• Control. Rear-panel interfaces only. Slot: 0.</li> <li>• Maintenance. Rear-panel interfaces only. Slot: 0.</li> <li>• 0 is the motherboard (rear-panel interface), if the name begins with "wancom."</li> <li>• 0 is the left Phy media slot on the front of the chassis.</li> <li>• 1 is the right Phy media slot on the front of the chassis.</li> </ul>

Field	Description
Virtual mac	Enter the virtual MAC address for this interface in hexadecimal format.
Admin state	Select to enable the administrative state of the Media interface. Not applicable for Control and Maintenance interfaces.
Auto negotiation	Select to enable auto negotiation on the Media interface. Not applicable for Control and Maintenance interfaces.
Duplex mode	Select the duplex mode for the Media interface. Default: Full.
Speed	Select the speed for the Media interface. Required only when auto-negotiation is set to disabled for 10/100 Phy cards. Default: 100.
Wancom health score	The amount to subtract from the E-SBC health score, if the wancom link goes down. Default: 50. Range: 0-100.

5. Click **OK**.
6. Save and activate the configuration.

#### Next Steps

- Configure the Network Interface. See "Configure the Network Interface."

## High Availability

High Availability (HA) is a network configuration used to ensure that planned and unplanned outages do not disrupt service. In an HA configuration, Oracle Enterprise Session Border Controllers (E-SBC) are deployed in a pair to deliver continuous high availability for interactive communication services. Two E-SBCs operating in this way are called an HA node. The HA node design ensures that no stable call is dropped in the event of an outage.

In an HA node, one E-SBC operates in the active mode and the other E-SBC operates in the standby mode.

- **Active.** The active member of the HA node is the system actively processing signal and media traffic. The active member continuously monitors itself for internal process and IP connectivity health. If the active member detects a condition that can interrupt or degrade service, it hands over its role as the active member of the HA node to the standby member.
- **Standby.** The standby member of the HA node is the backup system. The standby member is fully synchronized with active member's session status, but it does not actively process signal and media traffic. The standby member monitors the status of the active member and it can assume the active role without the active system having to instruct it to do so. When the standby system assumes the active role, it notifies network management using an SNMP trap.

The E-SBC establishes active and standby roles in the following ways.

- If an E-SBC boots up and is alone in the network, it is automatically the active system. If you pair a second E-SBC with the first one to form an HA node, the second system automatically establishes itself as the standby.
- If both E-SBCs in the HA node boot up at the same time, they negotiate with each other for the active role. If both systems have perfect health, then the E-SBC with the lowest HA rear interface IPv4 address becomes the active E-SBC. The E-SBC with the higher HA rear interface IPv4 address becomes the standby E-SBC.



If the rear physical link between the two E-SBCs is unresponsive during boot up or operation, both will attempt to become the active E-SBC. In this circumstance, processing does not work properly.

The standby E-SBC assumes the active role when:

- it does not receive a checkpoint message from the active E-SBC for a certain period of time.
- it determines that the active E-SBC health score declined to an unacceptable level.
- the active E-SBC relinquishes the active role.

To produce a seamless switch over from one E-SBC to the other, the HA node members share their virtual MAC and virtual IP addresses for the media interfaces in a way that is similar to Virtual Router Redundancy Protocol (VRRP). Sharing these addresses eliminates the possibility that the MAC address and the IPv4 address set on one E-SBC in an HA node will be a single point of failure. Within the HA node, the E-SBCs advertise their current state and health to one another in checkpointing messages to apprise each one of the other one's status. Using the Oracle HA protocol, the E-SBCs communicate with UDP messages sent out and received on the rear interfaces. During a switch over, the standby E-SBC sends out an ARP request using the virtual MAC address to establish that MAC address on another physical port within the Ethernet switch. To the upstream router, the MAC address and IP address are still alive. Existing sessions continue uninterrupted.

## High Availability on the Acme Packet 1100

The Acme Packet 1100 supports High Availability (HA), but the configuration differs from other Oracle Enterprise Session Border Controllers (E-SBC) because there is only one management interface on this device.

Unlike other E-SBCs, which provide two management interfaces and two media interfaces, the Acme Packet 1100 provides 1 management interface and 2 media interfaces. For HA, you must create a second management interface object on the Acme Packet 1100 with `wancom0` for the **name** and VLAN for the **sub-port-id**. You can configure only one management interface in an HA pair with these settings and the system does not support more than one HA interface with a VLAN tag.

### Note:

The Acme Packet 1100 E-SBC does not support High Availability (HA) for any call using the Time Division Multiplexing (TDM) interface.

## Configure the Acme Packet 1100 for HA

The details in the procedures for configuring High Availability (HA) on the Acme Packet 1100 differ from configuring HA for other models of the Oracle Enterprise Session Border Controller because the Acme Packet 1100 has a single management interface and it shares the `wancom0` port for HA operations.

Use the following Expert mode procedures to configure the Acme Packet 1100 for HA operations. You must perform the physical interface configuration twice. One configuration sets the Management operations the other configuration sets the Media operations.

### Procedure

1. Configure the physical interface for management. See "Configure the Physical Interface."

2. Configure the physical interface for media. See "Configure the Physical Interface."
3. Configure the network interface with addresses for the Primary and Secondary devices. See "Configure the Network Interface."
4. Configure the peers for redundancy. See "Configure Redundancy."

## Redundancy Configuration - Expert

In Expert mode, configure redundancy for a High Availability (HA) pair.

The following table describes the parameters that you must configure for HA redundancy. For configuration instructions, see "Configure Redundancy."

Configuration Element	Description
Name	The name of the HA node peer as it appears in the target name boot parameter. This is also the name of the system that appears in the system prompt. For example, in the system prompt ACMEPACKET#, ACMEPACKET is the target name for that Oracle Enterprise Session Border Controller (E-SBC).
State	Enable or disable HA for the E-SBC. Default is enabled.
Type	These values refer to the primary and secondary utility addresses in the network interface configuration. To determine what utility address to use for configuration checkpointing, set the type of E-SBC to either primary or secondary. You must change this field from unknown, which is the default. Valid values are: <ul style="list-style-type: none"> <li>• Primary. Set this type if you want the E-SBC to use the primary utility address.</li> <li>• Secondary. Set this type if you want the E-SBC to use the secondary utility address.</li> <li>• Unknown. If you leave this parameter set to this default value, the system cannot perform configuration checkpointing.</li> </ul>

## Configure Redundancy - Expert

You must configure the parameters to support redundancy for a High Availability (HA) pair of Oracle Enterprise Session Border Controller (ESBC) devices.

Confirm that the physical interface for Control, the physical interface for Media, and the Network interface on the primary ESBC are configured for HA pairing. See "Physical Interface Configuration" and "Network Interface Configuration."

In Expert mode, configure redundancy for High Availability (HA) pairing of the primary ESBC and the secondary ESBC. Perform this procedure for the primary ESBC.

1. From the Web GUI, go to **Configuration > Objects > System > redundancy-config**.
2. On the Add redundancy config page, click **Add**.
3. In the Add redundancy config/peer dialog, do the following:
  - a. Name. Enter the name of the HA peer as it appears in the target name boot parameter.
  - b. State. Select enable.

- c. Type. Select primary.
      - d. Destinations. Click **Add**.
4. In the Add redundancy-config / peer / destination dialog, do the following:
  - a. Address. Enter the pri-utility address from the network interface.
  - b. Network interface. Type **wancom0:<VLAN>**.
5. Click **OK**.
6. Click **Back**.

The system displays the Modify redundancy-config page.
7. In the Modify redundancy-config dialog, do the following:
  - a. Click **Add**.
  - b. Name. Enter the name of the secondary peer.
  - c. State. Select State.
  - d. Type. Select **secondary** from the drop down list.
8. Click **Show Advanced**.

The system displays the destinations dialog.
9. In the destinations dialog, do the following:
  - a. Click **Add**.
  - b. Address. Enter the sec-utility address from the network interface.
  - c. Network interface. Select **wancom0:<VLAN>** from the drop down list.
10. Click **OK**.
11. **Save** and **Activate** the configuration.
  - Reboot the system.

## SNMP Trap Receiver

A trap receiver is an application used to receive, log, and view SNMP traps for monitoring the Oracle Enterprise Session Border Controller (E-SBC).

An SNMP trap is the notification sent from a network device, such as an E-SBC, that declares a change in service. You can define one or more trap receivers on an E-SBC for redundancy or to segregate alarms with different severity levels to individual trap receivers. Each server on which an NMS is installed should be configured as a trap receiver on each E-SBC managed by an NMS.

You can select a filter level threshold that indicates the severity level at which a trap is sent to the trap receiver. The following table maps Syslog and SNMP alarms to trap receiver filter levels.

Filter Level	Syslog Severity Level	(SNMP) Alarm Severity Level
All	Emergency (1)	Emergency
	Critical (2)	Critical
	Major (3)	Major
	Minor (4)	Minor
	Warning (5)	Warning
	Notice (6)	
	Info (7)	
	Trace (8)	
	Debug (9)	
Critical	Emergency (1)	Emergency
	Critical (2)	Critical
Major	Emergency (1)	Emergency
	Critical (2)	Critical
	Major (3)	Major
Minor	Emergency (1)	Emergency
	Critical (2)	Critical
	Major (3)	Major
	Minor (4)	Minor

When configuring the trap-receiver element for use with Network Management Systems, Oracle recommends setting the filter-level parameter to All.

## Configure an SNMP Trap Receiver

You can define one or more SNMP trap receivers on an Oracle Enterprise Session Border Controller (E-SBC) for redundancy or to segregate alarms with different severity levels to individual trap receivers.

### Before You Begin

- Confirm that SNMP is configured.
- Note the names of users who are allowed to receive secure traps.
- Confirm that the system displays Expert mode.

Oracle recommends that you configure each server with an NMS installed as a trap receiver on each E-SBC managed by an NMS. When configuring the trap-receiver element for use with Network Management Systems, Oracle recommends setting the filter-level parameter to All.

### Procedure

1. From the Web GUI, click **Configuration > System > Show advanced > trap-receiver**.
2. On the trap receiver page, click **Add**.
3. On the Add trap receiver page, do the following:

Attributes	Instructions
IP address	Enter the IPv4 address and port number of an authorized NMS in dotted decimal format. Default: 0.0.0.0:162.

Attributes	Instructions
Filter level	Select the filter level threshold for the severity level at which a trap is sent to the trap receiver.
Community name	Enter the SNMP community name to which this trap receiver belongs.
User list	Create a list of users allowed to receive secure traps. Click <b>Add</b> , enter the name of a user, and do one of the following: <ul style="list-style-type: none"> <li>Click <b>OK</b>.</li> <li>Click <b>Apply/Add another</b>, add another user, and click <b>OK</b>. Repeat, as needed.</li> </ul>

 **Note:**

If SNMPv3 is enabled on the E-SBC, but no users are listed for this field, a warning message is sent during the verify-config execution.

- Click **OK**.
- Save and activate the configuration.

## SNMP Community

A Simple Network Management Protocol (SNMP) community is a grouping of network devices and management stations used to define where information is sent and accepted. An SNMP device or agent might belong to more than one SNMP community. SNMP communities provide a type of password protection for viewing and setting management information within a community.

An SNMP community is a string used as a password by the SNMP manager to communicate with the SNMP agent. The SNMP community string allows access to statistics of other devices. The access is used to support the monitoring of devices attached to the network for conditions that warrant administrative attention. When an SNMP community is configured, the Oracle Enterprise Session Border Controller (E-SBC) sends the community string along with all SNMP requests.

A community name value can also be used as a password to provide authentication, thereby limiting the NMS that has access to an E-SBC. With this field, the SNMP agent provides trivial authentication based on the community name that is exchanged in plain text SNMP messages. For example, public.

SNMP communities also include access level settings, which are used to define the access rights associated with a specific SNMP community. You can define two types of access level on the E-SBC, which are read-only and read-write. You can define multiple SNMP communities on an E-SBC to segregate access modes per community and NMS host. The access level determines the permissions that other NMS hosts can wield over this (E-SBC).

- Read-only. Allows GET requests. (Default)
- Read/Write. Allows both GET and SET requests.

IPv4 addresses that are valid within this SNMP community correspond with the IPv4 address of NMS applications that monitor or configure this E-SBC. Include the IPv4 addresses of each server on which an NMS is installed.

Only devices that support SNMPv1 and SNMPv2c protocol can use SNMP community strings. SNMPv3 uses username and password authentication, along with an encryption key.

## Configure SNMP Community

Configure a Simple Network Management Protocol (SNMP) community to support the monitoring of devices, such as the Oracle Enterprise Session Border Controller (E-SBC), attached to the network for conditions that warrant administrative attention.

### Before You Begin

- Confirm that SNMP is configured.
- Note the IP addresses that you want for this community.
- Confirm that the system displays Expert mode.

Use this procedure to group network devices and management stations, and to set the access rights for the community.



### Note:

Only devices that support SNMPv1 and SNMPv2c protocol can use SNMP community strings. SNMPv3 uses username and password authentication, along with an encryption key.

### Procedure

1. From the Web GUI, click **System > SNMP community**.
2. On the SNMP community page, click **Add**, and do the following:

Attributes	Instructions
Community name	Enter an SNMP community name of an active community where this E-SBC can send or receive SNMP information.
Access mode	Select the access level for all Network Management Systems (NMS) defined within this SNMP community.
IP address	Add one or more IPv4 addresses that are valid within this SNMP community, and click <b>OK</b> .

3. Click **OK**.
4. Save and activate the configuration.

## Configure an SPL Plugin

Use the spl-config element to configure the parameters for integrating System Programming Language (SPL) plugin extensions with the Oracle Enterprise Session Border Controller (E-SBC).

### Before You Begin

- Confirm that the SPL engine is installed on the E-SBC.
- Plan the order in which you configure multiple SPL plugins because the E-SBC executes the SPL plugins in the order of configuration.

 **Note:**

The E-SBC includes all SPL plugins, except for Comfort Noise Generation. You must manually upload the Comfort Noise Generation SPL plugin to the E-SBC performing the following procedure.

### Procedure

1. From the Web GUI, click **Configuration > system > spl-config**.
2. On the spl config / plugins page, do the following:

Attributes	Instructions
Spl options	Enter values for optional SPL parameters and features in a comma separated list enclosed in double quotation marks.
Plugins	Click <b>Add</b> , and do the following: <ul style="list-style-type: none"> <li>• State. Select to enable the SPL plugin on the E-SBC.</li> <li>• Name. Specify the name of the SPL plugin.</li> <li>• Click <b>OK</b>.</li> </ul>

3. Click **OK**.
4. Save and activate the configuration.

### Next Steps

- Execute the SPL plugin file.
- Synchronize the SPL across HA pairs.

