Oracle® Enterprise Session Border Controller

Web GUI User Guide

Release 8.0.0

February 2018

Oracle Enterprise Session Border Controller Web GUI User Guide, Release 8.0.0

Contents

5 Expert Mode Configuration

6 Monitor and Trace Tab

7 Widgets Tab

8 System Tab

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 documents included in the Oracle® Enterprise Session Border Controller (E-SBC) E-CZ8.0.0 documentation set.

ACLI Configuration Guide	Contains conceptual and procedural information for configuring, administering, and troubleshooting the E-SBC.
Administrative Security Guide	Contains conceptual and procedural information for supporting the Admin Security license, the Admin Security ACP license, and JITC 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 the E-CZ8.0.0 release, including platform support, new features, caveats, known issues, and limitations.
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 table describes related documentation for the Oracle® Enterprise Session Border Controller (E-SBC). You can find the listed documents on http://docs.oracle.com/en/industries/communications/ in the "Session Border Controller Documentation" and "Acme Packet" sections.

Accounting Guide	Contains information about the E-SBC accounting support, including details about RADIUS accounting.
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Acme Packet 1100 Hardware Installation Guide	Contains information about the hardware components and features of the Acme Packet 1100, as well as conceptual and procedural information for installation, start-up, operation, and maintenance.
Acme Packet 3900 Hardware Installation Guide	Contains information about the hardware components and features of the Acme Packet 3900, as well as conceptual and procedural information for installation, start-up, operation, and maintenance.
Acme Packet 4600 Hardware Installation Guide	Contains information about the hardware components and features of the Acme Packet 4600, as well as conceptual and procedural information for installation, start-up, operation, and maintenance.
Acme Packet 6300 Hardware Installation Guide	Contains information about the hardware components and features of the Acme Packet 6300, as well as conceptual and procedural information for installation, start-up, operation, and maintenance.
HDR Resource Guide	Contains information about the E-SBC Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Maintenance and Troubleshooting Guide	Contains information about E-SBC logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
MIB Reference Guide	Contains information about Management Information Base (MIBs), Acme Packet's enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Security Guide	Contains information about security considerations and best practices from a network and application security perspective for the E-SBC family of products.

Revision History

Date	Description
December 2017	Initial release
February 2018	• Adds a statement to the "Monitor and Trace Tab" topic about the number of viewers allowed per session.

1

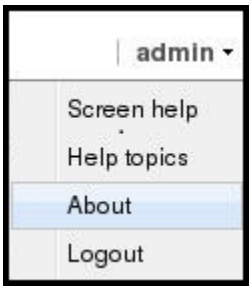
Getting Started

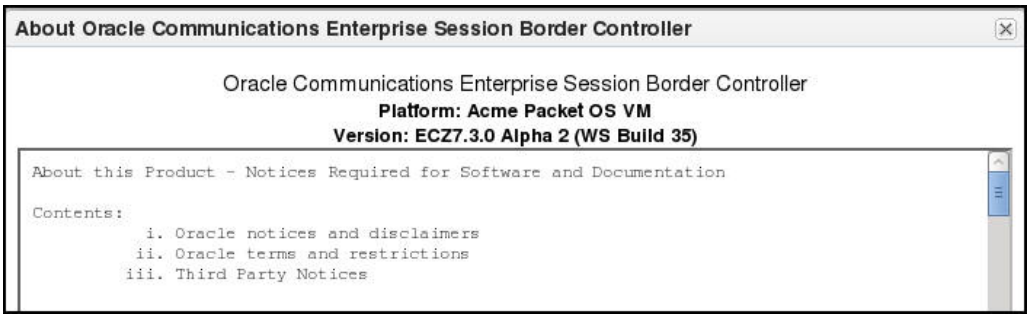
Oracle® recommends that you review the topics in "Getting Started" before working with the system to ensure success with the tools and functions provided.

About This Software

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

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





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

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

Browser Support

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

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

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

Internet Protocol Version Support

The Web GUI supports only IPv4.

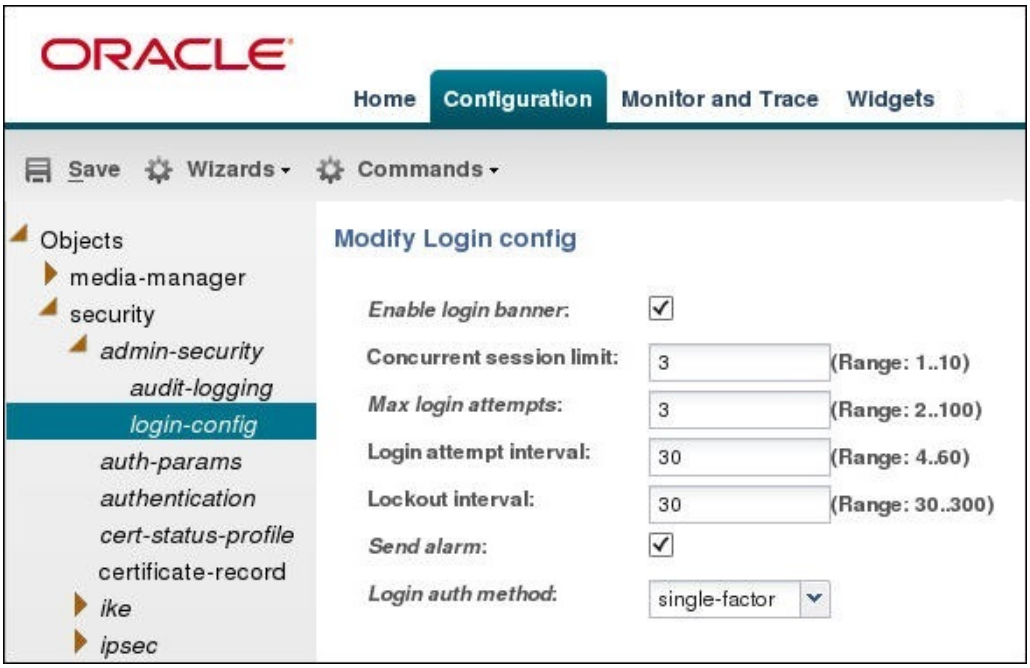
Web GUI Access with the Admin Security License

The Oracle® Enterprise Session Border Controller (E-SBC) supports installing the Admin Security License from the Web GUI. You may find this method more convenient than using the ACLI. When you install the Admin Security License, the system provides additional configuration parameters and behavioral controls to enhance security. 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 displays the login-config page and adds parameters to the password-policy page.

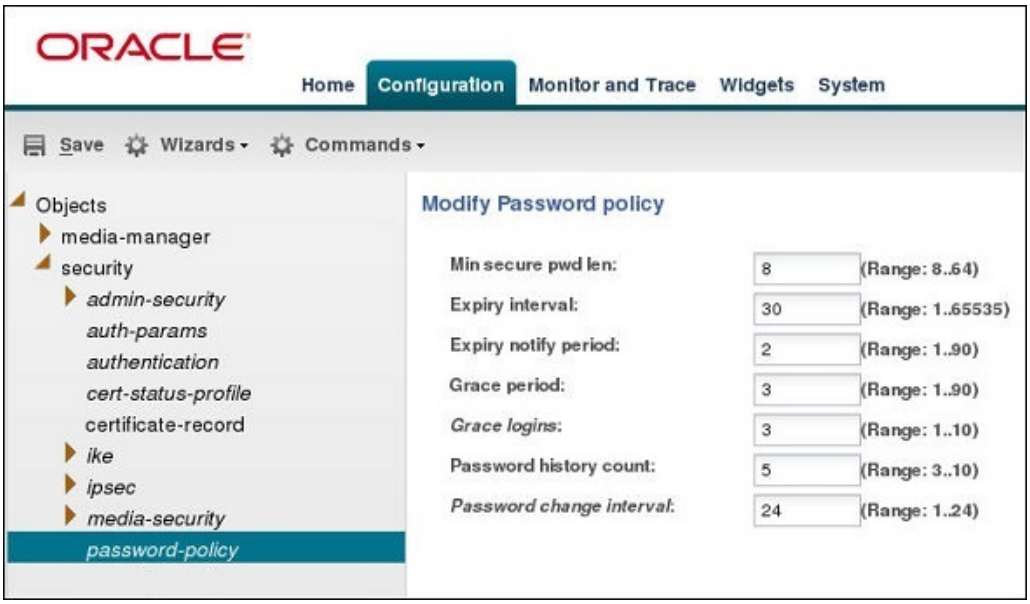
The login-config page provides the configuration parameters shown in the following illustration.



Note:

The system supports single-factor and two-factor authentication for `Login auth method`.

The password-policy page displays the advanced configuration parameters listed below `Min secure pwd len` in the following illustration.



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

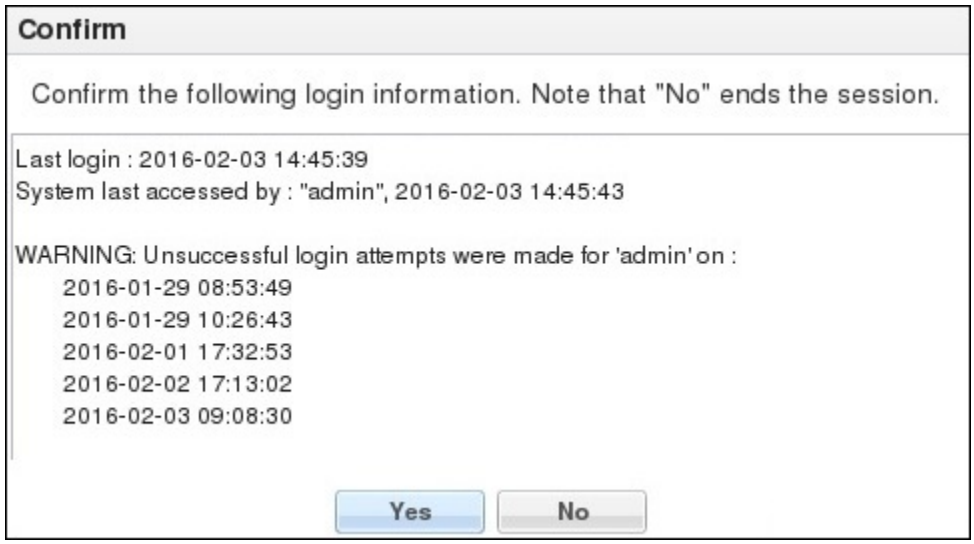
License. If the Web server is configured for HTTP when you install the Admin Security License, the system displays an error message when you attempt to Save. Note that after the Admin Security License is installed, the system does not allow changing HTTPS to HTTP.

Certificates—The system requires you to configure localCert and localCertCA 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

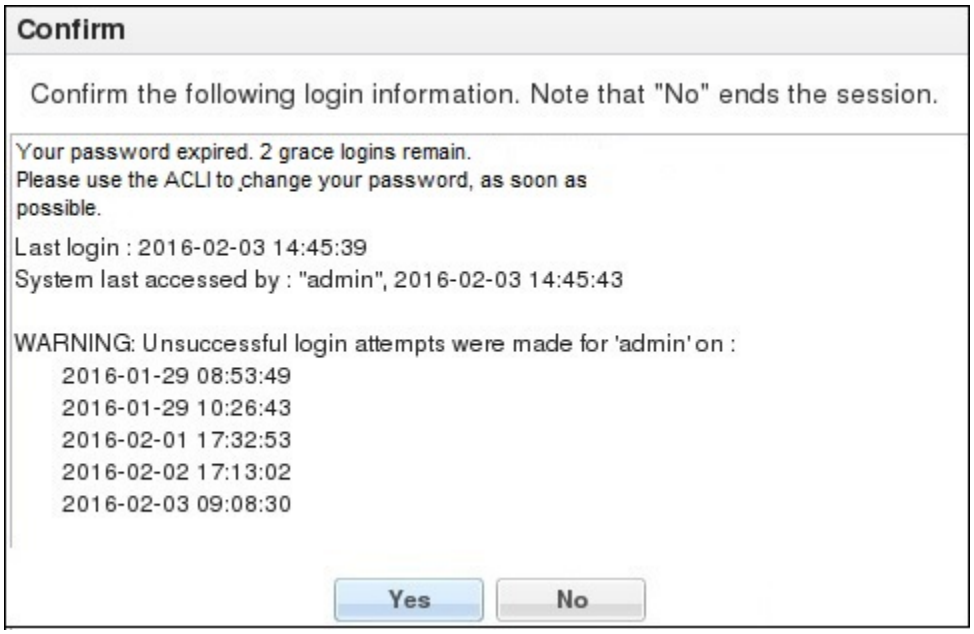
Concurrent Sessions Limit—In login-config, you can specify the maximum number of concurrent sessions allowed. When the limit is reached, the system allows no more logins until the number of active sessions falls below the maximum.

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.

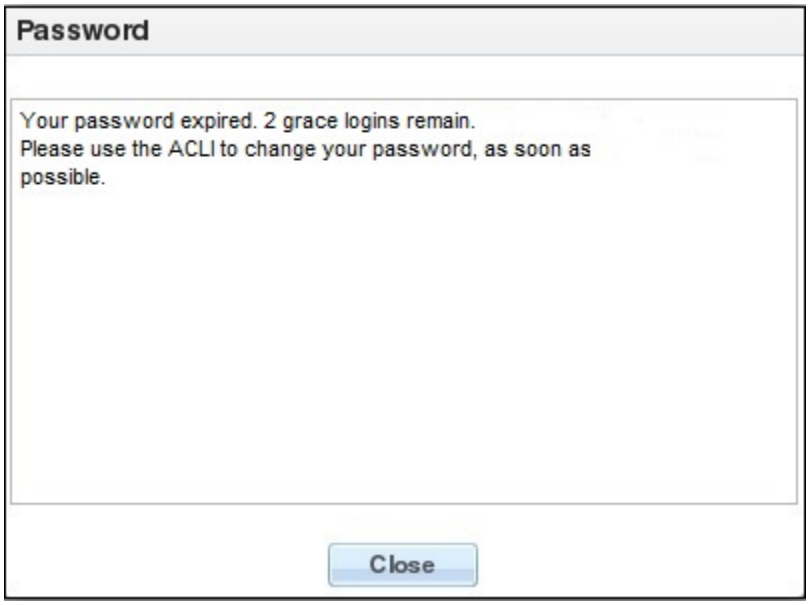


Password Expiry Notification—You can configure password-policy to notify the user up to 90 days in advance of password expiry. The system provides the notification in the following ways.

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



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



> **Note:**
>
> The Web GUI does not support changing a user password. 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:

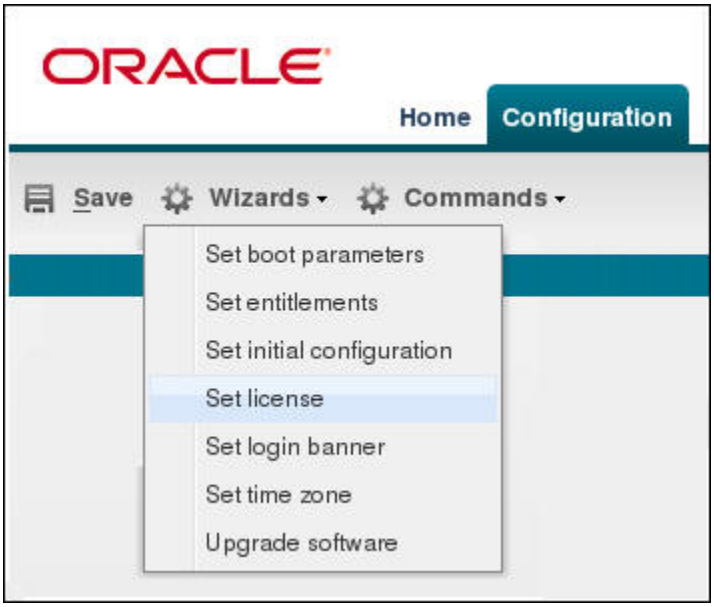
- The local Admin and User can login by way of the E-SBC console, the Web GUI, SSH or SFTP, and the system performs the local user authentication process.

- The local Admin and User can login 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.

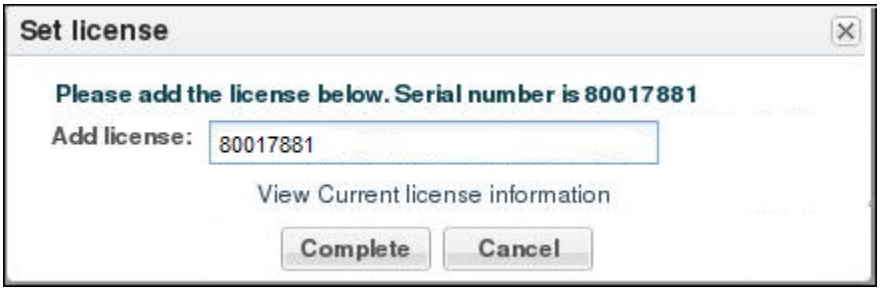
Two-Factor Authentication. When enabled, the system prompts the user for a passcode in addition to the User Name and Password. Change the default passcode upon the first login attempt. The length and strength requirements that apply to passwords also apply to passcodes. Other policy mandates such as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

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" in the *WEB GUI User Guide.* and the online Help.

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 E-SBC does not require either the hardware Security Service Module (SSM) or the software TLS license when configuring `certficate-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.

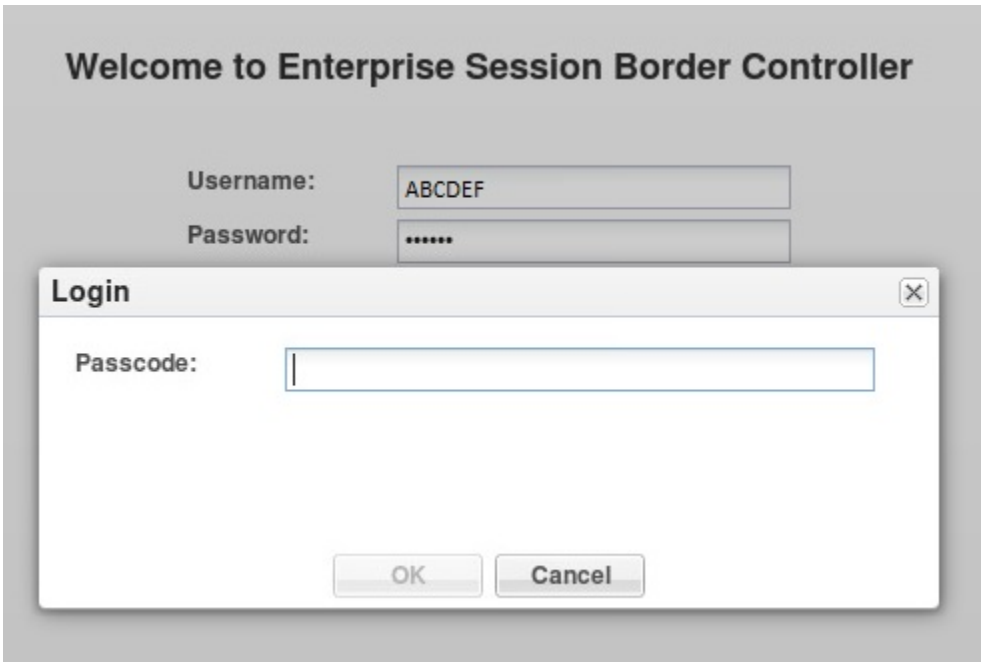
Note that virtual machines require the software TLS license.

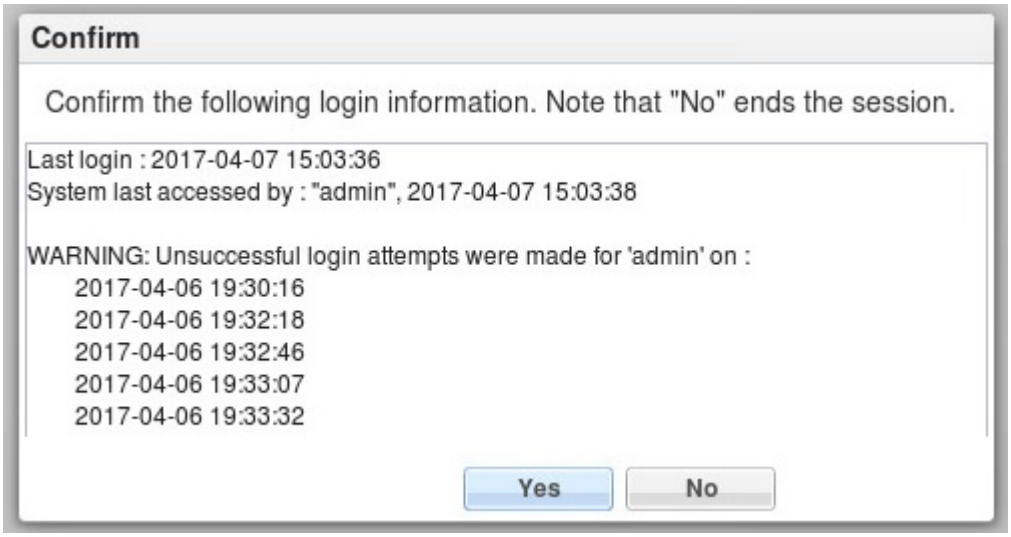
Two-Factor Authentication

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.





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 object.

   Configuration > **security** > **admin-security** > **login-config**.
2. In the Modify Login Config dialog, select **two-factor** from the Login Auth Method drop-down list.
3. Click **OK**.
4. Save the configuration.

Log On and Log Off

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

Log On to the Web GUI

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

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

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

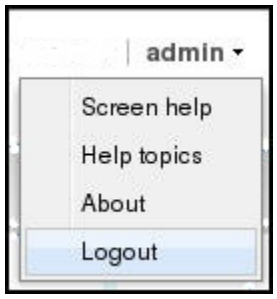
   ```
   http://<Server IP address>
   https://<Server IP address>
   ```

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

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

Log Off the Web GUI

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



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

User and Administrator Access Rules

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

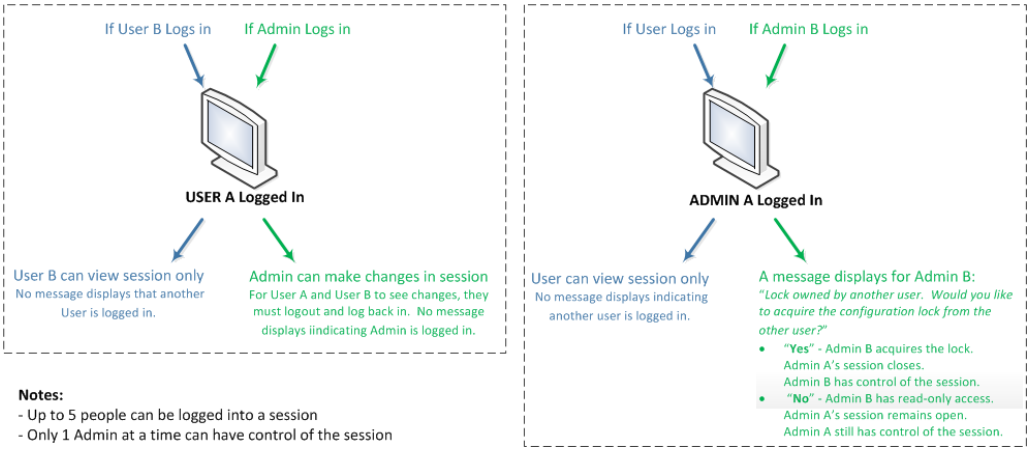
The following table describes the Web GUI access rules for the User and Administrator roles.

Role	Rule
User	User • Read-only access only • View basic and advanced configuration information • Cannot save and activate a configuration • Cannot add a configuration • Cannot edit a configuration
Administrator	Administrator • Add, edit, and view configurations • Add, edit, and view advanced 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 onto the session.

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



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

```
User limit reached. Please try again later.
```

Change the Log On Password

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

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

Radius Server in the Network

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

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

User Class	Access
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.

User Class	Access
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 SIP Monitor and Trace features and functions Can download the following files in System File Management: • Backup configuration • Configuration CSV • Local subscriber table (LST) • Log • Software image • SPL Plug-in (SPL)

Note:

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

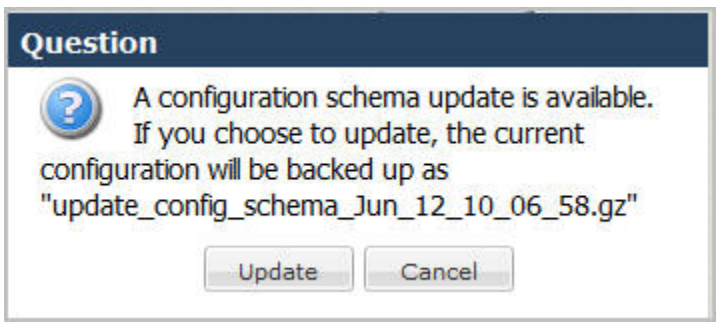
Update the Configuration Schema

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

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

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

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



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

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

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

Web GUI Tools

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

Shortcut Keys

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

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

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

Tabs

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

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

	Home Tab	Configuration Tab	Monitor and Trace Tab	Widgets Tab	System Tab
Basic Mode	The Home tab displays the Web GUI Dashboard, where SIP statistics are displayed on configurable widgets. On the Home tab, you can: • Add a widget • Specify the widget sampling parameters • Reset the display to the default • Refresh the data displaying in the widgets	In Basic Mode the Configuration tab displays a workspace where you drag and drop icons to configure the border controller in the network. The toolbar on the Configuration Tab contains the following buttons that display task controls: • Settings. Configure system settings. • Network. Configure the Host Route and Network Interface. • Security. Configure a Certificate Record, the SDES profile, and the TLS profile. • Management. Configure Accounting, SNMP Community, Trap Receiver, and Web Server. • Other. Configure Media Profile, Translation Rules, SIP	The Monitor and Trace tab displays data that the system collects about: • Sessions • Registrations • Subscriptions • Notable Events The page displays a toolbar that you can configure to display particular data for each of the data collection types. For example, you can choose the sort order and column headings. When data is present, the following task controls are 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	The Widgets tab is a portal to statistics about the system. • 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. • Displays a list of Favorite widgets.	The System tab displays the following management controls: • File management. Displays a list of file types and a set of controls to Refresh, Upload, Download, Backup, Restore, and Delete files. • 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. • Upgrade Software. Verify the health of the system software, for

Home Tab	Configuration Tab	Monitor and Trace Tab	Widgets Tab	System Tab
	Features, SIP Manipulations, and SPL. • Save. Save and activate the configuration. • Discard. Delete unsaved configuration changes. • Wizards. Set boot parameters, Set initial configuration, Set time zone, and Upgrade software. • Switch to Expert. Change from Basic mode to Expert mode. • Search. Search for objects and attributes.	external location. • Export summary. Save a summary of the data to an external location.		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.

	Home Tab	Configuration Tab	Monitor and Trace Tab	Widgets Tab	System Tab
Expert Mode	Same as in Basic Mode	In Expert Mode the Configuration tab displays a list of configuration objects, grouped like those in the Acme Command Line Interface (ACLI). For example: • Media Manager • Security • Session Router • System Each group contains the same configuration objects as the ACLI. Each object displays the corresponding configuration dialog.	Same as in Basic Mode	Same as in Basic Mode	Same as in Basic Mode

Search

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

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

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

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

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

Help

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

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

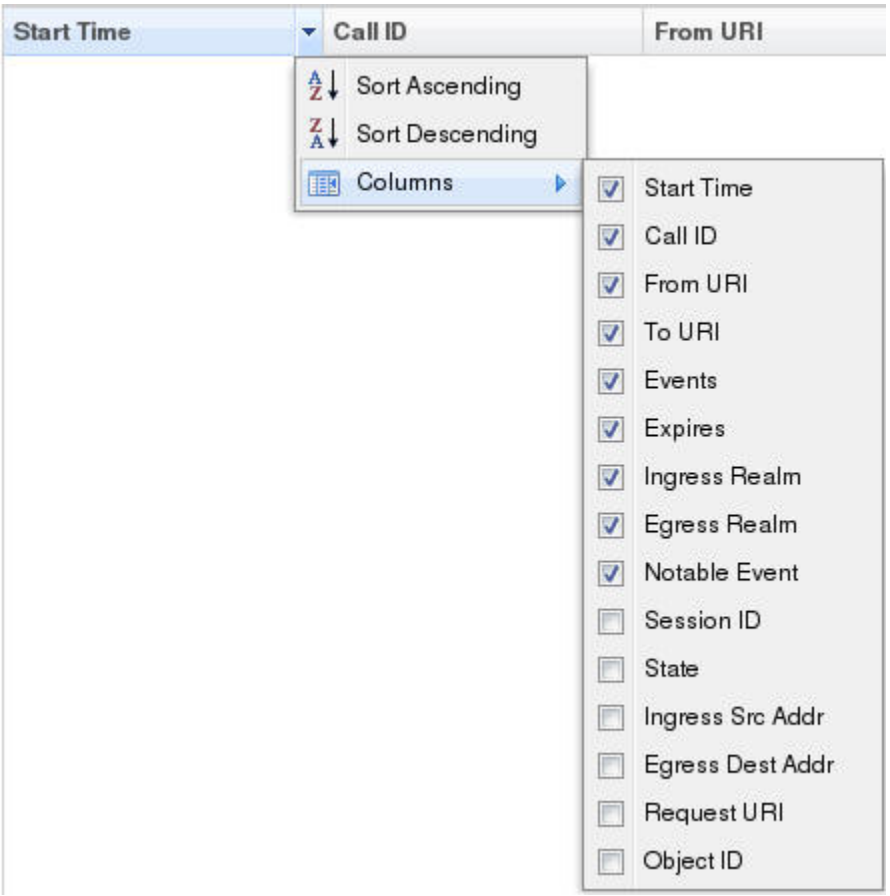
Customize the Page Display

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

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,



Discard Changes

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

1. From the Web GUI toolbar, click **Discard**.

   The system displays a confirmation message.

