Oracle® Enterprise Session Border Controller

Web GUI Guide

Release S-Cz8.3.0

F20181-01

October 2019

Oracle Enterprise Session Border Controller Web GUI Guide, Release S-Cz8.3.0

F20181-01

Contents

About This Guide

Revision History

1 Getting Started

2 Dashboard Tab Operations

3 Configuration Tab Operations

About This Guide

The *Web GUI User Guide* provides information about configuring and administering the Oracle® Enterprise Session Border Controller (E-SBC) from the Web GUI.

Documentation Set

The following table describes the documentation set for this release.

ACLI Configuration Guide	Contains conceptual and procedural information for configuring, administering, and troubleshooting the E-SBC.
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Administrative Security Guide	Contains conceptual and procedural information for supporting the Admin Security, Admin Security with ACP, and JITC feature sets on the E-SBC.
Call Traffic Monitoring Guide	Contains conceptual and procedural information for configuration using the tools and protocols required to manage call traffic on the E-SBC.
FIPS Compliance Guide	Contains conceptual and procedural information about FIPS compliance on the E-SBC.
HMR Guide	Contains conceptual and procedural information for header manipulation. Includes rules, use cases, configuration, import, export, and examples.
Installation and Platform Preparation Guide	Contains conceptual and procedural information for system provisioning, software installations, and upgrades.
Release Notes	Contains information about this release, including platform support, new features, caveats, known issues, and limitations.
SBC Family Security Guide	Contains information about security considerations and best practices from a network and application security perspective for the Oracle Communications Session Delivery Product family of products.
Time Division Multiplexing Guide	Contains the concepts and procedures necessary for installing, configuring, and administering Time Division Multiplexing (TDM) on the Acme Packet 1100 and the Acme Packet 3900.

Web GUI User Guide	Contains conceptual and procedural information for using the tools and features of the E-SBC Web GUI.

Related Documentation

The following list describes related documentation for the Oracle® Enterprise Session Border Controller. You can find the listed documents on http://docs.oracle.com/en/industries/communications/ in the "Session Border Controller Documentation" and "Acme Packet" sections.

Document Name	Document Description
Acme Packet 3900 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 3900.
Acme Packet 4600 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4600.
Acme Packet 6100 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6100.
Acme Packet 6300 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6300.
Acme Packet 6350 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6350.
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 Service Provider 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), Oracle Communication'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 and Diameter 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.

Document Name	Document Description
SBC Family 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.
Installation and Platform Preparation Guide	Contains information about upgrading system images and any pre-boot system provisioning.
Call Traffic Monitoring Guide	Contains information about traffic monitoring and packet traces as collected on the system. This guide also includes WebGUI configuration used for the SIP Monitor and Trace application.
HMR Resource Guide	Contains information about configuring and using Header Manipulation Rules to manage service traffic.
TSCF SDK Guide	Contains information about the client-side SDK that facilitates the creation of secure tunnels between a client application and the TSCF of the OCSBC.
REST API Guide	Contains information about the supported REST APIs and how to use the REST API interface.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request.
2. Select 3 for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
   - For technical issues such as creating a new Service Request (SR), select 1.
   - For non-technical issues such as registration or assistance with My Oracle Support, select 2.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://

www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click **Industries**.
3. Under the Oracle Communications sub-header, click the **Oracle Communications documentation** link.
   The Communications Documentation page appears. Most products covered by these documentation sets appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Revision History

This table provides the revision history for this document.

Date	Description
April 2019	• Initial release
October 2019	• Contents revised to reflect the major revision of the Web GUI. • Adds HTTP Interface List to web server configuration. • Updates the version of Google Chrome supported for the Web GUI.
December 2019	• Updates complete guide to correspond to S-Cz8.3.0m1p2 Web GUI reversion.

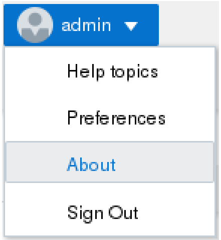
1 Getting Started

Oracle® recommends that you review the topics in "Getting Started" before working with the system to ensure success with the tools and functions provided.

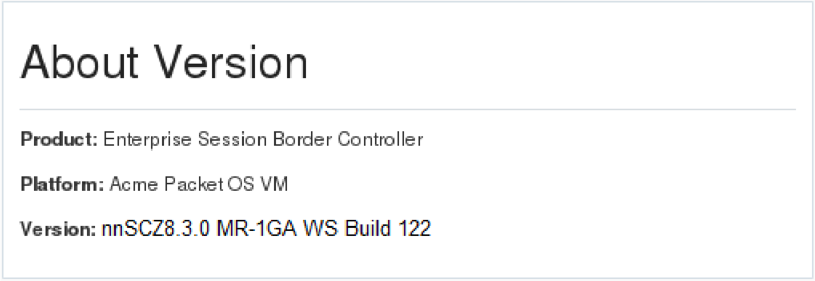
About This Software

You can display information about the software currently installed on the Oracle® Enterprise Session Border Controller (E-SBC) that you are logged on to by clicking **About** on the **User** menu located in the upper right corner of the Web GUI.

The following screen capture shows the location of **About** on the User menu.



The following screen capture shows an example of the information that the About link displays.



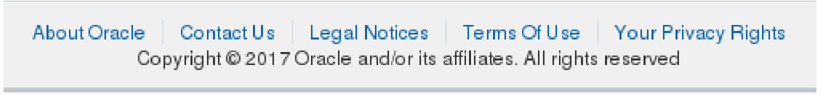
About Version

Product: Enterprise Session Border Controller

Platform: Acme Packet OS VM

Version: nnSCZ8.3.0 MR-1GA WS Build 122

The About page also displays the following links to more information about Oracle and the E-SBC.



Copyright © 2017 Oracle and/or its affiliates. All rights reserved

Browser Support

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

- Google Chrome (Recommended)—version 77.0.3865.120 and higher
- Internet Explorer—not supported
- Microsoft Edge—not supported

- Mozilla Firefox—not supported

> **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.

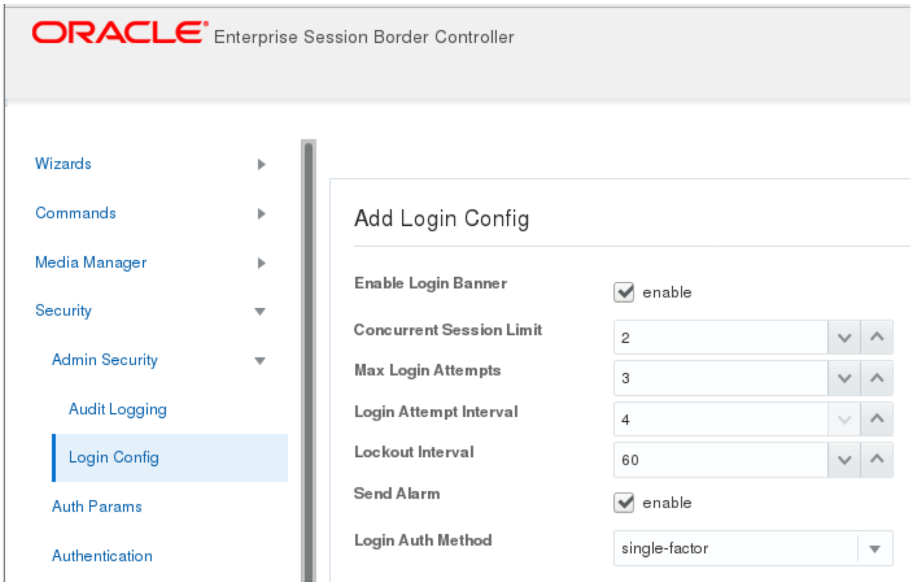
Web GUI Access with the Admin Security License

The Admin Security License provides additional configuration parameters and behavioral controls to enhance security. You can install the Admin Security License from the Web GUI, which you may find more convenient than using the ACLI. To support the Admin Security License, the system requires certificates and an HTTPS connection.

Additional Security Configuration Parameters

With the Admin Security License installed, the Web GUI adds the **Login Config** object under **Security** and adds parameters to the existing **Password Policy** object.

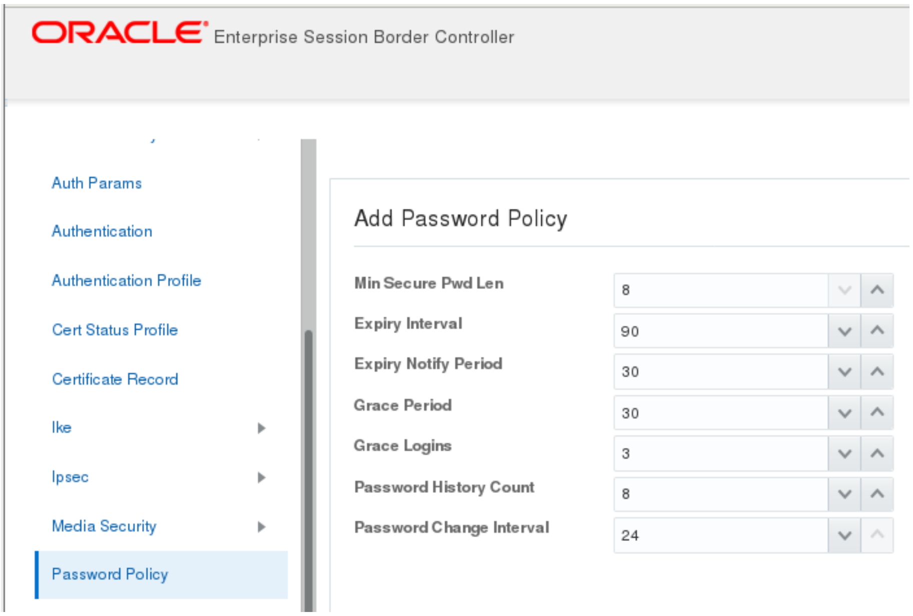
The **Login Config** dialog provides the configuration parameters shown in the following illustration.



Add Login Config

Enable Login Banner	☑ enable
Concurrent Session Limit	2
Max Login Attempts	3
Login Attempt Interval	4
Lockout Interval	60
Send Alarm	☑ enable
Login Auth Method	single-factor

The **Password Policy** dialog displays the additional configuration parameters available with the Admin Security license below **Min Secure Pwd Len** in the following illustration.



Add Password Policy

Min Secure Pwd Len	8
Expiry Interval	90
Expiry Notify Period	30
Grace Period	30
Grace Logins	3
Password History Count	8
Password Change Interval	24

Enhanced Security Requirements

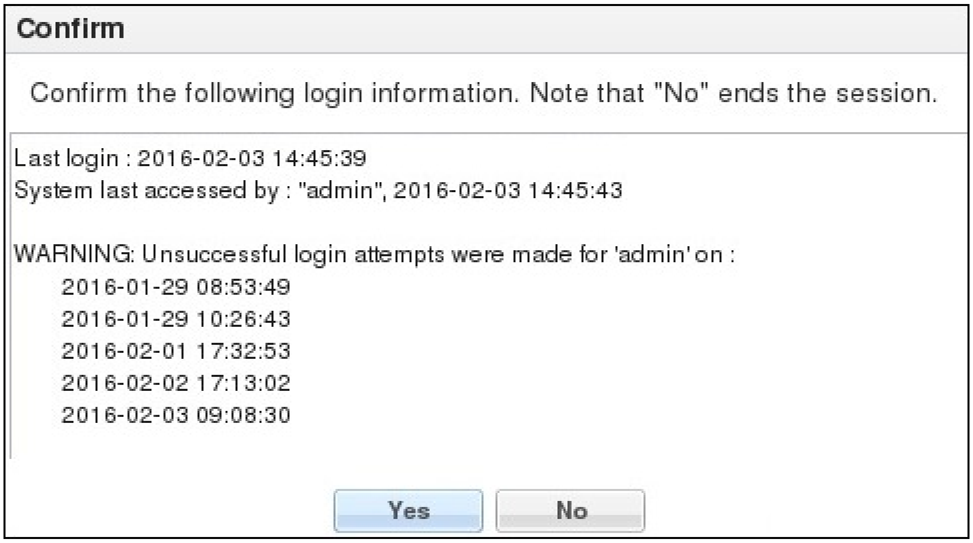
HTTPS—The system requires an HTTPS connection to access the Web GUI. Oracle recommends that you configure HTTPS on the Web server before installing the Admin Security License. If the Web server is configured for HTTP when you install the Admin Security License, the system displays an error message when you attempt to Save. Note that after you install the Admin Security License, the system does not allow changing HTTPS to HTTP.

Certificates—The system requires you to configure **Local Cert** and **Local Cert CA** on the E-SBC in order to gain access to the Web GUI with HTTPS. Oracle recommends configuring the certificates and a TLS profile before installing the Admin Security license. For instructions, see "Configuring TLS on the Web Server" in the *ACLI Configuration Guide*.

Enhanced Security Behavior

Concurrent Sessions Limit—In **Login Config**, you can specify the maximum number of concurrent sessions allowed. When the limit is reached, the system allows no more logins until the number of active sessions falls below the maximum.

Login History Confirmation—With the Admin Security License installed, and the login banner enabled, the system displays the previous login history. The user must acknowledge the login history. **Yes** allows the login attempt to proceed and **No** ends the session. The following illustration shows an example of the information provided.



Confirm

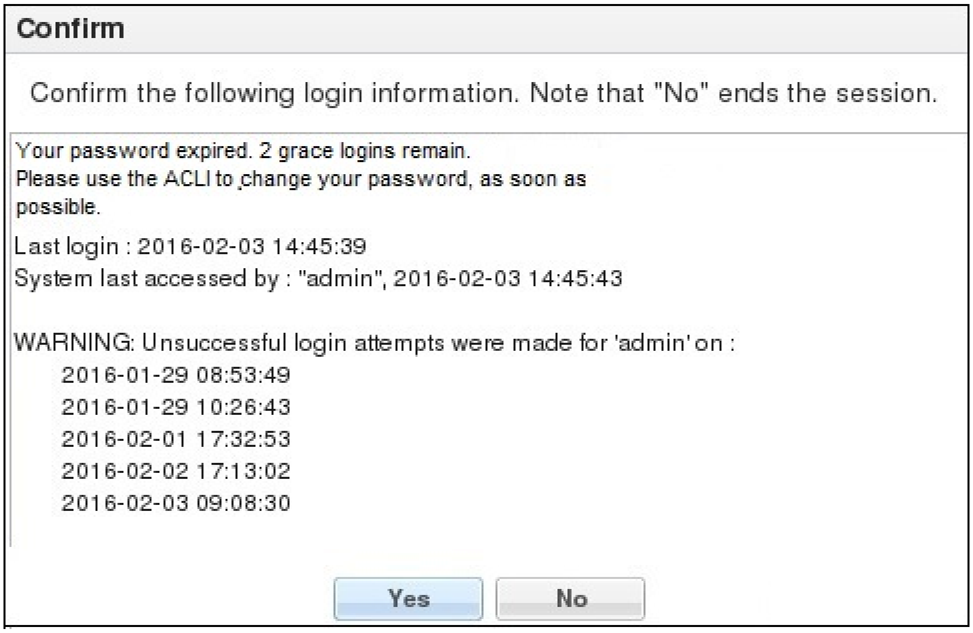
Confirm the following login information. Note that "No" ends the session.

Last login : 2016-02-03 14:45:39
System last accessed by : "admin", 2016-02-03 14:45:43

WARNING: Unsuccessful login attempts were made for 'admin' on :
2016-01-29 08:53:49
2016-01-29 10:26:43
2016-02-01 17:32:53
2016-02-02 17:13:02
2016-02-03 09:08:30

Password Expiry Notification—You can configure **Password Policy** to notify the user up to 90 days in advance of password expiry. The system provides the notification in the following ways.

- When you enable the login banner, the system displays the notification in the Confirm banner.



Confirm

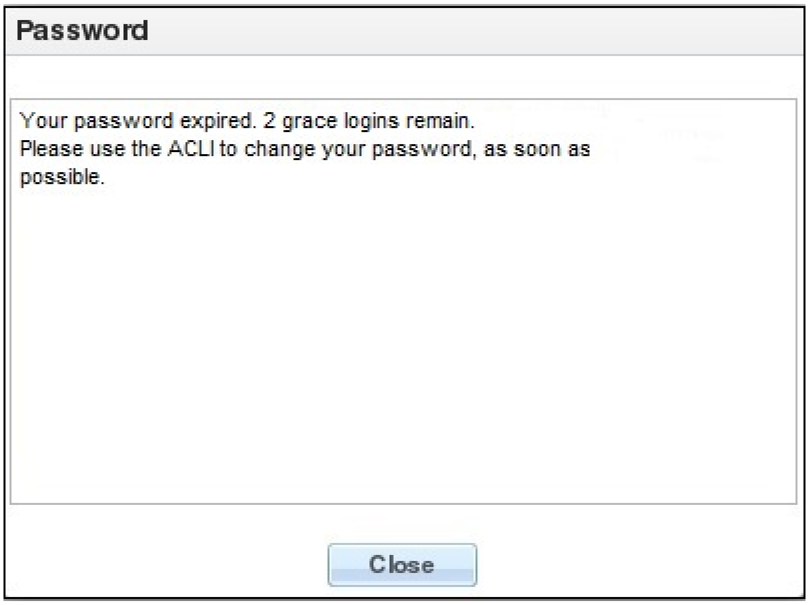
Confirm the following login information. Note that "No" ends the session.

Your password expired. 2 grace logins remain.
Please use the ACLI to change your password, as soon as possible.

Last login : 2016-02-03 14:45:39
System last accessed by : "admin", 2016-02-03 14:45:43

WARNING: Unsuccessful login attempts were made for 'admin' on :
2016-01-29 08:53:49
2016-01-29 10:26:43
2016-02-01 17:32:53
2016-02-02 17:13:02
2016-02-03 09:08:30

- When you do not enable the login banner, the system displays the notification in the Password banner upon a login attempt.



Your password expired. 2 grace logins remain.
Please use the ACLI to change your password, as soon as possible.

Note:

The Web GUI does not support changing a user password. You must use the `#secret enable` command from the ACLI.

Remote Authentication—In the Authentication configuration object, you can select RADIUS or TACACS for remote authentication. The system behaves as follows:

- The local Admin and User can log on by way of the E-SBC console, the Web GUI, SSH or SFTP, and the system performs the local user authentication process.
- The local Admin and User can log on only by way of the ACLI on the E-SBC when RADIUS is enabled. (No Web GUI, SSH, or SFTP login) You must configure the corresponding authentication type on the Session Director.
- RADIUS users can use their corresponding RADIUS user name to login to the Web GUI, and the system performs the secure user authentication process. The system displays the same login banner that local users see.

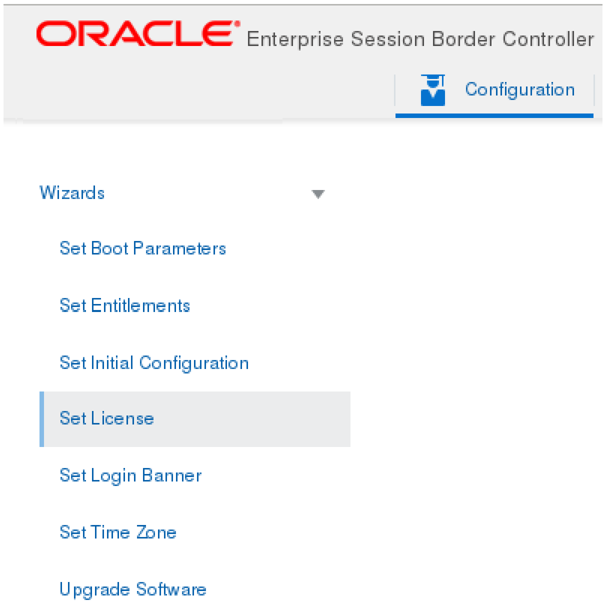
Two-Factor Authentication—When enabled, the system prompts the user for a passcode in addition to the User Name and Password. The length and strength requirements that apply to passwords also apply to passcodes. Other policy mandates such as history, re-use, and expiration do not apply to the passcode.

Note:

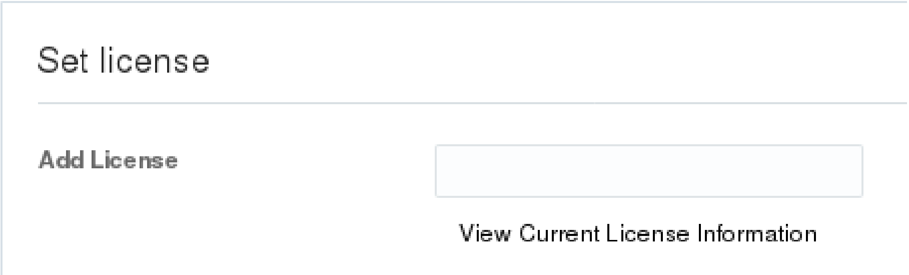
You must change the default passcode upon the first login attempt.

License Installation

From the Web GUI, install the Admin Security License by way of the Set License wizard on the Configuration tab.



The Set License wizard launches the Set License dialog, where you enter the license serial number.



When you click **Complete**, the system completes the installation. You do not need to Save and Activate or re-run the Set Initial Configuration wizard.

> **Note:**
>
> The system deactivates the Set Initial Configuration wizard in the current session, so that you cannot accidentally erase the existing configuration.

For license installation instructions, see "Set License."

Access the Web GUI with HTTPS

To provide secure access to the Web GUI from the Web server, you can enable HTTPS by creating a Transport Layer Security (TLS) profile. The Oracle® Enterprise Session Border Controller (E-SBC) does not require either the hardware Security Service Module (SSM) or the software TLS license when configuring **certificate record**, **tls-profile**, and **tls-global** for an HTTPS connection to the Web GUI from the Web server.

Note that the E-SBC requires the TLS license when you configure SIP for TLS.

Note:

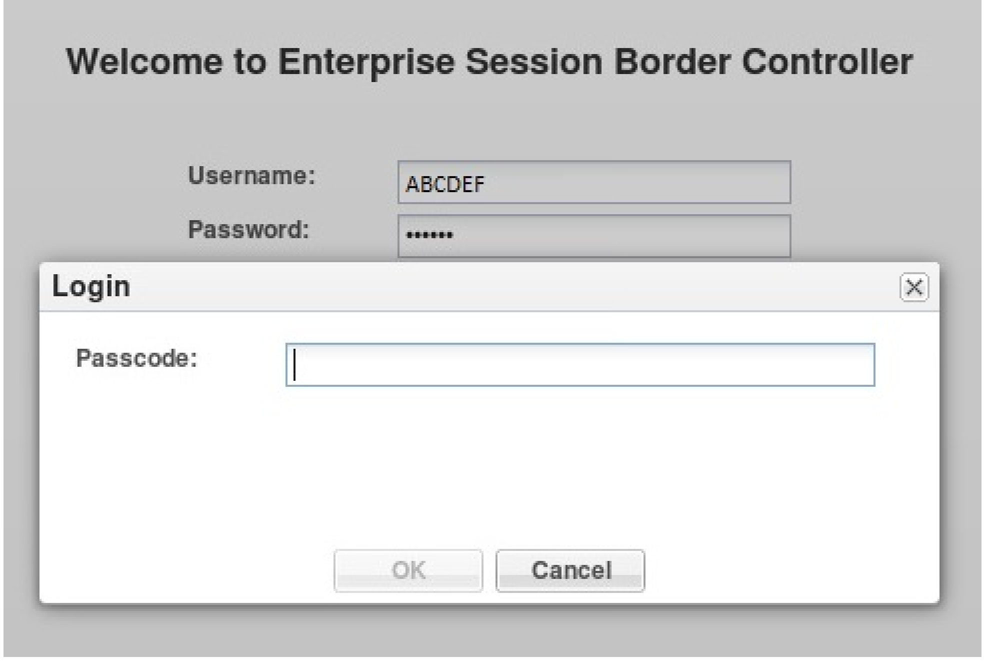
Virtual machines require the software TLS license.

Two-Factor Authentication

Two-factor authentication provides an extra level of security for the Oracle® Enterprise Session Border Controller (E-SBC) by requiring users to enter a Passcode during login, in addition to their Username and Password credentials. Two-factor authentication applies to the Super User for both local and SSH login to the ACLI, and for HTTPS login to the Web GUI.

The two-factor authentication option requires the Admin Security feature be provisioned, and you must enable the option by setting `login-auth-method` to "two-factor" and saving the configuration. After you set "two-factor" and save the configuration, the E-SBC prompts you to set the Passcode.

The following illustrations show the user login experience on the Web GUI after you enable two-factor authentication.



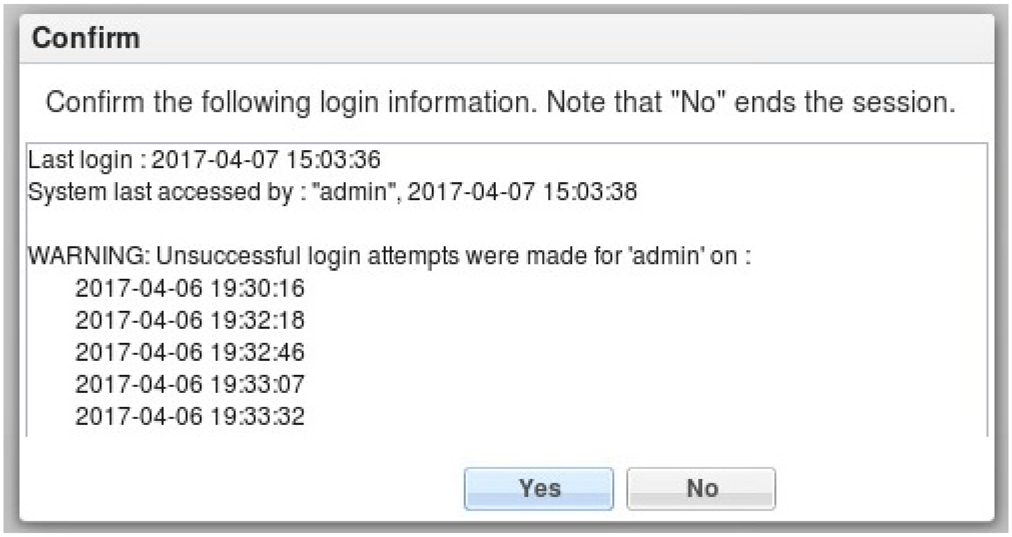
Welcome to Enterprise Session Border Controller

Username: ABCDEF

Password: ••••••

Login

Passcode:



Confirm

Confirm the following login information. Note that "No" ends the session.

```
Last login : 2017-04-07 15:03:36
System last accessed by : "admin", 2017-04-07 15:03:38

WARNING: Unsuccessful login attempts were made for 'admin' on :
    2017-04-06 19:30:16
    2017-04-06 19:32:18
    2017-04-06 19:32:46
    2017-04-06 19:33:07
    2017-04-06 19:33:32
```

Passcodes must conform to the length and strength requirements specified in "Enable Two-Factor Authentication."

When you want to change the Passcode in the future, use the **secret** command that you also use for changing the Username and Password.

You can enable two-factor authentication only from the ACLI.

Two-factor authentication does not support RADIUS, TACACS, and HTTP.

Enable Two-Factor Authentication

To enable two-factor authentication for local or SSH login, you must set two-factor as the login authentication method and set the required Passcode.

1. Import the local certificate and the local certificate CA into the E-SBC
2. Configure the Web server for HTTPS
3. Install the Admin Security license

A passcode must meet the following length and strength requirements:

- contain only upper and lower case alphabetical letters, numbers, and punctuation characters.
- contain a minimum of fifteen characters.
- contain two lower-case alphabetical letters.
- contain two upper-case alphabetical letters.
- contain two numerals.
- contain two special characters.
- not contain, repeat, or reverse the user name.
- not contain three of the same characters used consecutively.
- differ from the previous passcode by at least four characters.
- differ from the last three previous passcodes.
- not change more than once every 24 hours.

1. Access the Login Config configuration object: **Configuration**, **Security**, **Admin Security**, **Login Config**.
2. In the Login Config dialog, select **Two Factor** from the Login Auth Method drop-down list.
3. Click **OK**.
4. Save the configuration.

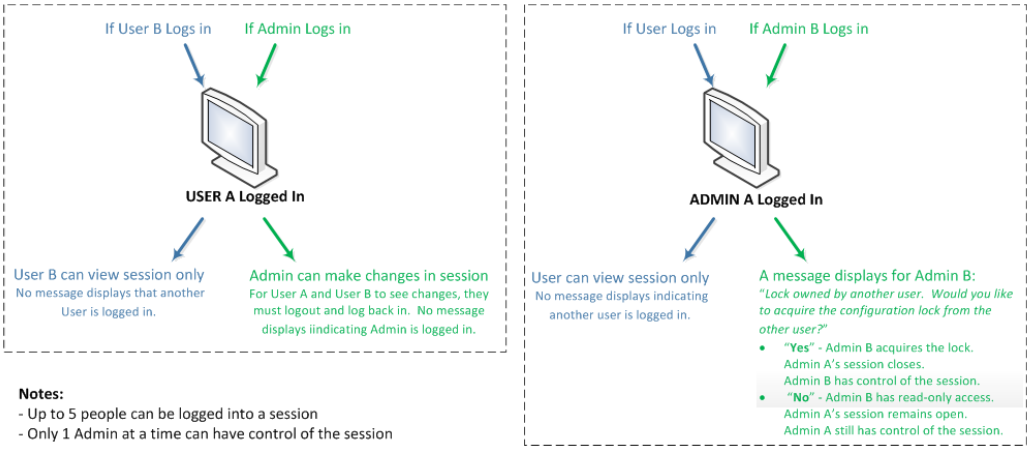
User and Administrator Access Rules

Users and Administrators can use the Oracle® Enterprise Session Border Controller (E-SBC) Web GUI according to the following rules for their role.

User	• Read-only access • View Basic and Expert configuration information • Cannot save and activate a configuration • Cannot add a configuration • Cannot edit a configuration
Administrator	• Add, edit, and view configurations • Save and activate a configuration • Switch between Basic mode and Expert mode

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 on to the session. The following illustrations depict and explain the system behavior when a User and an Administrator log on to a Web GUI session.


