

# Oracle® Enterprise Session Border Controller

## Maintenance Release Guide



Release E-CZ7.3.0

February 2018

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

ORACLE®

Copyright © 2013, 2018, Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

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

# Contents

## About This Guide

---

## 1 Oracle Enterprise Session Border Controller Description

---

## 2 ECZ7.3.0M1

---

Platforms Supported	2-1
CPU Support for the Acme Packet 3820 and Acme Packet 4500	2-1
Platform Boot Loaders	2-2
NIU and Feature Group Requirements	2-2
QoS NIU Version Requirement for Acme Packet 3820 and Acme Packet 4500	2-4
Supported SPL Engines	2-4
New Features and Enhancements	2-5
Content Map	2-5
Active Directory-Based Routing Enhancement	2-6
Enhanced Video Call Statistics	2-8
H.323 Destination Address Based Routing	2-8
Enable H.323 Destination Address-Based Routing	2-8
Increased SIP Monitoring and Tracing Sessions	2-8
Incremental QoS Updates	2-8
License Widget	2-9
Locally Generated SIP Response on License Exhaustion	2-12
Opus Codec Transcoding Support	2-12
PKCS #12 Container Import and Export Capability	2-14
Export to a PKCS #12 File	2-15
Import a PKCS #12 File	2-15
Quad-Span for TDM	2-16
SILK Codec Transcoding Support	2-20
Suite B TLS Cryptography	2-22
Set TDM Configuration Wizard	2-22
TDM Settings on the Session Delivery Manager	2-25
Telephony Fraud Protection	2-27

Telephony Fraud Protection Target Matching Rules	2-28
Telephony Fraud Protection File Activation	2-30
Telephony Fraud Protection File Management	2-31
Telephony Fraud Protection Data Types and Formats	2-33
Create a Telephony Fraud Protection File	2-34
Upload a Telephony Fraud Protection File	2-36
Configure Telephony Fraud Protection - ACLI	2-37
Configure Telephony Fraud Protection - GUI	2-38
Activate a New Telephony Fraud Protection File - GUI	2-39
Edit a Telephony Fraud Protection File	2-40
Refresh the Telephony Fraud Protection File - ACLI	2-42
Telephony Fraud Protection Widgets	2-42
Telephony Fraud Protection ACLI Show Commands	2-43
Web GUI Enhancements	2-44
Types of Widgets	2-44
Widgets Removed from the Web GUI	2-48
Inherited Features	2-48
Behavioral Changes	2-49
Known Issues	2-49
Limitations	2-49
Caveats	2-50
Closed Caveats	2-50

### 3 ECZ7.3.0M2

---

Supported Platforms and Image Files	3-1
CPU Support for the Acme Packet 3820 and Acme Packet 4500	3-1
Platform Boot Loaders	3-2
NIU and Feature Group Requirements	3-2
QoS NIU Version Requirement for Acme Packet 3820 and Acme Packet 4500	3-4
Supported SPL Engines	3-4
Supported Upgrade Paths	3-5
New Features and Enhancements	3-5
Access the Web GUI with HTTPS	3-8
Advanced Logging	3-9
Configure Advanced Logging - Command Line	3-10
Configure Advanced Logging - Configure Mode	3-11
Configure Advanced Logging	3-12
View Advanced Logging Status - Command Line	3-12
Audit Logs	3-13
Secure FTP Push Configuration	3-15

Configure Secure FTP Push with Public Key Authentication	3-16
Configure Audit Logging	3-18
Certificate Storage Limits	3-20
CLIP and COLP Support for TDM	3-20
Configure Subnet Ranges in SNMP Community	3-21
Disable Server Certificate Validation	3-21
Preserve SIPREC with SIP REFER Header	3-22
Secure the ACP Communications Link with TLS	3-22
Security Enhancements	3-23
Suite B Support	3-23
Surrogate Registration	3-26
Registration	3-26
Routing Calls from the IP-PBX	3-27
Configure Surrogate Registration - GUI	3-27
Configure Surrogate Registration	3-29
TCP Connection Tools	3-32
TCP and SCTP State Connection Counters	3-32
show sipd tcp connections	3-34
show sipd tcp	3-35
Updated Show Commands	3-38
Web GUI Access with the Admin Security License	3-46
Web GUI Enhancements	3-51
Inherited Features	3-52
Link Redundancy	3-52
Caveats	3-54
Phy Link Redundancy Configuration	3-54
Deprecated Features and Functions	3-54
Known Issues	3-55
Limitations	3-56
Caveats	3-56
Closed Caveats	3-59

## List of Tables

---

2-1	Acme Packet 1100 NIU and Feature Group Support Matrix	2-2
2-2	Acme Packet 3820 NIU and Feature Group Support Matrix	2-3
2-3	Acme Packet 4500 NIU and Feature Group Support Matrix	2-3
2-4	Acme Packet 4600 NIU and Feature Group Support Matrix	2-3
2-5	Acme Packet 6300 NIU and Feature Group Support Matrix	2-3
2-6	Virtual Machine and Feature Group Support Matrix	2-3
3-1	Acme Packet 1100 NIU and Feature Group Support Matrix	3-2
3-2	Acme Packet 3820 NIU and Feature Group Support Matrix	3-3
3-3	Acme Packet 4500 NIU and Feature Group Support Matrix	3-3
3-4	Acme Packet 4600 NIU and Feature Group Support Matrix	3-3
3-5	Acme Packet 6300 NIU and Feature Group Support Matrix	3-3
3-6	Virtual Machine and Feature Group Support Matrix	3-3

# About This Guide

The Oracle Enterprise Session Border Controller (E-SBC) Maintenance Release Guide provides information about the new features, inherited features, known issues, limitations, and caveats added to the software since the E-CZ7.3.0 GA release.

The information contained in this guide pertains to Enterprise customers, and the following Oracle platforms:

- VM Edition. Designed for distributed small to medium enterprises, runs on a generic server within a virtual environment. Supports a maximum of 1000 concurrent SIP audio calls per Virtual Machine (VM). The VM Edition supports VMware virtualization software.
- Acme Packet Platforms. For medium to large enterprises, the Acme Packet 3820 supports up to 8,000 concurrent SIP audio calls, the Acme Packet 4500 supports up to 16,000 concurrent SIP audio calls, the Acme Packet 4600 supports up to 32,000 concurrent SIP audio calls, and the Acme Packet 6300 supports up to 80,000 concurrent SIP audio calls.
- Acme Packet Platforms: For small enterprises, the Acme Packet 1100 supports up to 360 concurrent audio calls.

Refer to the E-SBC E-CZ7.3.0 documentation set for more information about each platform.

## Audience

Enterprise users who want to know about new features, inherited features, known issues, limitations, and caveats for the E-CZ7.3.0 M2 release.

## Licensing

The E-CZ7.3.0 M2 release is an aggregation of software from various sources and organizations including Oracle software, third-party commercial software used under license, and publicly available software packages distributed under various open source licenses. For more information about the applicable licenses and how to obtain the source code for the open source components, use the following methods:

- Click **About** on the Web GUI Admin menu.
- Enter the `show about` command from the CLI
- Ask your Oracle representative.

## Documentation Set

The following table describes the documents included in the Oracle Enterprise Session Border Controller E-C.7.3.0 documentation set.

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

### Related Documentation

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

Document Name	Document Description
Acme Packet 3820 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 3820.
Acme Packet 4500 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4500.
Acme Packet 4600 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4600.
Acme Packet 6300 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6300.
Release Notes	Contains information about the current documentation set release, including new features and management changes.
ACLI Configuration Guide	Contains information about the administration and software configuration of the Oracle Enterprise Session Border Controller.
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Maintenance and Troubleshooting Guide	Contains information about Oracle Enterprise Session Border Controller logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
MIB Reference Guide	Contains information about Management Information Base (MIBs), Acme Packet's enterprise MIBs, general trap



Document Name	Document Description
	information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Accounting Guide	Contains information about the Oracle Enterprise Session Border Controller's accounting support, including details about RADIUS accounting.
HDR Resource Guide	Contains information about the Oracle Enterprise Session Border Controller's Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Administrative Security Essentials	Contains information about the Oracle Enterprise Session Border Controller's support for its Administrative Security license.
Security Guide	Contains information about security considerations and best practices from a network and application security perspective for the Oracle Enterprise Session Border Controller family of products.

### Revision History

Date	Revision Number	Description
November 6, 2015	1.0.0	Initial Release
December 5, 2015	1.0.1	<ul style="list-style-type: none"> <li>Adds the "Quad-Span for TDM" topic.</li> <li>Moves the "LDAP Support and the Acme Packet 6300" Caveat to Closed Caveats.</li> <li>Revises the "High Availability Configuration" Caveat.</li> </ul>
May 5, 2016	1.02	<ul style="list-style-type: none"> <li>Adds the "Upgrade Can Affect High Availability Operations" Known Issue.</li> </ul>
August 5, 2016	1.03	<ul style="list-style-type: none"> <li>Adds M2 content.</li> <li>Removes statements of support for SNMP alerts and traps for Telephony Fraud Protection.</li> <li>Removes the Note from the Telephony Fraud Protection topic that stated the M1 release supported only the stand alone mode for the management source.</li> <li>Adds clarification to the "Session Replication for Recording" Caveat.</li> </ul>
August 17, 2016	1.04	<ul style="list-style-type: none"> <li>Adds the KPML to RFC 2833 Interworking item to Closed Caveats.</li> </ul>
December 19, 2017	1.05	<ul style="list-style-type: none"> <li>Adds known issues list to E-CZ7.3.0M2 chapter</li> </ul>
February 7, 2018	1.06	<ul style="list-style-type: none"> <li>Updates E-CZ7.3.0M2 chapter's Known Issues table to coincide with E-CZ7.3.0m2p17</li> </ul>
February 27, 2018	1.07	<ul style="list-style-type: none"> <li>Updates E-CZ7.3.0M2 chapter's Known Issues table</li> </ul>

# 1

## Oracle Enterprise Session Border Controller Description

The Oracle Enterprise Session Border Controller (E-SBC) connects disparate Internet Protocol (IP) communications networks while mitigating security threats, curing interoperability problems, and ensuring reliable communications. The E-SBC protects and controls real-time voice, video, and Unified Communications (UC) as they traverse IP network borders.

### Overview

Available in software and appliance configurations, the E-SBC is highly scalable and includes an industry-leading feature set.

- **Strong security.** As the E-SBC protects IP telephony and UC infrastructure, services, and applications, it also ensures confidentiality, integrity, and availability. The E-SBC protects against fraud, service theft, malicious attacks, system overloads, and other events that affect service.
- **Easy interoperability.** The E-SBC provides extensive signaling and media control features to help businesses overcome interoperability challenges that commonly occur when interfacing with public IP network services. The E-SBC also performs protocol interworking and dial plan management for integration with legacy systems.
- **Assured reliability.** The E-SBC ensures Public Switched Telephone Networks (PSTN)-like availability and service quality for IP communications. The E-SBC enforces service quality, balances loads across trunks, and reroutes sessions around interface disruptions to optimize network performance, circumvents equipment and facility problems, and ensures business continuity.

### Functions and Modes

Businesses install the E-SBC at Session Initiation Protocol (SIP) network borders, where enterprise communications systems interface with public network services and where disparate multi-vendor systems must be managed.

Customers use the E-SBC to:

- Connect to SIP trunking services and the Internet
- Access communications services
- Communicate securely with remote workers
- Manage sessions across a multi-vendor UC environment
- Connect contact center locations and Business Process Outsourcing (BPO) services

# 2

## ECZ7.3.0M1

### Platforms Supported

The following platforms support the ECZ7.3.0M1 release.

- Oracle Hardware Platforms: Acme Packet 1100, Acme Packet 3820, Acme Packet 4500, Acme Packet 4600, and Acme Packet 6300
- Virtual Platforms: VMWare 5.5 ESXi Hypervisor

#### Release Image File Names

Use the following files for a new deployment.

Oracle Hardware

- Image:
  - Use nnECZ730m1.64.bz for the Acme Packet 1100, the Acme Packet 4500, Acme Packet 4600, and the Acme Packet 6300 for new installations and for upgrades.
  - Use nnECZ730m1.32.bz for the Acme Packet 3820.
- Boot loader: November 2013 or newer

Virtual Machines

- VMWare: nnECZ730m1.64-img-bin\_vmware.ova

#### Upgrade Image File Names

Use the following files to upgrade virtual machine deployments.

- Image: nnECZ730m1.64.bz
- Boot loader: nnECZ730m1.64.boot

### CPU Support for the Acme Packet 3820 and Acme Packet 4500

Note the following requirements for CPU support on the Acme Packet 3820 and the Acme Packet 4500.

- The system supports the following versions for the 32-bit Acme Packet 3820.

Board Revision	Minimum Version
3	v3.13
4	v4.03

- The system supports only the 64-bit CPU2 on the Acme Packet 4500, and only CPU revision MOD-0026-xx. The system does not support CPU revision MOD-0008-xx.

Board Revision	Minimum Version
3	v3.18
4	v4.10

- An Acme Packet 3820 older than August 2009 with a revision lower than 3.08 requires a BIOS update.

## Platform Boot Loaders

Oracle Enterprise Session Border Controller platforms require a boot loader to load the operating system and software.

### Stage 1 and Stage 2 Boot Loaders

Stage 1 and Stage 2 boot loaders on the nn4500 and the nn3820 must not be dated any earlier than July 3, 2013 (MOS patch #1815632). From the command line, use the **show version boot** command to view the boot loader version.

#### Note:

Network booting for release 7.x by way of FTP and TFTP on the nn4500 and the nn3820 requires the November 2013 or later boot loader.

### Stage 3 Boot Loader

All platforms require the Stage 3 boot loader. Every new software release contains a system software image and a Stage 3 boot loader. When you plan to upgrade your system image, upgrade the Stage 3 boot loader before booting the new system image.

The boot loader file name corresponds to the software image filename. For example, if the software image filename is nnECZ730.64.bz, the corresponding Stage 3 boot loader filename is nnECZ730.boot. The boot loader file must be installed as /boot/bootloader on the target system.

The Stage 3 boot loader is compatible with previous releases.

## NIU and Feature Group Requirements

The following tables list the feature groups for all hardware and virtual platforms that require a specific Network Interface Unit (NIU).

**Table 2-1 Acme Packet 1100 NIU and Feature Group Support Matrix**

NIU	IPSec	SRTP	QoS	Transcoding	ISDN PRI
Acme Packet 1100 Ethernet interface	✗	✓	✓	✓ (requires transcoding module)	✗
Acme Packet 1100 TDM interface	Not applicable	Not applicable	Not applicable	Not applicable	✓

**Table 2-2 Acme Packet 3820 NIU and Feature Group Support Matrix**

NIU	IPSec	SRTP	QoS	Transcoding
Clear (RJ45)	X	X	X	X
Clear (SFP)	X	X	X	X
ETCv1 *	✓	✓	✓	X
ETCv2	✓	✓	✓	X
Encryption	✓	✓	X	X
QoS	X	X	✓ **	X
Encryption & QoS	✓	✓	✓ **	X
Transcoding	X	X	✓ ***	✓

**Table 2-3 Acme Packet 4500 NIU and Feature Group Support Matrix**

NIU	IPSec	SRTP	QoS	Transcoding
Clear (RJ45)	X	X	X	X
Clear (SFP)	X	X	X	X
ETCv1 *	✓	✓	✓	X
ETCv2	✓	✓	✓	X
Encryption	✓	✓	X	X
QoS	X	X	✓ **	X
Encryption & QoS	✓	✓	✓ **	X
Transcoding	X	X	✓ ***	✓

**Table 2-4 Acme Packet 4600 NIU and Feature Group Support Matrix**

NIU	IPSec	SRTP	QoS	Transcoding
4x1Gig or 2x10Gig NIU	✓	✓	✓	✓ (requires transcoding module)

**Table 2-5 Acme Packet 6300 NIU and Feature Group Support Matrix**

NIU	IPSec	SRTP	QoS	Transcoding
2x10Gig NIU	✓	✓	✓	Transcoding Carrier Unit

**Table 2-6 Virtual Machine and Feature Group Support Matrix**

	IPSec	SRTP	QoS	Transcoding
Virtual Machine	X	✓	✓	✓ (G729, PCMU, PCMA)

### Footnotes

- \* The system does not support an ETCv1 Card with 4GB RAM. This NIU is identified by a revision lower than 2.09. Use the **show prom-info phy** command and see the ETC NIU **Functionalrev** attribute to confirm compatibility.
- \*\* IPv4, only.
- \*\*\* IPv4, only. Non-transcoded calls, only.
- \*\*\*\* Limited codec support. G711u, G711a, G729

## QoS NIU Version Requirement for Acme Packet 3820 and Acme Packet 4500

A Network Interface Unit (NIU) that supports the Quality of Service (QoS) feature group on the Acme Packet 3820 and the Acme Packet 4500, except the two Enhanced Traffic Control (ETC) cards, requires QoS Field Programmable Gate Array (FPGA) revision 2.19 or higher for the E-CZ7.3.0M1 release. The 2.20 FPGA upgrade image is available at My Oracle Support, <https://support.oracle.com/>, with a customer account.