## Time Division Multiplexing (TDM)

The TDM functionality is for companies planning to migrate from TDM to SIP trunks by using a hybrid TDM-SIP infrastructure, rather than adopting VoIP-SIP as their sole means of voice communications. The TDM interface provides failover for egress audio calls, when the primary SIP trunk becomes unavailable.

- The Acme Packet 1100 is the only platform that supports TDM.
- TDM support requires the optional TDM card.
- TDM operations require the configuration of line mode profiles and local policy.
- The available configuration profiles include T1 line mode and E1 line mode.
- The software upgrade procedure supports the TDM configuration.

 **Note:**

When the Acme Packet 1100 is deployed in an HA pair, the active system cannot replicate calls between SIP and TDM to the standby system.

For more information, see the Acme Packet 1100 Hardware Installation Guide, the ACLI Configuration Guide, the Web GUI User Guide, and the Web GUI Help.

## TDM Configuration

Time Division Multiplexing (TDM) is an option that requires configuration. You must enable TDM on the device, specify the parameters for the TDM interface properties, and configure local policies for inbound and outbound TDM traffic. Two-way TDM call routing requires both inbound and outbound local policies. For inbound-only or outbound-only TDM call routing, the system requires a local policy only for the call direction that you want.

You can configure TDM from either the Acme Command Line Interface (ACLI) or the Web GUI.

- ACLI. Use the `tdm-config` object from the system group of elements.
- Web GUI - Basic mode. Double-click the TDM icon in the network diagram to display the TDM configuration dialog.
- Web GUI - Expert mode. Use the `tdm-config` object from the system group of objects.

In addition to configuring the TDM interface properties, you must configure an inbound local policy for traffic entering the TDM interface and an outbound local policy for traffic exiting the TDM interface. In the inbound local policy, you specify `tdmRealm` for the source realm. In the outbound local policy, you specify the next hop that you want for TDM traffic.

The TDM card always supports bidirectional calls, but TDM call routing can be unidirectional. For example, for inbound-only operations, configure the TDM interface and configure only the inbound TDM policy.

If you upgrade from a previous release in which you configured outbound TDM and you want to add inbound TDM, you need only to create the local TDM policy for inbound TDM calls.

You can configure TDM to support either the T1 line mode or the E1 line mode. You can configure all TDM properties, except for line mode, in realtime. For example, changing the default T1 line mode to the E1 line mode requires a system reboot.

After configuring TDM, you must save and activate the configuration. Activating the TDM configuration generates the `tdm-config` template, which you can view by way of the `show running-config generated` command. except for line mode

 **Note:**

The TDM configuration template includes the `media-sec-policy` object only when the SRTP license is activated. See "Licensing for Time Division Multiplexing (TDM)."



## Configure TDM

To activate Time Division Multiplexing (TDM), you must enable TDM, create a profile that specifies the TDM interface, and run the Set TDM Configuration wizard.

### Before You Begin

- You must have Superuser permissions.
- Confirm that the optional TDM card is present in the device.
- Confirm that logging is enabled for the system, if you want to enable TDM logging in this procedure.
- Confirm that the system displays the Expert mode.

You can configure TDM from the Web GUI in Expert Mode by way of the `tdm-config` object. The following procedure is provided as an example of a typical TDM profile. In this procedure, some profile parameters are specific to the selected line mode. For example, if you select the T1 line mode, you must select 1-23 for B channel. Configure the remaining settings, which are not specific to a line mode, according to the requirements of your deployment.

### Procedure

1. From the Web GUI, click **Configuration > system > tdm-config**.

The system displays the TDM configuration dialog.

2. In the Tdm-config dialog, click Tdm-profile, and do the following:

Attributes	Instructions
State	Select to enable TDM.
Logging	Select to enable logging.
Name	Enter a name for this TDM profile.
Line mode	Select T1 or E1.
Signalling	<ul style="list-style-type: none"> <li>• Select <code>pri_net</code>, if you want the TDM card to use the internal clock as the source for timing.</li> <li>• Select <code>pri_cpe</code>, if you want the TDM card to use an external clock as the source for timing.</li> </ul>
Switch type	Select a switch type for this configuration.
B channel	<ul style="list-style-type: none"> <li>• For T1, select 1-23.</li> <li>• For E1, select 1-15,17-31.</li> </ul>
D channel	<ul style="list-style-type: none"> <li>• For T1, select 24.</li> <li>• For T1, select 16.</li> </ul>
Span number	Enter 0.
Line build out	Enter a number from 0 to133.
Framing value	<ul style="list-style-type: none"> <li>• For T1, select ESF.</li> <li>• For E1, select CCS.</li> </ul>
Coding value	<ul style="list-style-type: none"> <li>• For T1, select b8zs.</li> <li>• For E1, select hdb3.</li> </ul>
Tone zone	<ul style="list-style-type: none"> <li>• For T1, select US.</li> <li>• For E1, select ES.</li> </ul>
Rx gain	Set the TDM Receive channel volume in decibels. Maximum value is 9.9.

Attributes	Instructions
Tx gain	Set the TDM Transmit channel volume in decibels. Maximum value is 9.9.
Echo cancellation	Select to enable.

3. Click **OK**.  
The system displays the Set TDM Configuration dialog.
4. Click **Complete**.  
The system completes the TDM configuration and displays the success dialog.
5. Click **OK**.

#### Next Steps

- Configure the inbound and outbound TDM local policies.

## Configure Outbound Local Policy with TDM Backup

To complete the Time Division Multiplexing (TDM) configuration for redundancy, you must configure the TDM local routing policy.

#### Before You Begin

- Confirm that a TDM configuration exists.
- Confirm that a policy exists for the realm.
- Confirm that the system displays the Expert mode.

To configure TDM for backup, add the tdm profile as a second attribute to the local policy.

#### Procedure

1. From the Web GUI, click **Configuration** > **session-router** > **local-policy**.
2. On the local policy page, click **Add**.
3. On the Add local policy page, under Policy attributes, click **Add**.
4. On the Add Local Policy / policy attribute page, select tdm:<profilename> from the Next hop drop down list.
5. Click **OK**.
6. Save and activate the configuration.

## Configure Inbound TDM Local Policy

You must configure a local policy for inbound Time Division Multiplexing (TDM) traffic.

#### Before You Begin

- Confirm that TDM is configured.
- Confirm that the system displays the Expert mode.

Successful TDM operations require policies for inbound and outbound traffic. In the following procedure, you specify the parameters for inbound TDM traffic. For the source-realm parameter, note that **tdmRealm** is case-sensitive. For more information about local policy configuration and parameters, see "Configuring Local Policy" in the ACLI Configuration Guide.

For more information about local policy configuration and parameters, see "Configuring Local Policy" in the ACLI Configuration Guide.

#### Procedure

1. From the Web GUI, click **Configuration** > **session-router** > **local-policy**.
2. On the Local policy page, click **Add**.
3. On the Add local policy page, do the following:

Attributes	Instructions
From address	Click <b>Add</b> , enter the origin IP address, and click <b>OK</b> .
To address	Click <b>Add</b> , enter the destination IP address, and click <b>OK</b> .
Source realm	Click <b>Add</b> , select tdmRealm from the drop-down list, and click <b>OK</b> .
Policy attributes	Click <b>Add</b> , and do the following: <ul style="list-style-type: none"> <li>• Next hop. Select tdm:&lt;profilename&gt; from the drop-down list.</li> <li>• Realm. Select the realm for the next hop from the drop-down list.</li> <li>• Click <b>OK</b>.</li> </ul>

4. Click **OK**.
5. Save and activate the configuration.

#### Next Steps

- If one does not exist, configure the outbound TDM local policy.

## Configure the Outbound TDM Local Policy

You must configure a local policy for outbound Time Division Multiplexing (TDM) traffic.

#### Before You Begin

- Confirm that TDM is configured.
- Confirm that the system displays the Expert mode.

Successful TDM operations require policies for inbound and outbound TDM traffic. In the following procedure, you specify the parameters for outbound TDM traffic. For the next-hop parameter, use the name that you entered for tdm-profile in the TDM configuration procedure.

For more information about local policy configuration and parameters, see "Configuring Local Policy" in the ACLI Configuration Guide.

#### Procedure

1. From the Web GUI, click **Configuration** > **session-router** > **local-policy**.
2. On the Local policy page, click **Add**.
3. On the Add local policy page, do the following:

Attributes	Instructions
From address	Click <b>Add</b> , enter the origin IP address, and click <b>OK</b> .

Attributes	Instructions
To address	Click <b>Add</b> , enter the destination IP address, and click <b>OK</b> .
Source realm	Click <b>Add</b> , select source realm from the drop-down list, and click <b>OK</b> .
Policy attributes	Click <b>Add</b> , and do the following: <ul style="list-style-type: none"> <li>• Next hop. Select tdm:&lt;profilename&gt; from the drop-down list.</li> <li>• Realm. Select tdmRealm from the drop-down list.</li> <li>• Click <b>OK</b>.</li> </ul>

4. Click **OK**.
5. Save and activate the configuration.

#### Next Steps

- If one does not exist, configure the inbound TDM local policy.

## Web Server Configuration

The Web server is a software application that helps to deliver Web content that you can access through the Internet. The Web server runs the Enterprise application called the Web GUI.

Every Web server has an IP address and sometimes a domain name. For example, if you enter the URL `http://www.acmepacket.com/index.html` in your browser, the browser sends a request to the Web server with domain name is `acmepacket.com`. The server fetches the page named `index.html` and sends it to the browser.

If you enter `http://132.45.6.5`, and this address has been configured by your Administrator to access the Web GUI, the server fetches the page and displays the Web GUI logon page to your browser.

This section provides a procedure for configuring the Web server in your network.

## Configure a Web Server - Expert

Use the web-server element to enable the Web server and to specify how you want it to communicate with the Oracle Enterprise Session Border Controller.

#### Before You Begin

Confirm that the system displays the Expert mode.

#### Procedure

1. From the Web GUI, click **Configuration** > **system** > **web-server**.
2. On the Add Web server config page, click **Show advanced**, and do the following.

Attributes	Instructions
State	Select to enable Web server.
Inactivity timeout	Enter the number of minutes you want the Web server to wait before timing out.
HTTP state	Select to enable an HTTP connection to the Web server.
Optional. HTTP port	(Optional) Enter the port number that you want to use instead of the default port 80.

Attributes	Instructions
HTTPS state	Select to enable HTTPS connection to the Web server.
Optional. HTTPS port	(Optional) Enter a the port number that you want to use instead of the default port 443.
TLS profile	Select a TLS profile to use for HTTPS from the drop down list.

3. Click **OK**.
4. Save and activate the configuration.

# 4

## Monitor and Trace Tab

The Monitor and Trace tab displays the results of filtered SIP session data from the Oracle Enterprise Session Border Controller (E-SBC). The page displays the results in a common log format for local viewing.

Monitor and Trace supports the following summary reports that you can export to a PC.

- Sessions
- Registrations
- Subscriptions
- Notable events

Each report provides sorting, searching, and paging functionality. You can customize the columns in each report and use the buttons on the page to display additional information or to perform a task.

The SIP Monitor and Trace function can store messages per session and it can store cumulative sessions across all report types. When the sessions maximum is reached, the system removes the oldest call and adds the newest call.

- On systems with less than 4GB of RAM, the system can store:
  - 50 messages
  - 2,000 sessions
- On systems with more than 4GB of RAM, the system can store:
  - 50 messages
  - 4,000 sessions

The call database is not persistent across reboots

The system can perform live paging from Monitor and Trace tables.

### Note:

Monitor and Trace does not support multiple, simultaneous viewers. Only one user at a time can view Monitor and Trace information.

## Configure SIP Monitoring

You must enable sip-monitoring and configure the options for displaying session data and notable event data on the Monitor and Trace page.

### Before You Begin

- Configure any filters that you want, if you don't want to monitor all SIP traffic. See "Filter Configuration."

- Confirm that the Web GUI is in Expert mode.

The only required setting is State, which enables sip-monitoring. You can optionally monitor all filters and you can specify one or more filters to monitor. You can specify a time for short session duration monitoring and you can configure interesting events to monitor.

### Procedure

1. From the web GUI, click **Configuration > Session-Router > SIP-Monitoring**.
2. On the Modify sip-monitoring page, click **Show advanced**, and do the following.

Attributes	Instructions
Match any filter	Select to monitor all SIP traffic. Default: Disabled.
State	Select to enable SIP monitoring.
Short session duration	Enter a value, in seconds, for the maximum session duration of a short session. Default: 0. Range 0-999999999.
Monitoring filters	Create a global list of monitoring filters. Click <b>Add</b> , enter the name of the filter, and do one of the following: <ul style="list-style-type: none"> <li>• Click <b>OK</b>.</li> <li>• Click <b>Apply/Add another</b>, add another NTP server, and click <b>OK</b>. Repeat, as needed.</li> </ul>
Interesting events	Create a global list of interesting events to monitor. Click <b>Add &gt; Show advanced</b> , and do the following: <ul style="list-style-type: none"> <li>• Type. Select an event type from the drop-down list.</li> <li>• Trigger threshold. Enter the number of events required to occur in within the trigger window before the system starts monitoring. Default: 0. Range: 0-999999999.</li> <li>• Trigger timeout. Enter the amount of time, in seconds, that the monitoring persists. Default: 0. Range: 0-999999999,</li> <li>• Click <b>OK</b>.</li> </ul> The system displays the SIP monitoring page.

3. Click **OK**.
4. Save and activate the configuration.

### Next Steps

- View SIP Session Summary and SIP Notable Event Summary on the Monitor and Trace tab.

## Monitor and Trace SIP Messages

The **Monitor and Trace** page on the Web GUI displays the results of filtered SIP session data from a Oracle Enterprise Session Border Controller (E-SBC). The page displays the results in a common log format for local viewing.

When the E-SBC filters the data from a SIP message, it captures the message, applies the Header Manipulation Rules (HMR), and applies the Session Plug-in Language (SPL) to that message. When the message is sent from the E-SBC, it applies the SPL, applies the HMR, and sends the captured SIP message.

Monitor and Trace supports the following summary reports that you can export to a PC.

- Hairpin call data
- Notable events
- Registrations
- Sessions
- Siprec call data
- Subscriptions

Each type of report provides sorting, searching, and paging functionality. You can customize the columns in each report and use the buttons on the page to display additional information or perform a task.