2. Click **Discard**.

2
Home Tab

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

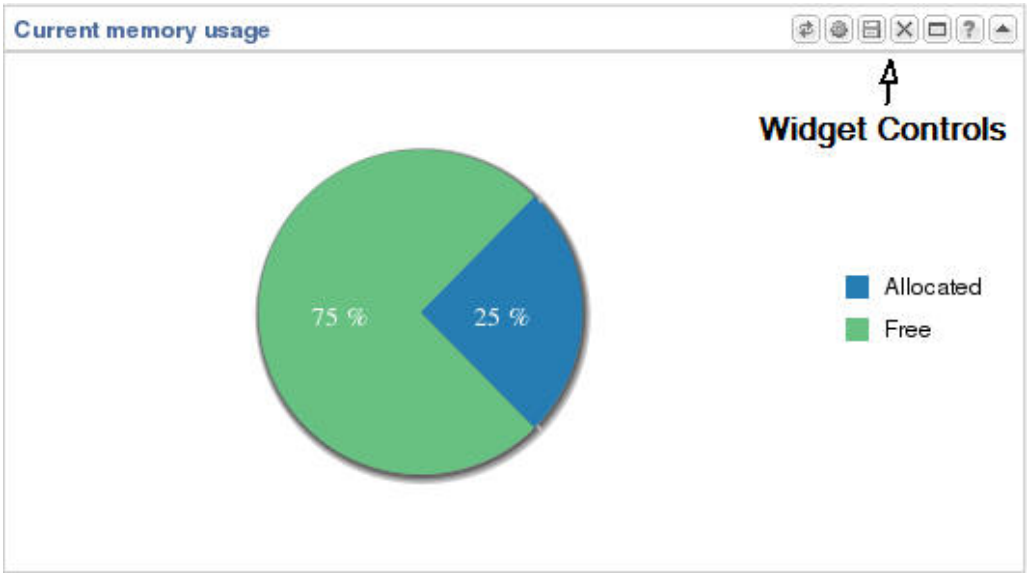
The Dashboard supports up to 18 widgets. Each widget can display up to 100 data samples in intervals of 1 hour, 1 minute, or 1 second. You can select a chart, a graph, a table, a web form, or text for the display. Customize the dashboard by adding, deleting, and moving the widgets. You can refresh the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

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

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

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

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



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

Add a Dashboard Widget

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

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

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

1. From the Home page, click **Add widget**.
2. From the list of **Widgets**, click the name of the widget to add.
3. Under the **Command** column header, click **Add** for the widget to add.

   The system displays a success message.
4. Click **OK**.
5. Click **Close**.

   The system displays the Dashboard with the newly added widget.

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

Configure Data Sampling Settings for a Dashboard Widget

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

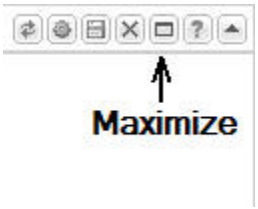
To see SIP and System statistics displayed on a Dashboard widget, the system requires a setting for how often to refresh the display. You can use the default interval or select one from the Auto-refresh interval drop-down list on the widget. Some widgets also display the Table Name drop-down list, where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

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

View a Dashboard Widget in Full-Screen Mode

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

Each Dashboard widget includes a maximize icon on its toolbar.



1. Click the maximize icon.

   The system displays a pop-up window of the selected widget.

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

View Any Widget in Full-Screen Mode

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

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

1. From the Web GUI, click the **Widgets** tab.
2. In the navigation pane, click a Dashboard Widget name.

   The system displays a list of the views available for the selected widget.
3. In the list of view types click the view that you want to see in full-screen.

3
Configuration Tab

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

The Web GUI provides the following configuration tools.

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

Configuration States and Behavior

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

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

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

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

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

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

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

Configuration from the Web GUI

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

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

The common beginning in Basic mode

Each Basic mode configuration procedure begins, as follows:

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

The common ending in Basic mode

Each Basic mode configuration procedure ends, as follows:

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

The common beginning in Expert mode

Each Expert mode configuration procedure begins, as follows:

1. From the Web GUI in Expert mode, click the **Configuration** tab.

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

The common ending in Expert mode

Each Expert mode configuration procedure ends, as follows:

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

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

Configuration Error Messages

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

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

Column	Description
Severity	Identifies the level of severity that the Oracle Enterprise Session Border Controller assigns to the error. Valid values are: • 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 Deletion Methods

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

Delete from an Icon

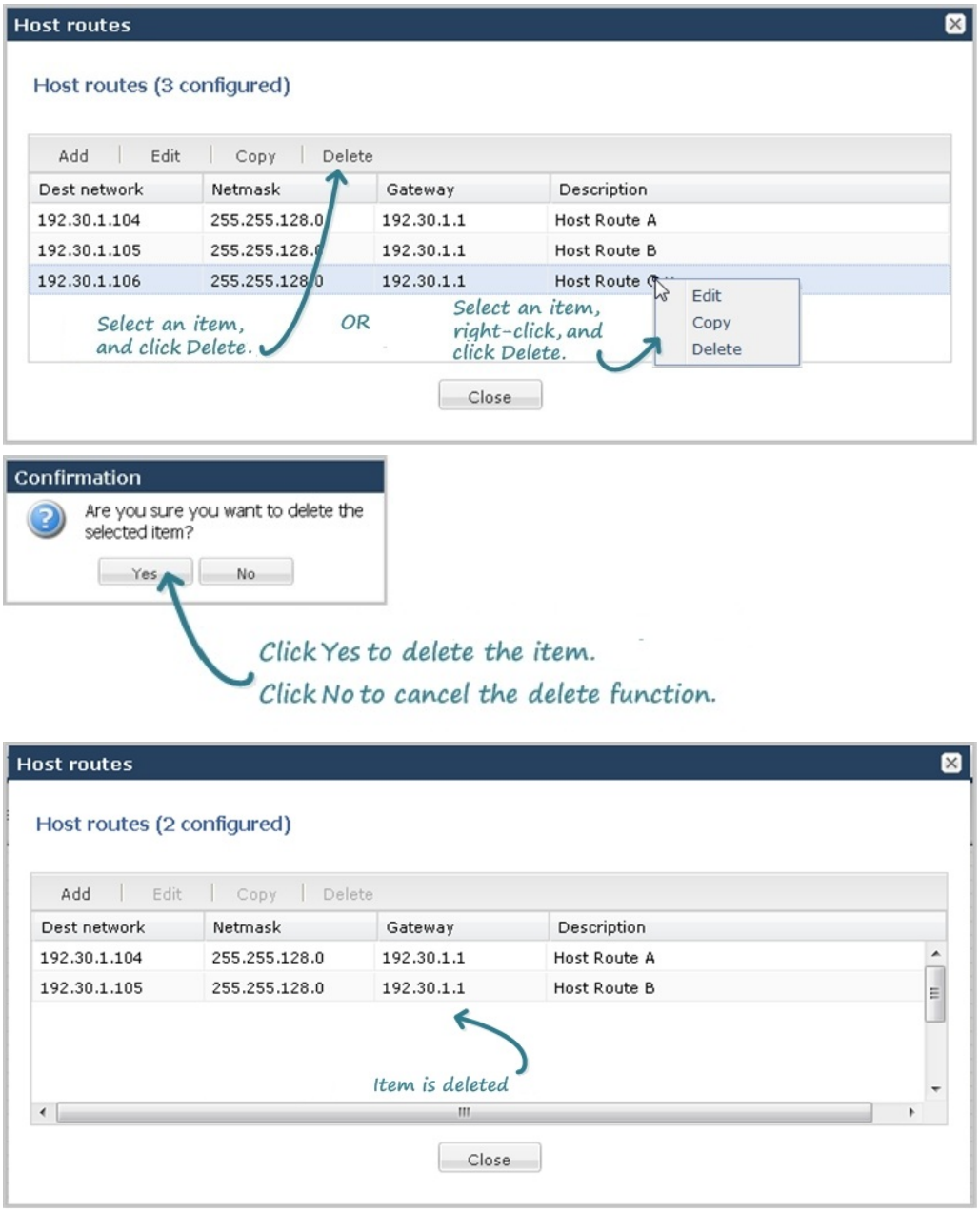
For any device or interface in the workspace, right-click the icon and select Delete from the drop-down menu. The following illustration shows an example of deleting a configuration by way of the PBX icon.

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

Delete from a Configuration Dialog

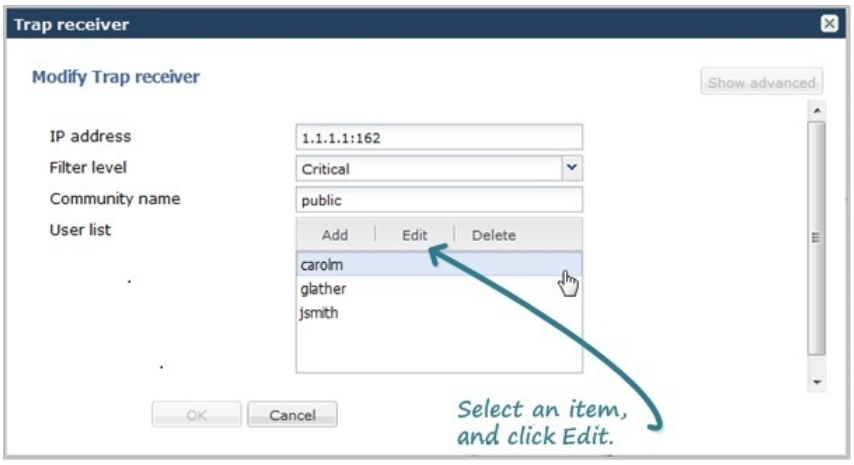
To delete a configuration from a toolbar menu, you click the configuration object that you want from the menu, and use one of the following methods to delete the configuration:

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



Delete an Individual Parameter Configuration

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



Note:

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

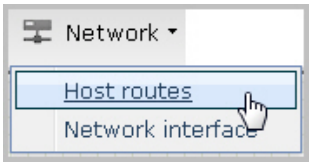
Configuration Copying Methods

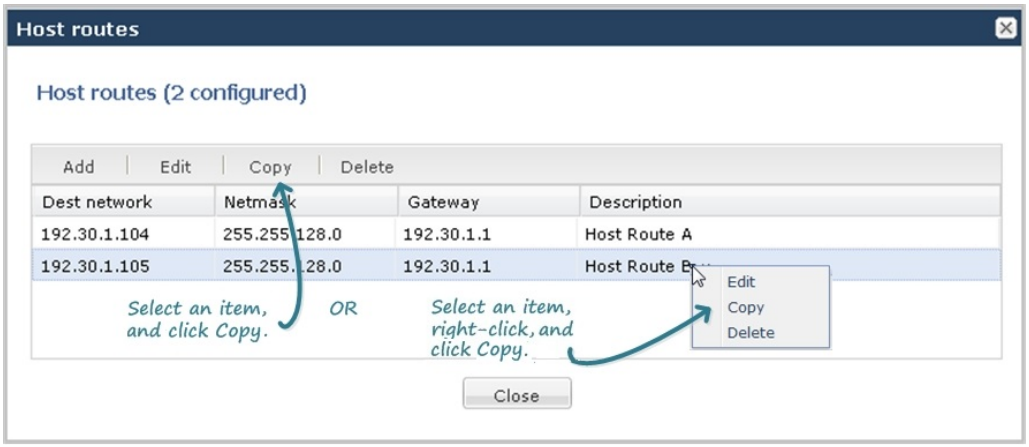
In Basic mode you can copy a configuration by way of the object menus on the toolbar, but not from the icons in the workspace.

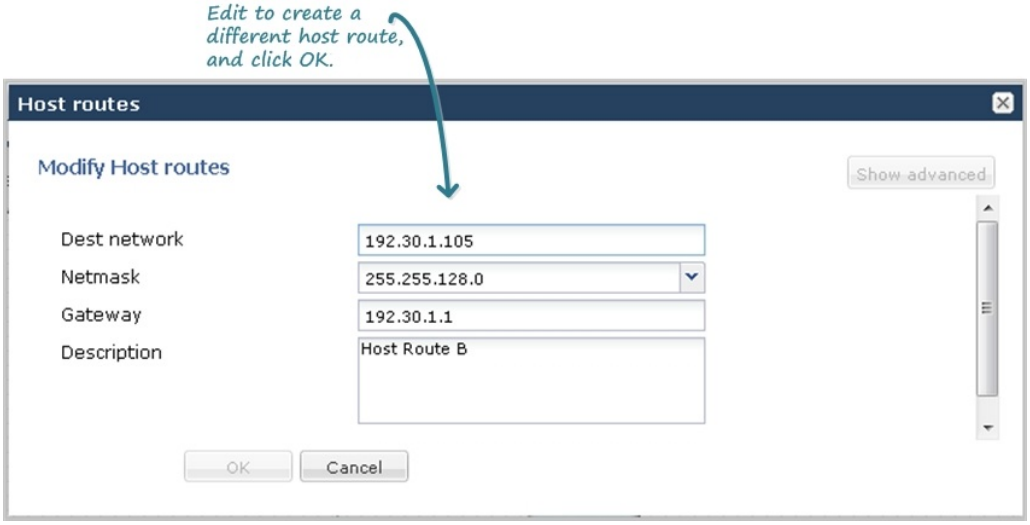
To copy a configuration, use one of the following methods:

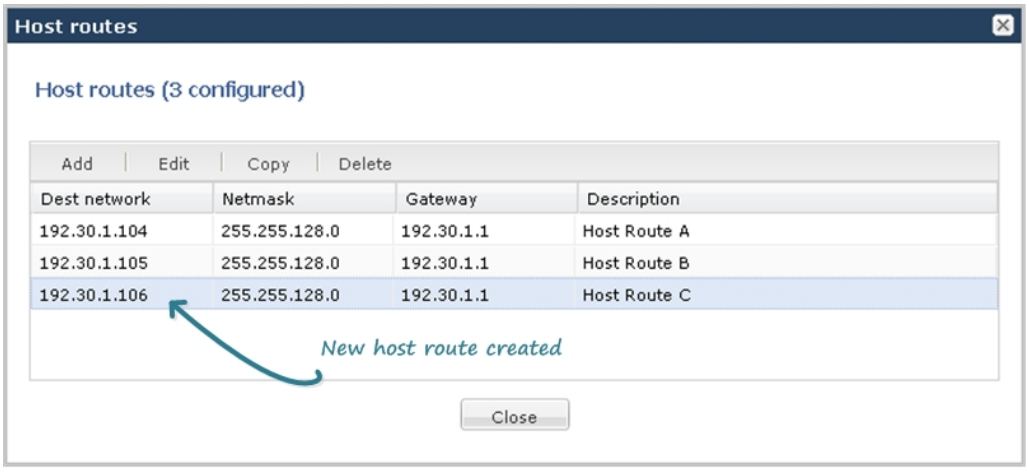
- Select an item on the list and click **Copy**.
- Select an item on the list, right click, and select **Copy** from the task menu.

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




Host routes
Host routes (2 configured)
Add
Edit
Copy
Delete
Dest network
Netmask
Gateway
Description
192.30.1.104
255.255.128.0
192.30.1.1
Host Route A
192.30.1.105
255.255.128.0
192.30.1.1
Host Route B
Select an item, and click Copy.
OR
Select an item, right-click, and click Copy.
Edit
Copy
Delete
Close


Edit to create a different host route, and click OK.
Host routes
Modify Host routes
Show advanced
Dest network
192.30.1.105
Netmask
255.255.128.0
Gateway
192.30.1.1
Description
Host Route B
OK
Cancel


Host routes
Host routes (3 configured)
Add
Edit
Copy
Delete
Dest network
Netmask
Gateway
Description
192.30.1.104
255.255.128.0
192.30.1.1
Host Route A
192.30.1.105
255.255.128.0
192.30.1.1
Host Route B
192.30.1.106
255.255.128.0
192.30.1.1
Host Route C
New host route created
Close

Configuration Editing Methods

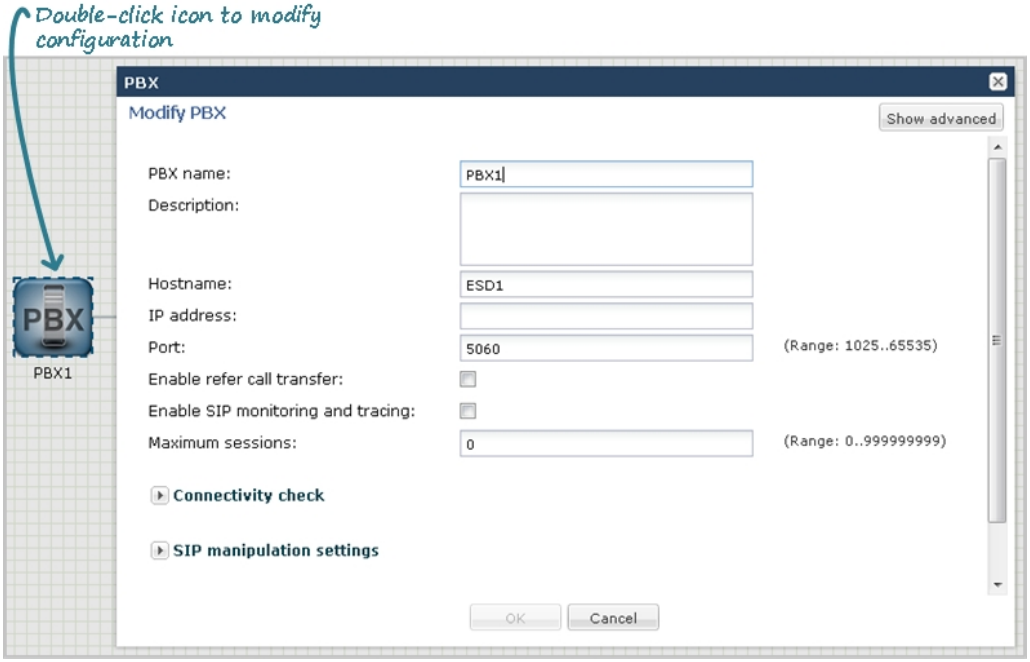
In Basic mode, you can edit a configuration by way of the following methods.

Edit from an Icon

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

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

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

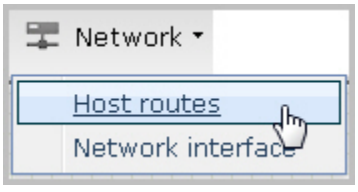


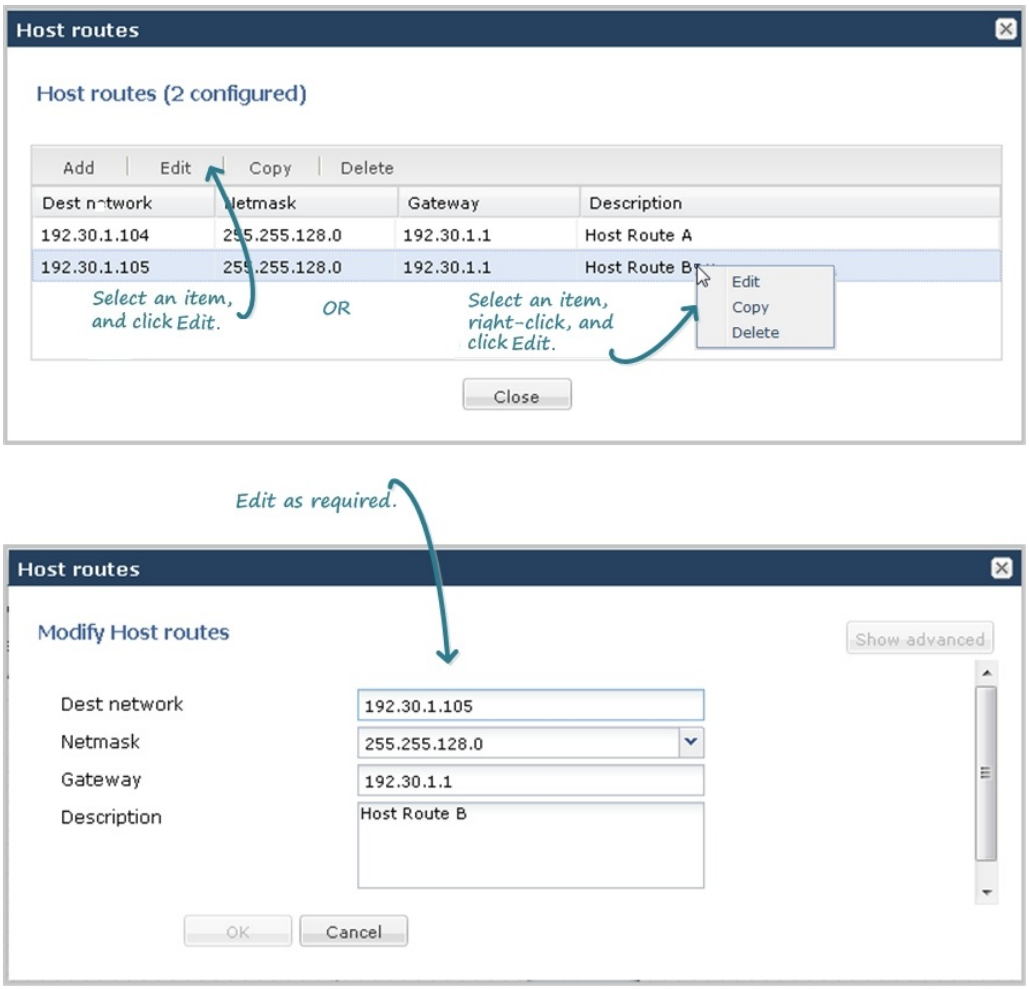
Edit from a Configuration Dialog

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

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

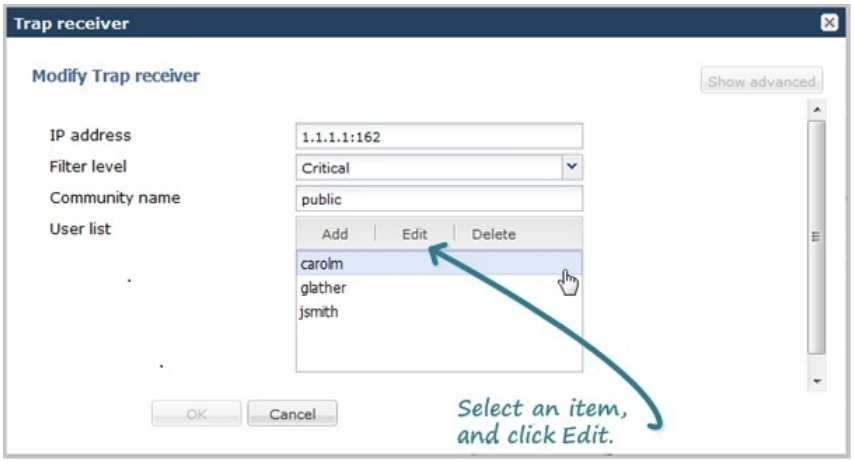
The following illustrations show examples of editing a host route configuration by both methods.





Edit an Individual Parameter

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



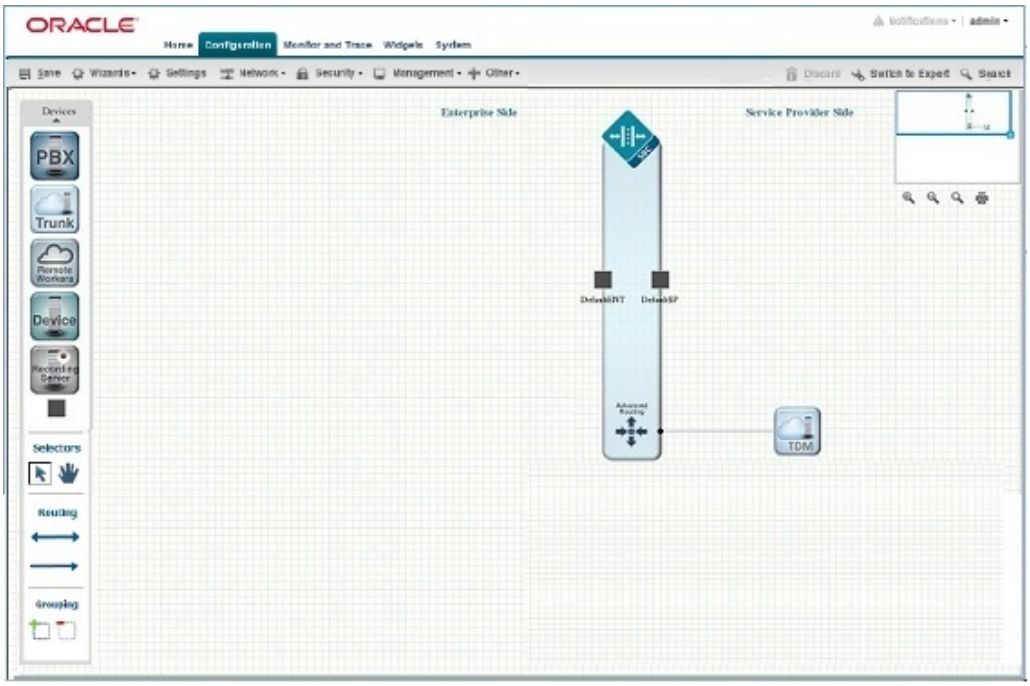
> **Note:**
>
> After editing a configuration, you must save and activate the configuration for the changes to take affect.

4

Basic Mode Configuration

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

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

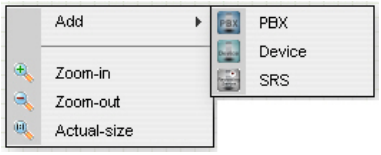
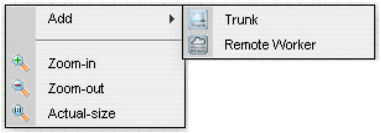


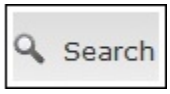
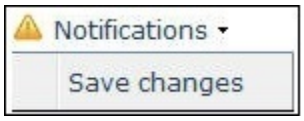
To populate the network, drag-and-drop elements from the Devices tool bar on the left of the page onto the workspace. As you drop an icon onto the workspace, the element connects to the E-SBC and a dialog displays where you configure that element. Elements in the toolbar are associated either with Enterprise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

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

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

Basic Mode Configuration Tools

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

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

Basic Mode Configuration Buttons and Dialogs

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

Buttons	Configuration Dialogs
Wizards	• Set boot parameters • Set entitlements • Set initial configuration • Set license • Set time zone • Upgrade software
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
Network	• Host route • Network interface
Security	• Certificate record • SDES profile • TLS profile
Management	• Accounting • SNMP community • Trap receiver • Web server
Other	• Media profile • Translation rules • SIP features • SIP manipulations • SPL

Device Icons Toolbar

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

The following table describes each icon on the Devices toolbar.

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

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

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

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

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

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

> **Note:**
>
> For more information about the workspace tools, see Workspace Tools.

Device Icon Connection Matrix

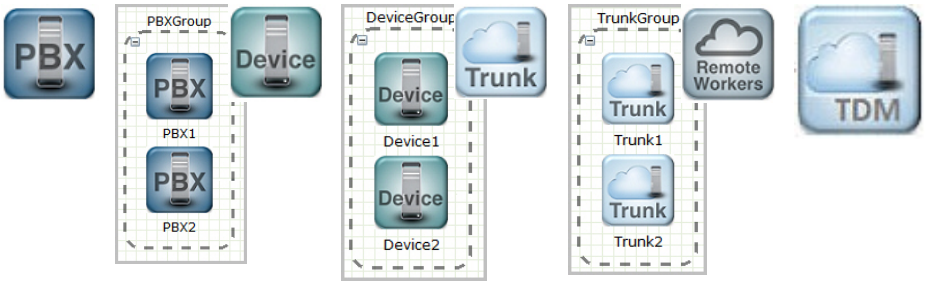
Before configuring the Oracle® Enterprise Session Border Controller (E-SBC) from the Web GUI workspace, you need to know the types of connections that the system supports between device icons.