If the QoS FPGA Hardware Revision is lower than 1.109 (which corresponds to 2.19 FPGA image), you need to upgrade the QoS FPGA image. Use the **show qos revision** command (or **show datapath ppx info** in S/E-CZ7.x.x forward) from the ACLI to find the QoS FPGA Hardware Revision number, for example:

```
ORACLE# show qos revision
QoS FPGA Hardware Revision is 1.109
ORACLE#
```

## Supported SPL Engines

Each release supports a number of versions of the SBC Programming Language (SPL) engine, which is required to run SPL plug-ins on the Oracle Enterprise Session Border Controller (E-SBC).

This release supports the following versions of the SPL engine.

- C2.0.0
- C2.0.1
- C2.0.2
- C2.0.9
- C2.1.0
- C2.1.1
- C2.2.0
- C2.2.1
- C2.3.1
- C3.0.0
- C3.0.1
- C3.0.2

- C3.0.3
- C3.0.4
- C3.0.6
- C3.0.7
- C3.1.0
- C3.1.1
- C3.1.2
- C3.1.3
- C3.1.4
- C3.1.5
- C3.1.6

Use the `show spl` command to see the version of the SPL engine running on the E-SBC.

## New Features and Enhancements

This chapter provides detailed information about each new feature and enhancement in the ECZ7.3.0M1 release.

## Content Map

The following table describes the new features and enhancements included in the E-CZ730M1 release.

Types	Descriptions
Adaptation	Active Directory Call Routing Enhancement - Adds the "or" and "and" operators for configuring an LDAP query with multiple attributes.
Adaptation	Enhanced Video Call Statistics - Adds H.264 to the list of available video call statistics.
Behavioral Change - Security	Default Passwords - Adds default password detection upon start up with forced password reset when detected.
Adaptation	H.323 Destination Address-Based Routing - When enabled, the E-SBC populates the Destination address/AliasAddress field with the IP address of the destination IP system and uses that address for the next hop.
Adaptation	Increased SIP Monitoring and Tracing Sessions - Increases the number of supported SIP monitoring and tracing sessions to 4,000 for all platforms, except the Acme Packet 3820.
Adaptation	Interim QoS Update - Adds a new setting for sampling voice quality on the Acme Packet 4600 and Acme Packet 6300 in 10 second increments.
Adaptation	License Widget - Adds a new widget to the Web GUI for viewing, adding, and deleting licenses.

Types	Descriptions
Adaptation	Locally Generated 503 Response for License Session Exhaustion - Adds capability for inserting custom text in the SIP Status and SIP reason fields on the local response map.
Adaptation	Opus Codec Transcoding Support - Adds the Opus codec as well as support for transrating, transcoding, and pooled transcoding to the Acme Packet 4600 and Acme Packet 6300 platforms.
Adaptation	PKCS #12 Container Import and Export Capability - Adds support for bundling a private key with the associated X509 public key certificate in a file for archiving, importing, and exporting.
Adaptation	SILK Codec Transcoding Support - Adds the SILK codec as well as support for transrating, transcoding, and pooled transcoding to the Acme Packet 4600 and Acme Packet 6300 platforms.
Adaptation	Quad Span TDM Card - Adds support for 4 spans with the new Time Division Multiplexing (TDM) card on the Acme Packet 1100.
Adaptation	Suite B Cryptography - Adds support for Suite B Transport Layer Security.
Adaptation	TDM Configuration Wizard - Adds the Set TDM Configuration wizard, which completes the TDM configuration after you create the tdm-object.
Feature	Telephony Fraud Protection - Adds configurable protection against fraudulent calls by way of blacklisting and the associated rules for handling fraudulent calls.
Adaptation	Web GUI Enhancements - Adds several enhancements to the Web GUI.

## Active Directory-Based Routing Enhancement

For configuring an LDAP query with multiple attributes, the Oracle Enterprise Session Border Controller (E-SBC) allows the **and** and **or** operators for more granular condition-based call routing.

On the Web GUI, the LDAP config / LDAP transactions dialog includes **and** and **or** in the Operation Type drop-down list.

**Add LDAP config / LDAP transactions**

App trans type:

Route mode:

Operation type:

or  
and



On the ACLI, the **and** and **or** operators display under the ldap-transactions element.

```

=====
LDAP Query No.1
=====
ldap-config
  name                               myLDAP
  state                               enabled
  ldap-servers                        1.1.1.1:1
  realm                               core
  authentication-mode                 Simple
  username                            cn=admin,dc=example,dc=com
  password                            *****
  ldap-search-base                    dc=example,dc=com
  timeout-limit                       16
  max-request-timeouts                3
  tcp-keepalive                       enabled
  ldap-sec-type                       None
  ldap-tls-profile                    None
  ldap-transactions
    app-trans-type                    ad-call-routing
    route-mode                        exact-match-only
    operation-type                    and
    ldap-cfg-attributes
      name                             telephoneNumber
      next-hop                         example.com
      realm                            peer
      extraction-regex                 (.*)
      value-format                     $1
    ldap-cfg-attributes
      name                             msRTCSIP-Options
      next-hop                         example.com
      realm                            peer
      extraction-regex                 .*
      value-format                     888

```

```

=====
LDAP Query No.2
=====
ldap-config
  name                               myLDAP2
  state                               enabled
  ldap-servers                        1.1.1.1:1
  realm                               core
  authentication-mode                 Simple
  username                            cn=admin,dc=example,dc=com
  password                            *****
  ldap-search-base                    dc=example,dc=com
  timeout-limit                       16
  max-request-timeouts                3
  tcp-keepalive                       enabled
  ldap-sec-type                       None
  ldap-tls-profile                    None
  ldap-transactions
    app-trans-type                    ad-call-routing
    route-mode                        exact-match-only
    operation-type                    or
    ldap-cfg-attributes
      name                             telephoneNumber
      next-hop                         example.com
      realm                            peer
      extraction-regex                 ^\+(.*)
      value-format                     $1
    ldap-cfg-attributes
      name                             msRTCSIP-Options
      next-hop                         example.com
      realm                            peer
      extraction-regex                 .*
      value-format                     999

```

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.

## Enhanced Video Call Statistics

The ECZ30M1 release adds H.264 to video call statistics. The **show sipd codecs <realm ID>** command displays media-processing statistics per SIP traffic. This command displays statistics per realm and requires a realm argument.

## H.323 Destination Address Based Routing

Users of H.323 video conferencing applications typically need to dial a publicly routable IP address to join the conference. When the Oracle Enterprise Session Border Controller (E-SBC) is deployed in a VPN environment, the E-SBC translates the dialed IP address as it routes the call from ingress to egress. When the H.323 destination address-based routing feature is enabled, the E-SBC populates the destinationAddress/AliasAddress field with the IP address of the destination IP system and uses that information to define the next-hop. This option requires enablement.

## Enable H.323 Destination Address-Based Routing

The H.323 destination address-based routing feature allows the Oracle Enterprise Session Border Controller (E-SBC) to populate the destinationAddress/AliasAddress field with the IP address of the destination IP system and use that information to define the next-hop. You can enable this option in the H.323 configuration.

### Procedure

To enable the H.323 destination address-based routing feature, enter `directDial` in the **Options** field in the H.323 configuration.

1. Access the **h323** configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# session-router
ORACLE(session-router)# h323
ORACLE(h323)#
```

2. For Options, enter `directDial`.
3. Save and activate the configuration.

## Increased SIP Monitoring and Tracing Sessions

The ECZ730M1 release increases the number of supported SIP monitoring and tracing sessions from 2,000 to 4,000 for all platforms except the Acme Packet 3820.

## Incremental QoS Updates

The Interim Quality of Service (QoS) Update setting on the Acme Packet 4600 and the Acme Packet 6300 provides a more granular view of voice quality for troubleshooting by providing updates in 10 second increments. Without the Interim QoS Update setting selected, the Oracle Enterprise Session Border Controller (E-SBC) probe provides an average Mean Opinion Score (MOS) only at the end of the call. A troubleshooter cannot see what occurred in other parts of the call. For example, suppose your employee or agent complains of poor voice quality that occurred in the middle of the call, but the average MOS score at the end of the call is 4.40. The

troubleshooter might determine that the quality is acceptable, without knowing that the score in the middle of the call is 2.50. The Interim QoS Update setting provides MOS scores every 10 seconds, and with more granular data to help troubleshooting efforts.

Standalone Palladion probes, such as those that run Palladion software on Linux COTS servers, provide MOS scores in 10 second time chunks. With the Interim QoS Update setting selected, the data presented in Palladion looks similar whether coming from an E-SBC probe, Palladion probe, or both. To configure the Acme Packet 4600 and the Acme Packet 6300 to sample voice quality information in 10 second increments, select **Interim QoS update** in system-config.

The E-SBC provides the following data, per ten second interval.

- start + end time of the stream
- IP 5-tuple information to correlate to SIP sessions
- correlation information if available
- SSRC of the RTP stream (to be checked)
- Codec type
- Codec change information (if codecs changed)

The E-SBC provides the following data, per ten second chunk.

- jitter
- min/avg/max
- histogram (optional), e.g. # of packets with jitter <5ms, <10ms, <20ms, ... >100ms.
- packet loss
- # of packets received
- # of packets lost
- discarded packets (optional, received 50+ms too late)
- R-factor (optional)
- MOS value (optional)

The E-SBC delivers voice quality details, as follows:

- Per RTP stream.
- In 10 second increments, where the increment starts on a full minute based on the NTP clock (not the start time of the stream).
- Intervals not covering the full 10 seconds do not have a MOS value.

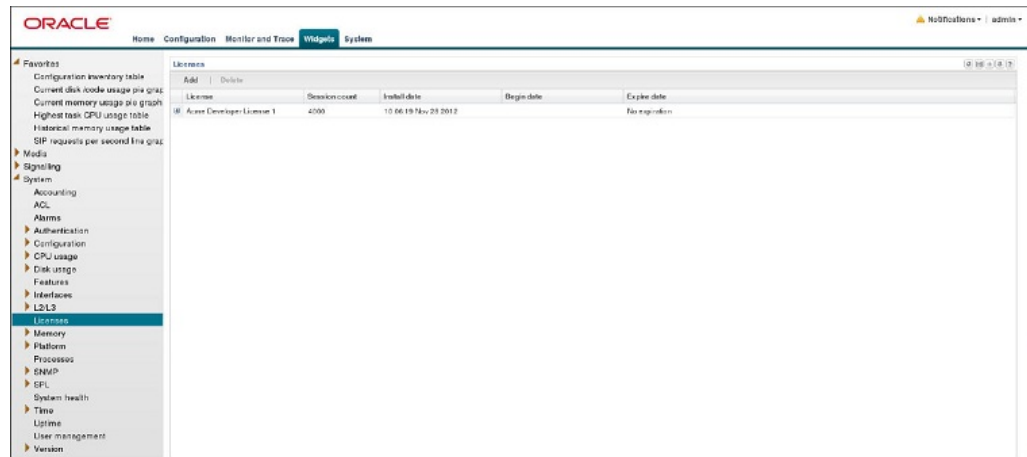
### Licensing

Interim QoS Update is already present in the native EOM probes. Using it requires a Media Quality Extension (MQE) license. This extension is already included in the base Enterprise license. Service Provider customers must purchase the MQE license in addition to the base Service Provider OCOM license.

## 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.

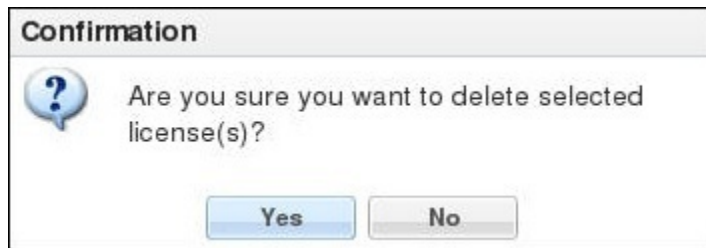


The Licenses widget provides the controls to Add and Delete licenses.

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.

## Locally Generated SIP Response on License Exhaustion

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 when you configure local response map entries.

When you configure the local response map in session-router, select licensed-session-capacity-reached from the Local Error list. You can add custom text about the error to the SIP header.

The following illustration shows the local response map configuration for licensed-session-capacity-reached from the Web GUI.

**Add Local response map / entries**

<b>Local error:</b>	<input type="text" value="licensed-session-capacity-reached"/>	
<b>SIP status:</b>	<input type="text" value="Custom text"/>	(Range: 100..699)
<b>Q850 cause:</b>	<input type="text" value="0"/>	(Range: 0..2147483647)
<b>SIP reason:</b>	<input type="text" value="Custom text"/>	
<b>Q850 reason:</b>	<input type="text"/>	
<b>Method:</b>	<input type="text"/>	
<b>Register response expires:</b>	<input type="text"/>	(Range: 0..999999999)

The following illustration shows the local response map configuration for licensed-session-capacity-reached from the ACLI.