If User B Logs in
If Admin Logs in
USER A Logged In
User B can view session only
No message displays that another User is logged in.
Admin can make changes in session
For User A and User B to see changes, they must logout and log back in. No message displays iindicating Admin is logged in.
Notes:
- Up to 5 people can be logged into a session
- Only 1 Admin at a time can have control of the session
If User Logs in
If Admin B Logs in
ADMIN A Logged In
User can view session only
No message displays indicating another user is logged in.
A message displays for Admin B:
"Lock owned by another user. Would you like to acquire the configuration lock from the other user?"
• "Yes" - Admin B acquires the lock. Admin A's session closes. Admin B has control of the session.
• "No" - Admin B has read-only access. Admin A's session remains open. Admin A still has control of the 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.
```

Log On to the Web GUI

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

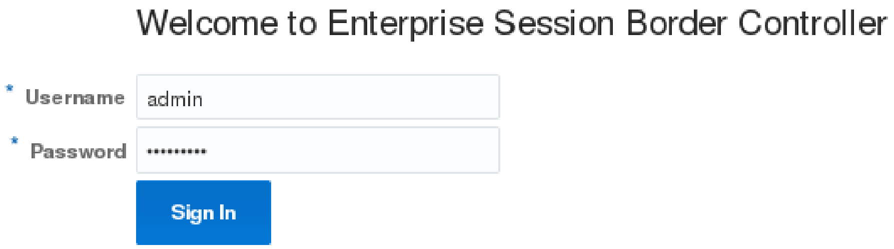
You need your User name, Password, and optionally your Passcode to log in. The system requires your passcode when two factor authentication is enabled. If your system Administrator configured the optional log on page message, the system displays the message after you enter your log on credentials. After reading the message, click **Close**, and the system displays the GUI.

1. On a PC, open a supported Internet browser. See "Browser Support."
2. Start the GUI with either the HTTP or HTTPS log on.

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

   > **Note:**
   >
   > Whether you log on using HTTP or HTTPS depends on the settings for your deployment.

3. In the Welcome dialog, enter your Web GUI username and password.



Welcome to Enterprise Session Border Controller

* Username: admin

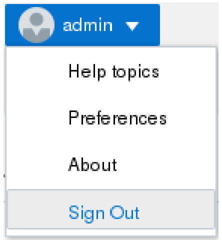
* Password: ••••••••••

4. If your E-SBC requires two-factor authentication, do the following:
   a. In the **Login** dialog, enter your passcode.
   b. In the **Confirm** dialog, acknowledge the Last Login information. Yes—allows you to login. No—ends the session.
5. Click Login.

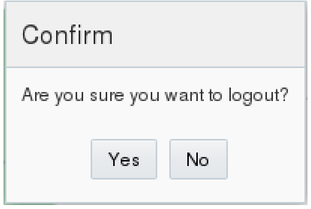
Log Off from the Web GUI

To log off from the Web GUI, you click **Sign Out** from the User menu and confirm.

1. On the User menu located in the upper right corner of the Web GUI, click **Sign Out**.



2. In the **Confirm** dialog, click **Yes**.



Are you sure you want to logout?

Change the Log On Password

Use the Oracle® Enterprise Session Border Controller ACLI to change a User or Administrator log on password.

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

RADIUS Server Roles and Access Privileges

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

Available functions depend on the role that you assign to the "userclass" on the RADIUS server.

- When you configure the RADIUS server as userclass=admin, the system allows the Administrator full access to all features and functions after logging onto the GUI.
- When you configure the RADIUS server as userclass=user, the system limits User access to the following features and functions after logging onto the GUI.
  - Full access to all System features and functions
  - Can download the following files in System File Management:
    - Backup Configuration
    - Configuration CSV
    - Fraud Protection Table
    - Log
    - Audit Log

- Playback Media
- Software image
- SPL Plug-in (SPL)

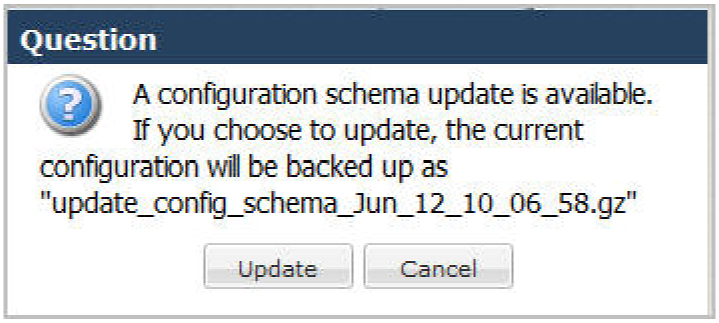
> **Note:**
>
> The "User" account cannot upload files in System File Management.

Update the Configuration Schema

When a release includes new parameters, you must update the schema to see them. The updated schema adds the new parameters to their respective configuration screens.

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

1. Log on to the Web GUI. The system displays the following prompt.



Question

A configuration schema update is available. If you choose to update, the current configuration will be backed up as "update_config_schema_Jun_12_10_06_58.gz"

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 Tabs Displays and Operations

The Web GUI displays tabs that you click to display information and perform tasks, such as configuring, managing, and monitoring the system. Each tab displays a unique set of tools to control its operations. The following information describes the operations and tool sets for each tab.

Home Tab

The Home tab displays the Web GUI Dashboard, which can display SIP statistics through configurable widgets that you add and remove as needed. You can add up to 18 Widgets to the dashboard. The Home Tab displays and operates in the same way for both Basic Mode and Expert Mode. On the Home tab, you can:

- Refresh the page.
- Add a widget.
- Reset the display to the default.

The controls, displayed as text within each widget, allow you to:

- Refresh—Refresh the data in the Widget.
- Settings—Set the data sampling parameters for the Widget.
- Remove—Remove the Widget from the Dashboard.
- Maximize—Display the Widget in full screen size.
- Show Information—Display data in a graph or table.
- Collapse—Minimize a maximized Widget.
- Export—Download the data displayed in the Widget.

Basic Mode Configuration Tab

In Basic Mode, the Configuration tab displays the following buttons and links that display configuration controls:
Branding Bar

- Save—Save and activate the configuration.
- Verify—Confirm that the configuration is valid, before saving and activating.
- Settings—Configure system settings.
- Discard—Delete unsaved configuration changes.
- Switch to Expert—Change from Basic mode to Expert mode.
- Search—Search for objects and attributes.

Navigation Pane

- Wizards—Set boot parameters, Set Entitlements, Set initial configuration, Set License, Set Login Banner, Set Time Zone, and Upgrade software.
- Devices—Add a PBX, a Trunk, Remote Workers, a Device, a Recording Server, and a SIP Interface.
- Management—Configure Accounting, SNMP Community, Trap Receiver, and Web Server.
- Network—Configure the Host Route and the Network Interface.
- Others—Configure a Media Profile, SIP Features, SIP Manipulation, SPL, and Translation Rules.
- SBC—Configure Advanced Routing and a Web Server.

- Security—Configure a Certificate Record, an SDES profile, and a TLS profile.

Each group contains the same configuration objects and sub-objects as the ACLI. Clicking an object displays the corresponding configuration dialog.

Expert Mode Configuration Tab

In Expert Mode, the Configuration tab displays the Wizards and Commands objects along with lists of configuration objects, grouped in the same tree-like structure as those in the Acme Command Line Interface (ACLI). The configuration objects include:

- Media Manager
- Security
- Session Router
- System

Monitoring Tab

The Monitoring tab displays information about system activities by way of summaries and Widgets. Summaries are lists that you can only view on the Monitoring tab and Widgets are graphical or textual displays that you can view on the Monitoring tab and the Dashboard.

The **Monitor and Trace** link displays summaries of data that the system collects about:

- Notable Events
- Registrations
- Sessions
- Subscriptions

When data is present, by way of running SIP calls, the following controls become active:

- Search—Configure a search filter.
- Show all—Override the display filter and show all data.
- Ladder diagram—Displays data in a ladder diagram.
- Export session details—Save the detailed data to an external location.
- Export summary—Save a summary of the data to an external location.

The **Widgets** link is a portal to statistics about the system that 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. The Widgets operate in the same way for both Basic Mode and Expert Mode. You can view any widget on the Monitoring tab, and you can add up to 18 widgets to the Dashboard to quickly see the ones you use most often. The system provides the following groups of widgets, along with a placeholder for Favorites:

- System
- Media
- Signaling

System Tab

The System tab displays controls for managing, booting, and upgrading the system. The System Tab operates in the same way for both Basic Mode and Expert Mode.

- Force HA Switchover—Manually place the system in the standby state.
- Reboot—Manually reboot the system at any time.
- Support information—Generate a file that displays troubleshooting information that you can save and send to Oracle Customer Support.
- File management—Displays a list of file types and a set of controls to Refresh, Upload, Download, Backup, Restore, and Delete files.
- Set Boot Parameters—Use the Web GUI to set boot parameters, instead of the ACLI command line.
- Upgrade Software—Verify the health of the system software, for 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.

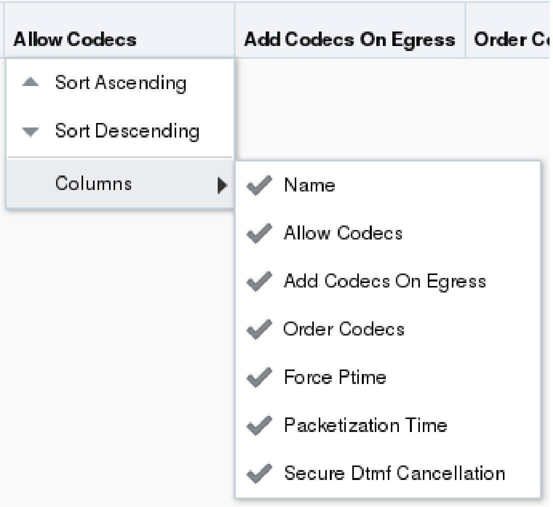
Customize the Page Display

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

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,

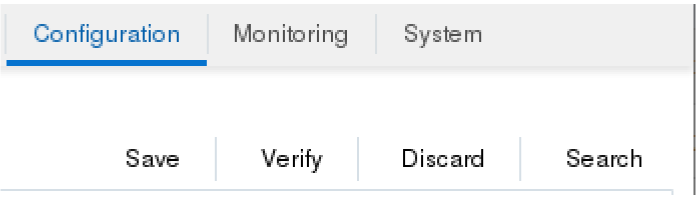


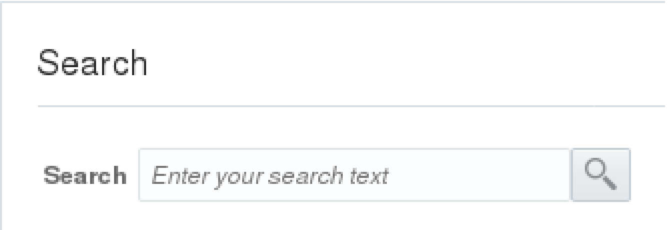
3. Select or deselect items, as needed.
4. Re-order the column headings by placing the cursor on a column heading and sliding it left or right into the location you want.

The Search Tool

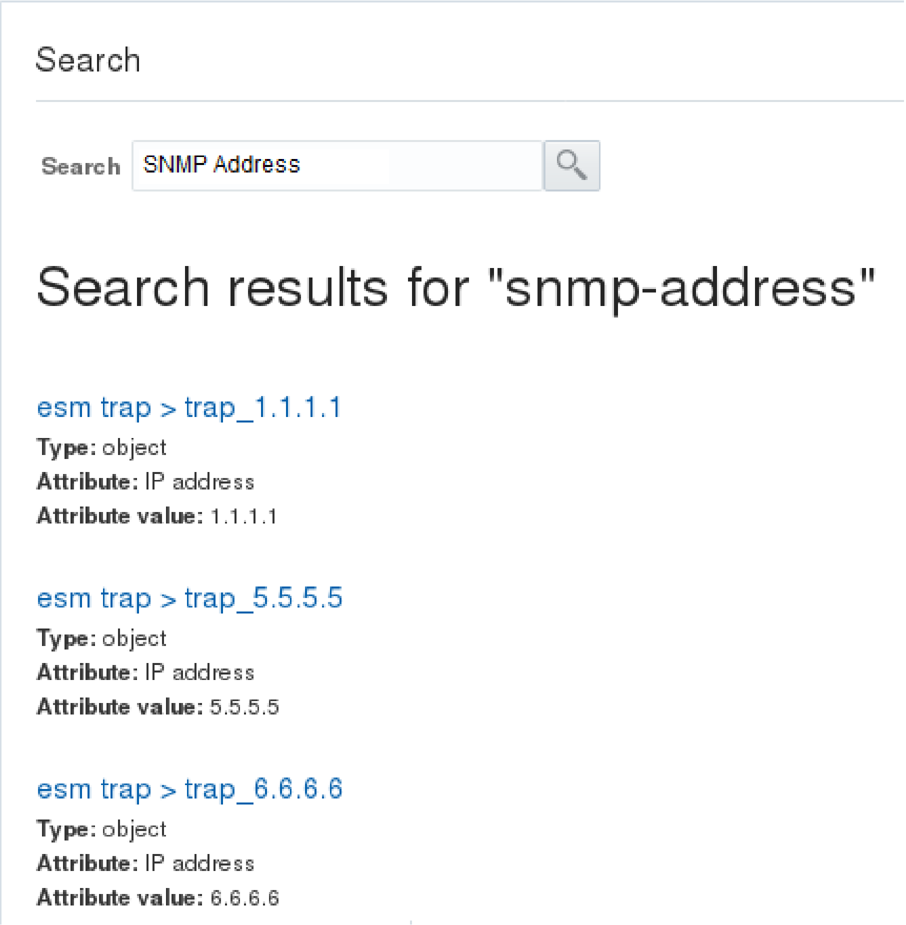
The Oracle® Enterprise Session Border Controller provides search operations for both system-wide and a configuration-specific objects.

The global Search button on the branding bar opens the Search text box where you enter the text to search for, such as an object name, an attribute, or value.





The resulting display includes links to the configuration object, for example:



Search SNMP Address

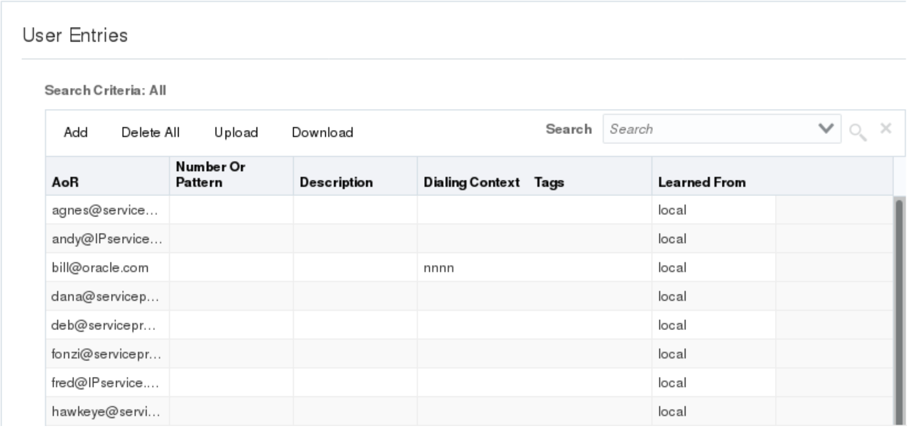
Search results for "snmp-address"

esm trap > trap_1.1.1.1
Type: object
Attribute: IP address
Attribute value: 1.1.1.1

esm trap > trap_5.5.5.5
Type: object
Attribute: IP address
Attribute value: 5.5.5.5

esm trap > trap_6.6.6.6
Type: object
Attribute: IP address
Attribute value: 6.6.6.6

Multi-instance configuration objects display a table of configurations and the table includes a text box for local search within the table.

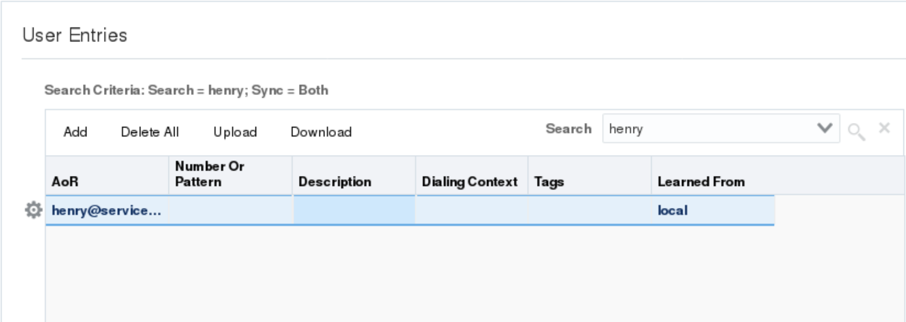


User Entries

Search Criteria: All

AoR	Number Or Pattern	Description	Dialing Context	Tags	Learned From
agnes@service...					local
andy@IPservice...					local
bill@oracle.com			nnnn		local
dana@servicep...					local
deb@servicepr...					local
fonzi@servicepr...					local
fred@IPservice....					local
hawkeye@servi...					local

The result of the search is displayed in the table. For example, searching for "henry" in the User Entries list above results in the display of henry's record, which you can edit, copy, or delete.



User Entries

Search Criteria: Search = henry; Sync = Both

Search: henry

AoR	Number Or Pattern	Description	Dialing Context	Tags	Learned From
henry@service...					local

2 Dashboard Tab Operations

The Oracle® Enterprise Session Border Controller (E-SBC) provides a web-based Dashboard that can display SIP data statistics to help you monitor and manage the system. 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, graph, table, web form, or text for the display, depending on the widget. You can 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
- Alarms

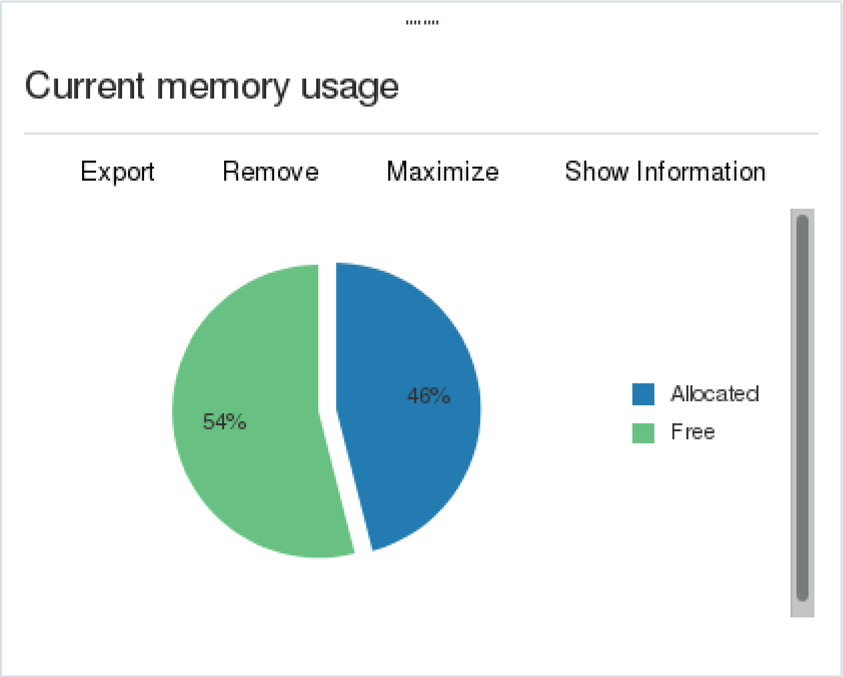
The Dashboard page provides the following controls to manage the widgets:

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 and removes all other widgets from the Dashboard.

Each widget contains the particular controls that you need to manage the widget. The controls display as text until you hover over one. Upon hover, the text becomes a button that you click to perform a task. The following screen capture shows Refresh as a button upon hover, while Settings, Export, Removed, and Maximize remain static text.



The controls that can display in a Widget include:

- Export—Download the data displayed in the Widget.
- Remove—Remove the Widget from the dashboard. When you remove all Widgets from the dashboard, the GUI displays the following message: " Your dashboard is empty, please add a widget or reset to restore the original dashboard."
- Settings—Set the data sampling parameters for the Widget.
- Maximize—Display the Widget in ful-screen size.
- Show Information—Display data in a graph or table.

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

You can add up to 18 widgets to the Web GUI Dashboard to display SIP and System statistics to help you monitor and manage the system.

The system does not require a re-boot after performing the following procedure.

1. On the Home page, click **Add Widget**.
2. On the **Add Widget** page, in the left pane, expand **Widgets**, and click the name of the Widget to add.

   The Web GUI displays the widget name in the center pane.
3. In the center pane, under **Command**, click **Add**.

   The system displays a success message.

> **Note:**
>
> If the system displays a warning that adding this widget requires enabling the SIP.Message module, the system enables the module when you add the widget.

4. Click **OK**.
5. Click **Close**.

   The system displays the newly added widget on the Dashboard right away.

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 display SIP and System statistics 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.

1. Click the **Home** tab.
2. On the Widget, click **Maximize**, and click **Settings**.
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**.
6. Click **Close**.

View A Widget That is Not on the Dashboard

The Dashboard is limited to displaying a maximum of 18 widgets. To see a widget that is not on the Dashboard, use the Widgets link on the Monitoring page to see a list of all of the Widgets.

Use the following procedure to view widgets that are not displayed on the Home page as Dashboard widgets.

1. Access Widgets: **Monitoring**, **Widgets**.
2. In the navigation pane, click a Dashboard Widget name.

   The system displays the Widget.
3. Optional—Add the widget to the Dashboard, if the Dashboard is not full.

3 Configuration Tab Operations

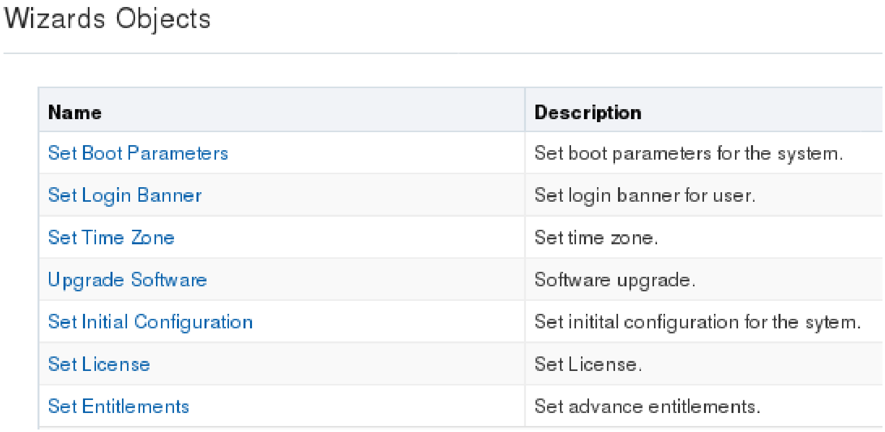
The Configuration tab on the Web GUI provides dialogs for the same configuration objects that you can access from the command line to configure the Oracle® Enterprise Session Border Controller (E-SBC). You may find the GUI easier to use than the command line.

The Web GUI provides the following configuration tools.

- Basic mode—Displays a limited set of configuration objects. Basic mode is used for quick prototyping of an E-SBC deployment for proof of concept or testing purposes. It is not meant for production use. You must switch to Expert mode to access the full array of configuration objects.

> **Note:**
>
> After switching to Expert Mode, you can only return to Basic mode if you have not saved and activated any changes that you made. After saving and activating, you must reinstall the software to enter Basic Mode again.

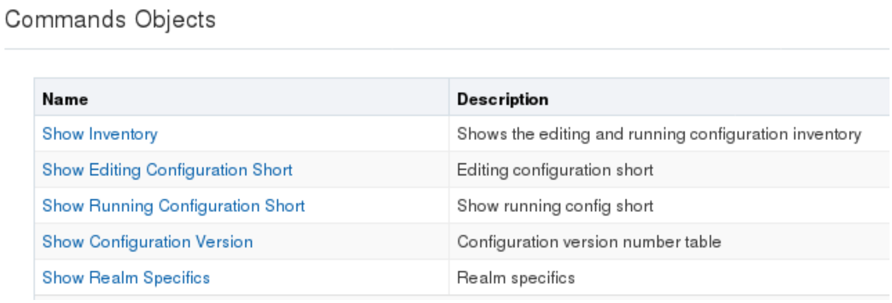
- Expert mode—Displays the complete list of the configuration objects. When you click an object on the list, the Web GUI displays the corresponding configuration dialog.
- Wizards—Displays the following list of Wizards that lead you through selected configuration tasks. You can use the Wizards in Basic mode and Expert mode.



Wizards Objects

Name	Description
Set Boot Parameters	Set boot parameters for the system.
Set Login Banner	Set login banner for user.
Set Time Zone	Set time zone.
Upgrade Software	Software upgrade.
Set Initial Configuration	Set initital configuration for the sytem.
Set License	Set License.
Set Entitlements	Set advance entitlements.

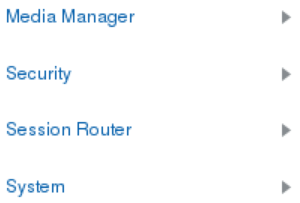
- Commands—Displays the following list of show commands that provide a view of the state of configuration on the E-SBC.



Commands Objects

Name	Description
Show Inventory	Shows the editing and running configuration inventory
Show Editing Configuration Short	Editing configuration short
Show Running Configuration Short	Show running config short
Show Configuration Version	Configuration version number table
Show Realm Specifics	Realm specifics

- Configuration objects—Displays a list of the configuration objects either by category, like the ACLI, or in alphabetical order. Use the arrow control to expand each list to see all of the configuration objects and sub-objects.



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.

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.

Severity	Identifies the level of severity that the Oracle Enterprise Session Border Controller assigns to the error. Valid values are: • ERROR—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. • WARNING—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. • CRITICAL—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.
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 Wizards

The Wizards control in the navigation pane displays a list of Wizards, for performing selected configuration procedures for the Oracle® Enterprise Session Border Controller (E-SBC).

The Wizards help you perform the following tasks:

Set Boot Parameters	Specify the boot file and the boot parameters.

Set Entitlements	Set the number of sessions that a license entitles you to, and enable advanced features.
Set Initial Configuration	Configure a new E-SBC or reconfigure an existing one. Includes configuring High Availability.
Set License	Enter the license number for a feature that requires a license.
Set Logon Banner	Customize the text on the Web GUI log on banner.
Set Time Zone	Select the time zone for the deployment.
Upgrade Software	Upload a newer 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.

1. Access the Set Boot Parameters Wizard: **Configuration**, **Wizards**, **Set Boot Parameters**.
2. In the Set Boot Parameters dialog, enter the following information:

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.
IPv6 Address	Enter the IPv6 address that you want to use.
IPv6 Gateway	Enter the IPv6 gateway that you want to use.
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.
Other	For miscellaneous and deployment-specific boot settings.

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:

- 0x04 - disables autoboot timeout (ap3820 and ap4500 only)
- 0x08 - extend autoboot countdown timer to 15 seconds
- 0x40 - use DHCP for wancom0 (VM Edition only)
- 0x80 - network boot using TFTP instead of FTP

Set Entitlements Wizard

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

- 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.

1. Access the Set Entitlements Wizard: **Configuration**, **Wizards**, **Set Entitlements**.
2. In the Set Entitlements dialog, do the following:

Advanced	Select to add the Advanced license.
Admin Security	Select to enable your Admin Security license.
Data Integrity (FIPS 140 2)	Select to enable FIPS 140 2 data integrity.
Transcode Codec AMR	Select to enable AMR transcoding.
Transcode Codec AMRWB	Select to enable AMRWB transcoding.
Transcode Codec EVS	Select to enable EVS transcoding.
Session Capacity	Set the session limit number from the license. Valid values: 0-512000
Transcode Codec AMR Capacity	Set the transcoding capacity for AMR. Valid values: 0-102375.
Transcode Codec AMRWB Capacity	Set the transcoding capacity for AMRWB. Valid values: 0-102375.
Transcode Codec EVS Capacity	Set the transcoding capacity forEVS. Valid values: 0-102375.
Transcode Codec Opus Capacity	Set the transcoding capacity for Opus. Valid values: 0-102375.
Transcode Codec SILK Capacity	Set the transcoding capacity for SILK. Valid values: 0-102375.

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.

Enable Web GUI: Yes or No	If you select **No**, 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 **Web Server Config** object from the ACLI.
Choose Web GUI Mode: Basic or Expert	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. • 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 **Save**, you cannot switch back to Basic Mode. The Web GUI will display the Expert Mode from then on, including after a new log on. • 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.
E-SBC Mode: Standalone or High Availability	• If you select Standalone, you can begin configuring the parameters displayed.

	• If you select High Availability, the GUI adds E-SBC Role: Primary/Secondary to the display.
E-SBC Role: Primary or Secondary	If you selected High Availability for E-SBC Mode: 1. Select Primary, and configure the displayed parameters. 2. Select Secondary, and select **Yes** or **No** for Acquire Configuration from Primary. If you select **No**, the GUI adds a field where you enter the Peer Target Name.

> **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.

Configure the System

The system requires an initial configuration of attributes, such as modes and IP addresses, before it can function in the network.

Use the Set Initial Configuration Wizard to define the attributes for the system. The system displays the Set Initial Configuration Wizard upon the first logon.

1. Logon to the Oracle® Enterprise Session Border Controller.

   The system displays the Set initial configuration wizard.

2. Run the Set Initial Configuration Wizard, and click **Complete**.

   The system saves the configuration, activates the configuration, and re-boots.

- Configure the system objects.

Reconfigure the System

You can reconfigure the system from the Web GUI.

Use the Set Initial Configuration Wizard to change the initial configuration on a configured system, for example, change attributes such as IP addresses and modes.

1. Log on to the system.
2. Access the Set Initial Configuration Wizard: **Configuration**, **Wizards**, **Set Initial Configuration**.
3. Run the Set Initial Configuration Wizard and change the attributes, as needed.
4. Click **Complete**.

The system saves a backup of the existing configuration, saves the new configuration, activates the new configuration, and automatically re-boots.

- (Optional) Reconfigure the system objects.

Set License Wizard

Use the Set License Wizard to enter the serial number for your license. You can use the Set License Wizard in Basic Mode and Expert Mode.

- 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 need the license number for the following procedure.

1. Access the Set License Wizard: **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 Login Banner Wizard

Use the Set Login Banner Wizard to add customized text to the log on page. You can use the Set Login Banner Wizard in Basic mode and Expert Mode.

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

1. Access the Set Login Banner Wizard: **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). You can use the Set Time Zone Wizard in Basic Mode and Expert Mode.

1. Access the Set Time Zone Wizard: **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. You can use the Upgrade Software Wizard in Basic Mode and Expert Mode.

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.

1. Access the Upgrade Software Wizard: **Wizards**, **Upgrade Software** .
2. (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.
3. In the Upgrade Software dialog, do the following:

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.

4. 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.
5. Click **OK**.

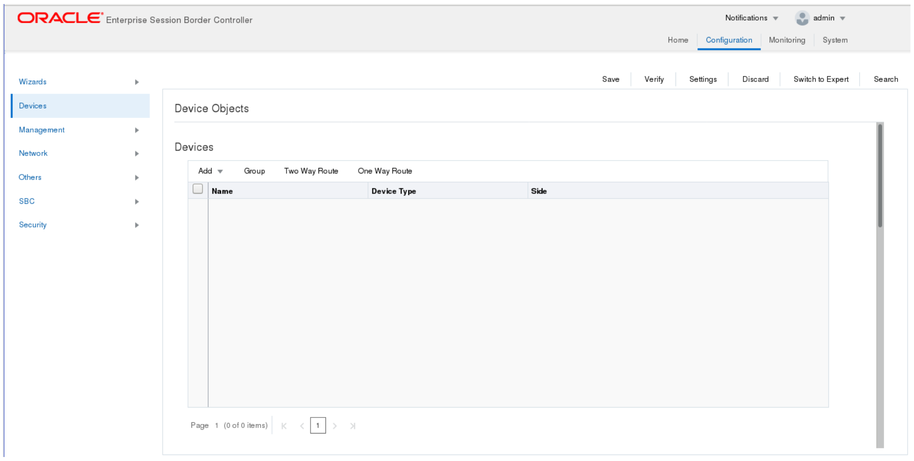
    The system performs the file transfer and any boot parameter changes. If you selected **Reboot After Update**, the system reboots.

Configuration in Basic Mode

The Oracle® Enterprise Session Border Controller (E-SBC) Web GUI displays both a Basic Mode and an Expert Mode for configuring the system. Basic Mode provides a subset of the Expert Mode configuration objects, and is intended for use as a quicker way to configure the E-SBC for proof-of-concept and testing purposes. Basic Mode provides only the minimum number of configuration objects required to get the system up and processing calls. After you are satisfied with system operations, you can switch to Expert Mode and continue to specify a more robust and customized configuration.

The E-SBC preserves the settings that you applied in Basic Mode and displays them in the corresponding dialogs in Expert Mode along with the additional settings available in Expert Mode. Using Basic Mode is optional. You can configure the E-SBC from start to finish in Expert Mode.

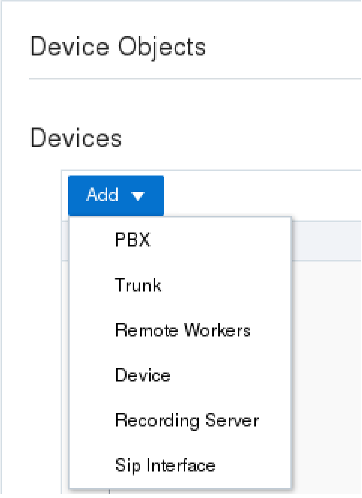
> **Note:**
>
> After you switch to Expert Mode, you can only switch back to Basic Mode if you have not saved and activated in Expert Mode.



Basic Mode configuration requires connecting the E-SBC to your network and setting the parameters for the operations that you want the E-SBC to perform. In Basic Mode, the Configuration tab displays a drop down list of possible devices that you can connect and a list of configuration objects. You can also group devices and establish one-way and two-way routes between each one and the E-SBC.

Connect to the Network

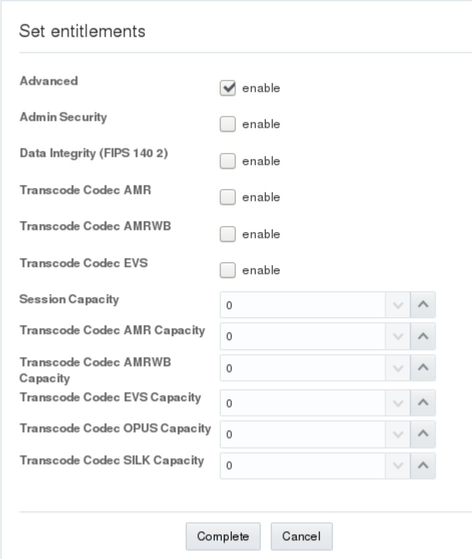
When you first click the Configuration tab in Basic Mode, the center pane displays the following list of "Devices" that you can connect to the E-SBC.



When you click a device, the GUI displays the corresponding configuration dialog. After you configure the device, click SIP Interface on the Devices list. The system prompts you specify whether you want the configured device on the Enterprise side or the Service Provider side of the E-SBC. When you complete the SIP Interface configuration, you can set one-way or two-way routes for traffic to and from the device to the E-SBC. You can also group devices.

Example 3-1 Set the Parameters

On the Configuration tab, the navigation panel lists all of the configuration objects that you need for the E-SBC in Basic Mode. Some objects, such as Set Entitlements, launch a configuration dialog directly because they are single-instance configurations. Such dialogs display a list of parameters that you can set. For example:

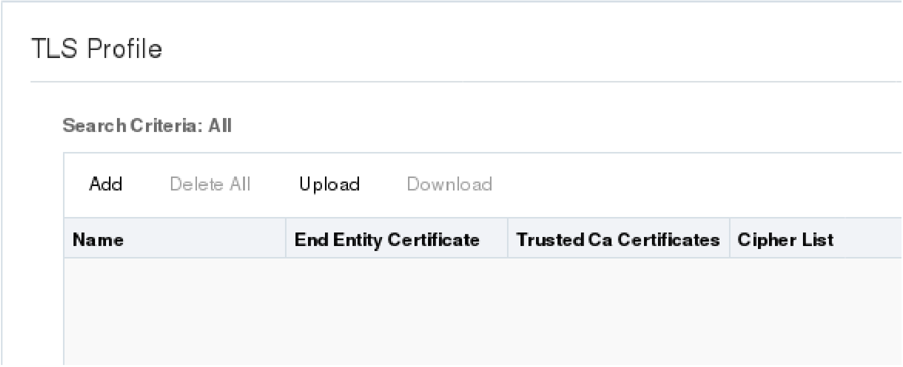


Set entitlements

Advanced	☑ enable
Admin Security	☐ enable
Data Integrity (FIPS 140 2)	☐ enable
Transcode Codec AMR	☐ enable
Transcode Codec AMRWB	☐ enable
Transcode Codec EVS	☐ enable
Session Capacity	0
Transcode Codec AMR Capacity	0
Transcode Codec AMRWB Capacity	0
Transcode Codec EVS Capacity	0
Transcode Codec OPUS Capacity	0
Transcode Codec SILK Capacity	0

When you complete the configuration, the dialog closes and displays the landing page for the object.

Other configuration objects, such as TLS Profile, are multi-instance objects that launch a page that can display a list of the configured objects. Such objects display the **Add** button and a table for listing configurations. For example:

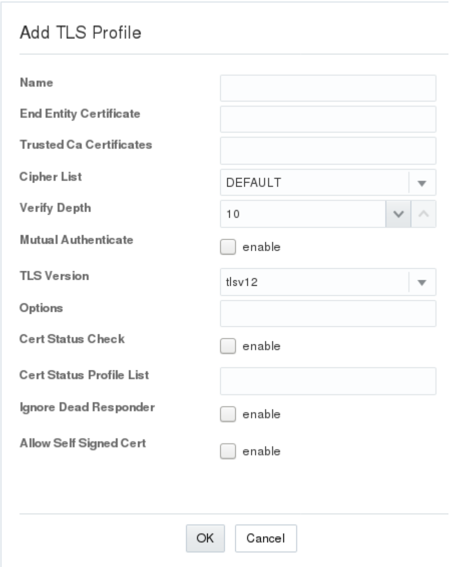


TLS Profile

Search Criteria: All

Name	End Entity Certificate	Trusted Ca Certificates	Cipher List

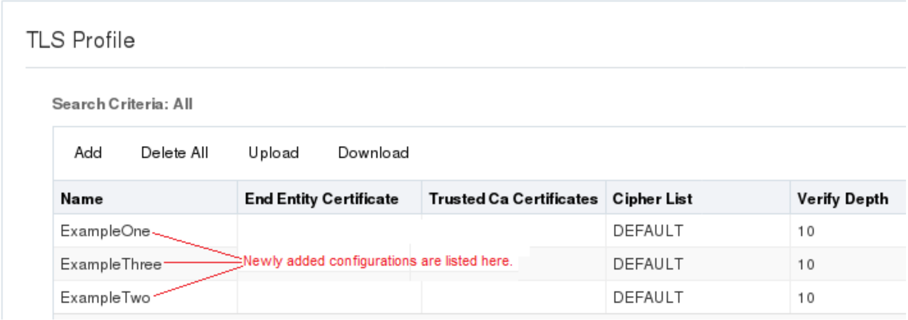
When you click **Add** on such a page, the Web GUI launches the configuration dialog. For example:



Add TLS Profile

Name	
End Entity Certificate	
Trusted Ca Certificates	
Cipher List	DEFAULT
Verify Depth	10
Mutual Authenticate	□ enable
TLS Version	tlsv12
Options	
Cert Status Check	□ enable
Cert Status Profile List	
Ignore Dead Responder	□ enable
Allow Self Signed Cert	□ enable

When you **OK** the configuration dialog, the system returns to the Configuration object list page and adds the new configuration to the list. For example:



TLS Profile

Search Criteria: All

Name	End Entity Certificate	Trusted Ca Certificates	Cipher List	Verify Depth
ExampleOne			DEFAULT	10
ExampleThree			DEFAULT	10
ExampleTwo			DEFAULT	10

Newly added configurations are listed here.

Repeat the process to add more configurations to the list.

Basic Mode Configuration Controls

In Basic mode, the Configuration page displays the following controls that lead to the listed configuration dialogs.

Branding Bar

The branding bar displays the following controls:

Save	Perform a verification and save the changes to the non-volatile memory. You must activate the changes before the system can apply them to the running configuration. If the configuration contains errors, the Web GUI displays them along with a dialog where you can confirm or cancel activating the changes.
Verify	Confirm that a configuration is valid before you save your changes.
Settings	Access the following settings: • Hostname and default gateway

	• NTP IP address • Enable restart on critical failure • Logging settings • SNMP settings • SIP settings • Denial of Service settings • Communications monitoring probe settings • High availability settings • Packet capture settings • Survivability
Discard	Undo any changes that you made and revert to the previous configuration.
Switch to Expert	Change to the Expert Mode to see more configuration objects than Basic Mode provides. **Note:** After switching to Expert Mode, you can only return to Basic Mode if you have not saved and activated any changes that you made. After saving and activating in Expert Mode, you must reinstall the software to enter Basic Mode again.
Search	Use to find one or more configuration objects. For example, if you type "host," the GUI displays a list of every configuration object that contains "host."

Navigation Pane

The Basic Mode navigation tree displays the configuration objects in the following groups.

Wizards	• Set Boot Parameters • Set Entitlements • Set Initial Configuration • Set License • Set Login Banner • Set Time Zone • Upgrade Software
Devices	• PBX

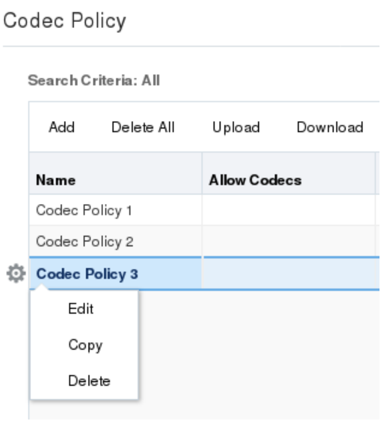
	• Trunk • Remote Workers • Device • Recording Server • SIP Interface
Management	• Accounting • SNMP Community • Trap Receiver • Web Server
Network	• Host Route • Network Interface
Others	• Media Profile • SIP Features • SIP Manipulation • SPL • Translation Rules
SBC	• Advanced Routing • Web Server
Security	• Certificate Record • SDES Profile • TLS Profile

Edit, Copy, and Delete Configurations

You can edit, copy, and delete one or more multi-instance configurations on the Oracle® Enterprise Session Border Controller (E-SBC) by way of the controls that the Web GUI displays on the Configuration tab. The edit and copy functions act only on a single instance of a configuration. The delete function can act on either a single instance or all instances.

> **Note:**
>
> You cannot copy or delete single-instance configurations. You can only edit them.

To edit, copy, or delete a single, multi-instance configuration, select the configuration and right-click. The Web GUI displays the Edit, Copy, and Delete menu.



- When you click Delete, the system displays a confirmation dialog before performing the operation.
- When you click either Copy or Edit, the GUI displays the corresponding configuration dialog.

To delete all configurations at the same time, use Delete All.

> **Caution:**
>
> Delete All does not act on a partial selection of the configurations. For example, if you select two of three configurations and click Delete All, the system deletes all three.

Settings Configuration

Use the Settings configuration to set the following parameters.

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. • SysLog Server IP Address • Process Log Level Default: Notice. Valid values: Critical | Debug | Info | Minor | Notice | Trace | Warning.

SNMP Settings	Enable SNMP traps and specify the MIB system. • MIB System Contact • MIB System Name • MIB System Location • Enable Event SNMP Traps
SIP Settings	Configure SIP and add SIP options. • Enable Dialog Transparency. Default: Enabled. • Maximum SIP Message Length. Default: 4096. Range: 0-65535. • Allow SIP UDP Fragmentation. Default: Enabled. • Set INVITE Expires at 100 Response. Default: Disabled.
Denial of Service Settings	Specify packet rate settings for Denial of Service protection. • Maximum Trusted Packet Rate. Default: 50000. Range: 20-200000. • Maximum Untrusted Packet Rate. Default: 50000. Range: 20-200000. • Maximum ARP Packet Rate. Default: 1000. Range: 20-10000.
Communications Monitoring Probe Settings	Enable the Communications Monitoring Probe and specify the collector. • Enable Monitoring. Default: Disabled. • SBC Group ID. Default: 0. Range: 0-999999999. • Network Interface: Default: SP0. • Collector IP Address. Default: 0.0.0.0. • Collector Port: Default: 4739. Range: 1025-65535.
High Availability Settings	Enable High Availability and specify the peers. • Enable High Availability • Name of Primary Peer • Name of Secondary Peer • ENT Phy Interface Virtual MAC • SP Phy Interface Virtual MAC For the Acme Packet 1100, see "High Availability for the Acme Packet 1100."
Packet Capture Settings	Enable packet capture and specify the receiver. • Enable Packet Capture. Default: Disabled. • Capture Receiver Network Interface

	• Capture Receiver IP Address. Default: 0.0.0.0. • SBC Platform
Survivability	Enable remote site survivability and specify the triggering device. • State: Default: Disabled. • Registration Expire Time • Extension Length • Trigger On

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.

- 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.

1. Access the Settings configuration object: **Configuration**, **Settings**.
2. On the Settings page, click **Logging Settings**, and do the following:

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. Default: Notice. Valid values: Critical | Debug | Info | Notice | Minor | Trace |Warning.

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.

- 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.

1. Access the Settings configuration object: **Configuration**, **Settings**.
2. In the Settings dialog, click **SNMP Settings**, and do the following:

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 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). You can use the protocol 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 cannot generate a unique Call-ID and from modifying the dialog tags. The E-SBC 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 signaling 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 are not reassembled and are forwarded to the egress interface instead.

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

Oracle recommends that you send large SIP INVITE messages 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.

- Confirm that the system displays the Basic mode.

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

1. Access the Settings configuration object: **Configuration**, **Settings**.
2. On the Settings page, click **SIP Settings**, and do the following.

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.
SIP Options	Enter one or more SIP options.

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

- 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.

- Plan the maximum number of packets per second that you want for trusted packets, un-trusted 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.

1. Access the Settings configuration object: **Configuration**, **Settings**.
2. On the Settings page, click **Denial of Service Settings**, and do the following.

Maximum Trusted Packet Rate	Maximum bandwidth for trusted hosts packets per second. Default 50000. Range: 20-200000.
Maximum Entrusted Packet Rate	Maximum bandwidth for un-trusted hosts in 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 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 exports protocol message traffic and data and the Palladion Mediation Engine collects the information.

- 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 ths function, and to specify the connection parameters.

1. Access the Settings configuration object: **Configuration**, **Settings**.

2. On the Settings page, click **Communications Monitoring Probe Settings**, and do the following:

Enable Monitoring	Select to enable.
SBC Group ID	Enter a number to assign to the E-SBC in its role as an information exporter. Default: 0. 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 Operations Monitor Mediation Engine. Default: 0.
Collector IP Address	Enter the IP address of the Operations Monitor Mediation Engine collector. Default: 0.0.0.0.
Collector Port	Enter the number of the Operations Monitor Mediation Engine collector port. Default: 4739. Range: 1025-65535.

3. Click **OK**.
4. Save 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.

When two E-SBCs work together in an HA node, one operates in active mode and the other one operates 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.
- 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 standbyE-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.

In the HA node, the E-SBCs advertise their current state and health to one another in checkpointing messages so that 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 health score of the active E-SBC has decreased to an unacceptable level.
- The active E-SBC relinquishes the active role.

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 active and the other E-SBC as the standby.

- 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.

1. Access the Settings configuration object: **Configuration**, **Settings**.
2. On the Settings page, click **High Availability Settings**, and do the following:

Enable High Availability	Select to enable HA.
Name of Primary Peer	Enter the name of the active E-SBC peer.
Name of Secondary Peer	Enter the name of the standby 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 the configuration.

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 Active Acme Packet 1100 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.

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

You must perform the following procedure on the active system before configuring the standby system for HA operations.

1. Access Run Setup: **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:

Enable Web GUI	Select **Yes** to enable the Web GUI.
Choose Web GUI Mode	Select **Basic Web GUI** mode.
SBC Mode	• Select **high availability** SBC mode. • Select primary.
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 re-boots.

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

Configure the Standby Acme Packet 1100 for HA

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

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

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

1. Access Run Setup: **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:

Enable Web GUI	Select **Yes** to enable the Web GUI.
Choose Web GUI Mode	Select **Basic Web GUI** mode.
SBC Mode	• Select **High Availability** SBC mode. • Select secondary.
IP Address on Management Interface	Enter the IP address of the management interface of the secondary.
Unique Target Name	Enter a unique target name for the secondary.
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 **Yes**.

3. Click **Complete**

   The system re-boots.

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.

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.	• If the /opt/traces directory contains 25 .pcap files, the system cannot add more files to the directory or overwrite the existing files.

	- 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.

Configure Packet Capture Settings

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

- Note the IP address and network interface of the device that you want the E-SBC to 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.

1. Access the Settings configuration object: **Configuration**, **Settings**.
2. Under Packet Capture Settings, do the following:

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.
SBC Platform	

3. Click **OK**.
4. Save 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.

- Confirm that at least one session is configured.

The Web GUI displays the Survivability configuration parameters on the Settings page. Use the following procedure to enable remote site survivability, specify a triggering device, and optionally change the default settings.

1. Access the Settings configuration object: **Configuration**, **Settings**.
2. Under Survivability, do the following:

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
Trigger On	Select the PBX, Trunk, device, or group from the drop-down list that you want to trigger survivability mode when it goes out of service.

Devices Configuration

Use Devices to access the following configuration objects.

PBX	Configure a privately owned switching system for handling multiple telephone lines. See "Add a PBX."
Trunk	Configure IP communications through your PBX outside of your Enterprise network on an Internet connection. See "Add a Trunk."
Remote Workers	Configure a device set up outside your network, but connects to the Oracle® Enterprise Session Border Controller from a remote location. See "Add Remote Workers."

Device	Configure a network device in the Local Area Network. See "Add a Device."
Recording Server	Configure a third-party call recorder or the Oracle ISR Record and Store Server to record media transmitted during a communications session between multiple user agents. See "Add a Recording Server."
SIP Interface	Add a SIP network interface to the Enterprise side of the Oracle® Enterprise Session Border Controller. See "Add a SIP Interface."

Add a PBX

You can perform the minimum configuration needed to connect a PBX to the Oracle® Enterprise Session Border Controller (E-SBC) from the Configuration tab in Basic mode.

- Configure inbound and outbound translation rules.
- Note any System Programming Language (SPL) options that you want to add.
- Confirm that the system displays the Basic mode.

1. Access the PBX configuration object: **Configuration**, **Devices**, **Add**, **PBX**.

   The system displays the Add PBX dialog.

2. In the Add PBX dialog, do the following:

PBX name	Enter the name to assign to this PBX in the Enterprise network. For example, PBX1. Valid values: Alpha-numeric characters.
Description	Enter a description for this PBX. For example, PBX for Enterprise. Valid values: Alpha-numeric characters.
Hostname	Enter the hostname of the Oracle® Enterprise Session Border Controller to which this PBX is connected. For example, SBC1. Valid values: Alpha-numeric characters.
IP Address	Enter the IP address of this PBX in dotted decimal format. For example, 1.1.1.1. Default is 0.0.0.0.
IP Port	Enter the IP port for this PBX. Default: 5060. Range: 1025-65535.
Enable Refer Call Transfer	Select to enable. Default: Disabled.
Enable SIP Monitoring and Tracing	Select to enable. Default: Disabled.
Maximum Sessions	Enter the maximum number of concurrent sessions. Default: 0. Range: 0-999999999,
Maximum Inbound Sessions	Enter the maximum number of concurrent inbound sessions. Default: 0. Range: 0-999999999,

Maximum Outbound Sessions	Enter the maximum number of concurrent outbound sessions. Default: 0. Range: 0-999999999,
Enable Connectivity Check	Select to enable. Default: Disabled.
Connectivity Check Interval	Enter the connectivity check interval. Default 30. Range: 0-9999.
Connectivity Check Method	Select a connectivity check method from the drop-down list.
Inbound Manipulation	Select inbound manipulation from the drop-down list.
Outbound Manipulation	Select outbound manipulation from the drop-down list.
Inbound Translation Rules	Click the field and select a rule from the list.
Outbound Translation Rules	Click the field and select a rule from the list.
Trust Mode	Select a trust level from the drop-down list.
Invalid Message Threshold	Enter the invalid message threshold. Default: 0. Range: 0-9999.
Maximum Message Threshold	Enter the maximum message threshold. Default: 0. Range: 0-9999.
SPL Options	Enter the name of the SPL option.

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

- Configure the Trunk.

Add a Trunk

You can perform the minimum configuration needed to make connect a SIP Trunk to the Oracle® Enterprise Session Border Controller (E-SBC) from the Configuration tab in Basic mode.

- Configure inbound and outbound translation rules.
- Note any System Programming Language (SPL) options that you want to add.
- Confirm that the system displays the Basic mode.

1. Access the Trunk configuration object: **Configuration**, **Devices**, **Add**, **Trunk**.

   The system displays the Add SIP Trunk dialog.
2. In the Add SIP Trunk dialog, do the following:

Trunk Name	Enter the name to assign to this SIP Trunk in the Service Provider network. For example, SIPT1. Valid values: Alpha-numeric characters.

Description	Enter a description for this SIP Trunk. For example, SIP Trunk for Service Provider. Valid values: Alpha-numeric characters.
Hostname	Enter the hostname of the Oracle® Enterprise Session Border Controller, to which this SIP Trunk is connected. For example, SBC1. Valid values are alpha-numeric characters.
IP Address	Enter the IP address of this SIP Trunk in dotted decimal format. For example, 1.1.1.1. Default: 0.0.0.0.
IP Port	Enter the IP port for this SIP Trunk. Default: 5060. Range: 1025-65535.
Enable SIP Monitoring and Tracing	Select to enable.
Maximum Sessions	Enter the maximum number of concurrent sessions. Range: 0-999999999.
Maximum Inbound Sessions	Enter the maximum number of concurrent inbound sessions. Range: 0-999999999.
Maximum Outbound Sessions	Enter the maximum number of concurrent outbound sessions. Range: 0-999999999.
Enable Connectivity Check	Select to enable.
Connectivity Check Interval	Enter the connectivity check interval. Default 30. Range: 0-9999.
Connectivity Check Method	Select a connectivity check method from the drop-down list.
Inbound Manipulation	Select inbound manipulation from the drop-down list.
Outbound Manipulation	Select outbound manipulation from the drop-down list.
Inbound Translation Rules	Click the field and select a rule from the list.
Outbound Translation Rules	Click the field and select a rule from the list.
Trust Mode	Select a trust level from the drop-down list.
Invalid Message Threshold	Enter the invalid message threshold. Default: 0. Range: 0-9999.
Maximum Message Threshold	Enter the maximum message threshold. Default: 0. Range: 0-9999.
SPL Options	Enter the name of the SPL option.

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

- Configure optional network elements, such as Time Division Multiplexing (TDM), additional devices, a recording server, or remote workers.
- Configure routing policies.

Add a Remote Worker

A remote worker is a device that you set up outside of your network, which you connect to the Oracle® Enterprise Session Border ControllerE-SBC) from the remote location.

1. Access the Remote Worker configuration object: **Configuration**, **Devices**, **Add**, **Remote Workers**.
2. In the Add Remote Worker dialog, do the following:

Name	Enter a name for this remote worker. Valid values: Alphanumeric characters.
Description	(Optional) Enter a description of this remote worker.

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

Add a SIP Device

- Configure inbound and outbound translation rules.
- Note any System Programming Language (SPL) options that you want to add.
- Confirm that the system displays the Basic mode.

1. Access the SIP Device configuration object: **Configuration**, **Devices**, **Add**, **Device**.

   The system displays the Add device dialog.
2. In the Add device dialog, do the following:

Device name	Enter the name to assign to this device in the Enterprise network. For example, device1. Valid values: Alpha-numeric characters.
Description	Enter a description for this device. For example, device for Enterprise. Valid values: Alpha-numeric characters.
Hostname	Enter the hostname of the Oracle® Enterprise Session Border Controller to which this device is connected. For example, SBC1. Valid values: Alpha-numeric characters.
IP Address	Enter the IP address of this device in dotted decimal format. For example, 1.1.1.1. Default is 0.0.0.0.
IP Port	Enter the IP port for this device. Default: 5060. Range: 1025-65535.

Enable Refer Call Transfer	Select to enable. Default: Disabled.
Enable SIP Monitoring and Tracing	Select to enable. Default: Disabled.
Maximum Sessions	Enter the maximum number of concurrent sessions. Default: 0. Range: 0-999999999.
Maximum Inbound Sessions	Enter the maximum number of concurrent inbound sessions. Default: 0. Range: 0-999999999.
Maximum Outbound Sessions	Enter the maximum number of concurrent outbound sessions. Default: 0. Range: 0-999999999.
Enable Connectivity Check	Select to enable. Default: Disabled.
Connectivity Check Interval	Enter the connectivity check interval. Default 30. Range: 0-9999.
Connectivity Check Method	Select a connectivity check method from the drop-down list.
Inbound Manipulation	Select inbound manipulation from the drop-down list.
Outbound Manipulation	Select outbound manipulation from the drop-down list.
Inbound Translation Rules	Click the field and select a rule from the list.
Outbound Translation Rules	Click the field and select a rule from the list.
Trust Mode	Select a trust level from the drop-down list.
Invalid Message Threshold	Enter the invalid message threshold. Default: 0. Range: 0-9999.
Maximum Message Threshold	Enter the maximum message threshold. Default: 0. Range: 0-9999.
SPL Options	Enter the name of the SPL option.

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

- Configure the Trunk.

Add a Session Recording Server

A session recording server is either a third-party call recorder or the Record and Store Server on the Oracle® Enterprise Session Border Controller (E-SBC) for recording the media transmitted in session between multiple user agents.

1. Access the Session Recording Server configuration object: **Configuration**, **Devices**, **Recording Server**, **Add**.
2. On the Add Session Recording Server page, do the following:

Recording Server Name	Enter the name to assign to this recording server. Valid values: Alpha-numeric characters.
Description	Enter a description for this recording server. Valid values: Alpha-numeric characters.
IP Address	Enter the IP address of this recording server in dotted decimal format. For example, 1.1.1.1. Default is 0.0.0.0.
IP Port	Enter the IP port for this recording server. Default: 5060. Range: 1025-65535.

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

Configure a SIP Interface

You can add up to five SIP interfaces to both the Enterprise side and the Service Provider side of your Oracle® Enterprise Session Border Controller (E-SBC). You can associate a SIP interface with any configured network interface.

- Create the TLS profile that you want to associate with each SIP interface that you configure.
- Create the SDES profile that you want to associate with each SIP interface that you configure.
- Configure the Session Recording Server that you want to associate with this each SIP interface that you configure.

Use the following procedure to configure a SIP interface for either the Enterprise side or the Service Provider side of the E-SBC. In the configuration process, you specify which side. Repeat the procedure for each additional SIP interface that you need.

The following list is a basic set of the available parameters. For the complete list of available parameters, see the *ACLI Reference Guide*. For more configuration instructions, see the *ACLI Configuration Guide*.

1. Access the SIP Interface configuration object: **Configuration**, **Devices**, **Add**, **SIP Interface**.

   The Web GUI displays the **Choose Side** dialog.
2. In the **Choose Side** dialog, click either Enterprise or Service Provider.

   The Web GUI displays the Add SIP Interface configuration page.
3. In the Add SIP Interface configuration, do the following:

Interface Name	Enter the name to assign to this SIP Interface. Valid values: Alpha-numeric characters.
Description	Enter a description of this interface.
Network Interface	
IP Address	Enter the IP address of this SIP interface in dotted decimal format. For example, 1.1.1.1. Default: 0.0.0.0.

SIP Port	Enter the SIP port for this SIP interface. Default: 5060. Range: 1025-65535.
IP Transport	Select an IP transport protocol from the drop-down list. Default: UDP. Valid values: UDP | TCP | TLS.
TLS Profile	Select a TLS profile from the drop-down list that you want to associate with this interface.
Allowed Requests From	Default: Agents Only. Valid Values: Agents Only | Registered | All.
Enable Registration Caching	Select to enable registration caching for all User Agents, not just ones behind a Network Address Translation. Default: Disabled.
Registration Interval	Set the registration entry interval, in seconds, for a non-HNT endpoint. Default: 3600 seconds. Range: 0-7200.
Enable Routing All Calls to Registrar	Select to enable routing calls to the registrar. Default: Enabled.
Transfer Calls on REFER	Select to enable transferring calls on REFER. Default; Disabled.
Allowed SIP Methods	Add one or more SIP methods that you want to allow. Valid values: INVITE | REGISTER | PRACK | OPTIONS | INFO | SUBSCRIBE | NOTIFY | REFER | UPDATE | MESSAGE | PUBLISH.
Media Start Port	Enter the number of the starting media port. Default: 10000. Range: 1-65535.
Media End Port	Enter the number of the ending media port. Default: 20000. Range: 1-65535.
Enable RFC2833 Payload Type	Select to enable RFC2833 payload type. Default: Disabled.
Enable Media Release in Network Interface	Select to enable the release of media for specific call flows between SIP peers or realms on two network interfaces of the same E-SBC, regardless of the attached media topology . Default: Disabled.
Enable Symmetric Latching	Select to enable Symmetric Latching for the RTP/RTCP flow. Default: Disabled.
Enable QoS	Select to enable QoS reporting. Default: Disabled.
Allowed Codecs	Enter one or more codecs that you want to allow.
Add Codes on Egress	Enter one or more codecs to add on egress.
Order Codecs	
Force Ptime	Select to enable setting a forced packetization time on egress. Default: Disabled.
Packetization Time	Set the media packetization time in milliseconds. Default: ? Range: ?

DTMF in Audio	Specify how to handle DTMF in the audio stream. Default: Disabled. Valid values: Disabled | Dual | Preferred.
Enable Media Security	Select to enable the media security policy that specifies the role of the E-SBC in the security negotiation. Default: Disabled.
SDES Profile	Select an SDES profile from the drop-down list that you want to associate with this interface.
Media Security Mode	Select a media security mode for Real-Time Transport Protocol from the drop-down list. Default: RTP. Valid values: RTP | SRTP | Any (means either RTP or SRTP).
Media Security Protocol	Select a media security protocol from the drop-down list.
Enable ToS Marking Rewrite	Select to enable ToS marking re-write.
ToS Value for Audio Packets	Set the ToS value for audio packets.
ToS Value for SIP Packets	Set the ToS value for SIP packets.
Inbound Manipulation	Select inbound manipulation from the drop-down list.
Outbound Manipulation	Select outbound manipulation from the drop-down list.
Inbound Translation Rules	Click the field and select a rule from the list.
Outbound Translation Rules	Click the field and select a rule from the list.
Trust Mode	Select a trust level from the drop-down list. Default; None. Valid values: None | Low | Medium | High.
Invalid Message Threshold	Enter the invalid message threshold. Default: 0. Range: 0-9999.
Maximum Message Threshold	Enter the maximum message threshold. Default: 0. Range: 0-9999.
Untrusted Message Threshold	Enter the untrusted message threshold. Default: 0. Range: 0-9999.
Deny Period	Default: 0. Range: 0-7200.
Session Recording Server	Select a Session Recording Server from the drop-down list.
Session Recording Mandatory	Select to make session recording mandatory.
SIP Options	Enter a list of SIP options that you want.

Management Configuration

Use the Management control to access the following configuration objects.

Accounting	Specify call accounting strategy, protocol, receivers, servers, parameters, and options. See the *Accounting Guide* and the "RADIUS Authentication" and "TACACS+" sections of Getting Started" in the *ACLI Configuration Guide*.
SNMP Community	Add and specify one or more Simple Network Management Protocol (SNMP) communities. See "SNMP v1 v2 Community Configuration" in the *ACLI Configuration Guide*.
Trap Receiver	Add and specify one or more SNMP trap receivers. See the "SNMP Community and Trap Receiver Management" section of the "System Management" chapter in the *Maintenance and Troubleshooting Guide*,
Web Server	Specify the web server. See "Web Server TLS Configuration" in the *ACLI Configuration Guide*.

Configure Call Accounting

- Confirm that the system displays the Basic mode.

1. Access the Accounting configuration object: **Configuration**, **Management**, **Accounting**.
2. In the Account Config dialog, do the following:

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 **Add**, and select one or more events to collect in a session. Default: Reinvite-Response.
Generate Event	Click **Add**, and select one or more Diameter events to collect in a session. 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. • Do not use /boot or /code file systems.

	• Default: /opt/logs/.
File Rotate Time	Enter a number for the time, in minutes, for the file rotation interval. Range: 0-2147483647.
Options. Add optional parameters.	Click **Add**, and enter one or more options.
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.
Push Receiver	Click **Add**, and do the following: a. Server—Enter the server IP address. b. Port—Enter the server port. Range: 1-65535. c. Admin state—Select to enable. d. Remote path—Enter the remote path name. e. File name prefix—Enter the prefix for file names pushed to the server. f. Priority—Enter the priority of the push receiver. Range 0 (highest)-4 (lowest). g. Protocol—Select a protocol from the drop-down list for pushing to the server. h. Enter the server User Name. i. Enter the server Password, and click **Set**. j. Public key—Enter the public key. k. Click **OK**.
CDR Output Redundancy	Select to enable.
Interim State ID Type	Click **Add**, and select one or more interim state ID types.
Account Servers	Click **Add**, and do the following: a. Hostname—Enter the hostname of the remote server. b. Min round trip—Enter the minimum time allowed to and from the remote server in milliseconds. Range: 10-5000. c. Max inactivity—Enter the maximum time allowed for remote server inactivity in seconds. Range: 1-300.

	d. Restart delay—Enter the delay time before retrying an inactive remote server in seconds. Range: 1-300. e. Bundle vsa—Select to enable. f. Secret—Enter the authentication secret. g. NAS ID—Enter the remote network accounting server ID. h. Domain name sufix—Enter the suffix to use for all domain names. i. Watchdog ka timer— Enter the time interval for keep alive messages in seconds. Range: 0, 6-65535. j. Diameter in manip—Enter the inbound Diameter manipulation to apply. k. Diameter out manipv—Enter the outbound Diameter manipulation to apply. l. Click **OK**.
Prevent Duplicate Attrs	Select to enable preventing duplicate accounting attributes.
VSA ID Range	Enter a comma delimited range of accounting attributes to include in CDRs. **Note:** Blank means that all attributes are included.
CDR Output Inclusive	Select to enable the inclusion of all empty fields.
Diam Attr ID Range	Enter a comma delimited range of accounting attributes to include in Diameter Rf accounting records. **Note:** Blank means that all attributes are included.
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 Srv Ctx Mnc Mcc	Enter the Mobile Country Code / Mobile Network Code tuple. Format: MNC.MCC.
Diam Srv Ctx Ext	Enter the operator-specific extension information.
Diam Ssrvc Attr ID Range	Enter a comma delimited range of Acme accounting attributes to include in Diameter Rf accounting records. **Note:** Blank means that all attributes are included.
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 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.

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

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.

1. Access the SNMP Community configuration object: **Configuration**, **Management**, **SNMP Community**.
2. On the SNMP community page, click **Add**, and do the following:

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	Enter an Pv4 address that is valid within this SNMP community.

3. Click **Close**.
4. Save 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.

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

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.

1. Access the Trap Receiver configuration object: **Configuration**, **Management**, **Trap Receiver**.
2. On the Trap receiver page, click **Add**.
3. On the Add trap receiver page, do the following.

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.

4. Click **OK**.
5. Save 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.

Configure a Web Server

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

- Confirm that at least one TLS profile exists.

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

1. Access Web Server configuration object: **Management**, **Web Server**.
2. On the Web Server Config page, do the following.

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.
HTTP Interface List	Select which HTTP interfaces to enable. Default: REST, GUI.
TLS Profile	Select a TLS profile to use for HTTPS from the drop-down list.

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

Network Configuration

Use the Network control to access the following configuration objects.

Host Route	Specify where to direct management traffic. See the "Host Routes" section of the "System Configuration" chapter in the *ACLI Configuration Guide*.
Network Interface	Specify a logical network interface over which you can configure one or more SIP interfaces. See the "Network Interfaces" section of the "System Configuration" chapter in the *ACLI Configuration Guide*.

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.

1. Access the Host Route configuration object: **Configuration**, **Network**, **Host Route**.
2. On the Host Route page, click **Add**.
3. In the Add Host Route dialog, do the following.

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.
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.

4. Click **OK** to save the host route.

   The host route that you created displays in the Host Routes table.
5. Click **Close**.
6. Save the configuration.

Network Interface Configuration

The Network Interface configuration object 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 configuration object 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 sub-port ID field is set to 0, the default value. When you set VLAN tags on a network interface, the valid sub-port ID value can range from 1-4096. The Network Interface object is a multiple instance configuration element. The combination of the name field and the sub-port 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.

1. Access the Network Interface configuration object: **Configuration**, **Network**, **Network Interface**.
2. In the Network Interface dialog, click **Add**.
3. In the Add Network Interface dialog, do the following:

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.”
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 in an HA pair in IP Address format.
Gw Heartbeat	Click to display the configuration fields.

State	Select to enable the front interface link detection and polling functionality on the 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 host names 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.
DNS Max TTL	Select the maximum TTL, in seconds, for a DNS record in the cache. Default: 86400. Range: 30-2073600.
Signaling 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.
HIP IP List	Add all IPv4 Host Identity Protocol lists for which you want the SBC to accept administrative traffic.
ICMP Address	Enter the IP address to pass standard ping packets to the host.
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 the configuration

Others Configuration

Use the Other control to access the following multi-instance configuration objects.

Media Profile	Use to add one or more media profiles. See the "Media Profiles Per Realm" and Multiple Media Profiles" sections of the "Realms and Nested Realms" chapter in the *ACLI Configuration Guide*.

SIP Features	Use to add one or more SIP features. See the "SIP Options" section of the "Realms and Nested Realms" chapter in the *ACLI Configuration Guide*.
SIP Manipulations	Use to add one or more rules for handling SIP headers. See "Configuring SIP Manipulations" in the *ACLI Configuration Guide*.
SPL	Use to add one or more SPL plug-ins. See the "Session Plug-In Language" chapter in the *ACLI Configuration Guide*.
Translation Rules	Use to add one or more translation rules. See the "Number Translation" chapter in the *ACLI Configuration Guide*.

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 sub-name to the configuration. The system uses the sub-name plus the profile name as the unique identifier.

1. Access the Media Profile configuration object: **Others**, **Media profile**.
2. On the Media Profile page, do the following.

Name	Set the name for this media profile. For example, PCMU, G723, G729. Valid values: Alpha-numeric characters.
Subname	Set the encoding sub-name used for the Codec variation. Valid values: Alpha-numeric characters. You must use a combination of alpha and numeric characters.
Media Type	Set the media type to use in SDP m lines. For example, audio, video, data.
Payload Type	Set the payload type to use in SDP media lines. Valid values: Alpha-numeric characters. **Note:** The Payload type value must be numeric if you use the RTP/AVP transport method.
Transport	Set the transport protocol to use in the SDP RTPMAP attribute. Default: RTP/AVP. Valid values: RTP/AVP | UDP.
Clock Rate	Set 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.

	Note: When configured with 0, the default, the system uses the clock rate for the Codec.
Req Bandwidth	Set the amount of bandwidth required in Kilobits. Range: 0-999999999.
Frames per Packet	Enter the maximum number of frames per packet. Range: 0-256.
Parameters	Add one or more parameters. **Note:** For each parameter, use the + character to add and the - character to remove. For example, +silenceSupression=0.
AS Bandwidth	Set the SDP b=AS value for this codec. Default: 0. Range: 0-4294967295.

3. Click **OK**.
4. Save 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.

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.

1. Access the Translation Rules configuration object: **Configuration**, **Others**, **Translation rules**.
2. On the Translation rules page, click **Add**, and do the following:

ID	Enter a descriptive ID name for this translation rule. Valid values: Alpha-numeric characters.
Type	Select the one of the following translation rules that you want to from the drop-down list.

	• Add—Adds a character or string of characters to the address. • Delete—Deletes a character or string of characters from the address. • None—(Default) Disables the translation rule function. • Replace—Replaces a character or string of characters within the address.
Add String	Enter the index for the Add string. Use the $ character to append the string at the end of the address. Valid values: 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: Alpha-numeric characters.
Delete String	Enter the string that you want deleted from the original address during address translation. Denote unspecified characters with the @ character. Valid values: Alpha-numeric characters. **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.
Delete Index	Enter the index for the Delete string.

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

Configure SIP Features

Use the SIP Feature configuration object 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.

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 is 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.

1. Access the SIP Features configuration object: **Configuration**, **Others**, **Sip Features**.
2. On the Sip Feature page, do the following:

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: • Select the Realm with which to associate this configuration. • Leave this parameter blank to make this configuration global.
Support Mode Inbound	Select the action tag in the Supported header in an inbound packet from the drop-down list. Default: Strip. Valid values: Pass | Strip.
Require Mode Inbound	Select the action tag in the Require header for an inbound packet from the drop-down list. Default: Reject. Valid values: Pass | Reject.
Proxy Require Mode Inbound	Select the action tag in the Proxy-Require header in an inbound packet from the drop-down list. Default: Reject. Valid values: Pass | Reject.
Support Mode Outbound	Select the action tag in the Supported header in an outbound packet from the drop-down list. Default: Pass. Valid values: Pass | Strip.
Require Mode Outbound	Select the action tag in the Require header for an outbound packet from the drop-down list. Default: Reject. Valid values: Pass | Reject.
Proxy Require Mode Outbound	Select the action tag in the Proxy-Require header for an outbound packet from the drop-down list. Default: Pass. Valid values: Pass | Reject.

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

SIP Manipulations

SIP header manipulation allows you to add, delete, or modify SIP message attributes on the Oracle® Enterprise Session Border Controller (E-SBC). For example, SIP headers and SIP header elements.

The most common reason for manipulating SIP headers and SIP header elements is to fix an incompatibility problem between two SIP endpoints. For example, Softswitch - PSTN incompatibility or a SIP messaging problem between two different IP PBX platforms in a multi-site deployment where calls between the platforms are unsuccessful due to problems in the SIP messaging.

To enable the SIP header manipulation, create rule sets in which you specify header manipulation rules and, optionally, header element manipulation rules. SIP header elements are the sub-parts of the header, such as the header value, the header parameter, the URI parameter, and so on, excluding the header name. You can specify the actions that you want the system to perform for each header element.

After creating the header manipulation rule set, apply it to a session agent or SIP interface as "inbound" or "outbound."

SIP Header Manipulation Configuration

Configuring SIP manipulations from the Web GUI is a multi-faceted process performed through a series of nested dialogs that differ depending on the particular header and header element that you want to manipulate. It is not practical to document the entire SIP manipulations configuration process in one procedure. The documentation begins with the "Configure SIP Manipulation", topic where you can set the global parameters, if that is all you need. The documentation continues with procedures for each particular header and header element that you can manipulate. Each of those topics includes the global settings, so you can set or modify them there, as well.

header and header element that you can manipulate include the following:

- Configure MIME Rule—includes the mime-header-rule element.
- Configure MIME ISUP Rule—includes the mime-header-rule and isup-param-rule elements.
- Configure MIME SDP Rule—includes the mime-header-rule, sdp-session-rule, and the sdp-media-rule.

When you finish configuring SIP manipulations, apply the rules to a session agent or SIP interface as "inbound" or "outbound."

SIP Manipulations Rules Attributes and Values Reference

Refer to the following table for information about the attributes that you can configure for SIP manipulation rules.

Attributes	Values and Descriptions
Action	• add—Adds a new header, if that header does not exist. • delete—Deletes the header, if it exists. • find-replace-all—Finds all matching headers and replaces 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. Default: None.

Attributes	Values and Descriptions
Comparison type	• 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. Default: Case-sensitive.
Format	• ascii-string - A character-encoding scheme that represents text (128 ASCII codes, 7 bits). • binary-ascii - An encoding scheme where each byte of an ASCII character is used. Can use up to 256 bit patterns . • hex-ascii - An encoding scheme that uses a string of numbers (no spaces) to represent each ASCII character.
Header name	The name of the header to which the rule applies. Case-sensitive.
Match value	The value that you want to match against the element value for an action to be performed.
Match val type	The type of value to match to the match-field entry for the action to be performed. • 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.

Attributes	Values and Descriptions
Media type (SDP descriptor for SDP media rule)	• m—Media name and transport address • i—Media title • c—Connection information (optional when configured at the session level) • b—Zero or more bandwidth information lines • k—Encryption key • a—Zero or more media attribute lines • t—The session time is active • r—Zero or more repeat times
Methods	SIP method names to which you want to apply the header rule. For example, INVITE, ACK, BYE. When this field is empty, the system applies the MIME rule to all methods. Default: Blank.
Mime header	The parameter name to which the rule applies. The parameter name depends on the element name you entered. 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. Alpha-numeric characters. Default: blank.
Msg type	• 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 Default: Any.
Name	The name you want to use for the rule. Default: Blank.

<table>
<tr><th>Attributes</th><th>Values and Descriptions</th></tr>
<tr><td>New value</td><td>The value for a new element or replacement value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators.
<ul>
<li>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.</li>
<li>Pre-defined values.—Pre-defined parameters always start with a $. For valid values, see the Pre-defined Parameters table.</li>
<li>Operators parameters—For valid values, see the Operators table.</li>
</ul>
The following table describes the pre-defined parameters.
<table>
<tr><th>Pre-defined Parameter</th><th>Description</th></tr>
<tr><td>$ORIGINAL</td><td>Original value of the element is used.</td></tr>
<tr><td>$LOCAL_IP</td><td>IP address of the SIP interface on which the message was received for inbound manipulation; or sent on for outbound manipulation.</td></tr>
<tr><td>$REMOTE_IP</td><td>IP address the message was received from for inbound manipulation; or being sent to for outbound manipulation.</td></tr>
<tr><td>$REMOTE_VIA_HOST</td><td>Host from the top Via header of the message is used.</td></tr>
<tr><td>$TRUNK_GROUP</td><td>Trunk group is used.</td></tr>
<tr><td>$TRUNK_GROUP_CONTEXT</td><td>Trunk group context is used.</td></tr>
</table>
The following table describes the Operators.
<table>
<tr><th>Operator</th><th>Description</th></tr>
<tr><td>+</td><td>Append the value to the end. For example:
acme”+”packet
generates acmepacket</td></tr>
<tr><td>+^</td><td>Prepends the value. For example:
acme”+^”packet
generates packetacme</td></tr>
<tr><td>-</td><td>Subtract at the end. For example:
112311”-”11</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Attributes</th><th>Values and Descriptions</th></tr>
<tr><td></td><td><table>
<tr><th>Operator</th><th>Description</th></tr>
<tr><td></td><td>generates 1123</td></tr>
<tr><td>-^</td><td>Subtract at the beginning. For example:
112311”-^”11
generates 2311</td></tr>
</table></td></tr>
<tr><td>Parameter name</td><td>The parameter name to which the rule applies. The parameter name depends on the element name you entered. 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. Alpha-numeric characters. Default: Blank.</td></tr>
</table>

Attributes	Values and Descriptions
Type	The type of element on which to perform the action. Default: Blank. • 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.

Attributes	Values and Descriptions
Type (SDP descriptor for SDP line rule)	• 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 when included in all media) • b—Zero or more bandwidth information lines or one or more time descriptions("t=" and "r=" lines) • z—Time zone adjustments • k—Encryption key • a—Zero or more session attribute lines or zero or more media descriptions • t—Time the session is active • r—Zero or more repeat times

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.

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.

1. Access the SIP Manipulation configuration object: **Configuration**, **Others**, **SIP Manipulation**.
2. In the SIP manipulation dialog, do the following.

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 comma separated list of headers that you want the system to split and treat separately before executing any manipulation rules.
Join Headers	Create a comma separated list of headers that you want the system to join and treat as one header after executing any manipulation rules.
Rules	Click **Add**, select one of the following header rules from the menu. See the following documentation for further instructions.

	• header rule—"Configure Header Rule" • mime rule—"Configure MIME Rule" • mime isup rule—"Configure MIME ISUP Rule" • mime sdp rule—"Configure MIME SDP Rule"

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

- Apply the rules to a session agent or SIP interface as "inbound" or "outbound."

Configure a SIP Manipulation Header Rule

You can configure SIP header rules and element rules on the Oracle® Enterprise Session Border Controller (E-SBC) from the "CfgRules" section of the "SIP Manipulations" page.

In the following procedure, you set the SIP Header Manipulation, Header Rule, and Element Rule parameters.

1. Access the SIP Manipulation configuration object.

   Configuration, **System Administration**, **SIP Manipulation**.
2. On the SIP Manipulation configuration page, do one of the following:
   a. Select and existing SIP manipulation configuration from the table, right-click, and click **Edit**. (Subsequent SIP manipulation pages use "Modify" in the title.)
   b. Click **Add**. (Subsequent SIP manipulation pages use "Add" in the title.)
3. On the Add or Modify SIP Manipulation page, do one of the following.
   a. If you chose **Add**, you must enter a name for this SIP Manipulation. (You can optionally complete the Description, Split Headers, and Join Headers parameters, at this time. See "Configure SIP Manipulation.") Proceed to the next step.
   b. If you chose to edit an existing configuration, proceed to the next step.
4. On the Add or Modify SIP Manipulation page under Cgf Rules, click **Add** and click **header-rule**.
5. On the Add SIP Manipulation / Header Rule page, do the following.

Name	Enter a unique name for this rule set. Valid values: Alpha-numeric.
Header Name	Enter the name of the header on which you want the E-SBC to use this HMR. Set this parameter to @status-line, where the at-sign (@)—not allowed in SIP header names—to prevent undesired matches with header having the name status-code. Default: Blank.
Action	Select an action from the drop-down list for the header rule. Default: None. Valid values: Add | Delete | Find Replace All | Log | Manipulate | Monitor | None | Reject | SIP Manip | Store.
Comparison Type	Specify how the E-SBC processes the match rules against the SIP header. Default: Refer Case Sensitive. Valid values: Boolean |

	Case Insensitive | Case Sensitive | Pattern Rule | Refer Case Insensitive | Refer Case Sensitive.
Msg Type	Specify the message type this rule applies to. Default: Any. Valid Values: Any | Out of Dialog | Reply | Request | Out of Dialog.
Methods	Enter the method type to use when this SIP HMR is used. Default: Blank. Valid values" ACK | CANCEL | INVITE. When you do not set the method, the E-SBC applies the rule to all SIP methods.
Match Value	Enter the value to match against the header value in SIP packets; the E-SBC matches these against the entire SIP header value. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators. When you configure HMR (using SIP manipulation rules and elements rules, you can use escape characters in the **match-value** parameter to support escaping Boolean and string manipulation operators. You can also escape the escape character itself, so that it is used as a literal string. For example, the E-SBC treats the string \+1234 as +1234. The following are escape characters: +, -, +^, -^, &, |, \, (,), ., $, ^, and “. You can also use the variables, $REMOTE_PORT and $LOCAL_PORT, which resolve respectively to the far-end and remote UDP or TCP port value.
New Value	When you set the action parameter Add or to Manipulate, enter the new value that you want to substitute for the entire header value. This is where you can set stored regular expression values for the E-SBC to use when it adds or manipulates SIP headers. When you configure HMR (using SIP manipulation rules and elements rules, you can use escape characters in the **match-value** parameter to support escaping Boolean and string manipulation operators. You can also escape the escape character itself, so that it is used as a literal string. For example, the E-SBC treats the string \+1234 as +1234. The following are escape characters: +, -, +^, -^, &, |, \, (,), ., $, ^, and “. You can also use the variables, $REMOTE_PORT and $LOCAL_PORT, which resolve respectively to the far-end and remote UDP or TCP port value.
Cfg Rules	(Optional) Click **Add**, **element-rule**, and do the following. • Name—Enter a unique name for this header element rule. You can enter up to 128 alphanumeric characters with no spaces. The name can include the _, ., or - characters, cannot begin with either the . or the - characters. • Parameter name—Enter the parameter name to apply to the rule. • Type—Select the element type to which to apply this rule. • Action—Select an action from the drop-down list to apply to the element rule. Default: None. • Match Val Type—Select a match value type that this rule applies to from the drop-down list. Default: Any. • Comparison Type—Select an element type from the drop-down list to which to apply the rule. Default: Case Sensitive.

	• Match Value—Enter the match value to compare against the current object. (To clear the value, enter and empty string.) • New Value—Enter a new value for the object. Quoted display named must be escaped within quotes. For example, \"MyName\". (To clear the value, enter and empty string.) • Click **OK**. The system displays the SIP Manipulation / Header Rule page. Do one of the following: • Add another Element Rule. • Finish the Header Rule configuration by completing the following steps.

6. Click **Back**.

   The system displays the Modify SIP Manipulation page.

7. Click **Back**.

   The system displays the SIP Manipulation page.

8. Save the configuration.

Configure a MIME Rule

You can configure Multi-Purpose Internet Mail Extensions (MIME) header rules and element rules on the Oracle® Enterprise Session Border Controller (E-SBC) from the "CfgRules" section of the "SIP Manipulations" page.

In the following procedure, you set the SIP Header Manipulation, MIME Rule, and MIME Header Rule parameters.

1. Access the SIP Manipulation configuration object.

   Configuration, **System Administration**, **SIP Manipulation**.

2. On the SIP Manipulation configuration page, do one of the following:

   a. Select and existing SIP manipulation configuration from the table, right-click, and click **Edit**. (Subsequent SIP manipulation pages use "Modify" in the title.)

   b. Click **Add**. (Subsequent SIP manipulation pages use "Add" in the title.)

3. On the Add or Modify SIP Manipulation page, do one of the following.

   a. If you chose **Add**, you must enter a name for this SIP Manipulation. (You can optionally complete the Description, Split Headers, and Join Headers parameters, at this time. See "Configure SIP Manipulation.") Proceed to the next step.

   b. If you chose to edit an existing configuration, proceed to the next step.

4. On the Add or Modify SIP Manipulation page under Cfg Rules, click **Add** and click **mime-rule**.

5. On the Add or Modify SIP Manipulation / Mime Rule page, do the following.

Name	Enter a unique name for this rule set. Valid values: Alpha-numeric.

Content Type	Enter the name of the header on which you want the E-SBC to use this HMR. Set this parameter to @status-line, where the at-sign (@)—not allowed in SIP header names—to prevent undesired matches with header having the name status-code. Default: Blank.
Msg Type	Specify the message type this rule applies to. Default: Any. Valid Values: Any | Out of Dialog | Reply | Request | Out of Dialog.
Methods	Enter the method type to use when this SIP HMR is used. Default: Blank. Valid values" ACK | CANCEL | INVITE. When you do not set the method, the E-SBC applies the rule to all SIP methods.
Format	Select the encode - decode format from the drop-down list for the MIME content.
Action	Select an action from the drop-down list for the header rule. Default: None. Valid values: Add | Delete | Find Replace All | Log | Manipulate | Monitor | None | Reject | SIP Manip | Store.
Comparison Type	Specify how the E-SBC processes the match rules against the SIP header. Default: Refer Case Sensitive. Valid values: Boolean | Case Insensitive | Case Sensitive | Pattern Rule | Refer Case Insensitive | Refer Case Sensitive.
Match Value	Enter the value to match against the header value in SIP packets; the E-SBC matches these against the entire SIP header value. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators. When you configure HMR (using SIP manipulation rules and elements rules, you can use escape characters in the **match-value** parameter to support escaping Boolean and string manipulation operators. You can also escape the escape character itself, so that it is used as a literal string. For example, the E-SBC treats the string \+1234 as +1234. The following are escape characters: +, -, +^, -^, &, |, \, (,), ., $, ^, and “. You can also use the variables, $REMOTE_PORT and $LOCAL_PORT, which resolve respectively to the far-end and remote UDP or TCP port value.
New Value	When you set the action parameter Add or to Manipulate, enter the new value that you want to substitute for the entire header value. This is where you can set stored regular expression values for the E-SBC to use when it adds or manipulates SIP headers. When you configure HMR (using SIP manipulation rules and elements rules, you can use escape characters in the **match-value** parameter to support escaping Boolean and string manipulation operators. You can also escape the escape character itself, so that it is used as a literal string. For example, the E-SBC treats the string \+1234 as +1234. The following are escape characters: +, -, +^, -^, &, |, \, (,), ., $, ^, and “. You can also use the variables, $REMOTE_PORT and $LOCAL_PORT, which resolve respectively to the far-end and remote UDP or TCP port value.
Cfg Rules	Click **Add**, **mime-header-rule**, and do the following.

- Name—Enter a unique name for this header element rule. You can enter up to 128 alphanumeric characters with no spaces. The name can include the _, ., or - characters, but cannot begin with either the . or the - characters.
- Mime Header Name—Enter header name within the MIME part to which to apply the rule. Use headername@peramble to change the preamble of a SIP body. Use headername@epilogue to change the epilog of a SIP body.
- Action—Select an action from the drop-down list to apply to the element rule. Default: None.
- Comparison Type—Select the type of comparison from the drop-down list to use for the match value. Default: Match Value. (To clear the value, enter and empty string.)
- Match Value—Enter the match value to compare against the current object. (To clear the value, enter and empty string.)
- New Value—Enter a new value for the object. Quoted display named must be escaped within quotes. For example, \"MyName\". (To clear the value, enter and empty string.)
- Click **OK**. The system displays the SIP Manipulation / Mime Rule dialog.

Do one of the following:

- Add another mime-header-rule.
- Finish the MIME Rule configuration by completing the following steps.

6. Click **Back**.

   The system displays the Add or Modify SIP Manipulation page.
7. Click **Back**.

   The system displays the SIP Manipulation page.
8. Save the configuration.

Configure a MIME ISUP Rule

You can configure Multi-Purpose Internet Mail Extensions (MIME) header rules and element rules on the Oracle® Enterprise Session Border Controller (E-SBC) from the "CfgRules" section of the "SIP Manipulations" page.

In the following procedure, you set the SIP Header Manipulation, MIME ISUP Rule, MIME Header Rule, and ISUP Param Rule parameters.

1. Access the SIP Manipulation configuration object.

   Configuration, **System Administration**, **SIP Manipulation**.
2. On the SIP Manipulation configuration page, do one of the following:
   a. Select and existing SIP manipulation configuration from the table, right-click, and click **Edit**. (Subsequent SIP manipulation pages use "Modify" in the title.)
   b. Click **Add**. (Subsequent SIP manipulation pages use "Add" in the title.)

3. On the Add or Modify SIP Manipulation page, do one of the following.
   a. If you chose **Add**, you must enter a name for this SIP Manipulation. (You can optionally complete the Description, Split Headers, and Join Headers parameters, at this time. See "Configure SIP Manipulation.") Proceed to the next step.
   b. If you chose to edit an existing configuration, proceed to the next step.
4. On the Add or Modify SIP Manipulation page under Cfg Rules, click **Add** and click **mime-header-rule**.
5. On the Add or Modify SIP Manipulation / Mime ISUP Rule page, do the following.

Name	Enter a unique name for this rule set. Valid values: Alpha-numeric.
Content Type	Enter the name of the header on which you want the E-SBC to use this HMR. Set this parameter to @status-line, where the at-sign (@)—not allowed in SIP header names—to prevent undesired matches with header having the name status-code. Default: Blank.
Msg Type	Specify the message type this rule applies to. Default: Any. Valid Values: Any | Out of Dialog | Reply | Request | Out of Dialog.
Methods	Enter the method type to use when this SIP HMR is used. Default: Blank. Valid values" ACK | CANCEL | INVITE. When you do not set the method, the E-SBC applies the rule to all SIP methods.
Format	Select the encode - decode format from the drop-down list for the MIME content.
Action	Select an action from the drop-down list for the header rule. Default: None. Valid values: Add | Delete | Find Replace All | Log | Manipulate | Monitor | None | Reject | SIP Manip | Store.
Comparison Type	Specify how the E-SBC processes the match rules against the SIP header. Default: Refer Case Sensitive. Valid values: Boolean | Case Insensitive | Case Sensitive | Pattern Rule | Refer Case Insensitive | Refer Case Sensitive.
Match Value	Enter the value to match against the header value in SIP packets; the E-SBC matches these against the entire SIP header value. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators. When you configure HMR (using SIP manipulation rules and elements rules, you can use escape characters in the **match-value** parameter to support escaping Boolean and string manipulation operators. You can also escape the escape character itself, so that it is used as a literal string. For example, the E-SBC treats the string \+1234 as +1234. The following are escape characters: +, -, +^, -^, &, |, \, (,), ., $, ^, and “. You can also use the variables, $REMOTE_PORT and $LOCAL_PORT, which resolve respectively to the far-end and remote UDP or TCP port value.
New Value	When you set the action parameter Add or to Manipulate, enter the new value that you want to substitute for the entire header

<table>
<tr><td></td><td>value. This is where you can set stored regular expression values for the E-SBC to use when it adds or manipulates SIP headers. When you configure HMR (using SIP manipulation rules and elements rules, you can use escape characters in the <b>match-value</b> parameter to support escaping Boolean and string manipulation operators. You can also escape the escape character itself, so that it is used as a literal string. For example, the E-SBC treats the string \+1234 as +1234. The following are escape characters: +, -, +^, -^, &, |, \, (,), ., $, ^, and “. You can also use the variables, $REMOTE_PORT and $LOCAL_PORT, which resolve respectively to the far-end and remote UDP or TCP port value.</td></tr>
<tr><td>Cfg Rules (instructions for configuring MIME HeaderRule)</td><td>Click <b>Add</b>, <b>MIME Header Rule</b>, and do the following.
• Name—Enter a unique name for this header element rule.
• Header Name—Enter header name within the MIME part to which to apply the rule.
• Action—Select an action from the drop-down list to apply to the element rule.
• Comparison Type—Select the type of comparison from the drop-down list to use for the match value. (To clear the value, enter and empty string.)
• Match Value—Enter the match value to compare against the current object. (To clear the value, enter and empty string.)
• New Value—Enter a new value for the object. Quoted display named must be escaped within quotes. For example, \"MyName\" .
• Click <b>OK</b>. The system displays the SIP manipulation / Mime isup rule dialog.
Do one of the following:
• Add another MIME Header Rule.
• Add an ISUP Param Rule, using the steps in the following table cell.
• Finish the MIME ISUP rule configuration by completing steps 3-6.</td></tr>
<tr><td>Cfg Rules (instructions for configuring ISUP Param Rule)</td><td>Click <b>Add</b>, <b>isup-param-rule</b>, and do the following.
• Name—Enter a unique name for this header element rule.
• Type—Enter the parameter type that specifies the part of the isup body to manipulate.
• Format—Select a format from the drop down list for the encode - decode mode of the binary body form string form-ascii.
• Action—Select an action from the drop-down list to apply to the element rule.</td></tr>
</table>

	• Comparison Type—Select the type of comparison from the drop-down list to use for the match value. (To clear the value, enter and empty string.) • Match Value—Enter the match value to compare against the current object. (To clear the value, enter and empty string.) • New Value—Enter a new value for the object. Quoted display named must be escaped within quotes. For example, "\"MyName\" " . • Click **OK**. The system displays the SIP manipulation / Mime isup rule dialog. Do one of the following: • Add another ISUP Param Rule. • Finish the MIME ISUP Rule configuration by completing the following steps.

6. Click **Back**.

   The system displays the Add or Modify SIP Manipulation page.

7. Click **Back**.

   The system displays the SIP Manipulation page.

8. Save the configuration.

Configure a MIME SDP Rule

You can configure Multi-Purpose Internet Mail Extensions (MIME) header rules and element rules on the Oracle® Enterprise Session Border Controller (E-SBC) from the "CfgRules" section of the "SIP Manipulations" page.

In the following procedure, you set the SIP Header Manipulation, MIME SDP Rule, MIME Header Rule, SDP Session Rule, and SDP Media Rule parameters.

1. Access the SIP Manipulation configuration object.

   Configuration, **System Administration**, **SIP Manipulation**.

2. On the SIP Manipulation configuration page, do one of the following:

   a. Select and existing SIP manipulation configuration from the table, right-click, and click **Edit**. (Subsequent SIP manipulation pages use "Modify" in the title.)

   b. Click **Add**. (Subsequent SIP manipulation pages use "Add" in the title.)

3. On the Add or Modify SIP Manipulation page, do one of the following.

   a. If you chose **Add**, you must enter a name for this SIP Manipulation. (You can optionally complete the Description, Split Headers, and Join Headers parameters, at this time. See "Configure SIP Manipulation.") Proceed to the next step.

   b. If you chose to edit an existing configuration, proceed to the next step.

4. On the Add or Modify SIP Manipulation page under Cfg Rules, click **Add** and click **mime-sdp-rule**.

5. In the Add or Modify SIP Manipulation / MIME SDP Rule page, do the following.

Name	Enter a unique name for this rule set. Valid values: Alpha-numeric.
Content Type	Enter the name of the header on which you want the E-SBC to use this HMR. Set this parameter to @status-line, where the at-sign (@)—not allowed in SIP header names—to prevent undesired matches with header having the name status-code. Default: Blank.
Msg Type	Specify the message type this rule applies to. Default: Any. Valid Values: Any | Out of Dialog | Reply | Request | Out of Dialog.
Methods	Enter the method type to use when this SIP HMR is used. Default: Blank. Valid values" ACK | CANCEL | INVITE. When you do not set the method, the E-SBC applies the rule to all SIP methods.
Format	Select the encode - decode format from the drop-down list for the MIME content.
Action	Select an action from the drop-down list for the header rule. Default: None. Valid values: Add | Delete | Find Replace All | Log | Manipulate | Monitor | None | Reject | SIP Manip | Store.
Comparison Type	Specify how the E-SBC processes the match rules against the SIP header. Default: Refer Case Sensitive. Valid values: Boolean | Case Insensitive | Case Sensitive | Pattern Rule | Refer Case Insensitive | Refer Case Sensitive.
Match Value	Enter the value to match against the header value in SIP packets; the E-SBC matches these against the entire SIP header value. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators. When you configure HMR (using SIP manipulation rules and elements rules, you can use escape characters in the **match-value** parameter to support escaping Boolean and string manipulation operators. You can also escape the escape character itself, so that it is used as a literal string. For example, the E-SBC treats the string \+1234 as +1234. The following are escape characters: +, -, +^, -^, &, |, \, (,), ., $, ^, and “. You can also use the variables, $REMOTE_PORT and $LOCAL_PORT, which resolve respectively to the far-end and remote UDP or TCP port value.
New Value	When you set the action parameter Add or to Manipulate, enter the new value that you want to substitute for the entire header value. This is where you can set stored regular expression values for the E-SBC to use when it adds or manipulates SIP headers. When you configure HMR (using SIP manipulation rules and elements rules, you can use escape characters in the **match-value** parameter to support escaping Boolean and string manipulation operators. You can also escape the escape character itself, so that it is used as a literal string. For example, the E-SBC treats the string \+1234 as +1234. The following are escape characters: +, -, +^, -^, &, |, \, (,), ., $, ^, and “. You can also use the variables, $REMOTE_PORT and $LOCAL_PORT, which resolve respectively to the far-end and remote UDP or TCP port value.

Cfg Rules (instructions for configuring mime-header-rule)	(Optional) Click **Add**, **mime-header-rule**, and do the following. • Name—Enter a unique name for this header element rule. • Mime Header Name—Enter header name within the MIME part to which to apply the rule. • Action—Select an action from the drop-down list to apply to the element rule. • Comparison Type—Select the type of comparison from the drop-down list to use for the match value. • Match Value—Enter the match value to compare against the current object. • New Value—Enter a new value for the object. Quoted display named must be escaped within quotes. For example, \"MyName\" . • Click **OK**. The system displays the SIP manipulation / Mime sdp rule dialog. Do one of the following: • Add another mime-header-rule. • Configure the sdp-session-rule and sdp-media-rule options, using the steps in the following table cells. • Finish the MIME SDP rule configuration by completing steps 3-6.
Cfg Rules (instructions for configuring sdp-session-rule)	(Optional) Click **Add**, **sdp-session-rule** , and do the following. • Name—Enter a unique name for this header element rule. • Action—Select an action from the drop-down list to apply to the this rule. • Comparison Type—Select the type of comparison from the drop-down list to use for the match value. • Match Value—Enter the match value to compare against the current object. • New Value—Enter a new value for the object. Quoted display named must be escaped within quotes. For example, \"MyName\". • CfgRules—(Optional) Click **Add**, **sdp-line-rule**. • Name—Enter a unique name for this rule. • Type—Enter a descriptor type to specify the SDP line to manipulate. • Action—Select an action from the drop-down list to apply to this rule. • Comparison Type—Select the type of comparison from the drop-down list to use for the match value. • Match Value—Enter the match value to compare against the current object.

	• New Value—Enter a new value for the object. Quoted display named must be escaped within quotes. For example, \"MyName\". • Click **OK**. The system displays the SIP manipulation / Mime sdp rule / Sdp session rule dialog. • (Optional) Add another sdp-line-rule. • Click **OK**. The system displays the SIP manipulation / Mime sdp rule dialog. Do one of the following: • Add another sdp-session-rule. • Configure the mime-header-rule and sdp-media-rule options, using the steps in the corresponding table cells in this procedure. • Finish the MIME SDP rule configuration by completing steps 3-6.
Cfg Rules (instructions for configuring sdp-media-rule)	(Optional) Click **Add**, **sdp-media-rule**. • Name—Enter a unique name for this header element rule. • Media Type—Enter the media type to manipulate. For example, audio or video. • Action—Select an action from the drop-down list to apply to the element rule. • Comparison Type—Select the type of comparison from the drop-down list to use for the match value. • Match Value—Enter the match value to compare against the current object. • New Value—Enter a new value for the object. Quoted display named must be escaped within quotes. For example, "\"MyName\" " . • Click **OK**. • CfgRules—(Optional) Click **Add**, **sdp-line-rule**. • Name—Enter a unique name for this rule. • Type—Enter a descriptor type to specify the SDP line to manipulate. • Action—Select an action from the drop-down list to apply to this rule. • Comparison type—Select the type of comparison from the drop-down list to use for the match value. (To clear the value, enter and empty string.) • Match Value—Enter the match value to compare against the current object. (To clear the value, enter and empty string.)

	• New Value—Enter a new value for the object. Quoted display named must be escaped within quotes. For example, \"MyName\". • Click **OK**. The system displays the SIP manipulation / Mime sdp rule / Sdp media rule dialog. • (Optional) Add another sdp-line-rule. • Click **OK**. The system displays the SIP manipulation / Mime sdp rule dialog. Do one of the following: • Add another sdp-media-rule. • Finish the MIME SDP rule configuration by completing the following steps.

6. Click **Back**.

   The system displays the Add or Modify SIP Manipulation page.

7. Click **Back**.

   The system displays the SIP Manipulation page.

8. Save the configuration.

Add an SPL

Add an SPL plug-in, which is a customized script, to quickly implement a feature on the Oracle® Enterprise Session Border Controller (E-SBC). The SPL plug-in augments running the software image on the E-SBC, and provides new features when you need them without having to upgrade the software.

- Confirm the name and location of the SPL plug-in 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.

1. Access the SPL configuration object: **Configuration**, **Other**, **SPL**.
2. In the **SPL Config** dialog, do the following:

State	Select State to enable the plugin.
Name	Enter the name of plugin to load.

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

SBC Configuration

Use the SBC control to access the following configuration objects. See the documentation specified in the following list for explanations of these configuration objects and how to set their parameters.

Advanced Routing	See the "Session Routing and Load Balancing" chapter in the *ACLI Configuration Guide*.
Web Server	Enable and configure a web server, including a TLS profile. See the "Web Server TLS Configuration" chapter in the *ACLI Configuration Guide*.

Security Configuration

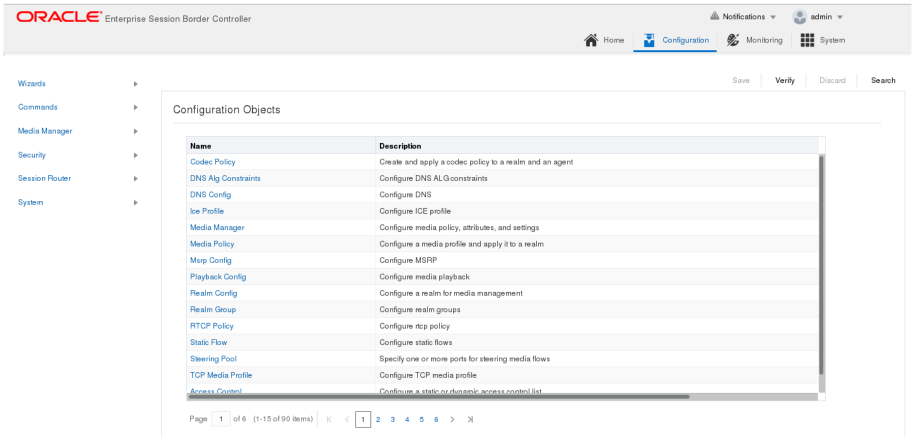
Use the Security control to access the following configuration objects. See the documentation specified in the following list for explanations of these configuration objects and how to set their parameters.

Certificate Record	Create a certificate record for either a CA or end entity. See "Online Certificate Status Protocol" in the *ACLI Configuration Guide*.
SDES Profile	Create a Session Description Protocol Security Descriptions (SDES) profile for media streams. See "Configure an SDES Profile" in the *ACLI Configuration Guide*.
TLS Profile	Create a profile to define communications security for running SIP over TLS See "Configure a TLS Profile" in the *ACLI Configuration Guide*.

Expert Mode Configuration

Expert mode offers more configuration objects than Basic mode, which offers a limited set of configuration objects and is generally used only for proof of concept and testing purposes. Use Expert mode to see all of the features and settings available to help you fully customize the Oracle® Enterprise Session Border Controller (E-SBC) to your requirements.

The Expert mode configuration workspace displays a list of configuration objects and elements in the navigation pane. You can display them in either tree view (categorical) or list view (alphabetical) by way of Preferences from the User menu. When you click an object in navigation pane, the corresponding configuration dialog displays in the center pane.



Configuration Objects

Name	Description
Codec Policy	Create and apply a codec policy to a realm and an agent
DNS Alg Constraints	Configure DNS ALG constraints
DNS Config	Configure DNS
Ice Profile	Configure ICE profile
Media Manager	Configure media policy, attributes, and settings
Media Policy	Configure a media profile and apply it to a realm
Msrp Config	Configure MSRP
Playback Config	Configure media playback
Realm Config	Configure a realm for media management
Realm Group	Configure realm groups
RTCP Policy	Configure rtcp policy
Static Flow	Configure static flows
Steering Pool	Specify one or more ports for steering media flows
TCP Media Profile	Configure TCP media profile
Access Control	Configure a static or dynamic access control list

Page 1 of 6 (1-15 of 90 items) 1 2 3 4 5 6

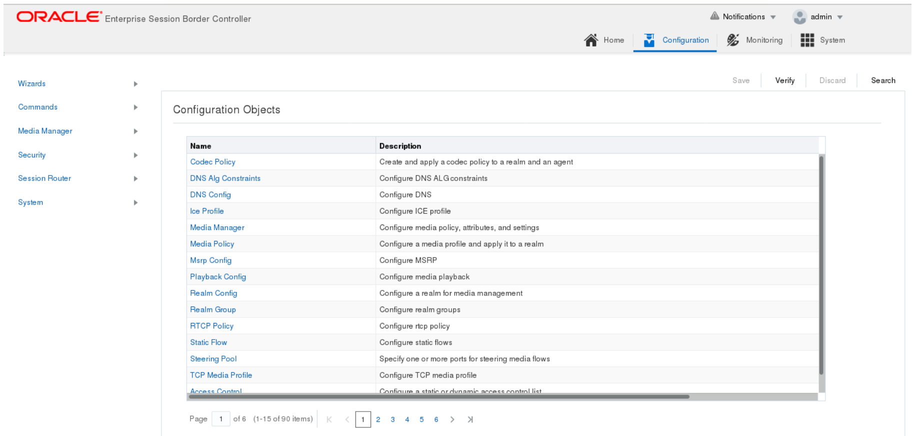
> **Caution:**
>
> The Web GUI does not indicate required parameters or display an error message for those that contain no value. You may be able to save a configuration with a missing required value because the E-SBC ignores the parameter when it is not configured. The end result is a faulty configuration. Use the verify control that displays in every configuration dialog to validate the configuration.

Expert Mode Configuration Controls

The Oracle® Enterprise Session Border Controller (E-SBC) Web GUI provides the following tools for working with configurations. Some tools are located in the navigation pane and others are located at the top of the center pane.

The Configuration Tab Display

The following screen capture shows the locations of all of the Configuration tab controls.



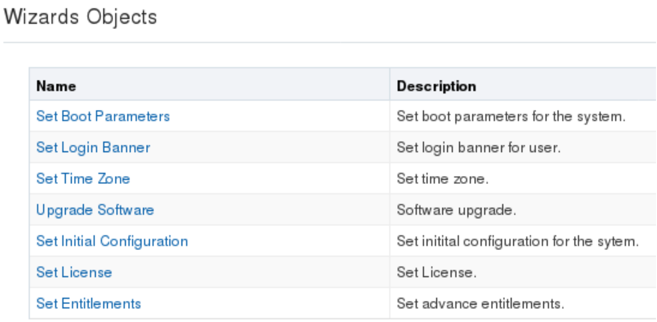
Configuration Objects

Name	Description
Codec Policy	Create and apply a codec policy to a realm and an agent
DNS Alg Constraints	Configure DNS ALG constraints
DNS Config	Configure DNS
Ice Profile	Configure ICE profile
Media Manager	Configure media policy, attributes, and settings
Media Policy	Configure a media profile and apply it to a realm
Msrp Config	Configure MSRP
Playback Config	Configure media playback
Realm Config	Configure a realm for media management
Realm Group	Configure realm groups
RTCP Policy	Configure rtcp policy
Static Flow	Configure static flows
Steering Pool	Specify one or more ports for steering media flows
TCP Media Profile	Configure TCP media profile
Access Control	Configure a static or dynamic access control list

Page 1 of 6 (1-15 of 90 items) 1 2 3 4 5 6

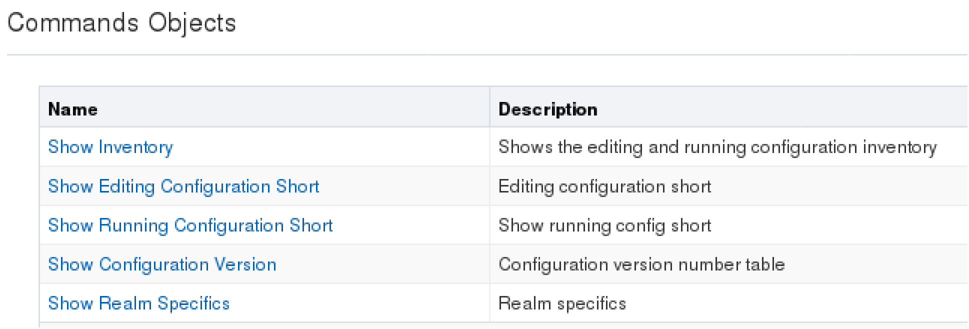
Controls in the Navigation Pane

The navigation pane displays links to Configuration Wizards and Show Commands. (Descriptions are listed in the center pane.) The Wizards help you specify certain parts of the configuration and the Commands show you information about the configuration of the system.



Wizards Objects

Name	Description
Set Boot Parameters	Set boot parameters for the system.
Set Login Banner	Set login banner for user.
Set Time Zone	Set time zone.
Upgrade Software	Software upgrade.
Set Initial Configuration	Set initital configuration for the sytem.
Set License	Set License.
Set Entitlements	Set advance entitlements.

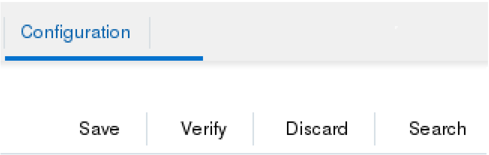


Commands Objects

Name	Description
Show Inventory	Shows the editing and running configuration inventory
Show Editing Configuration Short	Editing configuration short
Show Running Configuration Short	Show running config short
Show Configuration Version	Configuration version number table
Show Realm Specifics	Realm specifics

Controls in the Center Pane

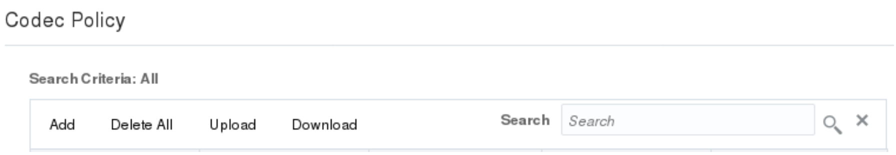
The controls located at the top of the center pane on a configuration page help you manage configuration objects.



Save	Use to save the current configuration session. Upon Save, the system displays a prompt giving you a choice of whether or not to activate the configuration. If you do not activate the configuration, you can continue to make changes and Save again. When finished, you can save and activate all of the configuration changes.
Verify	Use to confirm that the configuration is valid before you save it.
Discard	Use to undo all configuration changes made in the current session. The system can only discard the changes that you saved. It cannot discard any changes that you activated.
Search	Use to find and display the current settings for the configuration you are editing. Enter the name of the configuration object.

Controls for Multi-Instance Objects

The controls located at the top of a list of multi-instance objects help you manage the objects on the list. The following screen capture shows the controls.



Codec Policy

Search Criteria: All

Add	Use to add another instance of the configuration object with one or more parameters set differently.
Delete All	Use to delete all instances.

	Caution: You cannot select a sub-set of instances and delete only those. The system deletes all instances, regardless of how many you select.
Upload	Use to upload a configuration file in CSV format.
Download	Use to download a configuration file in CSV format.
Search	Use to search the list of multi-instances for a specific instance. When you enter the name of an instance, the Web GUI displays it at the top of the list.

Using Tag Fields

The Oracle® Enterprise Session Border Controller provides a configuration element data field referred to as a tag. You enter information into the tag field for descriptive and grouping purposes. You can establish your own criteria for labeling configuration elements with these tags. Tag fields have no operational effect on signaling services.

The following configuration objects display the Tags text field:

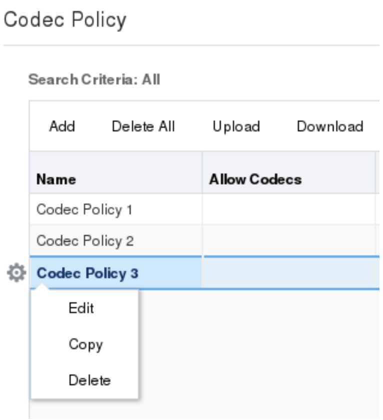
- Agents
- Users
- Routes

You can enter any text that you want into the field and you can apply as many tags to a configuration object as needed. You can filter the element list searches using tags as a means of organizing these objects. Applicable element list search fields include a down arrow that exposes a tag drop-down list, from which you select the tag on which to filter the list. Tags have no operational function other than supporting this kind of filtering.

Edit, Copy, and Delete Configurations

You can edit, copy, and delete multi-instance configurations by way of the controls that the Web GUI displays on each multi-instance configuration page. The edit and copy functions act only on a single instance of a configuration. The delete function can act on either a single instance or all instances.

To edit, copy, or delete a single multi-instance configuration, select the configuration and right-click. The Web GUI displays the edit, copy and delete menu.



Codec Policy

Search Criteria: All

Name	Allow Codecs
Codec Policy 1	
Codec Policy 2	
Codec Policy 3	

When you click Delete, the system displays a confirmation dialog before performing the operation. When you click either Copy or Edit, the GUI displays the configuration dialog.

To delete all configurations at the same time, use Delete All.

Caution:

You cannot select several instances and delete only those. The system deletes them all, regardless of how many you select. For example, if you select two of three configurations and click Delete All, the system deletes all three.

Media Manager Configuration

Use the Media Manager configuration object to define the settings for the media steering functions performed by the Oracle® Enterprise Session Border Controller (E-SBC), including timer limits, logging, and trust levels.

You can configure the following Media Manager objects from the Configuration tab on the Web GUI. See the documentation specified in the following list for explanations of these configuration objects and how to set their parameters.

Codec Policy	Create a codec policy to specify allowed codecs, the order of codecs, and codecs to add on egress. See "Codec Policy Configuration" in the *ACLI Configuration Guide*.
DNS ALG Constraints	Configure and enable DNS ALG constraints. See the "DNS ALG Service Name Configuration" section of the "Application Gateway Services" chapter in the *ACLI Configuration Guide*.
DNS Config	Configure the DNS ALG service. See "DNS Configuration" in the *ACLI Configuration Guide*.
ICE Profile	Configure ICE profile. See "Configure ICE Profile" in the *ACLI Configuration Guide*.
Media Manager	Configure media steering functions. See "Creating Steering Pools for Multiple Interface Realms" in the *ACLI Configuration Guide*.

Media Policy	Configure a media policy and ToS settings. See "Packet Marking Configuration" in the *ACLI Configuration Guide*.
MSRP Config	Configure and enable MSRP. See "RCS Services" in the *ACLI Configuration Guide*.
Playback Config	Configure media use for playback. See "Local Media Playback" in the *ACLI Configuration Guide*.
Realm Config	Configure a realm for media management. See "Realms and Nested Realms" in the *ACLI Configuration Guide*.
Realm Group	Configure realm groups for local media playback. See "Configuring Realm Groups" in the *ACLI Configuration Guide*.
RTCP Policy	Configure an RTCP policy. See "Configuring RTCP Generation" in the *ACLI Configuration Guide*.
Static Flow	Configure static network traffic flows. See "Static Flows" in the *ACLI Configuration Guide*.
Steering Pool	Specify one or more ports for steering media flows. See "Steering Pools" in the *ACLI Configuration Guide*.
TCP Media Profile	Configure the TCP media profile and profile entries. See "Configure TCP Media Profile" in the *ACLI Configuration Guide*.

Codec Policy Configuration

Codec policies describe how to manipulate SDP messages as they cross the Oracle® Enterprise Session Border Controller (E-SBC). The E-SBC bases its decision to transcode a call on codec policy configuration and the SDP. Each codec policy specifies a set of rules to be used for determining which codecs are retained or removed, and how they are ordered within SDP.

When configuring transcoding, you create a codec policy and associate the policy to a realm. In the codec policy, you specify:

- Which codecs to allow and which codecs to deny within a realm.
- Which codecs to add to the SDP m= lines for an egress realm.
- The preferred order of codecs shown in an SDP m= line.
- The packetization time to enforce within a realm for transrating.

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. Or, you might want to add codecs for transcoding. To simplify SIP end point management, the E-SBC can apply global codec policy enforcement to all end points.

Use the codec-policy configuration element to specify how the E-SBC handles codecs, and which codecs you want to allow.

1. Access the Codec Policy configuration object: **Configuration**, **Media Manager**, **Codec Policy**.
2. On the Add Codec Policy page, do the following:

Name	Enter a unique name for this policy.
Allow Codecs	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. • 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. • 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.
Add Codecs 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 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 (( )).
Force Ptime	Select to force a specified packetization time on the egress offer.
Packetization Time (ptime)	Enter the preferred time for an outgoing SDP offer, if you plan to enable Force Ptime. Valid values: • PCMU 10, 20, 30, 40, 50, 60 • PCMA 10, 20, 30, 40, 50, 60 • G729 10, 20, 30, 40, 50, 60 • G729A 10, 20, 30, 40, 50, 60
Secure DTMF Cancellation	Select to remove all traces of DTMF tones at ingress making them completely silent on egress. Requires DTMF in Audio.
DTMF in Audio	Select to handle DTMF in audio streams. Required for secure DTMF cancellation.
Tone Detect Renegotiate Timer	Set the time in milliseconds after which the system sends a re-invite, when the E-SBC has not received a re-invite from the endpoint. Default: 500.
Reverse Fax Tone Detection Reinvite	Select to force the E-SBC to send a re-invite to a realm other than the one on which fax tone detection is enabled.

EVRC TTY Baudot Transcode	Select to enable transcoding of EVRC TTY TDD to BAUDOT in EVRC-G7.11 transcoded calls. Default: Disabled.

3. Save and activate the configuration.

Configure DNS ALG Constraints

You can limit throughput bound for DNS ALG by using the DNS ALG Constraints configuration element. The system performs message throttling on request messages, and the responses are automatically throttled because DNS-ALG is transaction stateful. The system displays a list of configured DNS ALG Constraints in the DNS Config dialog, which allows you to create constraint profiles and apply them to multiple DNS configuration objects.

This procedure requires you to enter rate and time constraints, which you might want to determine in advance. Note that 0 (zero) means unlimited.

1. Access the DNS ALG Constraints configuration object: **Configuration**, **Media Manager**, **DNS ALG Constraints**.
2. On the DNS ALG Constraints page, click **Add**.
3. On the Add DNS ALG Constraints page, do the following:

Name	Enter a unique name for this constraint.
State	Select to enable.
Max Burst Rate	Set the maximum burst rate in requests per second. Default: 0. (0 = unlimited.) Range: 0-4294967295.
Max Sustain Rate	Set the maximum sustain rate in requests per second. Default: 0. (0 = unlimited.) Range: 0-4294967295.
Max Inbound Burst Rate	Set the maximum inbound burst rate in requests per second. Default: 0. (0 = unlimited.) Range: 0-4294967295.
Max Inbound Sustain Rate	Set the maximum inbound sustain rate in requests per second. Default: 0. (0 = unlimited.) Range: 0-4294967295.
Max Outbound Burst Rate	Set the maximum outbound burst rate in requests per second. Default: 0. (0 = unlimited.) Range: 0-4294967295.
Max Outbound Sustain Rate	Set the maximum outbound sustain rate in requests per second. Default: 0. (0 = unlimited.) Range: 0-4294967295.
Time to Resume	Set the time to wait, in seconds, after the constraints are exceeded to resume monitoring. Default: 0. (0 = unlimited.) Range: 0-4294967295.
Burst Rate Window	Set the time, in seconds, over which to compute the burst rate. Default: 0. (0 = unlimited.) Range: 0-4294967295
Sustain Rate Window	Set the time, in seconds, over which to compute the sustain rate. Default: 0. (0 = unlimited.) Range: 0-4294967295.
Max Latency	Set the maximum round trip time, in seconds. Default: 0. (0 = unlimited.) Range: 0-4294967295.

4. Click **OK**.

5. Save the configuration.

- Apply the constraint to a DNS configuration.

Configure DNS

Use the DNS Config element to configure the DNS ALG service.

- 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.

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

1. Access the DNS Config configuration object: **Configuration**, **Media Manager**, **DNS Config**.
2. On the Add DNS Config page, to the following:

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. Default: Disabled.
Extra DNSALG Stats	Select to enable. Default: Disabled.
DNS Max TTL	Set the maximum number of TTL seconds for a DNS response. Default: 86400. Range: 30-2073600.
Client Address List	Click **Add** to add one or more client address lists, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another client address list, and click • Click **OK**. Repeat as needed.
Server DNS Attributes	Click **Add** to add server DNS attributes, and do the following: • Server Realm—Select the server realm from the drop-down list. • Domain Suffix—Click **Add**, add a domain suffix list and click **OK**, or add another domain suffix list, click **OK**, and repeat as needed. • Server Address List—Click **Add**, add a server address list and click **OK**, or add another server list, click **OK**, and repeat as needed. • Source Address—Enter the source IPv4 address.

	• Source Port—Enter the source port. Range: 1025-65535. • Transaction Timeout—Enter the time in seconds for the DNS transaction timeout. Range: 0-999999999. 0 = unlimited. • Address Translation—Click **Add**, enter the Server Prefix and Client Prefix.

3. Click **OK**.
4. Click **OK**.
5. Click **OK**.
6. Save the configuration.

Configure ICE Profile

Interactive Connectivity Establishment - Session Traversal Utility for NAT (ICE STUN lite mode) enables a Advanced Media Termination client to perform connectivity checks, and can provide several STUN servers to the browser. ICE STUN support requires configuring an **ICE Profile** under **Realm Config**, where you define the STUN behavior.

- Confirm that the realm to which you want to apply this profile exists.

Use the following steps to create an **ICE Profile**.

1. Access the ICE Profile configuration object: **Configuration**, **Media Manager**, **ICE Profile**.
2. In the **Add ICE Profile** dialog, do the following:

Name	Set a unique name for this ice profile. Default: Empty.
Stun Conn Timeout	Set the maximum time interval, in seconds, between the first STUN binding request received in a media session and the time when a valid STUN binding request containing the USE CANDIDATE attribute is received. Default: 10. Range: 0-9999.
Stun Keepalive Interval	Set the interval, in seconds, since the last media packet or STUN binding request response after which a STUN keep alive message is sent. Default: 15. Range: 0-300. Zero means do not send keep-alive messages. The value must be less than the value set for subsq-guard-timer.
Stun Rate Limit	Set the number of STUN binding requests that you want the SBC to process per minute. Default: 100. Range: 0-99999. Zero means impose no limit.

3. Click **OK**.

- Set the **ICE Profile** parameter in **Realm Config**. See "Configure Advanced Media Termination in realm-config."

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.

1. Access the Media Manager configuration object: **Configuration**, **Media Manager**, **Media Manager**.
2. On the Media Manager page, do the following:

State	Select to enable Media Manager.
Flow Time Limit	Enter the time limit, in seconds, for a media flow. Default: 86400. Range: 0-4294967295.
Initial Guard Timer	Enter the time limit, in seconds, for a media flow guard timer. Default: 300. Range: 0-4294967295.
Subsq Guard Timer	Enter the time limit, in seconds, for a subsequent media flow guard timer. Default: 300. Range: 0-4294967295.
TCP Flow Time Limit	Enter the time limit, in seconds, for a TCP flow. Default: 86400. Range: 0-4294967295.
TCP Initial Guard Timer	Enter the time limit, in seconds, for the initial TCP flow. Default: 300. Range: 0-4294967295.
TCP Subsq Guard Timer	Enter the time limit, in seconds, for a subsequent TCP flow. Default: 300. Range: 0-4294967295.
Hnt RTCP	Select to enable RTCP for hosted NAT traversal.
ALGD Log Level	Select an ALGD log level from the drop-down list. Default: NOTICE.
MBCDLog Level	Select an MBCD log level from the drop-down list. Default: NOTICE.
Options	Add any optional parameters.
Red Max Trans	Set the number of redundancy sync transactions to keep. Default: 10000. Range: 0-50000.
Red Sync Start Time	Set the timeout for checking the transition from standby to active. Default: 5000. Range: 0-4294967295.
Red Synch Comp Time	Set the timeout for subsequent synch requests after a redundancy synch occurred. Default: 1000. Range: 0-4294967295.
Media Policing	Select to enable per session traffic rate policing in a media gateway. Default: Enabled.
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. Default: 10. Range: 20 to 10000.
Tolerance Window	Set the tolerance window size in seconds for measuring host access limits. Default: 30. Range: 0-4294967295.
Trap on Demote to Deny	Select to generate a trap when the endpoint is demoted from untrusted to deny. Default: Disabled.
Trap on Demote to Untrusted	Select to generate a trap when the endpoint is demoted from trusted to untrusted. Default: Disabled.
Syslog on Demote to Deny	Select to generate Syslog when the endpoint is demoted from untrusted to deny. Default: Disabled.
Syslog on Demote to Untrusted	Select to generate Syslog when the endpoint is demoted from trusted to untrusted. Default: Disabled.
Anonymous SDP	Select to enable the Use Name and Session Name fields in Session Description Protocol (SDP). Default: Disabled.
Translate Non rfc283 Event	Select to accept UII/INFO events for Inter-working Function (IWF), although RFC2833 is preferred. Default: Disabled.
Syslog on Call Reject	Select to enable Syslog on SIP call rejection.

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

Generate an RTCP Receiver Report

When you want to generate a Real-Time Transport Control Protocol (RTCP) Receiver Report separately from the default Sender-Receiver Report (RFC 3550), for example to encapsulate the receiver statistics differently, add the `xcode-gratuitous-rtcp-report-generation` option in the media-manager configuration. After you add the option and reboot the system, the E-SBC runs RTCP Receiver Reports for all media sessions that generate RTCP from DSPs.

When you add the `xcode-gratuitous-rtcp-report-generation` option, be sure to type the **+** character before the option. The **+** character appends the new option to the realm configuration's options list. Without the + character, the system overwrites any previously configured options.

1. Access the Media Manager configuration object: **Configuration**, **Media Manager**, **Media Manager**.
2. Go to the Options parameter, and do the following.
   a. Click **Add**.
   b. In the Add dialog, enter `+ xcode-gratuitous-rtcp-report-generation`.
   c. Click **OK**.

3. Save and activate the configuration.
4. Reboot the system.

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.

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)

1. Access the Media Policy configuration object: **Configuration** , **Media Manager**, **Media Policy**.
2. On the Media Policy page, click **Add**.
3. On the Add Media Policy page, do the following:

Name	Enter a name for this media policy.
TOS settings	Click **Add**.
Add Media Policy / ToS Settings	• Media Type—Enter any IANA-defined media type to use for this group of TOS settings. Range: 1-255 characters. Not case-sensitive. • Media Sub Type—Enter any IANA-defined media sub-type for the media type. Range: 1-255 characters. Not case-sensitive. • 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 med a types. Use decimal (0.0) or hexadecimal number (0x00) format. Default is hexadecimal 0x00. • Media Attributes—Click **Add**, 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, use a comma separator.

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

Configure a Realm

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

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

Note:

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

1. Access the Realm Config configuration object: **Configuration**, **Media Manager**, **Realm Config**, **Add**.
2. In the Realm Config object, do the following:

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 theE-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.
RTCP Mux	Select to enable RTCP multiplexing negotiation. Default: disabled. Valid values disabled | enabled.
ICE Profile	Specify an existing ICE profile. Default: none.

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.
InTtranslationid	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.
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	Select a restricted latching mode.
Options	Enter one or more optional features and parameters.
SPL Options.	Enter one or more SPL options.

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 Reinvite	Select to enable the hold-refer-reinvite option. Default: Disabled.
Refer Notify Provisional	Select the provisional mode for sending a NOTIFY message from the drop down list. Default: None. Valid values: None | Initial | All.
Dyn Refer Term	Select to enable terminating refer call transfer for this realm. Default: Disabled.
Codec Policy	Set 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. Default: Disabled.
Codec ManIP in Network	Select to enable codec policy for this network. Default: Disabled.
RTCP policy	Select the RTCP policy for this realm.
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. Use + to add the list. Use - to remove the list. Excluding + or -, replaces the list.
Node Functionality	Select a node function from the drop down list.

3. Save 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.

- Configure and name the network interface to which you want to steer media.

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

1. Access the Steering Pool configuration object: **Configuration**, **Media Manager**, **Steering Pool**.
2. On the Steering Pool page, do the following:

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.

3. Save the configuration.

Configure TCP Media Profile

The TCP Media Profile defines media operations in a realm. You can create multiple TCP Media Profiles, for example, to assign to different realms.

1. Access the TCP Media Profile configuration object: **Configuration**, **Media Manager**, **TCP Media Profile**, **Add**.
2. On the Add TCP media profile page, enter a **Name** for this profile. Required before you can proceed.
3. Under Profile List, click **Add**.
4. On the Add TCP media profile / profile entry page, do the following:

Media type	Set the media type subject to this profile. Default: message. Keep the default value for MSRP operations.
Transport Protocol	Set the Transport Layer Protocol (TLS) that you want for this profile. Use either **TCP/MSRP** to specify unsecured TCP traffic or **TCP/TLS/MSRP** to specify secured and encrypted TLS traffic.
Listen Port	Set the TCP port to use for incoming B2BUA MSRP connections. Range: 0-65535. Default: 0, which tells the B2BUA to choose the port from the steering pool of the realm associated with this profile.
Preferred Setup Role	Set the value the B2BUA uses for the a=setup attribute when negotiating the setup role. Valid values: Active (Allows the B2BUA to create an outgoing connection.) | Passive. Default: Passive (Allows the B2BUA to accept an incoming connection.) Oracle recommends Passive.

TLS Profile	If you set **TCP/TLS/MSRP** for transport-protocol, select a TLS profile that specifies cryptographic resources available to support TLS operations.
Require Fingerprint	If you set **TCP/TLS/MSRP** for transport-protocol, enable TLS fingerprint for endpoint authentication using the certificate fingerprint methodology defined in RFC 4572 *Connection-Oriented Media Transport over the Transport Layer Security (TLS) Protocol in the Session Description Protocol (SDP)*.. Valid values: enabled | disabled. Default: disabled.
MSRP CEMA Support	Specify whether or not the SBC negotiates support for the CEMA extension (RFC6714) for TCP or TLS connections to and from the realm associated with the current TCP media profile. Enable the CEMA extension to enable the SBC to exchange MSRP traffic through middleboxes that anchor the media, but do not touch the SDP a:path attribute. Valid values: enabled | disabled. Default: disabled.
MSRP Sessmatch	Specify whether or not the SBC validates the MSRP To-Path header based only on the session-id field and MSRP transport type of the MSRP URI (and not also on the IP address and port number in the authority part of the MSRP URI). Sessmatch enables the SBC to exchange MSRP traffic through Middleboxes that anchor the media and also adjust the SDP a=path attribute. Valid values: enabled | disabled. Default: disabled.
MSRP Message Size Enforce	Specify one element in a whitelist of allowed MSRP media types. Media types not included on the whitelist will be removed from the SDP a=accept-types attribute of the SDP offers. A "*" indicates that all MSRP media types are allowed. When left empty, it indicates that no media types filtering is performed. Valid value: MsrpMediaTypeList.
MSRP Message Size	Specify the maximum size (in bytes) that MSRP is allowed to negotiate for the messages. It represents the maximum limit for the SDP a=max-size attribute, for the "size" token of the SDP a=file-selector attribute and MSRP Byte-range header. A value of 0 indicates that no maximum limit is enforced. Valid values: 0-4,000. Default: 0.
MSRP Message Size File	Specify whether MSRP messages exceeding the negotiated size are rejected, respectively whether MRSP file transfers will be aborted when the negotiated size is exceeded. A value of 0 indicates that no maximum limit is enforced. Valid values: 0-4G. Default: 0.

MSRP Types Whitelist	Specify a list of registered MSRP media types (RFC4975) supported for the ingress realm.

5. Click **OK**.
6. Click **Back**.
7. (Optional) Repeat the preceding steps to configure another tcp-media-profile.
8. Save the configuration.

Advanced Media Termination Support

The Oracle® Enterprise Session Border Controller (E-SBC) supports VoIP calls through the browser-based, real-time communication known as Advanced Media Termination. Using W3C and IETF standards, Advanced Media Termination supports cross-browser video calls and data transfers, such as browser-based VoIP telephony and video streaming. Advanced Media Termination allows users to make and receive calls from within a web browser, relieving the need to install a soft phone application. With Advanced Media Termination, the E-SBC can enable users to communicate concurrently with one or more peers through various browsers and devices to stream voice and data communications in real-time through a variety of web applications. Advanced Media Termination also supports communications through end-user clients such as mobile phones and SIP User Agents.

Advanced Media Termination supports clients

- connected to networks with different throughput capabilities.
- on variable media quality networks (wireless).
- on fire-walled networks that don't allow UDP.
- on networks with NAT or IPv4 translation devices using any type of mapping and filtering behaviors (RFC 4787).

Supported Advanced Media Termination Services

The E-SBC supports the following services and functions for Advanced Media Termination:

- ICE-STUN (Lite mode) - Interactive Connectivity Establishment - Session Traversal Utility for NAT (ICE-STUN) enables an Advanced Media Termination client to perform connectivity checks. Use ICE to provide several STUN servers to the browser by way of the application. ICE processing chooses which candidate to address. Other benefits include support for IPv4, load balancing, and redundancy. ICE STUN support requires configuring an **ICE Profile** and specifying the profile in **Realm Config**. See "Configure ICE Profile" and "Configure Advanced Media Termination in Realm Config."
- RTP-RTCP multiplexing - Enables Real-Time Protocol (RTP) and Real-Time Control Protocol (RTCP) packets to use the same media port numbers. RTP is used for real-time multimedia applications, such as internet audio and video streaming, VoIP, and video conferencing. RTCP is used to monitor data transmission statistics and QoS, and helps to synchronize multiple streams. RTP-RTCP support requires enabling **RTCP Mux** in **Realm Config**. See "Configure Advanced Media Termination in Realm Config."
- DTLS-SRTP - Datagram Transport Layer Security (DTLS) provides integrated key and association management for secure data transfer for point-to-point media

sessions. DTLS is especially optimized for use with Secure Real Time Protocol (SRTP), where it enables a Advanced Media Termination client to establish keys for SRTP and Secure Real Time Control Protocol (SRTCP). DTLS-SRTP support requires configuring a **DTLS SRTP Profile** under **Media Security**, and specifying the profile in the **Realm Config**. See "Configure DTLS SRTP Profile" and "Configure Advanced Media Termination in realm-config."

- SIP services including codec renegotiation, late media, early media, PACK interworking, attended and unattended call transfer, call forking, music on hold, transcoding, and High Availability.

Supported Protocols

The E-SBC supports the following protocols for Advanced Media Termination.

- IPv4 for signaling and media
- UDP-RTP and UDP-RTCP on media

Supported Codecs

The E-SBC supports the following codecs for Advanced Media Termination.

- Silk, OPUS, G.729, and G.711

Advanced Media Termination Configuration Process

To configure Advanced Media Termination for theOracle® Enterprise Session Border Controller, access the Security and Media Manager configuration objects to create the necessary profiles and associations. For RTCP Multiplexing support, you need only to enable it in the target realm. Advanced Media Termination is configurable in real-time. The system does not require a reboot.

- Confirm that the realm you want to configure for Advanced Media Termination exists.
- Confirm that the TLS profile that you want to specify in the **DTLS SRTP Profile** exists.

The process for configuring Advanced Media Termination includes the following tasks:

1. In Security: Configure **DTLS SRTP Profile**, where you define the key exchange and DTLS handshake, the role the SBC negotiates when offered alternatives, and the crypto suites to use. See "Configure DTLS SRTP Profile."
2. In Media Manger:
   a. Configure **ICE Profile**, where you define STUN behavior. See "Configure ice-profile."
   b. Configure **Realm Config**, where you specify the **DTLS SRTP Profile**, the **ICE Profile**, and enable **RTCp Mux**. See "Configure Advanced Media Termination in Realm Config."

Configure DTLS SRTP Profile

To provide Datagram Transport Layer Security-Secure Real Time Control Protocol (DTLS-SRTP) Advanced Media Termination services on the SBC, you must create a **DTLS SRTP Profile**. This profile defines the key exchange and DTLS handshake on a media session, the role the SBC negotiates when offered alternatives, and the crypto suites to use. After you create this profile, enter its name in the **DTLS SRTP Profile** parameter in the **Realm Config**.

1. Access the DTLS SRTP Profile configuration object: **Configuration**, **Security**, **Media Security**, **DTLS SRTP Profile**, **Add**.
2. Do the following:

Name	Set a unique name for this DTLS profile. Default. Empty.
TLS Profile	Set the name of an existing TLS profile that defines the key exchange scheme used by the DTLS handshake. Default: Empty.
DTLS Complete Timeout	Set the maximum time interval, in seconds, between the moment when the DTLS handshake on a media session is initiated and the moment when the DTLS handshake is completed. Default: 10. Range: 0-9999.
Preferred Setup Role	Set to "passive," so that the Advanced Media Termination client always initiates the DTLS handshake. Default: Passive.
Crypto Suite	Set the crypto suites that the SBC negotiates in the use-srtp DTLS extension for this profile. Default: SRTP_AES128_CM_HMAC_SHA1_80. Valid values: SRTP_AES128_CM_HMAC_SHA1_80 and SRTP_AES128_CM_HMAC_SHA1_32.

3. Save the configuration.

- Specify this **DTLS SRTP Profile** in the **Realm Config**.

Configure ICE Profile

Interactive Connectivity Establishment - Session Traversal Utility for NAT (ICE STUN lite mode) enables a Advanced Media Termination client to perform connectivity checks, and can provide several STUN servers to the browser. ICE STUN support requires configuring an **ICE Profile** under **Realm Config**, where you define the STUN behavior.

- Confirm that the realm to which you want to apply this profile exists.

Use the following steps to create an **ICE Profile**.

1. Access the ICE Profile configuration object: **Configuration**, **Media Manager**, **ICE Profile**.
2. In the **Add ICE Profile** dialog, do the following:

Name	Set a unique name for this ice profile. Default: Empty.
Stun Conn Timeout	Set the maximum time interval, in seconds, between the first STUN binding request received in a media session and the time when a valid STUN binding request containing the USE CANDIDATE attribute is received. Default: 10. Range: 0-9999.
Stun Keepalive Interval	Set the interval, in seconds, since the last media packet or STUN binding request response after which a STUN keep alive message is sent. Default: 15. Range: 0-300. Zero means do not

	send keep-alive messages. The value must be less than the value set for subsq-guard-timer.
Stun Rate Limit	Set the number of STUN binding requests that you want the SBC to process per minute. Default: 100. Range: 0-99999. Zero means impose no limit.

3. Click **OK**.

- Set the **ICE Profile** parameter in **Realm Config**. See "Configure Advanced Media Termination in realm-config."

Configure Advanced Media Termination in Realm Config

To support Advanced Media Termination functionality, the Oracle® Enterprise Session Border Controller (E-SBC) requires setting the parameters for **RTCP Mux**, **DTLS SRTP Profile**, and **ICE Profile** in **Realm Config**.

- Confirm that the realm exists that you want to configure for Advanced Media Termination operations.
- Confirm that the **DTLS SRTP Profile** and the **ICE Profile** exist.

1. Access the Realm Config configuration object: **Configuration**, **Media Manager**, **Realm Config**, **Add**.
2. Do the following:

RTCP MUX	Specify "enable" to turn on RTCP multiplexing support. Default: Disable.
DTLS SRTP Profile	Specify the dtls-srtp-profile to associate with this realm. Default: Empty.
ICE Profile	Specify the ice-profile to associate with this realm. Default: Empty.

3. Save the configuration.

Advanced Media Termination Troubleshooting

The Oracle® Enterprise Session Border Controller (E-SBC) provides Session Traversal Utility for NAT (STUN) and Datagram Transport Layer Security (DTLS) tracing.

To set STUN and DTLS tracing, go to **Media Manager**, **Media Manager** and set **Options** to "stun-trace dtls-trace". The E-SBC stores the STUN and DTLS traces in the Advanced Media Termination.log file.

Debug logs: log.sipd, log.mbcd, sipmsg.log, Advanced Media Termination.log

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 to help 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 numerous features and architecture designs of the Net-SAFE framework. 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. See the documentation specified in the following list for explanations of these configuration objects and how to set their parameters.

Audit Logging	Configure the size, location, and conditions that trigger the transfer of logs to the specified location. See "Configure the Audit Log" in the "Audit Log" chapter in the *Administrative Security Guide*.
Auth Params	Configure authentication protocol, strategy, and servers. See the "Authentication and Authorization" section in the "Access" chapter in the *Administrative Security Guide*.
Authentication	Configure RADIUS and TACACS authentication. See "RADIUS Authentication" and "TACACS+" in the *ACLI Configuration Guide*.
Certificate Record	Create a certificate record for either a CA or end entity. See "Certificate Configuration Process" in the *ACLI Configuration Guide*.
IKE Accounting Param	See the "IKEv2 Global Configuration" and "Configuring IKEv2 Interfaces" chapters in the *Administrative Security Guide*.
DTLS SRTP Profile	Configure the key exchange and DTLS handshake on a media session, the role the SBC negotiates when offered alternatives, and the crypto suites to use. See the "Configure DTLS SRTP Profile" section in the "Advanced Media Termination Support" chapter of the *ACLI Configuration Guide*.
Password Policy	Create a password policy. See the "Password Policy" section in the "Access" chapter in the *Administrative Security Guide*.
Public Key	Set the public key type and size. See the *Administrative Security Guide*.
Security Config	Configure security for VoIP and other multi-media services. See the "Security" chapter in the *ACLI Configuration Guide*.
SSH Config	Configure the system for an SSH connection. See "SSH Remote Connections" in the *ACLI Configuration Guide*.
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. See "Configure a TLS Profile" in the *ACLI Configuration Guide*.

Audit Logs

The Oracle® Enterprise Session Border Controller (E-SBC) can record user actions in audit logs by way of the Web GUI. The audit logs record the creation, modification, and deletion of all user-accessible configuration elements, as well as attempted access to critical security data such as public keys. For each logged event, the system provides the associated user-id, date, time, event type, and success or failure data.

You can configure the system to record audit log information in either verbose mode or brief mode. Verbose mode captures the system configuration after every change, and displays both the previous settings and the new settings in addition to the event details. Brief mode displays only the event details. Although you can specify the recording mode, you cannot specify which actions the system records. The following list describes the actions that the system records.

Global	• Log on and log off. • Save a template configuration. • Click **Complete** in a Wizard.
Home tab	• Add, reset, and save. • Change Widget settings.
Configuration tab	• Save and activate a configuration. • Discard a configuration. • Add, edit, delete, and copy configuration changes. • Run the generate and import certificate commands.
System tab	• Add audit entries to the system file management actions, such as upload, download, restore, backup, add, edit, and delete. • Force an HA switch over. • Run the Show Support Information command. • Run the Upgrade Software wizard. • Download and view an audit log.
Monitoring tab	• Export the summary. • Export the session detail. • Export from a Widget. • Add a Widget to favorites. • Clear, clear all on alarm, add, and delete license.

The system writes audit log events in Comma Separated Values (CSV) lists in the following format:

```
{TimeStamp,
src-user@address:port,Category,EventType,Result,Resource,Prev,
Detail}
```

The following list describes each value written to an audit log event.

TimeStamp	Shows the time when the system wrote the event to the audit log.
src-user@address:port	Identifies the system that wrote the audit log line.
Category	Classifies the event as: • Configuration • Security • System
EventType	Identifies the action that caused the event as: • Activate-config • Acquire-config • Create • Data-access • Delete • Halt • Login • Logout • Modify • Reboot • Save-config
Result	Identifies the outcome of the event as: • Failure • Success
Resource	Describes the action within the event. Some of the numerous actions that the system can log include: • Authentication • Banner (Means that someone edited the log on banner text.) • Download <filename> • Generate public key

	• Reboot • Upload <filename>
Prev—(verbose mode)	Displays the setting prior to this change.
Details—(verbose mode)	Displays additional information about the change, depending on the following event types: • Create—displays “New = element added." • Data-access—displays “Element = accessed element.” • Delete—displays “Element = deleted element.” • Modify—displays “Previous = oldValue New = newValue.”

As the E-SBC records audit log data, users with admin privileges can read, copy, and download that information from the Web GUI. No one can delete or edit the original log. You can View, Refresh, and Download audit logs by way of the System tab. Go to Audit Log under File Management.

You can configure the system to transfer audit log files to an SFTP server by way of secure FTP push, when conditions satisfy one of the following specifications.

- The specified amount of time since the last transfer elapsed.
- The size of the audit log reached the specified threshold. (Measured in Megabytes)
- The size of the audit log reached the specified percentage of the allocated storage space.

The E-SBC transfers the audit logs to a designated directory on the target SFTP server. The audit log file is stored on the target SFTP server with a filename in the following format: **audit<timestamp>**. The timestamp is a 12-digit string the YYYYMMDDHHMM format.

Use the following process to configure transferring audit logs to an SFTP server.

1. Configure secure FTP push. See "Secure FTP Push Configuration."
2. Configure audit logging. See "Configure Audit Logging."

Secure FTP Push Configuration

You can configure the Oracle® Enterprise Session Border Controller (E-SBC) to securely send audit log files to an SFTP push receiver for storage. Configure secure FTP push before you configure audit logging.

You can configure the Oracle® Enterprise Session Border Controller (E-SBC) to log on to a push receiver using one of the following authentication methods to create a secure connection.

Password
Configure a username and password, and leave the **public-key** parameter blank. Note that you must also import the host key from the SFTP server to the E-SBC for this type of authentication.

Public key
Set the **public-key** parameter to a configured public key record name including an account **username**, and configure the SFTP server with the public key pair from the E-SBC.

It is also common for the SFTP server to run the Linux operating system. For Linux, the command ssh-keygen-e creates the public key that you need to import to the E-SBC. The ssh-keygen-e command sequence requires you to specify the file export type, as follows.