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

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

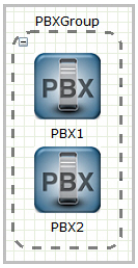
One-Way Routing Local Policy

From	To



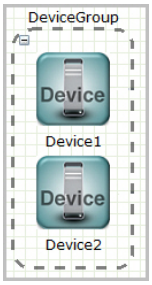
Yes	Yes	Yes	Yes	Yes	Yes	No	Yes

Yes	Yes	Yes	Yes	Yes	Yes	No	Yes



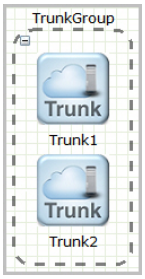
Yes	Yes	Yes	Yes	Yes	Yes	No	Yes

Yes	Yes	Yes	Yes	Yes	Yes	No	Yes



Yes	Yes	Yes	Yes	No	No	No	Yes

Yes	Yes	Yes	Yes	No	No	No	Yes

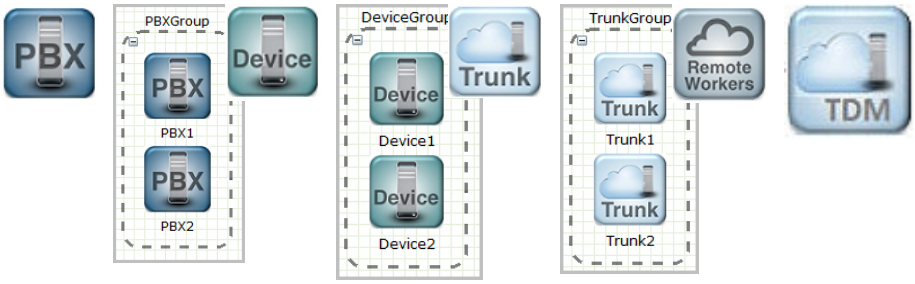


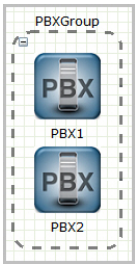
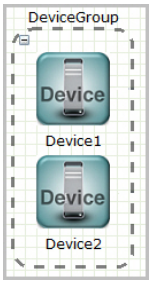
Yes	Yes	Yes	Yes	No	No	No	No

Yes	Yes	Yes	Yes	Yes	Yes	No	Yes

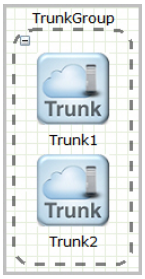
Two-Way Routing Local Policy

From	To



Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
							
Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
							
Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
							
Yes	Yes	Yes	Yes	Yes	Yes	No	Yes
							
Yes	Yes	Yes	Yes	No	No	No	Yes
							

Yes	Yes	Yes	Yes	No	No	No	Yes



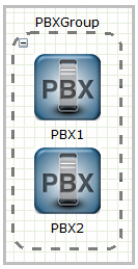
No	No	No	No	No	No	No	No

Yes	Yes	Yes	Yes	Yes	Yes	No	Yes

Advanced Routing Local Policy

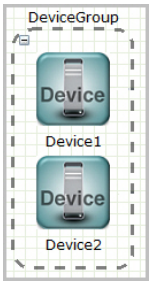
From	To
	
	Yes
	

Yes



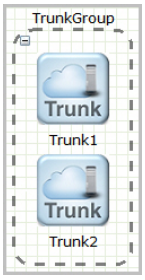
Yes

Yes



Yes

Yes



No

Yes

Network Configuration Using the Workspace Icons

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

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

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

Add a PBX

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.

Drag and drop the PBX icon from the device toolbar onto the workspace and the system displays the Add PBX dialog, where you enter the configuration parameters. After you perform the configuration and click **OK** in the Add PBX dialog, the PBX icon persists on the Enterprise side of the workspace. You can edit the PBX configuration any time by double-clicking the

icon and modifying the configuration in the Modify PBX dialog box. Save and activate the configuration after the initial configuration and after modifying the configuration.

1. From the device toolbar, click the **PBX** icon, and drag it to the Enterprise side of the E-SBC on the workspace.

   The system displays the Add PBX dialog.

2. In the Add PBX dialog, click **Show advanced**, and do the following:

Attributes	Instructions
PBX name	Enter the name to assign to this PBX in the Enterprise network. For example, PBX1. Valid values are alpha-numeric characters.
Description	Enter a description for this PBX. For example, PBX for Enterprise. Valid values are 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 are 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. Range: 1025-65535. Default: 5060.
Enable refer call transfer	Select to enable.
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. Range: 0-9999. Default 30.
Connectivity check methods	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	Use the arrow buttons to move one or more rules from the inactive list in the left pane into the active list in the right pane.
Outbound translation rules	Use the arrow buttons to move one or more rules from the inactive list in the left pane into the active list in the right pane.
Trust mode	Select a trust level from the drop-down list.
Invalid message threshold	Enter the invalid message threshold. Range: 0-9999.
Maximum message threshold	Enter the maximum message threshold. Range: 0-9999.

Attributes	Instructions
SPL options	Click **Add**, enter the name of the SPL option, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another SPL option, and click **OK**. Repeat, as needed.

3. Click **OK**.

   The system displays the PBX icon on the workspace with a connector line to the Enterprise side of the E-SBC.

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.

Drag and drop the Trunk icon from the device toolbar onto the workspace and the system displays the Add SIP Trunk dialog, where you enter the configuration parameters. After you perform the configuration and click **OK** in the Add SIP Trunk dialog, the Trunk icon persists on the Service Provider side of the workspace. You can edit the Trunk configuration any time by double-clicking the icon and modifying the configuration in the Modify SIP Trunk dialog box. Save and activate the configuration after the initial configuration and after modifying the configuration.

1. From the device toolbar, click the **Trunk** icon, and drag it to the Service Provider side of the E-SBC on the workspace.

   The system displays the Add SIP Trunk dialog.

2. In the Add SIP Trunk dialog, click **Show advanced**, and do the following:

Attributes	instructions
Trunk name	Enter the name to assign to this SIP Trunk in the Service Provider network. For example, SIPT1. Valid values are alpha-numeric characters.
Description	Enter a description for this SIP Trunk. For example, SIP Trunk for Service Provider. Valid values are 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 is 0.0.0.0.

Attributes	instructions
IP Port	Enter the IPport for this SIP Trunk. Range: 1025-65535. Default: 5060.
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. Range: 0-9999. Default 30.
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	Use the arrow buttons to move one or more rules from the inactive list in the left pane into the active list in the right pane.
Outbound translation rules	Use the arrow buttons to move one or more rules from the inactive list in the left pane into the active list in the right pane.
Trust mode	Select a trust level from the drop-down list.
Invalid message threshold	Enter the invalid message threshold. Range: 0-9999.
Maximum message threshold	Enter the maximum message threshold. Range: 0-9999.
SPL options	Click **Add**, enter the name of the SPL option, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another SPL option, and click **OK**. Repeat, as needed.

3. Click **OK**.

   The system displays the Trunk icon on the workspace with a connector line to the Service Provider side of the E-SBC.

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 One-Way Local Routing Policy

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

- Note the IP addresses of the devices that you want to affect with this policy.

- Confirm that the system displays the Basic mode.

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

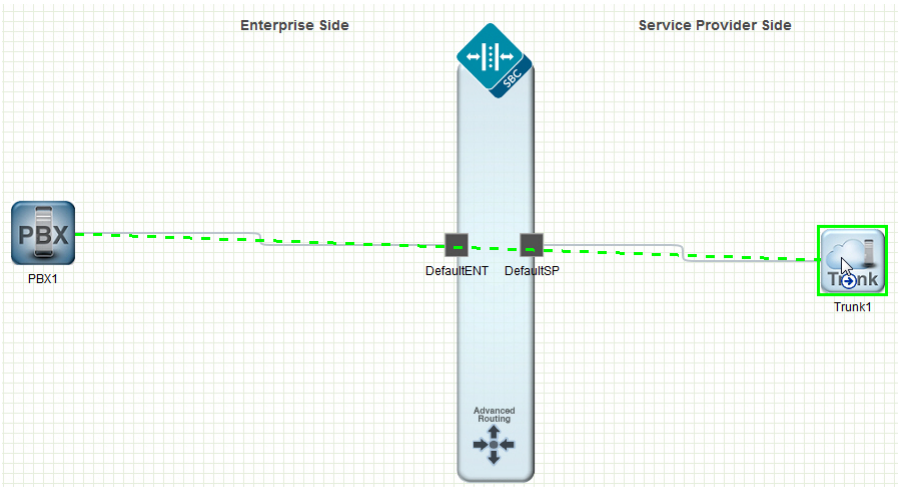
Drag and drop the one-way routing icon from the device toolbar onto the PBX icon and connect it to the Trunk icon. The system displays the Add One-Way Route Information dialog, where you enter the local routing policy parameters. After you perform the configuration and click **OK** in the Add One-Way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

1. From the Device toolbar, click the one-way arrow.

   The system frames the icon to indicate that it is ready to drag and drop.

2. Click center of the PBX icon on the Enterprise side of the E-SBC. The system displays a small arrow.

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



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

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

Attributes	Instructions
Route name	Enter a name for this route. For example, Route A.
Route cost	Range: 999999999
From address	a. Click **Add**, and enter the IP address of the PBX. b. Click **OK**.
To address	a. Click **Add**, and enter the IP address of the Trunk. b. Click **OK**.

5. Click **OK**

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

6. Save the configuration.

Add a Two-Way Local Routing Policy

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

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

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

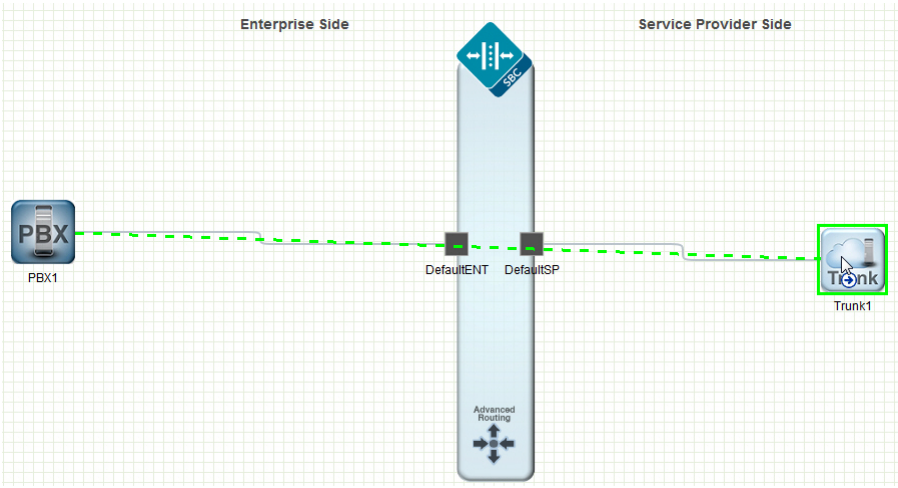
Drag and drop the two-way routing icon from the device toolbar onto the PBX icon and connect it to the Trunk icon. The system displays the Add Two-Way Route Information dialog, where you enter the local routing policy parameters. After you perform the configuration and click **OK** in the Add Two-Way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

1. From the Device toolbar, click the two-way arrow.

   The system frames the icon to indicate that it is ready to drag and drop.

2. Click center of the PBX icon on the Enterprise side of the E-SBC. The system displays a small arrow.

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



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

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

Attributes	Instructions
Route name	Enter a name for this route. For example, Route A.
Route cost	Range: 999999999
From address	a. Click **Add**, and enter the IP address of the PBX. b. Click **OK**.
To address	a. Click **Add**, and enter the IP address of the Trunk. b. Click **OK**.
From address	a. Click **Add**, and enter the IP address of the Trunk. b. Click **OK**.
To address	a. Click **Add**, and enter the IP address of the PBX. b. Click **OK**.

5. Click **OK**

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

6. Save the configuration.

Configure Advanced Local Routing Policy

After adding a one-way or two-way local policy route, you can configure the polices with advanced parameters from the Web GUI in Basic mode.

- Configure at least one local routing policy.
- Note the name of the local routing server.
- Confirm that the system displays the Basic mode.

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

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

Attributes	Instructions
Name	Enter the name of the local routing server.
File name	Enter the name of the XML file that contains the routing entries that you want to use for this policy. Note that the file must be located in the/code/lrt directory, must be gzipped, and must have a suffix of .gzip or .gz.
Prefix length	Enter the number of characters to use for local route matching. Range: 0-999999999
String lookup	Select to enable using string lookup instead of the E.164 phone number. Enable for tables with range entries containing alphanumeric prefixes.
Re-target requests	Select to enable replacing Request-URI in Forward requests.
Match mode	Select a lookup match mode from the drop-down list. Has no effect when table entries contain ranges.

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

- Configure LDAP.
- 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 tab in the Advanced routing dialog in Basic 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.

- Confirm that the system displays the Basic mode.

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

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

Attributes	Instructions
Name	Enter a unique name to identify this configuration. Valid values are alpha-numeric characters.
State	Select State to enable this configuration. When not selected, the E-SBC does not attempt to establish a connection with any corresponding LDAP server.
LDAP servers	Click **Add**, enter the name of the LDAP server, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another LDAP server, and click **OK**. Repeat, as needed.
SIP interface	Select the SIP interface for this configuration.
Authentication mode	Select the authentication mode for the LDAP bind request from the drop-down list.
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 signalling.
LDAP sec type	Select `None` or `LDAPS` for the type of LDAP security from the drop down list.
LDAP TLS profile	Select a TLS profile for this LDAP configuration.
LDAP transactions	Click **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, operation type, and add LDAP configuration attributes.

4. Click **OK**.
5. 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 the configuration of **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 Subscriber Office (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 Oracle® Enterprise Session Border Controller (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**.

Configure TDM

To perform Time Division Multiplexing (TDM) operations, the Oracle® Enterprise Session Border Controller (E-SBC) requires a profile that specifies the TDM interface.

- Confirm that the E-SBC contains the optional TDM card.
- If you want to enable TDM logging in this procedure, you must enable system logging before you begin.

In the following procedure, the line mode that you specify dictates certain corresponding settings, as noted. For example, when you select 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.

1. From the Web GUI in Basic Mode, click the **Configuration** tab.

   The system displays the TDM icon in the workspace.

2. Double-click the TDM icon.

   The system displays the TDM configuration dialog.

3. In the Tdm-config dialog, click Tdm-profile, and do the following:

Attributes	Instructions
State	Enable or disable TDM.
Logging	Enable or disable TDM logging.
Name	Set the name for this TDM profile.
Line mode	Set either T1 or E1.
Signalling	Do one of the following: • Set pri-net, if you want the TDM card to use the internal clock as the timing source. • Set pri-cpe, if you want the TDM card to use an external clock as the timing source.
Switch type	Set a switch type for this configuration.
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 0, whether the quad span card is present or not.
Line build out	Set a number from 1-13.
Framing value	Set the framing value according to the line mode that you specified for this configuration. • For T1: ESF • For E1: CCF
Coding value	Set the coding value according to the line mode that you specified for this configuration. • For T1: b8zs • For E1: hdb3
Tone zone	Set the tone zone value according to the line mode that you specified for this configuration. • For T1: US • For E1: ES
Rx gain	Set the TDM receive volume in decibels. Maximum: 9.9
Tx gain	Set the TDM transmit volume in decibels. Maximum: 9.9
Echo cancellation	Enable or disable.
Calling-Pres	Enable or disable call IP presentation for a SIP device. When you enable "calling pres," you must also enable "caller ID."

Attributes	Instructions
Caller-ID	Enable or disable caller ID for CLIP and COLP. When you enable "caller ID," you must also enable "calling pres."
Options	When the E-SBC contains the Quad-Span card, set the number of channels that you want to use. Enter number-of-span=<0-4>.

4. Click **OK**.

   The system displays the Set TDM Configuration dialog.

5. Click **Complete**.

   The system completes the TDM configuration and displays the success dialog when done.

6. Click **OK**.

Configure the inbound and outbound TDM local policies.

Configure Outbound Local Policy with TDM Backup

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

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

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

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

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

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

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

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

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

6. Click **OK**.

7. Save the configuration.

Configure Bidirectional Local Policy with TDM Backup

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

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

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

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

   The system displays an arrow in the center of the PBX icon.
4. Drag from the arrow in the center of the PBX icon to the Trunk icon.

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

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

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

Configure Outbound TDM Local Policy - Basic

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

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

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

1. From the Web GUI, click **Configuration**.
2. From the icon toolbar, under Routing, click the one-way arrow icon.

3. Click the center of the TDM icon.

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

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

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

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

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

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

Configure Bidirectional TDM Local Policy

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

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

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

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

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

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

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

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

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

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

Wizards Button

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

The Wizards button provides access to the following configuration wizards.

Configuration Wizard	Purpose
Set boot parameters	Specify the boot file and the boot parameters.
Set entitlements	Set the number of sessions that a license entitles, and enable advanced features.
Set initial configuration	Configure a new system and reconfigure an existing system. Includes configuring High Availability.
Set license	Enter the license number for a feature.
Set logon banner	Customize the text on the Web GUI logon banner.
Set time zone	Select the time zone for the deployment.
Upgrade Software	Upload a new version of the software.

Set Boot Parameters Wizard

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

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

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

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

Attributes	Instructions
Console Baud Rate	Select a console baud rate from the drop-down list.

3. Click **Complete**.

   The system displays a success message.

4. Click **OK**.

Configurable Boot Loader Flags

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

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

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

3. Click **Complete**.

   The system displays a success message.

4. Click **OK**.

Set Initial Configuration Wizard

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

Launch the Set Initial Configuration Wizard

- Unconfigured system. The system launches the Web GUI Set Initial Configuration wizard upon the first logon. When the initial configuration is complete, the system saves the

configuration, activates the configuration, and reboots. The system does not backup the initial configuration of an unconfigured system.

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

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

Selections	Behavior
Enable Web GUI: Yes/No	If you select **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/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/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/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 reboots.

- 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. From the Web GUI, go to **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 reboots.

- (Optional) Reconfigure the system objects.

Set License Wizard

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

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

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

1. From the Web GUI, click **Configuration** > **Wizards** > **Set License**.

2. In the Set License dialog, enter the license serial number in the Add license field.
3. Click **Complete**.

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

Set Logon Banner Wizard

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

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

1. From the Web GUI, click **Configuration** > **Wizards** > **Set Login Banner**.
2. In the Set Login Banner dialog, enter the text that you want to display on the log on page.
3. Click **Complete**.

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

Set Time Zone Wizard

The system requires a setting for time zone.

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

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

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

Upgrade Software Wizard

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

Use the Upgrade Software wizard to perform the following tasks:

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

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

1. From the Web GUI tool bar, click **Wizards**.

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

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

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

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

Settings Button

Use the Settings button to access the following configuration elements.

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

Configuration Element	Purpose
Survivability	Enable remote site survivability and specify the triggering device.

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

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

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

Simple Network Management Protocol

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

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

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

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

Configure SNMP Settings

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

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

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

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

SIP Settings

Session Initiation Protocol (SIP) is an IETF-defined signaling protocol widely used for controlling communication sessions such as voice and video calls over Internet Protocol (IP). The protocol can be used for creating, modifying and terminating two-party (unicast) or multiparty (multicast) sessions. Sessions may consist of one or several media streams.

Dialog Transparency

Dialog transparency prevents the Oracle® Enterprise Session Border Controller (E-SBC) from generating a unique Call-ID and modifying dialog tags. With dialog transparency enabled, the E-SBC is prevented from generating a unique Call-ID and from modifying the dialog tags. The Oracle® Enterprise Session Border Controller passes what it receives. When a call made on one E-SBC is transferred to another UA and crosses a second E-SBC, the second E-SBC does not note the context of the original dialog, and the original call identifiers are preserved end to

end. The signalling presented to each endpoint remains in the appropriate context regardless of how many times a call crosses through a E-SBC or how many E-SBCs a call crosses.

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

IPv6 Reassembly and Fragmentation Support

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

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

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

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

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

Configure SIP Settings

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

- Confirm that the system displays the Basic mode.

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

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

Attributes	Instructions
Enable dialog transparency	Select to enable.
Maximum SIP message length	Enter the maximum SIP message length. Default: 4096. Range: 0-65535.
Allow SIP UDP fragmentation	Select to enable.
Set INVITE expires at 100 responses	Select to enable.
Options	Click **Add**, enter a SIP option, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another media attribute, and click **OK**. Repeat, as needed.

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

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

Attributes	Instructions
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 is the exporter of protocol message traffic and data and the Palladion Mediation Engine is the information collector.

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

Attributes	Instructions
Enable monitoring	Select to enable.
SBC group ID	Enter a number to assign to the E-SBC in its role as an information exporter. Range: 0-999999999.

Attributes	Instructions
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.
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 from 1025-65535. 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.

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

- The active E-SBC checks itself for internal process and IP connectivity issues. If it detects that it is experiencing certain faults, it hands over its role as the active system to the standby E-SBC in the node.
- The standby E-SBC is the backup system, fully synchronized with the active E-SBCsession 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.

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

The standby E-SBCassumes the active role when:

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

High Availability on the Acme Packet 1100

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

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

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

Configure High Availability

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

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

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

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

Configure the Acme Packet 1100 Primary for HA

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

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

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

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

   The system displays the Set initial configuration dialog.

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

Attributes	Instructions
Enable Web GUI	Select **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 reboots.

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

Configure the Acme Packet 1100 Secondary for HA

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

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

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

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

   The system displays the Set initial configuration dialog.

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

Attributes	Instructions
Enable Web GUI	Select **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.
Acquire configuration from primary	Select **Yes**.

3. Click **Complete**

   The system reboots.

Packet Capture Settings

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

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

Option	Result	Packet Trace Command Behavior
Yes	Removes all existing files.	The system captures up to 25 new .pcap files. During the session, the system rotates the files in the /opt/traces directory by size. For example, the system keeps the last 25 files and rotates them when they reach 100 MB
No	Keeps all existing files.	• 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 to which the E-SBC will send captured packets.
- Confirm that the system displays the Basic mode.

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

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

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

3. Click **OK**.
4. Save 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, after you click **Show advanced**. Use the following procedure to enable ths function, specify a triggering device, and optionally change the default settings.

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

Attributes	Instructions
State	Select to enable.
Registration expire time	Enter the time, in seconds, that the E-SBC waits before entering survival mode. Default: 30. Range: 086400.
Extension length	Enter the maximum length allowed for a phone extension. Default: 4. Range :0-10
Trigger on	Select a PBX, Trunk, device, or group from the drop-down list that triggers survivability mode when it goes out of service.

Network Button

Use the Network button to access the following configuration elements.

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

Host Routes

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

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

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

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

Add a Host Route

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

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

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

Attributes	Instructions
Dest network	Enter the IPv4 address of the destination network that this host route points to. Dotted decimal format. For example, 192.30.1.104. No two host-route elements can use the same destination network address.
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 element specifies a logical network interface. In order to use a network port on a network interface, you must configure both the physical interface and the corresponding network interface configuration elements.

Add a Network Interface

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

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

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

Attributes	Instructions
Name	Enter the name of the physical interface with which this network-interface element is linked. For example Enterprise. Network-interface elements that correspond to phy-interface elements with an operation type of Control or Maintenance must start with “wancom.”
Sub port ID	Required only for a VLAN, where the operation type is Media. Enter the identification number from 1-4095 of a specific virtual interface in a physical interface. Otherwise, leave the default 0, which means this element is not using a virtual interface.
Description	Enter a description of this interface for easier identification.
Hostname	(Optional) Enter the hostname of this network interface in FQDN or IP Address format.
IP Address	Enter the IP address of this network interface in IP Address format.
Pri utility address	Enter the utility IP address for the primary High Availability (HA) peer in an HA architecture.
Sec utility address	Enter the utility IP address for the secondary Oracle Communications Session Border Controller in an HA architecture.
Netmask	Enter the netmask portion of the IP address for this network interface entered in IP address format.
Gateway	Enter the gateway this network interface uses to forward packets in IP Address format.
Sec gateway	Enter the gateway to use on the secondary Oracle® Enterprise Session Border Controller (E-SBC) in an HA pair in IP Address format.
Gw heartbeat	Click to display the configuration fields.
State	Select to enable the front interface link detection and polling functionality on the E-SBC.
Heartbeat	Enter the time interval in seconds between heartbeats for the front interface gateway.
Retry count	Enter the number of front interface gateway heartbeat retries before a gateway is considered unreachable.
Retry timeout	Enter the heartbeat retry timeout value in seconds.
Health score	Enter the amount to subtract from the health score if the front interface gateway heartbeat stops responding.
DNS IP primary	Enter the IP address of the primary DNS to be used for this interface.
DNS IP backup 1	Enter the IP address of the first backup DNS to be used for this interface.

Attributes	Instructions
DNS IP backup 2	Enter the IP address of the second backup DNS to use for this interface.
DNS domain	Set the default domain name used to populate incomplete hostnames that do not include a domain in Name format.
DNS timeout	Enter the total time in seconds to elapse before a query (and its retransmission) is sent to a DNS server timeout.
Signalling MTU	Enter the size of the Maximum Transmission Unit for packets leaving this interface. Default-inherits system-wide MTU. IPv4-0, 576-4096. IPv6-0, 1280-4096.
HIP IP list	Add all IPv4 Host Identity Protocol lists for which you want the E-SBC to accept administrative traffic.
FTP address	Enter a list of IP addresses from which FTP traffic can be received and acted upon by a front media interface.
ICMP address	Enter the IP address to pass standard ping packets to the host.
Telnet address	Enter the IP address where port 23 is open for Telnet access.
SSH address	Enter a list of IP addresses from which SSH traffic can be received and acted upon by a front media interface. Requires a valid IPv4 network address.

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

Security Button

Use the Security button to access the following configuration elements.

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

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

Management Button

Use the Management button to access the following configuration elements.

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

Configure Call Accounting

- Confirm that the system displays the Basic mode.

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

Attributes	Instructions
Strategy	Select the lookup algorithm from the drop-down list for the accounting server.
Protocol	Select a protocol from the drop-down list.
State	Select to enable call accounting.
Generate start	Select an event trigger from the drop-down list for session accounting recording .
Generate interim	Click **Add**, select an event to collect in a session, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another media attribute, and click **OK**. Repeat, as needed. Default: Reinvite-Response.
Generate event	Click **Add**, select a Diameter event to collect in a session, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another media attribute, and click **OK**. Repeat, as needed. 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**, enter an option, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another media attribute, and click **OK**. Repeat, as needed.

Attributes	Instructions
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** > **Show advanced**, 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 Namer. **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**, select an interim state ID type, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another media attribute, and click **OK**. Repeat, as needed.

Attributes	Instructions
Account servers	Click **Add** > **Show advanced**, 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 Diametger manipulation to apply. **k.** Diameter out manip. 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.

Attributes	Instructions
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 srvc ctx mnc mcc	Enter the Mobile Country Code / Mobile Network Code tuple. Format: MNC.MCC.
Diam srvc ctx ext	Enter the operator-specific extension information.
Diam srvc attr ID range	Enter a comma delimited range of Acme accounting attributes to include in Diameter Rf accounting records. **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. From the Web GUI, click **Configuration** > **Management** > **SNMP community**.
2. On the SNMP community page, click **Add**, and do the following:

Attributes	Instructions
Community name	Enter an SNMP community name of an active community where this E-SBC can send and receive SNMP information.
Access mode	Select the access level for all Network Management Systems (NMS) defined within this SNMP community.
IP address	Click **Add**, enter an Pv4 address that is valid within this SNMP community, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another media attribute, and click **OK**. Repeat, as needed.

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

Attributes	Instructions
IP address	Enter the IPv4 address and port number of an authorized NMS in dotted decimal format. Default: 0.0.0.0:162.
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.

Attributes	Instructions
Community name	Enter the SNMP community name to which this trap receiver belongs.
User list	Click **Add**, enter the name of a user allowed to receive secure traps, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another media attribute, and click **OK**. Repeat, as needed. **Note:** If SNMPv3 is enabled on the E-SBC, and no users are listed for this field, the system displays a warning message during a verify-config execution.

4. Click **Close**.
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.

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

Configure a Web Server

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

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

Attributes	Instructions
State	Select to enable Web server.
Inactivity timeout	Enter the number of minutes you want the Web server to wait before timing out. Range: 0-20.