```

local-response-map
entries
  local-error          licensed-session-capacity-reached
  sip-status           Custom text
  q850-cause           0
  sip-reason           Custom text
  q850-reason
  method
  register-response-expires
  
```

## Opus Codec Transcoding Support

Opus is an audio codec developed by the IETF that supports constant and variable bitrate encoding from 6 kbit/s to 510 kbit/s and sampling rates from 8 kHz (with 4 kHz bandwidth) to 48 kHz (with 20 kHz bandwidth, where the entire hearing range of the human auditory system can be reproduced). It incorporates technology from both Skype's speech-oriented SILK codec and Xiph.Org's low-latency CELT codec. This feature adds the Opus codec as well as support for transrating, transcoding, and pooled transcoding to the 4600 and 6300 platforms.

Opus can be adjusted seamlessly between high and low bit rates, and transitions internally between linear predictive coding at lower bit rates and transform coding at higher bit rates (as well as a hybrid for a short overlap). Opus has a very low algorithmic delay (26.5 ms by

default), which is a necessity for use as part of a low audio latency communication link, which can permit natural conversation, networked music performances, or lip sync at live events. Opus permits trading-off quality or bit rate to achieve an even smaller algorithmic delay, down to 5 ms. Its delay is very low compared to well over 100 ms for popular music formats such as MP3, Ogg Vorbis, and HE-AAC; yet Opus performs very competitively with these formats in terms of quality across bit rates.

Transcoding the Opus codec requires a special license as it is subject to a royalty agreement. Licensing supports up to the full density for this codec in bins of 25. A feature bit is required as well as a field for the capacity limit. The capacity limit is stored in 12 bits per codec allowing up to 102,375 licensed sessions. This limit is sufficient for future hardware iterations' projected session densities.

### Opus Supported Options

Required SDP Parameters:

**rate** — Specifies the sampling frequency. This parameter is mapped to the RTP clock rate in “a=rtpmap”. The range is limited to and must be 48000 Hz.

Optional SDP Parameters:

- **maxplaybackrate** — Specifies the maximum output sampling rate in Hz that the receiver is capable of rendering. The range is 8 kHz to 48 kHz; common values are 8, 12, 16, 24, and 48 kHz.
- **sprop-maxcapture** — Specifies the maximum input sampling rate in Hz that the sender is likely to produce. The Vocallo OCT2224 DSP currently supports only 8000 and 16000 Hz for transcoding. The range is 8 kHz to 48 kHz; common values are 8, 12, 16, 24, and 48 kHz.
- **ptime** — Specifies the packetization interval in milliseconds. The DSP supports packetization intervals of 10, 20, 40, 60, 80, and 100 ms. This parameter is mapped to “a=ptime” in the SDP. Possible values are 3, 5, 10, 20, 40, 60, or an arbitrary multiple of Opus frame sizes rounded up to the next full integer value up to a maximum value of 120. The default is 20 ms.
- **maxptime** — Specifies the maximum packetization interval allowed. The default is 100 ms.
- **minptime** — Specifies the minimum packetization interval allowed. The default is 20 ms.
- **maxaveragebitrate** — Specifies the maximum average rate of bits received for a session in bits per second. Although the range is 6000 to 51000, only bit rates of 6000 to 30000 bps are transcodable by the DSP. A media profile configured with a value for **maxaveragebitrate** greater than 30000 is not transcodable and cannot be added on egress in the **codec-policy** element.
- **stereo** — Specifies whether the decoder receives stereo or mono signals. The possible values are 0 (mono) and 1 (stereo). The default is 0.
- **sprop-stereo** — Specifies whether the sender is likely to produce stereo audio. The possible values are 0 (mono) and 1 (stereo). The default is 0.
- **cbr** — Specifies whether the decoder uses a constant or a variable bit rate. The possible values are 0 (variable bit rate) and 1 (constant bit rate). The default is 0.
- **useinbandfec** — Specifies whether the Opus decoder supports Forward Error Correction (FEC). The possible values are 0 (no) and 1 (yes). The default is 1.
- **usedtx** — Specifies whether the Opus decoder utilizes Discontinuous Transmission (DTX). The possible values are 0 (no) and 1 (yes). The default is 0.

The payload type is dynamic for this codec.

### Sample media-profile configuration for adding Opus

Parameter	Value
name	opus
subname	WB
media-type	audio
payload-type	104
transport	RTP/AVP
clock-rate	48000
req-bandwidth	0
frames-per-packet	0
parameters	maxplaybackrate=16000 sprop-maxcapture=16000 usedtx=0
average-rate-limit	5000
peak-rate-limit	0
max-burst-size	0
sdp-rate-limit-headroom	0
sdp-bandwidth	enabled
police-rate	0
standard-pkt-rate	0

### Monitoring and Debugging

CLI commands:

The **show sipd codecs** command is modified to add **opus Count**.

SNMP:

- New SNMP OID **apSysXCodeOPUSCapacity** is added to transcoding utilization statistics as reported in the **apSysMgmtGroupTrap**. When utilization falls below 80%, the **apSysMgmtGroupClearTrap** is sent.
- Opus realm statistic **apCodecRealmCountOPUS** is added to **apCodecRealmStatsEntry**.

Alarms:

Licensed Opus Transcoding Capacity Threshold Alarm — A warning level alarm that doesn't affect health is triggered when the Opus transcoding utilization exceeds 95% of licensed capacity. The alarm is cleared when the Opus transcoding utilization falls below 80% of licensed capacity.

## PKCS #12 Container Import and Export Capability

The Oracle Enterprise Session Border Controller (E-SBC) supports Public Key Cryptography Standard (PKCS) #12 for bundling a private key with the associated X.509 public key certificate in a file for archiving, importing, and exporting. The E-SBC does not support bundling all members of the chain of trust.

E-SBC customers often need to use keys and certificates stored in the E-SBC for Transport Layer Security (TLS) packet analysis and network troubleshooting, or to share with another E-



SBC or other device. The keys and certificates are packaged together and exchanged in the PKCS #12 archive file format.

 **Note:**

The E-SBC supports this functionality only by way of the ACLI.

## Export to a PKCS #12 File

You can export a local entity certificate from the Oracle Enterprise Session Border Controller (E-SBC) to a PKCS #12 file by way of the ACLI. You cannot do so from the Web GUI.

Use the following syntax on the ACLI.

 **Note:**

When prompted for password and passphrase, use the ones that you entered in system-config.

```
export-certificate <pkcs#12> <Certificate-record-name> [pkcs 12-file-name]
```

Where

- **Certificate-record-name**—the name of the local entity certificate record that you want to export.
- **Pkcs12-file-name**—the name of the target PKCS #12 file. The system creates the export file in the /opt directory. Use either .pfx or .p12 for the file extensions.

The following example shows the system display when exporting a certificate record named localCert to a PKCS #12 file from the E-SBC.

```
sd225v# export-pkcs12 localCert.p12
```

```
Creating pkcs12 for certificate-record: (localCert)
```

```
A certificate key found for making pkcs12 "localCert"
```

```
PKCS12 Certificate(s) exported successfully
```

## Import a PKCS #12 File

You can import a PKCS #12 key and certificate file that was generated elsewhere into the Oracle Enterprise Session Border Controller (E-SBC) by way of the ACLI.

Use the following syntax on the ACLI.

```
import-certificate <pkcs#12> <Certificate-record-name> [pkcs 12-file-name]
```

Where

- **Certificate-record-name**—must be a new name that does not exist as PKCS #12. This is different from other certificate imports, where the certificate record must already exist in the target destination.

- `Pkcs12-file-name`—the name of the PKCS #12 file that you want to import. Import the file to `/opt`.

The following example shows the system display when importing a PKCS #12 file named `localRecordCert.p12` into the E-SBC.

```
sd225v# import-certificate pkcs12 localCert localRecordCert.p12
```

```
The specified certificate-record (localCert) does not exist
```

```
Creating one...
```

```
Enter import password:
```

```
Certificate imported successfully...
```

```
Warning: Configuration changed. run 'save-config' and 'activate-config' commands to commit the changes.
```

## Quad-Span for TDM

If you want the Oracle Enterprise Session Border Controller (E-SBC) to handle more Time Division Multiplexing (TDM) calls than the single-span TDM card allows, you must order the optional quad-span TDM card. The quad-span card increases the maximum number of TDM calls by providing four ports to connect up to four PSTN or TDM networks. Each port handles one span of voice channels plus the corresponding signaling channel. With the quad-span card, T1 TDM calls can increase from 23 to 92 and E1 TDM calls can increase from 30 to 120.

When you configure the quad-span TDM card in `tdm-config`, the system defaults to the maximum of 4 spans. You can specify fewer spans by entering `number-of-spans` in the Options field along with the number of spans that you want. After you configure `tdm-config`, the system duplicates the configuration to each of the specified number of spans and automatically increments the b-channel and d-channel settings sequentially for each span. The system does not allow you to configure each span individually.

### Examples of Automatic Channel Incrementing Results

Suppose you keep the default of 4 spans and specify the T1 line-mode. The system duplicates the span 1 configuration to spans 2-4 and increments the bchan and dchan settings as follows:

Span	B Channel (voice)	D Channel (signaling)
Span 1	bchan=1-23	dchan=24
Span 2	bchan=25-47	dchan=48
Span 3	bchan=49-71	dchan=72
Span 4	bchan=73-95	dchan=96

Suppose you keep the default of 4 spans and specify the E1 line-mode. The system duplicates the span 1 configuration to spans 2-4 and increments the bchan and dchan settings as follows:

Span	B Channel (voice)	D Channel (signaling)
Span 1	bchan=1-15,17-31	dchan=16
Span 2	bchan=32-46, 79-93	dchan=47
Span 3	bchan=63-73,79-93	dchan=78
Span 4	bchan=94-108,110-124	dchan=109

## TDM Show Command Results

The system provides the following show commands for TDM spans and channels.

Command	Description
show-tdm-spans	Displays the following states for spans: <ul style="list-style-type: none"><li>• Active—The span is powered.</li><li>• Down—The span is not connected.</li><li>• In alarm—The connected span is down.</li><li>• Up—The span is connected.</li></ul>
show-tdm-span #	Displays the state and configuration profile of the specified span.
show-tdm-channels	Displays the following information about the TDM channels: <ul style="list-style-type: none"><li>• Context—Incoming TDM calls = from-pstn. Outgoing TDM calls = from-sbc.</li><li>• State—The status of the TDM channels, for example, In Service.</li></ul>
show-tdm-channel #	Displays the profile of the specified channel.

## Examples of the TDM Span and Channel Show Commands

The `show-tdm-spans` command always displays information about all four spans, whether or not they are all configured. For example, suppose that you specify one span in the configuration. The system displays the following:

```
show tdm spans
```

```
Tdm Command Output
```

```
PRI span 1/0: Up, Active  
PRI span 2/0: In Alarm, Down, Active  
PRI span 3/0: In Alarm, Down, Active  
PRI span 4/0: In Alarm, Down, Active
```

The `show-tdm-span #` command displays the following information for the specified span, which is TDM span 1 in this example.

```
show tdm span 1

Tdm Command Output
Primary D-channel: 16
Status: Up, Active
Switchtype: EuroISDN
Type: Network
Remote type: Network
Overlap Dial: 0
Logical Channel Mapping: 0
Timer and counter settings:
  N200: 3
  N202: 3
  K: 7
  T200: 1000
  T201: 1000
  T202: 10000
  T203: 10000
  T303: 4000
  T305: 30000
  T308: 4000
  T309: 6000
  T312: 6000
  T313: 4000
  T316: -1
  N316: 2
  T-HOLD: 4000
  T-RETRIEVE: 4000
  T-RESPONSE: 4000
  T-STATUS: 4000
  T-ACTIVATE: 10000
  T-DEACTIVATE: 4000
  T-INTERROGATE: 4000
  T-RETENTION: 30000
  T-CCBS1: 4000
  T-CCBS2: 2700000
  T-CCBS3: 20000
  T-CCBS4: 5000
  T-CCBS5: 3600000
  T-CCBS6: 3600000
  T-CCNR2: 10800000
  T-CCNR5: 11700000
  T-CCNR6: 11700000
Q931 RX: 0
Q931 TX: 0
Q921 RX: 241
Q921 TX: 241
Q921 Outstanding: 0 (TEI=0)
Total active-calls:0 global:0
CC records:
Overlap Recv: No
```

The `show-tdm-channels` command displays the following information about each channel in a specified span, which is E1 span 1 in this example.

```
show tdm channels
```

Tdm Chan	Command	Output	Context	Language	MOH Interpret	Blocked	State	Description
pseudo			default		default		In Service	
1			from-pstn		default		In Service	
2			from-pstn		default		In Service	
3			from-pstn		default		In Service	
4			from-pstn		default		In Service	
5			from-pstn		default		In Service	
6			from-pstn		default		In Service	
7			from-pstn		default		In Service	
8			from-pstn		default		In Service	
9			from-pstn		default		In Service	
10			from-pstn		default		In Service	
11			from-pstn		default		In Service	
12			from-pstn		default		In Service	
13			from-pstn		default		In Service	
14			from-pstn		default		In Service	
15			from-pstn		default		In Service	
17			from-pstn		default		In Service	
18			from-pstn		default		In Service	
19			from-pstn		default		In Service	
20			from-pstn		default		In Service	
21			from-pstn		default		In Service	
22			from-pstn		default		In Service	
23			from-pstn		default		In Service	
24			from-pstn		default		In Service	
25			from-pstn		default		In Service	
26			from-pstn		default		In Service	
27			from-pstn		default		In Service	
28			from-pstn		default		In Service	
29			from-pstn		default		In Service	
30			from-pstn		default		In Service	
31			from-pstn		default		In Service	

The `show-tdm-channel #` command displays the following information about the specified channel, which is TDM channel 1 in this example.