The SIP Monitor and Trace function can store up to 100 messages per session and it can store up to 2000 cumulative sessions across all report types. Once the 2000 sessions maximum is reached, the system removes the oldest call and adds the newest call. The call database is not persistent across reboots.

## Sessions Report

The Sessions Report is a SIP session summary of all logged call sessions on the Oracle Enterprise Session Border Controller (E-SBC). When Lightweight Directory Access Protocol (LDAP) is enabled on the Active Directory, LDAP session messages may also display.

The columns that display on the Sessions Report page depend on the columns that you specified in the "Customizing the Page Display" procedure.

Start Time	State	Call ID	Request URI	From URI
2013-10-17 13:56:41.083	FAILED-408	5-15779@192.168.200.2	sip:service@192.168.200.2	9788482942 <sip:97884
2013-10-17 13:56:40.984	FAILED-408	4-15779@192.168.200.2	sip:service@192.168.200.2	9788482942 <sip:97884
2013-10-17 13:56:40.884	FAILED-408	3-15779@192.168.200.2	sip:service@192.168.200.2	9788482942 <sip:97884
2013-10-17 13:56:40.784	FAILED-408	2-15779@192.168.200.2	sip:service@192.168.200.2	9788482942 <sip:97884
2013-10-17 13:56:40.683	FAILED-408	1-15779@192.168.200.2	sip:service@192.168.200.2	9788482942 <sip:97884
2013-10-17 13:56:21.338	TERMINATED-	5-15665@192.168.200.2	sip:service@192.168.200.2	9788482942 <sip:97884
2013-10-17 13:56:21.238	TERMINATED-	4-15665@192.168.200.2	sip:service@192.168.200.2	9788482942 <sip:97884
2013-10-17 13:56:21.136	TERMINATED-	3-15665@192.168.200.2	sip:service@192.168.200.2	9788482942 <sip:97884

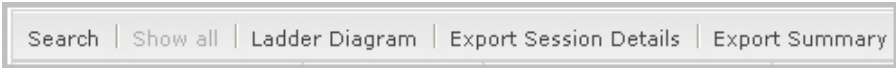
The following table describes the columns on the SIP Session Summary page.

Heading	Description
Start Time	Timestamp of the first SIP message in the call session.



Heading	Description
State	Status of the call or media session. Valid values are: INITIAL—Session for which an INVITE or SUBSCRIBE was forwarded. EARLY—Session that received the first provisional response (1xx other than 100). ESTABLISHED—Session for which a success (2xx) response was received. TERMINATED—Session that ended by receiving or sending a BYE for an “Established” session or forwarding an error response for an “Initial” or “Early” session. The session remains in the terminated state until all the resources for the session are freed up. FAILED—Session that failed due to a 4xx or 5xx error code.
Call ID	Identification of the call source. Includes the phone number and source IP address.
Request URI	Uniform Resource Identifier (URI) formatted string that identifies a resource by way of a protocol, name, location, and any other applicable characteristic that is sent by the E-SBC in REQUEST headers.
From URI	URI formatted string that identifies the call source information.
To URI	URI formatted string that identifies the call destination information.
Duration	Amount of time, in seconds, that the call or media event was active.
Notable Event	Indicates if a notable event has occurred on the call session. Valid values are: short session—Sessions that do not meet a minimum configurable duration threshold. Session dialogue, captured media information, and termination signalling. Any event flagged as a short session interesting event. local rejection—Sessions locally rejected at the E-SBC for any reason, for example, Session Agent (SA) unavailable, no route found, SIP signalling error, and so on. Session dialogue, capture media information, and termination signalling. Any event flagged as a local rejection interesting event.
Session ID	Identification assigned to the call session.
Ingress Src Addr	Source IP address of the incoming call or media event.
Egress Dest Addr	Destination IP address of the outgoing call or media event.

The following table describes the buttons on the SIP Session Summary page.

Button	Description
	
Search	Use to specify parameters for performing a search for specific session summary records within the current report.
Show all	Use to display all of the session summary records in the Sessions Report.
Ladder Diagram	Use to display a Ladder Diagram of a specific record in the table. The Ladder Diagram displays detailed information about a call session or media event.
Export Session Details	Use to export the SIP messages and media events associated with the selected session to a file in text format on the local machine.
Export Summary	Use to export all logged session summary records to a file in text format on the local machine.

## Display a Sessions Report

### Procedure

1. From the Web GUI, click **Monitor and Trace > Sessions**.  
The system displays the SIP Session Summary page.
2. Use the buttons on the top of the page to find, view, and export information about the records in the report.

## Ladder Diagram

A ladder diagram in the Web GUI schematic that shows the call and media flow of packets on ingress and egress routes by way of the Oracle Enterprise Session Border Controller.

A ladder diagram for the Sessions Report displays the following session summary information:

- Quality of Service (QoS) statistics for call sessions
- SIP messages and media events in time sequence

To display a ladder diagram for a specific record in the Sessions Report, click a record in the summary table or click **Ladder diagram** on the SIP Sessions Summary page.

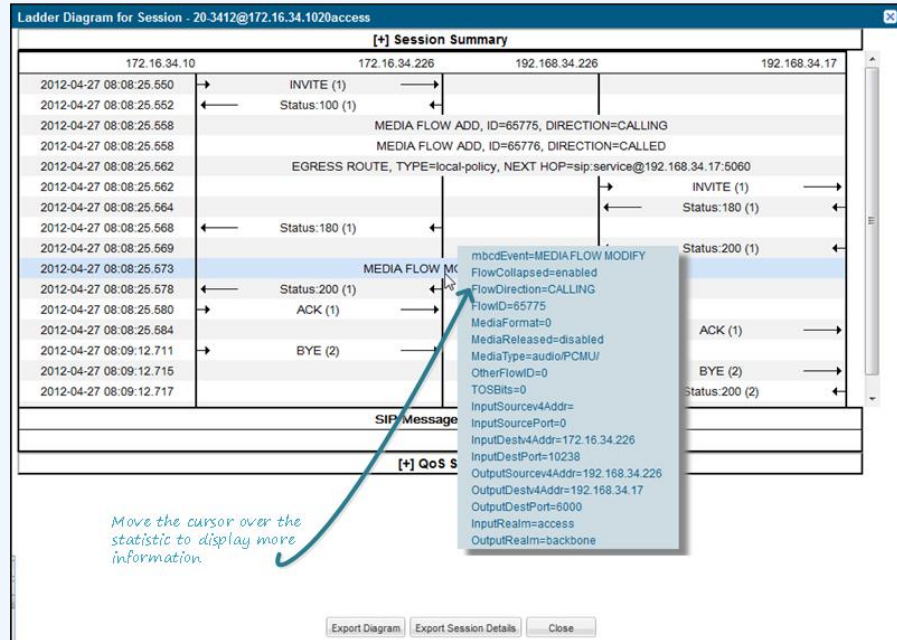
## Display a Ladder Diagram

To display a ladder diagram:

1. On the Sessions Report page, click **Ladder diagram**, or select a record in the table and double-click on that record. The following is an example of the ladder diagram that displays.

**Note:**

The Oracle Enterprise Session Border Controller (E-SBC) captures SIP messages, applies the Header Manipulation Rules (HMR) configured on the E-SBC, and then applies the Session Plug-in Language (SPL) to that message. When the message is sent out from the E-SBC, it applies the SPL, the HMR, and then sends out the captured SIP message. Therefore, when viewing the session detail on a Ladder Diagram, the HMR and SPL information may be present.

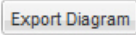


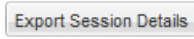
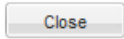
The Session Record Ladder Diagram consists of the following information:

- **Session Summary** - summary information about the call or media session in focus.
- **SIP Message Details** - SIP message and call flow information about the call or media session in focus.
- **QoS Statistics** - Quality of Service (QoS) statistic information about the call or media session in focus.

You can move your mouse over any statistic in the Ladder Diagram to view additional parameters and associated values for the statistic in a pop-up window.

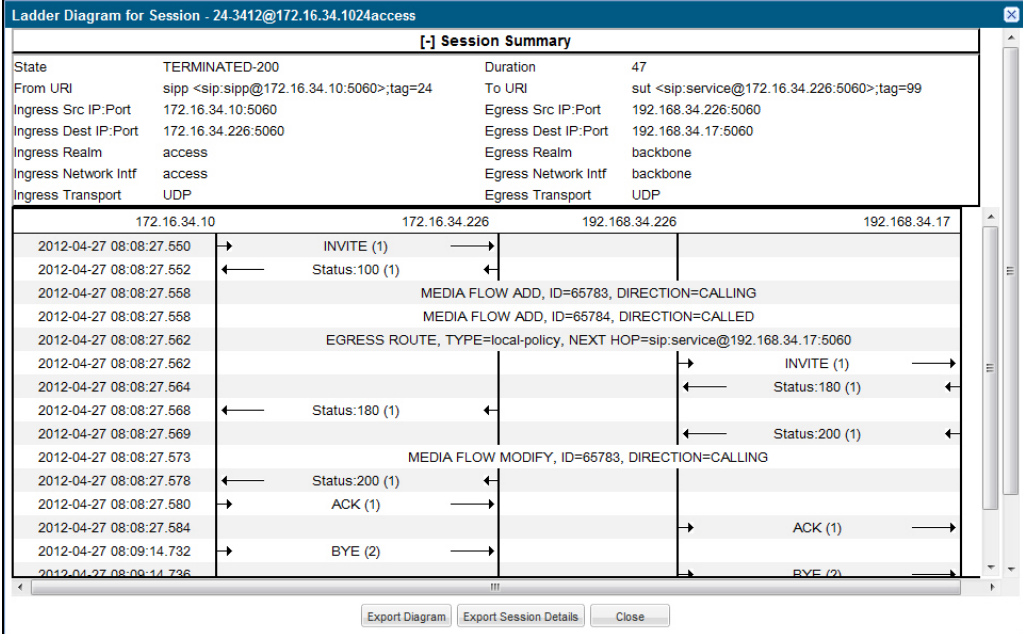
The following table describes the buttons in this Ladder Diagram window.

Button	Description
	Exports all of the information in the Ladder Diagram (Session Summary, SIP Message Details, and QoS statistics), to a file in text format on the local machine.

Button	Description
	Exports detailed information about the SIP messages and media events associated with the session in focus, to a file in text format on the local machine.
	Closes the Ladder Diagram window.

## Session Summary

The Session Summary window in the Ladder Diagram displays an overall summary of the call or media session in focus.



**[-] Session Summary**

State	TERMINATED-200	Duration	47
From URI	sipp <sip:sipp@172.16.34.10:5060>;tag=24	To URI	sut <sip:service@172.16.34.226:5060>;tag=99
Ingress Src IP:Port	172.16.34.10:5060	Egress Src IP:Port	192.168.34.226:5060
Ingress Dest IP:Port	172.16.34.226:5060	Egress Dest IP:Port	192.168.34.17:5060
Ingress Realm	access	Egress Realm	backbone
Ingress Network Intf	access	Egress Network Intf	backbone
Ingress Transport	UDP	Egress Transport	UDP

Sequence Diagram Details:

- 2012-04-27 08:08:27.550 → INVITE (1)
- 2012-04-27 08:08:27.552 ← Status:100 (1)
- 2012-04-27 08:08:27.558 MEDIA FLOW ADD, ID=65783, DIRECTION=CALLING
- 2012-04-27 08:08:27.558 MEDIA FLOW ADD, ID=65784, DIRECTION=CALLED
- 2012-04-27 08:08:27.562 EGRESS ROUTE, TYPE=local-policy, NEXT HOP=sip:service@192.168.34.17:5060
- 2012-04-27 08:08:27.562 → INVITE (1)
- 2012-04-27 08:08:27.564 ← Status:180 (1)
- 2012-04-27 08:08:27.568 ← Status:200 (1)
- 2012-04-27 08:08:27.573 MEDIA FLOW MODIFY, ID=65783, DIRECTION=CALLING
- 2012-04-27 08:08:27.578 ← Status:200 (1)
- 2012-04-27 08:08:27.580 → ACK (1)
- 2012-04-27 08:08:27.584 → ACK (1)
- 2012-04-27 08:09:14.732 → BYE (2)
- 2012-04-27 08:09:14.736 → BYE (2)

## Display the Session Summary

To display the Session Summary:

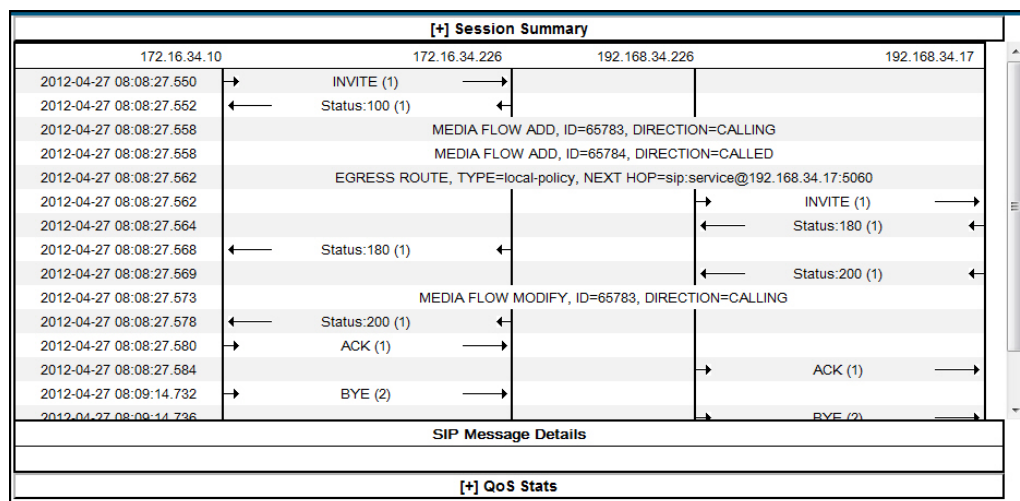
1. In the Ladder Diagram, click the [+] next to Session Summary at the top of the Ladder Diagram window. The Session Summary window expands. This window displays a summary of information about the call or media session in focus. The following table describes each field in the Session Summary window.