Attributes	Instructions
HTTP state	Select to enable HTTP connection to the Web server.
HTTP port	Enter the HTTP port number. Default: 80. Range: 1-65535.
HTTPS state	Select to enable HTTPS connection to the Web server.
HTTPS port	Enter the HTTPS port number. Default: 443. Range: 1-65535.
TLS profile	Select a TLS profile to use for HTTPS from the drop-down list.

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

Other Button

Use the Other button to access the following configuration elements.

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

Configure Media Profile

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

In the following procedure, you can configure:

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

1. From the Web GUI, click **Other** > **Media profile**.
2. On the Media profile page, click **Add** > **Show advanced**, and to the following.

Attributes	Instructions
Name	Enter the name for this media profile. For example, PCMU, G723, G729. Valid values are alpha-numeric characters.
Subname	Enter the encoding subname used for the Codec variation. Valid values are alpha-numeric characters. You must use a combination of alpha and numeric characters.

Attributes	Instructions
Media type	Enter the media type to use in SDP m lines. For example, audio, video, data.
Payload type	Enter the payload type to use in SDP media lines. Valid values are alpha-numeric characters. **Note:** The Payload type value must be numeric if you use the RTP/AVP transport method.
Transport	Enter the transport protocol to use in the SDP RTPMAP attribute. Default: RTP/AVP. Valid values are: • RTP/AVP • UDP
Clock rate	Enter the clock rate to use in the SDP RTPMAP attribute in Hz. For example, 8000 in narrowband Codecs and 16000 in wideband Codecs. Range: 0=4294967295. **Note:** When configured with 0, the default, the system uses the clock rate for the Codec.
Res bandwidth	Enter the amount of bandwidth required in Kilobits. Range: 0-999999999.
Frames per packet	Enter the maximum number of frames per packet. Range: 0-256.
Parameters	Click **Add**, enter the parameter, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another media attribute, and click **OK**. Repeat, as needed. **Note:** For each parameter, use the + character to add and the - character to remove. For example, +silenceSupression=0.

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

Attributes	Instructions
ID	Enter a descriptive ID name for this translation rule. Valid values are alpha-numeric characters.
Type	Select the one of the following translation rules that you want to configure 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: 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 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.

Attributes	Instructions
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 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.

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

Configure SIP Features

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

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** > **Other** > **Sip Features**.
2. On the Sip feature page, click **Add**, and do the following:

Attributes	Instructions
Name	Enter the action tag name to display in the Require, Supported, and Proxy-Require headers of SIP messages.
SIP interface	Do one of the following: • Select the SIP interface 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.

Attributes	Instructions
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.

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

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 Manipulations 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 a global procedure that leads you to a separate procedure for each particular header and header element that you want to manipulate.

To begin, start with the "Configure SIP Manipulations" procedure. When you reach the "Cfg Rules" section in the procedure, click **Add** to see a list of the header rules that you can create. For further instructions, refer to the following topics for the header rule and corresponding header element rule that you want to create. Note that creating a header element rule within a header rule is optional.

- Configure Header Rule

- Configure MIME Rule
- Configure MIME ISUP Rule
- Configure MIME SDP 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 this 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.
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.

Attributes	Values and Descriptions
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.
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.

Attributes	Values and Descriptions
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.

Attributes	Values and Descriptions
New value	The value for a new element or replacement a value for an existing element. You can enter an expression that includes a combination of absolute values, pre-defined parameters, and operators. • Absolute values—Use double quotes for clarity. You must escape all double quotes and back slashes that are part of an absolute value, and enclose the absolute value in double quotes. • Pre-defined values.—Pre-defined parameters always start with a $. For valid values, see the Pre-dedfined Parameters table. • Operators parameters—For valid values, see the Operators table. The following table describes the pre-defined parameters.

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

The following table describes the Operators.

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

Attributes	Values and Descriptions
	<table><tr><th>Operator</th><th>Description</th></tr><tr><td></td><td>generates 2311</td></tr></table>
Parameter name	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.
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 Manipulations

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. From the Web GUI, click **Configuration** > **Other** > **Sip manipulations**.
2. In the SIP manipulation dialog, click **Add**, and do the following.

Attributes	Instructions
Name	Enter the exact name of the header to which this rule applies. Alpha-numeric. No spaces. Case-sensitive.
Description	Enter a description of the purpose of this set of rules. Alpha-numeric.
Split headers	Create a list of headers that you want the system to split and treat separately before executing any manipulation rules. Click **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.

Attributes	Instructions
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, click **Close**.
4. Save the configuration.

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

Configure Header Rule

You can configure SIP header manipulations on the Oracle® Enterprise Session Border Controller (E-SBC) from the "CfgRules" section in the "Configuring SIP Manipulations" procedure.

- Begin the "Configure SIP Manipulations" procedure and complete the items in the Add SIP manipulation dialog prior to "CfgRules."

The following procedure is the continuation of the "Configure SIP Manipulations" procedure. It begins with adding header-rule to "CfgRules" and includes the optional element-rule sub-element configuration.

1. From the "CfgRules" section of the SIP manipulation configuration page, click **Add**, and select header-rule from the list.
2. In the SIP manipulation / Header rule dialog, do the following.

Attributes	Instructions
Name	Enter a unique name for this rule set. Alpha-numeric.
Header name	Enter the name of the header to which this rule applies. Case-sensitive.
Action	Select an action from the drop-down list for the header rule.
Comparison type	Select a comparison type from the drop-down list to use for the match value.
Msg type	Select the message type from the drop-down list to which this rule applies.

Attributes	Instructions
Methods	(Optional) Create a list of methods to which this rule applies. For example, INVITE, ACK, CANCEL. When no methods are listed, this rule applies to all methods. Click **Add**, enter the method, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another method, and click **OK**. Repeat, as needed.
Match value	Enter the value to match against the current object.
New value	Enter the new value for the object. You must escape quoted display names within quotes. For example, \"MyName\".
CfgRules	(Optional) Click **Add** > **element-rule**, and do the following. • Name. Enter a unique name for this header element rule. • Parameter name. Enter a parameter to which to apply the rule. • Type. Select an element type from the drop-down list to which to apply the rule. • Action. Select an action from the drop-down list to apply to the element rule. • Match val type. Select a value 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. Case-sensitive. • 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 / Header rule page. Do one of the following: • Add another element-rule. • Finish the Header rule configuration by completing steps 3-6.

3. Click **OK**.

   The system displays the Add SIP manipulation page.

4. Click **OK**.

   The system displays the SIP manipulation page.

5. Click **Close**.

6. Save the configuration.

Configure MIME Rule

You can configure a Multi-Purpose Internet Mail Extensions (MIME) data files exchange profile on the Oracle® Enterprise Session Border Controller (E-SBC) from the "CfgRules" section in the "Configuring SIP Manipulations" procedure.

- Begin the "Configure SIP Manipulations" procedure and complete the items in the Add SIP manipulation dialog prior to "CfgRules."

The following procedure is the continuation of the "Configure SIP Manipulations" procedure. It begins with adding mime-rule to "CfgRules" and includes the optional mime-rule sub-element configuration.

1. From the "CfgRule"s section of the SIP manipulation configuration page, click **Add**, and select mime-rule from the list.
2. In the SIP manipulation / Mime rule dialog, click **Show advanced**, and do the following.

Attributes	Instructions
Name	Enter a unique name for this rule.
Content type	Enter the name of the content-type header to which to apply this rule.
Msg type	Select the message type from the drop-down list to which this rule applies.
Methods	(Optional) Create a list of methods to which this rule applies. For example, INVITE, ACK, CANCEL. When no methods are listed, this rule applies to all methods. Click **Add**, enter the method, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another method, and click **OK**. Repeat, as needed.
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.
Comparison type	Select a comparison type from the drop-down list to use for the match value.
Match value	Enter the value to match against the current object.
New value	Enter the new value for the object. You must escape quoted display names within quotes. For example, \"MyName\".

Attributes	Instructions
CfgRules (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 rule dialog. Do one of the following: • Add another mime-header-rule. • Finish the MIME rule configuration by completing steps 3-6.

3. Click **OK**.

   The system displays the Add SIP manipulation page.

4. Click **OK**.

   The system displays the SIP manipulation page.

5. Click **Close**.

6. Save the configuration.

Configure MIME ISUP Rule

You can configure a Multi-Purpose Internet Mail Extensions (MIME) - ISDN User Part (ISUP) signalling profile on the Oracle® Enterprise Session Border Controller (E-SBC) from the "CfgRules" section in the "Configuring SIP Manipulations" procedure.

- Begin the "Configure SIP Manipulations" procedure and complete the items in the Add SIP manipulation dialog prior to "CfgRules."

The following procedure is the continuation of the "Configure SIP Manipulations" procedure. It begins with adding mime-isup-rule to "CfgRules" and includes the optional mime-header-rule and isup-param-rule sub-element configurations.

1. From the "CfgRules" section of the SIP manipulation configuration page, click **Add**, and select mime-isup-rule from the list.

2. In the SIP manipulation / Mime isup rule dialog, click **Show advanced**, and do the following.

Attributes	Instructions
Name	Enter a unique name for this rule.

Attributes	Instructions
Content type	Enter the name of the content type header to which to apply this rule.
Isup spec	Select an ISUP encoding specification from the drop-down list for the ISUP body.
Isup msg types	(Optional) Create a list of one or more ISUP message types to which the mime-isup rule applies. For example, IAM, ACM. When no methods are listed, this rule applies to all types. Click **Add**, enter the message type, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another message type, and click **OK**. Repeat, as needed.
Msg type	Select the message type from the drop-down list to which this rule applies.
Methods	(Optional) Create a list of methods to which this rule applies. For example, INVITE, ACK, CANCEL. When no methods are listed, this rule applies to all methods. Click **Add**, enter the method, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another method, and click **OK**. Repeat, as needed.
Action	Select an action from the drop-down list for the header rule.
Comparison type	Select a comparison type from the drop-down list to use for the match value.
Match value	Enter the value to match against the current object.
New value	Enter the new value for the object. You must escape quoted display names within quotes. For example, \"MyName\".

Attributes	Instructions
CfgRules (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 isup rule dialog. Do one of the following: • Add another mime-header-rule. • Add an isup-param-rule, using the steps in the corresponding table cell. • Finish the MIME ISUP rule configuration by completing steps 3-6.
CfgRules (instructions for configuring isup-param-rule)	(Optional) Click **Add** > **isup-param-rule** > **Show advanced**, 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. • 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 isup rule dialog. Do one of the following: • Add another isup-param-rule. • Add an mime-header-rule, using the steps in the corresponding table cell. • Finish the MIME ISUP rule configuration by completing steps 3-6.

3. Click **OK**.

   The system displays the Add SIP manipulation page.

4. Click **OK**.

   The system displays the SIP manipulation page.

5. Click **Close**.

6. Save the configuration.

Configure MIME SDP Rule

You can configure a Multi-Purpose Internet Mail Extensions (MIME) - Session Description Protocol (SDP) multimedia communications session profile on the Oracle® Enterprise Session Border Controller (E-SBC) from the "CfgRules" section in the "Configuring SIP Manipulations" procedure.

- Begin the "Configure SIP Manipulations" procedure and complete the items in the Add SIP manipulation dialog prior to "CfgRules."

The following procedure is the continuation of the "Configuring SIP Manipulations" procedure. It begins with adding the mime-sdp-rule to "CfgRules" and includes the optional mime-header-rule, sdp-session-rule, sdp-media-rule, and sdp-line-rule sub-element configurations.

In step 2 of this procedure, you can configure as few or as many of the "CfgRules" sub-element options that you want.

- If you do not configure an optional sub-element, proceed to step 3.
- If you configure an optional sub-element, you can configure another one or proceed to step 3.

1. From the "CfgRules" section of the SIP manipulation configuration page, click **Add**, and select mime-sdp-rule from the list.
2. In the SIP manipulation / Mime sdp rule dialog, do the following.

Attributes	Instructions
Name	Enter a unique name for this rule.
Msg type	Select the message type from the drop-down list to which this rule applies.
Methods	(Optional) Create a list of methods to which this rule applies. For example, INVITE, ACK, CANCEL. When no methods are listed, this rule applies to all methods. Click **Add**, enter the method, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another method, and click **OK**. Repeat, as needed.
Action	Select an action from the drop-down list for the header rule.
Comparison type	Select a comparison type from the drop-down list to use for the match value.
Match value	Enter the value to match against the current object.

Attributes	Instructions
New value	Enter the new value for the object. You must escape quoted display names within quotes. For example, \"MyName\".
CfgRules (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 corresponding table cells. • Finish the MIME SDP rule configuration by completing steps 3-6.

Attributes	Instructions
CfgRules (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. • Finish the MIME SDP rule configuration by completing steps 3-6.

Attributes	Instructions
CfgRules (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. • 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 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. • Configure the mime-header-rule and sdp-sesison-rule options, using the steps in the corresponding table cells. • Finish the MIME SDP rule configuration by completing steps 3-6.

3. Click **OK**.

   The system displays the Add SIP manipulation page.

4. Click **OK**.

   The system displays the SIP manipulation page.

5. Click **Close**.

6. Save the configuration.

Add an SPL

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

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

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

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

Attributes	Instructions
Spl options	Enter the name of SPL option.
Plugins	Click **Add**, and do the following: • Select State to enable the plugin. • Enter the name of plugin to load. • Click **OK**. The system displays the SPl config page.

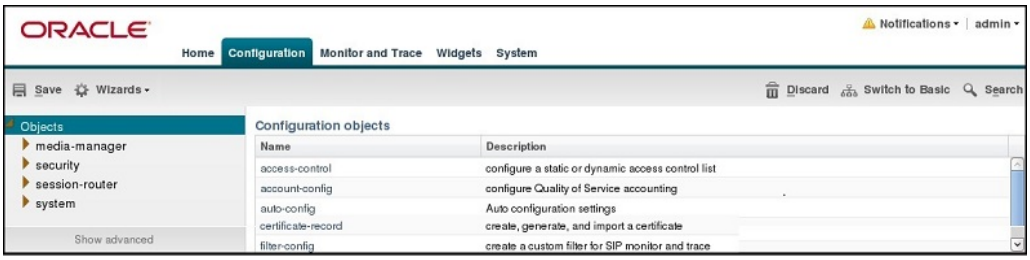
3. Click **OK**.
4. Save the configuration.

5

Expert Mode Configuration

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

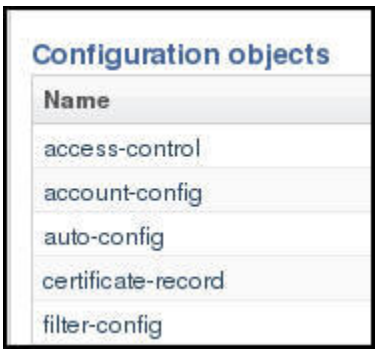
The Expert mode workspace displays a list of configuration objects and elements in the left pane of the configuration page, grouped like the ACLI configuration tree and displayed in command line format. The Configuration page also lists all of the configuration objects and elements in alphabetical order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



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

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

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

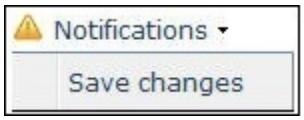
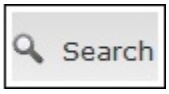


Note:

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

Expert Mode Configuration tools

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

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

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

Function Buttons

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

Button	Description
Add	Use to add configuration information to the Oracle® Enterprise Session Border Controller.
Edit	Use to edit existing configuration information. Note: Select an item in a list to enable the Edit button.
Clear	Use to clear the Search field.
Copy	Use to copy existing configuration information, and edit the information to create a new configuration. Note: Select an item in a list to enable the Copy button.
Delete	Use to delete a single entry from a list. Note: Select an item in a list to enable the Delete button.
Delete All	Use to delete all instances in the top-level object of a multi-instance object.
Download	Use to save and download a configuration file in the .csv format. Displays only in a multi-instance object.
Search	Use to search for configured objects.
Upload	Use to upload a .csv file. Displays only in a multi-instance object.

Media Manager Configuration

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

Object	Purpose
codec-policy	Create a codec policy to specify allowed codecs, the order of codecs, and codecs to add on egress.

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

Note:

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

Codec Policy Configuration

When configuring transcoding, you must 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. From the Web GUI, click **Configuration** > **media-manager** > **codec-policy**.
2. On the Add Codec policy page, do the following:

Attributes	Instructions
Name	Enter a unique name for this policy.
Allow codecs	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 (( )).
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
Force ptime	Select to force a specified packetization time on the egress offer.
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 detection	Select to enable tone detection.
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.

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. From the Web GUI, click **Configuration** > **media-manager** > **Show advanced** > **dns-alg-constraints**.
2. On the DNS ALG Constraints page, click **Add**.
3. On the Add DNS ALG Constraints page, click **Show advanced**, and do the following:

Attributes	Instructions
Name	Enter a unique name for this constraint.
State	Select to enable.
Max burst rate	Range: 0-4294967295 requests per second. 0 = unlimited.
Max sustain rate	Range: 0-4294967295 requests per second. 0 = unlimited.
Max inbound burst rate	Range: 0-4294967295 requests per second. 0 = unlimited.
Max inbound sustain rate	Range: 0-4294967295 requests per second. 0 = unlimited.
Max outbound burst rate	Range: 0-4294967295 requests per second. 0 = unlimited.
Max outbound sustain rate	Range: 0-4294967295 requests per second. 0 = unlimited.
Time to resume	Range: 0-4294967295 seconds to wait after the constraints are exceeded to resume monitoring the constraints . 0 = unlimited.
Burst rate window	Range: 0-4294967295 seconds over which to compute the burst rate. 0 = unlimited.
Sustain rate window	Range: 0-4294967295 seconds over which to compute the sustain rate. 0 = unlimited.
Max latency	Range: 0-4294967295 seconds maximum time for the round trip. 0 = unlimited.

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

Attributes	Instructions
Client realm	Select the realm from the drop-down list from which the system receives DNS queries.
Description	Enter a description of this configuration.
Constraint name	Select a DNS-ALG constraint from the drop-down list to apply to this configuration.
Trap on status change	Select to enable.
Extra dnsalg stats	Select to enable.
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, and click **OK**. Repeat as needed. Click **Back**. Click **Back**.

3. Save the configuration.

Configure Media Manager

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

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

Attributes	Instructions
State	Select to enable Media Manager.
Flow time limit	Enter the time limit, in seconds, for a media flow. Range: 0-4294967295.
Initial guard timer	Enter the time limit, in seconds, for a media flow guard timer. Range: 0-4294967295.
Subsq guard timer	Enter the time limit, in seconds, for a subsequent media flow guard timer. Range: 0-4294967295.
TCP flow time limit	Enter the time limit, in seconds, for a TCP flow. Range: 0-4294967295.
TCP initial guard timer	Enter the time limit, in seconds, for the initial TCP flow. Range: 0-4294967295.
TCP subsq guard timer	Enter the time limit, in seconds, for a subsequent TCP flow. Range: 0-4294967295.
Hnt rtcp	Select to enable RTCP for hosted NAT traversal.
Algd log level	Select an ALGD log level from the drop-down list.
Mbcd log level	Select an MBCD log level from the drop-down list.
Options	Add any optional parameters.
Red max trans	Enter the number of redundancy sync transactions to keep. Range: 0-50000.
Red sync start time	Range: 0-4294967295.
Red synch comp time	Range: 0-4294967295.
Media policing	Select to enable per session traffic rate policing in a media gateway.
Max untrusted packet rate	Enter the maximum untrusted signaling bandwidth allowed to the host path in bytes per second. Range: 20-200000.
Max trusted packet rate	Enter the maximum trusted signaling bandwidth allowed to the host path in bytes per second. Range 20 to 200000.
Max arp packet rate	Enter the maximum bandwidth that can be used by an ARP message. Range: 20 to 10000.
Tolerance window	Range: 0-4294967295.
Trap on demote to deny	Select to generate a trap when the endpoint is demoted from untrusted to deny.
Trap on demote to untrusted	Select to generate a trap when the endpoint is demoted from trusted to untrusted.
Syslog on demote to deny	Select to generate Syslog when the endpoint is demoted from untrusted to deny.
Syslog on demote to untrusted	Select to generate Syslog when the endpoint is demoted from trusted to untrusted.
Anonymous sdp	Select to enable the Use Name and Session Name fields in Session Description Protocol (SDP).
Translate non rfc283 event	Select to accept UII/INFO events for Inter-working Function (IWF), although RFC2833 is preferred.
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 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. From the Web GUI, click **Configuration** > **media-manager** > **media-policy**.
2. On the media policy page, click **Add**.
3. On the Add media policy page, do the following:

Attributes	Instructions
Name	Enter a name for this media policy.
TOS settings	Click **Add**.

Attributes	Instructions
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. • 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, enclose the entry in quotation marks, for example, "<attribute>". Do one of the following: – Click **OK**. – Click **Apply/Add another**, add another media attribute, and click **OK**. Repeat, as needed.

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

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

Attributes	Instructions
Identifier	Enter the name of the realm.
Description	Enter a description of this realm.

Attributes	Instructions
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.
Srtp msm passthrough	Select to enable the inclusion of information for multi-system SRTP passthrough.
Class profile	Enter the name of class-profile to use for this realm for ToS marking.
In translationid	Enter the name of a session-translation element. Only one is allowed.
Out translationid	Enter the name of a session-translation element. Only one is allowed.
Average rate limit	Enter the average data rate limit in bytes per second.
Access control trust level	Select a trust level for the host within the realm.
Invalid signal threshold	Enter the allowed invalid signalling message rate within the tolerance time period.
Maximum signal threshold	Enter the allowed signalling message rate within the tolerance time period.
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.

Attributes	Instructions
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 optional features and parameters. Click **Add**, and enter an option. Do one of the following: • Click **OK**. • Click **Apply/Add another**, add another media attribute, and click **OK**. Repeat, as needed.
SPL options.	Enter SPL options. Click **Add**, and enter an SPL option. Do one of the following: • Click **OK**. • Click **Apply/Add another**, add another media attribute, and click **OK**. Repeat, as needed.
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.
Refer notify provisional	Select provisional mode for sending a NOTIFY message from the drop down list.
Dyn refer term	Select to enable terminating refer call transfer for this realm.
Codec policy	Select the codec policy mode for this realm from the drop down list.
Codec manIP in realm	Select to enable codec manipulation support for this realm.
Codec manIP in network	Select to enable codec policy in this network.
RTCP policy	Select the RTCP policy for this realm.
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.

Attributes	Instructions
TCP media profile	Select a TCP media profile for this realm.
Monitoring filters	Add a comma-separated list of monitoring filters for this realm.
Node functionality	Select a node function from the drop down list.

3. Click **OK**.
4. Save 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. From the Web GUI, click **Configuration** > **media-manager** > **steering-pool**.
2. On the Steering pool page,. do the following:

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

Security Configuration

The Oracle® Enterprise Session Border Controller (E-SBC) can provide security for VoIP and other multi-media services. E-SBC security includes access control, DoS attack, and overload protection, which help to secure service and protect the network infrastructure. E-SBC security lets legitimate users place a call during attack conditions, while protecting the service itself.

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

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

Note:

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

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 table lists the actions that the system records.

Source	Actions Recorded
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.
Widgets tab	• Export from a Widget. • Add a Widget to favorites. • Clear, clear all on alarm, add, and delete license.
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.
Monitor and Trace tab	• Export the summary. • Export the session detail.

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 table describes each value written to an audit log event.

Log Element	Information Provided
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

Log Element	Information Provided
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. When you click File Management, the system displays the File Type drop-down list, which includes "Audit Log" as a selection.

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. From the Web GUI, click **Configuration** > **Security** > **Public key**.
2. On the Public Key page, click **Add**.
3. In the Add Public Key dialog, do the following:

Attributes	Instructions
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.

Attributes	Instructions
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. Log on to the E-SBC, and click **Configuration** > **Security** > **Admin-Security** > **Audit Logging**.
2. On the Audit Logging page, do the following:

Attributes	Instructions
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. Range: 0-65535. Default: 720. **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. Range: 0-32. Default: 32. • Minimum: 0 • Maximum: 32 (default)
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. range; 0-99. Default: 75. **Note:** 0 disables this parameter.

Attributes	Instructions
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. Range 0-10. Default: 5. **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. Range: 1-65535. Default: 22 • 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 element.

Configuration > **security** > **admin-security** > **ssh-config**.

2. In **ssh-config**, do the following:

Parameter	Instructions
rekey interval	Set the time in minutes after which the E-SBC rekeys an SSH or SFTP session. Range: 60-600. Default: 60.
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. Range: 20-31. Default: 31.
proto neg time	Set the time in seconds to complete the SSH protocol negotiation, establishing the secure connection. Range: 30-60. Default: 60.
keep alive enable	Enable the TCP keepalive timer. Valid Values: enabled | disabled. Default: enabled.
keep alive idle timer	Set the interval in seconds between the last data packet sent and the first keepalive probe. Range: 15-1800. Default: 15.
keep alive interval	Set the interval in seconds between two successful keepalive transmissions. Range: 15-120. Default: 15.
keep alive retries	Set the number of retransmission attempts before the E-SBC declares the remote end unavailable. Range: 2-10. Default: 2.

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 TACACS+, you enable TACACS+ client services and specify one or more TACACS+ servers.

1. Access the Login Authentication configuration object.

   Configuration > **Security** > **Login Authentication**.

2. On the Modify Authentication page, do the following:

Attributes	Instructions
Source port	Range: 1645-1812. Default: 1812.
Type	Select TACACS from the drop-down list.
Protocol	Select acsii for the authentication protocol.

Attributes	Instructions
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	Click **Add**, and do the following to add one or more authentication management servers: **a.** Enter the IP address of a management server. **b.** (Optional) Click **Apply / Add Another**. **c.** **OK**.
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. Range: 1025-65535. Default: 49. **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. Range: 10-10000 seconds. Default: 10. **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 dialogs available from the Security button allow you to perform the first two steps. You apply TLS profiles to SIP interfaces using controls within the SIP Interface dialog.

Certificate Configuration Process

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

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

Add a Certificate Record

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

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 object.

   Configuration > **security** > **admin-security** > **certificate-record**.
2. On the Certificate record page, click **Add**.
3. On the Add certificate record page, click **Show advanced**, and do the following:

Attributes	Instructions
Name	Enter the name of this certificate record.
Country	Enter the country name abbreviation. For example, CA for Canada. Range: 2 characters.
State	Enter the region abbreviation. For example, QC for Quebec. Range: 2 characters.
Locality	Enter the name of the locality in the region. For example, Quebec City. Range:1-128 characters.
Organization	Enter the name of the organization. For example, Office of Information Technology. 1-64 characters.

Attributes	Instructions
Unit	Enter the name of the unit in the organization. For example, Global Network Security. 1-64 characters.
Common name	Enter the common name for the certificate record. For example, your name. Range: 1-64 characters.
Key algor	Set a key algorithm. Valid algorithms: rsa | ecdsa.
Digest algor	Set a digest algorithm. Valid values: sha1 | sha256 | sha384.
Key size	For the RSA key algorithm, set the RSA key size. Valid key size: 512 | 1024 | 2048 | 4096.
Ecdsa key size	For the ECDSA key algorithm, set the ECDSA key size. Valid key size: p256 | p384.
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	Click **Add** and select a key that you want to use with this certificate record from the drop-down list, and do one of the following: • Click **OK**. • Click **Apply/Add Another**, add another key , and click **OK**. Repeat as needed. 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	Click **Add**, select an extended key that you want to use with this certificate record from the drop-down list, and do one of the following: • Click **OK**. • Click **Apply/Add Another**, add another extended key, and click **OK**. Repeat as needed. 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*.
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 from the GUI

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

- Confirm that the certificate record exists.

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

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

   The system displays a list of certificate records.
2. Select the certificate record for the device.
3. Click **Generate**.

   The system creates the request and displays it in a dialog.
4. Copy the information from the dialog and send it to your CA as a text file.

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

Import a Certificate

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

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

1. From the Web GUI, click **Configuration** > **security** > **certificate record** .
2. Select the certificate record for the device.
3. Click **Import**.

   The system displays a dialog from which you can import the certificate.
4. Select one of the following format types from the **Format** drop down list:
   - pkcs7
   - x509
   - Try-all. The system tries all possible formats until it can import the certificate.
5. Browse to the certificate file, and select the certificate to import.
6. Click **Import**.

   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.