```
show tdm channel 1

Tdm Command Output
Channel: 1
Description:
File Descriptor: 10
Span: 1
Extension:
Dialing: no
Context: from-pstn
Caller ID:
Calling TON: 0
Caller ID subaddress:
Caller ID name:
Mailbox: none
Destroy: 0
InAlarm: 0
Signalling Type: ISDN PRI
Radio: 0
Owner: <None>
Real: <None>
Callwait: <None>
Threeway: <None>
Confno: -1
Propagated Conference: -1
Real in conference: 0
DSP: no
Busy Detection: no
TDD: no
Relax DTMF: yes
Dialing/CallwaitCAS: 0/0
Default law: alaw
Fax Handled: no
Pulse phone: no
Gains (RX/TX): 0.00/0.00
Dynamic Range Compression (RX/TX): 0.00/0.00
DND: no
Echo Cancellation:
    128 taps
    currently OFF
Wait for dialtone: 0ms
PRI Flags:
PRI Logical Span: Implicit
Hookstate (FXS only): Onhook
```

## SILK Codec Transcoding Support

SILK is an audio codec developed by Skype Limited that supports bit rates from 6 kbit/s to 40 kbit/s and sampling rates of 8, 12, 16, or 24 kHz. It can also use a low algorithmic delay of 25 ms (20 ms frame size + 5 ms look-ahead). This feature adds the SILK codec as well as support for transrating, transcoding, and pooled transcoding.

Transcoding the SILK codec requires a special license as it is subject to a royalty agreement. Licensing supports up to the full density for this codec in bins of 25. A feature bit is required as well as a field for the capacity limit. The capacity limit is stored in 12 bits per codec allowing up to 102,375 licensed sessions. This limit is sufficient for future hardware iterations' projected session densities.

## SILK Supported Options

### Required SDP Parameters:

**rate** — Specifies the sampling frequency. SILK supports four different audio bandwidths – narrowband at 8 kHz, mediumband at 12 kHz, wideband at 16 kHz, and super wideband at 24 kHz. This parameter is mapped to the RTP clock rate in “a=rtpmap”. The DSP only supports audio sampling rates of 8 kHz and 16 kHz for transcoding; the 12 kHz and 24 kHz bandwidths are not transcodable.

### Optional SDP Parameters:

- **ptime** — Specifies the packetization interval in milliseconds. The DSP supports packetization intervals of 20, 40, 60, 80, and 100 ms. This parameter is mapped to “a=ptime” in the SDP. The default is 20 ms.
- **maxptime** — Specifies the maximum packetization interval in milliseconds. The default is 100 ms.
- **minptime** — Specifies the minimum packetization interval in milliseconds. The default is 20 ms.
- **maxaveragebitrate** — Specifies the maximum average rate of bits received for a session in bits per second. Bit rates of 5000 to 30000 bps are transcodable by the DSP.
- **usedtx** — Specifies whether the SILK decoder utilizes Discontinuous Transmission (DTX). The possible values are 0 (no) and 1 (yes). The default is 0.

The payload type is dynamic for this codec.

### Sample media-profile configuration for adding SILK

Parameter	Value
name	SILK
subname	wideband
media-type	audio
payload-type	103
transport	RTP/AVP
clock-rate	16000
req-bandwidth	0
frames-per-packet	0
parameters	
average-rate-limit	5000
peak-rate-limit	0
max-burst-size	0
sdp-rate-limit-headroom	0
sdp-bandwidth	enabled
police-rate	0
standard-pkt-rate	0

## Monitoring and Debugging

### CLI commands:

The **show sipd codecs** command is modified to add **SILK Count**.

SNMP:

- New SNMP OID **apSysXCodeSILKWBCapacity** is added to transcoding utilization statistics as reported in the **apSysMgmtGroupTrap**. When utilization falls below 80%, the **apSysMgmtGroupClearTrap** is sent.
- SILK realm statistic **apCodecRealmCountSILK** is added to the **apCodecRealmStatsEntry** table located in the `ap-tc.mib`.

Alarms:

Licensed SILK Transcoding Capacity Threshold Alarm — A warning level alarm that doesn't affect health is triggered when the SILK transcoding utilization exceeds 95% of licensed capacity. The alarm is cleared when the SILK transcoding utilization falls below 80% of licensed capacity.

## Suite B TLS Cryptography

The Oracle Enterprise Session Border Controller (E-SBC) supports Suite B for Transport Layer Security (TLS).

The E-SBC supports the following Elliptical Curve Digital Signature Algorithm (ECDSA) cipher suites.

- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384

You can enable one or both of these cipher suites by configuring the `cipher-list` parameter in `TLS-profile`.

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

- `key-algor`—Public key algorithm. Supports RSA and ECDSA. Default: RSA Security.
- `digest-algor`—Digest to use for signing a certificate. Supports SHA1, SHA256, and SHA384. Default: SHA1.
- `ecdsa-key-size`—ECDSA key size. Supports p256 and p384.

These parameters are included in the "Add a Certificate Record" procedure, which you can perform from the ACLI and the Web GUI.

## Set TDM Configuration Wizard

The Set TDM Configuration wizard is a tool that you use to complete the Time Division Multiplexing (TDM) configuration after you create the `tdm-object`. The wizard completes the configuration by creating the realm, SIP interface, steering pools, and other necessary configuration elements including the network interface and the physical interface for SIP call routing. If you have an SRTP license, 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 or the ACLI.

The Oracle Enterprise Session Border Controller (E-SBC) requires running the Set 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.



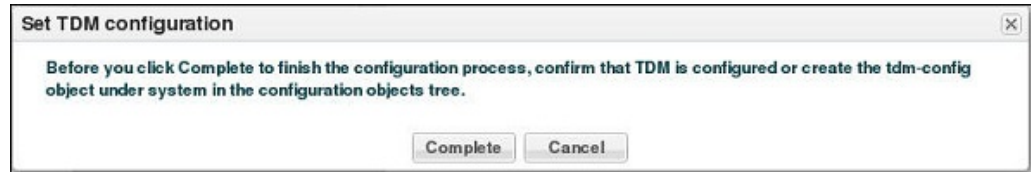
 **Note:**

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 Set TDM Configuration wizard. See "TDM Settings on the Session Delivery Manager" for the required settings.

The following sections describe the system behavior from the Web GUI and from the CLI.

**Web GUI**

When you create the tdm-config object from the Web GUI, and click **OK**, the system displays the Set TDM Configuration dialog.



When you click **Complete**, the wizard finishes the configuration and displays a success message upon successful completion or an error message if the completion is unsuccessful.

The following illustrations show the settings the that wizard configures.

Objects and Attributes	Settings
Realm	
SIP Interface	
Steering Pool	
Network Interface	
Physical Interface	
media-sec-policy (With the SRTP license)	
secured-network attribute for sip-interface (With the SRTP license)	
media-sec-policy attribute for realm-config (With the SRTP license)	

 **Note:**

- The Set TDM Configuration wizard is not available in Basic mode. When you configure TDM in Basic mode, the system automatically completes the configuration.
- The system displays the Set TDM Configuration wizard on the Web GUI only when you log on directly to Expert mode. When you log on to the Web GUI in Basic mode and switch to Expert mode, the system does not display the Set TDM Configuration wizard on the Wizards menu.

**ACLI**

When you configure the `tdm-config` object from the ACLI, use the `#setup tdm` command to run the wizard. The wizard finishes the configuration and displays a success message upon successful completion or an error message if the completion is unsuccessful.

The following illustration shows an example of the ACLI display after running the wizard on a system with an SRTP license.

```

codec-policy
  name                    e1CodecPolicy
  allow-codecs            *
  add-codecs-on-egress   PCMA
codec-policy
  name                    t1CodecPolicy
  allow-codecs            *
  add-codecs-on-egress   PCMU
media-sec-policy
  name                    tdmMediaSec
network-interface
  name                    tdm_p0
  ip-address              203.0.113.1
  netmask                 255.255.255.0
  gateway                 203.0.113.2
phy-interface
  name                    tdm_p0
  operation-type          Media
  slot                    2
realm-config
  identifier              tdmRealm
  network-interfaces     tdm_p0:0
  media-sec-policy       tdmMediaSec
  codec-policy           t1CodecPolicy
sip-config
sip-interface
  realm-id                tdmRealm
  sip-port
    address               203.0.113.1
  secured-network         enabled
snmp-community
  community-name         public
  ip-addresses           172.30.0.165
steering-pool
  ip-address              203.0.113.1
  start-port              20000
  end-port                40000

```

```

        realm-id                tdmRealm
    network-interface          tdm_p0:0
system-config
    default-gateway            172.30.0.1
tdm-config
    tdm-profile
        name                    tdm-config-test
web-server-config

```

The following illustration shows an example of the ACLI display after running the wizard on a system with no SRTP license.

```

codec-policy
    name                       e1CodecPolicy
    allow-codecs                *
    add-codecs-on-egress       PCMA
codec-policy
    name                       t1CodecPolicy
    allow-codecs                *
    add-codecs-on-egress       PCMU
network-interface
    name                       tdm_p0
    ip-address                  203.0.113.1
    netmask                     255.255.255.0
    gateway                     203.0.113.2
phy-interface
    name                       tdm_p0
    operation-type              Media
    slot                        2
realm-config
    identifier                  tdmRealm
    network-interfaces          tdm_p0:0
    codec-policy                t1CodecPolicy
sip-config
sip-interface
    realm-id                    tdmRealm
    sip-port
        address                 203.0.113.1
steering-pool
    ip-address                  203.0.113.1
    start-port                  20000
    end-port                    40000
    realm-id                    tdmRealm
    network-interface          tdm_p0:0
system-config
    default-gateway            172.30.0.1
tdm-config
    tdm-profile
        name                    tdm-config-test
web-server-config

```

## TDM Settings on the Session Delivery Manager

In a deployment where the Oracle Enterprise Session Border Controller (E-SBC) is managed by the Session Delivery Manager (SDM), and you want to use Time Division Multiplexing (TDM), configure TDM on the SDM with the following settings.

### With an SRTP License

Use the following settings for TDM when you own an SRTP License.

```

codec-policy
  name          e1CodecPolicy
  allow-codecs  *
  add-codecs-on-egress PCMA
codec-policy
  name          t1CodecPolicy
  allow-codecs  *
  add-codecs-on-egress PCMU
media-sec-policy
  name          tdmMediaSec
network-interface
  name          tdm_p0
  ip-address    203.0.113.1
  netmask       255.255.255.0
  gateway       203.0.113.2
phy-interface
  name          tdm_p0
  operation-type Media
  slot          2
realm-config
  identifier     tdmRealm
  network-interfaces tdm_p0:0
  media-sec-policy tdmMediaSec
  codec-policy  t1CodecPolicy
sip-config
sip-interface
  realm-id      tdmRealm
  sip-port
    address     203.0.113.1
  secured-network enabled
snmp-community
  community-name public
  ip-addresses  172.30.0.165
steering-pool
  ip-address    203.0.113.1
  start-port    20000
  end-port      40000
  realm-id      tdmRealm
  network-interface tdm_p0:0
system-config
  default-gateway 172.30.0.1
tdm-config
  tdm-profile
    name        tdm-config-test
web-server-config

```

### With No SRTP License

Use the following settings for TDM when you do not own an SRTP License.

```

codec-policy
  name          e1CodecPolicy
  allow-codecs  *
  add-codecs-on-egress PCMA
codec-policy
  name          t1CodecPolicy
  allow-codecs  *
  add-codecs-on-egress PCMU
network-interface
  name          tdm_p0
  ip-address    203.0.113.1

```

```

        netmask                255.255.255.0
        gateway                203.0.113.2
    phy-interface
        name                    tdm_p0
        operation-type          Media
        slot                    2
    realm-config
        identifier              tdmRealm
        network-interfaces      tdm_p0:0
        codec-policy            t1CodecPolicy
    sip-config
    sip-interface
        realm-id                tdmRealm
        sip-port
            address              203.0.113.1
    steering-pool
        ip-address              203.0.113.1
        start-port              20000
        end-port                 40000
        realm-id                tdmRealm
        network-interface        tdm_p0:0
    system-config
        default-gateway          172.30.0.1
    tdm-config
        tdm-profile
            name                  tdm-config-test
    web-server-config

```

## 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.

---

Character	Description
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: <ul style="list-style-type: none"><li>• 8019 matches</li><li>• 819 does not match</li><li>• 8119 matches</li></ul>
Character x	Use as a wildcard at the end of a dial pattern to mean 0-9. For example: 555xxx means match a number starting with 555 followed by 3 digits from 0-9.
Parentheses ( )	Use to enclose optional digits in a pattern. For example: 555xx(xxxx) means match a number starting with 555 plus a minimum of 2 digits, and optionally up to 4 more digits.

---

## Telephony Fraud Protection File Activation

After you create, edit, or upload the 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 CLI to refresh the fraud protection file, FTP 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:**

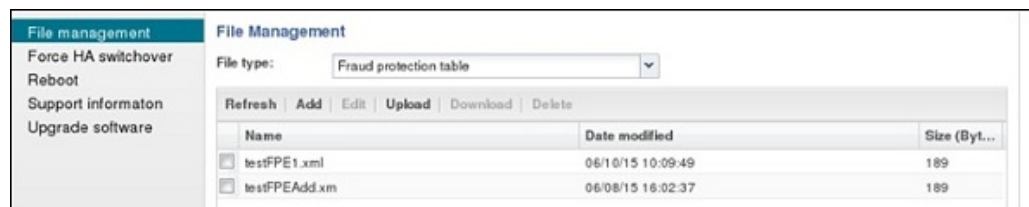
The system displays an alert on the Notifications menu to remind you that the fraud protection file needs activation.

## 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 CLI. 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.

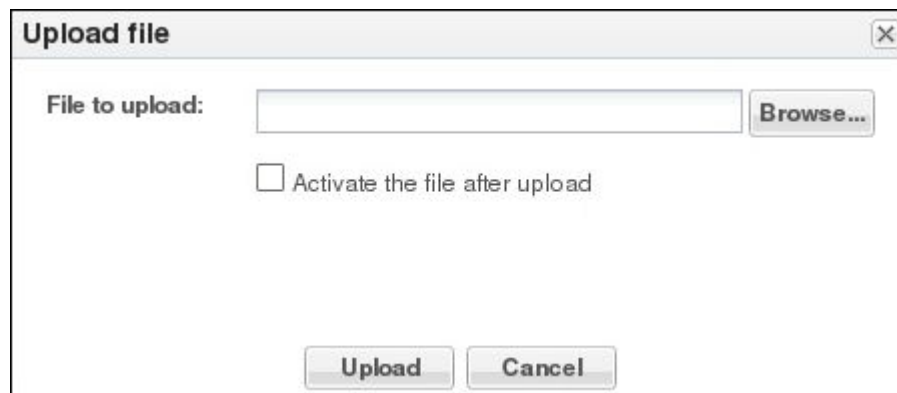
From the System tab, the File Management page displays the File Type drop-down list that includes the Fraud Protection Table item. The Fraud Protection Table displays the list of fraud protection files on the E-SBC, as shown in the following illustration.



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**.

Fraud protection table	
Search Criteria: All	
Add ▾	Edit
Copy	Delete
List type	Type
call-redirect	from-hostname
call-whitelist	from-hostname

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.

Type	Description
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.
phone-number	You can use the following characters for phone-number: <ul style="list-style-type: none"> <li>• 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.</li> <li>• Brackets [ ]. Use to enclose ranges in a pattern. Syntax: [min-max]. For example: 555 [0000-9999].</li> <li>• Parentheses. ( ) Use to enclose optional digits in a pattern. For example: 555xx(xxxx) means 555 with between 2 and 4 following digits.</li> <li>• Character x. Use as a wildcard at the end of a dial pattern to mean 0-9. For example: 555xxx means a number starting with 555 followed by 3 digits.</li> </ul>

## 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.

### Before You Begin

- Confirm that the system displays the Expert mode.

### Procedure

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	<ul style="list-style-type: none"> <li>• Type. Select the type of data to match from the drop-down list.</li> <li>• 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.</li> <li>• Ingress Realm. Select the ingress realm from the drop-down list to associate to the match value.</li> </ul>
White list	<ul style="list-style-type: none"> <li>• Type. Select the type of data to match from the drop-down list.</li> <li>• 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.</li> <li>• Ingress Realm. Select the ingress realm from the drop-down list to associate to the match value.</li> </ul>

Attributes	Instructions
Rate limit	<ul style="list-style-type: none"> <li>• Type. Select the type of data to match from the drop-down list.</li> <li>• 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.</li> <li>• Ingress realm. Select the ingress realm from the drop-down list to associate to the match value.</li> <li>• Calls per second. Enter the number of calls per second to allow for the entry. Range: 0-65535. 0 = unlimited.</li> <li>• Max active calls. Enter the maximum number of active calls allowed for the entry. Range: 0-65535. 0 = unlimited.</li> </ul>
Call redirect	<ul style="list-style-type: none"> <li>• Type. Select the type of data to match from the drop-down list.</li> <li>• 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.</li> <li>• Ingress realm. Select the ingress realm from the drop-down list to associate to the match value.</li> <li>• Target. Enter one of the following: Session agent, session agent group name, Hostname, or IP address.</li> </ul>

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**.

#### Next Steps

- 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.

#### Before You Begin

- 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.)

### Procedure

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**.

### Next Steps

- 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 - ACLI

The telephony fraud protection feature requires configuration, which you can perform from the Oracle Enterprise Session Border Controller (E-SBC) ACLI by way of the `fraud-protection` configuration element under `System`.

### Before You Begin

- 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 fraud protection file that you want to use. Confirm that the system displays the ACLI.

### Procedure

Use this procedure to enable telephony fraud protection management on the E-SBC. You must also specify the fraud protection file name and activate the configuration. You cannot specify multiple fraud protection files because the system recognizes only one file as the active source file.

 **Note:**

The first time you configure the E-SBC to manage fraud protection, the system activates the file when you save and activate the configuration. After the initial configuration, the system does not refresh the fraud protection file when you save and activate other configuration changes on the E-SBC. The exception occurs when you specify a new file name in the fraud protection configuration, make changes to other configurations, and save and activate all of the changes at one time.

1. Access the **fraud-protection** configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# system
ORACLE(session-router)# fraud-protection
```

2. Type **select**, and press ENTER.
3. Type **show**, and press ENTER.
4. Enter the following settings:

Attributes	Instructions
mode	Type one of the following modes: <ul style="list-style-type: none"> <li>• <b>local</b>—To use the E-SBC as the source of the fraud protection file.</li> <li>• <b>comm-monitor</b>—Not currently supported.</li> <li>• <b>disabled</b>—Default.</li> </ul>
file-name	Enter the name of the fraud protection file.
options	Add fraud protection options. (Not supported in some releases. )
allow-remote-call-terminate	Not currently supported.

5. Save and activate the configuration.

## Configure Telephony Fraud Protection - GUI

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.

### Before You Begin

- 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.)

### Procedure

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. <ul style="list-style-type: none"> <li>• local—Specifies the E-SBC as the source of the fraud protection file.</li> <li>• comm-monitor—Not currently supported.</li> <li>• disabled—Default</li> </ul>
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 and activate the configuration.

## Activate a New Telephony Fraud Protection File - GUI

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.

### Before You Begin

- 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.

### Procedure

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.