Heading	Description
State	Status of the call or media session. Valid values are: INITIAL Session for which an INVITE or SUBSCRIBE was forwarded. EARLY Session received the first provisional response (1xx other than 100). ESTABLISHED Session for which a success (2xx) response was received. TERMINATED Session that has ended by receiving or sending a BYE for an “Established” session or forwarding an error response for an “Initial” or Early session. The session remains in the terminated state until all the resources for the session are freed up. FAILED Session that has failed due to a 4xx or 5xx error code.
Duration	Amount of time, in seconds, that the call or media session was active.
From URI	URI formatted string that identifies the call source information.
To URI	URI formatted string that identifies the call destination information.
Ingress Src IP:Port	Source IP address and port number of the incoming call or media session.
Egress Src IP: Port	Source IP address and port number of the outgoing call or media session.
Ingress Dest IP:Port	Destination IP address and port number of the incoming call or media session.
Egress Dest IP: Port	Destination IP address and port number of the outgoing call or media session.
Ingress Realm	Incoming realm name.
Egress Realm	Outgoing realm name.
Ingress Network Intf	Name of the incoming network interface on the Oracle Enterprise Session Border Controller (E-SBC).
Egress Network Intf	Name of the outgoing network interface on the E-SBC.
Ingress Transport	Protocol type used on the incoming call or media session. Valid values are User Datagram Protocol (UDP) or Transport Control Protocol (TCP).
Egress Transport	Protocol type used on the outgoing call or media session. Valid values are User Datagram Protocol (UDP) or Transport Control Protocol (TCP).

- Click [-] to close the Session Summary window.

## SIP Message Details

The SIP Message Detail window displays detailed information and data flow (ingress and egress) about the call or media event.



When a session is routed using the a Lightweight Directory Access Protocol (LDAP) configuration (Active Directory) for the local policy, the LDAP information displays in the Session Summary window. The next hop value containing "enum:..." or "dns:..." displays. Similarly, the next hop value "ldap:..." displays for LDAP queries.

[+] Session Summary			
192.168.204.64	192.168.204.71	172.16.204.67	172.16.204.64
2012-07-09 15:30:58.328	→ INVITE (1)	→	
2012-07-09 15:30:58.334	← Status:100 (1)	←	
2012-07-09 15:30:58.354	MEDIA FLOW ADD, ID=65536, DIRECTION=CALLING		
2012-07-09 15:30:58.356	MEDIA FLOW ADD, ID=65537, DIRECTION=CALLED		
2012-07-09 15:30:58.371	EGRESS ROUTE, TYPE=local-policy, NEXT HOP=ldap:lookup		
2012-07-09 15:30:58.371		→ INVITE (1)	→
2012-07-09 15:30:58.625		← Status:180 (1)	←
2012-07-09 15:30:58.633	← Status:180 (1)		
2012-07-09 15:30:58.729		← Status:200 (1)	←
2012-07-09 15:30:58.738	MEDIA FLOW MODIFY, ID=65536, DIRECTION=CALLING		
2012-07-09 15:30:58.754	← Status:200 (1)		
2012-07-09 15:30:59.020	→ ACK (1)		
2012-07-09 15:30:59.028		→ ACK (1)	→
2012-07-09 15:31:01.754	→ BYE (2)		
2012-07-09 15:31:01.763		→ BYE (2)	→
2012-07-09 15:31:01.889		← Status:200 (2)	←
2012-07-09 15:31:01.900	← Status:200 (2)		
2012-07-09 15:31:01.893	MEDIA FLOW DELETE, ID=65536, DIRECTION=CALLING		
2012-07-09 15:31:01.895	MEDIA FLOW DELETE, ID=65537, DIRECTION=CALLED		
SIP Message Details			
[+] QoS Stats			

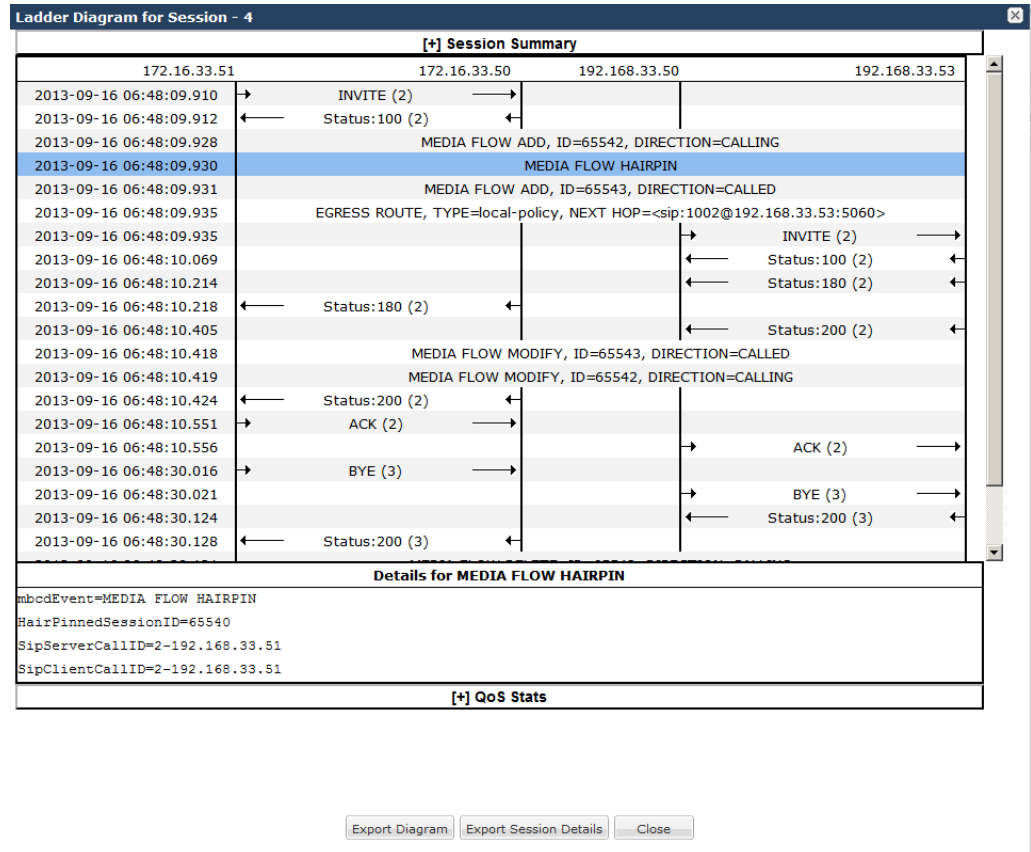
## SIPREC Call Data

The following diagram shows SIP Monitor and Trace output for a call with media forwarded by way of SIPREC.

[*] Session Summary				
192.168.33.1	192.168.33.100	172.16.33.100	172.16.33.1	192.168.33.2
2013-09-16 12:42:47.101	→ INVITE (1) →			
2013-09-16 12:42:47.104	← Status:100 (1) ←			
2013-09-16 12:42:47.128		MEDIA FLOW ADD, ID=65562, DIRECTION=CALLING		
2013-09-16 12:42:47.130		MEDIA FLOW ADD, ID=65563, DIRECTION=CALLED		
2013-09-16 12:42:47.170		→ INVITE (100021) →		
2013-09-16 12:42:47.190				← Status:100 (100021) ←
2013-09-16 12:42:47.200				← Status:200 (100021) ←
2013-09-16 12:42:47.226		EGRESS ROUTE, TYPE=local-policy, NEXT HOP=sip:service@172.16.33.1:5060		
2013-09-16 12:42:47.226			→ INVITE (1) →	
2013-09-16 12:42:47.255		→ ACK (100021) →		
2013-09-16 12:42:47.278				← Status:180 (1) ←
2013-09-16 12:42:47.285	← Status:180 (1) ←			
2013-09-16 12:42:47.287				← Status:200 (1) ←
2013-09-16 12:42:47.299		MEDIA FLOW MODIFY, ID=65563, DIRECTION=CALLED		
2013-09-16 12:42:47.301		MEDIA FLOW MODIFY, ID=65562, DIRECTION=CALLING		
2013-09-16 12:42:47.307	← Status:200 (1) ←			
2013-09-16 12:42:47.312	→ ACK (1) →			
2013-09-16 12:42:47.333			→ ACK (1) →	
2013-09-16 12:42:47.346		→ INVITE (100022) →		
2013-09-16 12:42:47.360				← Status:200 (100022) ←
2013-09-16 12:42:47.377		→ ACK (100022) →		
2013-09-16 12:43:19.323	→ BYE (2) →			
2013-09-16 12:43:19.334			→ BYE (2) →	
2013-09-16 12:43:19.356				← Status:200 (2) ←
2013-09-16 12:43:19.371		→ BYE (100023) →		
2013-09-16 12:43:19.395	← Status:200 (2) ←			
2013-09-16 12:43:19.409				← Status:200 (100023) ←
Details for INVITE (1)				
2013-09-16 12:42:47.101				
INVITE sip:service@192.168.33.100:5060 SIP/2.0				
Via: SIP/2.0/UDP 192.168.33.1:5060;branch=z9hG4bK-27311-1-0				
From: sipp <sip:sipp@192.168.33.1:5060>;tag=1				

## Hairpin Call Data

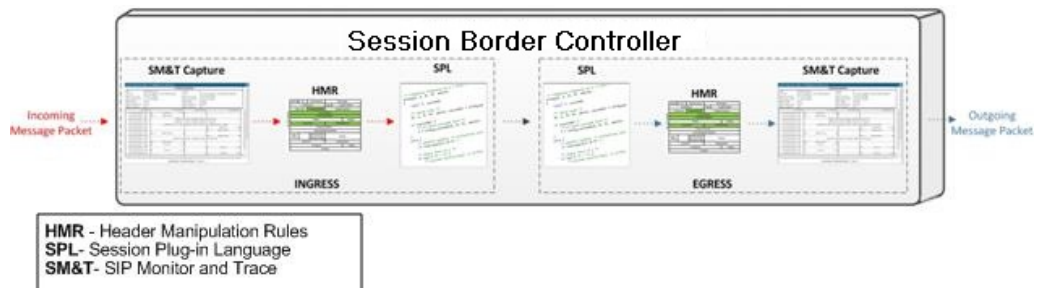
The following diagram shows SIP Monitor and Trace output for a hairpin call. Note the Media Flow Hairpin indication within the display.



## SIP Monitor & Trace Ingress Egress Messages

The SIP Monitor and Trace feature allows the Oracle Enterprise Session Border Controller (E-SBC) to monitor SIP sessions in your network. The system processes SIP Monitor and Trace data on incoming messages first and then sends the data out on outgoing messages. This allows the E-SBC to capture SIP Monitor and Trace data over the wire for display in the Web GUI.

The E-SBC captures a SIP message, applies the Header Manipulation Rules (HMR) configured on the E-SBC, and applies the Session Plug-in Language (SPL) to that message. When the message is sent out from the E-SBC, the E-SBC applies the SPL, applies the HMR, and sends out the captured SIP message.



## Display SIP Message Details

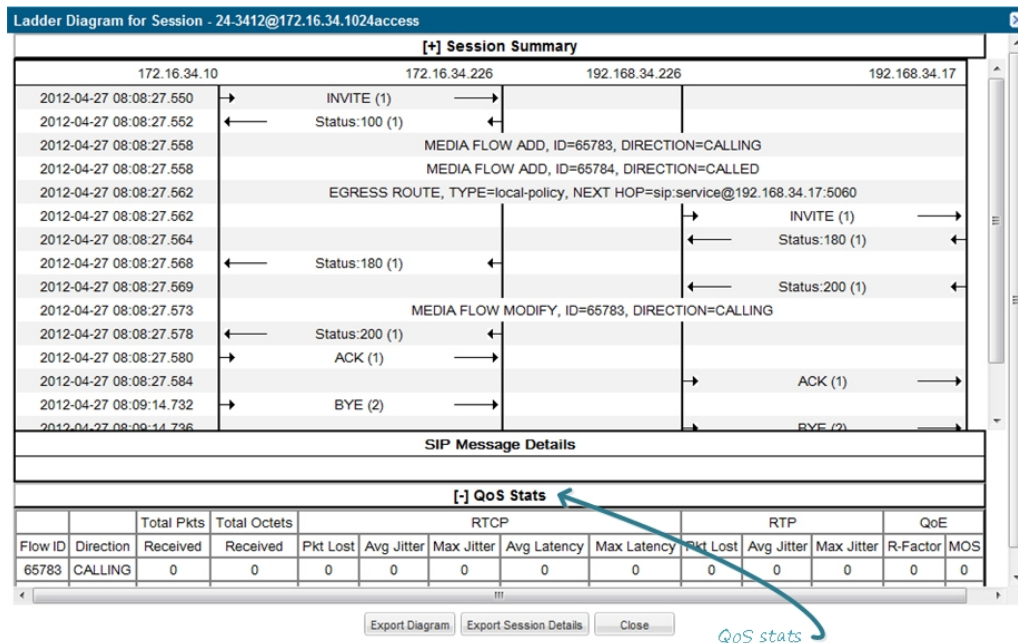
To display SIP Message Details:



1. On the Sessions Report page, click **Ladder diagram**, or select a record in the table and double-click on that record. The SIP Message Details window displays. This window displays the messages and status codes that occurred during the active call session or media event. You can use the information to troubleshoot calls and media events that failed or timed out when trying to connect.

## QoS Statistics

The Quality of Service (QoS) window displays information about the quality of the service used on the call session or media event when the call or event was active.



## Display QoS Statistics

To display QoS Statistics:

1. In the Ladder Diagram, click the [+] next to QoS Stats at the bottom of the Ladder Diagram window. The QoS window expands. This window displays the QoS statistics for the call session or media event in focus. The following table describes each field in the QoS Statistics window.

Heading	Description
Flow ID	ID number assigned to the call session or media event flow of data.
Direction	The direction of the call or media event flow. Valid values are: CALLING (egress direction) CALLED (ingress direction)
Total Pkts Received	Total number of data packets received on the interface during the active call session or media event.
Total Octets Received	Total number of octets received on the interface during the active call session or media event. An octet is a unit of digital information that consists of eight bits.