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

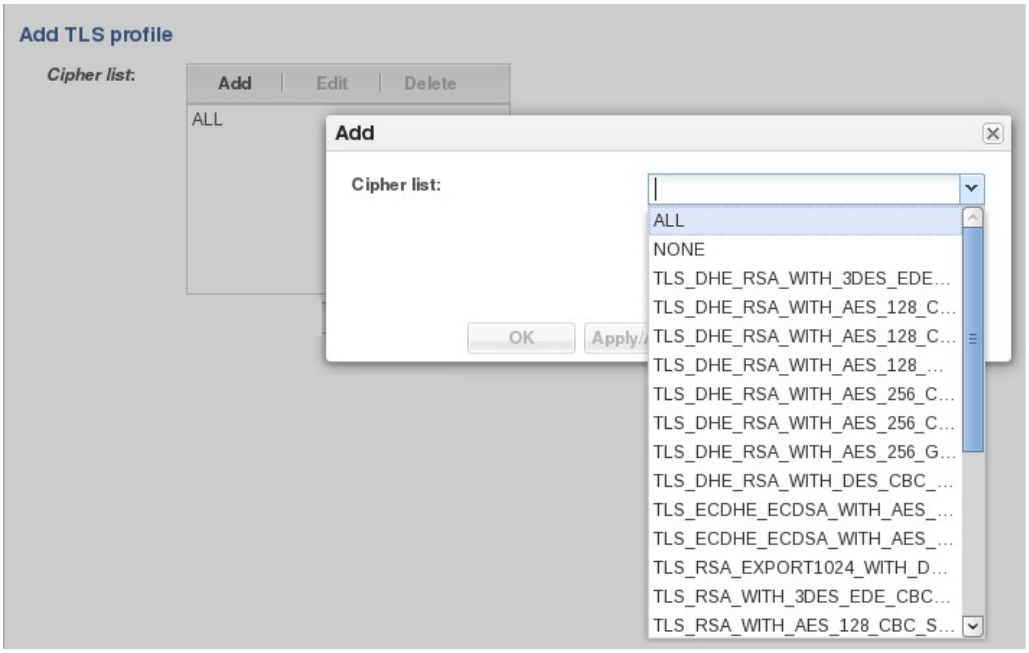
The Oracle® Enterprise Session Border Controller (E-SBC) supports full control of selecting the ciphers that you want to use for Transport Layer Security (TLS). The system defaults to ALL for the Cipher List parameter in the TLS Profile configuration. Oracle recommends that you delete ALL and add only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

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 and TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 are suite B-based ciphers.



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

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

4. Click **OK**.
5. Save 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 tls-global session caching to allow the Oracle® Enterprise Session Border Controller (E-SBC) to cache the session identifier for possible re-connection with a former client.

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

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

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

Configure an SPL Plugin

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

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

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

1. From the Web GUI, click **Configuration** > **system** > **spl-config**.
2. On the spl config / plugins page, do the following:

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

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

- Execute the SPL plugin 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:

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

Object	Purpose
session-agent	Configure and enable a session agent.
session-constraints	Configure and enable session constraints.
session-group	Configure a session agent group.
session-recording-group	Configure a session recording server group.
session-recording-server	Configure and enable a session recording server.
session-timer-profile	Configure a session timer profile.
session-translation	Configure the translation rules for calling and called numbers.
sip-advanced-logging	Configure logging of specific SIP requests by criteria.
sip-config	Configure and enable signaling and session management.
sip-feature	Configure SIP option tag parameters.
sip-interface	Configure and enable a SIP interface.
sip-manipulation	Configure SIP manipulation.
sip-monitoring	Configure and enable SIP monitor and trace features.
surrogate-agent	Configure a surrogate agent.
survivability	Configure and enable survivability.
translation-rules	Configure and apply session translation rules to an agent and a realm.

Note:

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

Configure Access Control

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

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

Attributes	Instructions
Realm ID	Enter the ingress realm of traffic destined to the host to apply this ACL.
Description	Type a brief description of this access-control configuration element.
Source address	Enter the source address, net mask, port number, and port mask to specify traffic matching for this ACL.

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

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

Dynamic ACL for the HTTP-ALG

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

When the dynamic ACL option is enabled, the static flow for the public listening socket defined in **http-alg > public** is created with at trust level set to **untrusted**. Each listening socket creates and manages its ACL list, which allows the listening socket to keep track of the

number of received and invalid messages, the number of connections per endpoint, and so on. You can configure a different setting for each **http-alg** object.

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

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

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

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

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

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

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

Enable Dynamic ACL for the HTTP ALG

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

- 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. On the Add http-alg page, click **Show advanced**.
4. In the Add http-alg dialog, do the following:

Attributes	Instructions
Name	Enter a name for this ACL.
State	Select State to enable this ACL.
Description	Enter a description of this ACL.
Realm id	Select the private realm to which to apply this ACL from the drop down list.
Address	Enter the IP address of the selected private realm.
Destination address	Enter the destination IP address.
Destination port	Enter the destination port. Range:1-65535. Default: 80.
TLS profile	Enter TLS profile to apply from the drop-down list.
Realm id	Select the public realm identifier from the drop down list.
Address	Enter the IP address of the selected public realm.
Port	Enter the listening port number. Range:1-65535. Default: 80.
TLS profile	Select a TLS profile to apply from the drop-down list.
Session-manager-mapping	Not applicable to this procedure.
Dynamic ACL	Select to enable dynamic ACL creation on SIP messages.
Max incoming conns	Enter a number for the maximum allowed incoming HTTP connections. Range: 0-4294967295.
Per src IP max incoming conns	Enter a number for the maximum allowed incoming connections per registered IP address. Range: 0-4294967295.

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

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

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

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

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

Accounting Configuration

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

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

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

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

Configure Call Accounting

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

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

Attributes	Instructions
Strategy	Select the lookup algorithm for the accounting server.
Protocol	Select RADIUS or Diameter.
State	Select to enable call accounting.

Attributes	Instructions
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 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 element to specify where and when you want the system to send accounting messages, and the strategy for selecting account servers. Use the following procedure to configure the minimum settings required for RADIUS call accounting.

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

Attributes	Instructions
Strategy	Select the strategy from the drop down list to use for selecting the server to which the E-SBC sends accounting messages.
Protocol	Select RADIUS from the drop down list.
State	Select to enable the call accounting configuration.
File output	Select to enable the system to store the .csv file locally.
File rotate time	Enter the number of minutes from 1-2147483647.
Options	(Optional) Click **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 Signalling Services" in the*ACLI Configuration Guide* for descriptions.

1. Access the h.323-config object.

   Configuration > **session-router** > **h323** > **h323-config**.

2. On the Add h3232 config page, do the following:

Attributes	Instructions
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 (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 IP address of the session manager and the public 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. From the Web GUI, go to **Configuration** > **session-router** > **http-alg**.
2. On the http-alg page, click **Show advanced** > **Add**.
3. In the Add http-alg dialog, enter the information in the fields and make the selections for the deployment.
4. Click **OK**.

   The system lists the new map on the http-alg page.
5. Save the configuration.

Configure IWF

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

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

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

Attributes	Instructions
State	Select to enable IWF.
Media profiles	Select the media profiles that you want to use for IWF translations.
Logging	Select to enable logging SIP messages related to the IWF.
Add reason hdr	Select to enable SIP-H323 Add Reason header for SIP.
Slow start no sdp in invite	Select to enable no offer SDP in INVITE for slow start H.323.
Options	Click **Add**, and enter an optional feature or parameter. Do one of the following: • Click **OK**. • Click **Apply/Add another**, add another feature or parameter, and click **OK**. Repeat, as needed.
Forward source call address	Select to enable adding the h225SourceCallSignalAddress IP for IWF to outgoing 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 Expert 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, click **Show advanced**, and do the following:

Attributes	Instructions
Name	Enter a unique name to identify this configuration. Valid values are alpha-numeric characters.
State	Select State to enable this configuration. When not selected, the E-SBC does not attempt to establish a connection with any corresponding LDAP server.

Attributes	Instructions
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 signalling.
LDAP sec type	Select `None` or `LDAPS` for the type of LDAP security from the drop down list.
LDAP TLS profile	Select a TLS profile for this LDAP configuration.
LDAP transactions	Click **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. The local policy specifies the protocol the

Use the local-policy element to configure where signalling 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 Add local-policy page, click **Show advanced**, and do the following:

Attributes	Instructions
From address	Click **Add**, and 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	Click **Add**, and 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	Click **Add**, and 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.
Policy priority	Select the policy priority for this local policy from the drop-down list. The default is none.

Attributes	Instructions
Policy attributes	Click **Add** > **Show advanced**, and do the following: • Next hop. Select the signaling host IP address, SAG, hostname, or ENUM config from the drop-down list. • 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. • 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. Enter a number from 0-9999999. • State. Select to enable. • App protocol. Select the application protocol for signalling the session agent from the drop-down list. • Lookup. Select an additional local policy lookup from the drop-down list. • 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 entries object.

   Configuration > **session-router** > **show advanced** > **local-response-map** > **Add**.

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

Attributes	Instructions
Local error	Select a local error condition from the drop-down list to trigger this map.
SIP status	Enter a SIP response code. Range: 100-699.
Q850 cause	Enter a Q850 cause code. 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. 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 Add local routing config page, do the following:

Attributes	Instructions
Name	Enter a unique name to use to refer to this local route table when you configure policy attributes. Required.
File name	Enter the name for the file from which the database corresponding to this local route table is created. Use the .gz format, and place the file in the /code/lrt/ directory. Required.
Prefix length	Enter the number of digits to use for lookup and cache storage. Range: 0-999999999.
String lookup	Select to enable lookup by string instead of E. 164 phone numbers, when lookup tables contain range entries with alphanumeric prefixes.
Retarget requests	Select to replace Request-URI in forwarded requests.
Match mode	Select a lookup matching mode from the drop-down list. Note that this setting has no effect when table entries are ranges.

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

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.

1. From the Web GUI, click **Configuration** > **session-router** > **session-agent**.
2. On the session-agent page, click **Add**, do the following:

Attributes	Instructions
Host name	Enter the name of the host associated with the agent in host name, FQDN, or IP address format. This field is required and the name cannot include blank spaces. The value entered here must be unique to this agent because no two agents can use the same host name. • 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.

Attributes	Instructions
Port	Enter the number of the port associated with this agent. • 0. If you enter zero, the E-SBC cannot initiate communication with this agent (although it will accept calls). • 1025-65535. • The default value is 5060. If the transport method value is TCP, the E-SBC will initiate communication on the TCP port of the agent.
State	Select State to enable this agent.
App protocol	Select the protocol to use to signal the session agent.
Transport method	Select the transport mode for connections to this agent. • UDP - Default • UDP+TCP • Dynamic TCP • Static TCP • Dynamic TLS • Static TLS • DTLS • TLS+DTLS • Static SCTP
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.
Max sessions	Enter the maximum number of sessions allowed for this constraint. 0-999999999.
Max inbound sessions	Enter the maximum number of inbound sessions allowed from this session agent. 0-999999999.
Max outbound sessions	Enter the maximum number of outbound sessions allowed for this constraint. 0-999999999.
Max burst rate	Enter the maximum number of invites allowed in a burst time period. 0-999999999.
Max inbound burst rate	Enter the maximum inbound burst rate in INVITEs per second from this session agent. 0-999999999.
Mac outbound burst rate	Enter the maximum outbound burst rate in INVITEs per second from this session agent. 0-999999999.
Max sustain rate	Enter the maximum rate of session invitations allowed within the current time period for this constraint. 0-999999999.

Attributes	Instructions
Max inbound sustain rate	Enter the maximum inbound sustain rate of session invitations allowed within the current time period for this constraint. 0-999999999.
Max outbound sustain rate	Enter the maximum outbound sustain rate of session invitations allowed within the current time period for this constraint. 0-999999999.
Time to resume	Enter the number of seconds that this session agent is out of service after reaching the constraint limit before attempting to re-initialize.
In service period	Enter the number of seconds that this session agent is allowed to re-initialize before returning to in-service status.
Burst rate window	Enter the time period, in seconds, used to measure the burst rate. 0-999999999.
Sustain rate window	Enter the time period, in seconds, used to measure the sustained rate. 0-999999999.
Proxy mode	Select a proxy mode for the E-SBC to use when a SIP request arrives from this agent.
Redirect action	Select a method for the redirect response from this agent. • 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.
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.
Ping send mode	Select the mode for pinging this session agent. • Continuous • Keep alive
Ping all addresses	Select to ping all addresses.
Ping in service response codes	Enter one or more response codes that keep the session agent in service.
Options	Add one or more options.
SPL solutions	Use to add, edit or delete an SPL against this agent.
Media profiles	Add the name of one or more media profiles.
In translation id	Select the inbound translation ID.
Out translation id	Select the outbound translation ID.
Manipulation string	Enter the string to use in header manipulation rules.
Manipulation pattern	Enter a regular expression to use in header manipulation rules.
Trunk group	Specify the name of the trunk group that you must use to reach this agent.
Max register sustain rate	Enter the maximum register sustain rate.
Invalidate registrations	Select to invalidate all registrations going to this session agent.

Attributes	Instructions
RFC2833 mode	Select the preferred mode for RFC2833.
RFC2833 payload	Enter a number for the RFC2833 payload type.
Codec policy	Select the codec policy to apply to this session agent.
Refer call transfer	Select the refer method for call transfer.
Refer notify provisional	Select the provisional mode for sending a NOTIFY message. • 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.
TCP keepalive	Select an option for the TCP keepalive function.
TCP reconn interval	Enter the re-connection interval for TCP re-connection.
Max register burst rate	Enter the number of seconds allowed for the maximum register burst rate.
KPML interworking	Select a status for KPML Interworking.
Monitoring filters	Add one or more monitoring filters.
Auth attribute	Add one or more authentication attributes.
Session recording server	Select a session recording server.
Session recording required	Select to enable.
Hold refer reinvite	Select to enable.

3. Click **OK**.
4. Save 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 Expert mode.

Enable hold-refer-reinvite

The SIP hold-refer-reinvite parameter for REFER with Replaces is a parameter that you enable to prevent premature call termination in a deployment where calls are proxied by the Oracle® Enterprise Session Border Controller.

- 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** > **session-router** > **session-agent**.
2. On the Session Agent page, select the agent and click **Edit**.
3. On the Modify Session Agent page, select Hold refer invite.
4. Click **OK**.
5. Save the configuration.

- Enable the refer-hold-reinvite parameter in the realm configuration.
- Enable the refer-hold-reinvite parameter in the session agent configuration.

Configure a Session Group

Use the sesison-group element to define a signalling 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 session group page, click **Add** > **Show advanced**.
3. On the Add session group page, do the following:

Attributes	Instructions
Group name	Enter the unique name of the session agent group element in the name format.
Description	Enter a description of this session group.
State	Select to enable.
App protocol	Select an application protocol from the drop-down list.

Attributes	Instructions
Strategy	Select a strategy from the drop-down list. • Hunt. System selects the session agent in list order. • Least Busy. System selects the session agent with the fewest number of sessions relative to the max-outbound-sessions constraint of the session-agent element. • Low Sus Rate. System selects the session agent with the lowest sustained rate of session initiations and incitations. • Prop Dist. System uses the proportional distribution strategy to distribute traffic among all available session agent elements, based on session constraint limits. • Round Robin. System selects each session agent, one per session, in the order in which it is listed in the destination list. After all each session agents on the list is used, the system begins at the top of the list and repeats the cycle.
Dest	Add one or more destinations to the list for this session agent group. The destination must correspond to a valid group name in another session agent group or to a valid hostname. Do one of the following, after adding a destination. • Click **OK**. • Click **Apply/Add another**, add another destination, and click **OK**. Repeat, as needed.
Trunk group	Add one or more trunk groups and context to the list for this session agent group. To use the default context case, omit : and the context. Preface with the + character to add, the - character to remove, and exclude and to remove and replace. Do one of the following, after adding a trunk group. • Click **OK**. • Click **Apply/Add another**, add another trunk group, and click **OK**. Repeat, as needed.
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.

4. Click **OK**.
5. 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 system-config object.

   Configuration > **session-router** > **session-recording-group**.

2. On the session recording group page, click **Add**.
3. In the Add session recording group dialog, do the following:

Attributes	Instructions
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	Click **Add**, enter the name of the session recording server, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another session recording server, and click **OK**. Repeat, as needed.
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. Valid values: 1 - 10. Default: 0.

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

Configure Advanced Logging

From the Configuration tab, define sip-advanced-logging and advanced-log-condition. The criteria that you configure remaps 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** > **Show Advanced** > **sip-advanced-logging** > **Show Advanced**, and click **Add**.
2. On the Add SIP Advanced Logging page, do the following:

Attributes	Instructions
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** > **Show Advanced** > **sip-advanced-logging** > **Show Advanced**
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 remaps 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** > **Show Advanced** > **sip-advanced-logging** > **Show Advanced**, and click **Add**.

2. On the Add SIP Advanced Logging page, do the following:

Attributes	Instructions
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. From the Web GUI, click **Configuration** > **session-router** > **sip-config**.
2. On the SIP config page, do the following:

Attributes	Instructions
State	Select to enable SIP operations.
Dialog transparency	Select to preserve call IDs and tags.
Home realm id	Select the home realm to connect to the E-SBC from the drop-down list.
Egress realm	Select the default egress realm from the drop-down list.
Nat mode	Select a Network Address Translation (NAT) mode from the drop-down list. • 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.

Attributes	Instructions
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.
Register use to for lp	Select to enable To header routing for REGISTER.
Refer src routing	Select to enable refer source realm routing.
Atcf stn sr	Enter the Session Transfer Number (STN-SR) allocated by Access Transfer Control Function (ACTF) in the REGISTER message.
Atcf psi dn	Enter the PSI-DN allocated by Access Transfer Control Function (ATCF) in the REGISTER message.
Atcf route to sccas	Select to enable routing the Access Transfer Control Function (ATCF) handover rate to SCCAS.
Eatf stn sr	Enter the E-TN-SR allocated by EATF in the INVITE handover message.
Sag lookup on redirect	Select to enable lookup of the Session Agent Group name on a redirect.
Set disconnect time on bye	Select to enable, if the disconnect time is set on receiving the BYE request.

Attributes	Instructions
Msrp delayed bye	Enter the maximum time, in seconds, to delay forwarding a BYE for an MSRP session. 0 = no delay. Range: 1-60.
Transcoding realm	Enter the name of the realm where transcoding agents reside.
Transcoding agents	Create a list of transcoding agents. Click **Add**, enter the name of a transcoding agent, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another calling translation rule, and click **OK**. Repeat, as needed.
Create dynamic sa	Select to enable the creation of dynamic session agents for service route.
Node functionality	Select a node functionality from the drop-down list.
Match SIP instance	Select to enable matching registration cache entries using the SIP instance parameter.
Sa routes stats	Select to enable tracking session agent statistics for routes resolved by DNS.
Sa routes traps	Select to enable generating traps when session agent routes change state.
Rx SIP reason mapping	Select to enable mapping RX disconnect events to the SIP Reason header.
Add ue location in pani	Select to enable adding the UE location string in the PANI header, when available.
Hold emergency calls for loc info	Enter a time to hold emergency calls until the E-SBC receives location information from PCRF over the RX interface. Range: 0-4294967295.

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

   Configuration > **session-router** > **sip-config**.
2. On the SIP Config page, do the following.

Attributes	Instructions
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 Features

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

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:

Attributes	Instructions
Name	Enter the action tag name to display in the Require, Supported, and Proxy-Require headers of SIP messages.
Realm	Do one of the following: • 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 element 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.

1. From the Web GUI, click **Configuration** > **session-router** > **isp-interface**.
2. On the SIP Interface page, click Add.
3. On the Add SIP Interface page, do the following:

Attributes	Instructions
State	Select to enable this SIP interface.
Realm id	Select the realm in which to apply this SIP interface from the drop-down list.
Description	Enter a description of this SIP interface.

<table>
<tr><th>Attributes</th><th>Instructions</th></tr>
<tr><td>SIP ports</td><td>Specify the following parameters for the ports that the SIP proxy or B2BUA uses for connections.
Address. Enter the IP address of the host associated with the sip-port entry.
Port. Enter the port number for this sip-port. Default is 5060. Range 1025-65535.
Transport protocol. Select the transport protocol associated with this SIP port. Default is UDP. Valid values are: DTLS, SCTP, TCP, TLS, and UDP.
TLS profile. Enter the TLS profile name.
Allow anonymous. Select the type of anonymous connection to allow from agents. Default is All. Valid values include:
<table>
<tr><th>Selection</th><th>Description</th></tr>
<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></td></tr>
<tr><td>Nat traversal</td><td>Select a Network Address Translation (NAT) traversal mode for SIP from the drop-down list.
None. NAT traversal is disabled.
Always. The system performs Hosted NAT Traversal (HNT), when the SIP-Via and the transport address do not match.
Rport. The system performs HNT, when the VIA rport parameter is present and the SIP-Via and transport addresses do not match.</td></tr>
<tr><td>Registration caching</td><td>Select to enable non-HNT registration caching.</td></tr>
<tr><td>Route to registrar</td><td>Select to enable routing requests to the registrar.</td></tr>
<tr><td>In manipulationid</td><td>Select an inbound SIP manipulation rule from the drop-down list.</td></tr>
<tr><td>Out manipulationid</td><td>Select an outbound SIP manipulation rule from the drop-down list.</td></tr>
<tr><td>Service tag</td><td>Enter the service tag for this interface.</td></tr>
</table>

4. Click **OK**.
5. 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** > **Show advanced**.
2. In the SIP manipulation dialog, click **Add** and do the following:

Attributes	Instructions
Name	Enter the exact name of the header to which this rule applies. Alpha-numeric. No spaces. Case-sensitive.
Description	Enter a description of the purpose of this set of rules. Alpha-numeric.
Split headers	Create a list of headers that you want the system to split and treat separately before executing any manipulation rules. Click **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 MIME ISUP Rule

You can configure a Multi-Purpose Internet Mail Extensions (MIME) - ISDN User Part (ISUP) signalling profile on the Oracle® Enterprise Session Border Controller (E-SBC) from the "CfgRules" section in the "Configuring SIP Manipulations" procedure.

- Begin the "Configure SIP Manipulations" procedure and complete the items in the Add SIP manipulation dialog prior to "CfgRules."

The following procedure is the continuation of the "Configure SIP Manipulations" procedure. It begins with adding mime-isup-rule to "CfgRules" and includes the optional mime-header-rule and isup-param-rule sub-element configurations.

1. From the "CfgRules" section of the SIP manipulation configuration page, click **Add**, and select mime-isup-rule from the list.
2. In the SIP manipulation / Mime isup rule dialog, click **Show advanced**, and do the following.

Attributes	Instructions
Name	Enter a unique name for this rule.
Content type	Enter the name of the content type header to which to apply this rule.
Isup spec	Select an ISUP encoding specification from the drop-down list for the ISUP body.
Isup msg types	(Optional) Create a list of one or more ISUP message types to which the mime-isup rule applies. For example, IAM, ACM. When no methods are listed, this rule applies to all types. Click **Add**, enter the message type, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another message type, and click **OK**. Repeat, as needed.
Msg type	Select the message type from the drop-down list to which this rule applies.
Methods	(Optional) Create a list of methods to which this rule applies. For example, INVITE, ACK, CANCEL. When no methods are listed, this rule applies to all methods. Click **Add**, enter the method, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another method, and click **OK**. Repeat, as needed.
Action	Select an action from the drop-down list for the header rule.
Comparison type	Select a comparison type from the drop-down list to use for the match value.
Match value	Enter the value to match against the current object.
New value	Enter the new value for the object. You must escape quoted display names within quotes. For example, \"MyName\".

Attributes	Instructions
CfgRules (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 isup rule dialog. Do one of the following: • Add another mime-header-rule. • Add an isup-param-rule, using the steps in the corresponding table cell. • Finish the MIME ISUP rule configuration by completing steps 3-6.
CfgRules (instructions for configuring isup-param-rule)	(Optional) Click **Add** > **isup-param-rule** > **Show advanced**, 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. • 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 isup rule dialog. Do one of the following: • Add another isup-param-rule. • Add an mime-header-rule, using the steps in the corresponding table cell. • Finish the MIME ISUP rule configuration by completing steps 3-6.

3. Click **OK**.

   The system displays the Add SIP manipulation page.

4. Click **OK**.

   The system displays the SIP manipulation page.

5. Click **Close**.

6. Save the configuration.

Configure MIME SDP Rule

You can configure a Multi-Purpose Internet Mail Extensions (MIME) - Session Description Protocol (SDP) multimedia communications session profile on the Oracle® Enterprise Session Border Controller (E-SBC) from the "CfgRules" section in the "Configuring SIP Manipulations" procedure.

- Begin the "Configure SIP Manipulations" procedure and complete the items in the Add SIP manipulation dialog prior to "CfgRules."

The following procedure is the continuation of the "Configuring SIP Manipulations" procedure. It begins with adding the mime-sdp-rule to "CfgRules" and includes the optional mime-header-rule, sdp-session-rule, sdp-media-rule, and sdp-line-rule sub-element configurations.

In step 2 of this procedure, you can configure as few or as many of the "CfgRules" sub-element options that you want.

- If you do not configure an optional sub-element, proceed to step 3.
- If you configure an optional sub-element, you can configure another one or proceed to step 3.

1. From the "CfgRules" section of the SIP manipulation configuration page, click **Add**, and select mime-sdp-rule from the list.

2. In the SIP manipulation / Mime sdp rule dialog, do the following.

Attributes	Instructions
Name	Enter a unique name for this rule.
Msg type	Select the message type from the drop-down list to which this rule applies.
Methods	(Optional) Create a list of methods to which this rule applies. For example, INVITE, ACK, CANCEL. When no methods are listed, this rule applies to all methods. Click **Add**, enter the method, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another method, and click **OK**. Repeat, as needed.
Action	Select an action from the drop-down list for the header rule.
Comparison type	Select a comparison type from the drop-down list to use for the match value.
Match value	Enter the value to match against the current object.

Attributes	Instructions
New value	Enter the new value for the object. You must escape quoted display names within quotes. For example, \"MyName\".
CfgRules (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 corresponding table cells. • Finish the MIME SDP rule configuration by completing steps 3-6.

Attributes	Instructions
CfgRules (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. • Finish the MIME SDP rule configuration by completing steps 3-6.

Attributes	Instructions
CfgRules (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. • 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 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. • Configure the mime-header-rule and sdp-sesison-rule options, using the steps in the corresponding table cells. • Finish the MIME SDP rule configuration by completing steps 3-6.

3. Click **OK**.

   The system displays the Add SIP manipulation page.

4. Click **OK**.

   The system displays the SIP manipulation page.

5. Click **Close**.

6. Save the configuration.

Configure Header Rule

You can configure SIP header manipulations on the Oracle® Enterprise Session Border Controller (E-SBC) from the "CfgRules" section in the "Configuring SIP Manipulations" procedure.

- Begin the "Configure SIP Manipulations" procedure and complete the items in the Add SIP manipulation dialog prior to "CfgRules."

The following procedure is the continuation of the "Configure SIP Manipulations" procedure. It begins with adding header-rule to "CfgRules" and includes the optional element-rule sub-element configuration.

1. From the "CfgRules" section of the SIP manipulation configuration page, click **Add**, and select header-rule from the list.
2. In the SIP manipulation / Header rule dialog, do the following.

Attributes	Instructions
Name	Enter a unique name for this rule set. Alpha-numeric.
Header name	Enter the name of the header to which this rule applies. Case-sensitive.
Action	Select an action from the drop-down list for the header rule.
Comparison type	Select a comparison type from the drop-down list to use for the match value.
Msg type	Select the message type from the drop-down list to which this rule applies.
Methods	(Optional) Create a list of methods to which this rule applies. For example, INVITE, ACK, CANCEL. When no methods are listed, this rule applies to all methods. Click **Add**, enter the method, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another method, and click **OK**. Repeat, as needed.
Match value	Enter the value to match against the current object.
New value	Enter the new value for the object. You must escape quoted display names within quotes. For example, \"MyName\".

Attributes	Instructions
CfgRules	(Optional) Click **Add** > **element-rule**, and do the following. • Name. Enter a unique name for this header element rule. • Parameter name. Enter a parameter to which to apply the rule. • Type. Select an element type from the drop-down list to which to apply the rule. • Action. Select an action from the drop-down list to apply to the element rule. • Match val type. Select a value 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. Case-sensitive. • 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 / Header rule page. Do one of the following: • Add another element-rule. • Finish the Header rule configuration by completing steps 3-6.

3. Click **OK**.

   The system displays the Add SIP manipulation page.

4. Click **OK**.

   The system displays the SIP manipulation page.

5. Click **Close**.

6. Save the configuration.

Configure MIME Rule

You can configure a Multi-Purpose Internet Mail Extensions (MIME) data files exchange profile on the Oracle® Enterprise Session Border Controller (E-SBC) from the "CfgRules" section in the "Configuring SIP Manipulations" procedure.

- Begin the "Configure SIP Manipulations" procedure and complete the items in the Add SIP manipulation dialog prior to "CfgRules."

The following procedure is the continuation of the "Configure SIP Manipulations" procedure. It begins with adding mime-rule to "CfgRules" and includes the optional mime-rule sub-element configuration.

1. From the "CfgRule"s section of the SIP manipulation configuration page, click **Add**, and select mime-rule from the list.