Attributes	Instructions
File name	Select the file to activate from the drop-down list or enter the file name.

3. Click **OK**.
4. Save and activate 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 CLI.

### Procedure

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	<ul style="list-style-type: none"> <li>• Type. Select the type of data to match from the drop-down list.</li> <li>• 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.</li> <li>• Ingress realm. Select the ingress realm to associate with the match value.</li> </ul>

Attributes	Instructions
White list	<ul style="list-style-type: none"> <li>Type. Select the type of data to match from the drop-down list.</li> <li>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.</li> <li>Ingress realm. Select the ingress realm to associate with the match value.</li> </ul>
Rate limit	<ul style="list-style-type: none"> <li>Type. Select the type of data to match from the drop-down list.</li> <li>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.</li> <li>Ingress realm. Select the ingress realm to associate with the match value.</li> <li>Calls per second. Enter the number of calls per second to allow for the entry. Range: 0-65535.</li> <li>Max active calls. Enter the maximum number of active calls allowed for the entry. Range: 0-65535.</li> </ul>
Call redirect	<ul style="list-style-type: none"> <li>Type. Select the type of data to match from the drop-down list.</li> <li>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.</li> <li>Ingress realm. Select the ingress realm to associate with the match value from the drop-down list.</li> <li>Redirect target. Enter one of the following: Session agent, session agent group name, Hostname, or IP address</li> </ul>

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.

## Refresh the Telephony Fraud Protection File - ACLI

You can refresh the telephony fraud protection file from the ACLI with the `notify fped refresh` command. This command updates the runtime table by reloading the entries from the file specified in the fraud-protection configuration.

### Before You Begin

- FTP the updated file to the E-SBC.
- Confirm that the name of the updated file matches the name of the configured file.

### Procedure

Use the following procedure apply updates to the fraud protection file.

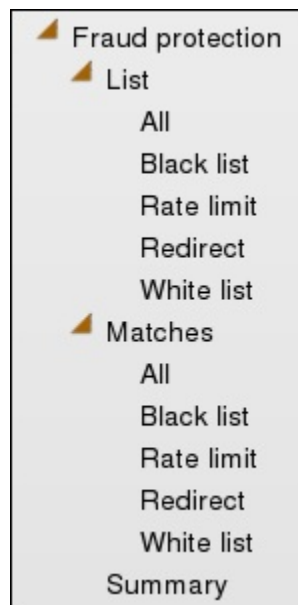
1. Log on to the ACLI.
2. Type `notify fped refresh`, and press ENTER.

The system confirms a successful refresh.

## 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.

## Telephony Fraud Protection ACLI Show Commands

The Oracle Enterprise Session Border Controller (E-SBC) supports viewing and refreshing telephony fraud protection statistics by way of ACLI commands. The displayed data is read-only.

The following ACLI commands provide displays of telephony fraud protection statistics.

`show-fraud-protection <list type> <matches-only>`—Use this command to display all entries or only entries on a particular fraud prevention list, and optionally, to show only the entries on the specified list that incurred a match. Use one of the following variables for `<list type>`:

- `all`—displays all entries
- `blacklist`—displays only the blacklist matches
- `whitelist`—displays only the white list matches
- `redirect`—displays only the redirect matches
- `ratelimit`—displays only the rate limit matches

Command Examples:

- `show-fraud-protection all`—displays all blacklist, redirect, white list, and rate limit entries.
- `show-fraud-protection all matches-only`—displays only the matches for blacklist, redirect, white list, and rate limit entries.
- `show-fraud-protection blacklist`—displays only the blacklist, showing all entries.
- `show-fraud-protection blacklist matches-only`—displays only the matches for blacklist entries.

Display Examples

```
show fraud-protection all
17:31:09-109
```

List Type	To/From	Match Value	Ingress Realm	No. of Hits		
				Recent	Total	PerMax
BLACKLIST	To	1809*	peer	0	0	0
BLACKLIST	To	22478300501	access	0	0	0
BLACKLIST	From	172.38.10.0/24	enterpriseco	0	0	0
BLACKLIST	From	192.168.39.0/24	peer	0	0	0
BLACKLIST	From	roberto.veras	peer	0	0	0
RATE_LIMIT	To	20.20.20.20	boston.com	0	0	0
RATE_LIMIT	From	18092059090	peer	0	0	0
RATE_LIMIT	From	peter.paker	nyrealm	0	0	0
REDIRECT	To	john.doe	domain	0	0	0
REDIRECT	From	10.10.10.10	nyrealm	0	0	0
REDIRECT	From	18092059080	peer	0	0	0
WHITELIST	To	1978973[0000-9999]	peer	0	0	0
WHITELIST	To	22478300501	access	0	0	0
WHITELIST	From	172.38.10.0/24	service_provider	0	0	0

```

Total hits: 0
Total entries: 14
Total displayed entries: 14
File name: my_entries.xml
Last file upload time: 2015-07-22 17:28:08
```

### BLACKLIST

`show-fraud-protection`—Use to display all entries with matches-only

`show fraud-protection stats`—Use to display Recent, Total, and Period Maximum statistics for the fraud protection lists: For example: STATS

```
show fraud-protection stats
```

Fraud Protection Engine Stats	---- Lifetime ----		
	Recent	Total	PerMax
Blacklisted Calls	0	0	0
Whitelisted Calls	0	0	0
Ratelimited Calls	0	0	0
Redirected Calls	0	0	0
Blacklist Rejected Calls	0	0	0
Ratelimit Rejected Calls	0	0	0

The following ACLI commands refresh displays of fraud protection entries.

`notify fped refresh`—Use to update the fraud protection lists table after you make changes. If for some reason the refresh command is unsuccessful and cannot update the list with new data, the system preserves the existing data.

`notify fped reset-stats`—Use to reset the fraud protection statistics counter to zero, for example, to begin a new data collection period.

## Web GUI Enhancements

The E-CZ730M1 release includes the following enhancements to the Web GUI.

- Adds the Settings button to the User Management Table widget for configuring the auto-refresh time.
- Adds the opt, boot, and crash partitions to the Disk Usage widget.
- Hides unconfigured objects from the display in the Configuration Inventory Widget.
- Shows the name of the object and the sub-object in the results of a global search.
- Opens the edit dialog when you double-click an item in a delimited list.

## 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 Widgets tab or the from the Home page by way of the Add Widget dialog. 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 dashboard widgets.

The Web GUI displays the following show command widgets:

Command Group	Widget Name and Command Executed
Media	Classify - show media classify Host stats - show media host-stats MBCD <ul style="list-style-type: none"> <li>• Acls - show mbcid acls</li> <li>• All - show mbcid all</li> <li>• Errors - show mbcid errors</li> <li>• Realms - show mbcid realms</li> <li>• Statistics - show mbcid statistics</li> </ul> NAT <ul style="list-style-type: none"> <li>• By index - show nat by-index</li> <li>• In tabular - show nat in-tabular</li> </ul> Realm <ul style="list-style-type: none"> <li>• Individual -show realm</li> <li>• Specifics - realm-specifics</li> <li>• Summary - show realm</li> </ul> Xcode <ul style="list-style-type: none"> <li>• Codecs - show xcode codecs</li> <li>• Load - show xcode load</li> <li>• Xlist - show xcode xlist</li> </ul>
Signaling	DNS - show dns ENUM - show enum Fraud protection List <ul style="list-style-type: none"> <li>• All - show fraud-protection all</li> <li>• Black list - show fraud-protection blacklist</li> <li>• Rate limit - show fraud-protection rate limit</li> <li>• Redirect - show fraud-protection redirect</li> <li>• White list - show fraud-protection white list</li> </ul> Matches <ul style="list-style-type: none"> <li>• All -show fraud-protection all matches-only</li> <li>• Black list - show fraud-protection blacklist matches-only</li> <li>• Rate limit - show fraud-protection rate limit matches-only</li> <li>• Redirect - show fraud-protection redirect matches-only</li> <li>• White list - show fraud-protection white list matches-only</li> </ul> Summary - show fraud-protection stats H323d - show h323d LRT - show lrt Recording - show rec

Command Group	Widget Name and Command Executed
	<p>Registration</p> <ul style="list-style-type: none"> <li>• By realm -show registration sipd by realm</li> <li>• H323d - show registration h323d</li> <li>• SIP - show registration SIP</li> <li>• Statistics - show registration statistics</li> </ul> <p>Sessions - show sessions</p> <p>SIP</p> <ul style="list-style-type: none"> <li>• Agent details - show sipd agents</li> <li>• Agent groups - show sipd groups</li> <li>• Agent individual - show sipd agents &lt;agent name&gt;</li> <li>• Client trans - show sipd client</li> <li>• Interface individual - show sipd interface</li> <li>• Interface summary - show sipd interface</li> <li>• LDAP - show ldap</li> <li>• Method ack - show sipd ack</li> <li>• Method bye - show sipd bye</li> <li>• Method cancel - show sipd cancel</li> <li>• Method info - show sipd info</li> <li>• Method invite - show sipd invite</li> <li>• Method message - show sipd message</li> <li>• Method notify - show sipd notify</li> <li>• Method options - show sipd options</li> <li>• Method prack -show sipd prack</li> <li>• Method publish - show sipd publish</li> <li>• Method refer - show sipd refer</li> <li>• Method register - show sipd register</li> <li>• Method subscribe - show sipd SUBSCRIBE</li> <li>• Method update - show sipd update</li> <li>• Realms all - show sipd realms</li> <li>• Realms individual - show sipd realms &lt;realm name&gt;</li> <li>• Redundancy - show sipd redundancy</li> <li>• Server trans - show sipd server</li> <li>• Session all - show sipd sessions all</li> <li>• Session summary - show sipd sessions</li> <li>• Codecs - show sipd codecs</li> <li>• Errors - show sipd errors</li> <li>• Status - show sipd status</li> </ul>



Command Group	Widget Name and Command Executed
System	<ul style="list-style-type: none"> <li>• Accounting - show accounting</li> <li>• ACL - show acl all</li> <li>• Alarms - show alarms</li> <li>• Authentication RADIUS - show radius all</li> <li>• Authentication TACACS - show tacacs stats</li> <li>• Configuration Editing - show configuration</li> <li>• Configuration Editing short - show configuration short</li> <li>• Configuration Inventory - show configuration inventory</li> <li>• Configuration Running - show running-config</li> <li>• Configuration Running short - show running-config short</li> <li>• Configuration Version - show version</li> <li>• CPU Usage - cpu-monitor</li> <li>• Disk Usage - show space</li> <li>• Features - show features</li> <li>• Interfaces All - show interfaces</li> <li>• Interfaces Brief - show interfaces brief</li> <li>• Interfaces Mapping - show interface mapping</li> <li>• Interfaces Virtual - show virtual interfaces</li> <li>• Interfaces Wancom - show Wancom</li> <li>• L2/L3 ARP Info - show arp</li> <li>• L2/L3 ARP Statistics - show arp info</li> <li>• L2/L3 ARP Summary - show arp statistics</li> <li>• L2/L3 Connections - show ip connections</li> <li>• L2/L3 Neighbor table - show neighbor-table</li> <li>• L2/L3 Routes - show routes</li> <li>• L2/L3 Summary - show ip</li> <li>• L2/L3 TCP - show ip tcp</li> <li>• L2/L3 UDP - show ip udp</li> <li>• Licenses - licence</li> <li>• Memory Current memory - no ACLI command</li> <li>• Memory Historical Memory - no ACLI command</li> <li>• Memory Summary - show memory</li> <li>• Platform All - show platform all</li> <li>• Platform CPU load - show platform cpu-load</li> <li>• Platform Errors - show platform errors</li> <li>• Platform Limits - show platform limits</li> <li>• PROM info - show prom info all</li> <li>• Temperature - show temperature</li> <li>• Processes - show processes</li> <li>• SNMP Community table - show snmp-community-table</li> <li>• SNMP Trap Receiver - show trap-receiver</li> <li>• SPL Memory - show spl memory</li> <li>• SPL Options - show spl-options</li> <li>• SPL Statistics - show spl statistics</li> <li>• SPL Version - show spl</li> <li>• System health - show health</li> </ul>

Command Group	Widget Name and Command Executed
	<ul style="list-style-type: none"> <li>• TDM Channels - show tdm channels</li> <li>• TDM Dialplan - show tdm dialplan</li> <li>• TDM Spans - show tdm spans</li> <li>• TDM Status - show tdm status</li> <li>• Time Clock - show clock</li> <li>• Time NTP Server - show ntp server</li> <li>• Time NTP Status - show ntp status</li> <li>• Time Time zone - show timezone</li> <li>• Time UTC - show clock utc</li> <li>• Uptime - show uptime</li> <li>• User management - show users</li> <li>• Version boot - show version boot</li> <li>• Version cpu - show version cpu</li> <li>• Version hardware - show version hardware</li> <li>• Version image - show version image</li> <li>• Version summary - show version</li> </ul>

## Widgets Removed from the Web GUI

The Web GUI no longer supports the following widgets.

- Agent status table
- Answer and Seizure ratio line graph
- Answer and Seizure ratio table
- Established sessions line graph
- Established sessions table
- Requests per second line graph
- Requests per second table
- Response bar graph
- Response pie graph
- Response table
- Session duration bar graph
- Session duration table
- SIP registration cache table

If you previously added any of these widgets to the Dashboard, the system will continue to display them.

## Inherited Features

The ECZ7.3.0M1 release inherits the following features from previous releases.

### Hardware Support

The Oracle Enterprise Session Border Controller supports IPsec and SRTP on Encryption, and Encryption + QoS NIUs.

## Behavioral Changes

The ECZ7.3.0M1 release includes the following changes in behavior since the previous GA release.

### Default Passwords

The Oracle Enterprise Session Border Controller (E-SBC) ships with hard-coded default passwords, which can pose a security risk when left unchanged. Upon startup, the E-SBC now checks for the presence of the default passwords. If the system detects the default passwords, you must change them before the system allows access.

If you attempt to access the E-SBC through Telnet, a Web server, SFTP, or another unsupported method before you change the default passwords, the system denies access. For Telnet users, the system displays a banner stating that connections other than SSH and Console access are not allowed. For Web server and SFTP users, the system denies authentication and terminates the connection immediately.

You can change the passwords only when accessing the system by way of SSH or Console connections.

## Known Issues

The following known issues apply to the ECZ7.3.0M1 release.

### Dynamic Trusted Entries

Dynamic trusted entries are set to the following values:

- Acme Packet 3820—62K
- Acme Packet 4500—125K
- Acme Packet 4600—125K

### PKCS12

The system cannot export CA certificates as PKCS12.

### Upgrade Can Affect High Availability Operations

**Problem:** In a High Availability (HA) configuration with the HA interfaces named eth1 and eth2, HA stops functioning when you upgrade to ECZ7.3.0M1.

**Workaround:** Name the HA interfaces wancom1 and wancom2 before performing the upgrade.

## Limitations

The following limitations apply to the ECZ7.3.0M1 release.

Topic	Limitation
H.323	The system does not support H.323 for fraud protection.
IPv6	The system does not support IPv6 for fraud protection.

---

Topic	Limitation
OPUS and SILK Support	The Acme Packet 1100 does not support transcoding for the OPUS and SILK codecs.
Suite B	Limited testing has been preformed for third-party interoperability with E-SBC Suite B implementation.

---

## Caveats

The following caveats apply to the ECZ7.3.0M1 release.

### High Availability Configuration

HA redundancy is unsuccessful when you create the first SIP interface, or the first time you configure the Session Recording Server on the Oracle Enterprise Session Border Controller (E-SBC). Oracle recommends that you perform the following work around during a maintenance window.

1. Create the SIP interface or Session Recording Server on the primary E-SBC, and save and activate the configuration.
2. Reboot both the Primary and the Secondary.

## Closed Caveats

The following resolved caveats apply to the ECZ7.3.0M1 release.