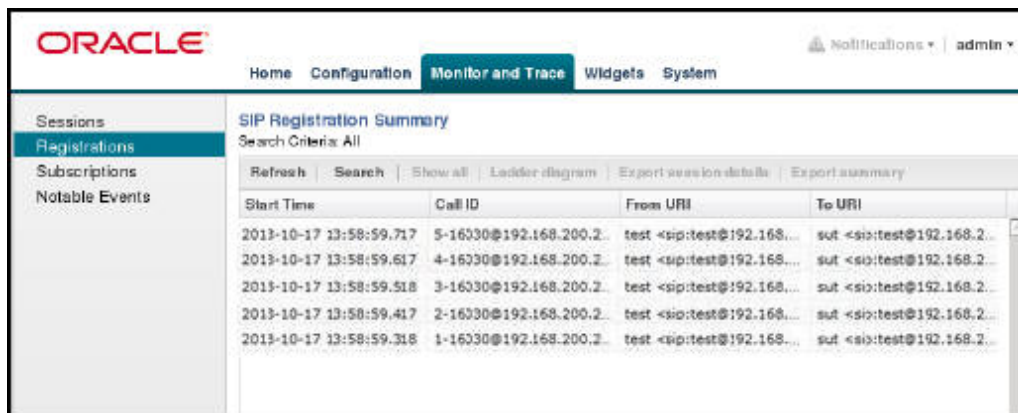
Heading	Description
RTCP	Real-time Transport Control Protocol - used to send control packets to participants in a call.
Pkts Lost	Number of RTCP data packets lost on the interface during the active call session or media event.
Avg Jitter	Average measure of the variability over time of the RTCP packet latency across a network. A network with constant latency has no variation (or jitter). Jitter is referred to as Packet Delay Variation (PDV). It is the difference in the one-way end-to-end delay values for packets of a flow. Jitter is measured in terms of a time deviation from the nominal packet interarrival times for successive packets.
Max Jitter	Maximum measure of the variability over time of the RTCP packet latency across a network. A network with constant latency has no variation (or jitter).
Avg Latency	Average observed one-way signaling latency during the active window period. This is the average amount of time the signaling travels in one direction.
Max Latency	Maximum observed one-way signaling latency during the sliding window period. This is the maximum amount of time the signaling travels in one direction.
RTP	Real-Time Transport Protocol - a standard packet format for delivering audio and video over the internet.
Pkts Lost	Number of RTP data packets lost on the interface during the active call session or media event.
Avg Jitter	Average measure of the variability over time of the RTP packet latency across a network. A network with constant latency has no variation (or jitter). Jitter is referred to as Packet Delay Variation (PDV). It is the difference in the one-way end-to-end delay values for packets of a flow. Jitter is measured in terms of a time deviation from the nominal packet interarrival times for successive packets.
Max Jitter	Maximum measure of the variability over time of the RTP packet latency across a network. A network with constant latency has no variation (or jitter).
QoE	Quality of Experience - measurement used to determine how well the network is satisfying the end user's requirements.
R-Factor	Average Quality of Service (QoS) factor observed during the active window period. Quality of service shapes traffic to provide different priority and level of performance to different data flows. R-factors are metrics in VoIP, that use a formula to take into account both user perceptions and the cumulative effect of equipment impairments to arrive at a numeric expression of voice quality. This statistic defines the call or transmission quality expressed as an R factor.
MOS	Mean Opinion Score (MOS) score. MOS is a measure of voice quality. MOS gives a numerical indication of the perceived quality of the media received after being transmitted and eventually compressed using Codecs.

- Click [-] to close the QoS Stats window.

## Registrations Report

The Registrations Report is a summary of all logged SIP registrations sessions on the Oracle Enterprise Session Border Controller.

The columns that display on the Registration Report page are dependent on the columns you selected in the "Customizing the Page Display" procedure.



The following table describes the columns on this page.

Heading	Description
Start Time	Timestamp of the first SIP message in the call session.
Call ID	Identification of the call source. Includes the phone number and source IP address.
To URI	URI formatted string that identifies the call destination information.
From URI	URI formatted string that identifies the call source information.
Local Expires	The current setting for the expiration of a registration request sent from the Integrated Media Gateway (IMG) to a Remote SIP User Agent. The default is 3600 sec.
Remote Expires	The current setting for the expiration of a registration request sent from the Remote SIP User Agent to the Integrated Media Gateway (IMG). The default is 3600 sec.
Ingress Realm	Incoming realm name.
Egress Realm	Outgoing realm name.
Notable Event	Indicates if a notable event has occurred on the call session. Valid value is: local rejection - Sessions locally rejected at the E-SBC for any reason (for example, Session Agent (SA) unavailable, no route found, SIP signalling error, etc.); Session dialogue, capture media information and termination signalling; Any event flagged as a local rejection interesting event
Session ID	Identification assigned to the call session.
Ingress Src Addr	Source IP address of the incoming call or media event.
Egress Dest Addr	Destination IP address of the outgoing call or media event.
Request URI	Uniform Resource Identifier (URI) formatted string that identifies a resource via a protocol, name, location, and any other applicable characteristic, and is sent by the E-SBC in REQUEST headers.

The following table describes the buttons on this page.

Button	Description
Search	Allows you to specify parameters for performing a search for specific session summary records within the current report.

Search

Button	Description
Show all	Displays all of the session summary records in the Session Report.
Ladder Diagram	Displays a Ladder Diagram of a specific record in the table. The Ladder Diagram displays detailed information about a call session or media event.
Export Session Details	Exports the SIP messages and media events associated with the selected session, to a file in text format on the local machine.
Export Summary	Exports all logged session summary records to a file in text format on the local machine.

## Display a Registrations Report

### Procedure

1. From the Web GUI, click **Monitor and Trace > Registrations**.
2. Use the buttons on the top of the page to view information about the records in this report.

## Subscriptions Report

The Subscriptions Report is a summary of all logged SIP subscription sessions on the Oracle Enterprise Session Border Controller (E-SBC).

The columns that display on the Subscription Report page are dependent on the columns you selected in the procedure, Customizing the Page Display (11).

Start Time	Call ID	From URI	To URI	Event
2013-10-17 13:58:59.717	5-16030@192.168.200.2	test <sip:test@192.168...	sut <sip:test@192.168.2...	
2013-10-17 13:58:59.617	4-16030@192.168.200.2	test <sip:test@192.168...	sut <sip:test@192.168.2...	
2013-10-17 13:58:59.518	3-16030@192.168.200.2	test <sip:test@192.168...	sut <sip:test@192.168.2...	
2013-10-17 13:58:59.417	2-16030@192.168.200.2	test <sip:test@192.168...	sut <sip:test@192.168.2...	
2013-10-17 13:58:59.318	1-16030@192.168.200.2	test <sip:test@192.168...	sut <sip:test@192.168.2...	

The following table describes the columns on this page.

Heading	Description
Start Time	Timestamp of the first SIP message in the call session.
Call ID	Identification of the call source. Includes the phone number and source IP address.
From URI	URI formatted string that identifies the call source information.
To URI	URI formatted string that identifies the call destination information.

Heading	Description
Events	<p>Specific subscribe event package that was sent from an endpoint to the destination endpoint. Applicable event packages can be:</p> <p>conference - Event package that allows users to subscribe to a conference Uniform Resource Identifier (URI).</p> <p>consent-pending additions - Event package used by SIP relays to inform user agents about the consent-related status of the entries to be added to a resource list.</p> <p>dialog - Event package that allows users to subscribe to another user, and receive notifications about the changes in the state of the INVITE-initiated dialogs in which the user is involved.</p> <p>message-summary - Event package that carries message-waiting status and message summaries from a messaging system to an interested User Agent (UA).</p> <p>presence - Event package that conveys the ability and willingness of a user to communicate across a set of devices. A presence protocol is a protocol for providing a presence service over the Internet or any IP network.</p> <p>reg - Event package that provides a way to monitor the status of *all* the registrations for a particular Address of Record (AoR).</p> <p>refer - Event package that provides a mechanism to allow the party sending the REFER to be notified of the outcome of a referenced request.</p> <p>winfo - Event package for watcher information. It tracks the state of subscriptions to a resource in another package.</p> <p>vq-rtcp - Event package that collects and reports the metrics that measure quality for RTP sessions.</p>
Local Expires	The current setting for the expiration of a registration request sent from the Integrated Media Gateway (IMG) to a Remote SIP User Agent. The default is 3600 sec.
Remote Expires	The current setting for the expiration of a registration request sent from the Remote SIP User Agent to the Integrated Media Gateway (IMG). The default is 3600 sec.
Ingress Realm	Incoming realm name.
Egress Realm	Outgoing realm name.
Notable Event	Indicates if a notable event has occurred on the call session. Valid value is: local rejection - Sessions locally rejected at the E-SBC for any reason (for example, Session Agent (SA) unavailable, no route found, SIP signalling error, etc.); Session dialogue, capture media information and termination signalling; Any event flagged as a local rejection interesting event
Session ID	Identification assigned to the call session.
Ingress Src Addr	Source IP address of the incoming call or media event.
Egress Dest Addr	Destination IP address of the outgoing call or media event.
Request URI	Uniform Resource Identifier (URI) formatted string that identifies a resource via a protocol, name, location, and any other applicable characteristic, and is sent by the E-SBC in REQUEST headers.

The following table describes the buttons on this page.

Button	Description
<div style="border: 1px solid gray; padding: 5px; display: flex; justify-content: space-around;"> <span>Search</span>   <span>Show all</span>   <span>Ladder Diagram</span>   <span>Export Session Details</span>   <span>Export Summary</span> </div>	

Button	Description
Search	Allows you to specify parameters for performing a search for specific session summary records within the current report.
Show all	Displays all of the session summary records in the Session Report.
Ladder Diagram	Displays a Ladder Diagram of a specific record in the table. The Ladder Diagram displays detailed information about a call session or media event.
Export Session Details	Exports the SIP messages and media events associated with the selected session, to a file in text format on the local machine.
Export Summary	Exports all logged session summary records to a file in text format on the local machine.

## Display a Subscriptions Report

### Procedure

1. From the Web GUI, click **Monitor and Trace > Subscriptions**.
2. Use the buttons on the top of the page to view information about the records in this report.

## Notable Events Report

The Notable Events Report contains all logged sessions that have a notable event associated with the session on the Oracle Enterprise Session Border Controller (E-SBC).

The columns that display on the Notable Events Report page are dependent on the columns you selected in the procedure, Customizing the Page Display.

Start Time	State	Call ID	Request URI	From URI
2013-10-17 13:56:41.083	FAILED-408	5-15779@192.168.200.2	sip:service@192.168.20...	9788482942
2013-10-17 13:56:40.984	FAILED-408	4-15779@192.168.200.2	sip:service@192.168.20...	9788482942
2013-10-17 13:56:40.884	FAILED-408	3-15779@192.168.200.2	sip:service@192.168.20...	9788482942
2013-10-17 13:56:40.784	FAILED-408	2-15779@192.168.200.2	sip:service@192.168.20...	9788482942
2013-10-17 13:56:40.683	FAILED-408	1-15779@192.168.200.2	sip:service@192.168.20...	9788482942
2013-10-17 13:56:21.338	TERMINATED-	5-15665@192.168.200.2	sip:service@192.168.20...	9788482942
2013-10-17 13:56:21.238	TERMINATED-	4-15665@192.168.200.2	sip:service@192.168.20...	9788482942

The following table describes the columns on this page.

Heading	Description
Start Time	Timestamp of the first SIP message in the call session.

Heading	Description
State	Status of the call or media event session. Valid values are: INITIAL Session for which an INVITE or SUBSCRIBE was forwarded. EARLY Session received the first provisional response (1xx other than 100). ESTABLISHED Session for which a success (2xx) response was received. TERMINATED Session that has ended by receiving or sending a BYE for an “Established” session or forwarding an error response for an “Initial” or Early session. The session remains in the terminated state until all the resources for the session are freed up. FAILED Session that has failed due to a 4xx or 5xx error code.
Call ID	Identification of the call source. Includes the phone number and source IP address.
Request URI	Uniform Resource Identifier (URI) formatted string that identifies a resource via a protocol, name, location, and any other applicable characteristic, and is sent by the E-SBC in REQUEST headers.
To URI	URI formatted string that identifies the call destination information.
From URI	URI formatted string that identifies the call source information.
Notable Event	Specific subscribe event package that was sent from an endpoint to the destination endpoint. Applicable event packages can be: conference - Event package that allows users to subscribe to a conference Uniform Resource Identifier (URI). consent-pending additions - Event package used by SIP relays to inform user agents about the consent-related status of the entries to be added to a resource list. dialog - Event package that allows users to subscribe to another user, and receive notifications about the changes in the state of the INVITE-initiated dialogs in which the user is involved. message-summary - Event package that carries message-waiting status and message summaries from a messaging system to an interested User Agent (UA). presence - Event package that conveys the ability and willingness of a user to communicate across a set of devices. A presence protocol is a protocol for providing a presence service over the Internet or any IP network. reg - Event package that provides a way to monitor the status of *all* the registrations for a particular Address of Record (AoR). refer - Event package that provides a mechanism to allow the party sending the REFER to be notified of the outcome of a referenced request. winfo - Event package for watcher information. It tracks the state of subscriptions to a resource in another package. vq-rtcp - Event package that collects and reports the metrics that measure quality for RTP sessions.
Ingress Realm	Incoming realm name.
Egress Realm	Outgoing realm name.
Notable Event	Indicates if a notable event has occurred on the call session. Valid values are: short session - Sessions that don’t meet a minimum configurable duration threshold; Session dialogue, captured media information and termination signalling; Any event flagged as a short session interesting event. local rejection - Sessions locally rejected at the E-SBC for any reason (for example, Session Agent (SA) unavailable, no route found, SIP signalling error, etc.); Session dialogue, capture media information and termination signalling; Any event flagged as a local rejection interesting event.
Session ID	Identification assigned to the call session.
Ingress Src Addr	Source IP address of the incoming call or media event.
Egress Dest Addr	Destination IP address of the outgoing call or media event.



The following table describes the buttons on this page.

Button	Description
	
Search	Allows you to specify parameters for performing a search for specific session summary records within the current report.
Show all	Displays all of the session summary records in the Session Report.
Ladder Diagram	Displays a Ladder Diagram of a specific record in the table. The Ladder Diagram displays detailed information about a call session or media event.
Export Session Details	Exports the SIP messages and media events associated with the selected session, to a file in text format on the local machine.
Export Summary	Exports all logged session summary records to a file in text format on the local machine.

## Display a Notable Events Report

### Procedure

1. From the Web GUI, click **Monitor and Trace > Notable Events**.
2. Use the buttons on the top of the page to view information about the records in this report.

## Search for a Record

The **Search** button at the top of the report page allows you to find a specific record within a Monitor and Trace report. It also allows you to specify criteria on which to perform the search.

After defining a search criteria in the Search Filter dialog box, clicking Search automatically populates the report page with the records that match the specified criteria specified. The search performs the filtering process of criteria dependent on the report page from which you are running the search.