```
[linux-vpn-1 ~]# ssh-keygen -e
Enter file in which the key is (/root/.ssh/id_rsa/): /etc/ssh/
ssh_host_rsa_key.pub
```

If you cannot access the SFTP server directly, but you can access it from another Linux host, use the ssh-keyscan command to get the key. An example command line follows.

```
root@server:~$ssh-keyscan -t dsa sftp.server.com
```

Configure Secure FTP Push with Public Key Authentication

For increased security when sending files from the Oracle® Enterprise Session Border Controller (E-SBC) to an SFTP server, you can choose authentication by public key exchange rather than by password. To use a public key exchange, you must configure public key profiles on both devices and import the key from each device into the other.

The following list of tasks shows the process for configuring authentication by public key between the E-SBC and an SFTP server. For each step in the process, see the corresponding topic for detailed instructions.

1. Generate an RSA public key on the E-SBC. See "Generate an RSA Public Key."
2. Create a DSA public key on the SFTP server. See "Generate a DSA Public Key."
3. Import the DSA public key from the SFTP server into the E-SBC using the **known-host** option in the Import Key dialog. See "Import a DSA Public Key."
4. Add the RSA public key to the authorized_keys file in the .ssh directory on the SFTP server. See "Copy the RSA Public Key to the SFTP Server."

Generate an RSA Public Key

Add a public key profile on the Oracle® Enterprise Session Border Controller (E-SBC) and generate an RSA key. You will later import the RSA key into the SFTP server to enable authentication by way of public key exchange with the E-SBC.

1. Access the Public Key configuration object: **Configuration**, **Security**, **Public key**.
2. On the Public Key page, click **Add**.
3. In the Add Public Key dialog, do the following:

Name	Enter the name of this profile.
Type	Select RSA.
Size	Enter one of the following:

	• 512 • 1024 • 2048 • 4096

4. Click **OK** to create the public key profile.

   The system displays the Public Key list box including the new profile.
5. Save and activate the configuration.
6. Select the newly created profile, and click **Generate key**.

   The E-SBC displays the key in the Generate Key text box for you to copy to the SFTP server.
7. Save the configuration.

- Generate a DSA public key.

Generate a DSA Public Key

Generate and save a DSA public key on the SFTP server. You will later import the DSA key into the Oracle® Enterprise Session Border Controller (E-SBC) to enable authentication by way of public key exchange with the SFTP server.

1. Run the following command on the SFTP server:
   ssh-keygen -e -f /etc/ssh/ssh_host_dsa_key.pub | tee sftp_host_dsa_key.pub
2. Save the key to the authorized_keys file in the .ssh directory on the SFTP server.

- Import the DSA key into the E-SBC.

Import a DSA Public Key

Import a DSA public key from the SFTP server into the Oracle® Enterprise Session Border Controller (E-SBC).

- Generate and save a DSA public key on the SFTP server.

Perform the following procedure on the E-SBC and select "known-host" for type.

1. Access the SSH file system on the SFTP server by way of a terminal emulation program.
2. On the SFTP server, copy the base64 encoded public file. Be sure to include the Begin and End markers, as specified by RFC 4716 *The Secure Shell (SSH) Public Key File Format*.

   For OpenSSH implementations host files are generally found at `/etc/ssh/ssh_host_dsa_key.pub`, or `/etc/ssh/sss_host_rsa.pub`. Other SSH implementations can differ.
3. On the E-SBC, click **Configuration**, **Security**, **Public Key**.
4. On the Public key page, click **Import key**, and do the following.

Type	Select known-host.

Name	Enter a name for your profile, which the E-SBC displays in public key drop-down lists.
SSH Public Key	Paste the DSA public key from the SFTP server into the text box. Ensure that the text of the key ends with a semi-colon.

5. Click **Import**.

   The E-SBC imports the key and makes it available for configuration as the public key on an external device.

Copy the RSA public key to the SFTP server.

Copy the RSA Public Key to the SFTP Server

Copy the RSA public key from the from the Oracle® Enterprise Session Border Controller (E-SBC) to the authorized_keys file in the .ssh directory on the SFTP server.

- Confirm that the .ssh directory exists on the SFTP server.
- Confirm the following permissions: Chmod 700 for .ssh and Chmod 600 for authorized_keys.

When adding the RSA key to the authorized_keys file, ensure that no spaces occur inside the key. Insert one space between the ssh-rsa prefix and the key. Insert one space between the key and the suffix. For example, ssh-rsa <key> root@1.1.1.1.

1. Access the SSH file system on a configured SFTP server with a terminal emulation program.
2. Copy the RSA key to the SFTP server, using a text editor such as vi or emacs, and paste the RSA key to the end of the authorized_keys file.

Configure Audit Logging

The Oracle® Enterprise Session Border Controller (E-SBC) provides a means of tracking user actions through Audit Logs. You can specify how the system records audit log information, and where to send the logs for archiving. You can configure the system to record in either brief or verbose mode. Verbose mode captures the system configuration after every change, and displays both the previous and new settings in addition to the event details. Brief mode displays only the event details.

- Configure one or more push receivers to receive the audit logs. See the documentation for the receiver.
- If you want to use public keys for authentication between the E-SBC and the push receiver, configure public key profiles on both devices before configuring audit logging. See "Configure Secure File Transfer with Public Keys."

1. Access the Audit Logging configuration object: **Configuration**, **Security**, **Security**, **Admin-Security**, **Audit Logging**.
2. On the Audit Logging page, do the following:

State	Select to enable event recording in the audit log.
Detail Level	Select brief (default) or verbose output.
Audit Trail	Enables logging every command that is processed by the E-SBC.

	• enabled: Logs all commands that the E-SBC can process. • disabled: Logs only relevant information. • Default: disabled
Audit Record Output	Indicates how the E-SBC logs audit records. • syslog: The E-SBC logs audit records over syslog. • file: The E-SBC logs audit records to a file. • both: The E-SBC logs audit records over both syslog and to a file. • Default: file
File Transfer Time	Specify the amount of time, in hours, from the completion of the last transfer to the beginning of the next transfer. This determines when a file transfer occurs unless the Max storage space or Max file size triggers the transfer first. Default: 720. Range: 0-65535. **Note:** 0 disables this parameter.
Max Storage Space	Specify the maximum amount of space that the audit log can consume on the E-SBC in MB. Default: 32. Range: 0-32.
Percentage Full	Use in conjunction with Max storage space to specify the percent of the Max storage space that triggers file transfer. This determines when a file transfer occurs unless the File transfer time or Max file size triggers the transfer first. Default: 75. Range: 0-99. **Note:** 0 disables this parameter.
Max File Size	Set the maximum size in Mega Bytes that the audit log can be before the system transfers the file. This determines when a file transfer occurs unless the Max storage space or Max file size triggers the transfer first. Default: 5. Range 0-10. **Note:** 0 disables this parameter.

Storage Path	Specifies the directory that houses the audit log. Default: /code/ audit .
Push Receiver	Add a push receiver and configure the following parameters for sending audit log files from the E-SBC to the receiver: • Server—Enter the IP address of the FTP/SFTP server to which you want the E-SBC to push audit log files. Default: 0.0.0.0. • Port—Enter the port number on the FTP/SFTP server to which the E-SBC will send audit log files. Default: 22 Range: 1-65535. • Remote Path—Enter the pathname to send the audit log files to the push receiver. Files are placed in this location on the FTP/SFTP server. Value: <string> remote pathname. • Filename Prefix—Enter the filename prefix to prepend to the audit log files that the E-SBC sends to the push receiver. The E-SBC does not rename local files. Values: <string> prefix for filenames. • Username—Enter the username the E-SBC uses to connect to this push receiver. • Auth Type—Select the authentication methodology. Password (default) or public key. • Do one of the following: Password—When you set the Auth type to password, click **Set** to enter and confirm the password used to access this push receiver. Public Key—When you set the Auth type to public key, select the public key profile that you want from the drop-down list.

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

Configure Login Timeouts

The single instance **SSH Config** configuration element specifies SSH re-keying thresholds.

Use the following procedure to set the SSH and TCP timeout values.

1. Access the SSH Config configuration object: **Configuration**, **Security**, **Admin Security**, **SSH Config**.
2. In **SSH Config**, do the following:

Rekey Interval	Set the time in minutes after which the E-SBC re-keys an SSH or SFTP session. Default: 60. Range: 60-600.
Rekey Byte Count	Set the number of bytes transmitted, in powers of 2, before re-keying an SSH or SFTP session. For example, entering a value of 24 sets this parameter to 2^24 (16777216) bytes. Default: 31. Range: 20-31.

Proto Neg Time	Set the time in seconds to complete the SSH protocol negotiation, establishing the secure connection. Default: 60. Range: 30-60.
Keep Alive Enable	Enable the TCP keepalive timer. Default: enabled. Valid Values: enabled | disabled.
Keep Alive Idle Timer	Set the interval in seconds between the last data packet sent and the first keepalive probe. Default: 15. Range: 15-1800.
Keep Alive Interval	Set the interval in seconds between two successful keepalive transmissions. Default: 15. Range: 15-120.
Keep Alive Retries	Set the number of retransmission attempts before the E-SBC declares the remote end unavailable. Default: 2. Range: 2-10.

3. Save the configuration.

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 and Servers

To configure Terminal Access Controller Access-Control System Plus (TACACS+), you enable TACACS+ client services and specify one or more TACACS+ servers.

1. Access the Login Config configuration object: **Configuration**, **Security**, **Admin Security**, **Login Config**.
2. On the Authentication page, do the following:

Source Port	Default: 1812. Range: 1645-1812.
Type	Select TACACS from the drop-down list.
Protocol	Select ACSII for the authentication protocol.
TACACS Accounting	Select to enable accounting of admin operations. Default: Enabled.
Server Assigned Privilege	Select to allow only Admin users to use configuration commands. Default: Disabled.
Allow Local Authentication	Select to enable local authentication. Default: Disabled.
Login as Admin	Select to enable logging in as Admin.
Management Strategy	Select an authentication management strategy from the drop-down list.

	• Use either Hunt or Round-Robin when using multiple TACACS+ servers. • Use Hunt when using a single TACACS+ server. Default: Hunt.
Management Servers	Enter the IP address of a management server.
TACACS Servers	Click **Add**, and do the following: a. Address—Enter the IP address of this server. b. Port—Enter the port number of the server you want to receive TACACS+ client requests. Default: 49. Range: 1025-65535. c. State—Select to enable this server. Default: Enabled. d. Secret—Enter and confirm the 16-digit string for the shared secret used by the TACACS+ client and the server to encrypt and decrypt TACACS+ messages. e. Dead Time—Enter the time, in seconds, for the quarantine period imposed upon a TACACS+ server that becomes unreachable. Default: 10. Range: 10-10000 seconds. f. Authentication Methods—Add one or more authentication methods. Default: All.

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

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 Certificate Records and TLS Profile configurations are located under Security on the Configuration page. Apply TLS profiles to SIP interfaces in the SIP Interface configuration under Session Router.

Certificate Configuration Process

You can perform the following certificate management tasks from the Web GUI in either Basic Mode or Advanced 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.

Create a Certificate Record

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

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. Access the Certificate Record configuration object: **Configuration**, **Security**, **Certificate Record**, **Add**.
2. On the Certificate record page, click **Add**.
3. On the Add certificate record page, do the following:

Name	Enter the name of this certificate record.
Country	Enter the country name abbreviation. For example, CA for Canada. Default: US. Valid Values: 2 country abbreviation characters.
State	Enter the region abbreviation. For example, QC for Quebec. Default: MA. Range: 1-128 characters.
Locality	Enter the name of the locality in the region. For example, Quebec City. Default: Burlington. Range:1-128 characters.
Organization	Enter the name of the organization. For example, Office of Information Technology. Default: Engineering. 1-64 characters.
Unit	Enter the name of the unit in the organization. For example, Global Network Security. Default: Empty. 1-64 characters.
Common Name	Enter the common name for the certificate record. For example, your name. Default: Empty. Range: 1-64 characters.
Key Size	For the RSA key algorithm, set the RSA key size. Valid key size: 512 | 1024 | 2048 | 4096.
Alternate Name	(Optional) Enter one or more alternative names for the certificate holder.
Trusted	Do one of the following: • Select to make the certificate trusted. (Default) • Deselect to make the certificate un-trusted.

Key Usage List	Add one or more keys that you want to use with this certificate record. 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 *ACLI Configuration Guide*.
Extended Key Usage List	Add one or more extended keys that you want to use with this certificate record. This parameter defaults to serverAuth. For a list of other valid values and their descriptions, see the section “Key Usage Control” in the *ACLI Configuration Guide*.
Key Algor	Set a key algorithm. Valid algorithms: rsa | ecdsa.
Digest Algor	Set a digest algorithm. Valid values: sha1 | sha256 | sha384.
ECDSA Key Size	For the ECDSA key algorithm, set the ECDSA key size. Valid key size: p256 | p384.
Cert Status Profile List	Enter a list of configured Cert Status Profile objects.
Options	Set any optional features or parameters that you want.

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

Use the Certificate Record configuration object 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. Access the Certificates configuration object.

   Configuration, **System Administration**, **Security**, **Certificates**.
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 configuration object 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. Access the Certificates configuration object.

   Configuration, **System Administration**, **Security**, **Certificates**.
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**.

   TheE-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.

Configure an SDES Profile

A Session Description Protocol Security Descriptions (SDES) profile specifies the parameter values offered or accepted during SDES negotiation.

In the following procedure, use the **Key** and **Salt** parameters to generate the synchronous key used to encrypt and decrypt SRTP/SRTCP traffic originated by theOracle® Enterprise Session Border Controller (E-SBC). The E-SBC passes these concatenated values to the remote SRTP peer. Upon reception, the remote peer inputs the key and salt values to the negotiated encryption algorithm (AES in the current implementation), and derives the key required to decrypt SRTP/SRTCP traffic received from the E-SBC. The **key** parameter provides the basic keying material, while the salt (a bit string) provides the randomsess/entropy required by the encryption algorithm.

1. Access the SDES Profile configuration object: **Configuration**, **Security**, **Media Security**, **SDES Profile**, **Add**.
2. In SDES Profile, do the following:

Name	Type the unique name of this profile.
Crypto Suite	Add one or more cryptography suites to this profile. Default: AES_CM_128_HMAC_SHA1_80. Valid values: AES_CM_128_HMAC_SHA1_80 | AES_CM_128_HMAC_SHA1_32.
SRTP Auth	Enable authentication of RTP packets. Default: Enable. Valid values: Enable | Disable.
SRTP Encrypt	• Enable to reject an answer that contains an UNENCRYPTED_SRTP session parameter in the crypto attribute. • Disable to not to offer RTP encryption and include an UNENCRYPTED_SRTP session parameter in the SDP crypto attribute and accept an answer that contains an UNENCRYPTED_SRTP session parameter. Default: Enable. Valid values: Enable | Disable.
SRTCP Encrypt	• Enable to offer RTCP encryption, and reject an answer that contains an UNENCRYPTED_SRTCP session parameter in the crypto attribute. • Disable to not offer RTCP encryption and include an UNENCRYPTED_SRTCP session parameter in the SDP crypto attribute; accepting an answer that contains an UNENCRYPTED_SRTCP session parameter. Default: Enable. Valid values: Enable | Disable.
MKI	Enable or disable the use of the master key identifier within the SDP crypto attribute that differentiates one key from another. • Enable—The E-SBC sends an MKI field within the crypto attribute (16 bytes maximum). Express MKI as a pair of decimal numbers in the form: |mki:mki_length| where MKI is the MKI integer value and MKI length is the length of the MKI field in bytes.

	• Disable—The E-SBC sends no MKI field. Default: disable. Valid values: enable | disable.
Egress Offer Format	Set the egress offer format for this profile to use when you also set the outbound mode in the associated media security policy to "any." If the media security policy requires either RTP or SRTP, ignore this parameter. • same-as-ingress—The E-SBC does not change the profile of the media lines. • simultaneous-best- effort—The E-SBC inspects the incoming offer SDP, and adds one of the following: – an RTP/SAVP media line for any media profile that has only the RTP/AVP media profile – an RTP/AVP media line for any media profile that has only the RTP/SAVP media profile Default: same as ingress. Valid values: same as ingress | simultaneous best effort.
Use Ingress Session Params	Add one or more allowable ingress session parameters. Default: None. Valid values: srtcp-encrypt | srtcp-auth | srtcp-encrypt.
Lifetime	Add the lifetime parameter value to a=crypto in the SDP offer. Default: 0 (Do not add lifetime to a=crypto.) Valid values: 20-48. (Express as 2^<value>. For example, using the value 2^20: inline:zYALksQps3ntUw/KsbDdNuxChEQ81Z3BqvTJH|2^20)
Options	Add one or more optional features and parameters.
Key	Type the master key. (for testing purposes)
Salt	Type the master salt. (for testing purposes)
SRTP Rekey on Re-invite	Enable to generate new outbound SRTP keys on every re-invite. Default: Disable. Valid values: Enable | Disable.

3. Save the configuration.

Configure DTLS SRTP Profile

To provide Datagram Transport Layer Security-Secure Real Time Control Protocol (DTLS-SRTP) Advanced Media Termination services on the SBC, you must create a **DTLS SRTP Profile**. This profile defines the key exchange and DTLS handshake on a media session, the role the SBC negotiates when offered alternatives, and the crypto suites to use. After you create this profile, enter its name in the **DTLS SRTP Profile** parameter in the **Realm Config**.

1. Access the DTLS SRTP Profile configuration object: **Configuration**, **Security**, **Media Security**, **DTLS SRTP Profile**, **Add**.
2. Do the following:

Name	Set a unique name for this DTLS profile. Default. Empty.
TLS Profile	Set the name of an existing TLS profile that defines the key exchange scheme used by the DTLS handshake. Default: Empty.
DTLS Complete Timeout	Set the maximum time interval, in seconds, between the moment when the DTLS handshake on a media session is initiated and the moment when the DTLS handshake is completed. Default: 10. Range: 0-9999.
Preferred Setup Role	Set to "passive," so that the Advanced Media Termination client always initiates the DTLS handshake. Default: Passive.
Crypto Suite	Set the crypto suites that the SBC negotiates in the use-srtp DTLS extension for this profile. Default: SRTP_AES128_CM_HMAC_SHA1_80. Valid values: SRTP_AES128_CM_HMAC_SHA1_80 and SRTP_AES128_CM_HMAC_SHA1_32.

3. Save the configuration.

- Specify this **DTLS SRTP Profile** in the **Realm Config**.

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.

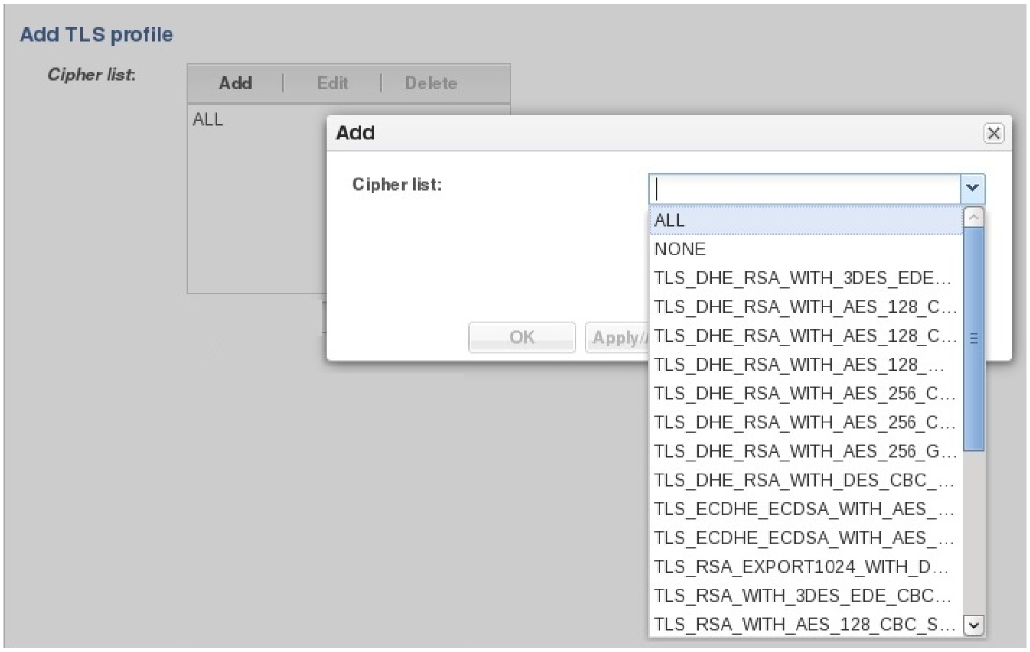
Suite B and Cipher List Support

The Oracle® Enterprise Session Border Controller (E-SBC) supports full control of selecting the ciphers that you want to use for Transport Layer Security (TLS). The system defaults to DEFAULT for the Cipher List parameter in the TLS Profile configuration. Oracle recommends that you delete ALL and add only the particular ciphers that you want, choosing the most secure ciphers for your deployment.

To support Suite B, the E-SBC certificate-record configuration includes the following parameters:

- Key Algor—Public key algorithm. Supports RSA and ECDSA. Default: RSA Security. You must select ECDSA to support suite B.
- ECDSA Key Size—ECDSA key size. Supports p256 and p384.

Configure the list of ciphers that you want to use from the Cipher List element in the TLS Profile configuration. The system provides a drop-down list of all supported ciphers. One-by-one, you can add as many ciphers as your deployment requires.


Add TLS profile
Cipher list:
Add
Edit
Delete
ALL
Add
Cipher list:
OK
Apply/
ALL
NONE
TLS_DHE_RSA_WITH_3DES_EDE...
TLS_DHE_RSA_WITH_AES_128_C...
TLS_DHE_RSA_WITH_AES_128_C...
TLS_DHE_RSA_WITH_AES_128_...
TLS_DHE_RSA_WITH_AES_256_C...
TLS_DHE_RSA_WITH_AES_256_C...
TLS_DHE_RSA_WITH_AES_256_G...
TLS_DHE_RSA_WITH_DES_CBC_...
TLS_ECDHE_ECDSA_WITH_AES_...
TLS_ECDHE_ECDSA_WITH_AES_...
TLS_RSA_EXPORT1024_WITH_D...
TLS_RSA_WITH_3DES_EDE_CBC...
TLS_RSA_WITH_AES_128_CBC_S...

TLS Cipher Updates

Note the following changes to the DEFAULT cipher list.

Oracle recommends the following ciphers, and includes them in the DEFAULT cipher list:

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256

The following ciphers have been added and included in the DEFAULT cipher list in CZ810m1p6:

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

Oracle supports the following ciphers, but does not include them in the DEFAULT cipher list:

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA

- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Oracle supports the following ciphers for debugging purposes only:

- TLS_RSA_WITH_NULL_SHA256 (debug only)
- TLS_RSA_WITH_NULL_SHA (debug only)
- TLS_RSA_WITH_NULL_MD5 (debug only)

Oracle supports the following ciphers, but considers them not secure. They are not included in the DEFAULT cipher-list, but they are included when you set the **cipher-list** attribute to **ALL**. Note that they trigger **verify-config** error messages.

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

To configure TLS ciphers, use the **cipher-list** attribute in the **tls-profile** configuration element.

> **WARNING:**
>
> When you set **tls-version** to either **tlsv1** or **tlsv11** and you want to use ciphers that Oracle considers not secure, you must manually add them to the **cipher-list** attribute.

Securing Communications Between the E-SBC and SDM with TLS

You can use the Transport Layer Security (TLS) protocol to secure the communications link between the Oracle® Enterprise Session Border Controller (E-SBC) and the Oracle Communications Session Delivery Manager (SDM). Note that the systems use Acme Control Protocol (ACP) for this messaging.

To configure the E-SBC to use TLS for this ACP messaging:

1. Configure a TLS profile. The tls-profile object is located under security, where you add certificates, select cipher lists, and specify the TLS version for each profile.
2. Configure system-config element's `acp-tls-profile` parameter to specify this TLS profile.

The `acp-tls-profile` parameter is empty by default, which means that ACP over TLS is disabled. When ACP over TLS is disabled, the SDM establishes a TCP connection with the E-SBC. When the `acp-tls-profile` parameter specifies a valid TLS profile, the E-SBC negotiates a TLS connection with SDM.

> **Note:**
>
> This feature requires SDM version 8.1 and above.

Add a TLS Profile

Use the TLS Profile configuration to specify the parameters for running SIP over Transport Layer Security (TLS).

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

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. Access the TLS Profile configuration object: **Configuration**, **Security**, **TLS Profile**, **Add**.
2. On the Add TLS profile page, do the following:

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.

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

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 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.

- Configure a TLS profile.

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.

1. Access the TLD Global Configuration object: **Configuration**, **Configuration**, **Security**, **TLS Global**.
2. On the Add TLS global page, do the following:

Session Caching	Select to enable.
Session Cache Timeout	Enter the number of hours to cache TLS sessions for re-connection. Default: 12. Range: 0-24. Zero (0) disables this parameter.

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

Configure an SPL Plugin

Use the SPL Config element to configure the parameters for integrating System Programming Language (SPL) plug-in extensions with the Oracle® Enterprise Session Border Controller (E-SBC).

- Confirm that the SPL engine is installed on the E-SBC.
- Plan the order in which you configure multiple SPL plug-ins because the E-SBC executes the SPL plug-ins in the order of configuration.

> **Note:**
>
> The E-SBC includes all SPL plug-ins, except for Comfort Noise Generation. You must manually upload the Comfort Noise Generation SPL plug-in to the E-SBC performing the following procedure.

1. Access the SPL Config configuration object: **Configuration**, **System**, **SPL Config**.
2. On the SPL Config page, do the following:

SPL Options	Enter values for optional SPL parameters and features in a comma separated list enclosed in double quotation marks.
Plugins	Click **Add**, and do the following: • State. Select to enable the SPL plug-in on the E-SBC. • Name. Specify the name of the SPL plug-in. • Click **OK**.

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

- Execute the SPL plug-in file.
- Synchronize the SPL across HA pairs.

Session Router Configuration

You can configure the following Session Router objects from the Configuration tab on the Web GUI. See the documentation specified in the following list for explanations of these configuration objects and how to set their parameters.

Access Control	Configure a static or dynamic access control list. See the *Security Guide* and "System Access Control" in the *ACLI Configuration Guide*.
Account Config	Configure and enable Quality of Service (QoS) accounting. See "Accounting Configuration" in the *ACLI Configuration Guide*.
Account Group	For future use. Not supported at this time.
Allowed Elements Profile	Configure an allowed elements profile to configure SIP white lists which, control the passage of unknown headers and parameters in request and response traffic. Includes the Rule Sets sub-object. See the "White Lists for Managing Incoming SIP Headers and Paremeters" section of the "Admission Control and QoS" chapter in the *ACLI Configuration Guide*.
Class Policy	Configure a classification profile policy. See "Using Class Profile for Packet Marking", " Class Profile and Class Policy Configuration", and " Applying a Class Policy to a Realm" in the *ACLI Configuration Guide*.

Diameter Manipulation	Configure diameter manipulation rules. See the "Diameter Rf Accounting" chapter in the *Accounting Guide*.
Enforcement Profile	Configure an enforcement profile. See "SIP Enforcement Profile and Allowed Methods" in the *ACLI Configuration Guide*.
ENUM Config	Configure an ENUM server. See "ENUM Server", and other ENUM topics in the *ACLI Configuration Guide*.
Filter Config	Configure a custom filter for SIP monitor and trace. See the "SIP Monitor and Trace" section of the "Introduction to SIP Monitor and Trace" chapter in the *ACLI Configuration Guide*.
H323 Config	Configure and enable an H.323 protocol. See the "Signaling" chapter in the *ACLI Configuration Guide*.
H323 Stack	Configure an H.323 stack. See the "Signaling" chapter in the *ACLI Configuration Guide*.
Home Subscriber Server	For future use. Not supported at this time.
HTTP ALG	Configure an HTTP proxy. See "Dynamic ACL for the HTTP-ALG" in the See the "Signaling" chapter in the *ACLI Configuration Guide*.
IWF Config	Configure and enable Inter-Working Function (IWF). See the "IWF Services" chapter in the See the "Signaling" chapter in the *ACLI Configuration Guide*.
LDAP Config	Configure and enable an LDAP server. See the "Active Directory-based Call Routing" section of the "Session Routing and Load Balancing" chapter in the *ACLI Configuration Guide*.
Local Policy	Configure a session request routing policy. See "The Role of Local Policy" and "Configuring the Local Policy Attribute" in the *ACLI Configuration Guide*.
Local Response Map	Configure a local SIP response map. See "Add a Local Response Map" in the *ACLI Configuration Guide*.
Local Routing Config	Configure the parameters for the local routing table. See the "Using the Local Route Table for Routing" section of the "Session Routing and Load Balancing" chapter in the *ACLI Configuration Guide*.
Media Profile	Configure a media profile and apply it to a media type. See the various "Media Profile Configuration" topics throughout the *ACLI Configuration Guide*.
Net Management Control	Configure and enable network management controls. See "Network Management Controls" in the *ACLI Reference Guide*.
QoS Constraints	Configure Quality of Service (QoS) constraints. See the "QoS-based Routing" section of the "Session Routing and Load Balancing" chapter in the *ACLI Configuration Guide*.
Response Map	Configure a SIP response map. See "Add a Local Response Map" in the *ACLI Configuration Guide*.

Service Health	Configure a service tag list to indicate the Session Agent Group assigned to the interface on the E-SBC.
Session Agent	Configure and enable a session agent. See "Session Agent Configuration" and "Configuring a Session Agent" in the *ACLI Configuration Guide*.
Session Agent ID Rule	Configure the SIP header and the parameter within the specified header to use to identify the Session Agent.
Session Constraints	Configure and enable session constraints. See "Aggregate Session Constraints Configuration" in the *ACLI Configuration Guide*.
Session Group	Configure a session agent group. See the "Session agent Groups" section of the "Session Routing and Load Balancing" chapter in the *ACLI Configuration Guide*.
Session Recording Group	Configure a session recording server group. See the "Configuring SIPREC" section of the "Selective Call Recording SIPREC" chapter in the*Call Traffic Monitoring Guide*.
Session Recording Server	Configure and enable a session recording server. See the "Configuring SIPREC" section of the "Selective Call Recording SIPREC" chapter in the*Call Traffic Monitoring Guide*.
Session Timer Profile	Configure a session timer profile. See "Sip-Config option session-timer-support" and "ACLI Configuration" in the *ACLI Configuration Guide*.
Session Translation	Configure the translation rules for calling and called numbers. See the session translation topics in the "Number Translation" chapter of the *ACLI Configuration Guide*.
SIP Advanced Logging	Configure logging of specific SIP requests by criteria. See "Advanced Logging" in the "Maintenance and Troubleshooting" chapter of the *ACLI Configuration Guide*.
SIP Config	Configure and enable signaling and session management. See the "SIP Signaling Services" chapter of the *ACLI Configuration Guide*.
SIP Feature	Configure SIP option tag parameters. See "SIP Options Tag Handling" in the "SIP Signaling Services" chapter of the *ACLI Configuration Guide*.
SIP Feature Caps	Configure to support SRVCC handover and other ATCF functionality. See "sip-feature-caps" in the *ACLI Reference Guide*.
SIP Interface	Configure and enable a SIP interface. See "SIP Interface Configuration" in the *ACLI Configuration Guide*.
SIP Manipulation	Configure SIP manipulation. See "Configuring SIP Manipulations" in the "SIP Signaling Services" chapter of the *ACLI Configuration Guide*.

SIP Monitoring	Configure and enable SIP monitor and trace features. See the "Introduction to SIP Monitor and Trace" chapter in the *Call Traffic Monitoring Guide*.
SIP Recursion Policy	Configure a recursion policy. See the "SIP Configurable Route Recursion" section of the "SIP Signaling Services" chapter of the *ACLI Configuration Guide*.
Surrogate Agent	Configure a surrogate agent. See the Surrogate Agents topics in the "SIP Signaling Services" chapter of the *ACLI Configuration Guide*.
Survivability	Configure and enable survivability. See the "Remote Survivability" chapter in the *ACLI Configuration Guide*.
Translation Rules	Configure and apply session translation rules to an agent and a realm. See the "Translation Rules" section of the "Number Translation" chapter in the *ACLI Configuration Guide*.

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.

1. From the Web GUI, click **Configuration**, **Session Router**, **Access Control**.
2. In the Add Access Control dialog, and do the following:

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 signaling messages allowed within the tolerance window. Range is 0-4294967295.
Untrusted Signal Threshold	Enter the maximum number of untrusted signaling 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 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 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 you enable the dynamic ACL option, the system sets the trust level for static flow for the public listening socket defined in **HTTP ALG, Public** 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 promoted
Exceed maximum number of error packets	Realm Config, invalid-signal-threshold	Connection denied and peer is promoted

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 **Ream Config**, **Access Control Trust Level** setting for the realm. 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.

- Confirm that the session manager is mapped to the Oracle® Enterprise Session Border Controller.

Two ACL entires 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.

1. From the Web GUI, on the Configuration tab, click **Configuration**, **Session Router**, **HTTP ALG**.
2. Click **Add**.

   The system displays the Add HTTP ALG page.
3. In the Add HTTP ALG dialog, do the following:

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.
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.

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

Dynamic Access Control List Settings for the HTTP Application Layer Gateway

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*.

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 object to set the destination parameters for accounting messages.

1. From the Web GUI, click **Configuration**, **Account Config**.
2. In the Account Config dialog, do the following:

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 the configuration.

Configure RADIUS Call Accounting

You can configure the Oracle® Enterprise Session Border Controller (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, to monitor traffic, and to troubleshoot the system.

To set the RADIUS call accounting parameters, use the Account Config Object 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.

1. From the Web GUI, click **Configuration**, **Session Router**, **Account Config**.
2. In the Account Config dialog do the following:

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 **Add** to add options.
FTP Push	(Optional) Select to enable.
Push Receiver	(Optional) Click **Add** to add a push receiver to the list.
Account Servers	Click **Add** to add a RADIUS server to the list.

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

Configure H.323 Global Settings

Configuring H.323 signaling for theOracle® Enterprise Session Border Controller (E-SBC) requires setting global parameters and parameters for each interface. The global parameters govern how the E-SBC performs general H.323 operations. The E-SBC applies the global settings to all interfaces that you configure to use H.323. For example, you can turn H.323 support on and off for the entire E-SBC, using the global settings. Use the following procedure to configure the global H.323 parameters.

- Configure the basic parameters for physical interfaces, network interfaces, global system parameters, SNMP, trap receiver, accounting support, and any holiday information that you need.
- Decide how you want to configure realms and routing, including the use of session agents and session agent groups, to support H.323 operations.
- Determine the settings that you want to use for the attributes in this procedure.
- Know the names of any Options that you want to add. See "H.323 Signaling Services" in the*ACLI Configuration Guide* for descriptions.

1. Access the H.323 Config configuration object:

   Configuration, **Session Router**, **H323**, **H323 Config**.
2. On the H323 Config page, do the following:

State	Select to enable the configuration.
Log Level	Select a log level for H.323 stacks from the drop-down list. Default: Notice.
Response Tmo	Set the maximum waiting time for response to a SETUP message in seconds. Default: 4. Range: 1-2147483647
Connect Tmo	Set the maximum waiting time for establishment of a call in seconds. Default: 32. Range: 1-2147483647
RFC2833 Payload	Enter the payload type used by the H.322 stack in preferred rfc 2833-mode. Default: 101. Range: 96-127
Alternate Routing	Select an alternate route means from the drop-down list. Default: Proxy.
Codec Feedback	Select to enable slow-start to fast-start codec negotiation. Default: Disabled.
ENUM Sag Match	Select to enable matching Session Agent Group names with the hostname from an ENUM query or Local Route Table next-hop entry. Default: Disabled.
Remove T38	Select to enable removing T.38 fax capabilities in the TCS for IWF calls. Default: Disabled (means T.38 is functional)
Options	Set any options for H.323 features that you want to use. a. Click **Add**, and enter an option. For example, **directDial** for H.323 destination-based routing. b. Do one of the following: • Click **OK** to complete the task. • Click **Apply/Add another**, for as many options as needed, and click **OK** when done.

3. Save the configuration.

Session Manager Mapping

The Oracle® Enterprise Session Border Controller (E-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.

- Note the private realm and IP address of the session manager and the public realm and SIP interface IP address of the session border controller that you want to map.

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

1. Access HTTP ALG: **Configuration**, **Session Router**, **HTTP ALG**.
2. On the HTTP ALG page, click **Add** and do the following:

Name	Enter a name for this HTTP Application Layer Gateway.
State	Select to enable this configuration.
Description	Enter a description of this HTTP Application Layer Gateway.
Private Realm ID	Select the private realm from the drop-down list.
Private Address	Enter the private IP address.
Private Destination Address	Enter the private destination IP address.
Destination Port	Default: 80. Valid values: 1-65535.
Public Realm ID	Select the public realm from the drop-down list.
Public Address	Enter the public IP address.
Public Port	Default: 80. Valid values: 1-65535.
Session Manager Mapping	Click **Add**, and do the following: • Enter the IP address of the session manager. • Enter the IP address of the public interface. • Set the port for SIP calls. Default:5050. Valid values: 1-65535. • Set the transport protocol. Default: TCP. Valid values: TCP | TLS | UDP.
Dynamic ACL	Select to enable dynamic ACL.
Max Incoming Conns	Set the maximum number of incoming connections allowed. Default: 0. Valid values: 0-4294967295.
Per Sec IP Max Incoming Conns	Set the maximum number of HTTP connections allowed per peer. Default: 0. Valid values: 0-4294967295.

3. Click **OK**.

   The system lists the new map on the HTTP ALG page.

4. Save the configuration.

Configure IWF

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

- Configure SIP, including SIP interfaces, SIP ports, SIP NAT, if needed, and SIP features
- Configure H.323 configuration, including H.323 global and H.323 interface configurations
- Configure local policy and local policy attributes
- Configure media profiles
- Configure session agents and, if needed, session groups

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

1. From the Web GUI, click **Configuration**, **Session Router**, **IWF Config**.
2. On the IWF Config page, do the following:

State	Select to enable IWF to translate SIP and H.323 sessions. Default: Disabled.
Media Profiles	Select the media profiles that you want to use for IWF translations. Valid values: An SDP codec or a telephone event if you want the SBC to support DTMF.
Logging	Select to enable the SBC to log SIP messages related to the IWF. Default: Disabled.
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.
Options	Enter an optional feature or parameter.
Forward Source Call Address	Select to enable adding the H225SourceCallSignalAddress IP for IWF to egress SIP INVITEs.

3. Click **OK**.
4. Save 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 Advanced mode to create and enable an LDAP configuration on the E-SBC.

- Confirm that one or more authentication modes exist.

- Confirm that one or more Transport Layer Security (TLS) profiles exist.

In the following procedure, you configure the LDAP server, filters, security, and local policy. Note that you can use multiple LDAP Config configurations that reference the same LDAP server within different Local Policy Policy Attributes to allow for multiple LDAP queries to the same LDAP server.

1. From the Web GUI, click **Configuration**, **Session Router**, **LDAP Config**.
2. On the LDAP config page, click **Add**.
3. On the Add LDAP config page, do the following:

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.
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 `LDAP sec type` on this page.
Username	Enter the username that the LDAP bind request uses for authentication before the LDAP server grants access.
Password	Click **Set**, 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 **OK**.
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 signaling.
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 **Add** 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, the operation type for configuring multiple attributes, and add LDAP configuration attributes.

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

Configure Local Policy

Configure local policy and local policy attributes for session routing based on the next hop parameter.

Use the local-policy element to configure where signaling messages are routed and forwarded.

For the Policy priority parameter, the priority hierarchy from lowest to highest is none, normal, non-urgent, urgent, emergency. None means no priority. Each higher priority handles sessions at its level plus the sessions in the priorities above it. For example, non-urgent also handles sessions for urgent and emergency.

1. From the Web GUI, click **Configuration**, **Session Router**, **Local Policy**.
2. On the Local Policy page, do the following:

From Address	Enter the source IP address, the POTS number, the E.164 number, or the hostname for the local-policy element. • This list requires at least one address. • You can add as many addresses as necessary. • You can use a wildcard or a DS:prefix (dialed string) for this parameter.
To address	Enter the destination IP address, the POTS number, the E.164 number, or the hostname for the local-policy element. • This list requires at least one address. • You can add as many addresses as necessary. • You can use a wildcard for this parameter.
Source Realm	Enter one or more valid realms for identifying coming into a realm. The default is *.
Description	Enter a description of this local policy.
State	Select to enable this policy. Default: Enabled.
Policy Priority	Select the policy priority for this local policy from the drop-down list. Default: None. Valid values: None | Normal | Non-urgent | Urgent | Emergency.
Next Hop	Enter the signaling host IP address, SAG, hostname, or ENUM Config

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.
Action	Select an action for the next hop from the drop-down list. Default: None. Valid values: None | Replace URI | Redirect.
Terminate Recursion	Select to terminate route recursion with the next hop. Deselect to include next hops after this one.
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. Valid Values: 0-9999999.
State	Select to enable.
App Protocol	Select the application protocol for signaling the session agent from the drop-down list. Default: None. Valid values: Agent | SIP | H323 | MGCP | H248 | BGF | BFD | SCF | RTSP | DD | Diameter | IKE | None | " ".
Methods	Enter a list of SIP methods to match with a SIP request method. Double quote the list with a comma between methods. Valid values: INFO | INVITE | MESSAGE | NOTIFY | OPTIONS | PRACK | PUBLISH | REFER | REGISTER | SUBSCRIBE.
Lookup	Select an additional local policy lookup from the drop-down list. Default: Single. Valid values: Single | Multi.
Next Key	Enter the next stage key for multi-stage local policy lookups.

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

Add a Local Response Map

Configuring cause and reason mapping for SIP to SIP calls requires a local response map. The entries in the map generate the SIP response and Q850 cause code value for particular error scenarios.

- If you plan to add a Reason header, enable the function in the global SIP configuration.

You can customize the SIP status SIP reason for a local error. For example, the default 503 message for the error that the Oracle® Enterprise Session Border Controller (E-SBC) sends when the licensed session capacity is reached is "503 licensed session capacity reached". You can customize the number for this error message in the SIP Status field, and you can customize the reason in the SIP Reason field. Select licensed-session-capacity-reached from the Local Error list and you can add custom text about the error to the SIP header.

.
Repeat the following procedure to create as many local response map entries as you need.

1. Access the Local Response Map configuration object: **Configuration**, **Session Router**, **Local Response Map**, **Add**.

2. In the Local response map entries configuration, do the following.

Local Error	Select a local error condition from the drop-down list to trigger this map.
SIP Status	Enter a SIP response code. Default: 0. Range: 100-699.
Q850 Cause	Enter a Q850 cause code. Default: 0. Range: 0-2147483647.
SIP Reason	Enter a SIP response comment in quotation marks.
Q850 Reason	Enter a Q850 cause comment in quotation marks.
Method	Select a SIP failure response message from the drop-down list to map to a 200 OK. To deactivate this function, make no selection.
Register Response Expires	Enter the number of seconds after which the REGISTER response expires. Default: 0. Range: 0-999999999.

3. Click **OK**.
4. Save 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.

1. From the Web GUI, click **Configuration**, **Session Router**, **Local Routing Config**.
2. On the Local Routing Config page, click **Add**.
3. On the Local Routing Config page, do the following:

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. Default: 0. 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. Default: Exact. Valid values: All | Best | Exact.

4. Click **OK**.
5. Save 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.

Configure the following before you configure a session agent.

- Media profile
- Out Translation ID
- Local Response Maps
- Codec Policy
- Session Recording Server
- TLS Profile
- SIP Header Manipulation IDs
- LDAP
- One or more target groups
- SIP recursion policy

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.

- From the Web GUI, click **Configuration**, **Session Router**, **Session Agent**.
- On the session-agent page, click **Add**, and do the following:

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. – 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. – 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.
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. Default: 5060. Range: 1025-65535.

	– If you enter zero, the E-SBC cannot initiate communication with this agent (although it can accept calls). – 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. Default: Enabled.
App Protocol	Select the protocol to use to signal the session agent. Default: SIP. Valid values: SIP | H323.
App Type	Select the type of application from the drop-down list. Valid values: " " | H323 -GW | H323-GK.
Transport Method	Select the transport mode for connections to this agent. – DTLS – Dynamic TCP – Dynamic TLS – Static SCTP – Static TCP – Static TLS – TLS+DTLS – UDP - Default – UDP+TCP
Realm ID	Select the name of the realm where this agent is located.
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.
Match Identifier	Click **Add**, and do the following: – Identifier Rule—Specify the session agent identifier rule to use to identify this agent when not matching by IP address. – Match Value—Enter the value to match in the SIP header field that identifies this session agent.
Max Sessions	Enter the maximum number of sessions allowed for this constraint. Default: 0. Valid values: 0-999999999.
Max Inbound Sessions	Enter the maximum number of inbound sessions allowed from this session agent. Default: 0. Valid values: 0-999999999.

Max Outbound Sessions	Enter the maximum number of outbound sessions allowed for this constraint. Default: 0. Valid values: 0-999999999.
Max Burst Rate	Enter the maximum number of invites allowed in a burst time period. Default: 0. Valid values: 0-999999999.
Max Inbound Burst Rate	Enter the maximum inbound burst rate in INVITEs per second from this session agent. Default: 0.Valid values: 0-999999999.
Mac Outbound Burst Rate	Enter the maximum outbound burst rate in INVITEs per second from this session agent. Default: 0. Valid values: 0-999999999.
Max Sustain Rate	Enter the maximum rate of session invitations allowed within the current time period for this constraint. Default: 0. Valid values: 0-999999999.
Max Inbound Sustain Rate	Enter the maximum inbound sustain rate of session invitations allowed within the current time period for this constraint. Default: 0. Valid values: 0-999999999.
Max Outbound Sustain Rate	Enter the maximum outbound sustain rate of session invitations allowed within the current time period for this constraint. Default: 0. Valid values: 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. Default: 0. Valid values: 0-999999999
In Service Period	Enter the number of seconds that this session agent is allowed to re-initialize before returning to in-service status. Default: 0. Valid values: 0-999999999
Burst Rate Window	Enter the time period, in seconds, used to measure the burst rate. Default: 0. Valid values: 0-999999999.
Sustain Rate Window	Enter the time period, in seconds, used to measure the sustained rate. Default: Valid values: 0. 0-999999999.
Proxy Mode	Select a proxy mode for the E-SBC to use when a SIP request arrives from this agent – Proxy—Forward requests. – Redirect—Return redirect (3xx) responses. – Proxy Record Route—Forward proxy requests with Record Route. (Stateless and transaction modes, only.)
Redirect Action	Select a method for the redirect response from this agent. – Proxy—Send the response back to the previous hop. – Recurse—Recurse on the contacts in the response. – Recurse 305, only—Recurse on the contacts in the 305 response, only.
Loose Routing	Select to enable loose routing.

Response Map	Select the name of the response map.
Ping Method	Enter the SIP ping method.
Ping Interval	Enter the time, in seconds, to ping this session agent. Default: 0. Valid values: 0-4294967295.
Ping Send Mode	Select the mode for pinging this session agent. Default: Keep alive. – Continuous – Keep alive
Ping All Addresses	Select to ping all addresses from the DNS query.
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 Translation ID	Select the inbound translation ID.
Out Translation ID	Select the outbound translation ID.
Trust Me	Select to trust this agent. Default: Disabled.
Local Response Map	Select a local response map for this agent.
In Manipulation ID	Select the in bound manipulation ID.
Out Manipulation ID	Set the outbound manipulation 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 trunk group name and context to use as the default context to reach this agent. For example: tgname1:tgcontext1.
Max Register Sustain Rate	Enter the maximum register sustain rate per second. Default: 0. Valid values: 0-999999999.
Invalidate Registrations	Select to invalidate all registrations going to this session agent. Default: Disabled.
RFC2833 Mode	Select the preferred mode for RFC2833. Default: None. Valid values: None | Transparent | Preferred | Dual.
RFC2833 Payload	Enter a number for the payload used by the agent in Preferred RFC2833 mode. Default: 0. Valid values: 0-127.
Codec Policy	Select the codec policy to apply to this session agent.

Refer Call Transfer	Select the refer method for call transfer. Default: Disabled. Valid values: Disabled | Enabled | Dynamic.
Refer Notify Provisional	Select the provisional mode for sending a NOTIFY message. Default: None. Valid values: – None—The system sends no intermediate NOTIFY message. – Initial—The system sends an intermediate 100 Trying NOTIFY message. – All—The system sends an intermediate 100 Trying NOTIFY message, plus a NOTIFY for each non-100 provisional received by the E-SBC.
Reuse Connections	Select the protocol for SIP reuse connection. Default: None. Valid values: None | TCP | SCTP.
TCP Keepalive	Select an option for the TCP keepalive function. Default: None. Valid values: None | Disabled | Enabled.
TCP Reconn Interval	Enter the TCP/SCTP e-connection interval. Default: 0. Valid values: 0-300.
Max Register Burst Rate	Enter the number of seconds allowed for the maximum register burst rate. Default: 0. Valid values: 0-999999999.
KPML Interworking	Select a status for KPML Interworking inherit from the SIP interface. Default: Inherit. Valid values: Inherit | Disabled | Enabled.
KMPL 2833 IWF on Hairpin	Select a status for KPML Interworking on a hairpin call. Default: Inherit. Valid values: Inherit | Disabled | Enabled.
Precedence	Set the order of precedence for this agent among agents with the same IP address. Default: 0. Valid values: 0-4294967295.
Monitoring Filters	Add one or more comma separated monitoring filters. Preface with the + character to add, the - character to remove, and the word exclude to replace.
Auth Attribute	Click **Add**, and do the following: – Auth Realm—Select an authentication realm. – Username—Enter the user name for the selected realm. – Password—Enter the password for the selected realm. – In Dialog Methods—Add one or more in dialog methods to add authentication headers.
Session Recording Server	Select a single session recording server <SRS-name> or a session recording group <SRS-group-name>.
Session Recording Required	Select to enable calls upon successful set up and interaction with the Session Recording Server. Default: Disabled.
Hold Refer Reinvite	Select to enable holding the re-INVITE. Default: Disabled.

Send TCP Fin	Select to enable sending TCP FIN messages when the Session Agent stops responding. Default: Disabled.
SIP Recursion Policy	Select a SIP recursion policy from the list.
Sm ICSI Match for INVITE	Set the ICSI value to match for INVITE per RFC 6050.
Sm ICSI Match for Message	Set the ICSI value to match for Message per RFC 6050..

- Click **OK**.
- Save 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 ACLI command line or the Web GUI in Advanced 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.

- 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.

To enable Hold Refer Reinvite, select a configured session agent and enable the parameter on the selected agent.

1. From the Web GUI, click **Configuration**, **Ssession Router**, **Session Agent**.
2. On the Session Agent page, select the agent and click **Edit**.
3. On the Session Agent page, select Hold Refer Invite.
4. Click **OK**.
5. Save the configuration.

- Enable the Hold Refer Invite parameter in the Realm configuration.
- Enable the Hold Refer Invite parameter in the Session Agent configuration.

Configure a Session Group

Use the Session Group element to define a signaling endpoint configured to apply traffic shaping attributes and information about next hops and previous hops.

1. From the Web GUI, click **Configuration** , **Session Router**, **Session Group**.
2. On the Add Session Group page, click **Add**, and do the following:

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. • Hunt—The system selects the session agent in list order. • Least Busy—The system selects the session agent with the fewest number of sessions relative to the max-outbound-sessions constraint of the session-agent element. • Low Sus Rate—The system selects the session agent with the lowest sustained rate of session initiations and incitations. • Prop Dist—The system uses the proportional distribution strategy to distribute traffic among all available session agent elements, based on session constraint limits. • Round Robin—The 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.
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.
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.
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 an comma-separated list or as a range. Default: 401, 407.

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

Configure Session Recording Group

The Oracle® Enterprise Session Border Controller (E-SBC) uses the Session Recording Group attribute under session-router to define a collection of session recording servers.

- Enable the SIP Session Recording licence. See "Getting Started."
- Configure multiple session recording servers. See "Session Recording Server Attribute."
- Determine the load balancing strategy that you want the E-SBC to use. See "Load Balancing."

In the configuration, you list the session recording servers that you want in the group, select a load balancing strategy, and set the number of simultaneous SIP dialogs.

1. Access the Session Recording Group configuration object: **Configuration**, **Session Router**, **Session Recording Group**, **Add**.
2. In the Session Recording Group dialog, do the following:

Name	Enter a unique name for the session recording group. You may need this name when configuring realm-config, session-agent, and sip-interface. Valid values: Alpha-numeric characters.
Description (Optional)	Enter a description for the session recording group. Valid values: Alpha-numeric characters.
Session Recording Servers	Enter the names of the session recording servers you want in this group. Use the + character to add a recording server to the existing list and the - character to remove one. Omit the + and - characters to replace the list. For example, +acme, -packet, or acme packet.
Strategy	Enter the load balancing strategy that you want the E-SBC to use when sending recordings to the session reporting server. • Round robin—Go to the next session recording server on the list, since the last session. • Hunt—Look for a session recording server, starting with the first one on the list.
Simultaneous Recording Servers	Enter the number of simultaneous SIP dialogs that the E-SBC establishes to the session reporting servers in the session reporting group per communication session. Default: 0. Valid values: 1-10.

3. Click **OK**.
4. Save the configuration.
5. Save the configuration.

Configure Advanced Logging

From the Configuration tab, define SIP Advanced Logging and Advanced Log Condition. The criteria that you configure re-maps the message logging and modifies the system configuration. You must save and activate these changes to the configuration.

When configuring multiple SIP Advanced Logging configurations, note the following.

- The system evaluates each configuration individually in an OR relationship.
- The system evaluates all conditions and they must all match in an AND relationship.

1. From the Web GUI, go to **Configuration**, **Session Router**, **SIP Advanced Logging**, and click **Add**.
2. On the SIP Advanced Logging page, do the following:

Name	Type a name to display on the log message for this set of criteria.
Level	Select one: zero, none, emergency, critical, major, minor, warning, notice, info, trace, debug, or detail.
Scope	Select one: request-only, transaction, session, or session-and-media.
Matches Per Window	Type a number between 1 and 999999999.
Window Size	Type a number between 1 and 999999999.
Conditions	Click **Add**, and do the following: • Match type—Select one or more with either "and" or "or" between items: request-type, recv-agent, recv-realm, request-uri-user, request-uri-host, to-header-user, to-header-host, from-header-user, from-header-host, or call-id. • Match value—Type the string that you want to match the incoming message. For example, to match "To-header-user" to the value 1234@<companyname>.com, type 1234.

3. Save the configuration.

Disable Advanced Logging

From the Configuration tab, clear the advanced logging settings.

1. From the Web GUI, go to **Configuration**, **Session Router**, **SIP Advanced Logging**.
2. On the SIP Advanced Logging page, clear all of the settings.
3. Save the configuration.

Configure Advanced Logging

From the Configuration tab, define SIP Advanced Logging and Advanced Log Condition. The criteria that you configure re-maps the message logging and modifies the system configuration. You must save and activate these changes to the configuration.

When configuring multiple SIP Advanced Logging configurations, note the following.

- The system evaluates each configuration individually in an OR relationship.
- The system evaluates all conditions and they must all match in an AND relationship.

1. From the Web GUI, go to **Configuration**, **Session Router**, **SIP Advanced Logging**, and click **Add**.
2. On the SIP Advanced Logging page, do the following:

Name	Type a name to display on the log message for this set of criteria.
Level	Select one: zero, none, emergency, critical, major, minor, warning, notice, info, trace, debug, or detail.
Scope	Select one: request-only, transaction, session, or session-and-media.
Matches Per Window	Type a number between 1 and 999999999.
Window Size	Type a number between 1 and 999999999.
Conditions	Click **Add**, and do the following: • Match type—Select one or more with either "and" or "or" between items: request-type, recv-agent, recv-realm, request-uri-user, request-uri-host, to-header-user, to-header-host, from-header-user, from-header-host, or call-id. • Match value—Type the string that you want to match the incoming message. For example, to match "To-header-user" to the value 1234@<companyname>.com, type 1234.

3. Save 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).

- Configure at least one home realm, egress realm, and transcoding realm.

1. Access the SIP Config configuration object: **Configuration**, **Session Router**, **SIP Config**.
2. On the SIP Config page, do the following:

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.

	• None—No SIP-NAT function. • Public—Means the home realm is public address space. Encrypt any URI from an external realm. • Private—Means the home realm is private address space. Encrypt any URI from the home realm.
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.
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. Default: 0. Range: 0-999999999.
Register Use To for IP	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. Default: 15. Range: 1-60. 0 = no delay.
Transcoding Realm	Enter the name of the realm where transcoding agents reside.
Transcoding Agents	Create a list of transcoding agents. For a single agent use <hostname>, <IPv4 | IPv6 | IPport>, or <SessionAgentName> plus the address. For example: somehostname 1 1.1.1.1. For multiple entries, list the agents and the address. For example, sa1 sa2 1.1.1.1. Use the + character to add an agent to the existing list and the - character to remove one.
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. Valid values: BGCF | E-CSCF | IBCF | P-CSCF.
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.
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. Default: 0. : 0-4294967295.

Cache Loc Info Expire	Enter the number of seconds for the SBC to rely on cached location information. The number must be higher than the transaction expiration time. Default: 32. Range: 1-4294967295.
Msg Hold for Loc Info	Enter the number of seconds to hold MESSAGEs until hte SBC receives location information from PCRF. Default: 0. Range: 0-30.
Npli Upon Register	Select to include the location provided by the network in REGISTER messages. Default: Disabled.

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

Configure Pooled Transcoding

You must configure a transcoding realm and transcoding agents on the Access Session Border Controller, when used in a pooled transcoding deployment model. Set the parameters as part of the global SIP configuration.

- Configure a realm as the separate realm for the public SIP interface for exclusive communication with the Transcoding Session Border Controller (T-SBC) in a pooled transcoding deployment
- Configure one or more agents
- Configure SIP
- Configure the Access Session Border Controller (A-SBC)
- Configure the Transcoding Session Border Controller (T-SBC)

1. Access the SIP Config configuration object: **Configuration**, **Session Router**, **SIP Config**.
2. On the SIP Config page, do the following.

Transcoding Realm	Enter the name of a configured realm designated as the separate realm for the public SIP interface for exclusive communication with the Transcoding Session Border Controller (T-SBC) in a pooled transcoding deployment.
Transcoding Agents	Add any IP address, IP address - port combination, session agent, hostname, or session agent group to use as a transcoding agent. You can add multiple entries to the list. For example, you might list an IPv6 address and port, a session agent, and a session agent group.

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

Configure SIP Feature

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.

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 is 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.

1. From the Web GUI, click **Configuration**, **Session Router**, **SIP Feature**.
2. On the SIP Feature page, do the following:

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: • Select the realm with which to associate this configuration. • Leave this parameter blank to make this configuration global.
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 the configuration.

Configure SIP Interface

Use the SIP Interface object to define SIP signaling.

- Confirm that a TLS profile exists.
- Confirm that rules exist for inbound and outbound SIP manipulation.

Configure a SIP Interface for each network or realm to which you want to connect the Oracle® Enterprise Session Border Controller. The following list is a basic set of the available parameters. For the complete list of available parameters, see the *ACLI*

Reference Guide. For more configuration instructions, see the *ACLI Configuration Guide*.

1. From the Web GUI, click **Configuration**, **Session Router**, **SIP Interface**.
2. On the SIP Interface page, click Add, and do the following:

<table>
<tr><td>State</td><td>Select to enable this SIP interface.</td></tr>
<tr><td>Realm ID</td><td>Select the realm in which to apply this SIP interface from the drop-down list.</td></tr>
<tr><td>Description</td><td>Enter a description of this SIP interface.</td></tr>
<tr><td>SIP Ports</td><td>Specify the following parameters for the ports that the SIP proxy or B2BUA uses for connections.
<ul>
<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:
<table>
<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>
</table>
</li>
</ul>
</td></tr>
<tr><td>NAT Traversal</td><td>Select a Network Address Translation (NAT) traversal mode for SIP from the drop-down list.
<ul>
<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>
</td></tr>
</table>

Registration Caching	Select to enable non-HNT registration caching.
Route to Registrar	Select to enable routing requests to the registrar.
In Manipulation ID	Select an inbound SIP manipulation rule from the drop-down list.
Out Manipulation ID	Select an outbound SIP manipulation rule from the drop-down list.
Service Tag	Enter the service tag for this interface.

3. Click **OK**.
4. Save 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.

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.

1. From the Web GUI, click **Configuration**, **Session Router**, **SIP Manipulation**.
2. In the SIP manipulation dialog, click **Add**, and do the following:

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 **Add**, enter the header, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another header, and click **OK**. Repeat, as needed.
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 **Add**, enter the header that you want the system to join, and do one of the following: • Click **OK**.

	• Click **Apply/Add another**, add another header, and click **OK**. Repeat, as needed.
CFG Rules	Click **Add**, select one of the following header rules from the menu, and see the corresponding documentation for further instructions. • header rule—"Configure Header Rule" • mime rule—"Configure MIME Rule" • mime isup rule—"Configure MIME ISUP Rule" • mime sdp rule—"Configure MIME SDP Rule"

3. When you finish configuring SIP manipulations, and the system returns you to the SIP manipulation page, save and activate the configuration.

- Apply the rules to a session agent or SIP interface as "inbound" or "outbound."

Configure a MIME ISUP Rule

You can configure Multi-Purpose Internet Mail Extensions (MIME) header rules and element rules on the Oracle® Enterprise Session Border Controller (E-SBC) from the "CfgRules" section of the "SIP Manipulations" page.

In the following procedure, you set the SIP Header Manipulation, MIME ISUP Rule, MIME Header Rule, and ISUP Param Rule parameters.

1. Access the SIP Manipulation configuration object.

   Configuration, **System Administration**, **SIP Manipulation**.

2. On the SIP Manipulation configuration page, do one of the following:

   a. Select and existing SIP manipulation configuration from the table, right-click, and click **Edit**. (Subsequent SIP manipulation pages use "Modify" in the title.)

   b. Click **Add**. (Subsequent SIP manipulation pages use "Add" in the title.)

3. On the Add or Modify SIP Manipulation page, do one of the following.

   a. If you chose **Add**, you must enter a name for this SIP Manipulation. (You can optionally complete the Description, Split Headers, and Join Headers parameters, at this time. See "Configure SIP Manipulation.") Proceed to the next step.

   b. If you chose to edit an existing configuration, proceed to the next step.

4. On the Add or Modify SIP Manipulation page under Cfg Rules, click **Add** and click **mime-header-rule**.

5. On the Add or Modify SIP Manipulation / Mime ISUP Rule page, do the following.

Name	Enter a unique name for this rule set. Valid values: Alpha-numeric.
Content Type	Enter the name of the header on which you want the E-SBC to use this HMR. Set this parameter to @status-line, where the at-sign (@)—not allowed in SIP header names—to prevent undesired matches with header having the name status-code. Default: Blank.

<table>
<tr><td>Msg Type</td><td>Specify the message type this rule applies to. Default: Any. Valid Values: Any | Out of Dialog | Reply | Request | Out of Dialog.</td></tr>
<tr><td>Methods</td><td>Enter the method type to use when this SIP HMR is used. Default: Blank. Valid values" ACK | CANCEL | INVITE. When you do not set the method, the E-SBC applies the rule to all SIP methods.</td></tr>
<tr><td>Format</td><td>Select the encode - decode format from the drop-down list for the MIME content.</td></tr>
<tr><td>Action</td><td>Select an action from the drop-down list for the header rule. Default: None. Valid values: Add | Delete | Find Replace All | Log | Manipulate | Monitor | None | Reject | SIP Manip | Store.</td></tr>
<tr><td>Comparison Type</td><td>Specify how the E-SBC processes the match rules against the SIP header. Default: Refer Case Sensitive. Valid values: Boolean | Case Insensitive | Case Sensitive | Pattern Rule | Refer Case Insensitive | Refer Case Sensitive.</td></tr>
<tr><td>Match Value</td><td>Enter the value to match against the header value in SIP packets; the E-SBC matches these against the entire SIP header value. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators. When you configure HMR (using SIP manipulation rules and elements rules, you can use escape characters in the <b>match-value</b> parameter to support escaping Boolean and string manipulation operators. You can also escape the escape character itself, so that it is used as a literal string. For example, the E-SBC treats the string \+1234 as +1234. The following are escape characters: +, -, +^, -^, &, |, \, (,), ., $, ^, and “. You can also use the variables, $REMOTE_PORT and $LOCAL_PORT, which resolve respectively to the far-end and remote UDP or TCP port value.</td></tr>
<tr><td>New Value</td><td>When you set the action parameter Add or to Manipulate, enter the new value that you want to substitute for the entire header value. This is where you can set stored regular expression values for the E-SBC to use when it adds or manipulates SIP headers. When you configure HMR (using SIP manipulation rules and elements rules, you can use escape characters in the <b>match-value</b> parameter to support escaping Boolean and string manipulation operators. You can also escape the escape character itself, so that it is used as a literal string. For example, the E-SBC treats the string \+1234 as +1234. The following are escape characters: +, -, +^, -^, &, |, \, (,), ., $, ^, and “. You can also use the variables, $REMOTE_PORT and $LOCAL_PORT, which resolve respectively to the far-end and remote UDP or TCP port value.</td></tr>
<tr><td>Cfg Rules (instructions for configuring MIME HeaderRule)</td><td>Click <b>Add</b>, <b>MIME Header Rule</b>, and do the following.
• Name—Enter a unique name for this header element rule.
• Header Name—Enter header name within the MIME part to which to apply the rule.</td></tr>
</table>

	• Action—Select an action from the drop-down list to apply to the element rule. • Comparison Type—Select the type of comparison from the drop-down list to use for the match value. (To clear the value, enter and empty string.) • Match Value—Enter the match value to compare against the current object. (To clear the value, enter and empty string.) • New Value—Enter a new value for the object. Quoted display named must be escaped within quotes. For example, \"MyName\" . • Click **OK**. The system displays the SIP manipulation / Mime isup rule dialog. Do one of the following: • Add another MIME Header Rule. • Add an ISUP Param Rule, using the steps in the following table cell. • Finish the MIME ISUP rule configuration by completing steps 3-6.
Cfg Rules (instructions for configuring ISUP Param Rule)	Click **Add**, **isup-param-rule**, and do the following. • Name—Enter a unique name for this header element rule. • Type—Enter the parameter type that specifies the part of the isup body to manipulate. • Format—Select a format from the drop down list for the encode - decode mode of the binary body form string form-ascii. • Action—Select an action from the drop-down list to apply to the element rule. • Comparison Type—Select the type of comparison from the drop-down list to use for the match value. (To clear the value, enter and empty string.) • Match Value—Enter the match value to compare against the current object. (To clear the value, enter and empty string.) • New Value—Enter a new value for the object. Quoted display named must be escaped within quotes. For example, "\"MyName\" " . • Click **OK**. The system displays the SIP manipulation / Mime isup rule dialog. Do one of the following: • Add another ISUP Param Rule. • Finish the MIME ISUP Rule configuration by completing the following steps.

6. Click **Back**.

The system displays the Add or Modify SIP Manipulation page.

7. Click **Back**.

   The system displays the SIP Manipulation page.

8. Save the configuration.

Configure a MIME SDP Rule

You can configure Multi-Purpose Internet Mail Extensions (MIME) header rules and element rules on the Oracle® Enterprise Session Border Controller (E-SBC) from the "CfgRules" section of the "SIP Manipulations" page.

In the following procedure, you set the SIP Header Manipulation, MIME SDP Rule, MIME Header Rule, SDP Session Rule, and SDP Media Rule parameters.

1. Access the SIP Manipulation configuration object.

   Configuration, **System Administration**, **SIP Manipulation**.

2. On the SIP Manipulation configuration page, do one of the following:

   a. Select and existing SIP manipulation configuration from the table, right-click, and click **Edit**. (Subsequent SIP manipulation pages use "Modify" in the title.)

   b. Click **Add**. (Subsequent SIP manipulation pages use "Add" in the title.)

3. On the Add or Modify SIP Manipulation page, do one of the following.

   a. If you chose **Add**, you must enter a name for this SIP Manipulation. (You can optionally complete the Description, Split Headers, and Join Headers parameters, at this time. See "Configure SIP Manipulation.") Proceed to the next step.

   b. If you chose to edit an existing configuration, proceed to the next step.

4. On the Add or Modify SIP Manipulation page under Cfg Rules, click **Add** and click **mime-sdp-rule**.

5. In the Add or Modify SIP Manipulation / MIME SDP Rule page, do the following.

Name	Enter a unique name for this rule set. Valid values: Alpha-numeric.
Content Type	Enter the name of the header on which you want the E-SBC to use this HMR. Set this parameter to @status-line, where the at-sign (@)—not allowed in SIP header names—to prevent undesired matches with header having the name status-code. Default: Blank.
Msg Type	Specify the message type this rule applies to. Default: Any. Valid Values: Any | Out of Dialog | Reply | Request | Out of Dialog.
Methods	Enter the method type to use when this SIP HMR is used. Default: Blank. Valid values" ACK | CANCEL | INVITE. When you do not set the method, the E-SBC applies the rule to all SIP methods.
Format	Select the encode - decode format from the drop-down list for the MIME content.
Action	Select an action from the drop-down list for the header rule. Default: None. Valid values: Add | Delete | Find Replace All | Log | Manipulate | Monitor | None | Reject | SIP Manip | Store.

Comparison Type	Specify how the E-SBC processes the match rules against the SIP header. Default: Refer Case Sensitive. Valid values: Boolean | Case Insensitive | Case Sensitive | Pattern Rule | Refer Case Insensitive | Refer Case Sensitive.
Match Value	Enter the value to match against the header value in SIP packets; the E-SBC matches these against the entire SIP header value. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators. When you configure HMR (using SIP manipulation rules and elements rules, you can use escape characters in the **match-value** parameter to support escaping Boolean and string manipulation operators. You can also escape the escape character itself, so that it is used as a literal string. For example, the E-SBC treats the string \+1234 as +1234. The following are escape characters: +, -, +^, -^, &, |, \, (,), ., $, ^, and “. You can also use the variables, $REMOTE_PORT and $LOCAL_PORT, which resolve respectively to the far-end and remote UDP or TCP port value.
New Value	When you set the action parameter Add or to Manipulate, enter the new value that you want to substitute for the entire header value. This is where you can set stored regular expression values for the E-SBC to use when it adds or manipulates SIP headers. When you configure HMR (using SIP manipulation rules and elements rules, you can use escape characters in the **match-value** parameter to support escaping Boolean and string manipulation operators. You can also escape the escape character itself, so that it is used as a literal string. For example, the E-SBC treats the string \+1234 as +1234. The following are escape characters: +, -, +^, -^, &, |, \, (,), ., $, ^, and “. You can also use the variables, $REMOTE_PORT and $LOCAL_PORT, which resolve respectively to the far-end and remote UDP or TCP port value.
Cfg Rules (instructions for configuring mime-header-rule)	(Optional) Click **Add**, **mime-header-rule**, and do the following. • Name—Enter a unique name for this header element rule. • Mime Header Name—Enter header name within the MIME part to which to apply the rule. • Action—Select an action from the drop-down list to apply to the element rule. • Comparison Type—Select the type of comparison from the drop-down list to use for the match value. • Match Value—Enter the match value to compare against the current object. • New Value—Enter a new value for the object. Quoted display named must be escaped within quotes. For example, \"MyName\" . • Click **OK**. The system displays the SIP manipulation / Mime sdp rule dialog.

	Do one of the following: • Add another mime-header-rule. • Configure the sdp-session-rule and sdp-media-rule options, using the steps in the following table cells. • Finish the MIME SDP rule configuration by completing steps 3-6.
Cfg Rules (instructions for configuring sdp-session-rule)	(Optional) Click **Add**, **sdp-session-rule** , and do the following. • Name—Enter a unique name for this header element rule. • Action—Select an action from the drop-down list to apply to the this rule. • Comparison Type—Select the type of comparison from the drop-down list to use for the match value. • Match Value—Enter the match value to compare against the current object. • New Value—Enter a new value for the object. Quoted display named must be escaped within quotes. For example, \"MyName\". • CfgRules—(Optional) Click **Add**, **sdp-line-rule**. • Name—Enter a unique name for this rule. • Type—Enter a descriptor type to specify the SDP line to manipulate. • Action—Select an action from the drop-down list to apply to this rule. • Comparison Type—Select the type of comparison from the drop-down list to use for the match value. • Match Value—Enter the match value to compare against the current object. • New Value—Enter a new value for the object. Quoted display named must be escaped within quotes. For example, \"MyName\". • Click **OK**. The system displays the SIP manipulation / Mime sdp rule / Sdp session rule dialog. • (Optional) Add another sdp-line-rule. • Click **OK**. The system displays the SIP manipulation / Mime sdp rule dialog. Do one of the following: • Add another sdp-session-rule. • Configure the mime-header-rule and sdp-media-rule options, using the steps in the corresponding table cells in this procedure. • Finish the MIME SDP rule configuration by completing steps 3-6.

Cfg Rules (instructions for configuring sdp-media-rule)	(Optional) Click **Add**, **sdp-media-rule**. • Name—Enter a unique name for this header element rule. • Media Type—Enter the media type to manipulate. For example, audio or video. • Action—Select an action from the drop-down list to apply to the element rule. • Comparison Type—Select the type of comparison from the drop-down list to use for the match value. • Match Value—Enter the match value to compare against the current object. • New Value—Enter a new value for the object. Quoted display named must be escaped within quotes. For example, "\"MyName\" " . • Click **OK**. • CfgRules—(Optional) Click **Add**, **sdp-line-rule**. • Name—Enter a unique name for this rule. • Type—Enter a descriptor type to specify the SDP line to manipulate. • Action—Select an action from the drop-down list to apply to this rule. • Comparison type—Select the type of comparison from the drop-down list to use for the match value. (To clear the value, enter and empty string.) • Match Value—Enter the match value to compare against the current object. (To clear the value, enter and empty string.) • New Value—Enter a new value for the object. Quoted display named must be escaped within quotes. For example, \"MyName\". • Click **OK**. The system displays the SIP manipulation / Mime sdp rule / Sdp media rule dialog. • (Optional) Add another sdp-line-rule. • Click **OK**. The system displays the SIP manipulation / Mime sdp rule dialog. Do one of the following: • Add another sdp-media-rule. • Finish the MIME SDP rule configuration by completing the following steps.

6. Click **Back**.

   The system displays the Add or Modify SIP Manipulation page.

7. Click **Back**.

   The system displays the SIP Manipulation page.

8. Save the configuration.

Configure a SIP Manipulation Header Rule

You can configure SIP header rules and element rules on the Oracle® Enterprise Session Border Controller (E-SBC) from the "CfgRules" section of the "SIP Manipulations" page.

In the following procedure, you set the SIP Header Manipulation, Header Rule, and Element Rule parameters.

1. Access the SIP Manipulation configuration object.

   Configuration, **System Administration**, **SIP Manipulation**.

2. On the SIP Manipulation configuration page, do one of the following:

   a. Select and existing SIP manipulation configuration from the table, right-click, and click **Edit**. (Subsequent SIP manipulation pages use "Modify" in the title.)

   b. Click **Add**. (Subsequent SIP manipulation pages use "Add" in the title.)

3. On the Add or Modify SIP Manipulation page, do one of the following.

   a. If you chose **Add**, you must enter a name for this SIP Manipulation. (You can optionally complete the Description, Split Headers, and Join Headers parameters, at this time. See "Configure SIP Manipulation.") Proceed to the next step.

   b. If you chose to edit an existing configuration, proceed to the next step.

4. On the Add or Modify SIP Manipulation page under Cgf Rules, click **Add** and click **header-rule**.

5. On the Add SIP Manipulation / Header Rule page, do the following.

Name	Enter a unique name for this rule set. Valid values: Alpha-numeric.
Header Name	Enter the name of the header on which you want the E-SBC to use this HMR. Set this parameter to @status-line, where the at-sign (@)—not allowed in SIP header names—to prevent undesired matches with header having the name status-code. Default: Blank.
Action	Select an action from the drop-down list for the header rule. Default: None. Valid values: Add | Delete | Find Replace All | Log | Manipulate | Monitor | None | Reject | SIP Manip | Store.
Comparison Type	Specify how the E-SBC processes the match rules against the SIP header. Default: Refer Case Sensitive. Valid values: Boolean | Case Insensitive | Case Sensitive | Pattern Rule | Refer Case Insensitive | Refer Case Sensitive.
Msg Type	Specify the message type this rule applies to. Default: Any. Valid Values: Any | Out of Dialog | Reply | Request | Out of Dialog.
Methods	Enter the method type to use when this SIP HMR is used. Default: Blank. Valid values" ACK | CANCEL | INVITE. When you do not set the method, the E-SBC applies the rule to all SIP methods.
Match Value	Enter the value to match against the header value in SIP packets; the E-SBC matches these against the entire SIP header value. This

	is where you can enter values to match using regular expression values. Your entries can contain Boolean operators. When you configure HMR (using SIP manipulation rules and elements rules, you can use escape characters in the **match-value** parameter to support escaping Boolean and string manipulation operators. You can also escape the escape character itself, so that it is used as a literal string. For example, the E-SBC treats the string \+1234 as +1234. The following are escape characters: +, -, +^, -^, &, |, \, (,), ., $, ^, and “. You can also use the variables, $REMOTE_PORT and $LOCAL_PORT, which resolve respectively to the far-end and remote UDP or TCP port value.
New Value	When you set the action parameter Add or to Manipulate, enter the new value that you want to substitute for the entire header value. This is where you can set stored regular expression values for the E-SBC to use when it adds or manipulates SIP headers. When you configure HMR (using SIP manipulation rules and elements rules, you can use escape characters in the **match-value** parameter to support escaping Boolean and string manipulation operators. You can also escape the escape character itself, so that it is used as a literal string. For example, the E-SBC treats the string \+1234 as +1234. The following are escape characters: +, -, +^, -^, &, |, \, (,), ., $, ^, and “. You can also use the variables, $REMOTE_PORT and $LOCAL_PORT, which resolve respectively to the far-end and remote UDP or TCP port value.
Cfg Rules	(Optional) Click **Add**, **element-rule**, and do the following. • Name—Enter a unique name for this header element rule. You can enter up to 128 alphanumeric characters with no spaces. The name can include the _, ., or - characters, cannot begin with either the . or the - characters. • Parameter name—Enter the parameter name to apply to the rule. • Type—Select the element type to which to apply this rule. • Action—Select an action from the drop-down list to apply to the element rule. Default: None. • Match Val Type—Select a match value type that this rule applies to from the drop-down list. Default: Any. • Comparison Type—Select an element type from the drop-down list to which to apply the rule. Default: Case Sensitive. • Match Value—Enter the match value to compare against the current object. (To clear the value, enter and empty string.) • New Value—Enter a new value for the object. Quoted display named must be escaped within quotes. For example, \"MyName\". (To clear the value, enter and empty string.) • Click **OK**. The system displays the SIP Manipulation / Header Rule page. Do one of the following:

	- Add another Element Rule. - Finish the Header Rule configuration by completing the following steps.

6. Click **Back**.

   The system displays the Modify SIP Manipulation page.

7. Click **Back**.

   The system displays the SIP Manipulation page.

8. Save the configuration.

Configure a MIME Rule

You can configure Multi-Purpose Internet Mail Extensions (MIME) header rules and element rules on the Oracle® Enterprise Session Border Controller (E-SBC) from the "CfgRules" section of the "SIP Manipulations" page.

In the following procedure, you set the SIP Header Manipulation, MIME Rule, and MIME Header Rule parameters.

1. Access the SIP Manipulation configuration object.

   Configuration, **System Administration**, **SIP Manipulation**.

2. On the SIP Manipulation configuration page, do one of the following:

   a. Select and existing SIP manipulation configuration from the table, right-click, and click **Edit**. (Subsequent SIP manipulation pages use "Modify" in the title.)

   b. Click **Add**. (Subsequent SIP manipulation pages use "Add" in the title.)

3. On the Add or Modify SIP Manipulation page, do one of the following.

   a. If you chose **Add**, you must enter a name for this SIP Manipulation. (You can optionally complete the Description, Split Headers, and Join Headers parameters, at this time. See "Configure SIP Manipulation.") Proceed to the next step.

   b. If you chose to edit an existing configuration, proceed to the next step.

4. On the Add or Modify SIP Manipulation page under Cfg Rules, click **Add** and click **mime-rule**.

5. On the Add or Modify SIP Manipulation / Mime Rule page, do the following.

Name	Enter a unique name for this rule set. Valid values: Alpha-numeric.
Content Type	Enter the name of the header on which you want the E-SBC to use this HMR. Set this parameter to @status-line, where the at-sign (@)—not allowed in SIP header names—to prevent undesired matches with header having the name status-code. Default: Blank.
Msg Type	Specify the message type this rule applies to. Default: Any. Valid Values: Any | Out of Dialog | Reply | Request | Out of Dialog.
Methods	Enter the method type to use when this SIP HMR is used. Default: Blank. Valid values" ACK | CANCEL | INVITE. When you do not set the method, the E-SBC applies the rule to all SIP methods.

Format	Select the encode - decode format from the drop-down list for the MIME content.
Action	Select an action from the drop-down list for the header rule. Default: None. Valid values: Add | Delete | Find Replace All | Log | Manipulate | Monitor | None | Reject | SIP Manip | Store.
Comparison Type	Specify how the E-SBC processes the match rules against the SIP header. Default: Refer Case Sensitive. Valid values: Boolean | Case Insensitive | Case Sensitive | Pattern Rule | Refer Case Insensitive | Refer Case Sensitive.
Match Value	Enter the value to match against the header value in SIP packets; the E-SBC matches these against the entire SIP header value. This is where you can enter values to match using regular expression values. Your entries can contain Boolean operators. When you configure HMR (using SIP manipulation rules and elements rules, you can use escape characters in the **match-value** parameter to support escaping Boolean and string manipulation operators. You can also escape the escape character itself, so that it is used as a literal string. For example, the E-SBC treats the string \+1234 as +1234. The following are escape characters: +, -, +^, -^, &, |, \, (,), ., $, ^, and “. You can also use the variables, $REMOTE_PORT and $LOCAL_PORT, which resolve respectively to the far-end and remote UDP or TCP port value.
New Value	When you set the action parameter Add or to Manipulate, enter the new value that you want to substitute for the entire header value. This is where you can set stored regular expression values for the E-SBC to use when it adds or manipulates SIP headers. When you configure HMR (using SIP manipulation rules and elements rules, you can use escape characters in the **match-value** parameter to support escaping Boolean and string manipulation operators. You can also escape the escape character itself, so that it is used as a literal string. For example, the E-SBC treats the string \+1234 as +1234. The following are escape characters: +, -, +^, -^, &, |, \, (,), ., $, ^, and “. You can also use the variables, $REMOTE_PORT and $LOCAL_PORT, which resolve respectively to the far-end and remote UDP or TCP port value.
Cfg Rules	Click **Add**, **mime-header-rule**, and do the following. • Name—Enter a unique name for this header element rule. You can enter up to 128 alphanumeric characters with no spaces. The name can include the _, ., or - characters, but cannot begin with either the . or the - characters. • Mime Header Name—Enter header name within the MIME part to which to apply the rule. Use headername@peramble to change the preamble of a SIP body. Use headername@epilogue to change the epilog of a SIP body. • Action—Select an action from the drop-down list to apply to the element rule. Default: None.

	• Comparison Type—Select the type of comparison from the drop-down list to use for the match value. Default: Match Value. (To clear the value, enter and empty string.) • Match Value—Enter the match value to compare against the current object. (To clear the value, enter and empty string.) • New Value—Enter a new value for the object. Quoted display named must be escaped within quotes. For example, \"MyName\". (To clear the value, enter and empty string.) • Click **OK**. The system displays the SIP Manipulation / Mime Rule dialog. Do one of the following: • Add another mime-header-rule. • Finish the MIME Rule configuration by completing the following steps.

6. Click **Back**.

   The system displays the Add or Modify SIP Manipulation page.

7. Click **Back**.

   The system displays the SIP Manipulation page.

8. Save the configuration.

Configure SIP Monitoring

Use the SIP Monitoring object to configure SIP Monitor and Trace features and to set filters for SIP monitoring.

- 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.

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.

1. From the Web GUI, click **Configuration**, **Session Router**, **SIP Monitoring**.
2. On the SIP Monitoring page, do the following:

Match Any Filter	Select to enable. Default: Disabled.
State	Select to enable the sip-monitoring configuration. Default: Enabled.

Short Session Duration	Enter the maximum number of seconds for a session to be considered short duration. Default: 0. Range: 0-999999999.
Monitoring Filters	Enter one or more custom monitoring filters to the list to use when monitoring on a global-basis. Use the + character to add a recording server to the existing list and the - character to remove one. Omit the + and - characters to replace the list.
Interesting Events	Click **Add**, and do the following: • Type—Select either short session or local rejection. • Trigger Threshold—Enter the number of interesting events to raise the trigger. Default:0. Range 0-999999999. • Trigger Timeout—Enter the timeout trigger in seconds. Default: 0. Range:999999999.
Trigger Window	Enter a number from 0-999999999.

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

Surrogate Registration

The Oracle® Enterprise Session Border Controller surrogate registration feature lets the Oracle® Enterprise Session Border Controller explicitly register on behalf of a Internet Protocol Private Branch Exchange (IP-PBX). After you configure a surrogate agent, the Oracle® Enterprise Session Border Controller periodically generates a REGISTER request and authenticates itself using a locally configured username and password, with the Oracle® Enterprise Session Border Controller as the contact address. Surrogate registration also manages the routing of class from the IP-PBX to the core and from the core to the IP-PBX.

Configure Surrogate Registration

Surrogate registration allows the Oracle® Enterprise Session Border Controller (E-SBC) to explicitly register on behalf of an Internet Protocol Private Branch Exchange (IP-PBX). Surrogate registration also manages the routing of calls from the IP-PBX and from the core to the IP-PBX. The E-SBC uses the configuration information of the surrogate agent that corresponds to a specific IP-PBX to send REGISTER requests. You can configure the number of requests to send.

Configure a surrogate agent for each IP-PBX proxy that you want the E-SBC to register.

> **Note:**
>
> To view all surrogate agent configuration parameters, enter a **?** at the Surrogate Agent prompt.

1. From the Web GUI, click **Configuration**, **Session Router**, **Surrogate Agent**.
2. On the Add Surrogate Agent page, click **Add**, and do the following:

Register Host	Enter the registrar’s hostname to be used in the Request-URI of the REGISTER request. This name is also used as the host portion of the AoR To and From headers.
Register User	Enter the user portion of the AoR (Address of Record).
Description	Optional. Enter a description of this surrogate agent.
Realm ID	Enter the name of realm where the surrogate agent resides (where the IP-PBX proxy resides). There is no default.
State	Set the state of the surrogate agent to indicate whether the surrogate agent is used by the application. The default value is **enabled**.
Customer Host	Optional. Enter the domain or IP address of the IP-PBX, which is used to determine whether it is different than the one used by the registrar.
Customer Next Hop	Enter the next hop to this surrogate agent: • session agent group: <session agent group name> • session agent: <hostname> or <IPV4>
Register Contact Host	Enter the hostname to be used in the Contact-URI sent in the REGISTER request. This should always point to the E-SBC. If specifying a IP address, use the egress interface’s address. If there is a SIP NAT on the registrar’s side, use the home address in the SIP NAT.
Register Contact User	Enter the user part of the Contact-URI that the E-SBC generates.
Password	If you are configuring the auth-user parameter, you need to enter the password used when the registrar sends the 401 or 407 response to the REGISTER request.
Register Expires	Enter the expires in seconds for the REGISTER requests. The default value is **600,000** (1 week). The valid range is 0-999999999.
Replace Contact	This specifies whether the E-SBC needs to replace the Contact in the requests coming from the surrogate agent. If this is enabled, Contact will be replaced with the Contact-URI the E-SBC sent in the REGISTER request. The default value is **disabled**. The valid values are enabled and disabled.
Options	Optional. Enter non-standard options or features.
Route to Registrar	This indicates whether requests coming from the surrogate agent should be routed to the registrar if they are not explicitly addressed to the E-SBC. The default value is **enabled**. The valid values are enabled and disabled.
AoR Count	Enter the number of registrations to do on behalf of this IP-PBX. If you enter a value greater than **1**, the E-SBC increments the register-user and the register-contact-user values by that number. For example, if this count is 3 and register-user is john

	then users for three different register messages will be john, john1, john2. It does the same for the register-contact-user values. The default value is **1**. The valid range is 0-999999999.
Auth User	Enter the authentication user name you want to use for the surrogate agent. This name is used when the E-SBC receives a 401or 407 response to the REGISTER request and has to send the REGISTER request again with the Authorization or Proxy-Authorization header. The name you enter here is used in the Digest username parameter. If you do not enter a name, the E-SBC uses the value of the register-user parameter.
Max Register Attempts	Enter the total number of times to attempt registration until success. Range 1-10
Registry Retry Time	Enter the time to wait after an unsuccessful registration before re-attempting. Range 30-3600
Count Start	Enter the starting value for numbering when performing multiple registrations. Range 0-9999999999
Register Mode	Select automatic (default) or triggered (upon trigger from PBX).
Triggered Inactivity Interval	Enter the maximum time with no traffic from the corresponding PBX. (Valid only with Triggered inactivity interval.) Range 5 -300
Triggered OoS Response	503 (Default. Send 503 response for core network failure) or drop response (Do not respond to PBX or core network failure

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

- Add the surrogate agent as a session-agent under session-router.

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.

- Configure at least one Session Agent.

1. From the Web GUI, click **Configuration**, **Session Router**, **Session Router**, **Survivability**.
2. On the Add Survivability page, do the following:

State	Select to enable Survivability.
Service Tag	Enter one or more service tags.
Reg Expires	Enter the number of seconds that the E-SBC waits before entering the remote site survivability mode when the registration expires. Default: 30. Range: 0-86400.
Prefix Length	Enter the maximum number of digits allowed for a phone extension. Default: 4. Range: 0-10.
Session Agent Hostname	Select or enter the agent hostname or the session agent group name from the drop down list. For a Session Agent Group, use the session agent group name. For a single Session Agent, use the hostname, IPv4, o IPv6 address.

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

- Configure a ping method on the Session Agent. See "Configure a Session Agent."

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 object to create unique sets of translation rules to apply to calling and called party numbers.

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.

1. From the Web GUI, click **Configuration**, **Session Router**, **Translation Rules**.
2. On the Translation rules page, do the following:

ID	Enter the identifier or name for this rule.
Type	Select the address translation type from the drop-down list. • Add—Add one or more characters to the address.

	• Delete—Delete one or more characters from the address. • None—Disable the translation rule. • Replace—Replace one or more characters in the address.
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.
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. **Note:** The @ character only works when you set the Type parameter 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.
Delete Index	Enter the index for the string to delete.

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

System Configuration

You can configure the following System objects from the Configuration tab on the Web GUI. See the documentation specified in the following list for explanations of these configuration objects and how to set their parameters.

Capture Receiver	Enable and configure a capture receiver. See the "Capture Receiver" section of the *ACLI Reference Guide*.
Fraud Protection	Enable and configure fraud protection. See the "Telephony Fraud Protection" section of the "System Configuration" chapter in the *ACLI Configuration Guide*.

Host Route	Add one or more host routes. See the "Host Routes" section of the "System Configuration" chapter in the *ACLI Configuration Guide*.
HTTP Client	For future use. Not supported at this time.
HTTP Server	For future use. Not supported at this time.
Network Interface	Add one or more network interfaces. See the "Network Interfaces" section of the "System Configuration" chapter in the *ACLI Configuration Guide*.
Network Parameters	Configure SCTP and TCP parameters for the network. See the "Stream Control Transfer Protocol Overview" and "System TCP Keepalive Settings" sections of the "System Configuration" chapter in the *ACLI Configuration Guide*.
NTP Config	Add one or more NTP servers and authentication servers. See the "NTP Synchronization" section of the "System Configuration" chapter in the *ACLI Configuration Guide*.
Phy Interface	Add one or more physical interfaces. See the "Phy Interfaces" section of the "System Configuration" chapter in the *ACLI Configuration Guide*.
Redundancy Config	Enable redundancy and add one or more peers. See the "SIP Server Redundancy" section of the "SIP Signaling Services" chapter in the *ACLI Configuration Guide*.
SNMP Address Entry	Add one or more SNMP addressees. See "SNMP-Address-Entry" in the *ACLI Reference Guide*.
SNMP Community	Add and specify one or more Simple Network Management Protocol (SNMP) communities. See "SNMP v1 v2 Community Configuration" in the *ACLI Configuration Guide* and "SNMP-Community" in the *ACLI Reference Guide*.
SNMP Group Entry	Add one or more SNMP groups. See "SNMP-Group-Entry" in the *ACLI Reference Guide*.
SNMP User Entry	Add one or more SNMP users. See "SNMP-User-Entry" in the *ACLI Reference Guide*.
SNMP View Entry	Add one or more SNMP views. See "SNMP-View-Entry" in the *ACLI Reference Guide*.
SPL Config	Add an SPL option and one or more plugins. See the "SPL Plug-in Language" chapter in the *ACLI Configuration Guide*.
System Access List	Add one or more system access lists. See "System Access List" in the *ACLI Reference Guide*.
System Config	Configure the system settings for MIBS, SNMP functions, syslog servers, comm monitor, and more. See the "System Configuration" chapter in the *ACLI Configuration Guide*.
TDM Config	Enable and configure Time Division Multiplexing (TDM). See the *Time Division Multiplexing Guide*. For the Acme Packet 1100, only.

Threshold Crossing Alert	Configure an alarm threshold type to indicate the resource to monitor. See "Configurable Alarm Thresholds and Traps" section in the "System Configuration" chapter in the *ACLI Configuration Guide*.
Trap Receiver	Add one or more trap receivers. See "Trap Receiver" in the *ACLI Reference Guide*.
Web Server Config	Enable and configure a web server, including a TLS profile. See the "Web Server TLS Configuration" chapter in the *ACLI Configuration Guide*.

Telephony Fraud Protection

You can use the Oracle® Enterprise Session Border Controller (E-SBC) to protect against fraudulent calls by enabling Telephony Fraud Protection and creating lists of phone numbers to block, allow, redirect, and rate limit calls. The lists reside together in a single source-file that you create and manage. The source-file can contain any combination of the list types and it can reside on either the E-SBC or in Session Delivery Manager (SDM) because you can manage Telephony Fraud Protection from either one. The following information explains using Telephony Fraud Protection on the E-SBC. See the *Oracle Communications Session Element Manager User Guide for the Enterprise Edge and Core Plug-in* for managing Telephony Fraud Protection from SDM.

Fraud Protection List Types and Uses

The E-SBC supports the following types of lists for protecting against fraudulent calls.

Blacklist—Use the blacklist to specify a fraudulent call based on the destination phone number or URI. You can add a known fraudulent destination to the blacklist by prefix or by fixed number. When the E-SBC receives a call to an entry on the blacklist, the system rejects the call according to the SIP response code that you specify. When the system determines a match and blocks a call, the default response is "403 Forbidden." You can set another SIP response code from the standard list of responses defined in RFC3261 by way of the **Local Response Map** configuration and the local error **Fraud Protection Reject Call** setting.

White List—Use the white list to manage any exception to the blacklist. Suppose you choose to block a prefix such as +49 555 123 by way of the blacklist. This also blocks calls to individual numbers starting with this prefix, such as +49 555 123 666. If you add a prefix or individual number to the white list, the system allows calls to the specified prefix and number. Continuing with the example, if you add +49 555 123 6 to the white list, the system allows calls to +49 555 123 666, which was blocked by the blacklist entry of +49 555 123.

Redirect List—Use the redirect list to send a fraudulent call to an Interactive Voice Response (IVR) system, or to a different route. For example, you can intercept and redirect a call going to a revenue-share fraud target in a foreign country to an end point that defeats the fraud. Or, you might want to redirect subscribers dialing a particular number and URI to an announcement to make them aware that an account is compromised and tell them what they should do. You can use an external server to provide such an announcement or you can use the E-SBC media playback function.

Rate Limit List—Use rate limiting to limit the loss of money, performance, and availability that an attack might cause. While local ordinances may not allow you to completely block or suppress communication, you may want to reduce the impact of a disruption with rate limiting until a network engineer can analyze an attack and plan remediation. For example, you might want time to find the origin of an attack or to add attackers to a blacklist. Note that rate limiting may not function immediately after a High Availability switch over because the newly active system must re-calculate the call rate before it can apply rate limiting.

Configuration

The process for using Telephony Fraud Protection includes the following steps:

1. Enable Telephony Fraud Protection
2. Specify the source of fraud protection management
3. Create the file that contains the list of phone numbers to manage
4. Activate the fraud protection file

You can create the fraud protection phone number list on the File Management page on the Web GUI, or you can create it externally in XML and upload it to the E-SBC. Save the file to /code/fpe/<filename>. In the *Web GUI User Guide*, see "Configure Telephony Fraud Protection," "Create a Telephony Fraud Protection File," and "Telephony Fraud Protection File Activation." If you want to create the fraud protection file externally, see "Fraud Protection XML Source File Example."

You can enable Telephony Fraud Protection from either the Web GUI or from the ACLI command line, but you cannot manage fraud protection from the ACLI. You must use the Web GUI for management, and only in Expert Mode.

Telephony Fraud Protection is included in the advanced license.

Administration

When you configure the E-SBC to manage Telephony Fraud Protection, the system applies the following behavior:

- An Administrator with privileges can Refresh, Add, and Upload an unselected file, and Edit, Download, and Delete a selected file.
- An Administrator with no privileges can only view the fraud protection file.

To view fraud protection data:

- From the ACLI, use the show commands to view fraud protection statistics. See "Telephony Fraud Protection Show Commands."
- From the Web GUI, use the Show Summary, Show Blacklist, Show White List, Show Call Redirect List, and Show Rate Limit Widgets.

> **Note:**
>
> The Telephony Fraud Protection feature does not affect emergency calls or block any calls while you are loading entries.

High Availability

Telephony Fraud Protection supports High Availability (HA).

- When the E-SBC manages the Telephony Fraud Protection file—Use the **Synchronize File <filename>** command to copy the Telephony Fraud Protection file to the standby after an HA switch over.
- When the Enterprise Telephony Fraud Manager in SDM manages the Telephony Fraud Protection file—After an HA switch over, the newly active E-SBC sends the RESYNC command to the Fraud Manager on SDM, requesting the latest file. SDM responds with the name and location of the file, which the E-SBC downloads from SDM.
- Note that after a switch over, rate limiting may not take effect immediately because the new Active system needs time to recalculate the call rate before it can apply rate limiting.

Telephony Fraud Protection Management from SDM

If you prefer to manage Telephony Fraud Protection from the Enterprise Fraud Manager in SDM, rather than from the E-SBC, store the fraud protection list in a file named **sbc_fpe_entries.xml** (case sensitive) in SDM. You can edit the file in SDM, which will notify the E-SBC afterwards to download the file to its **/code/fpe** directory. When the E-SBC is part of an HA pair, the Active partner automatically pushes the updated file to the Standby partner. In the event of an unsuccessful download, the system raises an SNMP alarm. Should the connection to SDM ever go down, the system also raises an SNMP alarm and sends a trap. When the connection gets re-established, the alarm and trap clear, and the E-SBC sends a RESYNC command to SDM.

Unsupported Functions

Telephony Fraud Protection for the E-SBC does not support the following:

- IPv6
- H.323
- InterWorking Function (IWF)
- Comm Monitior

Telephony Fraud Protection Target Matching Rules

When matching a call to an entry on a telephony fraud protection list, the Oracle® Enterprise Session Border Controller (E-SBC) performs the matching only on the ingress leg of the initial INVITE. In the initial INVITE, the E-SBC uses the From, To, and User-Agent headers for matching. Because you can place a phone number on multiple types of fraud prevention lists in the same source file, the E-SBC uses the following evaluation hierarchy to determine which number takes precedence:

1. Longest match—The most specific entry takes precedence. For example, when 555-123-4000 is blacklisted and 555-123-* is white listed, the system blocks the call from 555-123-4000 because it is the longest match.
2. Destination—When the system detects matches in both the SIP **From** header and the SIP **To** header, the match for the **To** header takes precedence.
3. URI—When the system detects matches in both the **USER** and **Host** parts of a SIP URI, the match for the **USER** part takes precedence.
4. SIP User-Agent header—Lowest priority. When nothing else matches, and there is a match for the User-Agent field, the E-SBC acts as instructed.

5. Multiple instances—When the system detects multiple instances of the same match length, or when the target resides in multiple lists, the system uses the following order of precedence:
   1. White list—Entries on the white list take precedence with no restrictions. For example, when 555-123-4567 is on both the blacklist and the white list, the system allows this call because the number is on the white list.

   2. Blacklist

   3. Redirect

   4. Rate limiting

> **Note:**
>
> The telephony fraud protection feature does not affect emergency calls.

The telephony fraud protection feature uses source or destination IP, source or destination name or phone number, and caller user-agent to identify a caller. The system enforces the following rules for formatting entries on a fraud protection list:

Hostname

Format: Enter the exact IP address or FQDN.

User name

Format: Enter the exact user name. For example: joe.user or joe_user.

User-Agent-Header

The User-Agent header text in the INVITE message from the first call leg. This text usually contains the brand and firmware version of the SIP device making the call. For example, sipcli/v1.8, Asterisk PBX 1.6.026-FONCORE-r78.

Format: Enter the exact text.

Phone Number

Format: Enter the exact number or a partial number using the following characters to increase the scope of the matches.

Asterisk *	Use to indicate prefix matching, but only at the end of the pattern. For example, use 555* not *555. Do not use * in any other patterns, for example, in brackets [ ], parentheses ( ), or with an x.
Square Brackets [ ]	Use to enclose ranges in a pattern. Syntax: [min-max]. For example: 555 [0000-9999]. The system considers 8[1-20]9 and 8[01-20]9 to contain the same number of characters because the leading 0 is implied. The system strictly enforces this pattern with respect to the range and the number of characters, as follows: • 8019 matches • 819 does not match

	• 8119 matches
Character x	Use as a wildcard a the end of a dial pattern to mean 0-9. For example: 555xxx means match a number starting with 555 followed by 3 digits from 0-9.
Parentheses ( )	Use to enclose optional digits in a pattern. For example: 555xx(xxxx) means match a number starting with 555 plus a minimum of 2 digits, and optionally up to 4 more digits.

Telephony Fraud Protection File Activation

After you create, edit, or upload the telephony fraud protection file, you must activate the file before the Oracle® Enterprise Session Border Controller (E-SBC) can use it as the source of the fraud protection lists. The system recognizes only one file at a time as the active file.

The first time you configure the E-SBC to manage fraud protection, the system activates the file when you save and activate the configuration. After the initial configuration, the system does not automatically refresh the fraud protection file when you save and activate other configuration changes on the E-SBC. You must upload a new file or edit the existing file and activate it to update the file. The exception occurs when you specify a new file name in the fraud protection configuration and coincidentally make changes to other configurations, and then save and activate all of the changes at the same time.

After the initial configuration, use the following methods to activate the fraud protection file.

- New File—After you create or upload a new file, go to Fraud Protection configuration, enter the name of the new file, and click Save. The system prompts for activation upon a successful Save. Note that you can decline the inline activation and manually activate the file later. For example, you might want to edit an uploaded file before activation.
- Overwrite File—When you upload a file with the same name as the existing file, the system prompts for activation upon upload.
- Edit File—When you edit the existing file directly from the Web GUI, the system prompts for activation after you save the edits.
- Refresh File—When you want to use the ACLI to refresh the fraud protection file, send the file to the E-SBC and use the `notify fped refresh` command. The name of the file that you refresh must match the name of the file specified in the configuration.

Note:

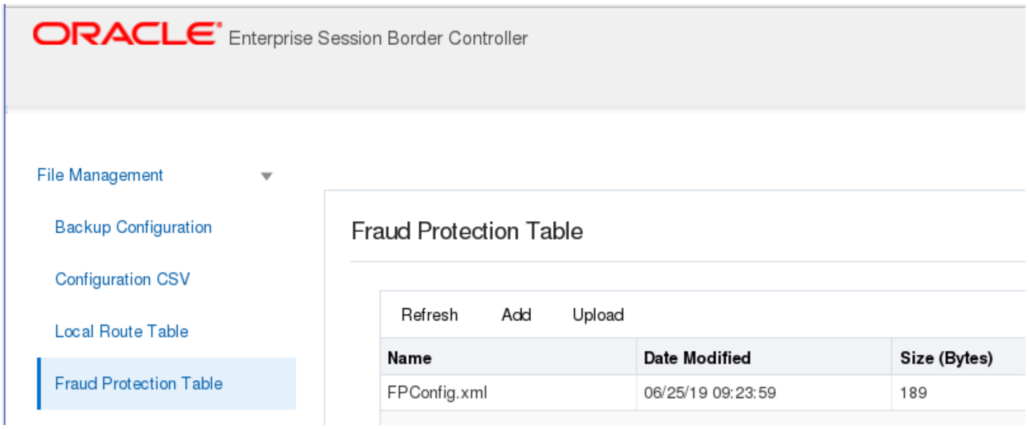
The system displays an alert on the Notifications menu to remind you that the fraud protection file needs activation.

Telephony Fraud Protection File Management

When you want to edit the telephony fraud protection file managed by the Oracle® Enterprise Session Border Controller (E-SBC), use the Web GUI. You cannot manage the fraud protection file from the ACLI. When another device manages the file, you can edit the file on the device and upload the file to the E-SBC or you can upload the file to the E-SBC and perform edits prior to activation.

A user with Admin privileges can work with the fraud protection file, while a user with no Admin privileges can only view the file. The Web GUI supports fraud protection file management only in the Expert mode.

From the System tab, the File Management page displays the Fraud Protection Table object. The Fraud Protection Table displays the list of fraud protection files on the E-SBCand management controls, as shown in the following illustration.



Name	Date Modified	Size (Bytes)
FPConfig.xml	06/25/19 09:23:59	189

A privileged Admin can **Refresh** the display, **Add** a new file, and **Upload** a file. Upon selecting a file, the Admin can **Edit**, **Download**, and **Delete** a file.

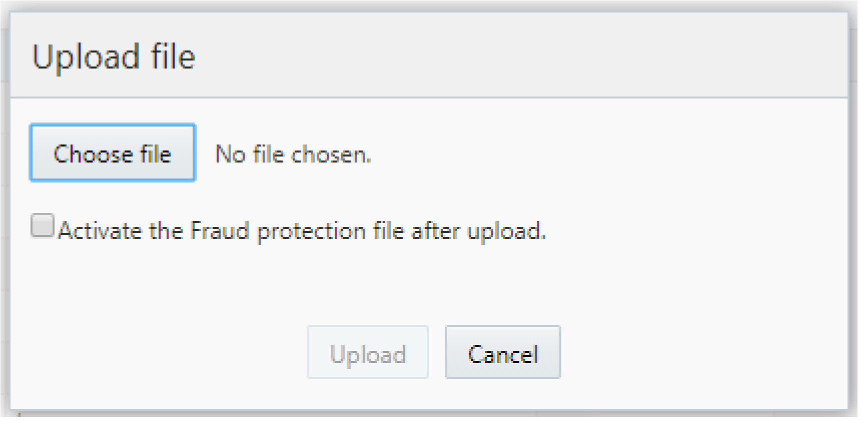
File Activation

The first time you configure the E-SBC to manage fraud protection, the system activates the file when you save and activate the configuration.

> **Note:**
>
> After the initial configuration, the system does not refresh the fraud protection file until you specify a new file name in the fraud protection configuration or upload a new version of the existing file.

File Upload from an External Source

When you want to use a fraud protection file from another source, you can upload the file to the E-SBC. The system puts the file into the /code/fpe directory. The system supports only the .gz, .gzip, and .xml file extensions for a fraud protection file. The Upload File dialog provides the option to activate the fraud protection file upon upload when the uploaded file name matches the configured file name, as shown in the following illustration.



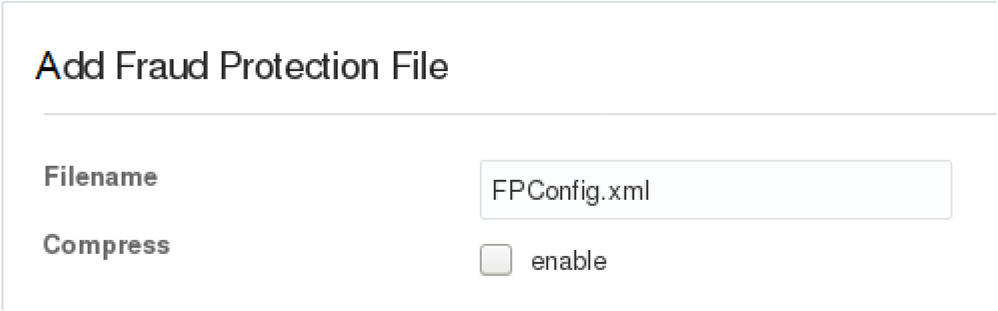
No file chosen.

□ Activate the Fraud protection file after upload.

You can activate the file upon upload, or at a later time. For example, you might not activate the file upon upload because you want to edit the entries before activation. If you do not select the option to activate the file now, you must manually activate the file before the system can use the file. When the name of the uploaded file differs from the one specified in the configuration, the Upload dialog does not display the option to activate the file because the system cannot use the file until you specify the file name in the fraud protection configuration and activate the configuration.

File Creation

When you want to create a new fraud protection file on the E-SBC, use the **Add** control on the File Management page to launch the following dialog.



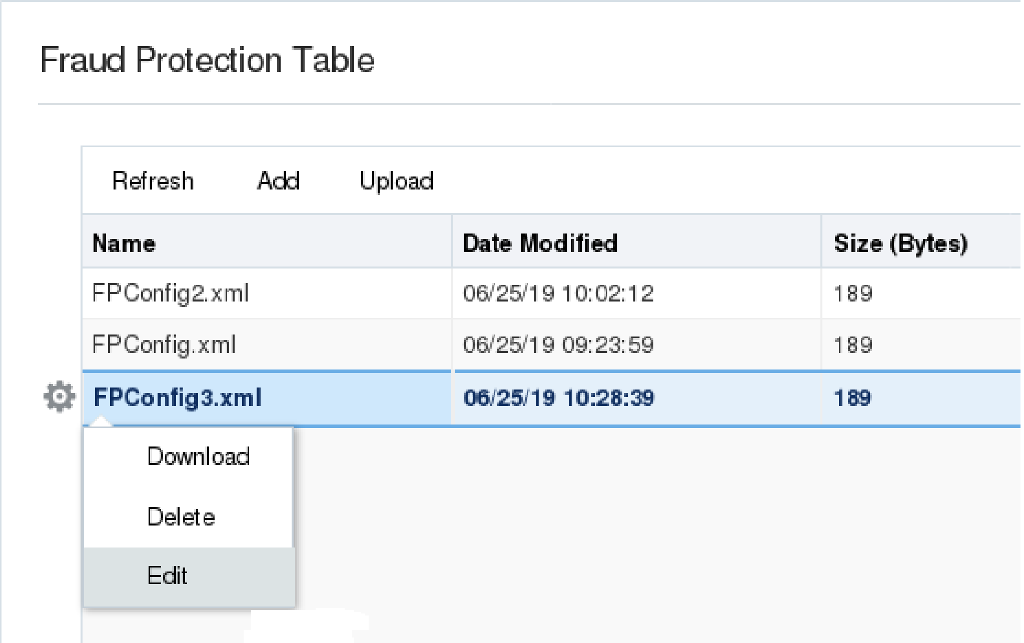
Filename: FPConfig.xml

Compress: □ enable

After you enter the file name and click **OK**, the system adds the new file to the list of Fraud Protection Tables on the File Management page. To make the new file the source file for Fraud Protection, you must specify the file name in the fraud protection configuration and activate the configuration.

List Maintenance

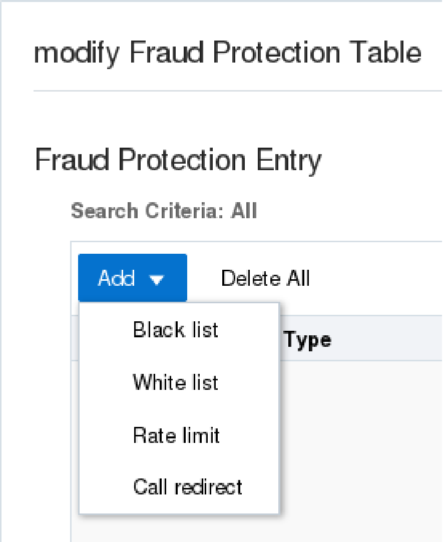
When you want to edit a fraud protection list, select the file on the File Management page, right-click, and click **Edit**.



Fraud Protection Table

Name	Date Modified	Size (Bytes)
FPConfig2.xml	06/25/19 10:02:12	189
FPConfig.xml	06/25/19 09:23:59	189
FPConfig3.xml	06/25/19 10:28:39	189

On the Modify Fraud Protection Table page, click the Add arrow, and select a file type from the drop-down list.



modify Fraud Protection Table

Fraud Protection Entry

Search Criteria: All

The Web GUI displays the corresponding dialog for editing.

Telephony Fraud Protection Data Types and Formats

Use the information in the following tables when you create or edit a fraud protection list in the Add Fraud Protection Entry and Modify Fraud Protection Entry dialogs.

Data Type Descriptions

The following table describes the data types listed in the **Type** drop-down list.

from-hostname	The hostname from the SIP FROM header.
from-phone-number	The phone number from the SIP FROM header

from-username	The user name from the SIP FROM header.
to-hostname	The hostname from the SIP TO header.
to-phone-number	The phone number from the SIP TO header.
to-username	The user name from the SIP TO header.
user-agent-header	The SIP User-Agent header.

Match Value Formats

The following table describes the formats required for the data types.

hostname	Enter the exact IP address or FQDN.
username	Enter the exact user name. For example: joe.user or joe_user.
user-agent-header	Enter the exact text match to the SIP User-Agent header. For example: equipment vendor information.
phone-number	You can use the following characters for phone-number: • Asterisk *. Use to indicate prefix matching, but only at the end of the pattern. For example, use 555* not *555. Do not use * in any other patterns, for example, in brackets [ ], parentheses ( ), or with an x. • Brackets [ ]. Use to enclose ranges in a pattern. Syntax: [min-max]. For example: 555 [0000-9999]. • Parentheses. ( ) Use to enclose optional digits in a pattern. For example: 555xx(xxxx) means 555 with between 2 and 4 following digits. • Character x. Use as a wildcard a the end of a dial pattern to mean 0-9. For example: 555xxx means a number starting with 555 followed by 3 digits.

> **Caution:**
>
> The use of encoding characters is especially susceptible to creating overlapping dial pattern matches that can result in unexpected behavior.

Create a Telephony Fraud Protection File

When you want to use the Oracle® Enterprise Session Border Controller (E-SBC) to manage telephony fraud protection, the system requires a specified file to use as the source of the fraud protection lists. When you do not want to upload a file from elsewhere, you can create a new file on the E-SBC. You can create more files now or anytime after configuring fraud protection, but the system uses only the file named in the Fraud Protection configuration as the source file. Note that you cannot create a fraud protection file by way of the ACLI. You must use the Web GUI.

- Confirm that the system displays the Expert mode.

Use the following procedure to create a new fraud protection file on the E-SBC, either before or after enabling fraud protection. See "Telephony Fraud Protection Data Types and Formats" for more information about the selections and formats for Type and Match Value.

1. Access the File Management configuration object: **Configuration**, **System**, **File Management.**.
2. On the File Management page, select Fraud Protection Table from the File Management list.
3. Click **Add**.
4. In the Add Fraud Protection table dialog, do the following:

Filename	Enter the name of the file. File extensions allowed: .gz, .gzip, or .xml.
Compress	(Optional) Select to compress the file.

5. Click **OK**.

   The system displays the Fraud Protection Entry page.
6. Click **Add**, select a list type to add to the file, and do the following according to the list type:

Blacklist	• Type—Select the type of data to match from the drop-down list. • Match Value—Enter the value in the format that corresponds to the Type. Phone (exact match or prefix), Name (exact match), Source or destination IP or FQDN (exact match), or User agent. • Ingress Realm—Select the ingress realm from the drop-down list to associate to the match value.
White List	• Type—Select the type of data to match from the drop-down list. • Match Value—Enter the value in the format that corresponds to the Type. Phone (exact match or prefix), Name (exact match), Source or destination IP or FQDN (exact match), or User agent. • Ingress Realm—Select the ingress realm from the drop-down list to associate to the match value.
Rate Limit	• Type—Select the type of data to match from the drop-down list. • Match Value—Enter the value in the format that corresponds to the Type. Phone (exact match or prefix), Name (exact match), Source or destination IP or FQDN (exact match), or User agent. • Ingress Realm—Select the ingress realm from the drop-down list to associate to the match value. • Calls Per Second—Enter the number of calls per second to allow for the entry. Range:0-65535. 0 = unlimited. • Max Active calls—Enter the maximum number of active calls allowed for the entry. Range: 0-65535. 0 = unlimited.

Call Redirect	• Type—Select the type of data to match from the drop-down list. • Match Value—Enter the value in the format that corresponds to the Type. Phone (exact match or prefix), Name (exact match), Source or destination IP or FQDN (exact match), or User agent. • Ingress Realm—Select the ingress realm from the drop-down list to associate to the match value. • Redirect Target—Enter one of the following: Session agent, session agent group name, Hostname, or IP address.

7. Click **OK**.
8. (Optional) Repeat steps 6 and 7 to add more entries.
9. Click **Verify**.

   The system checks for valid entries in the configuration fields and saves a successful configuration.
10. Click **Save**.
11. Click **Close**.

    The Web GUI displays the Fraud Protection Table.

- When fraud protection is not configured, see "Configure Telephony Fraud Protection - GUI."
- When fraud protection is configured, see "Activate a New Telephony Fraud Protection File -GUI."

Upload a Telephony Fraud Protection File

When you want to use a telephony fraud protection file from another source, you can upload the file to the Oracle® Enterprise Session Border Controller (E-SBC) by way of the Web GUI. You cannot upload the file by way of the ACLI.

- Confirm that the file to upload uses one of the following file extensions: .gz, .gzip, or .xml.
- Log on to the Web GUI directly to the Expert mode. (The system does not allow this procedure when you log on to Basic mode and switch to Expert mode.)

When you upload a fraud protection file, the system puts the file into the /code/fpe directory. The Upload File dialog provides the option to activate the fraud protection file immediately after the upload, or at a later time. For example, you might defer activation because you want to edit the uploaded file before it becomes the active file.

1. Access the File Management configuration object: **System**, **File Management**.
2. On the File Management page, select Fraud Protection Table from the list.
3. Select a file, and click **Upload**.
4. In the Upload file dialog, click **Choose file**do the following:

File to Upload.	Browse to the file to upload.
(Optional) Activate the File After Upload.	Select to activate the file now.

5. Click **Upload**, and select the file.

6. Click **Open**.
7. Click **Upload**.

   The Web GUI displays the file in the Fraud Protection table.

- When fraud protection is not configured, see "Configure Telephony Fraud Protection - GUI."
- When fraud protection is configured, see "Activate a New Telephony Fraud Protection File - GUI."

Configure Telephony Fraud Protection

The telephony fraud protection feature requires configuration, which you can perform from the Oracle® Enterprise Session Border Controller (E-SBC) Web GUI by way of **Fraud Protection** listed under System on the Configuration tab.

- Confirm that you own the Advanced license.
- Add or upload at least one telephony fraud protection file to the E-SBC.
- Note the name of the telephony fraud protection file that you want to use.
- Login to Expert Mode directly. (The system does not allow this procedure when you login to Basic mode and switch to Expert Mode.)

Use this procedure to enable telephony fraud protection management on the E-SBC. You must also specify the fraud protection file name and activate the configuration. You cannot specify multiple fraud protection files because the system recognizes only one file as the active source file.

> **Note:**
>
> The first time you configure the E-SBC to manage fraud protection, the system activates the file when you save and activate the configuration. After the initial configuration, the system does not refresh the fraud protection file when you save and activate other configuration changes on the E-SBC. The exception occurs when you specify a new file name in the fraud protection configuration, make changes to other configurations, and save and activate all of the changes at one time.

1. Access the Fraud Protection configuration object: **Configuration**, **System**, **Fraud Protection**.
2. On the Fraud Protection page, do the following:

Mode	Select one of the following modes from the drop-down list. • Local—Specifies the E-SBC as the source of the fraud protection file. • Comm Monitor—Not currently supported. • Disabled—Default
File Name	Enter the name of the fraud protection file or select a file from the drop-down list.

Options	Add fraud protection options. (Not supported in some releases.)
Allow Remote Call Terminate	Not currently supported.

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

Activate a New Telephony Fraud Protection File

When you create or upload a new telephony fraud protection file, you must activate the file before the system can use it as the source of the fraud protection lists. A new file is a file with a different name than one already in the system.

- Create or upload the new file.
- Note the name of the file that you want to activate.
- Confirm that the system displays the Expert Mode. You can activate a fraud protection file from the Web GUI only in Expert Mode.

In the following procedure, the Local Mode establishes the Oracle® Enterprise Session Border Controller (E-SBC) as the source of fraud protection management.

1. Access the Fraud Protection configuration object: **Configuration**, **System**, **Fraud Protection**.
2. On the Fraud Protection page, do the following:

Mode	Select Local.
File Name	Select the file to activate from the drop-down list or enter the file name.

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

Edit a Telephony Fraud Protection File

When you want to edit a telephony fraud protection file on the Oracle® Enterprise Session Border Controller (E-SBC), use the Web GUI. You cannot edit a telephony fraud protection file from the ACLI.

To edit a fraud protection file, go to the Web GUI and select a file from the list on the File Management page. When you click **Edit**, the system displays the fraud protection lists in the file. Select a list type and click **Edit**. The system displays the corresponding dialog for editing the selected type of list. See "Telephony Fraud Protection Data Types and Formats" for more information about the selections and formats for Type and Match Value.

You can use this procedure to edit any fraud protection file, but the system cannot use the file unless it is the file named in the activated configuration. The following procedure assumes editing the configured file.

1. Access the File Management configuration object: **System**, **File Management**.
2. On the File Management page, select Fraud Protection Table from the list.
3. Select a file, right-click, and click **Edit**.

4. Select a list type, and click **Edit**.

   The system displays the corresponding dialog for editing that type of list.

5. Do the following according to the list type:

Blacklist	• Type—Select the type of data to match from the drop-down list. • Match Value—Enter the value in the format that corresponds to the Type. Phone (exact match or prefix), Name (exact match), Source or destination IP or FQDN (exact match), or User agent. • Ingress Realm—Select the ingress realm to associate with the match value.
White List	• Type—Select the type of data to match from the drop-down list. • Match Value—Enter the value in the format that corresponds to the Type. Phone (exact match or prefix), Name (exact match), Source or destination IP or FQDN (exact match), or User agent. • Ingress Realm—Select the ingress realm to associate with the match value.
Rate Limit	• Type—Select the type of data to match from the drop-down list. • Match Value—Enter the value in the format that corresponds to the Type. Phone (exact match or prefix), Name (exact match), Source or destination IP or FQDN (exact match), or User agent. • Ingress Realm—Select the ingress realm to associate with the match value. • Calls Per Second—Enter the number of calls per second to allow for the entry. Range:0-65535. • Max Active calls—Enter the maximum number of active calls allowed for the entry. Range: 0-65535.
Call Redirect	• Type—Select the type of data to match from the drop-down list. • Match Value—Enter the value in the format that corresponds to the Type. Phone (exact match or prefix), Name (exact match), Source or destination IP or FQDN (exact match), or User agent. • Ingress Realm—Select the ingress realm to associate with the match value from the drop-down list. • Redirect Target—Enter one of the following: Session agent, session agent group name, Hostname, or IP address

6. Click **OK**.
7. (Optional) Click **Verify**.

   The system checks for valid entries in the configuration fields.

8. Click **OK**.
9. Click **Save**.

10. Click **OK**.
11. Click **Close**.
12. Go to **Configuration**, **System**, **System**, **Fraud Protection**, **Fraud Protection**, and Save and Activate the configuration.

    The system uses the edited file as the fraud protection source file.

Configure a Host Route

Use the Host Routes object to insert entries into the Oracle® Enterprise Session Border Controller routing table to steer management traffic to the correct network.

- 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.

1. Access the Host Route configuration object: **Configuration**, **System**, **Host Route**.
2. On the Host Route page, click **Add**.
3. On the Add host route page, do the following:

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 the configuration.

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.

- Confirm that the physical interface is configured. For more information, see "Physical Interface Configuration."
- Confirm that the system displays the Advanced 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.

1. Access the Network Interface configuration object: **Configuration**, **Objects**, **System**, **Network Interface**.
2. On the Network Interface page, click **Add**, and do the following:

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	• State—Select to enable front interface link detection and polling functionality on the E-SBC for this network-interface element. Default: enabled. • Heartbeat—Enter the time interval in seconds between heartbeats for the front interface gateway. Default: 0. Range: 0-65535. • Retry count—Enter the number of front interface gateway heartbeat retries before a gateway is considered unreachable. Default: 0. Range: 0- 65535. • Retry timeout—Enter the heartbeat retry timeout value in seconds. Default: 1. Range: 1-65535. • Health score—Enter the amount to subtract from the health score if the front interface gateway heartbeat expires. Range: 0 -100.
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.
Signaling MTU	Enter the Maximum Transmission Unit (MTU) size for signaling 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.
FTP Address	Enter the FTP address.
ICMP Address	Create a list of Internet Control Message Protocol (ICMP) addresses.
SSH Address	Enter the SSH IP address. The gateway address of this interface must be default gateway.

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

- 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 theOracle® Enterprise Session Border Controller (E-SBC).

Use the following procedure to configure synchronization of the NTP server with the E-SBC.

1. Access the NTP Config configuration object: **Configuration**, **System**, **NTP Config**.
2. On the NTP Config page, do the following:

Server	Enter the name or IP address of one or more NTP servers in your network that you want to use for the E-SBC.
Auth Servers	a. Click **Add**. b. IP Address—Enter the IPv4 address of the NTP server. c. ¶KeyID—Enter the Key ID. Range: 1-999999. d. Key—Enter the authentication key in bytes. Range: 1-28. e. Click **OK**.

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

Configure the Physical Interface

You must configure the physical interface of the Oracle® Enterprise Session Border Controller to connect to the network.

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.

1. Access the Phy Interface configuration object: **Configuration**, **System**, **Phy Interface**.
2. On the Phy Iinterface page, click **Add**, and do the following:

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. • Media • Control • Maintenance
Port	Enter the physical port number for the operation type. • Media—Front-panel interfaces only. Port: 0-3. • Control—Rear-panel interfaces only. Port 0-2. • Maintenance—Rear-panel interfaces only. Port 0-2.
Slot	Enter the physical slot number for the operation type. • Media—Front-panel interfaces only. Slot: 0 or 1. • Control—Rear-panel interfaces only. Slot: 0. • Maintenance—Rear-panel interfaces only. Slot: 0. • 0 is the motherboard (rear-panel interface), if the name begins with "wancom." • 0 is the left Phy media slot on the front of the chassis. • 1 is the right Phy media slot on the front of the chassis.
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.

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

- 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-SBCoperates 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 processes 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 the 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 twoE-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.

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.

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."

Configure Redundancy

Use the Redundancy Config element to configure the parameters to support redundancy for a High Availability (HA) pair of Oracle® Enterprise Session Border Controller (E-SBC) devices.

- Confirm that the physical interface for Control, the physical interface for Media, and the Network interface on the primaryE-SBC are configured for HA pairing.

Perform this procedure to configure redundancy for High Availability (HA) pairing of the primary E-SBC and the secondary E-SBC.

1. Access the Redundancy Config configuration object: **Configuration**, **System**, **Redundancy Config**.
2. On the Redundancy Config page, do the following:

State	Select to enable redundancy. Default: Enabled.
Log Level	Select a log level for redundancy processes from the drop-down list. Default: Info.

Becoming Standby Time	Enter the maximum time, in milliseconds, to wait complete synchronization. Deafult:180000. Range: 5-2147483674.
Becoming Active Time	Enter the maximum time, in milliseconds, to wait for incremental synchronization. Deafult:100. Range: 5-2147483674.
Media if Peer Check Time	Enter the media interface peer check timeout in milliseconds. Default: 0 = disabled. Range: 0-500.
Peer	Click **Add**, and do the following: a. Name—Enter the name of the primary 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 E-SBC. b. State—Select State to enable HA for the E-SBC. c. Type—Select Primary. If you select Unknown, the system cannot perform configuration checkpointing. d. Destination—Click **Add**, enter the destination address of the peer, select the network interface from the drop-down list, and click **OK**. e. Click **OK**. The system displays the Redundancy Config / Peer page. f. Name—Enter the name of the secondary 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 E-SBC. g. Type—Select Secondary. h. Destination—Click **Add**, enter the destination address of the peer, select the network interface from the drop-down list, and click **OK**.

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

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) Critical (2) Major (3) Minor (4) Warning (5) Notice (6) Info (7) Trace (8) Debug (9)	Emergency Critical Major Minor Warning
Critical	Emergency (1) Critical (2)	Emergency Critical
Major	Emergency (1) Critical (2) Major (3)	Emergency Critical Major
Minor	Emergency (1) Critical (2) Major (3) Minor (4)	Emergency Critical Major 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 and send alarms with different severity levels to individual trap receivers.

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

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.

1. Access the Trap Receiver configuration object: **Configuration**, **System**, **Trap Receiver**.
2. On the Trap Receiver page, click **Add**, and do the following:

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 for the severity level at which a trap is sent to the trap receiver. Default: Critical. Valid values: Critical | Major | Minor.
Community Name	Enter the SNMP community name to which this trap receiver belongs.

3. Click **OK**.
4. Save 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.

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

Use this procedure to group network devices and management stations, and to set the access rights for the community. If you want to narrow the scope of the this community, use the Network Addresses option to specify one or more subnets. See "Subnet Ranges for SNMP Community" for more information.

> **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.

1. Access the SNMP Community configuration object: **System**, **SNMP community**.
2. On the SNMP Community page, click **Add**, and do the following:

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 Addresses	Add one or more IPv4 addresses, or network address prefixes for subnets, that are valid within this SNMP community, and click **OK**.

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

Configure Subnet Ranges in SNMP Community

The SNMP system can dynamically originate SNMP GET requests from any host among a wide range of IP addresses. Due to the distributed nature of a typical network, the SNMP GET request may come from any IP address on an /8 netblock. It is not feasible to add all 16,777,216 possible IP addresses, one-by-one, to the SNMP Community configuration. The solution for the Oracle® Enterprise Session Border Controller (E-SBC) is to allow subnet ranges in the SNMP Community configuration. In this way, the (E-SBC) can accept SNMP GET requests from any host in the specified subnet.

You can configure the subnet range from the ACLI and the Web GUI by way of the `IP Addresses` parameter in the SNMP Community configuration object.

The IP Addresses parameter accepts subnet addresses in address prefix format (<Net_addr>/<Net_mask>), for example, 10.0.0.0/24. For an exact match, omit the number of bits, for example, 10.196.0.0. For multiple entries, use the parenthesis separated by comma format, for example, (172.16.0.0/16,192.168.4.0/24).

Configure System Config

The System Config configuration object contains attributes and sub-objects that you use to configure system-level operations for the Oracle® Enterprise Session Border Controller (E-SBC).

1. Access the System Config configuration object: **Configuration**, **System**, **System Config**.
2. In the System Config object, do the following:

Hostname	Set the primary hostname used to identify the system.

Description	(Optional) Type a description of this system for informational purposes.
Location	(Optional) Type the location of this system for informational purposes. For example, note the physical location of this chassis.
MIB System Contact	Set the name and contact information for the person you want named in MIB transactions as the system contact.
MIB System Name	Set the name of this E-SBC that you want displayed in MIB transactions.
MIB System Location	Set the physical location of thisE-SBC that you want displayed in MIB transactions. This parameter does not relate to the "Location" element in this configuration.
ACP TLS Profile	Set the TLS profile that you want to use.
SNMP Enabled	Enable or disable the SNMP system on this E-SBC. Default: enabled.
Enable SNMP Auth Traps	Enable or disable the E-SBC to send SNMP authentication traps. Default: Disabled.
Enable SNMP Syslog Notify	Enable or disable the E-SBC to send SNMP traps when the system generates an alarm message. Default: Disabled. Note: You must enable SNMP to support this function.
Enable SNMP Monitor Traps	Enable or disable the E-SBC to generate SNMP monitor traps with unique IDs. • Enabled—generate a unique trap ID for each syslog event. • Disabled—generate a single trap ID for all events, with different values in the description string.
Enable Env Monitor traps	Enable or disable the E-SBC to provide SNMP environment traps. Default: Disabled.
Enable MBLK Tracking	Default: Disabled.
Enable SNMP Syslog His Table Length	Set the number of entries that you want the syslog trap history table to contain. Default: 1. Valid values: 1-500.
SNMP System Log Level	Set the log severity level that triggers the E-SBC to send the syslog trap to an Network Management System (NMS). Default: Warning. Valid values: emergency | critical | major | minor | warning | notice | info | trace | debug | detail.
Syslog Servers	Access the **syslog server** configuration, and do the following: a. Address—Set the IP address of the Syslog server. b. Port—Set the Syslog server port. Default: 514.

<table>
<tr><td></td><td>c. Facility—Set a number to help identify the E-SBC as the source of a syslog message. Default: 4. RFC 3164 specifies the other valid values.</td></tr>
<tr><td>System Log Level</td><td>Set the log severity levels that trigger the E-SBC to write to the syslog. Default: Warning. Valid values: emergency | critical | major | minor | warning | notice | info | trace | debug | detail.</td></tr>
<tr><td>Process Log Level</td><td>Set the starting log severity level that you want all processes running on the E-SBC to use. Default: Notice. Valid values: emergency | critical | major | minor | warning | notice | info | trace | debug | detail.</td></tr>
<tr><td>Process Log IP Address</td><td>Set the IP address of the process log server. Default: 0.0.0.0 (Writes logs to the standard log file.)</td></tr>
<tr><td>Process Log Port</td><td>Set the port number for the process log server. Default: 0 (Writes logs to the standard log file.) Range: 0-65535.</td></tr>
<tr><td>Collect</td><td>Access the `collect` configuration, and do the following:
a. Sample Interval—Set the data collection sampling interval in minutes. Default: 5. Valid values: 1-120.
b. Push Interval—Set the data collection push interval in minutes. Default 15. Valid values: 1-120.
c. Boot State—Set **Enable** to enable the collection process. Default: Disabled.
d. Push Receiver—Configure one or more servers to receive push data.
i. Address—Set the IP address of the push receiver.
ii. User Name—Set the user name for pushing collect data.
iii. Password—Set the login password for pushing collect data.
iv. Data Store—Set the server directory in which to store the collected data.
v. Protocol—Set the protocol for pushing data to the server. Default: FTP. Valid values: FTP | SFTP.
e. Group settings—Configure the collector group parameters.
i. Group Name—Set a name for this group.
ii. Sample Interval—Set the group data collection sampling interval in minutes. Default: 5. Valid values: 1-120.
iii. Start Time—Set the date and time to start data collection. Format: yyyy-mm-dd:hh:mm:ss or yyyy-mm-dd-hh:mm:ss, where yy =year | mm= month | dd=day |</td></tr>
</table>

	hh=hour (24 hour clock) | mm=minutes | ss=seconds. Minimum format requirement: hh:mm. Default: Now. iv. End Time—Set the date and time to end data collection. Set the date and time to end data collection. Format: yyyy-mm-dd:hh:mm:ss or yyyy-mm-dd-hh:mm:ss, where yy =year | mm= month | dd=day | hh=hour (24 hour clock) | mm=minutes | ss=seconds. Minimum format requirement: hh:mm. Default: Never. v. Boot State—Select to enable this group from the collection process. Default: DIsabled.
Comm Monitor	Access the `comm-monitor` configuration, and do the following: a. State—Select to enable Comm Monitor. Default: Disabled. b. SBC Grp ID—Set the group ID as identified in the Palladion ME. Default: 0. Valid values: 0-999999999. c. TLS Profile—Select the TLS profile that you want to use for TLS connections. d. QoS Enable—Select to enable the system to send QoS information. Default: Enabled. e. Interim QoS Update—Select to enable incremental QoS sampling every 10 seconds for the duration of the call. Default: Disabled. f. Monitor Collector—Click **Add**, and do the following: i. Address—Set the IP destination address for data that the system pushes. ii. Port—Set the Palladion ME listening port. Default: 4739. Valid values: 1025-65535. iii. Network Interface—Set the local network interface to use for the connection. Format: <name>:<subport-ID>. Default: wancom0.0.
Default Gateway	Set the default egress gateway for traffic with no explicit destination.
Restart	Select enable to restart the system when a task suspends. Default: Enabled.
SSH Timeout	Set the number of seconds for the E-SBC to wait before disconnecting an SSH session. Default: 0. Range: 0-65535.
Console Timeout	Set the number of seconds for the E-SBC to wait before disconnecting a console session. Default: 0. Range: 0-65535.
Alarm Threshold	Access the **Alarm Threshold** configuration, and do the following: a. Type—Select a threshold from the drop-down list. b. Severity—Select a severity from the drop-down list.

	c. Value—Enter a threshold value, as a percentage. Range: 1-100. d. Click **OK**. e. (Optional) Repeat to add another alarm threshold profile.
Source Routing	Select to set the egress route for the HIP packet, based on the source IP address. Default: Disabled.
Debug Timeout	Set the number of seconds for the E-SBC to wait before timing out log levels for system processes set to "debug." Range: 0-65535.
PKO Rake Pkt	Set the packet rate for the ETC PKO rate limiter. Default: 0. Valid values: 0-32768.
PKO Rake Burst	Set the burst rate for the ETC PKO rate limiter. Default: 0. Valid values: 0-1024.
Default v6 Gateway	Set the default IPv6 gateway for egress traffic on this E-SBC with no explicit destination. Format: <ipv6>.
IPv6 Signaling MTU	Set the system-wide default MTU for IPv6 network interfaces. Default: 1500 bytes. Valid values: 1280-4096.
IPv4 Signaling MTU	Set the system-wide default MTU for IPv4 network interfaces. Default: 1500 bytes. Valid values: 576-4096.
SNMP Rate Limit	Set the SNMP rate limit in packets per second. Default: 0. Valid values: 0-9999.
Forwarding Cores	Set the number of CPU cores dedicated for forwarding frames. Default: 1. Valid values: 1-128.
DoS Cores	Set the number of CPU cores dedicated for Denial of Service protection. Default: 0. Valid values: 0-1.
Transcoding Cores	Set the number of CPU cores dedicated for transcoding media. Default: 0. Valid values: 0-128.

3. Save the configuration.

Time Division Multiplexing

Oracle® designed the Time Division Multiplexing (TDM) functionality 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 on the Oracle® Enterprise Session Border Controller (E-SBC) provides switchover for egress audio calls, when the primary SIP trunk becomes unavailable. You can use TDM with legacy PBXs and other TDM devices.

- Only the Acme Packet 1100 and the Acme Packet 3900 platforms support TDM, which requires the optional TDM card.
- TDM supports bidirectional calls as well as unidirectional calls.
- TDM operations require you to configure **TDM Config** and **TDM Profile**, as well as local policies for inbound and outbound traffic.

- The software upgrade procedure supports the TDM configuration.
- Options for the Acme Packet 1100 and the Acme Packet 3900 platforms include Calling-Line Identification Presentation (CLIP) and Connected-Line Identification Presentation (COLP).
- Options for the Acme Packet 1100 platform include the four-port Primary Rate Interface (PRI), the Euro ISDN Basic Rate Interface (BRI), and the Foreign Exchange Office-Foreign Exchange Subscriber (FXO-FXS) card.

Interface Requirements

PRI—Digium1TE133F single-port or Digium 1TE435BF four-port card.

BRI—Digium 1B433LF four-port card

FXS—Digium 1A8B04F eight-port card, green module (ports 1-4)

FXO—Diguim 1A8B04F eight-port card, red module (ports 5-8)

Notes

When you deploy either the Acme Packet 1100 or the Acme Packet 3900 in a High Availability (HA) pair, the active system cannot replicate calls between SIP and TDM to the standby system.

The Acme Packet 1100 does not support HA for the PRI, BRI, and FXO-FXS interfaces.

Time Division Multiplexing Configuration

To perform Time Division Multiplexing (TDM) operations on the Oracle® Enterprise Session Border Controller (E-SBC), you must enable TDM, specify the parameters for the interface in use, run the TDM configuration wizard, and create local policies for routing TDM traffic.

TDM configuration requires the following process:

1. Configure the **TDM Config** element and its corresponding sub-elements. The **TDM Config** element, located under **System**, contains the parameters that are common to all TDM configurations. The sub-elements contain the particular parameters for the interface that the system detects in use on the E-SBC. The system displays the sub-elements, as follows:
   - When the E-SBC detects either the Primary Rate Interface (PRI) or the Basic Rate Interface (BRI) interface, **TDM Config** displays the **TDM Profile** sub-element with the parameters that correspond to the interface. See "Primary Rate Interface Support" and "Basic Rate Interface Support."
   - When the E-SBC detects the Analog interface, **TDM Config** displays both the **FXO Profile** and the **FXS Profile** sub-elements with the parameters that correspond to the interface. See "Foreign Exchange Office-Foreign Exchange Subscriber Support."
2. Run the TDM configuration wizard to complete the configuration. The wizard creates the realm, SIP interface, steering pools, and other necessary configuration elements including the network interface and the phy-interface for SIP call routing. With SRTP enabled (default), the wizard also creates the **Media Sec Policy** object, enables the **Secured Network** attribute for the **SIP Interface** object, and configures the **Media Sec Policy** attribute for **Realm Config**. You can run the

wizard from either the Web GUI (**Set TDM Configuration**) or the ACLI (**Setup TDM**).
The E-SBC requires running the TDM configuration wizard only after the initial TDM configuration. The system does not require you to run the wizard after you make changes to the existing configuration.

> **Note:**
>
> When the Oracle Session Delivery Manager (SDM) manages the E-SBC, you configure TDM from the SDM and you do not need to run the TDM configuration wizard. See "Time Division Multiplexing (TDM) Settings on the Session Delivery Manager (SDM)" for the required settings.

3. Configure the local policy for routing traffic through the TDM interface. For unidirectional TDM call routing, the system requires a local policy only for the call direction that you want. For example, inbound-only or outbound-only. For bi-directional TDM call routing, create both inbound and outbound local policies. See "Local Policy Configuration for Time Division Multiplexing."

You can configure TDM from the following locations:

- ACLI—Use the **TDM Config**, **TDM Profile**, **FXO Profile**, and **FXS Profile** elements located under **System**.
- 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**, **TDM Profile**, **FXO Profile**, and **FXS Profile** elements located under **System**.
- Session Delivery Manager (SDM)—Launch the Web GUI from SDM and use the **TDM Config**, **TDM Profile**, **FXO Profile**, and **FXS Profile** elements located under **system**.

Incoming Call Pattern Guidelines

When you configure either the Primary Rate Interface (PRI) or Basic Rate Interface (BRI) interface for Time Division Multiplexing (TDM), you can set a list of extension numbers and match patterns for routing incoming calls. You can specify exact matches as well as patterns that route to a range of destinations.

For example, suppose that a company with 300 employees deploys the Oracle® Enterprise Session Border Controller (E-SBC) and connects to the PSTN network by way of an ISDN interface. The company allocates 300 extension numbers: numbers 7100 - 7399 for employee desk phones, and number 70 for the reception desk so that it is easy to remember.

The service provider assigns the prefix 49331200 to the company, so the reception desk PSTN number becomes 4933120070 and the employee numbers become 493312007100, 493312007101-493312007399.

The incoming pattern in this example will match either the reception desk number or one of the other extensions. When the match is successful, the received number is complete and the call setup can proceed. You can configure TDM to match the reception desk number as a whole: "4933120070," and to match any of the other extensions through a single pattern: "_493312007[1-3]XX". To put these rules together, set the **incoming-pattern** parameter to the following value: "4933120070|_493312007[1-3]XX".

In match patterns, separate single extension numbers with the vertical bar (|) character. Start a match pattern with the underscore (_) character before the first number of the pattern. Do not use the underscore with an exact match. Type the exact match, starting with the first number because an exact match does not use an extension pattern. Note the meaning of the following characters:

X matches any digit from 0-9

Z matches any digit from 1-9

N matches any digit from 2-9

[1237-9] matches any digit in the brackets (in this example, 1,2,3,7,8,9).

. wildcard, matches one or more characters

! wildcard, matches zero or more characters immediately

Configure the Single-Port Primary Rate Interface

The Acme Packet 1100 and the Acme Packet 3900 support the single-port ISDN Primary Rate Interface (PRI). To configure the PRI interface, you must set the parameters in **tdm-config** and **tdm-profile** under **system**. After you create the configuration, you must run either the **Set TDM Configuration** wizard from the Web GUI or the **setup tdm** command from the ACLI to complete the configuration.

- Confirm the presence of the single-port PRI interface on the Acme Packet 1100.

Note that because the single-port interface supports only one profile, you can set either **pri_cpe** (Customer Premises Equipment) or **pri_net** (Network) for signaling. The setting you choose depends on the setting at the other end of the connection. Set this configuration to the opposite of the other end. For example, when the setting at the other end is **pri_net**, set **pri_cpe** in this configuration.

> **Note:**
>
> The system requires the four-port interface to support profiles for both **pri_cpe** and **pri_net**.

1. Access the TDM Config configuration object: **Configuration**, **System**, **TDM Config**.
2. In **TDM Config**, set the following:

State	Set to **enable** to allow TDM operations.
Logging	Set to **enable** to allow logging.
Line Mode	Set either t1 (North America) or e1 (Europe).
Tone Zone	Set the TDM tone zone. Valid values: ae, ar, at, au, be, bg, br, ch, cn, cr, cz, de, dk, ee, es, fi, fr, gr, hu, il, in, it, jp, lt, mo, mx, my, nl, no, nz, pa, ph, pl, pt, ru, se, sq, th, tw, uk, us, us-old, ve, za. Default: us.

Calling Pres	Set the type of call ID presentation for this profile. Valid values: allowed_not_screened, allowed_failed_screen, allowed_passed_screen, prohib_not_screened, prohib_passed_screen, prohib_failed_screen, prohib, unavailable. Default: allowed_not_screened
Caller ID	Set the type of caller ID for CLIP and COLP that you want for the SIP header. Valid values: no, rpid (remote-party-ID), pai (p-asserted-ID) Default: No

3. In **tdm-profile**, set the following:

Name	Set the name for this TDM profile.
Signaling	Do one of the following: • Set pri_net when you want the E-SBC to represent the network side of the connection. • Set pri_cpe when you want the E-SBC to represent the Customer Premises Equipment side of the connection. Default.
Switch Type	Set a switch type for this configuration. Valid values: national, dms100, 4ess, 5ess, euroisdn, ni1, qsig.
B-channel	Set the B channel value according to the line mode that you specified for this configuration. • For t1: 1-23 • For e1: 1-15,17-31
D-channel	Set the D channel value according to the line mode that you specified for this configuration. • For t1: 24 • For e1: 16
Span Number	Set the span number to 1.
Route Group	Set the number of the associated route group to use this profile. Valid values: 0-63.
Line Build Out	Set the decibel (db) level per foot of line length. Valid values: 0-7. 0db up to 133 feet. Increment by 1db/133 feet after 133 feet. For example, 2db for 266-399 feet.
Framing Value	Set the framing value according to the line mode that you specified for this configuration. • For t1: esf

	• For e1: ccs
Coding Value	Set the coding value according to the line mode that you specified for this configuration. • For t1: b8zs • For e1: hdb3
CRC4 Checking	For e1, only. Enable or disable crc4-checking to match the setting of the PBX or service provider. Default: Disabled.
Time Source	Set the timing source. Valid values: 0-4. Default: 1. • 0—The interface provides its own timing. • 1—The interface receives timing from the remote end. • 2—The interface receives secondary timing from the remote end. • 3—The interface receives tertiary backup timing from the remote end. • 4—The interface receives quaternary backup timing from the remote end.
RX Gain	Set the decibel level that increases or decreases the TDM receiving channel volume. Valid values: 0.0-9.9. Default: 0.0.
TX Gain	Set the decibel level that increases or decreases the TDM transmitting channel volume. Valid values: 0.0-9.9. Default: 0.0.
Echo Cancellation	Enable or disable echo cancellation.
Overlap Dial	Set the overlap dialing function to either **no** or **incoming**, where incoming means yes.
Incoming Pattern	Set a list of extension numbers or match patterns. Separate single extension numbers with the vertical bar (|) character. A pattern starts with the underscore (_) character. In an extension pattern, note the meaning of the following characters: X matches any digit from 0-9 Z matches any digit from 1-9 N matches any digit from 2-9 [1237-9] matches any digit in the brackets (in this example, 1,2,3,7,8,9). . wildcard matches one or more characters ! wildcard matches zero or more characters immediately Syntax examples:

	Suppose the main number is 800-555-1234, one key extension is number 80, and the range of other extensions is from 8100-8399. • Match the exact number including the extension: 800555123480 • Match the extension in a range: _80055512348[1-3]XX • Match the exact number including the extension or match an extension in a range: 800555123480|_80055512348[1-3]XX

4. Click **OK**.
5. Click **OK**.
6. Save the configuration.

- Run the TDM configuration wizard.
- Configure the inbound and outbound TDM local policies.

Configure the Four-Port Primary Rate Interface

The Acme Packet 1100 and the Acme Packet 3900 support the four-port ISDN Primary Rate Interface (PRI) for carrying multiple Digital Signal 0 (DS0) voice and data transmissions between the network and an endpoint. To configure the PRI interface, you must set the parameters in **tdm-config** and **tdm-profile** under **system**. After you create the configuration, you must run either the **Set TDM Configuration** wizard from the Web GUI or the **setup tdm** command from the ACLI to complete the configuration.

- Confirm the presence of the four-port PRI.
- Plan the number of TDM profiles that you want. (You can add or delete profiles later, if your needs change.)

When the Oracle® Enterprise Session Border Controller (E-SBC) detects the PRI interface interface, it displays the corresponding configuration parameters. In the PRI configuration, the line mode that you specify dictates certain corresponding settings. You can set either t1 or e1 for line-mode, but note that each one requires certain uniquely compatible settings. For example, when you specify the t1 line mode you must specify esf for the framing-value. Do not specify an e1 value for the t1 line mode or a t1 value for the e1 line mode. The following procedure shows the specific t1 and e1 settings, where required.

1. Access the TDM Config configuration object: **Configuration**, **System**, **TDM Config**.
2. In **TDM Config**, set the following:

State	Set to **enable** to allow TDM operations.
Logging	Set to **enable** to allow logging.
Line Mode	Set either **t1** (North America) or **e1** (Europe).
Tone Zone	Set the TDM tone zone. Valid values: ae, ar, at, au, be, bg, br, ch, cn, cr, cz, de, dk, ee, es, fi, fr, gr, hu, il, in, it, jp, lt, mo, mx, my, nl, no, nz, pa, ph, pl, pt, ru, se, sq, th, tw, uk, us, us-old, ve, za. Default: us.

Calling Pres	Set the type of call ID presentation for this profile. Valid values: allowed_not_screened, allowed_failed_screen, allowed_passed_screen, prohib_not_screened, prohib_passed_screen, prohib_failed_screen, prohib, unavailable. Default: allowed_not_screened
Caller ID	Set the type of caller ID for CLIP and COLP for this profile. Valid values: no, rpid (remote-party-ID), pai (p-asserted-ID) Default: No

3. In **tdm-profile**, set the following:

Name	Set the name for this TDM profile.
Signaling	Do one of the following: • Set pri_net when you want the E-SBC to represent the network side of the connection. • Set pri_cpe when you want the E-SBC to represent the Customer Premises Equipment side of the connection. Default.
Switch Type	Set a switch type for this configuration. Valid values: national, dms100, 4ess, 5ess, euroisdn, ni1, qsig.
B-channel	Set the B channel value according to the line mode that you specified for this configuration. • For t1: 1-23 • For e1: 1-15,17-31
D-channel	Set the D channel value according to the line mode that you specified for this configuration. • For t1: 24 • For e1: 16
Span Number	Set the number of the spans affected by this profile. Valid values: Single numbers 1-4. Any combination of 1,2,3,4 comma separated.
Route Group	Set the number of the associated route group to use this profile. Valid values: 0-63.
Line Build Out	Set the decibel (db) level per foot of line length. Valid values: 0-7. 0db up to 133 feet. Increment by 1db/133 feet after 133 feet. For example, 2db for 266-399 feet.
Framing Value	Set the framing value according to the line mode that you specified for this configuration.

	- For t1: esf - For e1: ccs
Coding Value	Set the coding value according to the line mode that you specified for this configuration. - For t1: b8zs - For e1: hdb3
CRC4 Checking	For e1, only. Enable or disable crc4-checking to match the setting of the PBX or service provider. Default: Disabled.
Time Source	Set the timing source. Valid values: 0-4. Default: 1. - 0—The interface provides its own timing. - 1—The interface receives timing from the remote end. - 2—The interface receives secondary timing from the remote end. - 3—The interface receives tertiary backup timing from the remote end. - 4—The interface receives quaternary backup timing from the remote end.
RX Gain	Set the decibel level that increases or decreases the TDM receiving channel volume. Valid values: 0.0-9.9. Default: 0.0.
TX Gain	Set the decibel level that increases or decreases the TDM transmitting channel volume. Valid values: 0.0-9.9. Default: 0.0.
Echo Cancellation	Enable or disable echo cancellation.
Overlap Dial	Set the overlap dialing function to either **no** or **incoming**, where incoming means yes.
Incoming Pattern	Set a list of extension numbers or match patterns. Separate single extension numbers with the vertical bar (|) character. A pattern starts with the underscore (_) character. In an extension pattern, note the meaning of the following characters: X matches any digit from 0-9 Z matches any digit from 1-9 N matches any digit from 2-9 [1237-9] matches any digit in the brackets (in this example, 1,2,3,7,8,9). . wildcard matches one or more characters ! wildcard matches zero or more characters immediately

	Syntax examples: Suppose the main number is 800-555-1234, one key extension is number 80, and the range of other extensions is from 8100-8399. • Match the exact number including the extension: 800555123480 • Match the extension in a range: _80055512348[1-3]XX • Match the exact number including the extension or match an extension in a range: 800555123480|_80055512348[1-3]XX

4. Click **OK**.
5. Click **OK**.
6. Save the configuration.

- Run the TDM configuration wizard.
- Configure the inbound and outbound TDM local policies.

Configure the Basic Rate Interface

To configure the Basic Rate Interface (BRI) card, you must set the parameters in **TDM Config** and **TDM Profile** under **System**. Note that the system supports coexisting profiles for both **bri_cpe** (Customer Premises Equipment) and **bri_net** (Network). After you create the configuration, you must run either the **Set TDM Configuration** wizard from the Web GUI or the **Setup TDM** command from the ACLI to complete the configuration.

- Confirm the presence of the BRI interface on the Acme Packet 1100.
- Plan the number of TDM profiles that you want. (You can add or delete profiles later, if your needs change.)

When the Oracle® Enterprise Session Border Controller (E-SBC) detects the BRI interface, it displays the corresponding parameters and inserts certain values that you cannot change.

1. Access the TDM Config configuration object: **Configuration**, **System**, **TDM Config**.
2. In **TDM Config**, set the following:

State	Set to **ebable** to allow TDM operations.
Logging	Set to **ebable** to allow logging.
Line Mode	The system sets BRI.
Tone Zone	Set the tone zone. Valid values: ae, ar, at, au, be, bg, br, ch, cn, cr, cz, de, dk, ee, es, fi, fr, gr, hu, il, in, it, jp, lt, mo, mx, my, nl, no, nz, pa, ph, pl, pt, ru, se, sq, th, tw, uk, us, us-old, ve, za. Default: es.
Calling Pres	Set the type of call ID presentation for this profile.

	Valid values: allowed_not_screened, allowed_failed_screen, allowed_passed_screen, prohib_not_screened, prohib_passed_screen, prohib_failed_screen, prohib, unavailable. Default: allowed_not_screened
Caller ID	Set the type of caller ID for CLIP and COLP that you want for this profile. Valid values: no, rpid (remote-party-ID), pai (p-asserted-ID) Default: No

3. In **tdm-profile**, do the following:

name	Set the name for this TDM profile.
signaling	Do one of the following: • Set bri_net, if you want the E-SBC to represent the network side of the connection. • Set bri_cpe, if you want the E-SBC to represent the Customer Premises Equipment side of the connection. Default.
switch-type	Set the switch type for this configuration. Valid value: euroisdn
b-channel	Set 1-2 for the B channel value.
d-channel	Set 3 for the D channel value.
span-number	Set a span list for this profile. Separate multiple spans with commas. Default: 1.
route-group	Set the number of the associated route group to use this profile. Valid values: 0-63.
line-build-out	Set the decibel (db) level per foot of line length. Valid values: 0-7. 0db up to 133 feet. Increment by 1db/133 feet after 133 feet. For example, 2db for 266-399 feet.
framing-value	Set the framing value to **ccs**.
coding-value	Set the framing value to **hdb3**.
term-resistance	Enable or disable terminating resistance. Default: Disabled. • Enable terminating resistance when the E-SBC operates as the CPE side. For example, the E-SBC is a terminal endpoint connecting to a Telco through NT1. • Disable terminating resistance when the E-SBC operates as the NET side, and you encounter difficulties establishing a link to the terminal endpoint. For example, the E-SBC is emulating a Telco line.

time-source	Set the timing source. Valid values: 0-4. Default: 1. • 0—The card provides its own timing. • 1—The card receives timing from the remote end. • 2—The card receives secondary timing from the remote end. • 3—The card receives tertiary backup timing from the remote end. • 4—The card receives quaternary backup timing from the remote end.
rx-gain	Set the decibel level that increases or decreases the TDM receiving channel volume. Valid values: 0.0-9.9. Default: 0.0.
tx-gain	Set the decibel level that increases or decreases the TDM transmitting channel volume. Valid values: 0.0-9.9. Default: 0.0.
echo-cancellation	Enable or disable echo cancellation.
overlap-dial	Set the overlap dialing function to either **no** or **incoming**.
incoming-pattern	Set a list of extension numbers or match patterns. Separate single extension numbers with the vertical bar (|) character. A pattern starts with the underscore (_) character. In an extension pattern, note the meaning of the following characters: X matches any digit from 0-9 Z matches any digit from 1-9 N matches any digit from 2-9 [1237-9] matches any digit in the brackets (in this example, 1,2,3,7,8,9). . wildcard matches one or more characters ! wildcard matches zero or more characters immediately Syntax examples: Suppose the main number is 800-555-1234, one key extension is number 80, and the range of other extensions is from 8100-8399. • Match the exact number including the extension: 800555123480 • Match the extension in a range: _80055512348[1-3]XX • Match the exact number including the extension or match an extension in a range: 800555123480|_80055512348[1-3]XX

4. Click **OK**.
5. Click **OK**.

6. Save the configuration.

- Run the TDM configuration wizard.
- Configure the inbound and outbound TDM local policies.

Configure Inbound TDM Policy

Time Division Multiplexing (TDM) operations require policies for directing traffic to and from the TDM realm. In the following procedure, you specify the attributes for inbound TDM traffic.

- Configure TDM.

For the Policy priority parameter, the priority hierarchy from lowest to highest is none, normal, non-urgent, urgent, emergency. None means no priority. Each higher priority handles sessions at its level plus the sessions in the priorities above it. For example, non-urgent also handles sessions for urgent and emergency.

In the following procedure, the **to-address** and **from-address** can match the caller and called phone number or you can use any of the valid values noted. Note that you must use **tdmRealm**, which is case sensitive, for source-realm.

1. Access the Local Policy configuration object: **Configuration**, **Session Router**, **Local Policy**, **Add**.
2. On the Local policy page, click **Add**.
3. On the Add local policy page, set the following:

To address	Click **Add**, set the destination IP address, and click **OK**. Valid values: <ipv4> | <ipv6> | POTS Number | E.164 Number | hostname | wildcard.
Source realm	Click **Add**, set tdmRealm as the source realm, and click **OK**.
Description	Enter a description of the policy.
State	Select state to enable this policy.
Policy priority	Set the priority of the policy. Valid values: none | normal | urgent | non-urgent | emergency.
Policy attributes	Click **Add**, and do the following: • Next hop. Next hop. Set the next hop. Valid values: Only for the PRI and BRI interfaces—**next-hop tdm:span:<number>** Only for the Analog interface—**next-hop tdm:channel:<number>** **next-hop tdm:group:<number>** **next-hop tdm:<profileName>** • Realm. Set the realm for the next hop. • Action: Set the action to take. Valid values: none | redirect | replace-uri. Default: none. • Cost: Set the cost. Range: 0-999999999. Default: 0.

	• Click **OK**.

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

- If your deployment requires an outbound TDM local policy, see "Configure the Outbound TDM Policy."

Configure the Outbound TDM Policy

Time Division Multiplexing (TDM) operations require policies for directing traffic to and from the TDM realm. In the following procedure, you specify the attributes for outbound TDM traffic.

For the Policy priority parameter, the priority hierarchy from lowest to highest is none, normal, non-urgent, urgent, emergency. None means no priority. Each higher priority handles sessions at its level plus the sessions in the priorities above it. For example, non-urgent also handles sessions for urgent and emergency.

For the next-hop parameter in policy-attributes, use the name of the **tdm-profile** that you want associate with this policy.

1. Access the Local Policy configuration object: **Configuration**, **Session Router**, **Local Policy**, **Add**.
2. On the Add local policy page, set the following:

From address	Click **Add**, set the origin address, and click **OK**. Valid values: <ipv4> | <ipv6> | POTS Number | E.164 Number | hostname | wildcard.
To address	Click **Add**, set the destination IP address, and click **OK**. Valid values: <ipv4> | <ipv6> | POTS Number | E.164 Number | hostname | wildcard.
Source realm	Click **Add**, set the source realm, and click **OK**.
Description	Enter a description of the policy.
State	Select state to enable this policy.
Policy priority	Set the priority of the policy. Valid values: none | normal | non-urgent | urgent | emergency.
Policy attributes	Click **Add**, and do the following: • Next hop. Set the next hop. Valid values: Only for the PRI and BRI interfaces—**next-hop tdm:span:<number>** Only for the Analog interface—**next-hop tdm:channel:<number>** **next-hop tdm:group:<number>** **next-hop tdm:<profileName>** • Realm. Set the realm for the next hop.

	• Action: Set the action to take. Valid values: none | redirect | replace-uri. Default: none. • Cost: Set the cost. Range: 0-999999999. Default: 0. • Click **OK**.

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

- If your deployment requires an inbound TDM local policy, see "Configure the Inbound TDM Policy."

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.

- Confirm that a TDM configuration exists.
- Confirm that a policy exists for the realm.

To configure TDM for backup, add the tdm profile as a second attribute to the local policy.

1. Access the Local Policy configuration object: **Configuration**, **Session Router**, **Local Policy**, **Add**.
2. On the Add local policy page, under Policy attributes, click **Add**.
3. On the Add Local Policy / policy attribute page, select tdm:<profilename> from the Next Hop drop down list.
4. Click **OK**.
5. Save the configuration.
6. Save the configuration.

Add an FXO-FXS Profile

When your deployment requires Foreign Exchange Office-Foreign Exchange Subscriber (FXO-FXS) profiles, you can add up to four profiles each to support different attributes at different endpoints. For example, you might create profiles based on user name, department, location, and so on. You can create FXO profiles only, FSO profiles only, or both. To configure the FXO-FXS profiles, go to **TDM Config** under **System**, and create the profiles that you need.

- Requires the FXO-FXS interface

The configuration process includes configuring **TDM Config** and a corresponding **FXO Profile** or **FXS Profile**.

1. Access the TDM Config configuration object: **Configuration**, **System**, **TDM Config**.
2. In **TDM Config**, set the following:

State	Enable or disable the configuration. Default: Disabled.
Logging	Enable or disable logging. Default: Disabled.

Line Mode	The system sets Analog, when it detects the FXO-FXS interface.
Tone Zone	Set the tone zone value. Default: us. Valid values: ae, ar, at, au, be, bg, br, ch, cn, cr, cz, de, dk, ee, es, fi, fr, gr, hu, il, in, it, jp, lt, mo, mx, my, nl, no, nz, pa, ph, pl, pt, ru, se, sq, th, tw, uk, us, us-old, ve, za.
Caller ID	Set the type of caller ID for CLIP and COLP that you want for this profile. Default: No. Valid values: no, rpid (remote-party-ID), pai (p-asserted-ID).

3. For each **FXO Profile** and **FXS Profile** that you want to create, set the following:

Name	Enter a name for this profile.
Channels	Enter the channels that apply to this profile. You can enter any combination of the four that apply to the particular card. • FXS—1,2,3,4 • FXO—5,6,7,8
RX Gain	Set the TDM receive volume in decibels. Default: 0.0. Valid values: 0.0-9.9.
TX Gain	Set the TDM transmit volume in decibels. Default: 0.0. Valid values: 0.0-9.9.
Echo Cancellation	Enable or disable. Default: Enabled.
Fax Detect	For fax transcoding, set fax-detect to one of the following: • both (default) • incoming • outgoing • no
Route Group	Enter the number of the route-group for this profile. Range: 0-63.
Signaling	Set the signaling type. • For the fxo-profile—Valid values: fxs_ls, fxs_gs, fxs_ks. Default: fxs_ks. • For the fxs-profile—Valid values: fxo_ls, fxo_gs, fxo_ks. Default: fxo_ks.
Phone Number	Enter the caller's number. Required.
Full Name	Enter the caller's name.
CID Signaling	Set the Caller ID signaling type. Default: Bell. Valid values: Bell, v23, v23_ip, dtmf, of smdi.

4. Click **OK**.
5. Click **OK**

6. Save the configuration.

- Run the TDM Configuration Wizard.
- Configure the inbound and outbound TDM local policies.

Perform FXO Port Tuning

Tuning the Foreign Exchange Office (FXO) ports can help the echo canceller to work more efficiently. The **setup fxotune run** command creates the fxotune configuration file, which contains the script that fine tunes the Digium Asterisk Hardware Device Interface (DAHDI) FXO channels, and restarts the system. The tuning takes place during the restart. After FXO tuning, the system saves the result in a configuration file that is automatically applied after each subsequent restart. No additional user action is necessary.

- Configure one or more FXO profiles and activate the configuration.

Note that the following procedure requires a system restart, which can take longer than usual due to the tuning process.

1. From the command line, type **setup fxotune run**.
2. Restart the E-SBC.

Reset the FXO Port Tuning Defaults

If you ever want to reset the **setup fxotune run** boot parameter, use the **setup fxotune reset** command. The command resets the boot parameter for **setup fxotune run** to the default tuning values and removes the fxotune configuration file.

Note that the following procedure requires a system restart.

1. From the command line, type **setup fxotune reset**.
2. Restart the E-SBC.

Configure Fax Transcoding for the Acme Packet 1100

The system requires two codec policies, two local policies, and two realms to support fax transcoding.

- Before you begin, configure one realm that points to the Internet and one realm that points to the Time Division Multiplexing (TDM) interface.

For example, suppose you name the internet-facing codec policy "Remote" and you name the TDM-facing codec policy "TDM." Use the following guidelines for configuration:

Codec policies

- In the "Remote" **codec-policy**, set **allow-codecs** to **T.38 PCMU PCMA** and set **add-codecs-on-egress** to **T.38OFD**.
- In the "TDM" **codec-policy**, set **allow-codecs** to **PCMU PCMA** and set **add-codecs-on-egress** to **G711FB**.

Local Policies

- In the "Remote" **local-policy**, set **source-realm** to **remote**.
- In the "TDM" **local-policy**, set **source-realm** to **tdmRealm**.

Realms

- In the "Remote" **realm-config**, set **identifier** to **remote**, set the **codec-policy** type, and set **codec-manip-in-realm** to **enabled**.
- In the "TDM" **realm-config**, set **identifier** to **tdmRealm**, set the **codec-policy** type, and set **codec-manip-in-realm** to **enabled**.

Configure Overlap Dialing for Call Routing

When you enable overlap dialing and set the incoming match pattern, the Oracle® Enterprise Session Border Controller (E-SBC) can work with the information in the SETUP message to successfully route calls through the Primary Rate Interface (PRI) and Basic Rate Interface (BRI) in a Time Division Multiplexing (TDM) deployment.

- Plan the match patterns that you want for incoming calls. See "Incoming Call Patterns Guidelines" for rules and syntax.
- Confirm that the **TDM Profile** that you want to enable for overlap dialing exists.

> **Note:**
>
> If the **TDM Profile** that you want does not exist, you can set the **Overlap Dial** and **Incoming Pattern** parameters when you create the profile. The following procedure assumes the profile already exists.

Access **TDM Config** and use the **TDM Profile** sub-element to set the **OverlapDial** and **Incoming Pattern** parameters.

1. Access the TDM Config configuration object: **Configuration**, **System**, **TDM Config**.
2. Select the TDM profile that you want.
3. Set the **Overlap Dial** parameter to **Incoming**.
4. Set a list of extension numbers or match patterns for the **Incoming Pattern** parameter.

   Separate single extension numbers with the vertical bar (|) character. A pattern starts with the underscore (_) character. In an extension pattern, note the meaning of the following characters:

   X matches any digit from 0-9

   Z matches any digit from 1-9

   N matches any digit from 2-9

   [1237-9] matches any digit in the brackets (in this example, 1,2,3,7,8,9).

   . wildcard matches one or more characters

   ! wildcard matches zero or more characters immediately

   Syntax examples:
   Suppose the main number is 800-555-1234, one key extension is number 80, and the range of other extensions is from 8100-8399.

   - Match the exact number including the extension: 800555123480
   - Match the extension in a range: _80055512348[1-3]XX

- Match the exact number including the extension or match an extension in a range: 800555123480|_80055512348[1-3]XX

5. Save 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.

Configure a Web Server

Use the Web Server configuration object to enable the Web server and to specify how you want it to communicate with the Oracle® Enterprise Session Border Controller.

1. Access the Web Server configuration object: **Configuration**, **System**, **Web Server**.
2. On the Add Web Server Config page, do the following.

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.
HTTP Port	(Optional) Enter the port number that you want to use instead of the default port 80.
HTTPS State	Select to enable HTTPS connection to the Web server.
HTTPS Port	(Optional) Enter a the port number that you want to use instead of the default port 443.
HTTP Interface List	Select which HTTP interfaces to enable. Default: REST, GUI.
TLS Profile	Select a TLS profile to use for HTTPS from the drop down list.

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

4
Monitoring Tab Operations

The Monitoring tab displays tools to help you see the results of system and session data from the Oracle® Enterprise Session Border Controller. The Monitor and Trace link provides summary reports that include session data, ladder diagrams of call and media flows, and Quality of Service statistics. The Widgets link displays Widgets that you can use to monitor the system in a graphical or textual format.

Monitor and Trace

Monitor and Trace displays the results of filtered SIP session data from the Oracle® Enterprise Session Border Controller. Each summary page displays the results in a common log format for local viewing, which you can export as HTML and text files.

Monitor and Trace supports the following summary reports.

- Notable Events Summary
- Registrations Summary
- Sessions Summary
- Subscriptions Summary

Each summary provides sorting, searching, paging, and exporting functionality, as well as a link to a ladder diagram view where you can see a session summary, session details, and QoS statistics. You can choose which of the available columns that you want each summary to display.

The 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 re-boots

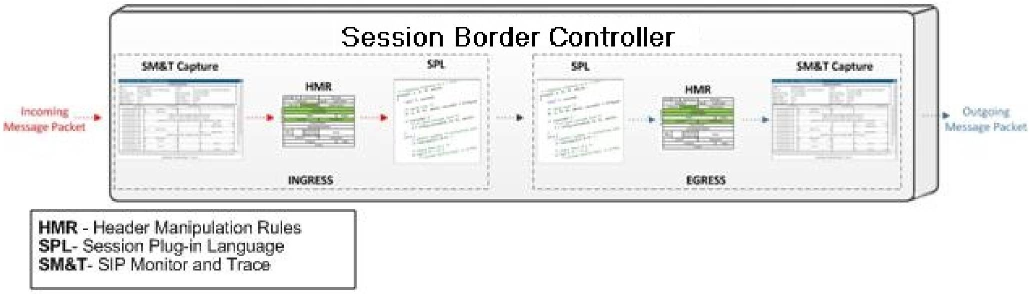
The system can perform live paging from Monitor and Trace tables.

> **Note:**
>
> Only one user at a time can view Monitor and Trace information. Monitor and Trace does not support multiple, simultaneous viewers.

SIP Monitor and Trace for Ingress and Egress Messages

SIP Monitor and Trace operations allow 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 process allows the E-SBC to capture SIP Monitor and Trace data for display in the Web GUI.

The E-SBC captures a SIP message in ingress, applies the Header Manipulation Rules (HMR) that you configured, and applies the Session Plug-in Language (SPL). When the E-SBC sends the message on egress, the E-SBC applies the SPL, applies the HMR, and sends out the captured SIP message.


Session Border Controller
Incoming Message Packet
SM&T Capture
HMR
SPL
INGRESS
SPL
HMR
SM&T Capture
EGRESS
Outgoing Message Packet
HMR - Header Manipulation Rules
SPL- Session Plug-in Language
SM&T- SIP Monitor and Trace

SIP Notable Events Summary

The SIP Notable Events Summary contains all logged sessions that have a notable event on the Oracle® Enterprise Session Border Controller (E-SBC) associated with the session. The columns that display on the Notable Events Summary page depend on the columns that you selected in the "Customizing the Page Display" procedure.

The following table describes the columns that Notable Events Summary page can display.

Start Time	Timestamp of the first SIP message in the call session.
State	Status of the call or media event session. Valid values: 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 through a protocol, name, location, and any other applicable characteristic, and 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.
Ingress Realm	Name of the inbound realm.
Egress Realm	Name of the outbound realm.
Notable Event	Indicates if a notable event has occurred on the call session. Valid values: 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 signaling; 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.
Ingress Src Port	Source port of the incoming call or media event.
Egress Dest Addr	Destination IP address of the outgoing call or media event.
Object ID	ID number of the object in a row. Use to aid troubleshooting.

SIP Registrations Summary

The SIP Registrations Summary displays a summary of all logged SIP registrations sessions on the Oracle® Enterprise Session Border Controller (E-SBC). The columns that display on the Registrations Summary page depend on the columns you selected in the "Customizing the Page Display" procedure.

The following table describes the columns available on the Registrations Summary page.

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.
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. Default: 3600 seconds.
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). Default: 3600 seconds.
Ingress Realm	Incoming realm name.
Egress Realm	Outgoing realm name.
Notable Event	Indicates a notable event that occurred on the call session. Valid value: 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 with the protocol, name, location, and any other applicable characteristic. The SBC only sends the URI in REQUEST headers.
Object ID	ID number of the object in a row. Use to aid troubleshooting.

SIP Sessions Summary

The SIP Sessions Summary is a SIP session summary of all logged call sessions on the Oracle® Enterprise Session Border Controller (E-SBC). When you enable Lightweight Directory Access Protocol (LDAP) on the Active Directory, LDAP session messages may also display. The columns that display on the Sessions Summary page depend on the columns that you specified in the "Customizing the Page Display" procedure.

The following table describes the columns on the SIP Session Summary page.

Start Time	Timestamp of the first SIP message in the call session.
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.
Ingress Realm	Name of the inbound realm.
Egress Realm	Name of the outbound realm.
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 signaling error, and so on. Session dialogue, capture media information, and termination signaling. 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.
Calling Pkts	
Called Pkts	
Calling R	
Called R	
Calling MOS	
Called MOS	

Ingress Src Port	Source port of the incoming call or media event.
Object ID	ID number of the object in a row. Use to aid troubleshooting.

SIP Subscriptions Summary

The SIP Subscriptions Report displays 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 depend on the columns you selected in the "Customizing the Page Display" procedure.

The following table describes the columns on Subscriptions Report page.

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.
Events	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-rtcpx—Event package that collects and reports the metrics that measure quality for RTP sessions.

Expires	The current setting for the expiration of a registration request. Default: 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 signaling; Any event flagged as a local rejection interesting event
Session ID	Identification assigned to the call session.
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.
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.
Object ID	ID number of the object in a row. Use to aid troubleshooting.

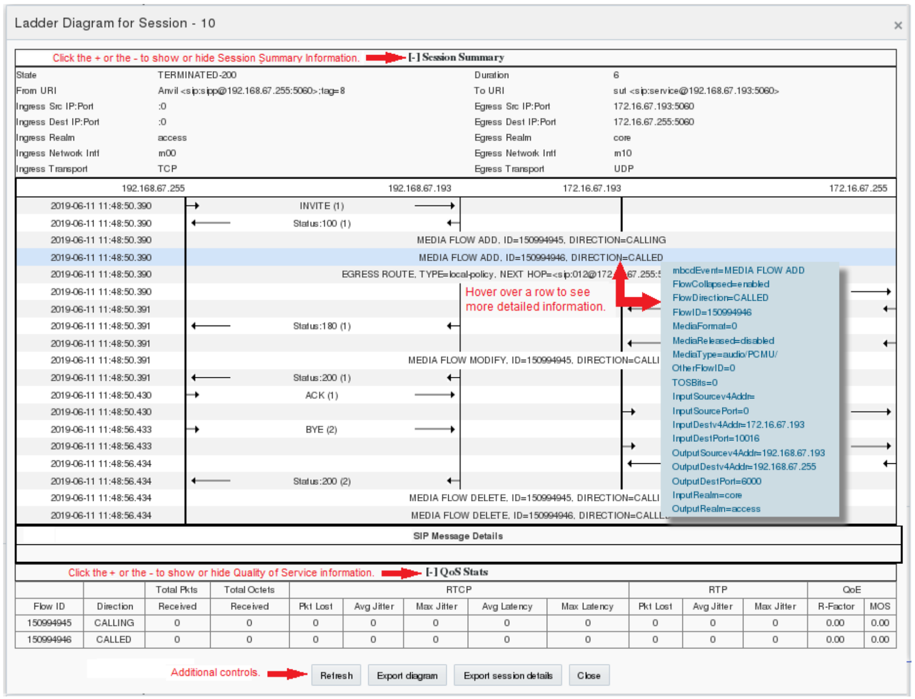
Ladder Diagrams and Information Display Controls

A ladder diagram is a graphical representation of the flow of call and media packets on ingress and egress routes through the Oracle® Enterprise Session Border Controller (E-SBC), which can help you with troubleshooting efforts. The Web GUI can display a ladder diagram for each of the summary reports available through Monitor and Trace.

To display a ladder diagram for a specific record in a Summary Report, select a record in the summary table and right-click. Click **Ladder diagram** on the pop-up menu. Each ladder diagram contains the following sections.

- Session Summary—Displays session data. Use the [+] and [-] controls to toggle between show and hide.
- Ladder Diagram—Displays SIP message and call flow information. Hover over a line in the ladder diagram to see more information for the highlighted flow.
- QoS Statistics—Displays Quality of Service (QoS) information. Use the [+] and [-] controls to toggle between show and hide.

The following illustration shows an example of an E-SBC ladder diagram, and how you can make it display more information.



Ladder Diagram for Session - 10

Click the + or the - to show or hide Session Summary Information.

[-] Session Summary

State	TERMINATED-200	Duration	6
From URI	Anvil <sip:sipp@192.168.67.255:5060>;tag=8	To URI	sut <sip:service@192.168.67.193:5060>
Ingress Src IP:Port	:0	Egress Src IP:Port	172.16.67.193:5060
Ingress Dest IP:Port	:0	Egress Dest IP:Port	172.16.67.255:5060
Ingress Realm	access	Egress Realm	core
Ingress Network Intf	m00	Egress Network Intf	m10
Ingress Transport	TCP	Egress Transport	UDP