### Local Media Playback

The system resumes Local Media Playback support, which was supported in the EC[xz]640 release and was not supported in the subsequent series of ECZ7.x releases.

### LDAP Support and the Acme Packet 6300

The Active Directory Call Routing enhancement included in this release works on the Acme Packet 6300.

# 3

## ECZ7.3.0M2

### Supported Platforms and Image Files

The following platforms and image files support the E-CZ7.3.0M2 release.

- Oracle Hardware Platforms: Acme Packet 1100, Acme Packet 3820, Acme Packet 4500, Acme Packet 4600, and Acme Packet 6300.
- Virtual Platforms: VMWare 5.5 ESXi Hypervisor.

#### Release Image File Names

Use the following files for a new deployment.

#### Oracle Hardware

- Image:
  - Use nnECZ730m2.64.bz for the Acme Packet 1100, the Acme Packet 4500, Acme Packet 4600, and the Acme Packet 6300 for new installations and for upgrades.
  - Use nnECZ730m2.32.bz for the Acme Packet 3820.
- Boot loader: November 2013 or newer

#### Virtual Machines

- VMWare: nnECZ730m2.64-img-bin\_vmware.ova

#### Upgrade Image File Names

Use the following files to upgrade virtual machine deployments.

- Image: nnECZ730m2.64.bz
- Boot loader: nnECZ730m2.64.boot

### CPU Support for the Acme Packet 3820 and Acme Packet 4500

Note the following requirements for CPU support on the Acme Packet 3820 and the Acme Packet 4500.

- The system supports the following versions for the 32-bit Acme Packet 3820.

Board Revision	Minimum Version
3	v3.13
4	v4.03

- The system supports only the 64-bit CPU2 on the Acme Packet 4500, and only CPU revision MOD-0026-xx. The system does not support CPU revision MOD-0008-xx.

Board Revision	Minimum Version
3	v3.18

Board Revision	Minimum Version
4	v4.10

- An Acme Packet 3820 older than August 2009 with a revision lower than 3.08 requires a BIOS update.

## Platform Boot Loaders

Oracle Enterprise Session Border Controller platforms require a boot loader to load the operating system and software.

### Stage 1 and Stage 2 Boot Loaders

Stage 1 and Stage 2 boot loaders on the nn4500 and the nn3820 must not be dated any earlier than July 3, 2013 (MOS patch #1815632). From the command line, use the **show version boot** command to view the boot loader version.

#### Note:

Network booting for release 7.x by way of FTP and TFTP on the nn4500 and the nn3820 requires the November 2013 or later boot loader.

### Stage 3 Boot Loader

All platforms require the Stage 3 boot loader. Every new software release contains a system software image and a Stage 3 boot loader. When you plan to upgrade your system image, upgrade the Stage 3 boot loader before booting the new system image.

The boot loader file name corresponds to the software image filename. For example, if the software image filename is nnECZ730.64.bz, the corresponding Stage 3 boot loader filename is nnECZ730.boot. The boot loader file must be installed as /boot/bootloader on the target system.

The Stage 3 boot loader is compatible with previous releases.

## NIU and Feature Group Requirements

The following tables list the feature groups for all hardware and virtual platforms that require a specific Network Interface Unit (NIU).

**Table 3-1 Acme Packet 1100 NIU and Feature Group Support Matrix**

NIU	IPSec	SRTP	QoS	Transcoding	ISDN PRI
Acme Packet 1100 Ethernet interface	✗	✓	✓	✓ (requires transcoding module)	✗
Acme Packet 1100 TDM interface	Not applicable	Not applicable	Not applicable	Not applicable	✓

**Table 3-2 Acme Packet 3820 NIU and Feature Group Support Matrix**

NIU	IPSec	SRTP	QoS	Transcoding
Clear (RJ45)	X	X	X	X
Clear (SFP)	X	X	X	X
ETCv1 *	✓	✓	✓	X
ETCv2	✓	✓	✓	X
Encryption	✓	✓	X	X
QoS	X	X	✓ **	X
Encryption & QoS	✓	✓	✓ **	X
Transcoding	X	X	✓ ***	✓

**Table 3-3 Acme Packet 4500 NIU and Feature Group Support Matrix**

NIU	IPSec	SRTP	QoS	Transcoding
Clear (RJ45)	X	X	X	X
Clear (SFP)	X	X	X	X
ETCv1 *	✓	✓	✓	X
ETCv2	✓	✓	✓	X
Encryption	✓	✓	X	X
QoS	X	X	✓ **	X
Encryption & QoS	✓	✓	✓ **	X
Transcoding	X	X	✓ ***	✓

**Table 3-4 Acme Packet 4600 NIU and Feature Group Support Matrix**

NIU	IPSec	SRTP	QoS	Transcoding
4x1Gig or 2x10Gig NIU	✓	✓	✓	✓ (requires transcoding module)

**Table 3-5 Acme Packet 6300 NIU and Feature Group Support Matrix**

NIU	IPSec	SRTP	QoS	Transcoding
2x10Gig NIU	✓	✓	✓	Transcoding Carrier Unit

**Table 3-6 Virtual Machine and Feature Group Support Matrix**

	IPSec	SRTP	QoS	Transcoding
Virtual Machine	X	✓	✓	✓ (G729, PCMU, PCMA)

### Footnotes

- \* The system does not support an ETCv1 Card with 4GB RAM. This NIU is identified by a revision lower than 2.09. Use the **show prom-info phy** command and see the ETC NIU **Functionalrev** attribute to confirm compatibility.
- \*\* IPv4, only.
- \*\*\* IPv4, only. Non-transcoded calls, only.
- \*\*\*\* Limited codec support. G711u, G711a, G729

## QoS NIU Version Requirement for Acme Packet 3820 and Acme Packet 4500

A Network Interface Unit (NIU) that supports the Quality of Service (QoS) feature group on the Acme Packet 3820 and the Acme Packet 4500, except the two Enhanced Traffic Control (ETC) cards, requires QoS Field Programmable Gate Array (FPGA) revision 2.19 or higher for the E-CZ7.3.0M1 release. The 2.20 FPGA upgrade image is available at My Oracle Support, <https://support.oracle.com/>, with a customer account.

If the QoS FPGA Hardware Revision is lower than 1.109 (which corresponds to 2.19 FPGA image), you need to upgrade the QoS FPGA image. Use the **show qos revision** command (or **show datapath ppx info** in S/E-CZ7.x.x forward) from the ACLI to find the QoS FPGA Hardware Revision number, for example:

```
ORACLE# show qos revision
QoS FPGA Hardware Revision is 1.109
ORACLE#
```

## Supported SPL Engines

Each release supports a number of versions of the SBC Programming Language (SPL) engine, which is required to run SPL plug-ins on the Oracle Enterprise Session Border Controller (E-SBC).

This release supports the following versions of the SPL engine.

- C2.0.0
- C2.0.1
- C2.0.2
- C2.0.9
- C2.1.0
- C2.1.1
- C2.2.0
- C2.2.1
- C2.3.1
- C3.0.0
- C3.0.1
- C3.0.2



- C3.0.3
- C3.0.4
- C3.0.6
- C3.0.7
- C3.1.0
- C3.1.1
- C3.1.2
- C3.1.3
- C3.1.4
- C3.1.5
- C3.1.6

Use the `show spl` command to see the version of the SPL engine running on the E-SBC.

## Supported Upgrade Paths

E-CZ7.3.0M2 supports the following upgrade paths, which include all maintenance releases and patches up to E-CZ7.3.0M2.

- E-C[xz]6.4.0 > E-CZ7.3.0
- E-CZ7.1.0 > E-CZ7.3.0
- E-CZ7.2.0 > E-CZ7.3.0

## New Features and Enhancements

The following new features and enhancements apply to the E-CZ7.3.0M2 release.

Features and Enhancements	Descriptions
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 <code>certificate-record</code> , <code>tls-profile</code> , and <code>tls-global</code> for an HTTPS connection to the Web GUI from the Web server..

Features and Enhancements	Descriptions
Advanced Logging	Advanced Logging allows targeted logging by overriding log levels, so that only a specific SIP request and its related messages are logged. The system matches criteria that you configure to determine which requests to log. The system also logs all messages related to the request, such as any responses, in-dialog messages, media, timers, and so on. Advanced Logging supports multiple matching criteria for incoming requests and rate limiting. Advanced log files are smaller than debug files because the system logs only the specified number of matches in the specified period of time. Since the files are smaller, Advanced Logging uses fewer system resources than debug logging. To make searching easier, the system labels each log.
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.
Certificate Storage Limits	On the Acme Packet 3820, with either an ETC1 or ETC2 NIU, the public certificate storage limit is 50 and the private certificate storage limit is 20.
CLIP and COLP Support for TDM	The Time Division Multiplexing (TDM) option on the Acme Packet 1100 supports Calling-Line Identification Presentation (CLIP ) and Connected-Line Identification Presentation (COLP) to provide ISDN facility messages. With CLIP and COLP support enabled, each party on the call can receive identification of the other.
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.

Features and Enhancements	Descriptions
Disable Server Certificate Validation	With the growth of video conferencing adoption and B2B video in all IP networks, Oracle Enterprise Session Border Controller (E-SBC) customers may want to conduct video conferencing with a destination where the Certificate Authority (CA) is not pre-loaded in the E-SBC. In such a scenario the E-SBC cannot successfully establish a TLS session, due to lacking the correct root CA certificate to validate the server certificate. To handle the scenario in which a TLS session lacks the correct root CA, the "ignore-root-ca=yes" tls-profile option allows the E-SBC to ignore the root CA certificate during the validation process.
Opus and SILK Transcoding for the Acme Packet 1100	Adds support to the Acme Packet 1100 for transcoding Opus and SILK CODECs. Support for Opus and SILK transcoding was added for other session border controllers in E-CZ7.3.0M1. See the "New Features" section in the M1 chapter of this guide and the Transcoding chapter of the ACLI Configuration Guide for complete information.
Preserve SIPREC with SIP REFER Header	When the Oracle Enterprise Session Border Controller (E-SBC) generates a new INVITE as part of terminating a SIP REFER, the E-SBC evaluates the SIPREC configuration of the realms and session agents involved in the new call leg and responds accordingly. The REFER and Transfer mechanism automatically preserves the UCID, XUCID, GUID, GUCID, and UUI in the metadata, and can forward this information to the Session Recording Server. The E-SBC can Start, Stop, Pause, and Resume SIPREC sessions in response to any re-INVITE, UPDATE, new INVITE, REFER, or specified SIP Response Message.
Secure the ACP Communications Link with TLS	In the absence of IPsec, for example on the Multi-Service Gateway (MSG) 10G platform, the Transport Layer Security (TLS) protocol can provide security for the Acme Communication Protocol (ACP) communications link between the Oracle Enterprise Session Border Controller (E-SBC) and the Oracle Communications Session Delivery Manager (SDM).

 **Note:**

See "Caveats" for important information about SDM behavior in this release.

Features and Enhancements	Descriptions
Security enhancements	<ul style="list-style-type: none"> <li>Increases the certificate default RSA key-size from 1024 to 2048.</li> <li>Updates the default digest algorithm from SHA1 to SHA256.</li> <li>Disables the arcfour cipher and the 96-bit HMAC algorithms.</li> </ul>
Suite B 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.
Surrogate Registration	Allows the E-SBC to explicitly register on behalf of a Internet Protocol Private Branch Exchange (IP-PBX).
TCP Connection Debugging Tool	Transmission Control Protocol (TCP) connection tools can assist you in gauging performance, identifying potential memory leaks, and debugging connections for performance tracking and improvement.
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.
Web GUI Enhancements	<ul style="list-style-type: none"> <li>Adds <b>Delete all</b>, <b>Upload</b>, and <b>Download</b> buttons to the tool bar of all top-level objects that display lists.</li> <li>Adds the .csv configuration file type to File Management on the System Tab.</li> <li>Adds support for uploading and downloading .csv configuration files by way of the Web GUI.</li> </ul>

## 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 `certificate-record`, `tls-profile`, and `tls-global` for an HTTPS connection to the Web GUI from the Web server.

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

Note that virtual machines require the software TLS license.

## Advanced Logging

Advanced Logging allows targeted logging by overriding log levels, so that only a specific SIP request and its related messages are logged. The system matches criteria that you configure to determine which requests to log. The system also logs all messages related to the request, such as any responses, in-dialog messages, media, timers, and so on. Advanced Logging supports multiple matching criteria for incoming requests and rate limiting. Advanced log files are smaller than debug files because the system logs only the specified number of matches in the specified period of time. Since the files are smaller, Advanced Logging uses fewer system resources than debug logging. To make searching easier, the system labels each log.

You can deploy advanced logging by one or both of the following methods.

- **Configure mode.** Define sip-advanced-logging under session-router. This method reconfigures the system and the configuration persists after a system reboot.
- **Command line.** From the Advanced Logging SPL plug-in that is included in the software, you can enable, start, and stop advanced logging without changing the system configuration. When configured from the command line, advanced logging does not persist after a system reboot.

 **Note:**

Configure mode and Command Line are separate deployment methods that do not depend on each other or affect each other.

The system provides the following options for configuring the scope of advanced logging.

- **Request-only.** Logs only the matched message.
- **Transaction.** Logs only the request and the response.
- **Session.** Logs the matched message and anything else related to the session.
- **Session and Media.** Logs the matched message, anything related to the session, and media.

The system provides the following options for configuring the advanced logging criteria.

- **Received Session-Agent.** By IP address or hostname
- **Request Type.** Such as INVITE vs. SUBSCRIBE
- **Received Realm Name.**
- **Request URI.** User and host. Limited to 2 condition entries, when using both types.
- **To header.** User and host. Limited to 2 condition entries, when using both types.
- **From header.** User and host. Limited to 2 condition entries, when using both types.
- **Call-id.** Matches the Call-id header.
- **Rate Limiting.** By specified number of matched requests over a specified period of time.
- **Scope of Logging.** Options include Request Only, Transaction, All Relating to Session, All Relating to Session and Media.

## Configure Advanced Logging - Command Line

You can enable advanced logging and set the log matching criteria from the command line by way of the AdvancedLogging.lua SPL-plugin. When adding log matching criteria, note that within in each set of criteria:

- an AND relationship means that all conditions must match before the system generates the log.
- an OR relationship means that only one set of conditions must match before the system generates the log.

### Note:

The system does not require you to **save** and **activate** after performing this procedure.

### Procedure

1. Use the `spl start sip advanced-logging` command to enable advanced logging.
2. Use the following commands to configure advanced logging.

Command	Description
<code>spl set sip advanced-logging add-criteria</code>	Adds another set of matching criteria.
<code>spl set sip advanced-logging log-label &lt;label string&gt;</code>	Any logs of requests that are matched will have the specified <label string> appended before each log message for easier searching.
<code>spl set sip advanced-logging rate-count &lt;match count&gt;</code>	Sets the rate-limiting to log only <match count> number of matching requests per time window.
<code>spl set sip advanced-logging rate-time &lt;time window&gt;</code>	Sets the rate-limiting time window in seconds.
<code>spl set sip advanced-logging in-agent &lt;session-agent&gt;</code>	Adds to the current set of matching criteria that the request must come from the specified incoming session-agent hostname.
<code>spl set sip advanced-logging in-realm &lt;realm-id&gt;</code>	Adds to the current set of matching criteria that the request must come from the specified incoming realm identifier.
<code>spl set sip advanced-logging request-type &lt;method name&gt;</code>	Adds to the current set of matching criteria that the request must be of the specified request method type, for example, INVITE and REGISTER.
<code>spl set sip advanced-logging from-uri-host &lt;FROM URI host portion&gt;</code>	Adds to the current set of matching criteria that the request FROM headerURI host portion must match the specified value exactly.