2. In the SIP manipulation / Mime rule dialog, click **Show advanced**, and do the following.

Attributes	Instructions
Name	Enter a unique name for this rule.
Content type	Enter the name of the content-type header to which to apply this rule.
Msg type	Select the message type from the drop-down list to which this rule applies.
Methods	(Optional) Create a list of methods to which this rule applies. For example, INVITE, ACK, CANCEL. When no methods are listed, this rule applies to all methods. Click **Add**, enter the method, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another method, and click **OK**. Repeat, as needed.
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.
Comparison type	Select a comparison type from the drop-down list to use for the match value.
Match value	Enter the value to match against the current object.
New value	Enter the new value for the object. You must escape quoted display names within quotes. For example, \"MyName\".
CfgRules (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 rule dialog. Do one of the following: • Add another mime-header-rule. • Finish the MIME rule configuration by completing steps 3-6.

3. Click **OK**.

   The system displays the Add SIP manipulation page.

4. Click **OK**.

The system displays the SIP manipulation page.

5. Click **Close**.
6. Save the configuration.

Configure SIP Monitoring

Use the sip-monitoring element 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, click **Show advanced**, and do the following:

Attributes	Instructions
Match any filter	Select to enable.
State	Select to enable the sip-monitoring configuration.
Short session duration	Enter a number of minutes from 0-999999999.
Monitoring filters	Click **Add** to add one or more custom monitoring filters to the list to use when monitoring on a global-basis. Enter the name of the filter, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another media attribute, and click **OK**. Repeat, as needed.
Interesting events	Click **Add**, and select either short-session or local-rejection.
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** > **show advanced** > **surrogate-agent** > **show advanced**.
2. On the Surrogate Agent page, click **Add**.
3. On the Add Surrogate Agent page, do the following:

Attributes	Instructions
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>

Attributes	Instructions
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

Attributes	Instructions
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

4. Click **OK**.
5. 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** > **survivability**.
2. At the bottom of the left pane, click **Show advanced**.
3. On the Add survivability page, do the following:

Attributes	Instructions
State	Select to enable Survivability.
Reg expires	Enter the number of seconds that the Oracle® Enterprise Session Border Controller waits before entering the remote site survivability mode when the registration expires.
Prefix length	Enter the maximum number of digits allowed for a phone extension. Range: 0-10.

Attributes	Instructions
Session agent hostname	Select the agent hostname or the session agent group name from the drop down list.

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

- 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 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. From the Web GUI, click **Configuration** > **session-router** > **translation-rules**.
2. On the Translation rules page, click **Show advanced**, and do the following:

Attributes	Instructions
Id	Enter the identifier or name for this rule.
Type	Select the address translation type from the drop-down list. • 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.

Attributes	Instructions
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 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 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:

Note:

Click **Show Advanced** in the navigation pane to display all of the System objects in the following list.

Object	Purpose
capture-receiver	Enable and configure a capture receiver.
fraud-protection	Enable and configure fraud protection.
host-route	Add one or more host routes.
network-interface	Add one or more network interfaces.
network-parameters	Configure TCP and SCTP parameters for the network.
ntp-config	Add one or more NTP servers and authentication servers.
phy-interface	Add one or more physical interfaces.
redundancy-config	Enable redundancy and add one or more peers.

Object	Purpose
snmp-community	Add one or more SNMP communities, including subnet ranges.
spl-config	Add an SPL option and one or more plugins.
system-access-list	Add one or more system access lists.
system-config	Configure the system settings for MIBS, SNMP functions, syslog servers, comm monitor, and more.
tdm-config	Enable and configure Time Division Multiplexing (TDM).
trap-receiver	Add one or more trap receivers.
web-server-config	Enable and configure a web server, including a TLS profile.

Telephony Fraud Protection

You can configure the Oracle® Enterprise Session Border Controller (E-SBC) to protect against fraudulent calls by using lists of phone numbers to block, allow, redirect, and rate limit calls, according to rules that you configure to manage fraudulent traffic. The lists reside together in a single file that you specify as the source file in the fraud protection configuration. You can enable and manage fraud protection from the Web GUI, but only in Expert mode. You can enable fraud protection from the ACLI, but you cannot manage fraud protection from the ACLI. Telephony Fraud Protection is part of the advanced license. If you owned an Advanced license before the introduction of Telephony Fraud Protection, you must re-enable the license to access this feature.

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.

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 previous 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 to a revenue-share fraud target in a foreign country to an end point that defeats the fraud. For example, you can redirect subscribers dialing a particular number and URI to an announcement to make them aware that an account is compromised and 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, as with a blacklist, you may want to reduce the impact with rate limiting until a network engineer can analyze an attack and plan remediation. 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

To configure fraud protection, you must specify the source of fraud protection management and specify the file that contains the list of phone numbers to manage. The E-SBC or another device can manage fraud protection. You can create or upload the phone number list file by way of the File Management page on the Web GUI.

Administration

When you configure the E-SBC to manage fraud protection, the system applies the following behavior:

- An Admin with privileges can Refresh, Add, and Upload an unselected file, and Edit, Download, and Delete a selected file.
- An Admin with no privileges can only view the files.

The system provides the following methods for viewing fraud protection data.

- From the ACLI, use the show commands to view fraud protection statistics.
- 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.

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 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.

Character	Description
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]. 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.

Character	Description
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 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 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.

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 the Fraud Protection configuration page, 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 specified file, for example a file that you updated outside of the E-SBC, the system prompts for activation upon upload.
- Edit File—When you edit the specified 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.

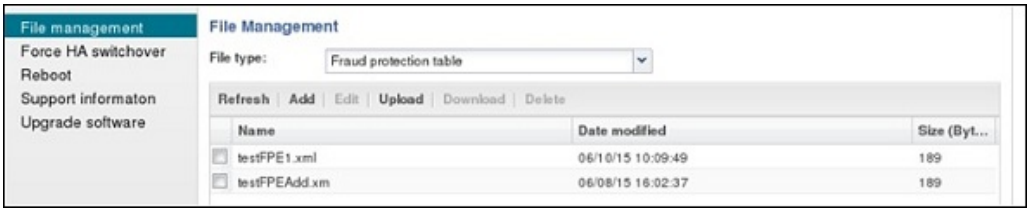
> **Note:**
>
> The system displays an alert on the Notifications menu to remind you that the fraud protection file needs activation.

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 File Type drop-down list that includes the Fraud Protection Table item. The Fraud Protection Table displays the list of fraud protection files on the E-SBC, as shown in the following illustration.



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 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.

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** button on the File Management page to launch the following dialog.

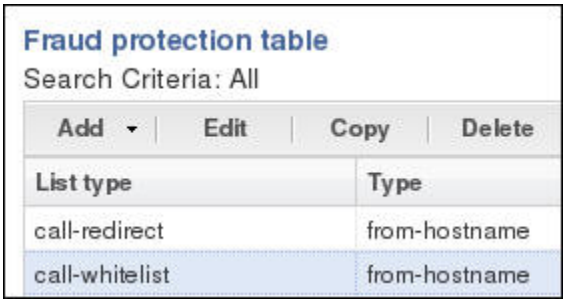
After you enter the file name and click **OK**, the system adds the new file to the list of Fraud Protection Tables on the File Management page. To make the new file the source file for Fraud Protection, you must specify the file name in the fraud protection configuration and activate the configuration.

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. After the initial configuration, the system does not refresh the fraud protection file when you save and activate configuration changes on the E-SBC, except when you specify a new file name in the fraud protection configuration.

List Maintenance

When you want to edit a fraud protection list, select the file on the File Management page, click **Edit**, select a list type on the Fraud Protection Table page, and click **Edit**.



The system displays the corresponding dialog for editing the selected list type. For example, suppose that you selected call-whitelist in the preceding illustration. The system displays the following dialog.

List Viewing Filters

The default view of the Fraud Protection Table displays all of the fraud protection entries in the system for all list types. For easier viewing, you can sort the table by list type. The following illustration shows the sorting selections.

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.

Type	Description
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.

Match Value	Format
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.

Match Value	Format
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.

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 system. You can create more files now or anytime after configuring fraud protection, but the system uses only the file named in the 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. From the Web GUI click **Configuration** > **System** > **File Management.**
2. On the File Management page, select Fraud Protection Table from the File Type drop-down list.
3. Click **Add**.
4. In the Add Fraud Protection table dialog, do the following:

Attributes	Instructions
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 Edit Fraud Prevention Table <filename> dialog.
6. (Optional) Click **Verify**.

   The system checks that the file name is unique and uses a valid extension.
7. (Optional) Click **OK**.

The system displays the Edit Fraud Prevention Table <filename> dialog.

8. Click **Add**.
9. Select a list type from the drop-down list to add to the file, and do the following according to the list type:

Attributes	Instructions
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. • Target. Enter one of the following: Session agent, session agent group name, Hostname, or IP address.

10. Click **OK**.
11. (Optional) Repeat steps 8-10 to add more entries.
12. Click **Verify**.

    The system checks for valid entries in the configuration fields.
13. Click **Save**.
14. Click **OK**.
15. Click **Close**.

- 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. From the Web GUI, click **System** > **File management**.
2. On the File management page, select Fraud protection table from the File type drop-down list, and click **Upload**.
3. In the Upload file dialog, do the following:

Attributes	Instructions
File to upload.	Browse to the file to upload.
(Optional) Activate the File After Upload.	Select to activate the file now.

4. Click **Upload**.
5. Click **Close**.

- 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 the `fraud-protection` element 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. From the Web GUI, click **Configuration** > **system** > **fraud-protection**.
2. On the Fraud Protection page, do the following:

Attributes	Instructions
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 E-SBC as the source of fraud protection management.

1. From the Web GUI, click **Configuration** > **system** > **fraud-protection**.
2. On the Fraud protection page, do the following:

Attributes	Instructions
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. From the Web GUI, click **System** > **File management**.
2. On the File Management page, select Fraud Protection Table from the File type drop-down list.
3. Select a file, and click **Edit**.

   The system displays the Fraud Protection Table dialog.
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:

Attributes	Instructions
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** > **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 element 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. From the Web GUI, click **Configuration** > **system** > **host-route**.
2. On the Host Route page, click **Add**.
3. On the Add host route page, do the following:

Attributes	Instructions
Dest network	Enter the IPv4 address of the destination network for this host route.
Netmask	Select the netmask associated with the destination network from the drop-down list.
Gateway	Enter the gateway address for traffic going to the Dest network parameter to use as the first hop when forwarding a packet out of the originator's LAN.
Description	Enter a description for this host route. Alpha-numeric characters.

4. Click
5. Save 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 Expert mode.

Use the network-interface object to configure the parameters for the network interface, which specifies a logical network interface over which you can configure one or more application SIP interfaces. Note that the E-SBC supports only one network interface.

1. From the Web GUI, click **Configuration** > **Objects** > **System** > **network-interface**.
2. On the network-interface page, click **Add**.
3. On the Add network-interface page, click **Show Advanced**.

4. In the Add network-interface dialog, do the following:

Attributes	Instructions
Name	Enter the name of the physical interface linked to this network interface. Control and Maintenance operation types must start with “wancom.”
Sub port ID	Enter the sub port ID to identify a specific virtual interface in a physical interface (e.g., a VLAN tag). A value of 0 indicates that this element is not using a virtual interface. The sub-port-id field value is required only if the operation type is Media. Default: 0. Range: 0-4095.
Description	Enter a description of this network interface.
Hostname	Enter the hostname of this network interface in Fully Qualified Domain Name (FQDN) format or IP address format.
IP address	The IP address of this network interface in the IP address format.
Pri utility addr	Enter the utility IP address of the primary peer in an HA pair.
Sec utility addr	Enter the utility IP address of the secondary peer in an HA pair.
Netmask	Enter the netmask portion of the IP address for this network interface in IP address format.
Gateway	Enter a description for this host route. Alpha-numeric characters.
Gw heartbeat	• 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.

Attributes	Instructions
Signalling mtu	Enter the Maximum Transmission Unit (MTU) size for signalling packets. Default: 0. Range: 576-4096.
HIP IP list	Create a list of IP addresses allowed to access signaling and maintenance protocol stacks by way of this front interface using the Hosted IP (HIP) feature. Click **Add**, enter the HIP IP address, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another HIP IP address, and click **OK**. Repeat, as needed.
Ftp address	Enter the FTP address.
ICMP address	Create a list of Internet Control Message Protocol (ICMP) addresses. Click **Add**, enter the ICMP address, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another ICMP address, and click **OK**. Repeat, as needed.
Telnet address	Enter the Telnet address.
Ssh address	Enter the SSH IP address. The gateway address of this interface must be default gateway.

5. Click **OK**.
6. Save 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. From the Web GUI, click **Configuration** > **system** > **ntp-config**
2. On the ntp-config page, do the following:

Attributes	Instructions
Server	Click **Add**, enter the name or IP address of the NTP server in your network that you want to use for the E-SBC, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another NTP server, and click **OK**. Repeat, as needed.

Attributes	Instructions
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. From the Web GUI, click **Configuration** > **Objects** > **System** > **phy-interface**.
2. On the phy-interface page, click **Add**.
3. On the Add phy-interface page, click **Show Advanced**.
4. In the Add phy-interface dialog, do the following:

Attributes	Instructions
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.

Attributes	Instructions
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.

5. Click **OK**.
6. 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. From the Web GUI, click **Configuration** > **system** > **redundancy-config**.
2. On the Add redundancy config page, click **Show advanced**, and do the following:

Attributes	Instructions
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.

Attributes	Instructions
Peers	Click **Add** > **Show advanced**, 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.** Destinations. 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.** Destinations. 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)	Emergency Critical
	Major (3)	Major
	Minor (4)	Minor
	Warning (5)	Warning
	Notice (6)	
	Info (7)	
	Trace (8)	
	Debug (9)	
Critical	Emergency (1) Critical (2)	Emergency Critical
Major	Emergency (1) Critical (2)	Emergency Critical
	Major (3)	Major
Minor	Emergency (1) Critical (2)	Emergency Critical
	Major (3)	Major
	Minor (4)	Minor

When configuring the trap-receiver element for use with Network Management Systems, Oracle recommends setting the filter-level parameter to All.

Configure an SNMP Trap Receiver

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

- 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. From the Web GUI, click **Configuration** > **System** > **Show advanced** > **trap-receiver**.
2. On the trap receiver page, click **Add**.
3. On the Add trap receiver page, do the following:

Attributes	Instructions
IP address	Enter the IPv4 address and port number of an authorized NMS in dotted decimal format. Default: 0.0.0.0:162.
Filter level	Select the filter level threshold for the severity level at which a trap is sent to the trap receiver.
Community name	Enter the SNMP community name to which this trap receiver belongs.

Attributes	Instructions
User list	Create a list of users allowed to receive secure traps. Click **Add**, enter the name of a user, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another user, and click **OK**. Repeat, as needed. **Note:** If SNMPv3 is enabled on the E-SBC, but no users are listed for this field, a warning message is sent during the verify-config execution.

4. Click **OK**.
5. 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. From the Web GUI, click **System** > **SNMP community**.
2. On the SNMP community page, click **Add**, and do the following:

Attributes	Instructions
Community name	Enter an SNMP community name of an active community where this E-SBC can send or receive SNMP information.
Access mode	Select the access level for all Network Management Systems (NMS) defined within this SNMP community.
IP 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. Such configuration allows the (E-SBC) to 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 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 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 object.

   Configuration > **system** > **system-config**.

2. In the system-config object, do the following:

Attributes	Instructions
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. Range: 1-500.

Attributes	Instructions
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. **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.
System log level	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.
Process log level	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.
Process log IP address	Set the IP address of the process log server. Default: 0.0.0.0 (Writes logs to the standard log file.)
Process log port	Set the port number for the process log server. Default: 0 (Writes logs to the standard log file.) Range: 0-65535.

Attributes	Instructions
Collect	Access the `collect` configuration, and do the following: **a.** Sample interval—Set the data collection sampling interval. **b.** Push interval—Set the data collection push interval. **c.** Boot state—Set **Enable** to enable the collection process. **d.** Start time—Set the date and time to start data collection. **e.** End time—Set the date and time to end data collection. **f.** Red collect state—Set **Enable** to enable collector redundancy. **g.** Red max trans—Set the maximum number of transactions to keep. **h.** Red sync start time—Set the time for redundancy sync start timeout. **i.** Red sync comp time—Set the time for redundancy sync completion timeout. **j.** 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 collect data. **v.** Protocol—Set the protocol for pushing data to the server. **k.** 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. **iii.** Start time—Set the date and time to start data collection. **iv.** End time—Set the date and time to end data collection. **v.** Boot state—Enable or disable this group from the collection process.

Attributes	Instructions
	l. Push success trap state—Type **Enable** to enable the collector HDR push data success trap.
Comm Monitor	Access the `comm-monitor` configuration, and do the following: a. State—Select to enable Comm Monitor. b. SBC group ID—Set the group ID for the Palladion ME. c. TLS profile—Select the TLS profile that you want to use for TLS connections. d. QoS enable—Enable or disable the system to send QoS information. e. Interim QoS Update—Select to enable incremental QoS sampling every 10 seconds. f. Monitor collector—Click **Add**, and do the following: i. Port—Set the Palladion ME listening port. ii. Address—Set the IP destination address for data that the system pushes. iii. Interface—Set the local network interface to use for the connection. Format: <name>:<subport-ID>
Call trace	Enable or disable protocol message tracing, regardless of the process log level setting. **Note:** You cannot disable call trace when the process log level specifies "trace" or "debug."
Internal trace	Enable or disable internal ACP message tracing for all processes, except sipmsg.log and alg,log, regardless of the process log level setting. **Note:** You cannot disable call trace when the process log level specifies "trace" or "debug."

Attributes	Instructions
Log filter	Set the combination of protocol traces and logs that you want sent to the log server specified in "process-log-level." Use "fork" to keep "trace" and "log" information in local storage as well as on the server. Valid values: none | traces | traces-fork | logs | logs-fork | all | all-fork.
Default gateway	Set the default egress gateway for traffic with no explicit destination.
Restart	Enable or disable a system restart when a task suspends.
Exceptions	Take no action when the named tasks suspend.
Telnet timeout	Set the number of seconds for the E-SBC to wait before disconnecting a Telnet or 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.
Remote control	Allow remote ACP control
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.
CLI audit trail	Enable the ACLI command audit trail.
Link redundancy state	Enable or disable the E-SBC to run a pair of redundant media interfaces for switch over when a network or link disruption occurs.
Source routing	Set the egress route for the HIP packet, based on the source IP address.
CLI more	Enable the ACLI more paging function to work persistently with the E-SBC across the console, Telent, and SSH sessions. Set to disabled, if you want set this function on a per session basis.
Terminal height	Configure ACLI tty more terminal height.
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.
Trap event lifetime	Set the maximum number of days traps remain in the table.
IDS syslog facility	Set the facility number for syslog messages.
Options	Add optional features and parameters.
Default v6 gateway	Set the IPv6 gateway for egress traffic on this E-SBC with no explicit destination. Format: <ipv6>.

Attributes	Instructions
IPv6 signalling MTU	Set the system-wide default MTU for IPv6 network interfaces. Default: 1500 bytes.
IPv4 signalling MTU	Set the system-wide default MTU for IPv4 network interfaces. Default: 1500 bytes.
Clean up time of day	Set the time for the system to perform directory cleanup.
Directory cleanup	Configure the directories that you want the E-SBC to automatically clean up.
SNMP engine ID suffix	Set a customized suffix to uniquely identify the SNMP engine ID.
SNMP agent mode	Set the SNMP agent mode that you want. Valid values: SNMPv1v2 or SNMPv3.

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 the configuration of **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 Subscriber Office (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 Oracle® Enterprise Session Border Controller (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 preceding the first number of the pattern. Do not use the underscore with an exact match. Type the exact match, starting with the first number. An exact match does not use 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

Configure the Single-Port Primary Rate Interface

The Acme Packet 1100 Supports 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 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**, which 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.)

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 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**, which 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 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 **ccs**.
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 element.

   Configuration > **session-router** > **show advanced** > **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 element.

   Configuration > **session-router** > **show advanced** > **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 element.

   Configuration > **session-router** > **show advanced** > **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 **fxo-profile**.

1. Access the tdm-config 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. Valid values: Bell, v23, v23_ip, dtmf, of smdi. Default: Bell.

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-confg** and use the **tdm-profile** sub-element to set the **overlap dial** and **incoming-pattern** parameters.

1. Access the tdm-config 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.

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

Configure a Web Server

Use the web-server element to enable the Web server and to specify how you want it to communicate with the Oracle® Enterprise Session Border Controller.

1. From the Web GUI, click **Configuration** > **system** > **web-server**.
2. On the Add Web server config page, click **Show advanced**, and do the following.

Attributes	Instructions
State	Select to enable Web server.
Inactivity timeout	Enter the number of minutes you want the Web server to wait before timing out.
HTTP state	Select to enable an HTTP connection to the Web server.
Optional. HTTP port	(Optional) Enter the port number that you want to use instead of the default port 80.
HTTPS state	Select to enable HTTPS connection to the Web server.

Attributes	Instructions
Optional. HTTPS port	(Optional) Enter a the port number that you want to use instead of the default port 443.
TLS profile	Select a TLS profile to use for HTTPS from the drop down list.

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

6

Monitor and Trace Tab

The Monitor and Trace tab displays the results of filtered SIP session data from the Oracle® Enterprise Session Border Controller. The page displays the results in a common log format for local viewing.

Monitor and Trace supports the following summary reports that you can export to a PC.

- Sessions
- Registrations
- Subscriptions
- Notable events

Each report provides sorting, searching, and paging functionality. You can customize the columns in each report and use the buttons on the page to display additional information or to perform a task.

The SIP Monitor and Trace function can store messages per session and it can store cumulative sessions across all report types. Once the sessions maximum is reached, the system removes the oldest call and adds the newest call.

- On systems with less than 4GB of RAM, the system can store:
  - 50 messages
  - 2,000 sessions
- On systems with more than 4GB of RAM, the system can store:
  - 50 messages
  - 4,000 sessions

The call database is not persistent across reboots

The system can perform live paging from Monitor and Trace tables.

> **Note:**
>
> Monitor and Trace does not support multiple, simultaneous viewers. Only one user at a time can view Monitor and Trace information.

Configure SIP Monitoring

You must enable sip-monitoring and configure the options for displaying session data and notable event data on the Monitor and Trace page.

- 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. From the web GUI, click **Configuration** > **Session-Router** > **SIP-Monitoring**.
2. On the Modify sip-monitoring page, click **Show advanced**, and do the following.

Attributes	Instructions
Match any filter	Select to monitor all SIP traffic. Default: Disabled.
State	Select to enable SIP monitoring.
Short session duration	Enter a value, in seconds, for the maximum session duration of a short session. Default: 0. Range 0-999999999.
Monitoring filters	Create a global list of monitoring filters. Click **Add**, enter the name of the filter, and do one of the following: • Click **OK**. • Click **Apply/Add another**, add another NTP server, and click **OK**. Repeat, as needed.
Interesting events	Create a global list of interesting events to monitor. Click **Add** > **Show advanced**, and do the following: • Type. Select an event type from the drop-down list. • Trigger threshold. Enter the number of events required to occur in within the trigger window before the system starts monitoring. Default: 0. Range: 0-999999999. • Trigger timeout. Enter the amount of time, in seconds, that the monitoring persists. Default: 0. Range: 0-999999999, • Click **OK**. The system displays the SIP monitoring page.

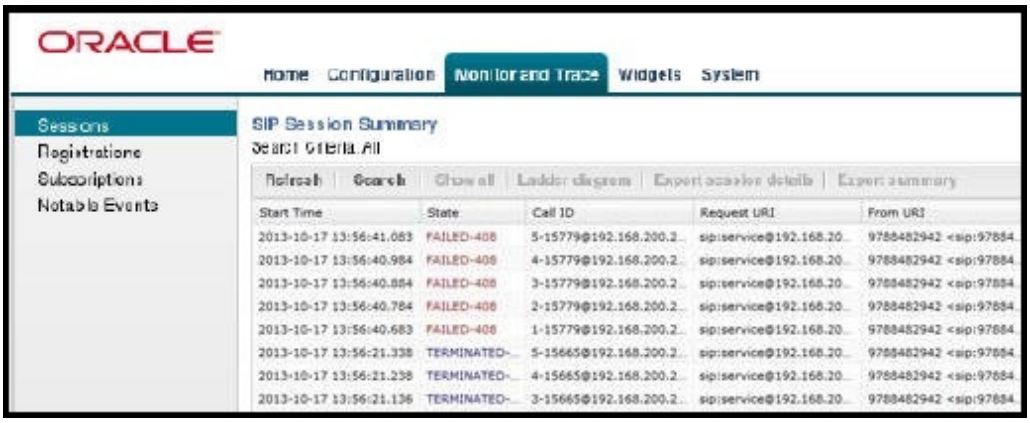
3. Click **OK**.
4. Save the configuration.

- View SIP Session Summary and SIP Notable Event Summary on the Monitor and Trace tab.

Sessions Report

The Sessions Report is a SIP session summary of all logged call sessions on the Oracle® Enterprise Session Border Controller (E-SBC). When Lightweight Directory Access Protocol (LDAP) is enabled on the Active Directory, LDAP session messages may also display.

The columns that display on the Sessions Report page depend on the columns that you specified in the "Customizing the Page Display" procedure.

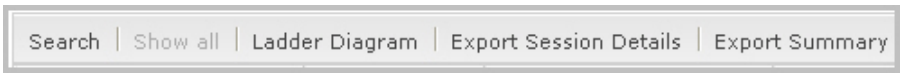


The following table describes the columns on the SIP Session Summary page.

Heading	Description
Start Time	Timestamp of the first SIP message in the call session.
State	Status of the call or media session. Valid values are: INITIAL—Session for which an INVITE or SUBSCRIBE was forwarded. EARLY—Session that received the first provisional response (1xx other than 100). ESTABLISHED—Session for which a success (2xx) response was received. TERMINATED—Session that ended by receiving or sending a BYE for an “Established” session or forwarding an error response for an “Initial” or "Early" session. The session remains in the terminated state until all the resources for the session are freed up. FAILED—Session that failed due to a 4xx or 5xx error code.
Call ID	Identification of the call source. Includes the phone number and source IP address.
Request URI	Uniform Resource Identifier (URI) formatted string that identifies a resource by way of a protocol, name, location, and any other applicable characteristic that is sent by the E-SBC in REQUEST headers.
From URI	URI formatted string that identifies the call source information.
To URI	URI formatted string that identifies the call destination information.
Duration	Amount of time, in seconds, that the call or media event was active.

Heading	Description
Notable Event	Indicates if a notable event has occurred on the call session. Valid values are: short session—Sessions that do not meet a minimum configurable duration threshold. Session dialogue, captured media information, and termination signalling. Any event flagged as a short session interesting event. local rejection—Sessions locally rejected at the E-SBC for any reason, for example, Session Agent (SA) unavailable, no route found, SIP signalling error, and so on. Session dialogue, capture media information, and termination signalling. Any event flagged as a local rejection interesting event.
Session ID	Identification assigned to the call session.
Ingress Src Addr	Source IP address of the incoming call or media event.
Egress Dest Addr	Destination IP address of the outgoing call or media event.

The following table describes the controls on the SIP Session Summary page.

Button	Description
	
Search	Use to specify parameters for performing a search for specific session summary records within the current report.
Show all	Use to display all of the session summary records in the Sessions Report.
Ladder Diagram	Use to display a Ladder Diagram of a specific record in the table. The Ladder Diagram displays detailed information about a call session or media event.
Export Session Details	Use to export the SIP messages and media events associated with the selected session to a file in text format on the local machine.
Export Summary	Use to export all logged session summary records to a file in text format on the local machine.

Display a Sessions Report

1. From the Web GUI, click **Monitor and Trace** > **Sessions**.

   The system displays the SIP Session Summary page.