```
                          192.168.67.255      192.168.67.193      172.16.67.193      172.16.67.255
2019-06-11 11:48:50.390   INVITE (1)
2019-06-11 11:48:50.390   Status:100 (1)
2019-06-11 11:48:50.390   MEDIA FLOW ADD, ID=150994945, DIRECTION=CALLING
2019-06-11 11:48:50.390   MEDIA FLOW ADD, ID=150994946, DIRECTION=CALLED
2019-06-11 11:48:50.390   EGRESS ROUTE, TYPE=local-policy, NEXT HOP=<sip:012@172 67.255:5
2019-06-11 11:48:50.390
2019-06-11 11:48:50.391
2019-06-11 11:48:50.391   Status:180 (1)
2019-06-11 11:48:50.391
2019-06-11 11:48:50.391   MEDIA FLOW MODIFY, ID=150994945, DIRECTION=CALLI
2019-06-11 11:48:50.391   Status:200 (1)
2019-06-11 11:48:50.430   ACK (1)
2019-06-11 11:48:50.430
2019-06-11 11:48:56.433   BYE (2)
2019-06-11 11:48:56.433
2019-06-11 11:48:56.434
2019-06-11 11:48:56.434   Status:200 (2)
2019-06-11 11:48:56.434   MEDIA FLOW DELETE, ID=150994945, DIRECTION=CALLI
2019-06-11 11:48:56.434   MEDIA FLOW DELETE, ID=150994946, DIRECTION=CALLL
```

Hover over a row to see more detailed information.