Command	Description
<code>spl set sip advanced-logging from-uri-user &lt;FROM URI username portion&gt;</code>	Adds to the current set of matching criteria that the request FROM headerURI username portion must match the string and the specified value exactly.
<code>spl set sip advanced-logging to-uri-host &lt;TO URI host portion&gt;</code>	Adds to the current set of matching criteria that the request TO headerURI host portion must match the string and the specified value exactly.
<code>spl set sip advanced-logging to-uri-user &lt;TO URI username portion&gt;</code>	Adds to the current set of matching criteria that the request TO headerURI username portion must match the string and the specified value exactly.
<code>spl set sip advanced-logging request-uri-host &lt;RURI host portion&gt;</code>	Adds to the current set of matching criteria that the request RURI headerURI host portion must match the string and the specified value exactly.
<code>spl set sip advanced-logging request-uri-user &lt;RURI username portion&gt;</code>	Adds to the current set of matching criteria that the request RURI headerURI username portion must match the string and the specified value exactly.
<code>spl set sip advanced-logging header &lt;header-type&gt; &lt;header-value&gt;</code>	Adds to the current set of matching criteria that the request must have a header of type <header-type> with a value of <header-value> with exact string matches.

## Configure Advanced Logging - Configure Mode

From Configure mode, 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 the 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 Configure Mode, go to `session-router > sip-advanced-logging` and configure the following.
    - Name. Name to display on the log message for this set of criteria.
    - Level. Type one: zero, none, emergency, critical, major, minor, warning, notice, info, trace, debug, or detail.
    - Scope. Type one: request-only, transaction, session, or session-and-media.
    - Matches-per-window. Type a number between 1 and 999999999 for how many matches to log per window of time.
    - Window-size. Type a number between 1 and 999999999 seconds for the length of time the logging window is open.
    - Type conditions.  
The system displays the `adv-log-condition` subelement.

2. From the adv-log-condition prompt, do the following:
  - Match-type. Type one or more of the following sip objects with either the "and" or the "or" operator between objects: 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 incoming message string that you want to match.  
For example, to match "To-header-user" to the value 1234@<companyname>.com, type "to-header-user" for Match type and type " 1234" for Match value.
3. Exit, save, and activate.

## 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 <b>Add</b> , and do the following: <ul style="list-style-type: none"> <li>• 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.</li> <li>• Match value: Type the string that you want to match the incoming message. For example, to match "To-header-user" to the value 1234@&lt;companyname&gt;.com, type 1234.</li> </ul>

3. Save and activate the configuration.

## View Advanced Logging Status - Command Line

View the status of advanced logging to see its state, configuration criteria, and count data.



### Procedure

1. From the AdvancedLogging.lua SPL-plugin, run the `spl show sip advanced-logging` command.

The system displays the following information.

- State
- Log Label
- Rate Limit
- Matching Criteria
- Match Count
- Logged Count

## 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	<ul style="list-style-type: none"> <li>• Log on and log off.</li> <li>• Save a template configuration.</li> <li>• Click <b>Complete</b> in a Wizard.</li> </ul>
Home tab	<ul style="list-style-type: none"> <li>• Add, reset, and save.</li> <li>• Change Widget settings.</li> </ul>
Configuration tab	<ul style="list-style-type: none"> <li>• Save and activate a configuration.</li> <li>• Discard a configuration.</li> <li>• Add, edit, delete, and copy configuration changes.</li> <li>• Run the generate and import certificate commands.</li> </ul>
Widgets tab	<ul style="list-style-type: none"> <li>• Export from a Widget.</li> <li>• Add a Widget to favorites.</li> <li>• Clear, clear all on alarm, add, and delete license.</li> </ul>
System tab	<ul style="list-style-type: none"> <li>• Add audit entries to the system file management actions, such as upload, download, restore, backup, add, edit, and delete.</li> <li>• Force an HA switch over.</li> <li>• Run the Show Support Information command.</li> <li>• Run the Upgrade Software wizard.</li> <li>• Download and view an audit log.</li> </ul>

Source	Actions Recorded
Monitor and Trace tab	<ul style="list-style-type: none"> <li>Export the summary.</li> <li>Export the session detail.</li> </ul>

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: <ul style="list-style-type: none"> <li>Configuration</li> <li>Security</li> <li>System</li> </ul>
EventType	Identifies the action that caused the event as: <ul style="list-style-type: none"> <li>Activate-config</li> <li>Acquire-config</li> <li>Create</li> <li>Data-access</li> <li>Delete</li> <li>Halt</li> <li>Login</li> <li>Logout</li> <li>Modify</li> <li>Reboot</li> <li>Save-config</li> </ul>
Result	Identifies the outcome of the event as: <ul style="list-style-type: none"> <li>Failure</li> <li>Success</li> </ul>
Resource	Describes the action within the event. Some of the numerous actions that the system can log include: <ul style="list-style-type: none"> <li>Authentication</li> <li>Banner (Means that someone edited the log on banner text.)</li> <li>Download &lt;filename&gt;</li> <li>Generate public key</li> <li>Reboot</li> <li>Upload &lt;filename&gt;</li> </ul>
Prev—(verbose mode)	Displays the setting prior to this change.

Log Element	Information Provided
Details—(verbose mode)	Displays additional information about the change, depending on the following event types: <ul style="list-style-type: none"> <li>• Create—displays “New = element added.”</li> <li>• Data-access—displays “Element = accessed element.”</li> <li>• Delete—displays “Element = deleted element.”</li> <li>• Modify—displays “Previous = oldValue New = newValue.”</li> </ul>

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 in 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.

To add a public key profile and generate an RSA public key:

1. Log on to the E-SBC and 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: <ul style="list-style-type: none"> <li>• 1024 (default)</li> <li>• 2048</li> <li>• 512</li> </ul>

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 and Activate the configuration.

**Next Steps**

- 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.

To generate and save a DSA public key:

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.

**Next Steps**

- 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.

To import the DSA public key:

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/ssh\_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.

### Next Steps

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 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`.

To copy the RSA key to the SFTP server:

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."

To configure audit logging:

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.

---

Attributes	Instructions
File transfer time	<p>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.</p> <ul style="list-style-type: none"><li>• Minimum: 0, which disables this file transfer time function.</li><li>• Maximum: 65535</li><li>• Default: 720</li></ul>
Max storage space	<p>Specify the maximum amount of space that the audit log can consume on the E-SBC in MB.</p> <ul style="list-style-type: none"><li>• Minimum: 0</li><li>• Maximum: 32 (default)</li></ul>
Percentage full	<p>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.</p> <ul style="list-style-type: none"><li>• Minimum: 0, which disables this percentage full function.</li><li>• Maximum: 99</li><li>• Default: 75</li></ul>
Max file size	<p>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.</p> <ul style="list-style-type: none"><li>• Minimum: 0, which disables this maximum file size function.</li><li>• Maximum: 10</li><li>• Default: 5</li></ul>

Attributes	Instructions
Push receiver	<p>Add a push receiver and configure the following parameters for sending audit log files from the E-SBC to the receiver:</p> <ul style="list-style-type: none"> <li>• <b>Server</b>—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.</li> <li>• <b>Port</b>—Enter the port number on the FTP/SFTP server to which the E-SBC will send audit log files. Range: 1-65535. Default: 22</li> <li>• <b>Remote path</b>—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: &lt;string&gt; remote pathname.</li> <li>• <b>Filename prefix</b>—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: &lt;string&gt; prefix for filenames.</li> <li>• <b>Username</b>—Enter the username the E-SBC uses to connect to this push receiver.</li> <li>• <b>Auth type</b>—Select the authentication methodology. Password (default) or public key.</li> <li>• <b>Do one of the following:</b> <ul style="list-style-type: none"> <li><b>Password</b>—If you set the Auth type to password, click <b>Set</b> to enter and confirm the password used to access this push receiver.</li> <li><b>Public key</b>—If you set the Auth type to public key, select the public key profile that you want from the drop-down list.</li> </ul> </li> </ul>

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

## Certificate Storage Limits

On the Acme Packet 3820, with either an ETC1 or ETC2 NIU, the public certificate storage limit is 50 and the private certificate storage limit is 20.

## CLIP and COLP Support for TDM

The Time Division Multiplexing (TDM) option on the Acme Packet 1100 supports Calling-Line Identification Presentation (CLIP) and Connected-Line Identification Presentation (COLP) to provide ISDN facility messages. With CLIP and COLP support enabled, each party on the call can receive identification of the other.

The default setting for CLIP and COLP support is disabled. To enable CLIP and COLP, use the **calling-Pres** and **caller-ID** parameters in the tdm-profile object from either the ACLI or the Web GUI.



```
(tdm-prfl)#
name          Configure tdm profile name
line-mode     Configure TDM line mode t1 or e1
signalling    Configure TDM for pri_cpe or pri_net use
switch-type   Configure TDM switch type
b-channel     Configure TDM B channel value
d-channel     Configure TDM D channel value
span-number   Configure TDM D channel value
line-build-out Configure the TDM Line Build Out (LBO) value
framing-value Configure TDM framing value
coding-value  TDM coding value
tone-zone     Configure TDM tone zone
rx-gain       Configure attribute rx-gain
tx-gain       Configure attribute tx-gain
echo-cancellation enable tdm echo cancellation
calling-pres  Caller-IP Presentation for SIP device
caller-id     Caller-ID for CLIP-COLP
options       Configure TDM options
select        select configuration to edit
no            delete configuration
show          show configuration information
done          write configuration information
quit         quit out of configuration mode
exit         return to previous menu
```

The **calling-Pros** parameter specifies that the end-point is allowed to see the caller's ID. You must select the `allowed_passed_screen` value for this parameter.

The **caller-ID** parameter enables CLIP and COLP. Set the SIP identification header to either Remote-party-ID (`rpId`) or P-Asserted-ID (`pai`).

## 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 CLI 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)`.

## Disable Server Certificate Validation

With the growth of video conferencing adoption and B2B video in all IP networks, Oracle Enterprise Session Border Controller (E-SBC) customers may want to conduct video conferencing with a destination where the Certificate Authority (CA) is not pre-loaded in the E-SBC. In such a scenario the E-SBC cannot successfully establish a TLS session, due to lacking the correct root CA certificate to validate the server certificate. To handle the scenario in which a TLS session lacks the correct root CA, the `"ignore-root-ca=yes"` `tls-profile` option allows the E-SBC to ignore the root CA certificate during the validation process.

When you disable server certificate validation the normal TLS handshake still occurs to allow secure connections to any destination, but certificate verification is not performed.

Due to security concerns, Oracle does not recommend using this feature. If you do want to use this feature go to "tls-profile" and set "options" to "ignore-root-ca=yes."

## Preserve SIPREC with SIP REFER Header

When the Oracle Enterprise Session Border Controller (E-SBC) generates a new INVITE as part of terminating a SIP REFER, the E-SBC evaluates the SIPREC configuration of the realms and session agents involved in the new call leg and responds accordingly. The REFER and Transfer mechanism automatically preserves the UCID, XUCID, GUID, GUCID, and UII in the metadata, and can forward this information to the Session Recording Server. The E-SBC can Start, Stop, Pause, and Resume SIPREC sessions in response to any re-INVITE, UPDATE, new INVITE, REFER, or specified SIP Response Message.

The E-SBC can establish a new session or update the existing session with the SIPREC server in the following ways.

- When the A-B call leg SA-realm-sipinterface is configured for SIPREC, and the B-C call leg SA-realm-sipinterface is not configured for SIPREC, the E-SBC sends metadata to the Session Recording Server to stop the recording on the sessionID associated with the original call.
- When both the A-B call leg and the B-C call leg have the same SIPREC configuration on their SA-realm-sipinterface, the E-SBC sends metadata to the Session Recording Server to stop Party A participation and start Party C participation within the same sessionID.
- When the A-B and B-C call legs have a different SIPREC configurations on their SA-realm-sipinterface, the E-SBC sends metadata to the A-B call leg Session Recording Server to stop the current recording session and sends metadata to the B-C call leg Session Recording Server to start a new recording session with a new sessionID.

## Secure the ACP Communications Link with TLS

In the absence of IPsec, for example on the Multi-Service Gateway (MSG) 10G platform, the Transport Layer Security (TLS) protocol can provide security for the Acme Communication Protocol (ACP) communications link between the Oracle Enterprise Session Border Controller (E-SBC) and the Oracle Communications Session Delivery Manager (SDM).

To use the security protection provided by TLS, establish a successful TLS connection between the E-SBC and the SDM. A successful connection requires configuring a valid TLS profile on the E-SBC and associating the profile with the management interface on the SDM that will negotiate the TLS connection. See the *Oracle Session Delivery Manager Security Guide* for information about associating the TLS profile from the E-SBC with the management interface on the SDM.

To configure the E-SBC to use TLS for ACP communication, do the following:

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 in the profile.
2. Select the TLS profile in `system-config`. The `system-config` object is located under `system`. Use the `acp-tls-profile` parameter to specify the TLS profile that you want to use for ACP.

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 TLS, the SDM negotiates a TLS connection with the E-SBC.

## Security Enhancements

Note the following security enhancements.

- The default RSA key size for the E-SBC certificate is increased from 1024 to 2048.
- The default message-digest algorithm is increased from SHA1 to SHA256.
- The arcfour cipher and any 96-bit Keyed-Hash Method Authentication Code (HMAC) algorithms are disabled. The SSH key exchange initialization message no longer sends arcfour and 96-bit HMAC algorithms.

## Suite B 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.

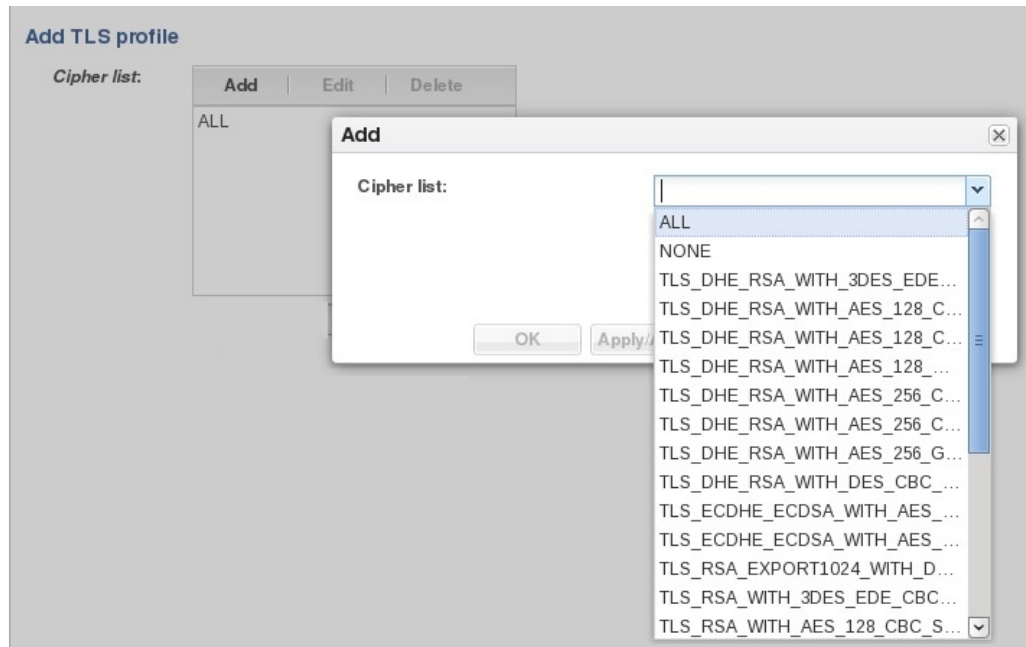
To support Suite B, the E-SBC certificate record includes the following parameters:

- `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.

These parameters are included in the "Add a Certificate Record" procedure, which you can perform from the ACLI and the Web GUI.

### From the Web GUI

When you click **Add** for the cipher list parameter in `tls-profile`, the system provides a drop-down list of 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.