For example, performing a search from the Sessions report page displays only the reports pertaining to call sessions. If you perform a search on the Registration report page, only the reports pertaining to call registrations displays on the report page. The search string containing the criteria on which you performed the search, displays in the top left corner of the page.

### Note:

A SIP Monitor and Trace global search can find items in the SIP headers, as well. The system saves the search criteria until you click **Reset** in the dialog box, or until you log out of the HTTP session.

## Perform a Search

To perform a search:



You can specify a value for any or all of the fields in the Search box. The search process searches for records with all of the values you specify and displays only the records with these values. If you perform a “Global Search”, AND specify values in other fields, the search process searches the other specified fields first and then filters on the “Global Search” field.

If you specify a “\*” in a search string, the search is performed on that exact string. For example, if you search for “123\*45”, the search shows results for all strings containing “123\*45”.

You can use quotes (“ ”) to specify a search. For example, you can enter Smith and the search finds all of the records that match Smith, such as: John  
`Smithfield<sip:sipp@192.168.1.70:5070>;tag=12260SIPpTag001.`

If you enter a space before or after a quotation mark, (for example, “Smith “), the search returns no data.

1. In any reports page, click **Search**.
2. In the Global Search field, specify a string to search all parameters in all records. Valid values are alpha-numeric characters.

 **Note:**

The Global Search option searches all parameters in all the session records stored in memory. All values you specify in other fields are searched before the value specified in the Global Search field is used.

3. In the From URI field, enter the URI formatted string of the call source information you are searching. Valid values are alpha-numeric characters. For example,  
`sipp<sip:sipp@172.16.34.10:5060;tag=24.`
4. In the Requested URI field, enter the URI formatted string that contains a protocol, name, location, or any other applicable characteristic, that is sent by the Net-Net ECB in the REQUEST header. Valid values are alpha-numeric characters. For example,  
`sip:service@172.16.34.226:5060.`
5. In the To URI field, enter URI formatted string of the call destination information you are searching. Valid values are alpha-numeric characters. For example,  
`sut<sip:service@172.16.34.226:5060;tag=99.`
6. In the Start Date/Time (HH mm ss) field, enter a starting date to search on in the first text box in the format YYYY-MM-DD (where Y =year, M=month, and D=day). or Click on the calendar icon in this field to display a calendar from which you can select a date. Navigate the calendar to find the date you want and click on it to enter it into this field, or click **<Today>** to enter today’s date. For example, 2012-04-15 would search for all records starting on April 15, 2012. Valid values are numeric characters only. Enter a start time to search on in the last three text boxes in the format HH mm ss (where H=hour, m=minutes, and s=seconds). For example, 01 30 45 would search for all records starting at 1:30 and 45 seconds. Valid value are numeric characters only.

Start Date/Time(HH mm ss)

End Date/Time(HH mm ss)

7. In the End Date/Time (HH mm ss) field, repeat the process of entering a date and time as provided in Step 7.
8. To search on additional parameters, click on the Additional Identifiers down arrow to expand the dialog box.

## Specify Additional Identifiers

To specify additional identifiers:

1. In the Session Id field, enter the ID of the call session you want to search. Valid values are alpha-numeric characters. For example, 22-3412@172.16.34.1.
2. In the In Call ID field, enter the ID of the incoming call (phone number and source IP address). Valid values are alpha-numeric characters. For example, 25-3412@172.16.34.10.
3. In the Out Call ID field, enter the ID of the outgoing call (phone number and IP address). Valid values are alpha-numeric characters. For example, 14-3412@172.14.54.6.
4. In the State (with result code) field, enter the status of the call session with the result code for which you want to search. Valid values are (case-sensitive):
  - INITIAL-<result code>
  - EARLY-<result code>
  - ESTABLISHED-<result code>
  - TERMINATED-<result code>
  - FAILED-<result code>

Result codes can range from 1xx to 5xx. For example, terminated-200, or failed-400.
5. In the Notable Event field, select the notable event for which you want to search. Valid values are:
  - any-event - search displays any notable event that was stored in memory.
  - short-session - search displays only records that indicate a short-session duration has occurred.
  - local-rejection - search displays only records that indicate a local-rejection has occurred.
6. To search on additional parameters, click on the Additional Search Options down arrow to expand the dialog box.

## Specify Additional Search Options

To specify additional search options:

1. In the “**In Realm**” field, enter the name of the realm for which the incoming call belongs. Valid values are alpha-numeric characters. For example, access.
2. In the “**Out Realm**” field, enter the name of the realm for which the outgoing call belongs. Valid values are alpha-numeric characters. For example, backbone.
3. In the “**In SA**” field, enter the name of the session agent (SA) on the incoming call session. Valid values are alpha-numeric characters. For example, SA1.
4. In the “**Out SA**” field, enter the name of the session agent (SA) on the outgoing call session. Valid values are alpha-numeric characters. For example, SA2.
5. In the “**In Source Addr**” field, enter the source IP address of the SA that accepted the incoming call session. IP Address must be entered in dotted decimal format (0.0.0.0). For example, 172.45.6.7.
6. In the “**Out Dest Addr**” field, enter the destination IP address of the SA that accepted the outgoing call session. IP Address must be entered in dotted decimal format (0.0.0.0). For example, 172.64.56.7.
7. In the In Network Interface field, enter the incoming core network interface that connects the Net-Net ECB to your network. IP Address must be entered in dotted decimal format (0.0.0.0). For example, 192.45.6.7.
8. In the Out Network Interface field, enter the outgoing network interface that connects your Net-Net ECB to the outside network. IP Address must be entered in dotted decimal format (0.0.0.0). For example, 192.45.6.8.
9. Click <Search> to perform the search with the values you specified. A list of the records that the search process filtered, display in the window. The GUI saves the search specifications until you click <Reset> in the search dialog box, OR until you log out of the GUI.

## Exporting Information to a Text File

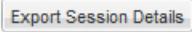
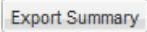

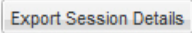
Monitor and Trace allows you to export information to a text file from the Sessions, Registrations, Subscriptions and Notable Events Reports, as well as from a specific ladder diagram, or from a page containing the results of a search. The system exports data to a file that you can open and view as required.

You can export any of the following:

- All information from each report
- Information from a specific record only
- Information from a search result
- Information from a Ladder Diagram

The following table identifies the buttons to use to export specific information from Monitor and Trace. All the export buttons in the GUI export to text files.

Button	Description
From the Sessions, Registrations, Subscriptions, and Notable Events Reports:	

Button	Description
	Exports the SIP messages and media events associated with the selected session, to a file in text format on the local machine.
	Exports all logged session summary records to a file in text format on the local machine. Note: This button exports ALL call session summary records or the records that matched a search criteria to the file.
From the Ladder Diagram:	
	Exports all of the information in the Ladder Diagram (Session Summary, SIP Message Details, and QoS statistics), to an HTML file format on the local machine.
	Exports detailed information about the SIP messages and media events in the Ladder Diagram associated with the selected session, to a file in text format on the local machine.

## Export Report Information to a Text File

To export information from a Monitor and Trac report to a text file:

### Note:

The GUI exports Ladder Diagrams as HTML files.

1. From the Web GUI, click the **Monitor and Trace** tab.
2. On the Monitor and Trace page, select a report type. For example, Subscriptions.
3. On the report Summary page, select a report from the list, and do one of the following:
  - Click **Export session details**.
  - Click **Export summary**.
4. In the SessionDetails.txt or SummaryExport.txt dialog, do one of the following:
  - Click **Open with**, and select the application with which to open the resulting text file.
  - Click **Save file** to save the text file to your local PC.
5. Click **OK** to export the report information.

# 5

## Widgets Tab

The Widgets tab contains a list of all available widgets that you can use to view system data and statistics.

When you click the name of a Widget in either the navigation pane or the All Widgets list, the system displays the widget in full-screen mode. If you view a certain widget frequently, you might want to add it to the Favorite Widgets list on the Widgets page or add it to the Dashboard on the Home page. You can perform both tasks from the widget with the icons displayed in the upper right corner of the widget.

### Types of Widgets

The following tables describe the types of widgets that you can add to the Dashboard to display Command, Session Initialization Protocol (SIP), and System, statistics.

<b>Command Widget</b>	<b>Description</b>
Show Configuration	Displays either the running configuration or the editing configuration for the selected configuration. Note: Not available on the Home tab. See the Widgets tab.

<b>SIP Widget</b>	<b>Description</b>
Message - Requests per second	Displays the number of SIP requests per second, during a period of time.
Message - Response	Displays the number of SIP responses per second, during a period of time.
Session - Answer Seizure Ratio (ASR)	Displays the percentage of answered calls with respect to the number of calls attempted during a period of time.
Session- Duration	Displays the total number of sessions and their durations.
Session - Established	Displays the number of sessions established during a period of time.

<b>System Widget</b>	<b>Description</b>
Alarms	Displays existing alarms, which you can clear individually or collectively from the widget.

System Widget	Description
Configuration Inventory	<p>Displays a list of changes made to configuration elements. The display shows the Running Count and counts for the following types of Changes Not Activated.</p> <ul style="list-style-type: none"> <li>• Total</li> <li>• Added</li> <li>• Modified</li> <li>• Deleted</li> </ul> <p>Use the filter to change the display from Total count to the difference between the Running Count and the Changes Not Activated Count.</p>
Configuration Version	Displays the version number that is configured and the version number that is running.
CPU Usage	Displays 5 to 10 tasks with the highest percent of CPU usage during a period of time.
Current Disk	Displays the disk usage for the code directory on the Oracle Enterprise Session Border Controller. The system uploads data from the Web GUI to the code directory.
Current Memory	Displays the current percentage of free memory.
Historical Memory	Displays the number of kilobytes of free and allocated memory over a period of time.
System Health	<ul style="list-style-type: none"> <li>• Displays the current health score and state of the system.</li> <li>• Displays the Synchronization health button. Use to display the Synchronization health table, which shows the relative ability of the system to perform as the primary in an HA pair.</li> <li>• Displays the Switchover log button, when the device is deployed in an HA configuration. Use to display information about switchover events.</li> </ul>
User Management	<ul style="list-style-type: none"> <li>• Displays a table listing the users who are logged on to the system.</li> <li>• Displays the user's remote IP address, duration, type, state, and user name.</li> <li>• Displays the Disconnect button. A privileged administrator can disconnect a logged on user.</li> </ul>

## Add a Widget to Favorites

If you view a widget often, you may want to add it to the Favorites list on the Widgets tab.

When you select a widget to add to Favorites, the system displays an icon of a push-pin on the tool bar at the top of the widget. Use the push-pin icon to add the widget to Favorites.

### Procedure

1. From the Web GUI Home page, click the Widgets tab.
2. From the All Widgets list, click the widget that you want to add to Favorites.

The system displays the widget.

3. From the displayed widget, click the "Add the view to the favorites" icon. (Top, right. Shaped like a push-pin.)  
The system displays a success message.
4. Click **OK**.

# 6

## System Tab

The System tab on the Web GUI provides the following ways to manage files on the system:

- File Management. Refresh. Upload, Download, Backup, Restore, and Delete files.
- Force HA Switchover. Force the system to switch from the primary to the secondary.
- Reboot. Reboot the system.
- Support information. Generate a file that displays troubleshooting information.
- Upgrade software. Verify system health, upload software, and reboot the system.

### Note:

You can activate an LRT file, fraud protection file, or an SPL file dynamically upon an upload, if required. You can also immediately apply a backup configuration file during the upload process.

## File Management

You can manage system files from the Web GUI on the File Management page.

The following table describes the files that you can manage under **File Management** on the Oracle Enterprise Session Border Controller (E-SBC).

File Type	Format	Description
Backup configuration	.gz	File that contains a backup of the E-SBC software configuration. You can apply this file to restore a previous configuration if required.
Local route table (LRT)	.xml, .gz	Local routing table (LRT) file that you can apply to the E-SBC. The LRT is an in-memory table that contains IP addresses that the local router recognizes. It calculates the destinations of messages it is responsible for forwarding.
Fraud protection table	.gz, .gzip, .xml	Lists fraud protection files that you can upload, download, delete, or open to modify.



File Type	Format	Description
Log	Text	Log files that contain information about the various aspects of the E-SBC. For example, information logged about the ACLI, SIP, or H323.  Note: Only the Download and Delete functions are applicable to log files on the E-SBC.
Playback media	Any media format valid in an RTP audio stream	Call progress playback files. The E-SBC can use these files in generated media streams if required.  Note: The media files are raw binary files that contain data for the codec that a user wants to have played in the media stream. The E-SBC plays the data on the first audio flow in the Session Description Protocol (SDP).
Software Image	.gz, .bz	These files are bootable images.
SPL Plug-in	.lua	Session Plug-in Language (SPL) file that you can apply to the E-SBC to incorporate additional functionality. The SPL file contains a programming language that is capable of performing various tasks by utilizing APIs and callbacks in the E-SBC.

The following table describes the file management buttons.

Button	Description
Refresh	Updates the screen to display the latest data.
Upload	Uploads a file type from your server or PC to the E-SBC. The LRT, SPL, and backup configuration upload process provide the option of dynamically applying these files to the E-SBC.
Download	Downloads the file type from the E-SBC to your local server or PC (typically to the download directory on your system). Note: Download All applies only to log files.
Backup	File that contains a backup of the device software configuration. You can apply this file to restore a previous configuration.
Restore (Applicable to the “Backup configuration” file type only.)	Restores and applies a Backup configuration file to the E-SBC.
Delete	Deletes the file type from the E-SBC. Note: Delete All applies only to log files.

## Manage Files

You can manage system files from the Web GUI on the File Management page.

 **Note:**

You can activate an LRT file or an SPL file dynamically during an upload. You can also immediately apply a backup configuration file during the upload process.

### Procedure

1. From the Web GUI, click **System**.
2. On the System page, in the navigation pane, click **File management**.
3. On the File management page, select a file to view from the File type drop-down list.  
The system displays the file.
4. Use the controls on the tool bar to manage the file.

## Group By Field

To customize the display of the File Management page on the System tab, you can group the elements by column head.

### Procedure

1. From the Web GUI, click **System**.
2. On the System page, under File management, select a file type from the drop-down list to group by field.
3. On the File Management page, click the column title by which you want to group the items.  
The system displays an arrow control to the right of the column title.
4. Click the arrow control, and click **Group By This Field** on the menu.  
The system displays the data by the selected group.

## Upload a File

Procedure and conditions for uploading a file to the Oracle Enterprise Session Border Controller (E-SBC).