```
mbcdEvent=MEDIA FLOW ADD
FlowCollapsed=enabled
FlowDirection=CALLED
FlowID=150994946
MediaFormat=0
MediaReleased=disabled
MediaType=audio/PCMU/
OtherFlowID=0
TOSBits=0
InputSourcev4Addr=
InputSourcePort=0
InputDestv4Addr=172.16.67.193
InputDestPort=10016
OutputSourcev4Addr=192.168.67.193
OutputDestv4Addr=192.168.67.255
OutputDestPort=6000
InputRealm=core
OutputRealm=access
```

SIP Message Details

Click the + or the - to show or hide Quality of Service information.

[-] QoS Stats

		Total Pkts	Total Octets	RTCP					RTP			QoE	
Flow ID	Direction	Received	Received	Pkt Lost	Avg Jitter	Max Jitter	Avg Latency	Max Latency	Pkt Lost	Avg Jitter	Max Jitter	R-Factor	MOS
150994945	CALLING	0	0	0	0	0	0	0	0	0	0	0.00	0.00
150994946	CALLED	0	0	0	0	0	0	0	0	0	0	0.00	0.00

Additional controls.

The following table describes the additional controls on a Ladder Diagram page.

Refresh	Refreshes the data on the page.
Export Diagram	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.
Export Session Details	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.
Close	Closes the Ladder Diagram page.

Note:

The E-SBC captures SIP messages, applies the Header Manipulation Rules (HMR) that you configured on the E-SBC, and applies the Session Plug-in Language (SPL) to that message. When the E-SBC sends the message, it applies the SPL, the HMR, and sends the captured SIP message. When viewing the session detail on a Ladder Diagram, the HMR and SPL information may be present.

Display a Ladder Diagram

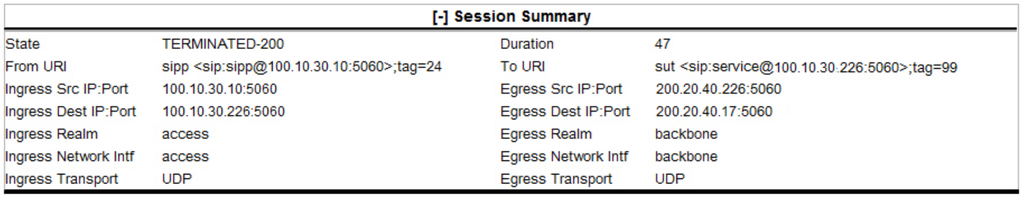
You can display a ladder diagram of call and media flow from any of the Monitor and Trace summary pages in the Web GUI. Each summary page displays a table, where each row represents one session. You can view a ladder diagram for each session with the following procedure.

1. Access a Summary: **Monitoring**, **Monitor and Trace**.
2. Under **Monitor and Trace**, select one of the following summaries:
   - Notable Events
   - Registrations
   - Sessions
   - Subscriptions
3. On the Summary page, select a row in the table and right-click.
4. On the pop-up menu, click **Ladder Diagram**.
5. (Optional)—On the ladder diagram, click the [+] to expand the Session Summary and QoS Stats sections.

Session Summary

To see a Session Summary, open a ladder diagram from a record in a Summary report and click the [+] control that precedes "Session Summary" at the top of the page. Monitor and Trace displays the session data and statistics.

The following screen capture shows a sample Session Summary page generated from a selected item on a ladder diagram.



[-] Session Summary

State	TERMINATED-200	Duration	47
From URI	sipp <sip:sipp@100.10.30.10:5060>;tag=24	To URI	sut <sip:service@100.10.30.226:5060>;tag=99
Ingress Src IP:Port	100.10.30.10:5060	Egress Src IP:Port	200.20.40.226:5060
Ingress Dest IP:Port	100.10.30.226:5060	Egress Dest IP:Port	200.20.40.17:5060
Ingress Realm	access	Egress Realm	backbone
Ingress Network Intf	access	Egress Network Intf	backbone
Ingress Transport	UDP	Egress Transport	UDP

The following table describes each field in the Session Summary report.

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).

Display a Session Summary

You can view data and statistics about a call or media session by displaying the Session Summary from a ladder diagram.

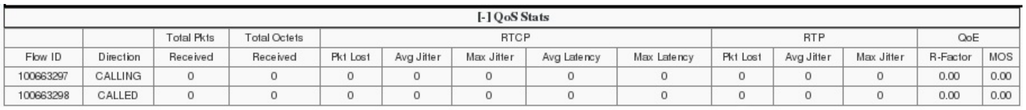
1. Access a Summary: **Monitoring**, **Monitor and Trace**.

2. Under **Monitor and Trace**, select one of the following summaries:
   - Notable Events
   - Registrations
   - Sessions
   - Subscriptions
3. On the Summary page, select a row in the table and right-click.
4. On the pop-up menu, click Ladder Diagram.
5. (Optional)—On the ladder diagram, click the [+] to expand the Session Summary section.

QoS Statistics

The Quality of Service (QoS) Stats section of the Session Summary displays information about the quality of the service for a selected call session or media event. To see the QoS statistics, open a ladder diagram from a record in a Summary report and click the [+] control that precedes "QoS Statistics" at the bottom of the page.

Expand QoS Stats section with the [+} control.



[-] QoS Stats

		Total Pkts	Total Octets	RTCP					RTP			QoE	
Flow ID	Direction	Received	Received	Pkt Lost	Avg Jitter	Max Jitter	Avg Latency	Max Latency	Pkt Lost	Avg Jitter	Max Jitter	R-Factor	MOS
100663297	CALLING	0	0	0	0	0	0	0	0	0	0	0.00	0.00
100663298	CALLED	0	0	0	0	0	0	0	0	0	0	0.00	0.00

The following table describes each column in the QoS Stats report.

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. 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.
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, called jitter, over time of the RTCP packet latency across a network. A network with constant latency has no 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 inter-arrival times for successive packets.

Max Jitter	Maximum measure of the variability, called jitter, over time of the RTCP packet latency across a network. A network with constant latency has no variation 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, called jitter, over time of the RTP packet latency across a network. A network with constant latency has no 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 inter-arrival times for successive packets.
Max Jitter	Maximum measure of the variability, called jitter, over the time of the RTP packet latency across a network. A network with constant latency has no jitter.
QoE	Quality of Experience—measurement used to determine how well the network is satisfying the end user's requirements.
R-Factor	Rating Factor—An average Quality of Service (QoS) factor observed during the active window period. QoS 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, which is expressed as an R factor.
MOS	Mean Opinion Score (MOS) score—MOS is a measure of voice quality. MOS provides a numerical indication of the perceived quality of the media received after being transmitted and eventually compressed using Codecs.

Display QoS Statistics

When you want to view QoS statistics for a call or media flow session, you can do so from a ladder diagram in **Monitor and Trace**.

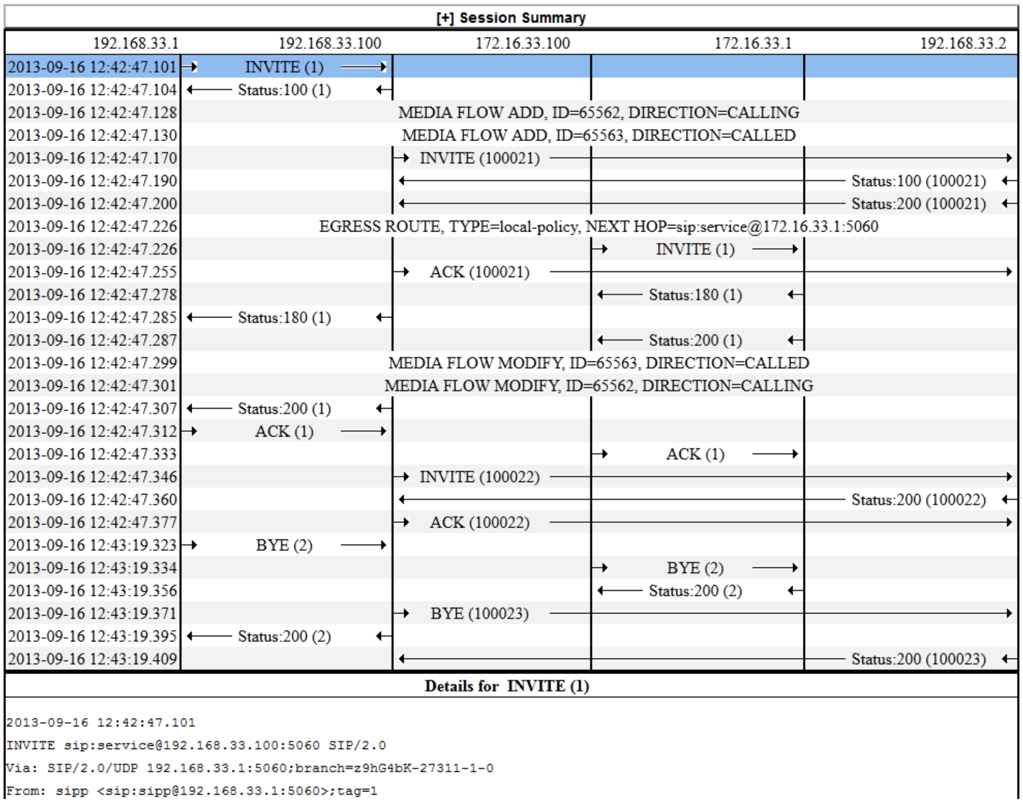
1. Access a Summary: **Monitoring**, **Monitor and Trace**.
2. Under **Monitor and Trace**, select one of the following summaries:
   - Notable Events
   - Registrations
   - Sessions

- Subscriptions

3. On the Summary page, select a row in the table and right-click.
4. On the pop-up menu, click Ladder Diagram.
5. On the ladder diagram, click the [+] to expand the **QoS Stats** section.

SIPREC Call Data Example

The following example shows SIP Monitor and Trace output for a call with media forwarded by way of SIPREC.



[+] Session Summary

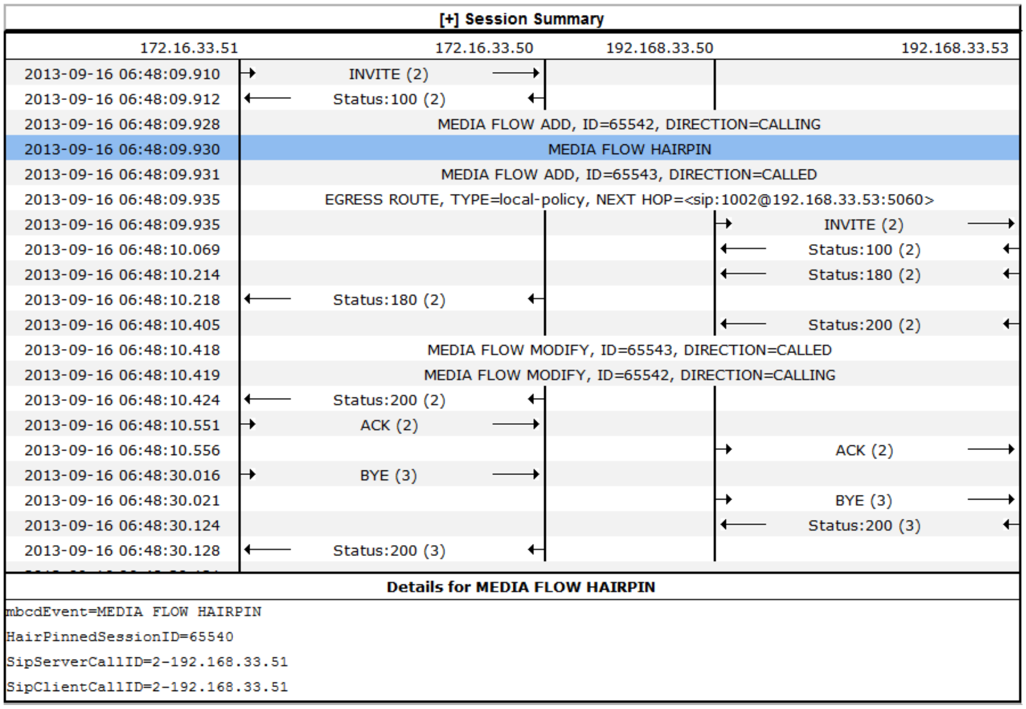
	192.168.33.1	192.168.33.100	172.16.33.100	172.16.33.1	192.168.33.2
2013-09-16 12:42:47.101	INVITE (1) →				
2013-09-16 12:42:47.104	← Status:100 (1)				
2013-09-16 12:42:47.128	MEDIA FLOW ADD, ID=65562, DIRECTION=CALLING				
2013-09-16 12:42:47.130	MEDIA FLOW ADD, ID=65563, DIRECTION=CALLED				
2013-09-16 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 Example

The following example shows SIP Monitor and Trace output for a hairpin call. The Media Flow Hairpin indication is highlighted.



[+] Session Summary