2. Use the buttons on the top of the page to find, view, and export information about the records in the report.

Ladder Diagram

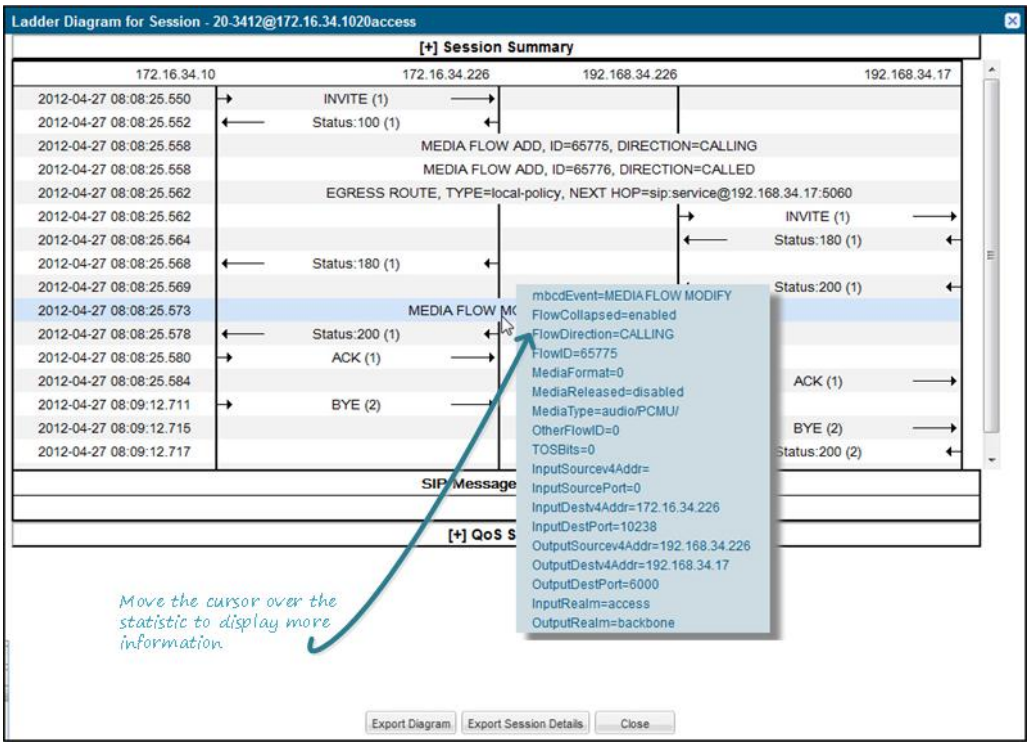
A ladder diagram is a graphical representation in the Web GUI that shows the call and media flow of packets on ingress and egress routes by way of the Oracle® Enterprise Session Border Controller (E-SBC).

A ladder diagram for the Sessions Report displays the following session summary information, which may be useful for troubleshooting:

- Quality of Service (QoS) statistics for call sessions
- SIP messages and media events in time sequence

To display a ladder diagram for a specific record in the Sessions Report, click a record in the summary table or click **Ladder diagram** on the SIP Sessions Summary page.

The following illustration is an example of an E-SBC ladder diagram.



When you hover the mouse over any statistic in the Ladder Diagram, the system displays additional parameters and associated values.

The SIP Session Summary ladder diagram includes the following information about the call or media session in focus:

- Session Summary—Summary information.
- SIP Message Details—SIP message and call flow information.
- QoS Statistics—Quality of Service (QoS) statistic information.

The following table describes the buttons in the Ladder Diagram page.

Button	Description
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) configured on the E-SBC, and applies the Session Plug-in Language (SPL) to that message. When the message is sent from the E-SBC, 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

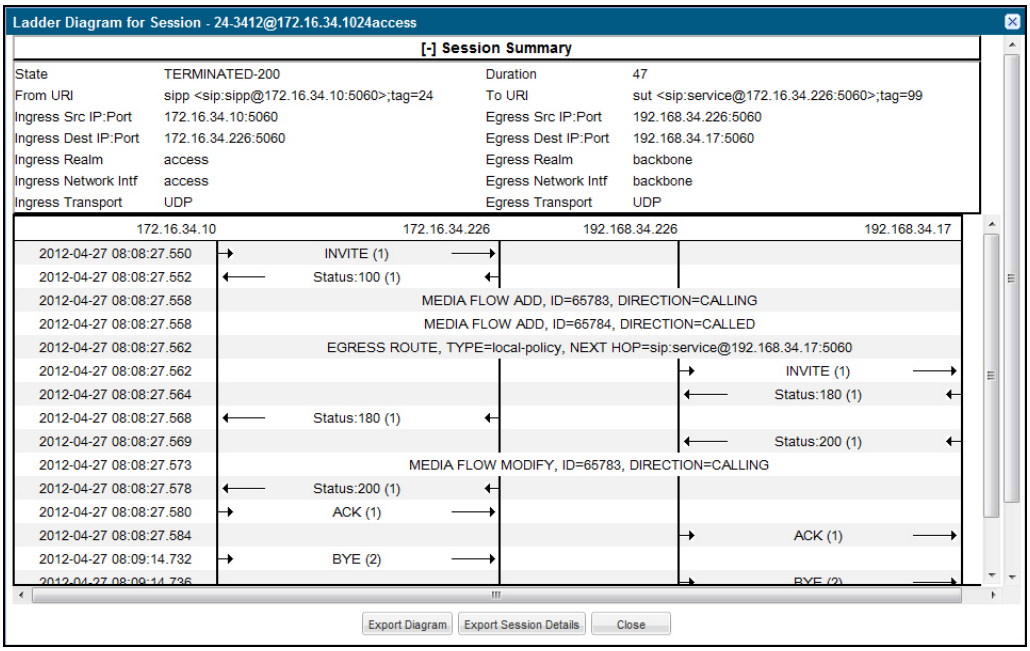
You can display a ladder diagram of call and media flow from the SIP Session Summary page in the Web GUI.

1. From the Web GUI, click **Monitor and Trace** > **Sessions**.
2. On the SIP Session Summary page, do one of the following:
   - Click Ladder Diagram.
   - Click a record in the table.

Session Summary

From a ladder diagram, you can launch a summary of a selected call or media session.

The following illustration shows a sample Session Summary page generated from a selection on the ladder diagram.



The following table describes each field in the Session Summary window.

Heading	Description
State	Status of the call or media session. Valid values are: INITIAL Session for which an INVITE or SUBSCRIBE was forwarded. EARLY Session received the first provisional response (1xx other than 100). ESTABLISHED Session for which a success (2xx) response was received. TERMINATED Session that has ended by receiving or sending a BYE for an "Established" session or forwarding an error response for an "Initial" or Early session. The session remains in the terminated state until all the resources for the session are freed up. FAILED Session that has failed due to a 4xx or 5xx error code.
Duration	Amount of time, in seconds, that the call or media session was active.
From URI	URI formatted string that identifies the call source information.
To URI	URI formatted string that identifies the call destination information.
Ingress Src IP:Port	Source IP address and port number of the incoming call or media session.
Egress Src IP: Port	Source IP address and port number of the outgoing call or media session.
Ingress Dest IP:Port	Destination IP address and port number of the incoming call or media session.
Egress Dest IP: Port	Destination IP address and port number of the outgoing call or media session.
Ingress Realm	Incoming realm name.
Egress Realm	Outgoing realm name.
Ingress Network Intf	Name of the incoming network interface on the Oracle® Enterprise Session Border Controller (E-SBC).
Egress Network Intf	Name of the outgoing network interface on the E-SBC.
Ingress Transport	Protocol type used on the incoming call or media session. Valid values are User Datagram Protocol (UDP) or Transport Control Protocol (TCP).
Egress Transport	Protocol type used on the outgoing call or media session. Valid values are User Datagram Protocol (UDP) or Transport Control Protocol (TCP).

Display a Session Summary

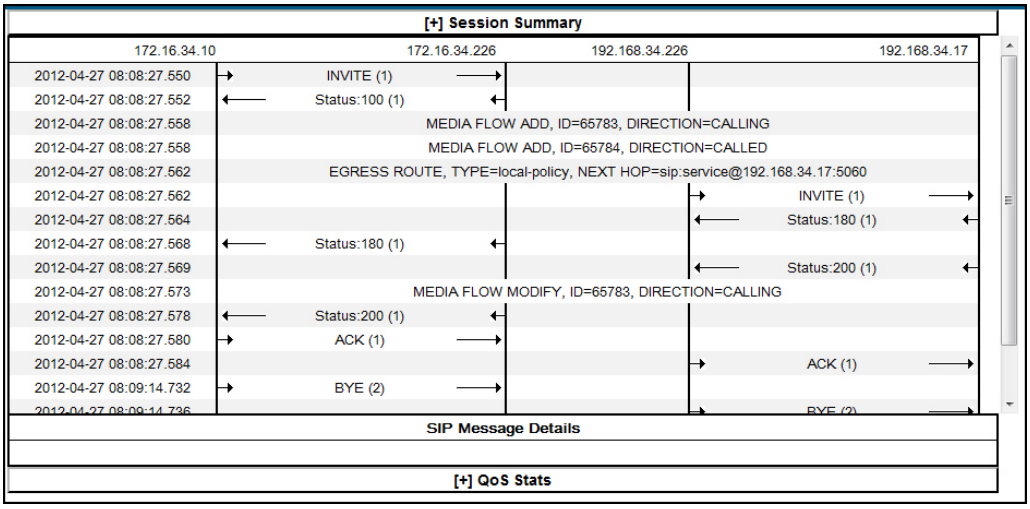
You can view the details of a call or media session by displaying the session summary from a selected record on a ladder diagram.

1. From the Web GUI, click **Monitor and Trace** > **Sessions**.
2. On the SIP Session Summary page, do one of the following:
   - Click Ladder Diagram.
   - Click a record in the table.
3. In the ladder diagram, click the **[+]** next to Session Summary at the top of the ladder diagram window.

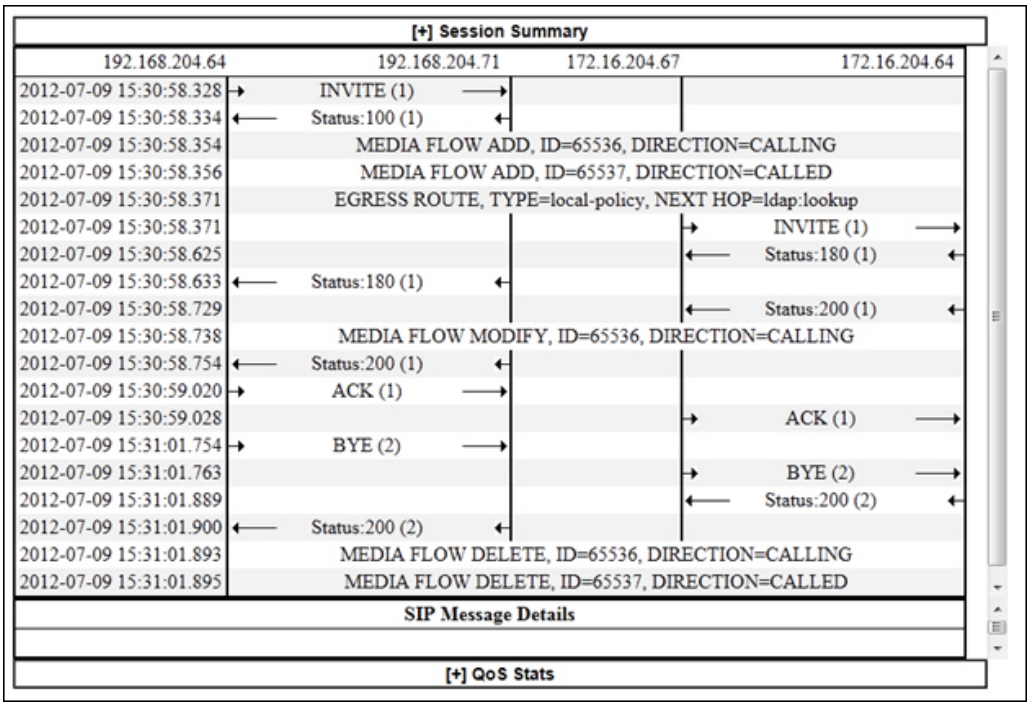
   The Session Summary window expands and displays a summary of information about the selected call or media session.

SIP Message Details

The SIP Message Detail window displays detailed information and data flow (ingress and egress) about the call or media event.

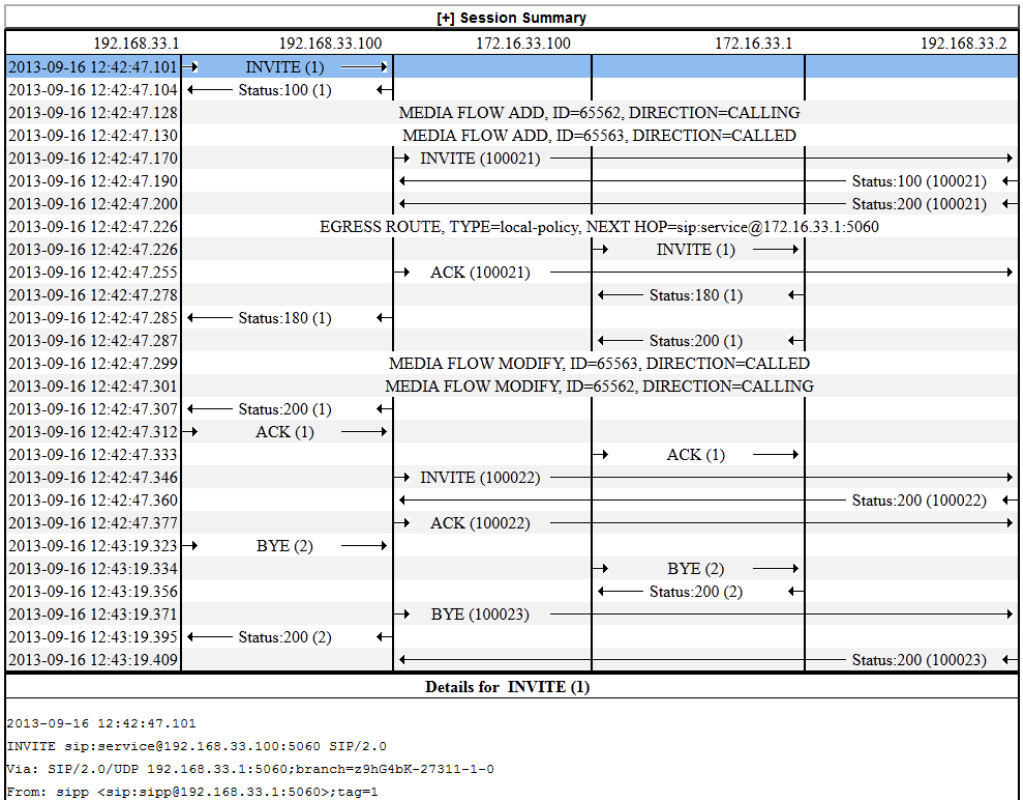


When a session is routed using the a Lightweight Directory Access Protocol (LDAP) configuration (Active Directory) for the local policy, the LDAP information displays in the Session Summary window. The next hop value containing "enum:…" or "dns:…" displays. Similarly, the next hop value "ldap:…" displays for LDAP queries.



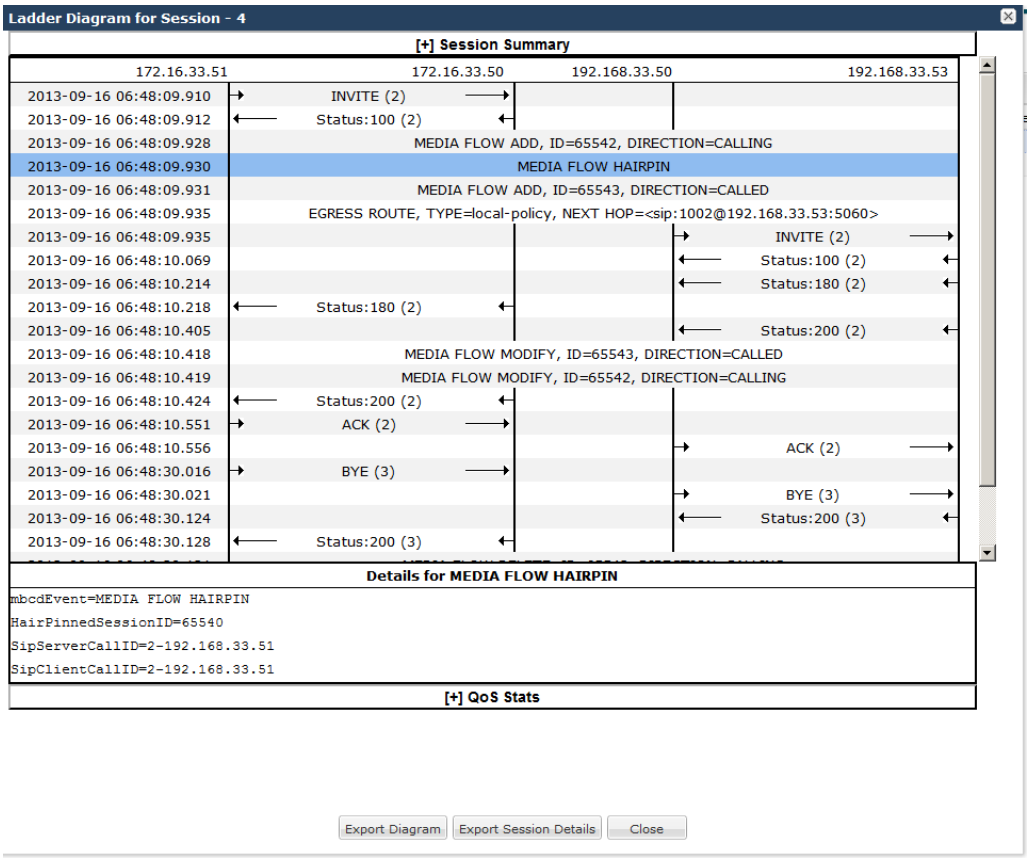
SIPREC Call Data

The following diagram shows SIP Monitor and Trace output for a call with media forwarded by way of SIPREC.



Hairpin Call Data

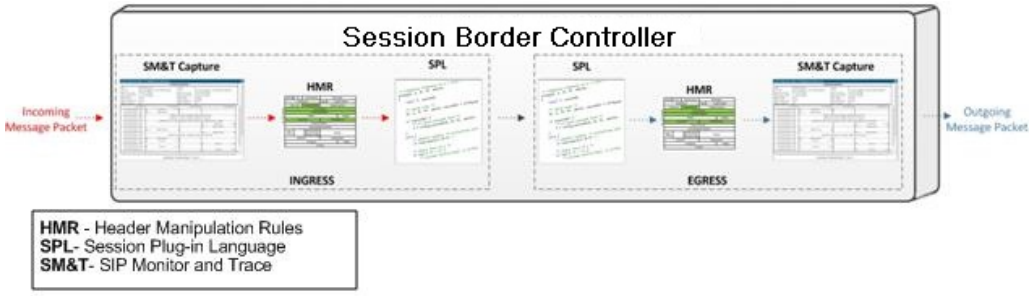
The following diagram shows SIP Monitor and Trace output for a hairpin call. Note the Media Flow Hairpin indication within the display.



SIP Monitor & Trace Ingress Egress Messages

The SIP Monitor and Trace feature allows the Oracle® Enterprise Session Border Controller (E-SBC) to monitor SIP sessions in your network. The system processes SIP Monitor and Trace data on incoming messages first and then sends the data out on outgoing messages. This allows the E-SBC to capture SIP Monitor and Trace data over the wire for display in the Web GUI.

The E-SBC captures a SIP message, applies the Header Manipulation Rules (HMR) configured on the E-SBC, and applies the Session Plug-in Language (SPL) to that message. When the message is sent out from the E-SBC, the E-SBC applies the SPL, applies the HMR, and sends out the captured SIP message.



Display SIP Message Details

Display the SIP Message Details window to view the messages and status codes that occurred during the active call session or media event. You can use the information to troubleshoot calls and media events that were unsuccessful or timed out while trying to connect.

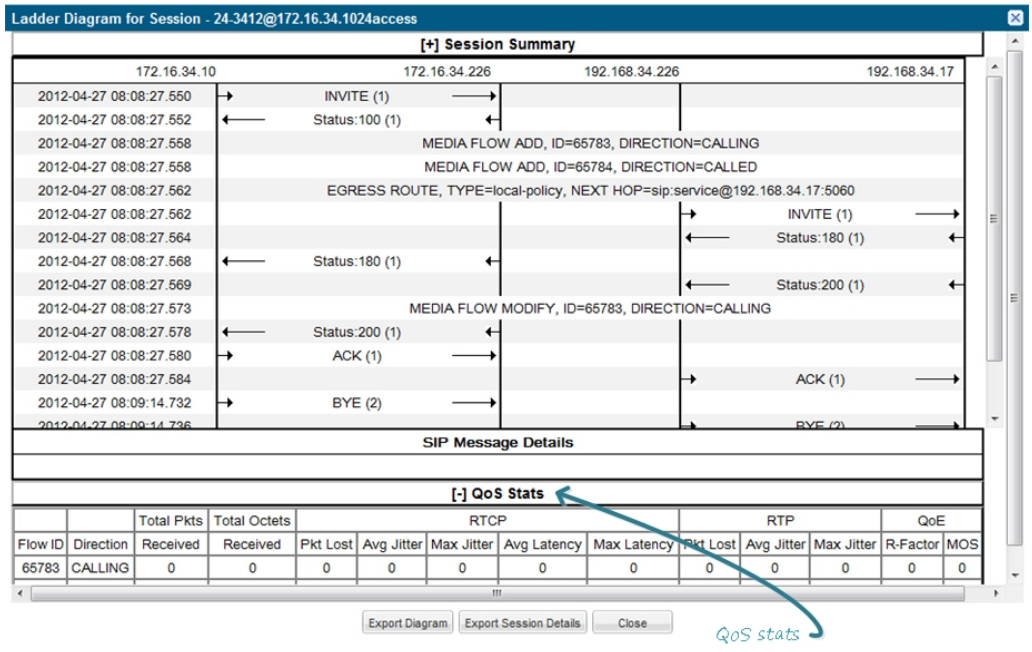
1. From the Web GUI, click **Monitor and Trace** > **Sessions**.
2. On the SIP Session Summary page, do one of the following:
   - Click Ladder Diagram.
   - Click a record in the table.

   The system displays the SIP Message Details window

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.

Expand QoS Stats section with the [+} control.



The following table describes each column in the QoS Stats display.

Heading	Description
Flow ID	ID number assigned to the call session or media event flow of data.
Direction	The direction of the call or media event flow. 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

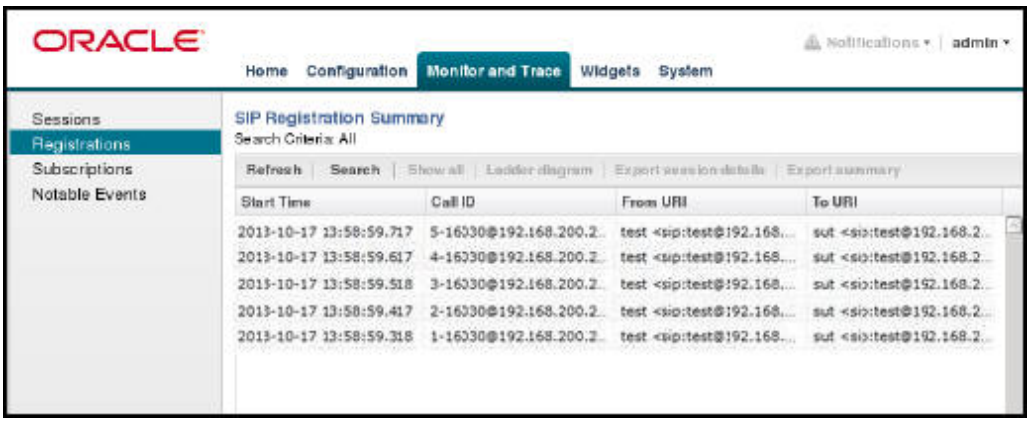
1. From the Web GUI, click **Monitor and Trace** > **Sessions**.
2. On the SIP Session Summary page, do one of the following:
   - Click Ladder Diagram.
   - Click a record in the table.
3. In the ladder diagram, click the **[+]** next to the QoS Stats section heading.

   The section expands and displays the QoS information about the selected call or media session.

Registrations Report

The Registrations Report displays a summary of all logged SIP registrations sessions on the Oracle® Enterprise Session Border Controller (E-SBC.

The columns that display on the Registration Report page depend on the columns you selected in the "Customizing the Page Display" procedure.

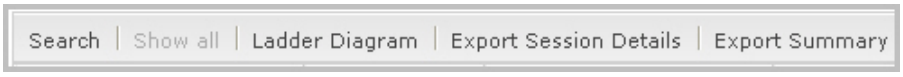


The following table describes the columns on this page.

Heading	Description
Start Time	Timestamp of the first SIP message in the call session.
Call ID	Identification of the call source. Includes the phone number and source IP address.
To URI	URI formatted string that identifies the call destination information.
From URI	URI formatted string that identifies the call source information.
Local Expires	The current setting for the expiration of a registration request sent from the Integrated Media Gateway (IMG) to a Remote SIP User Agent. The default is 3600 sec.

Heading	Description
Remote Expires	The current setting for the expiration of a registration request sent from the Remote SIP User Agent to the Integrated Media Gateway (IMG). The default is 3600 sec.
Ingress Realm	Incoming realm name.
Egress Realm	Outgoing realm name.
Notable Event	Indicates if a notable event has occurred on the call session. Valid value is: local rejection - Sessions locally rejected at the E-SBC for any reason (for example, Session Agent (SA) unavailable, no route found, SIP signalling error, etc.); Session dialogue, capture media information and termination signalling; Any event flagged as a local rejection interesting event
Session ID	Identification assigned to the call session.
Ingress Src Addr	Source IP address of the incoming call or media event.
Egress Dest Addr	Destination IP address of the outgoing call or media event.
Request URI	Uniform Resource Identifier (URI) formatted string that identifies a resource via a protocol, name, location, and any other applicable characteristic, and is sent by the E-SBC in REQUEST headers.

The following table describes the buttons on this page.

Button	Description
	
Search	Allows you to specify parameters for performing a search for specific session summary records within the current report.
Show all	Displays all of the session summary records in the Session Report.
Ladder Diagram	Displays a Ladder Diagram of a specific record in the table. The Ladder Diagram displays detailed information about a call session or media event.
Export Session Details	Exports the SIP messages and media events associated with the selected session, to a file in text format on the local machine.
Export Summary	Exports all logged session summary records to a file in text format on the local machine.

Display a Registrations Report

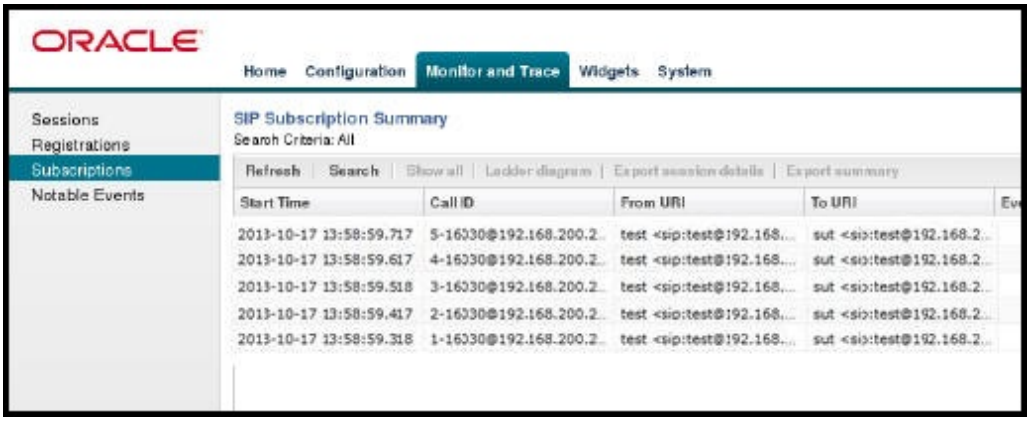
1. From the Web GUI, click **Monitor and Trace** > **Registrations**.

2. Use the buttons on the top of the page to view information about the records in this report.

Subscriptions Report

The Subscriptions Report 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 procedure, "Customizing the Page Display."



The following table describes the columns on this page.

Heading	Description
Start Time	Timestamp of the first SIP message in the call session.
Call ID	Identification of the call source. Includes the phone number and source IP address.
From URI	URI formatted string that identifies the call source information.
To URI	URI formatted string that identifies the call destination information.

Heading	Description
Events	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.
Local Expires	The current setting for the expiration of a registration request sent from the Integrated Media Gateway (IMG) to a Remote SIP User Agent. The default is 3600 sec.
Remote Expires	The current setting for the expiration of a registration request sent from the Remote SIP User Agent to the Integrated Media Gateway (IMG). The default is 3600 sec.
Ingress Realm	Incoming realm name.
Egress Realm	Outgoing realm name.
Notable Event	Indicates if a notable event has occurred on the call session. Valid value is: local rejection - Sessions locally rejected at the E-SBC for any reason (for example, Session Agent (SA) unavailable, no route found, SIP signalling error, etc.); Session dialogue, capture media information and termination signalling; Any event flagged as a local rejection interesting event
Session ID	Identification assigned to the call session.

Heading	Description
Ingress Src Addr	Source IP address of the incoming call or media event.
Egress Dest Addr	Destination IP address of the outgoing call or media event.
Request URI	Uniform Resource Identifier (URI) formatted string that identifies a resource via a protocol, name, location, and any other applicable characteristic, and is sent by the E-SBC in REQUEST headers.