You can upload the following file types from your local server or PC to the E-SBC:

- Backup configuration
- Local route table (LRT)
- Fraud protection table
- Playback media
- Software image
- SPL Plug-in (SPL)

**Note:**

You cannot upload log files.

The file extension must be applicable to the file type you select. For example, an SPL Plug-in file requires the .lua extension. The following table shows the file extensions required for each file type, and the directory on the E-SBC where the system stores the uploaded file.

File Type	File Format	Directory
Backup Configuration	.gz	/code/bkups
Local route table (LRT)	.xml, .gz	/code/gzConfig
Fraud protection table	.gz, .gzip, .xml	/code/fpe
Playback media	Any media format valid in an RTP audio stream	/code/media
Software image	.bz	/code/images
SPL Plug-on (SPL)	.lua	/code/spl

You can dynamically activate the Local route table and SPL Plug-in during the upload process.

You can immediately restore a backup configuration file after an upload is complete.

**Procedure**

1. From the Web GUI, click **System > File management**.
2. On the File management page, from the File type drop down list, select the type of file you want to upload.
3. In the Name column, select the file you want to upload.
4. Click **Upload**.
5. In the Upload file dialog, do the following:
  - a. Click **Browse**.
  - b. Select the file that you want to upload.
  - c. Optional. For the Backup configuration file, select Restore the configuration after upload to apply a previous backed up configuration file immediately to the after the upload is complete.
  - d. Optional. For the Local route table file type, select Activate the LRT file after upload to apply the LRT upon upload.
  - e. Optional. For a Fraud protection file, select Activate the file after upload to apply the file upon upload.
  - f. Optional. For the SPL Plug-in file type, select Activate the SPL file after upload to apply the SPL file upon upload.
  - g. Click **Upload**.

## Download a File

Procedure and conditions for downloading from the Oracle Enterprise Session Border Controller (E-SBC).

You can download any of the following file types from your local server or PC to the E-SBC:

- Backup configuration
- Local route table (LRT)
- Fraud protection table
- Log
- Playback media
- Software image
- SPL Plug-in (SPL)

### Procedure

1. From the Web GUI, click **System > File management**.
2. On the File Management page, select the type of file you want to download from the File type drop down list.
3. In the Name column, select the file you want to download.

#### Note:

For Log file types, you can select multiple log files to download, or place a checkmark in the box to the left of the Name column heading to select all log files to download. When downloading multiple log files, the File Management GUI compresses the files into one .tar file and downloads that file to your local server or PC.

4. Click **Download**.
5. Do one of the following:
  - Click **Open with** and select the application to open the file.
  - Click **Save file** to save the file to your local server or PC.
6. Click **OK**.

The system downloads the file to the folder on your local server or PC where your Browser sends all downloads (typically your “Download” folder) or opens (decompresses) the file type on your local server or PC (typically in the “Download” folder).

## Delete a File

Procedure and conditions for deleting a file from the Oracle Enterprise Session Border Controller (E-SBC).

You can delete any of the following file types from your local server, PC, and E-SBC:

- Backup configuration Software image

- Local route table (LRT)
- Fraud protection table
- Log
- Playback media
- Software image
- SPL Plug-in (SPL)

 **Note:**

You can select a single or multiple files to delete.

**Procedure**

1. On the System tab, in the **File type** drop down list, select the type of file that you want to delete.
2. In the Name column, select one or more files you want to delete.

 **Note:**

For Log file types, place a checkmark in the box to the left of the Name column heading to select all log files to delete.

3. Click **Delete**. The system displays following message.  
Are you sure you want to delete the file?
4. Click **Yes**.

## Back up a File

You can backup a configuration file from the Oracle Enterprise Session Border Controller (E-SBC) to your local server or PC. This allows you to save configurations that you can restore to your E-SBC at a later time.

**Procedure**

1. From the Web GUI, click **System**.
2. In the Select the file type field, select Backup configuration.
3. Select one or more configuration files to backup to your server or PC.
4. Click **Backup**.
5. Click **OK** to backup the configuration.

The system downloads the file to your server or PC, typically into the download directory.

## Restore a File

You can restore a backed up configuration file to the Oracle Enterprise Session Border Controller (E-SBC).

When you select a file to restore, and click Restore, the system restores the selected backup configuration file to the E-SBC.

### Procedure

1. In the **Select the file type** field, select **Backup configuration**.
2. Select a backup file to restore to the E-SBC.



#### Note:

**Restore** activates only when you select a backup file.

3. Click **Restore**.
4. Click **Yes**.

The system downloads the backup file to the E-SBC. The E-SBC reboots and restores the configuration from the backup file.

## Force an HA Switch Over

You can manually initiate a High Availability (HA) switch over from the Web GUI.

### Before You Begin

- The Oracle Enterprise Session Border Controller (E-SBC) from which you initiate the switchover must be in one of the following states: active, standby, or becoming standby.
- A manual switch over to the active state is allowed on an E-SBC only in the standby or becoming standby state when it has achieved full media, signaling, and configuration synchronization.
- A manual switch over to the active state is allowed on an E-SBC only in the standby or becoming standby state when it has a health score above the value that you configured for the threshold.

Performing this procedure forces the E-SBCs in an HA pair to trade roles. The active system becomes the standby, and the standby system becomes active.

### Procedure

1. From the Web GUI, click the **System** tab.
2. On the System page, in the navigation pane, click **Force HA switchover**.
3. On the Force HA switch over page, click **Switch to standby**.

The system performs the role change.

## System Reboot

You can manually reboot the Oracle Enterprise Session Border Controller (E-SBC) from the Web GUI. Note that when you reboot the system from the Web GUI, the Web GUI is unavailable until the reboot is complete. If you have a High Availability (HA) deployment, connectivity to the secondary E-SBC is lost until the reboot is complete.

When the reboot is complete, the primary and secondary systems both display the logon screen. You must manually log on to each system.

When you perform a reboot from the Web GUI	The system behaves
and no boot is in process and the system is not failing over to the secondary system in an HA environment	The GUI session closes and the system displays the Logon screen. You cannot log on to the Web GUI until the reboot is complete on the E-SBC.
and a reboot is already in progress	The system displays a message indicating that a reboot cannot occur. The first reboot must complete before another reboot is initiated.
and the primary system is currently failing over to the secondary system in an HA environment	The system displays a message indicating that a reboot cannot occur. The HA switch over is underway. The secondary E-SBC is updating and getting its configuration from the primary E-SBC.

## Obtain Support Information

You can manually generate a predefined file by way of the Web GUI that contains troubleshooting information. You can save the file and send it to Oracle Customer Support.

### Procedure

1. From the Web GUI, click the **System** tab.
2. On the System page, in the navigation pane, click **Support Information**.
3. On the Support information page, click **Support Information**.  
The system generates the file.
4. Save the file.

## Upgrade Software - Web GUI System Tab

You can upgrade the system software from the System tab on the Web GUI. The system requires a reboot after the upgrade.

1. From the Web GUI, click the **System** tab.
2. Click **Upgrade Software**.
3. Click **Verification**.
4. Verify that system health, synchronization health, current configuration version, and disk usage are appropriate and adequate for the upgrade.
5. From the drop-down list, select **Upload method**, and select one of the following methods.
  - **Local**. Use to select a file from your system for transfer.

- Flash. Use to select a file already on the device.
- Network. Use to specify parameters for network boot by way of file transfer.

The system displays the Upgrade Software dialog with the fields required for your upgrade.

6. Complete the required fields.
  - Software file to upload. (Local) Use `Browse` to locate the file on your local system.
  - Software file. (Flash) The location and name of the file on the device.
  - Boot file. (Network) The complete name of the boot file.
  - Host IP. (Network) The IP address of the FTP server.
  - FTP username. (Network) The user name to log onto the FTP server.
  - FTP password. (Network) The password to log onto the FTP server.
7. Optional. Select `Reboot after upload`.
8. Click `Complete`.
  - If you did not select `Reboot after upload`, the system displays a message stating that a reboot is required for the changes to take effect.
  - If you selected `Reboot after upload`, the system displays a message stating that it is about to reboot.
9. Click `OK`.

If you selected `Reboot after upload`, the system reboots.



# 7

## Format of Exported Text Files

### Introduction

This Appendix provides a sample and format of each type of exported file from the Web-based GUI. Sample information in these files are provided as a reference for your convenience.

Exported file examples include:

- Session Summary exported file (text format)
- Session Details exported file (text format)
- Ladder Diagram exported file (HTML format)



#### Note:

Oracle recommends you open an exported text file using an application that provides advanced text formatting to make it easier to read.

### Exporting Files

The Web-based GUI allows you to export Monitor and Trace information to a text file from the Sessions, Registrations, Subscriptions and Notable Events Reports, as well as from a specific ladder diagram, or from a page containing the results of a search. The data exports to a file that you can open and view as required.

You can export any of the following to a file:

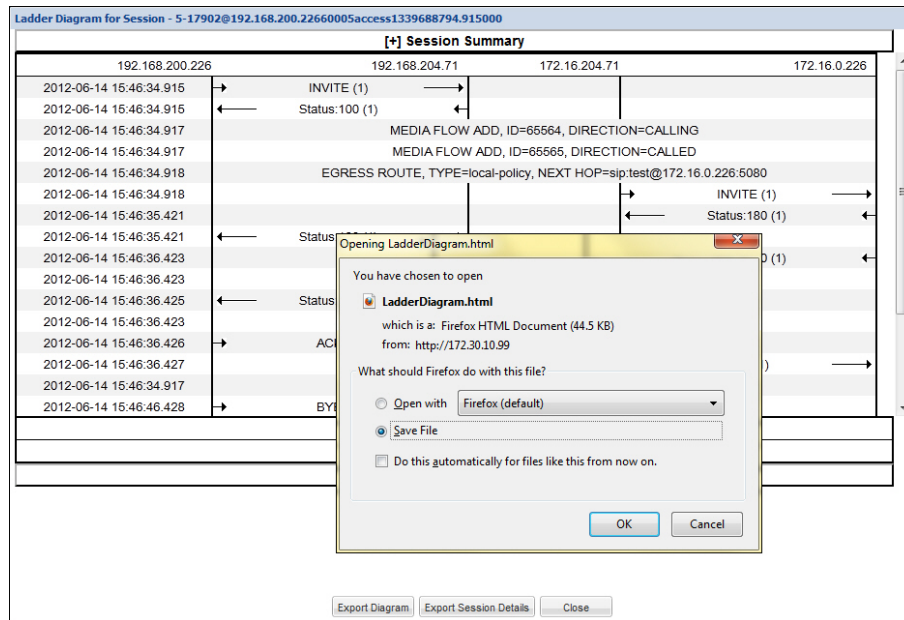
From the Sessions, Registrations, Subscriptions, and Notable Events Reports:

- **Export session details** - Exports the SIP messages and media events associated with the selected session, to a text file.
- **Export summary** - Exports all logged session summary records, to a text file. (Exports ALL call session summary records or the records that matched a search criteria).

From the Ladder Diagram:

- **Export diagram** - Exports all of the information in the Ladder Diagram to an HTML file (Session Summary, SIP Message Details, and QoS statistics).
- **Export session details** - Exports detailed information about the SIP messages and media events in the Ladder Diagram associated with the selected session, to a text file.

The following example shows the export of a Ladder Diagram to a file called LadderDiagram.html.



## Session Summary Exported Text File

The following is an example of a Session Summary exported text file from the Web-based GUI.

### Example

```
-----Session Summary-----
Startup Time: 2011-09-20 12:58:44.375

State: TERMINATED-200
Duration: 5
From URI: sipp < > ;sip:sipp@172.16.34.16:5060 >;tag=1
To URI: sut < > ;sip:service@172.16.34.225:5060 >;tag=13451
Ingress Src Address: 172.16.34.16
Ingress Src Port: 5060
Ingress Dest Address: 172.16.34.225
Ingress Dest Port: 5060
Egress Source Address: 192.168.34.225
Egress Source Port: 5060
Egress Destination Address: 192.168.34.17
Egress Destination Port: 5060
Ingress Realm: access
Egress Realm: backbone
Ingress NetworkIf: access
Egress NetworkIf: backbone

-----Session Summary-----
Startup Time: 2011-09-20 12:58:05.340
State: TERMINATED-200
Duration: 5
From URI: sipp < > ;sip:sipp@172.16.34.16:5060 >;tag=1
To URI: sut < > ;sip:service@172.16.34.225:5060 >;tag=13450
Ingress Src Address: 172.16.34.16
Ingress Src Port: 5060
```

```
Igress Dest Address: 172.16.34.225
Igress Dest Port: 5060
Egress Source Address: 192.168.34.225
Egress Source Port: 5060
Egress Destination Address: 192.168.34.17
Egress Destination Port: 5060
Igress Realm: access
Egress Realm: backbone
Igress NetworkIf: access
Egress NetworkIf: backbone
```

## Session Details Exported Text File

The following is an example of the a Session Details exported text file from the Web-based GUI.