```
                          172.16.33.51        172.16.33.50      192.168.33.50          192.168.33.53
2013-09-16 06:48:09.910   INVITE (2) →
2013-09-16 06:48:09.912   ← Status:100 (2)
2013-09-16 06:48:09.928   MEDIA FLOW ADD, ID=65542, DIRECTION=CALLING
2013-09-16 06:48:09.930   MEDIA FLOW HAIRPIN
2013-09-16 06:48:09.931   MEDIA FLOW ADD, ID=65543, DIRECTION=CALLED
2013-09-16 06:48:09.935   EGRESS ROUTE, TYPE=local-policy, NEXT HOP=<sip:1002@192.168.33.53:5060>
2013-09-16 06:48:09.935                                                 INVITE (2) →
2013-09-16 06:48:10.069                                                 ← Status:100 (2)
2013-09-16 06:48:10.214                                                 ← Status:180 (2)
2013-09-16 06:48:10.218   ← Status:180 (2)
2013-09-16 06:48:10.405                                                 ← Status:200 (2)
2013-09-16 06:48:10.418   MEDIA FLOW MODIFY, ID=65543, DIRECTION=CALLED
2013-09-16 06:48:10.419   MEDIA FLOW MODIFY, ID=65542, DIRECTION=CALLING
2013-09-16 06:48:10.424   ← Status:200 (2)
2013-09-16 06:48:10.551   ACK (2) →
2013-09-16 06:48:10.556                                                 ACK (2) →
2013-09-16 06:48:30.016   BYE (3) →
2013-09-16 06:48:30.021                                                 BYE (3) →
2013-09-16 06:48:30.124                                                 ← Status:200 (3)
2013-09-16 06:48:30.128   ← Status:200 (3)
```

Details for MEDIA FLOW HAIRPIN

```
mbcdEvent=MEDIA FLOW HAIRPIN
HairPinnedSessionID=65540
SipServerCallID=2-192.168.33.51
SipClientCallID=2-192.168.33.51
```

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.

- Configure any filters that you want, if you don't want to monitor all SIP traffic. See "Filter Configuration."

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.

1. Access SIP Monitoring: **Configuration**, **Session Router**, **SIP Monitoring**.
2. On the SIP Monitoring page, do the following.

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.
Interesting Events	Create a global list of interesting events to monitor. Click **Add**, and do the following: • Type—Select an event type from the drop-down list. Default: None. Valid values: Short Session, Local Rejection.

	• Trigger Threshold—Set the number of events required to occur in within the trigger window before the system starts monitoring. Default: 0. Range: 0-999999999. • Trigger Timeout—Set the amount of time, in seconds, that the monitoring persists. Default: 0. Range: 0-999999999, • Click **OK**. The system displays the SIP monitoring page.

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

- View the SIP Session Summary and SIP Notable Event Summary on the Monitoring tab.

Search for a Report 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.

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 **Smith**field<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. On any reports page, click **Search** and do the following in the Search Filter dialog.

Global Search—Search all parameters in all records.	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.
From URI—Search on the From-URI header.	Enter the URI formatted string that contains a protocol, name, location, or any other applicable characteristic, that is sent by the E-SBC in the FROM header. Valid values are alpha-numeric characters. For example, sip:service@172.16.34.226:5060.
Request URI—Search on the Request-URI header.	Enter the URI formatted string that contains a protocol, name, location, or any other applicable characteristic, that is sent by the E-SBC in the REQUEST header. Valid values are alpha-numeric characters. For example, sip:service@172.16.34.226:5060.

To URI—Search on the To-URI header.	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.
Start Date—Search from messages that start at the specified date and time.	• 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). For example, 2012-04-15 would search for all records ending 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.
End Date—Search from messages that end at the specified date and time.	• Enter an end date to search on in the first text box in the format YYYY-MM-DD (where Y =year, M=month, and D=day). For example, 2012-04-15 would search for all records starting on April 15, 2012. Valid values are numeric characters only. • Enter an end 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 ending at 1:30 and 45 seconds. Valid value are numeric characters only.
Session ID—Search on the monitored SIP session ID, as shown in the Summary table.	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.
In Call ID—Search on the SIP call ID of the initial received request.	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.
Out Call ID—Search on the SIP call ID of the first routed request.	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.
State (with result code)—Search on the state of the call, as shown in the Summary table.	Enter the status of the call session with the result code for which you want to search. Result codes can range from 1xx to 5xx. For example, terminated-200, or failed-400. Case-sensitive. Valid values include: • INITIAL—<result code> • EARLY—<result code> • ESTABLISHED—<result code> • TERMINATED—<result code>

	- FAILED—<result code>
Notable Event—Search on a notable event type that you select from the drop-down list.	Select the notable event for which you want to search. Valid values include: - any event—search displays any notable event that was stored in memory. - hort 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.
In Realm—Search the realm from which the initial request was received.	Enter the name of the realm for which the incoming call belongs. Valid values are alpha-numeric characters. For example, access.
Out realm—Search the realm to which the first routed request was sent.	Enter the name of the realm for which the outgoing call belongs. Valid values are alpha-numeric characters. For example, backbone.
Destination Agent—Search on the name of the session agent from which the initial request was received.	Enter the name of the session agent (SA) on the incoming call session. Valid values are alpha-numeric characters. For example, SA1.
Destination Session Agent—Search on the realm to which the first routed request was sent.	Enter the name of the session agent (SA) on the outgoing call session. Valid values are alpha-numeric characters. For example, SA2.
Ingress Destination Address—Search on the IP address from which the initial request was received.	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.
Egress Destination Address—Search on the IP address to which the initial request was sent.	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.

In Network Interface—Search on the IP address on which the initialƒ request was received.	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.
Out Network Interface—Search on the IP address that was the source for the routed request.	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.

2. Click **Search**.

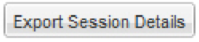
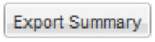
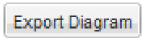
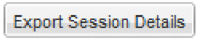
Exporting Information to a Text File

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 list identifies the buttons to use to export specific information from Monitor and Trace. All the export buttons in the GUI export to text files.

 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. Note: This button exports ALL call session summary records or the records that matched a search criteria to the file.
 Export 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.
 Export Session Details	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 Trace report to a text file:

> **Note:**
>
> The GUI exports Ladder Diagrams as HTML files.

1. Access Monitor and Trace: **Monitoring**, **Monitor and Trace**.
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, right-click, 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.

Widgets

For each **show** command that you can use from the ACLI to see System, Media, and Signaling data about the Oracle® Enterprise Session Border Controller (E-SBC), the system provides a corresponding Widget on the Web GUI. Widgets display the data in a graphical or textual format.

A Widget can display a table, text, a pie graph, or a line graph depending on the type of data and the purpose of the display. For example, the SIP Realms All widget displays an actionable table and the Recording widget displays static text. You can access the list of widgets from either the navigation pane on the Monitoring tab or from the Home page by clicking Add Widget.

Most of the Widgets automatically display any available data when you click the name of the Widget, but some Widgets require further input. Such Widgets include a Settings button in their display that launches a parameters dialog were you specify the data to display. For example, the Realm Specifics Widget requires you to set the name of the realm and the auto refresh interval.

> **Note:**
>
> You must set up a valid SIP configuration before the E-SBC can display any SIP data in a Widget, including the default Widgets.

The following tables list and describe the Widgets in the same order as they are displayed on the Web GUI.

System

The following table lists all of the System widgets in the left column. The middle column displays the corresponding ACLI **show** command, when there is one. The right column describes the data that the Widget displays.

Widget	Show Command	Description
Accounting	show accounting	Displays a summary of statistics for configured external accounting servers.
ACL	show acl all	Displays cumulative and per-interface statistics on ACL traffic and drops, displaying Recent, Total, and PerMax counts. The display also separates traffic from trusted from untrusted sites.
Alarms	show alarms	Displays existing alarms and allows you to clear them.
Authentication RADIUS	show radius all	Displays the status of established RADIUS accounting connections.
Authentication TACACS	show tacacs stats	Displays statistics related to communications between the E-SBC and configured TACACS servers .
Communications Monitor Errors	show comm-monitor errors	Displays Communications Monitor aggregate error statistics information.
Communications Monitor Internal	show comm-monitor internal	Displays Communications Monitor aggregate internal statistics information.
Communications Monitor Stats	show comm-monitor stats	Displays statistics related to connections between the E-SBC Communications Monitor probe and any configured Communications Monitor servers.
Editing Configuration	show configuration	Displays the current editing configuration.
Editing Configuration Short	show configuration short	Displays only the parameters that you modified in the editing configuration.
Configuration Inventory	show configuration inventory	Displays the editing and running configuration inventory of all configured elements.
Running Configuration	show running-config	Displays the current running configuration.
Running Configuration Short	show running-config short	Displays only the parameters that you modified in the running configuration.
Configuration Version	show version	Displays the configuration version number table.
Highest Task CPU Usage	No show command	Displays a line graph with 5-10 tasks with the highest CPU usage in percent, during a specific period of time.

Widget	Show Command	Description
Highest Task CPU Usage	No show command	Displays a table with 5-10 tasks with the highest CPU usage in percent, during a specific period of time.
Current Disk Usage Pie Graph	No show command	Displays the current disk usage in a pie graph.
Current Disk Usage Table	No show command	Displays the current disk usage in a table.
Features	show features	Displays the features that are currently enabled, based on added licenses.
Interfaces	show interfaces	Displays all of the information concerning the rear interfaces.
Interfaces Brief	show interfaces brief	Displays key running statistics about the rear interfaces in one graphic.
Interface Mapping	show interface mapping	Displays the configured physical interfaces with their MAC addresses and label.
Virtual Interfaces	show virtual interfaces	Displays the virtual interfaces for signaling services.
Wancom	show Wancom	Displays negotiated duplex mode and speed for all system control interfaces.
ARP Info	show arp info	Displays the current Internet-to-Ethernet address mappings in the ARP table.
ARP Statistics	show arp statistics	Displays ARP statistics.
ARP Summary	show arp	Displays the current Internet-to-Ethernet address mappings in the ARP table.
IP Connections	show ip connections	Displays all TCP and UDP connections.
Neighbor Table	show neighbor table	Displays the IPv6 neighbor table and validates that an entry for the link local address exists and that the gateway uses that MAC address.
Routes	show routes	Displays the current system routing table.
IP Summary	show ip	Displays IP statistics.
IP TCP	show ip tcp	Displays all TCP statistics.
IP UDP	show ip udp	Displays all UDP statistics.
Licenses	license	Displays existing licenses and allows you to add or delete them.
Current Memory Usage	No show command	Displays the current percentage of free and allocated memory in a pie graph.

Widget	Show Command	Description
Current Memory Usage	No show command	Displays the current percentage of free and allocated memory in a table.
Historical Memory Usage	No show command	Displays a line graph of the kilobytes of free and allocated memory over a period of time.
Historical Memory Usage	No show command	Displays a table of the kilobytes of free and allocated memory over a period of time.
Memory Summary	show memory	Displays statistic related to the memory.
Platform All	show platform all	Displays full platform information.
Platform CPU load	show platform cpu-load	Displays current CPU load.
Platform Errors	show platform errors	Displays service pipe write errors.
Platform Limits	show platform limits	Displays platform related limits.
PROM Info	show prom info all	Displays all available PROM information.
Temperature	show temperature	Displays the temperature in Celsius for all components with temperature sensors.
Processes	show processes	Displays statistics for all active processes.
SNMP Community Table	show snmp-community-table	Displays all information for configured SNMP communities including requests and responses for each community.
Trap Receiver	show trap-receiver	Displays trap receiver information for each configured SNMP community.
SPL Memory	show spl memory	Displays SPL memory for each task SPL engine.
SPL Options	show spl-options	Displays information on all SPL options.
SPL Statistics	show spl statistics	Displays statistics for all tasks.
SPL Version	show spl	Displays the version of the SPL engine.
System Health	show health	Displays the system health table for HA pairs.
TDM Channels	show tdm channels	Displays the TDM b and d channel configurations.
TDM Dialplan	show tdm dialplan	Displays the TDM dial plan configuration.
TDM Spans	show tdm spans	Displays the TDM spans configuration.
TDM Status	show tdm status	Displays the status of TDM operations.
Clock	show clock	Displays the current date and time.

Widget	Show Command	Description
NTP Server	show ntp server	Displays information about the quality of the time used for offset and the delay measurement maximum error bounds.
NTP Status	show ntp status	Displays information about configuration status, NTP daemon synchronization, NTP synchronization in process, and if NTP is not responding.
Time Zone	show timezone	Displays the time zone.
Clock UTC	show clock utc	Displays the current date and time in Coordinated Universal Time (UTC).
Uptime	show uptime	Displays information about the length of time the system has been running in days, hours, and seconds. Also displays the current date and time information.
User Management	show users	Displays a table that lists all users currently logged on to the system.
Version Boot	show version boot	Displays the boot version.
Version CPU	show version cpu	Displays the CPU version.
Version Hardware	show version hardware	Displays the hardware version.
Version Image	show version image	Displays the image version.
Version Summary	show version	Displays the Operating System version information, including the OS version number, the manufacturing date of the current version, and other details.

Media

The following table lists all of the Media widgets in the left column. The middle column displays the corresponding ACLI **show** command. The right column describes the data that the Widget displays.

Widget	Show Command	Description
Media Classify	show media classify	Displays network processor statistics.
Media Host Stats	show media host-stats	Displays statistics for the host processor, including the number and types of packets received at a specific port.
MBCD Acls	show mbcd acls	Displays Middlebox Control Daemon (MBCD) Access Control statistics.

Widget	Show Command	Description
MBCD All	show mbcd all	Displays related to many of the show MBCD sub-commands. The widget shows only those MBCD messages that show statistics.
MBCD Errors	show mbcd errors	Displays MBCD error statistics.
MBCD Realms	show mbcd realms	Displays statistics of all MBCD realms.
MBCD Statistics	show mbcd statistics	Displays information related to media flows established by the MBCD task.
NAT By Index	show nat by-index	Displays the specified range of entries in the NAT table, with a maximum of 5024 entries. The default range is 1-200. The range corresponds to the line numbers in the table, not to the number of the entry.
NAT in Tabular	show nat in-tabular	Displays a specified range of entries in the NAT table.
Realm Specifics	realm-specifics	Displays all realm-specific configuration based on the specified realm-id.
Realm Summary	show realm	Displays the realm summary statistics.
Xcode Codecs	show xcode codecs	Displays counts of codec pairs and ptime transrating in use.
Xcode Load	show xcode load	Displays the transcoding resources in use.
Xcode Xlist	show xcode xlist	Displays the XCode Xlist.

Signaling

The following table lists all of the Signaling widgets in the left column. The middle column displays the corresponding ACLI **show** command. The right column describes the data that the Widget displays.

Widget	Show Command	Description
DNS	show dns	Displays statistics for the DNS configuration.
ENUM	show enum	Displays ENUM statistics.
Fraud Protection All	show fraud-protection all	Displays all Fraud Protection entries.
Fraud Protection Black list	show fraud-protection blacklist	Displays the Fraud Protection blacklist entries.
Fraud Protection Rate limit	show fraud-protection rate limit	Displays the Fraud Protection rate limit list entries.
Fraud Protection Re-direct	show fraud-protection redirect	Displays the Fraud Protection redirect list entries.
Fraud Protection White List	show fraud-protection white list	Displays the Fraud Protection white list entries.

Widget	Show Command	Description
Fraud Protection All Matches	show fraud-protection all matches-only	Displays the Fraud Protection match-only entries.
Fraud Protection Blacklist Matches	show fraud-protection blacklist matches-only	Displays the Fraud Protection blacklist match-only entries.
Fraud Protection Rate Limit Matches	show fraud-protection rate limit matches-only	Displays the Fraud Protection rate limit match-only entries.
Fraud Protection Redirect Matches	show fraud-protection redirect matches-only	Displays the Fraud Protection redirect match-only entries.
Fraud Protection White List Matches	show fraud-protection white list matches-only	Displays the Fraud Protection white list match-only entries.
Fraud Protection Summary	show fraud-protection stats	Displays the Fraud Protection summary.
H323d	show h323d	Displays H323 statistics.
LDAP	show ldap	Displays LDAP statistics.
LRT	show lrt	Displays the Local Routing Table statistics.
Recording	show rec	Displays SIP REC statistics for the Recording Agent.
Registration by Realm	show registration sipd by realm	Displays calls that registered through a specified ingress realm for which you want to view cache information.
Registration H323 d	show registration h323d	Displays H323d registrations.
Registration SIP	show registration SIP	Displays SIP registrations.
Registration Statistics	show registration statistics	Displays a table of counters showing the total and periodic number of registrations by protocol.
Sessions	show sessions	Displays the session capacity for license and session use.
Agent Details	show sipd agents	Displays statistics related to defined DIP session agents.
Agent Groups	show sipd groups	Displays cumulative information for all session agent groups.
Agent Individual	show sipd agents <agent name>	Displays statistics related to the specified SIP session agent.
Client Trans	show sipd client	Displays statistics for SIP client events when the SBC is acting as a SIP client in the B2BUA role.
SIP Codecs	show sipd codecs	Displays codec usage for a realm.
SIP Errors	show sipd errors	Displays statistics for SIP media event errors.
Interface Individual	show sipd interface	Displays SIP interface statistics for the specified realm.
Interface Summary	show sipd interface	Displays all SIP interface statistics.

Widget	Show Command	Description
Method Ack	show sipd ack	Displays all SIP ACK method statistics.
Method Bye	show sipd bye	Displays the SIP BYE method statistics.
Method Cancel	show sipd cancel	Displays all SIP CANCEL method statistics.
Method Info	show sipd info	Displays the SIP INFO method statistics.
Method Invite	show sipd invite	Displays the SIP INVITE method statistics.
Method Message	show sipd message	Displays the SIP MESSAGE statistics.
Method Notify	show sipd notify	Displays the SIP NOTIFY statistics.
Method Options	show sipd options	Displays the SIP OPTIONS statistics.
Method Prack	show sipd prack	Displays the SIP PRACK method statistics.
Method Publish	show sipd publish	Displays the SIP PUBLISH method statistics.
Method Refer	show sipd refer	Displays the SIP REFER method statistics.
Method Register	show sipd register	Displays the SIP REGISTER method statistics.
Method Subscribe	show sipd SUBSCRIBE	Displays the SIP SUBSCRIBE method statistics.
Method Update	show sipd update	Displays the SIP UPDATE method statistics.
SIP Realms All	show sipd realms	Displays realm statistics related to SIP processing.
SIP Realms Individual	show sipd realms <realm name>	Displays realm statistics related to SIP processing for the specified realm.
SIP Redundancy	show sipd redundancy	Displays information about SIP redundancy.
Server Trans	show sipd server	Displays statistics for SIP server events when the SBC acts as a SIP server in the B2BUA role.
SIP Sessions All	show sipd sessions all	Displays all SIP sessions currently on the system.
SIP Sessions	show sipd sessions	Displays the number of sessions and dialogs in various states for the Period and Lifetime spans.
SIP Status	show sipd status	Displays information about SIP transactions.

License Widget

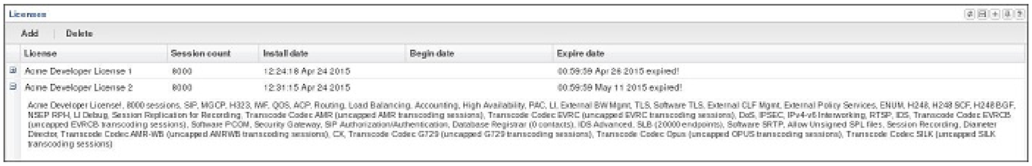
The License widget on the Web GUI provides a workspace where you can view, add, and delete Oracle® Enterprise Session Border Controller (E-SBC) licenses.

From the Widgets tab on the Web GUI, the system displays the Licenses page when you click **Widgets**, **System**, **Licences**.

The Licenses page displays a list of your E-SBC licenses with the following information.

Licenses	The name of the license.
Session Count	The number of session entitlements for the license.
Install Date	The date when the license is added to the system.
Begin Date	The date when the license begins service.
Expire Date	The date when the license ends service.

If you want to see the details of a particular license, click the show-hide toggle by the license name to expand the view to show all of the details. The following illustration shows an example of license details.



	License	Session count	Install date	Begin date	Expire date
⊞	Acme Developer License 1	8000	12:24:18 Apr 24 2015		00:59:59 Apr 26 2015 expired!
⊟	Acme Developer License 2	8000	12:31:15 Apr 24 2015		00:59:59 May 11 2015 expired!

Acme Developer License!, 8000 sessions, SIP, MGCP, H323, IWF, QOS, ACP, Routing, Load Balancing, Accounting, High Availability, PAC, LI, External BW Mgmt, TLS, Software TLS, External CLF Mgmt, External Policy Services, ENUM, H248, H248 SCF, H248 BGF, NSEP RPH, LI Debug, Session Replication for Recording, Transcode Codec AMR (uncapped AMR transcoding sessions), Transcode Codec EVRC (uncapped EVRC transcoding sessions), DoS, IPSEC, IPv4-v6 Interworking, RTSP, IDS, Transcode Codec EVRCB (uncapped EVRCB transcoding sessions), Software PCOM, Security Gateway, SIP Authorization/Authentication, Database Registrar (0 contacts), IDS Advanced, SLB (20000 endpoints), Software SRTP, Allow Unsigned SPL files, Session Recording, Diameter Director, Transcode Codec AMR-WB (uncapped AMRWB transcoding sessions), CX, Transcode Codec G729 (uncapped G729 transcoding sessions), Transcode Codec Opus (uncapped OPUS transcoding sessions), Transcode Codec SILK (uncapped SILK transcoding sessions)

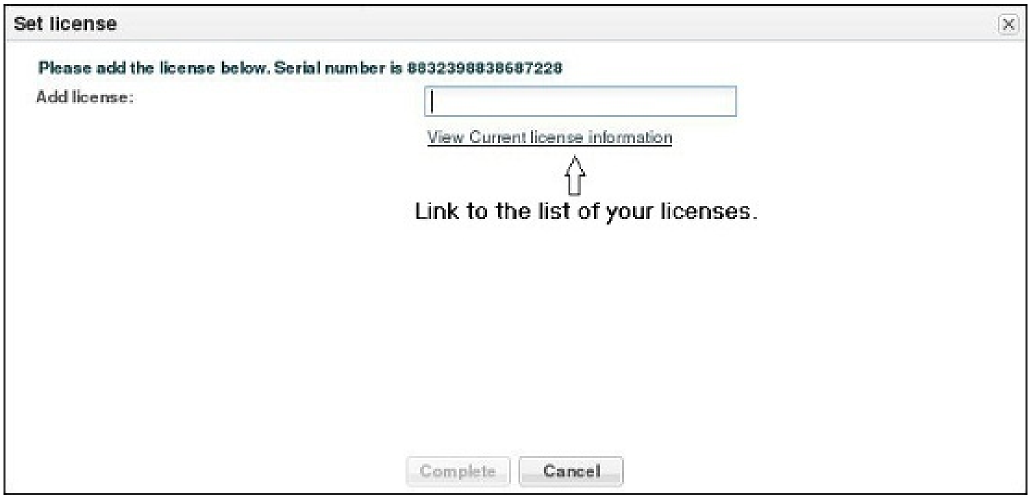
The Licenses widget provides the controls to Add and Delete licenses.

When you click **Add**, the system displays the Set license dialog.

When you select a license from the Licenses list and click **Delete**, the system displays the delete Confirmation dialog.

The License widget includes the Refresh, Download, Add to Dashboard, Pin to Favorites, and Help icons, familiar from other widgets, in the top, right-hand corner. Note that the License widget does not include the Settings icon and the Auto-refresh function because these operations do not apply to licenses.

The Set License wizard is linked to the License widget, so that you can view your licences from the wizard. After launching the Set License wizard, use the "View current license information" link in the Set License dialog to see a view-only list of your E-SBC licenses.



Set license

Please add the license below. Serial number is 8832398838687228

Add license:

View Current license information
Link to the list of your licenses.
Complete
Cancel

The only operations allowed in view mode are Refresh and Download.

5

System Tab Operations

The System tab on the Web GUI provides the following ways to manage files on the system:

- File Management—Displays a list of file types and a set of controls to Refresh, Upload, Download, Backup, Restore, and Delete files.
- Set Boot Parameters—Use the Web GUI to set boot parameters, instead of the ACLI command line.
- Upgrade Software—Verify the health of the system software, for 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.
- Force HA Switchover—Manually place the system in the standby state.
- Reboot—Manually reboot the system at any time.
- Support information—Generate a file that displays troubleshooting information that you can save and send to Oracle Customer Support.

System File Management Types and Descriptions

You can manage Oracle® Enterprise Session Border Controller (E-SBC) system and configuration files from the Web GUI on the **System tab** under **File Management**.

The following table describes the system file types that you can manage.

File Type	Format	Description
Backup Configuration	.gz	Contains a backup of the E-SBC software configuration. You can apply this file to restore a previous configuration.
Configuration CSV	.csv	Contains Comma Separated Value configuration files that you can upload.
Local Route Table (LRT)	.xml, .gz	Contains the Local Routing Table (LRT) file that you can apply to theE-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	Contains fraud protection files that you can upload, download, delete, or open to modify.

File Type	Format	Description
Log	Text	Contains Log files with 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.
Audit Log	Text	Contains a list of files that log system events.
Playback Media	Any media format valid in an RTP audio stream	Contains call progress playback files. The E-SBC can use these files in generated media streams. Note: The media files are raw binary files that contain data for the codec that you want 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	Contains bootable images.
SPL Plug-in	.lua	Contains a 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 capable of performing various tasks by utilizing APIs and callbacks in the E-SBC.

The following table lists and describes the file management controls that display in the system file type dialogs, according to the supported behavior for the file type.

Control	Description
Refresh	Updates the screen to display the latest data.
Add (Fraud Protection files, only.)	Adds a new Fraud Protection file.
Upload	Uploads a file from your server or PC to the E-SBC. The LRT, SPL, and backup configuration upload process provides the option of dynamically applying these files to the E-SBC.
Download All (Log files, only.)	Downloads all Log files from the E-SBC to your local server or PC (typically to the download directory on your system).
Backup	Creates a file that contains a backup of the device software configuration. You can apply this file to restore a previous configuration.
Restore (Backup configuration files, only.)	Restores and applies a Backup configuration file to the E-SBC.

Control	Description
Delete	Deletes the file type from the E-SBC.
Delete All (Log files, only.)	Deletes all Log files from the E-SBC.

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.

1. Access File Management: **System**, **File Management**.
2. On the System page, in the navigation pane, click **File Management**.
3. Select a file to view from the list.

   The system displays the file.
4. Use the controls on the tool bar to manage the file.

Upload a File

You can upload the following file types from your local server or PC to the Oracle® Enterprise Session Border Controller (E-SBC).

> **Note:**
>
> The Log and Audit Log files do not support uploading.

File Type	File Format	Directory
Backup Configuration	.gz	/code/bkups
Configuration CSV	.csv	
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, .tar or no extension specified	/code/images
SPL Plug-on (SPL)	.lua, .spl	/code/spl

The file extension must be applicable to the file type you select. For example, an SPL Plug-in file requires the .lua extension

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.

> **Note:**
>
> You cannot upload log files.

1. Access File Management: **System**, **File management**.
2. On the File management page, 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
- CSV file
- Local route table (LRT)
- Fraud protection table
- Log
- Playback media
- Software image
- SPL Plug-in (SPL)

1. Access File Management: **System**, **File management**.
2. On the File Management page, select the type of file you want to download from the File type list.

3. Place your cursor on the row of the file that 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. Right-click the selected row, and 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

The following information describes the 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 the E-SBC:

- Backup configuration Software image
- CSV
- Local route table (LRT)
- Fraud protection table
- Log
- Playback media
- Software image
- SPL Plug-in (SPL)

> **Note:**
>
> You can only delete multiple files at the same time when the GUi displays the **Delete All** button. For example, on the log file page.

1. Access File Management: **System**, **File Management**.
2. From the File Management list, select the type of file that you want to delete.
3. Put your cursor in the row of the file you want to delete, and right-click.

Note: If the GUI does not display a menu upon right-click, use the **Delete All** control located above the list of files.

4. Click **Delete**. The system displays following message.

   Are you sure you want to delete the file?

5. Click **Delete**.

Back Up a Configuration File

You can back up a configuration file from the Oracle® Enterprise Session Border Controller (E-SBC) to your local server or PC. Back up allows you to save configurations that you can restore to the E-SBC at a later time.

1. Access File Management: **System**, **File Management**.
2. Select a file from the list in the table.
3. Click **Backup**.
4. Click **OK**.

   The system adds the file to the Backup Configuration table.

Restore a Configuration File

You can restore a backed up configuration file to the Oracle® Enterprise Session Border Controller (E-SBC).

1. Access File Management: **System**, **File Management**.
2. On the File Management page, select Backup Configuration.
3. Select a back up, and right-click.

   > **Note:**
   >
   > **Restore** activates only when you select a back up file.

4. Click **Restore**.

   The GUI displays a confirmation dialog.

5. Click **Restore**.

   The system downloads the back up file to the E-SBC. The E-SBC re-boots and restores the configuration from the back up file.

Force an HA Switch Over

You can manually initiate a High Availability (HA) switch over from the Web GUI to reverse the roles of the active and standby peers in an HA pair.

- The Oracle® Enterprise Session Border Controller (E-SBC) from which you initiate the switch over 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.

The following procedure forces the E-SBCs in an HA pair to trade roles. The active system becomes the standby, and the standby system becomes active.

1. Access Force HA Switchover: **System**, **Force HA switchover**.
2. 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. If you have a High Availability (HA) deployment, connectivity to the standby E-SBC stops until the reboot completes.

When the reboot completes, the active and standby systems each display the log on screen and you must manually log on to each system.

> **Note:**
>
> When you reboot the system from the Web GUI, the Web GUI is unavailable until the reboot completes.

When you perform a reboot from the Web GUI	The system behaves
and no boot is in process and the system is not switching over to the standby system of an HA pair,	the GUI session closes and the system displays the Log On screen. You cannot log on to the Web GUI until the reboot completes on the E-SBC.
and a reboot is already in progress,	the system displays a message stating that a reboot cannot occur. The first reboot must complete before another reboot is initiated.
and the active system is currently switching over to the standby system in an HA environment,	the system displays a message stating that a reboot cannot occur because the HA switch over is underway. The standby E-SBC is updating and getting its configuration from the active E-SBC.

Obtain Support Information

You can manually generate a file by way of the Web GUI that contains troubleshooting information. You can save the file and send it to Oracle Customer Support.

1. Access Support Information: **System**, **Support Information**.
2. In the **Confirm** dialog, click Confirm.

The system generates the file.

3. The browser asks you to do one of the following:
   - Open the file—Select the browser and click **OK**, select the tool and click **OK**. The GUI displays the file.
   - Save the file—Click **OK**. The GUI saves the file.
4. Click **OK**.

   The system downloads the file to the specified location.

Upgrade Software

You can upgrade the Oracle® Enterprise Session Border Controller (E-SBC) software from the System tab. The system requires a reboot after the upgrade.

1. Access Upgrade Software: **System**, **Upgrade Software**.
2. In the Upgrade Software dialog, click **Verification**, and do the following:
   - View the health score.
   - Click **View Health Information**, 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.
3. Select one of the following upload methods.

Local	Select a file from your system, and proceed to Step 4
Flash	Select a file already on the E-SBC, and proceed to Step 4.
Network	Do the following: • Boot file. (Network) Enter the complete name of the boot file. • Host IP. (Network) Enter the IP address of the FTP server. • FTP username. (Network) Enter the user name to log onto the FTP server. • FTP password. (Network) Enter the password to log onto the FTP server. • Optional. Select `Reboot after upload`. Proceed to Step 6.

4. Select a file to upload.
5. (Optional) Select `Reboot after upload`.
6. 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.

7. Click `OK`.

   If you selected `Reboot after upload`, the system reboots.