The following table describes the buttons on this page.

Button	Description
	
Search	Allows you to specify parameters for performing a search for specific session summary records within the current report.
Show all	Displays all of the session summary records in the Session Report.
Ladder Diagram	Displays a Ladder Diagram of a specific record in the table. The Ladder Diagram displays detailed information about a call session or media event.
Export Session Details	Exports the SIP messages and media events associated with the selected session, to a file in text format on the local machine.
Export Summary	Exports all logged session summary records to a file in text format on the local machine.

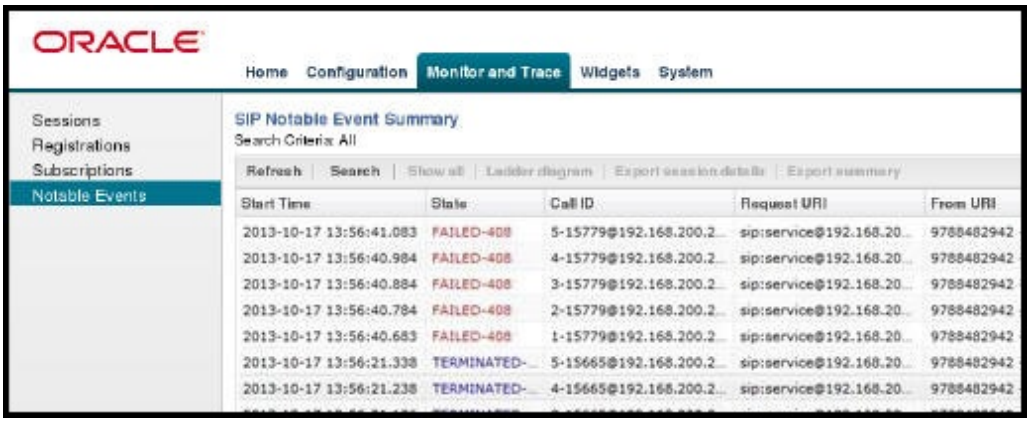
Display a Subscriptions Report

1. From the Web GUI, click **Monitor and Trace** > **Subscriptions**.
2. Use the buttons on the top of the page to view information about the records in this report.

Notable Events Report

The Notable Events Report contains all logged sessions with a notable event associated with the session on the Oracle® Enterprise Session Border Controller (E-SBC).

The columns that display on the Notable Events Report page depend on the columns that you selected in the procedure, "Customizing the Page Display."



The following table describes the columns that this page can display.

Heading	Description
Start Time	Timestamp of the first SIP message in the call session.
State	Status of the call or media event session. Valid values are: INITIAL Session for which an INVITE or SUBSCRIBE was forwarded. EARLY Session received the first provisional response (1xx other than 100). ESTABLISHED Session for which a success (2xx) response was received. TERMINATED Session that has ended by receiving or sending a BYE for an “Established” session or forwarding an error response for an “Initial” or Early session. The session remains in the terminated state until all the resources for the session are freed up. FAILED Session that has failed due to a 4xx or 5xx error code.
Call ID	Identification of the call source. Includes the phone number and source IP address.
Request URI	Uniform Resource Identifier (URI) formatted string that identifies a resource via a protocol, name, location, and any other applicable characteristic, and is sent by the E-SBC in REQUEST headers.
From URI	URI formatted string that identifies the call source information.
To URI	URI formatted string that identifies the call destination information.

Heading	Description
Notable Event	Indicates if a notable event has occurred on the call session. Valid values are: short session - Sessions that don't meet a minimum configurable duration threshold; Session dialogue, captured media information and termination signalling; Any event flagged as a short session interesting event. local rejection - Sessions locally rejected at the E-SBC for any reason (for example, Session Agent (SA) unavailable, no route found, SIP signalling error, etc.); Session dialogue, capture media information and termination signalling; Any event flagged as a local rejection interesting event.
Session ID	Identification assigned to the call session.
Ingress Src Addr	Source IP address of the incoming call or media event.
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.
Egress Dest Port	Destination port of the outgoing call or media event.
Object ID	ID number of the object in a row. Use to aid troubleshooting.

The following table describes the buttons on this page.

Button	Description
	
Search	Allows you to specify parameters for performing a search for specific session summary records within the current report.
Show all	Displays all of the session summary records in the Session Report.
Ladder Diagram	Displays a Ladder Diagram of a specific record in the table. The Ladder Diagram displays detailed information about a call session or media event.
Export Session Details	Exports the SIP messages and media events associated with the selected session, to a file in text format on the local machine.
Export Summary	Exports all logged session summary records to a file in text format on the local machine.

Display a Notable Events Report

1. From the Web GUI, click **Monitor and Trace** > **Notable Events**.

2. Use the buttons on the top of the page to view information about the records in this report.

Search for a 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.

Filter	Search Behavior	Instructions
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 REQUEST 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.

Filter	Search Behavior	Instructions
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 starting on April 15, 2012. Valid values are numeric characters only. • Enter a start time to search on in the last three text boxes in the format HH mm ss (where H=hour, m=minutes, and s=seconds). For example, 01 30 45 would search for all records starting at 1:30 and 45 seconds. Valid value are numeric characters only.
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 starting 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>

Filter	Search Behavior	Instructions
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.
In SA	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.
Out SA	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.
In Source Addr	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.
Out Dest Addr	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 initial*f* 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 table identifies the buttons to use to export specific information from Monitor and Trace. All the export buttons in the GUI export to text files.

Button	Description
From the Sessions, Registrations, Subscriptions, and Notable Events Reports:	
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.
From the Ladder Diagram:	
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 Trac report to a text file:

> **Note:**
>
> The GUI exports Ladder Diagrams as HTML files.

1. From the Web GUI, click the **Monitor and Trace** tab.
2. On the Monitor and Trace page, select a report type. For example, Subscriptions.
3. On the report Summary page, select a report from the list, and do one of the following:
   - Click **Export session details**.
   - Click **Export summary**.
4. In the SessionDetails.txt or SummaryExport.txt dialog, do one of the following:
   - Click **Open with**, and select the application with which to open the resulting text file.
   - Click **Save file** to save the text file to your local PC.
5. Click **OK** to export the report information.

7

Widgets Tab

The Widgets tab contains a list of all available widgets that you can use to view system data and statistics.

When you click the name of a Widget in either the navigation pane or the All Widgets list, the system displays the widget in full-screen mode. If you view a certain widget frequently, you might want to add it to the Favorite Widgets list on the Widgets page or add it to the Dashboard on the Home page. You can perform both tasks from the widget with the icons displayed in the upper right corner of the widget.

Types of Widgets

For each `show` command that you can use on the ACLI, the system provides a corresponding widget on the Web GUI.

A show command widget can display either a table or text, 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 show command widgets from either the list on the Widgets tab or the Add Widget dialog on the Home page. The Widgets tab displays a description for each show command.

Most of the show command widgets display any available data when you click the name of the widget. Some widgets require further input, and they display a settings dialog when you click the name of the widget. For example, the Realm Individual widget displays a dialog that requires the name of the realm and the auto refresh interval.

> **Note:**
>
> You must set up a valid SIP configuration before the Oracle® Enterprise Session Border Controller can display any SIP data on a widget, including the default widgets on the dashboard.

The Web GUI displays the following show command widgets:

Command Group	Web GUI Widget Name - ACLI Command the System Executes
Media	Classify - show media classify Host stats - show media host-stats MBCD • Acls - show mbcd acls • All - show mbcd all • Errors - show mbcd errors • Realms - show mbcd realms • Statistics - show mbcd statistics

Command Group	Web GUI Widget Name - ACLI Command the System Executes
	NAT • By index - show nat by-index • In tabular - show nat in-tabular Realm • Specifics - realm-specifics • Summary - show realm Xcode • Codecs - show xcode codecs • Load - show xcode load • Xlist - show xcode xlist
Signaling	DNS - show dns ENUM - show enum Fraud protection List • All - show fraud-protection all • Black list - show fraud-protection blacklist • Rate limit - show fraud-protection rate limit • Redirect - show fraud-protection redirect • White list - show fraud-protection white list Matches • All -show fraud-protection all matches-only • Black list - show fraud-protection blacklist matches-only • Rate limit - show fraud-protection rate limit matches-only • Redirect - show fraud-protection redirect matches-only • White list - show fraud-protection white list matches-only Summary - show fraud-protection stats H323d - show h323d LRT - show lrt Recording - show rec Registration • By realm -show registration sipd by realm • H323 - show registration h323d • SIP - show registration SIP • Statistics - show registration statistics Sessions - show sessions

Command Group	Web GUI Widget Name - ACLI Command the System Executes
	SIP • Agent details - show sipd agents • Agent groups - show sipd groups • Agent individual - show sipd agents <agent name> • Client trans - show sipd client • Codecs - show sipd codecs • Errors - show sipd errors • Interface individual - show sipd interface • Interface summary - show sipd interface • Method ack - show sipd ack • Method bye - show sipd bye • Method cancel - show sipd cancel • Method info - show sipd info • Method invite - show sipd invite • Method message - show sipd message • Method notify - show sipd notify • Method options - show sipd options • Method prack -show sipd prack • Method publish - show sipd publish • Method refer - show sipd refer • Method register - show sipd register • Method subscribe - show sipd SUBSCRIBE • Method update - show sipd update • Realms all - show sipd realms • Realms individual - show sipd realms <realm name> • Redundancy - show sipd redundancy • Server trans - show sipd server • Session all - show sipd sessions all • Session summary - show sipd sessions • Status - show sipd status

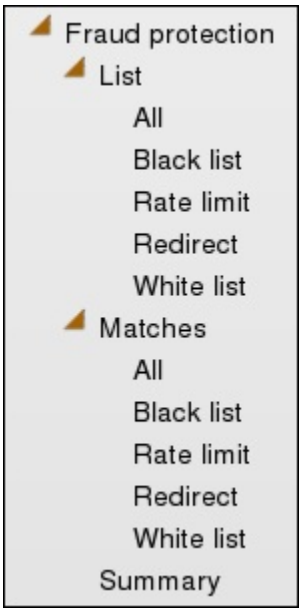
Command Group	Web GUI Widget Name - ACLI Command the System Executes
System	• Accounting - show accounting • ACL - show acl all • Alarms - show alarms • Authentication RADIUS - show radius all • Authentication TACACS - show tacacs stats • Communications Monitor Errors - show comm-monitor errors • Communications Monitor Internal - show comm-monitor internal • Communications Monitor Stats - show comm-monitor stats • Configuration Editing - show configuration • Configuration Editing short - show configuration short • Configuration Inventory - show configuration inventory • Configuration Running - show running-config • Configuration Running short - show running-config short • Configuration Version - show version • CPU Usage - cpu-monitor • Disk Usage - show space • Features - show features • Interfaces All - show interfaces • Interfaces Brief - show interfaces brief • Interfaces Mapping - show interface mapping • Interfaces Virtual - show virtual interfaces • Interfaces Wancom - show Wancom • L2/L3 ARP Info - show arp • L2/L3 ARP Statistics - show arp info • L2/L3 ARP Summary - show arp statistics • L2/L3 Connections - show ip connections • L2/L3 Neighbor table - show neighbor-table • L2/L3 Routes - show routes • L2/L3 Summary - show ip • L2/L3 TCP - show ip tcp • L2/L3 UDP - show ip udp • Licenses - licence • Memory Current memory - no ACLI command • Memory Historical Memory - no ACLI command • Memory Summary - show memory • Platform All - show platform all • Platform CPU load - show platform cpu-load • Platform Errors - show platform errors • Platform Limits - show platform limits • PROM info - show prom info all • Temperature - show temperature • Processes - show processes • SNMP Community table - show snmp-community-table

Command Group	Web GUI Widget Name - ACLI Command the System Executes
	• SNMP Trap Receiver - show trap-receiver • SPL Memory - show spl memory • SPL Options - show spl-options • SPL Statistics - show spl statistics • SPL Version - show spl • System health - show health • TDM Channels - show tdm channels • TDM Dialplan - show tdm dialplan • TDM Spans - show tdm spans • TDM Status - show tdm status • Time Clock - show clock • Time NTP Server - show ntp server • Time NTP Status - show ntp status • Time Time zone - show timezone • Time UTC - show clock utc • Uptime - show uptime • User management - show users • Version boot - show version boot • Version cpu - show version cpu • Version hardware - show version hardware • Version image - show version image • Version summary - show version

Telephony Fraud Protection Widgets

The Web GUI includes a set of widgets that displays lists of phone numbers used by the Oracle® Enterprise Session Border Controller (E-SBC) for telephony fraud protection. The lists under **List** show all entries. The lists under **Matches** show only the entries for which there was a match. The system requires an advanced license to enable the fraud protection widgets.

The navigation pane on the Widgets tab includes a node under Signaling called Fraud Protection, which you expand to display the following set of fraud protection widgets:

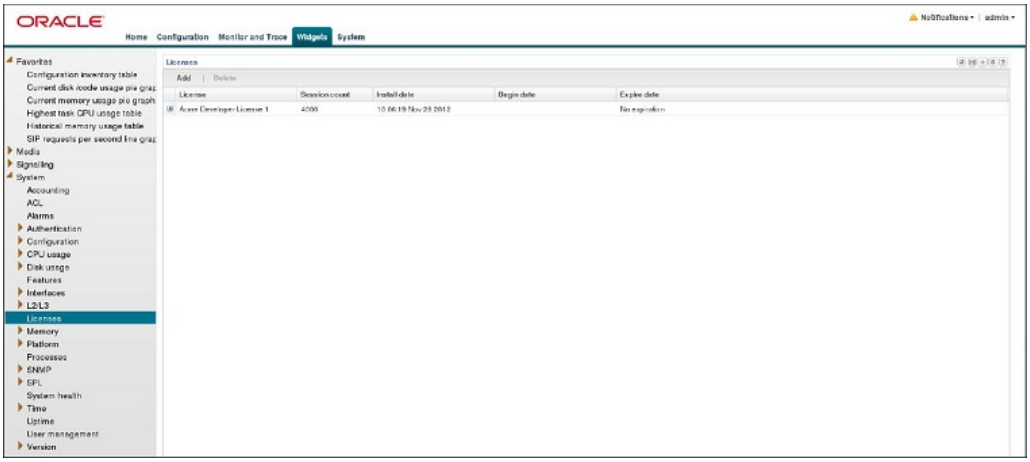


You cannot perform any actions on the entries displayed in any of these widgets. Use File Management on the System tab to work with entries on the fraud protection lists.

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**.



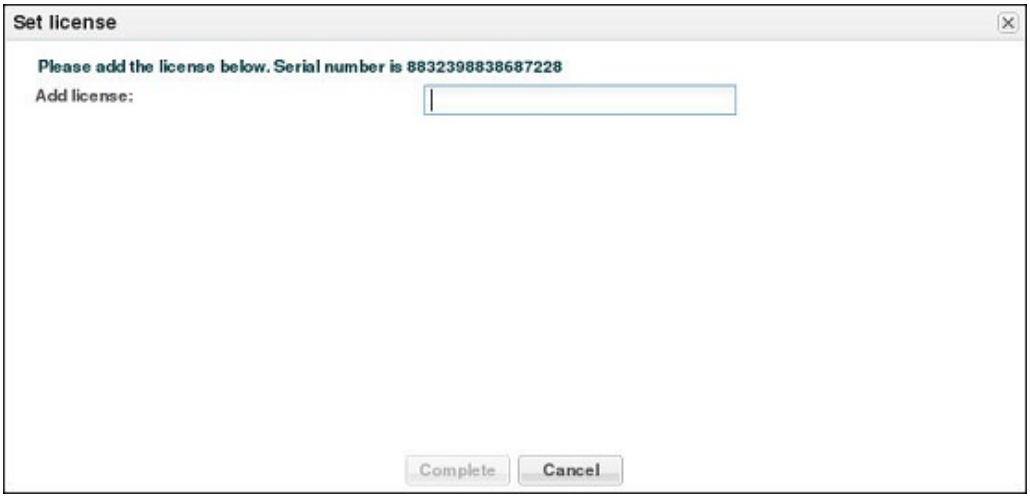
The Licenses page displays a list of your E-SBC licenses with the following information.

Column	Description
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.

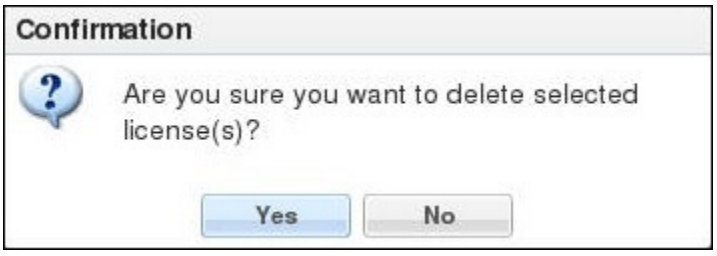
If you want to see the details of a particular license, click the show-hide toggle by the license name to expand the view to show all of the details. The following illustration shows an example of license details.

The Licenses widget provides the controls to Add and Delete licenses.

When you click **Add**, the system displays the Set license dialog.

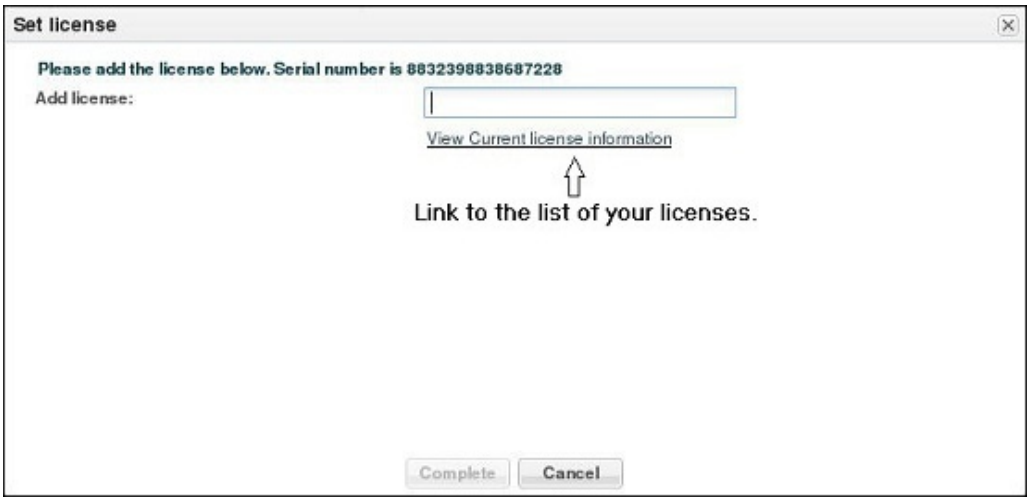


When you select a license from the Licenses list and click **Delete**, the system displays the delete Confirmation dialog.



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.



The only operations allowed in view mode are Refresh and Download.

Add a Widget to Favorites

If you view a widget often, you may want to add it to the Favorites list on the Widgets tab.

When you select a widget to add to Favorites, the system displays an icon of a push-pin on the tool bar at the top of the widget. Use the push-pin icon to add the widget to Favorites.

1. From the Web GUI Home page, click the Widgets tab.
2. From the All Widgets list, click the widget that you want to add to Favorites.

   The system displays the widget.
3. From the displayed widget, click the "Add the view to the favorites" icon. (Top, right. Shaped like a push-pin.)

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

8
System Tab

The System tab on the Web GUI provides the following ways to manage files on the system:

- File Management. Refresh. Upload, Download, Backup, Restore, and Delete files.
- Force HA Switchover. Force the system to switch from the primary to the secondary.
- Reboot. Reboot the system.
- Support information. Generate a file that displays troubleshooting information.
- Upgrade software. Verify system health, upload software, and reboot the system.

> **Note:**
>
> You can activate an LRT file, fraud protection file, or an SPL file dynamically upon an upload, if required. You can also immediately apply a backup configuration file during the upload process.

File Management

You can manage system files from the Web GUI on the File Management page.

The following table describes the files that you can manage under **File Management** on the Oracle® Enterprise Session Border Controller (E-SBC).

File Type	Format	Description
Backup configuration	.gz	File that contains a backup of the E-SBC software configuration. You can apply this file to restore a previous configuration if required.
Local route table (LRT)	.xml, .gz	Local routing table (LRT) file that you can apply to 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	Lists fraud protection files that you can upload, download, delete, or open to modify.

File Type	Format	Description
Log	Text	Log files that contain information about the various aspects of the E-SBC. For example, information logged about the ACLI, SIP, or H323. Note: Only the Download and Delete functions are applicable to log files on the E-SBC.
Playback media	Any media format valid in an RTP audio stream	Call progress playback files. The E-SBC can use these files in generated media streams if required. Note: The media files are raw binary files that contain data for the codec that a user wants to have played in the media stream. The E-SBC plays the data on the first audio flow in the Session Description Protocol (SDP).
Software Image	.gz, .bz	These files are bootable images.
SPL Plug-in	.lua	Session Plug-in Language (SPL) file that you can apply to the E-SBC to incorporate additional functionality. The SPL file contains a programming language that is capable of performing various tasks by utilizing APIs and callbacks in the E-SBC.

The following table describes the file management buttons.

Button	Description
Refresh	Updates the screen to display the latest data.
Upload	Uploads a file type from your server or PC to the E-SBC. The LRT, SPL, and backup configuration upload process provide the option of dynamically applying these files to the E-SBC.
Download	Downloads the file type from the E-SBC to your local server or PC (typically to the download directory on your system). Note: Download All applies only to log files.
Backup	File that contains a backup of the device software configuration. You can apply this file to restore a previous configuration.
Restore (Applicable to the “Backup configuration” file type only.)	Restores and applies a Backup configuration file to the E-SBC.
Delete	Deletes the file type from the E-SBC. Note: Delete All applies only to log files.

Manage Files

You can manage system files from the Web GUI on the File Management page.

> **Note:**
>
> You can activate an LRT file or an SPL file dynamically during an upload. You can also immediately apply a backup configuration file during the upload process.

1. From the Web GUI, click **System**.
2. On the System page, in the navigation pane, click **File management**.
3. On the File management page, select a file to view from the File type drop-down list.

   The system displays the file.
4. Use the controls on the tool bar to manage the file.

Group By Field

To customize the display of the File Management page on the System tab, you can group the elements by column head.

1. From the Web GUI, click **System**.
2. On the System page, under File management, select a file type from the drop-down list to group by field.
3. On the File Management page, click the column title by which you want to group the items.

   The system displays an arrow control to the right of the column title.
4. Click the arrow control, and click **Group By This Field** on the menu.

   The system displays the data by the selected group.

Upload a File

Procedure and conditions for uploading a file to the Oracle® Enterprise Session Border Controller (E-SBC).

You can upload the following file types from your local server or PC to the E-SBC:

- Backup configuration
- Local route table (LRT)
- Fraud protection table
- Playback media
- Software image
- SPL Plug-in (SPL)

> **Note:**
>
> You cannot upload log files.

The file extension must be applicable to the file type you select. For example, an SPL Plug-in file requires the .lua extension The following table shows the file extensions required for each file type, and the directory on the E-SBC where the system stores the uploaded file.

File Type	File Format	Directory
Backup Configuration	.gz	/code/bkups
Local route table (LRT)	.xml, .gz	/code/gzConfig
Fraud protection table	.gz, .gzip, .xml	/code/fpe
Playback media	Any media format valid in an RTP audio stream	/code/media
Software image	.bz	/code/images
SPL Plug-on (SPL)	.lua	/code/spl

You can dynamically activate the Local route table and SPL Plug-in during the upload process.

You can immediately restore a backup configuration file after an upload is complete.

1. From the Web GUI, click **System** > **File management**.
2. On the File management page, from the File type drop down list, select the type of file you want to upload.
3. In the Name column, select the file you want to upload.
4. Click **Upload**.
5. In the Upload file dialog, do the following:
   a. Click **Browse**.
   b. Select the file that you want to upload.
   c. Optional. For the Backup configuration file, select Restore the configuration after upload to apply a previous backed up configuration file immediately to the after the upload is complete.
   d. Optional. For the Local route table file type, select Activate the LRT file after upload to apply the LRT upon upload.
   e. Optional. For a Fraud protection file, select Activate the file after upload to apply the file upon upload.
   f. Optional. For the SPL Plug-in file type, select Activate the SPL file after upload to apply the SPL file upon upload.
   g. Click **Upload**.

Download a File

Procedure and conditions for downloading from the Oracle® Enterprise Session Border Controller (E-SBC).

You can download any of the following file types from your local server or PC to the E-SBC:

- Backup configuration
- Local route table (LRT)
- Fraud protection table
- Log
- Playback media
- Software image
- SPL Plug-in (SPL)

1. From the Web GUI, click **System** > **File management**.
2. On the File Management page, select the type of file you want to download from the File type drop down list.
3. In the Name column, select the file you want to download.

> **Note:**
>
> For Log file types, you can select multiple log files to download, or place a checkmark in the box to the left of the Name column heading to select all log files to download. When downloading multiple log files, the File Management GUI compresses the files into one .tar file and downloads that file to your local server or PC.

4. Click **Download**.
5. Do one of the following:
   - Click **Open with** and select the application to open the file.
   - Click **Save file** to save the file to your local server or PC.
6. Click **OK**.

   The system downloads the file to the folder on your local server or PC where your Browser sends all downloads (typically your “Download” folder) or opens (decompresses) the file type on your local server or PC (typically in the “Download” folder).

Delete a File

Procedure and conditions for deleting a file from the Oracle® Enterprise Session Border Controller (E-SBC).

You can delete any of the following file types from your local server, PC, and E-SBC:

- Backup configuration Software image
- Local route table (LRT)
- Fraud protection table
- Log
- Playback media
- Software image
- SPL Plug-in (SPL)

> **Note:**
>
> You can select a single or multiple files to delete.

1. On the System tab, in the **File type** drop down list, select the type of file that you want to delete.
2. In the Name column, select one or more files you want to delete.

> **Note:**
>
> For Log file types, place a checkmark in the box to the left of the Name column heading to select all log files to delete.

3. Click **Delete**. The system displays following message.

   Are you sure you want to delete the file?
4. Click **Yes**.

Back up a File

You can backup a configuration file from the Oracle® Enterprise Session Border Controller (E-SBC) to your local server or PC. Backup allows you to save configurations that you can restore to the E-SBC at a later time.

1. From the Web GUI, click **System**.
2. In the Select the file type field, select Backup configuration.
3. Select one or more configuration files to backup to your server or PC.
4. Click **Backup**.
5. Click **OK** to backup the configuration.

   The system downloads the file to your server or PC, typically into the download directory.

Restore a File

You can restore a backed up configuration file to the Oracle® Enterprise Session Border Controller (E-SBC).

1. In the **Select the file type** field, select **Backup configuration**.
2. Select a backup file to restore to the E-SBC.

> **Note:**
>
> **Restore** activates only when you select a backup file.

3. Click **Restore**.
4. Click **Yes**.

The system downloads the backup file to the E-SBC. The E-SBC re-boots and restores the configuration from the backup file.

Force an HA Switch Over

You can manually initiate a High Availability (HA) switch over from the Web GUI.

- 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.

Performing 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. From the Web GUI, click the **System** tab.
2. On the System page, in the navigation pane, click **Force HA switchover**.
3. On the Force HA switch over page, click **Switch to standby**.

   The system performs the role change.

System Reboot

You can manually reboot the Oracle® Enterprise Session Border Controller (E-SBC) from the Web GUI. Note that when you reboot the system from the Web GUI, the Web GUI is unavailable until the reboot is complete. If you have a High Availability (HA) deployment, connectivity to the secondary E-SBC is lost until the reboot is complete.

When the reboot is complete, the primary and secondary systems both display the logon screen. You must manually log on to each system.

When you perform a reboot from the Web GUI	The system behaves
and no boot is in process and the system is not failing over to the secondary system in an HA environment	The GUI session closes and the system displays the Logon screen. You cannot log on to the Web GUI until the reboot is complete on the E-SBC.
and a reboot is already in progress	The system displays a message indicating that a reboot cannot occur. The first reboot must complete before another reboot is initiated.
and the primary system is currently failing over to the secondary system in an HA environment	The system displays a message indicating that a reboot cannot occur. The HA switch over is underway. The secondary E-SBC is updating and getting its configuration from the primary E-SBC.

Obtain Support Information

You can manually generate a predefined file by way of the Web GUI that contains troubleshooting information. You can save the file and send it to Oracle Customer Support.

1. From the Web GUI, click the **System** tab.
2. On the System page, in the navigation pane, click **Support Information**.
3. On the Support information page, click **Support Information**.

   The system generates the file.
4. Save the file.

Upgrade Software

You can upgrade the system software from the System tab. The system requires a reboot after the upgrade.

1. From the Web GUI, click **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.

Upload method	Instructions
Local	Select a file from your system, and proceed to Step 4
Flash	Select a file already on the device, 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.