### Example

Session Details:

```
-----
Nov 3 08:50:56.852 On [2:0]172.16.34.225:5060 received from 172.16.34.16:5060
```

```
INVITE sip:service@172.16.34.225:5060 SIP/2.0
Via: SIP/2.0/UDP 172.16.34.16:5060;branch=z9hG4bK-1-0
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>
Call-ID: 1-668@172.16.34.16
CSeq: 1 INVITE
Contact: sip:sipp@172.16.34.16:5060
Max-Forwards: 70
Subject: Performance Test
Content-Type: application/sdp
Content-Length: 135
```

```
v=0
o=user1 53655765 2353687637 IN IP4 172.16.34.16
s=-
c=IN IP4 172.16.34.16
t=0 0
m=audio 6000 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

```
-----
Nov 3 08:50:56.855 On [2:0]172.16.34.225:5060 sent to 172.16.34.16:5060
```

```
SIP/2.0 100 Trying
Via: SIP/2.0/UDP 172.16.34.16:5060;branch=z9hG4bK-1-0
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>
Call-ID: 1-668@172.16.34.16
CSeq: 1 INVITE
```

```
----MBCD Evt
Nov 3 08:50:56.862 On 127.0.0.1:2945 sent to 127.0.0.1:2944
mbcdEvent=FLOW ADD
FlowCollapsed=enabled
FlowDirection=CALLING
FlowID=65541
```

MediaFormat=0  
MediaReleased=disabled  
MediaType=audio/PCMU/  
OtherFlowID=0  
TOSBits=0  
InputSourcev4Addr=  
InputSourcePort=0  
InputDestv4Addr=172.16.34.225  
InputDestPort=10004  
OutputSourcev4Addr=192.168.34.225  
OutputDestv4Addr=  
OutputDestPort=0  
InputRealm=access  
OutputRealm=backbone  
----MBCD Evt  
Nov 3 08:50:56.862 On 127.0.0.1:2945 received from 127.0.0.1:2944

mbcdEvent=FLOW ADD  
FlowCollapsed=enabled  
FlowDirection=CALLED  
FlowID=65542  
MediaFormat=0  
MediaReleased=disabled  
MediaType=audio/PCMU/  
OtherFlowID=0  
TOSBits=0  
InputSourcev4Addr=  
InputSourcePort=0  
InputDestv4Addr=192.168.34.225  
InputDestPort=20004  
OutputSourcev4Addr=172.16.34.225  
OutputDestv4Addr=172.16.34.16  
OutputDestPort=6000  
InputRealm=backbone  
OutputRealm=access

-----  
Nov 3 08:50:56.865 On [1:0]192.168.34.225:5060 sent to 192.168.34.17:5060

INVITE sip:service@192.168.34.17:5060 SIP/2.0  
Via: SIP/2.0/UDP 192.168.34.225:5060;branch=z9hG4bK4od0io20183g8ssv32f1.1  
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1  
To: sut <sip:service@172.16.34.225:5060>  
Call-ID: 1-668@172.16.34.16  
CSeq: 1 INVITE  
Contact: <sip:sipp@192.168.34.225:5060;transport=udp>  
Max-Forwards: 69  
Subject: Performance Test  
Content-Type: application/sdp  
Content-Length: 140

v=0  
o=user1 53655765 2353687637 IN IP4 192.168.34.225  
s=-  
c=IN IP4 192.168.34.225  
t=0 0  
m=audio 20004 RTP/AVP 0  
a=rtpmap:0 PCMU/8000

-----  
Nov 3 08:50:56.868 On [1:0]192.168.34.225:5060 received from 192.168.34.17:5060

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 192.168.34.225:5060;branch=z9hG4bK4od0io20183g8ssv32f1.1
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>;tag=2578
Call-ID: 1-668@172.16.34.16
CSeq: 1 INVITE
Contact: <sip:192.168.34.17:5060;transport=UDP>
Content-Length: 0
```

-----  
Nov 3 08:50:56.872 On [2:0]172.16.34.225:5060 sent to 172.16.34.16:5060

```
SIP/2.0 180 Ringing
Via: SIP/2.0/UDP 172.16.34.16:5060;branch=z9hG4bK-1-0
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>;tag=2578
Call-ID: 1-668@172.16.34.16
CSeq: 1 INVITE
Contact: <sip:service@172.16.34.225:5060;transport=udp>
Content-Length: 0
```

-----  
Nov 3 08:50:56.872 On [1:0]192.168.34.225:5060 received from 192.168.34.17:5060

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 192.168.34.225:5060;branch=z9hG4bK4od0io20183g8ssv32f1.1
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1
To: sut <sip:service@172.16.34.225:5060>;tag=2578
Call-ID: 1-668@172.16.34.16
CSeq: 1 INVITE
Contact: <sip:192.168.34.17:5060;transport=UDP>
Content-Type: application/sdp
Content-Length: 137
v=0
o=user1 53655765 2353687637 IN IP4 192.168.34.17
s=-
c=IN IP4 192.168.34.17
t=0 0
m=audio 6000 RTP/AVP 0
a=rtpmap:0 PCMU/8000
```

----MBCD Evt  
Nov 3 08:50:56.878 On 127.0.0.1:2945 sent to 127.0.0.1:2944

```
mbcdEvent=FLOW MODIFY
FlowCollapsed=enabled
FlowDirection=CALLING
FlowID=65541
MediaFormat=0
MediaReleased=disabled
MediaType=audio/PCMU/
OtherFlowID=0
TOSBits=0
InputSourcev4Addr=
InputSourcePort=0
InputDestv4Addr=172.16.34.225
InputDestPort=10004
OutputSourcev4Addr=192.168.34.225
OutputDestv4Addr=192.168.34.17
OutputDestPort=6000
InputRealm=access
```

OutputRealm=backbone

-----  
Nov 3 08:50:56.881 On [2:0]172.16.34.225:5060 sent to 172.16.34.16:5060

SIP/2.0 200 OK  
Via: SIP/2.0/UDP 172.16.34.16:5060;branch=z9hG4bK-1-0  
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1  
To: sut <sip:service@172.16.34.225:5060>;tag=2578  
Call-ID: 1-668@172.16.34.16  
CSeq: 1 INVITE  
Contact: <sip:service@172.16.34.225:5060;transport=udp>  
Content-Type: application/sdp  
Content-Length: 138  
v=0  
o=user1 53655765 2353687637 IN IP4 172.16.34.225  
s=-  
c=IN IP4 172.16.34.225  
t=0 0  
m=audio 10004 RTP/AVP 0  
a=rtpmap:0 PCMU/8000

-----  
Nov 3 08:50:56.883 On [2:0]172.16.34.225:5060 received from 172.16.34.16:5060

ACK sip:service@172.16.34.225:5060 SIP/2.0  
Via: SIP/2.0/UDP 172.16.34.16:5060;branch=z9hG4bK-1-5  
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1  
To: sut <sip:service@172.16.34.225:5060>;tag=2578  
Call-ID: 1-668@172.16.34.16  
CSeq: 1 ACK  
Contact: sip:sipp@172.16.34.16:5060  
Max-Forwards: 70  
Subject: Performance Test  
Content-Length: 0

-----  
Nov 3 08:50:56.887 On [1:0]192.168.34.225:5060 sent to 192.168.34.17:5060

ACK sip:192.168.34.17:5060;transport=UDP SIP/2.0  
Via: SIP/2.0/UDP 192.168.34.225:5060;branch=z9hG4bK48k3k1301ot00ssvflv0.1  
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1  
To: sut <sip:service@172.16.34.225:5060>;tag=2578  
Call-ID: 1-668@172.16.34.16  
CSeq: 1 ACK  
Contact: <sip:sipp@192.168.34.225:5060;transport=udp>  
Max-Forwards: 69  
Subject: Performance Test  
Content-Length: 0

-----  
Nov 3 08:51:01.883 On [2:0]172.16.34.225:5060 received from 172.16.34.16:5060

BYE sip:service@172.16.34.225:5060 SIP/2.0  
Via: SIP/2.0/UDP 172.16.34.16:5060;branch=z9hG4bK-1-7  
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1  
To: sut <sip:service@172.16.34.225:5060>;tag=2578  
Call-ID: 1-668@172.16.34.16  
CSeq: 2 BYE  
Contact: sip:sipp@172.16.34.16:5060  
Max-Forwards: 70  
Subject: Performance Test

Content-Length: 0

-----  
Nov 3 08:51:01.887 On [1:0]192.168.34.225:5060 sent to 192.168.34.17:5060

BYE sip:192.168.34.17:5060;transport=UDP SIP/2.0  
Via: SIP/2.0/UDP 192.168.34.225:5060;branch=z9hG4bK5oq46d301gv0dus227f1.1  
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1  
To: sut <sip:service@172.16.34.225:5060>;tag=2578  
Call-ID: 1-668@172.16.34.16  
CSeq: 2 BYE  
Contact: <sip:sipp@192.168.34.225:5060;transport=udp>  
Max-Forwards: 69  
Subject: Performance Test  
Content-Length: 0

-----  
Nov 3 08:51:01.889 On [1:0]192.168.34.225:5060 received from 192.168.34.17:5060

SIP/2.0 200 OK  
Via: SIP/2.0/UDP 192.168.34.225:5060;branch=z9hG4bK5oq46d301gv0dus227f1.1  
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1  
To: sut <sip:service@172.16.34.225:5060>;tag=2578  
Call-ID: 1-668@172.16.34.16  
CSeq: 2 BYE  
Contact: <sip:192.168.34.17:5060;transport=UDP>  
Content-Length: 0

-----  
Nov 3 08:51:01.892 On [2:0]172.16.34.225:5060 sent to 172.16.34.16:5060

SIP/2.0 200 OK  
Via: SIP/2.0/UDP 172.16.34.16:5060;branch=z9hG4bK-1-7  
From: sipp <sip:sipp@172.16.34.16:5060>;tag=1  
To: sut <sip:service@172.16.34.225:5060>;tag=2578  
Call-ID: 1-668@172.16.34.16  
CSeq: 2 BYE  
Contact: <sip:service@172.16.34.225:5060;transport=udp>  
Content-Length: 0

----MBCD Evt  
Nov 3 08:51:01.891 On 127.0.0.1:2945 sent to 127.0.0.1:2944

mbcdEvent=FLOW DELETE  
FlowCollapsed=enabled  
FlowDirection=CALLING  
FlowID=65541  
MediaFormat=0  
MediaReleased=disabled  
MediaType=audio/PCMU/  
OtherFlowID=0  
TOSBits=0  
InputSourcev4Addr=  
InputSourcePort=0  
InputDestv4Addr=172.16.34.225  
InputDestPort=10004  
OutputSourcev4Addr=192.168.34.225  
OutputDestv4Addr=192.168.34.17  
OutputDestPort=6000  
InputRealm=access  
OutputRealm=backbone

```
----MBCD Evt
mbcdEvent=FLOW DELETE
FlowCollapsed=enabled
FlowDirection=CALLED
FlowID=65542
MediaFormat=0
MediaReleased=disabled
MediaType=audio/PCMU/
OtherFlowID=65541
TOSBits=0
InputSourcev4Addr=
InputSourcePort=0
InputDestv4Addr=192.168.34.225
InputDestPort=20004
OutputSourcev4Addr=172.16.34.225
OutputDestv4Addr=172.16.34.16
OutputDestPort=6000
InputRealm=backbone
OutputRealm=access

-----Session Summary-----
Startup Time: 2012-01-25 10:28:30.394

State: TERMINATED-200
Duration: 5
From URI: sipp < &lt; sip:sipp@172.16.34.16:5060 &gt; ;tag=1
To URI: sut < &lt; sip:service@172.16.34.225:5060 &gt; ;tag=2578
Ingress Src Address: 172.16.34.16
Ingress Src Port: 5060
Ingress Dest Address: 172.16.34.225
Ingress Dest Port: 5060
Egress Source Address: 192.168.34.225
Egress Source Port: 5060
Egress Destination Address: 192.168.34.17
Egress Destination Port: 5060
Ingress Realm: access
Egress Realm: backbone
Ingress NetworkIf: access
Egress NetworkIf: backbone
```

## Ladder Diagram Exported HTML File

The following is an example of a Ladder Diagram for a session, exported to an HTML file from the Web-based GUI.



# Example

The screenshot shows the Oracle SIP Session Summary interface. The top navigation bar includes 'Home', 'Configuration', 'Monitor and Trace', 'Widgets', and 'System'. The left sidebar has 'Sessions' selected, with other options like 'Registrations', 'Subscriptions', and 'Notable Events'. The main content area displays a table of SIP session details.

Start Time	State	Call ID	Request URI	From URI
2013-10-17 13:56:41.083	FAILED-408	5-15779@192.168.200.2	sip:service@192.168.200.2	9788482942 <sip:97884
2013-10-17 13:56:40.984	FAILED-408	4-15779@192.168.200.2	sip:service@192.168.200.2	9788482942 <sip:97884
2013-10-17 13:56:40.884	FAILED-408	3-15779@192.168.200.2	sip:service@192.168.200.2	9788482942 <sip:97884
2013-10-17 13:56:40.784	FAILED-408	2-15779@192.168.200.2	sip:service@192.168.200.2	9788482942 <sip:97884
2013-10-17 13:56:40.683	FAILED-408	1-15779@192.168.200.2	sip:service@192.168.200.2	9788482942 <sip:97884
2013-10-17 13:56:21.338	TERMINATED-	5-15665@192.168.200.2	sip:service@192.168.200.2	9788482942 <sip:97884
2013-10-17 13:56:21.238	TERMINATED-	4-15665@192.168.200.2	sip:service@192.168.200.2	9788482942 <sip:97884
2013-10-17 13:56:21.136	TERMINATED-	3-15665@192.168.200.2	sip:service@192.168.200.2	9788482942 <sip:97884

[+] Session Summary

State	TERMINATED-200	Duration	10
From URI	"*2273636" <tel:781-414-2345>;tag=60005	To URI	sut <sip:kam@192.168.204.71:5060>;tag=50004
Ingress Src IP-Port	192.168.200.226:5070	Egress Src IP-Port	172.16.204.71:5060
Ingress Dest IP-Port	192.168.204.71:5060	Egress Dest IP-Port	172.16.0.226:5070
Ingress Realm	access	Egress Realm	core
Ingress Network Intf	N100	Egress Network Intf	M10
Ingress Transport	UDP	Egress Transport	UDP

192.168.200.226      192.168.204.71      172.16.204.71      172.16.0.226

2012-06-14 15:46:34.915	→	INVITE (1)	→										
2012-06-14 15:46:34.915	←	Status:100 (1)	←										
2012-06-14 15:46:34.917													
2012-06-14 15:46:34.917													
2012-06-14 15:46:34.918													
2012-06-14 15:46:34.918													
2012-06-14 15:46:35.421													
2012-06-14 15:46:35.421	←	Status:180 (1)	←										
2012-06-14 15:46:36.423													
2012-06-14 15:46:36.423													
2012-06-14 15:46:36.423	←	Status:200 (1)	←										
2012-06-14 15:46:36.425													
2012-06-14 15:46:36.426	→	ACK (1)	→										
2012-06-14 15:46:36.427													
2012-06-14 15:46:36.427													
2012-06-14 15:46:36.427	→	ACK (1)	→										
2012-06-14 15:46:39.17													
2012-06-14 15:46:46.428	→	BYE (2)	→										
2012-06-14 15:46:46.428													
2012-06-14 15:46:46.430													
2012-06-14 15:46:46.431													
2012-06-14 15:46:46.430	←	Status:200 (2)	←										
2012-06-14 15:46:46.430													
2012-06-14 15:46:46.430													
2012-06-14 15:46:46.430													

SIP Message Details

[+] QoS Stats

Flow ID	Direction	Total Pkts Received	Total Octets Received	RTCP			RTP			QoS			
				Pkt Lost	Avg Jitter	Max Jitter	Avg Latency	Max Latency	Pkt Lost	Avg Jitter	Max Jitter	R-Factor	MOS
65564	CALLING	0	0	0	0	0	0	0	0	0	0	0	0
65565	CALLED	0	0	0	0	0	0	0	0	0	0	0	0