#### From the ACLI

The `tls-profile` object contains the cipher list parameter and the `tlsCipherList` command displays the list of ciphers that you can specify.

`TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256` and

`TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384` are suite B based ciphers.

```
sd225v(tls-profile)# show
tls-profile
  name                webapp
  end-entity-certificate localCert
  trusted-ca-certificates localCertCA
  cipher-list          ALL
  verify-depth         10
  mutual-authenticate disabled
  tls-version          compatibility
  options
  cert-status-check    disabled
  cert-status-profile-list
  ignore-dead-responder disabled
  allow-self-signed-cert disabled
  last-modified-by     admin@console
  last-modified-date   2015-11-18 14:44:02
```

```
sd225v(tls-profile)# cipher-list
```

```
<tlsCipherList> List of TLSv1/TLSv11/TLSv12/SSLv3 ciphers.
<TLS_DHE_RSA_WITH_AES_256_GCM_SHA384,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256,
TLS_DHE_RSA_WITH_AES_256_CBC_SHA,
TLS_RSA_WITH_AES_256_GCM_SHA384,
TLS_RSA_WITH_AES_256_CBC_SHA256,
TLS_RSA_WITH_AES_256_CBC_SHA,
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256,
TLS_DHE_RSA_WITH_AES_128_CBC_SHA,
TLS_RSA_WITH_AES_128_GCM_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA256,
TLS_RSA_WITH_AES_128_CBC_SHA,
TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_DHE_RSA_WITH_DES_CBC_SHA,
TLS_RSA_WITH_3DES_EDE_CBC_SHA,
TLS_RSA_WITH_DES_CBC_SHA,
TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA,
TLS_RSA_WITH_NULL_SHA256,
TLS_RSA_WITH_NULL_SHA,
TLS_RSA_WITH_NULL_MD5,
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256,
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384,
ALL,
NONE>
```

## 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.

## Registration

The Oracle Enterprise Session Border Controller uses the configuration information of the surrogate agent that corresponds to a specific IP-PBX. After the surrogate agents are loaded, the Oracle Enterprise Session Border Controller starts sending the REGISTER requests on their behalf. (You can configure how many requests are sent.)

The SIP surrogate agent supports the ability to cache authorization or proxy-authorization header values from a REGISTER 401, 407, and 200 OK messages and reuse it in subsequent requests, such as in an INVITE. This allows the Oracle Communications Session Delivery Manager to support authorization of subsequent requests in cases such as, when a customer PBX doesn't support registration and authentication. It also supports the generation of authorization/proxy-authorization header if subsequent requests get challenged with a 401/407 response.

If the Oracle Enterprise Session Border Controller receives 401 or 407 responses to REGISTER, requests, it will use the Message Digest algorithm 5 (MD5) digest authentication to generate the authentication information. You need to specify the password. The Oracle Enterprise Session Border Controller also supports authentication challenge responses with the quality of protection code set to auth (qop=auth), by supporting the client nonce (cnonce) and nonce count parameters.

The Oracle Enterprise Session Border Controller creates a registration cache entry for each of the AoRs for which it is sending the REGISTER requests. When the Oracle Enterprise Session Border Controller receives the associated URIs, it checks whether the customer host parameter is configured. If it is configured, the Oracle Enterprise Session Border Controller changes the host in the received Associated-URI to the customer host. If it is not configured, the Oracle Enterprise Session Border Controller does not change the Associated-URI. It makes the registration cache entries that correspond to each of the Associated-URIs. The From header in the INVITE for calls coming from the IP-PBX should have one of the Associated-URIs (URI for a specific phone). If the Oracle Enterprise Session Border Controller receives a Service-Route in the 200 (OK) response, it stores that as well.

The Oracle Enterprise Session Border Controller uses the expire value configured for the REGISTER requests. When it receives a different expire value in the 200 OK response to the registration, it stores the value and continues sending the REGISTER requests once half the expiry time has elapsed.

REGISTER requests are routed to the registrar based on the configuration. The Oracle Enterprise Session Border Controller can use the local policy, registrar host and the SIP configuration's registrar port for routing.

If the Oracle Enterprise Session Border Controller is generating more than one register on behalf of the IP-PBX, the user part of the AoR is incremented by 1 and the register contact-user parameter will also be incremented by 1. For example, if you configure the register-user

parameter as caller, the Oracle Enterprise Session Border Controller uses caller, caller1, caller2 and so on as the AoR user.

## Routing Calls from the IP-PBX

The Oracle Enterprise Session Border Controller (E-SBC) looks for a match in the registration cache based on the From header or the P-Preferred-Identity header. The header should contain the user portion of one of the Associated-URIs that it received from the registrar in the 200 (OK) responses to REGISTER requests. It should also have the same hostname that is configured in the customer-host parameter. If that parameter is not configured, then the hostname should be same as the one configured for the register-host parameter.

After the corresponding registration Service-Router entry is found, the E-SBC uses the Service-Route for this endpoint to route the call, if it exists. If no Service-Route exists but the SIP interface's route-to-registrar parameter is enabled, the E-SBC tries to route this to the registrar. You can configure the surrogate agent to override the SIP interface's route-to-register setting. If the surrogate agent's route-to-register parameter is set to disable, it takes precedence over the SIP interface's setting. The E-SBC will not try to route the call to the registrar.

## Configure Surrogate Registration - GUI

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.

Set the system to Super User mode.

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.

Attributes	Instructions
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 <b>enabled</b> .
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: <ul style="list-style-type: none"> <li>• session agent group: &lt;session agent group name&gt;</li> <li>• session agent: &lt;hostname&gt; or &lt;IPV4&gt;</li> </ul>
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 <b>600,000</b> (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 <b>disabled</b> . 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 <b>enabled</b> . 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 <b>1</b> , 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 <b>1</b> . The valid range is 0-999999999.



Attributes	Instructions
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 401 or 407 response to the REGISTER request and has to send the REGISTER request again with the Authorization or Proxy-Authorization header. The name you enter here is used in the Digest username parameter. If you do not enter a name, the E-SBC uses the value of the register-user parameter.
Max register attempts	Enter the total number of times to attempt registration until success. Range 1-10
Registry retry time	Enter the time to wait after an unsuccessful registration before re-attempting. Range 30-3600
Count start	Enter the starting value for numbering when performing multiple registrations. Range 0-9999999999
Register mode	Select automatic (default) or triggered (upon trigger from PBX).
Triggered inactivity interval	Enter the maximum time with no traffic from the corresponding PBX. (Valid only with Triggered inactivity interval.) Range 5 -300
Triggered OoS response	503 (Default. Send 503 response for core network failure) or drop response (Do not respond to PBX or core network failure)

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

#### Next Steps

You must add the surrogate agent as a session-agent under session-router.

## 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.

Set the system to Super User mode.

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.

- Access the **surrogate-agent** configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# session-router
```

```
ORACLE(session-router)# surrogate-agent
ORACLE(surrogate-agent)#
```

2. 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 <b>enabled</b> .
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: <ul style="list-style-type: none"> <li>session agent group: &lt;session agent group name&gt;</li> <li>session agent: &lt;hostname&gt; or &lt;IPV4&gt;</li> </ul>
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 <b>600,000</b> (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 <b>disabled</b> . 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 <b>enabled</b> . The valid values are enabled and disabled.

Attributes	Instructions
AoR count	Enter the number of registrations to do on behalf of this IP-PBX. If you enter a value greater than <b>1</b> , 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 <b>1</b> . 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 401 or 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 0-999999999
Register mode	Select automatic (default) or triggered (upon trigger from PBX).
Triggered inactivity interval	Enter the maximum time with no traffic from the corresponding PBX. (Valid only with Triggered inactivity interval.) Range 5 -300
Triggered OoS response	503 (Default. Send 503 response for core network failure) or drop response (Do not respond to PBX or core network failure)

### 3. Save and activate your configuration.

#### Next Steps

You must add the surrogate agent as a session-agent under session-router.

## Example

The following example shows the surrogate agent configuration.

```

surrogate-agent
register-host    acmepacket.com
register-user    234567
state           enabled
realm-id        public
description
customer-host   acmepacket.com
customer-next-hop 111.222.333.444
register-contact-host 111.222.5.678
register-contact-user eng
password
register-expires 600000

```

```

replace-contact    disabled
route-to-registrar enabled
aor-count          1
options
auth-user
last-modified-date 2006-05-04 16:01:35

```

## TCP Connection Tools

Transmission Control Protocol (TCP) connection tools can assist you in gauging performance, identifying potential memory leaks, and debugging connections for performance tracking and improvement.

The **show ip tcp** command shows the following socket connections by state:

- inbound
- outbound
- listen
- IMS-AKA (Although the Oracle Enterprise Session Border Controller (E-SBC) displays the IMS-AKA statistics fields, the E-SBC does not support providing the corresponding values.)

The **show sipd tcp** and **show sipd tcp connections** commands display counters to track usage. Use the **reset sipd** command to reset the counters.

## TCP and SCTP State Connection Counters

The Oracle Enterprise Session Border Controller (E-SBC) can provide systemwide counts of Transmission Control Protocol (TCP) and Stream Control Transmission Protocol (SCTP) states by way of the **show ip tcp** and **show ip sctp** commands from the ACLI.

The **show ip tcp** command includes the following section of counters that correspond to counts of TCP states per active connections, including counts differentiated by inbound, outbound, listen and IMS-AKA connections.

### Note:

Although the Oracle Enterprise Session Border Controller (E-SBC) displays the IMS-AKA statistics fields, the E-SBC does not support providing the corresponding values.

```

Connections By State:
0      CLOSED
0      LISTEN
0      SYN_SENT
0      SYN_RCVD
0      ESTABLISHED
0      CLOSE_WAIT
0      FIN_WAIT_1
0      CLOSING
0      LAST_ACK
0      FIN_WAIT_2
0      TIME_WAIT

```

```
Inbound Socket Connection By State:
```

```

0    CLOSED
0    LISTEN
0    SYN_SENT
0    SYN_RCVD
50   ESTABLISHED
0    CLOSE_WAIT
0    FIN_WAIT_1
0    CLOSING
0    LAST_ACK
0    FIN_WAIT_2
0    TIME_WAIT

```

Outbound Socket Connection By State:

```

0    CLOSED
0    LISTEN
0    SYN_SENT
0    SYN_RCVD
1    ESTABLISHED
0    CLOSE_WAIT
0    FIN_WAIT_1
0    CLOSING
0    LAST_ACK
0    FIN_WAIT_2
0    TIME_WAIT

```

Listen Socket Connection By State:

```

0    CLOSED
2    LISTEN
0    SYN_SENT
0    SYN_RCVD
0    ESTABLISHED
0    CLOSE_WAIT
0    FIN_WAIT_1
0    CLOSING
0    LAST_ACK
0    FIN_WAIT_2
0    TIME_WAIT

```

IMSAKA Inbound Socket Connection By State:

```

0    CLOSED
0    LISTEN
0    SYN_SENT
0    SYN_RCVD
0    ESTABLISHED
0    CLOSE_WAIT
0    FIN_WAIT_1
0    CLOSING
0    LAST_ACK
0    FIN_WAIT_2
0    TIME_WAIT

```

IMSAKA Outbound Socket Connection By State:

```

0    CLOSED
0    LISTEN
0    SYN_SENT
0    SYN_RCVD
0    ESTABLISHED

```

```

0    CLOSE_WAIT
0    FIN_WAIT_1
0    CLOSING
0    LAST_ACK
0    FIN_WAIT_2
0    TIME_WAIT

```

IMSACA Listen Socket Connection By State:

```

0    CLOSED
0    LISTEN
0    SYN_SENT
0    SYN_RCVD
0    ESTABLISHED
0    CLOSE_WAIT
0    FIN_WAIT_1
0    CLOSING
0    LAST_ACK
0    FIN_WAIT_2
0    TIME_WAIT

```

```

Number of Connections Counted = 0
Maximum Connection Count = 0
Maximum Number of Connections Supported = 220000

```

The **show ip sctp** command includes the following section of counters that correspond to counts of SCTP states per active connections.

Connections By State:

```

0    CLOSED
0    BOUND
0    LISTEN
0    COOKIE_WAIT
0    COOKIE_ECHOED
0    ESTABLISHED
0    SHUTDOWN_SENT
0    SHUTDOWN_RECEIVED
0    SHUTDOWN_ACK_SENT
0    SHUTDOWN_PENDING

```

```

Number of Connections Counted = 0
Maximum Connection Count = 0
Maximum Number of Connections Supported = 10000

```

The output of the state counters indicates the number of connections currently in each state. The statistics from the counters do not accumulate like many of the other statistics in the **show ip** command tree. Most states are ephemeral, and you may see many "0" counters for states other than LISTEN and ESTABLISHED.

## show sipd tcp connections

The **show sipd tcp connections** command displays Transmission Control Protocol (TCP) connection information details on remote and local address/port and connection states for analysis. Oracle recommends that you use the command only during non-peak times or maintenance windows.

The **show sipd tcp connections** command displays all SIP/TCP connections including each connection's direction, type, state, local and remote addresses, SIP interface and IMS-AKA details. Arguments include:

- `sip-interface`—Optional parameter that limits output to sockets in the specified sip-interface
- `start start`—Integer indicating which connection to start displaying. This can be a negative number. When the number selected for the start variable is greater than the number of TCP connections, the system displays nothing.
- `start-count start`—Integer as per above plus the count integer, specifying how many TCP connections to display from the start.
- `all`—Display all of the sipd tcp connections. Exercise caution due to the possibility of consuming all CPU time; preferably use during a maintenance window

 **Note:**

Although the Oracle Enterprise Session Border Controller (E-SBC) displays the IMS-AKA statistics fields, the E-SBC does not support providing the corresponding values.

For example:

```
ORACLE# show sipd tcp connections
```

```
sipd tcp connections
```

Dir	Type	State	Local Address	Remote Address	sip-
interface-id		isImsaka			
	LISTEN	TCP_LISTENING	172.16.101.149:5060		
net172	in FORKED	TCP_CONNECTED	172.16.101.149:5060	172.16.23.100:51678	
net172	in FORKED	TCP_CONNECTED	172.16.101.149:5060	172.16.23.100:51679	
net172	[...]				
net172	in FORKED	TCP_CONNECTED	172.16.101.149:5060	172.16.23.100:51727	
net172	in FORKED	TCP_CONNECTED	172.16.101.149:5060	172.16.23.100:51728	
net172	in FORKED	TCP_CONNECTED	172.16.101.149:5060	172.16.23.100:51729	
net172	LISTEN	TCP_LISTENING	192.168.101.149:5060		
net192	out CONNECT	TCP_CONNECTED	192.168.101.149:8192	192.168.23.100:5060	
net192					
Connections Displayed:			53		
Total Connections:			53		

## show sipd tcp

The **show sipd tcp** command displays TCP connection state information for the following:

- inbound
- outbound

- listen
- total
- IMS-AKA (Although the Oracle Enterprise Session Border Controller (E-SBC) displays the IMS-AKA statistics fields, the E-SBC does not support providing the corresponding values.)

For example:

```
ORACLE# show sipd tcp
11:11:54-110
SIP TCP Sockets
```

	Active	-- Period --		----- Lifetime -----		
		High	Total	Total	PerMax	High
All States	53	53	108	108	108	53
TCP_INITIAL	0	0	0	0	0	0
TCP_STARTING	0	0	0	0	0	0
TCP_AVAILABLE	0	1	51	51	51	1
TCP_BOUND	0	1	3	3	3	1
TCP_CONNECTED	51	51	51	51	51	51
TCP_CONNECTING	0	1	1	1	1	1
TCP_LISTENING	2	2	2	2	2	2
TCP_DISCONNECT	0	0	0	0	0	0
TCP_CLOSED	0	0	0	0	0	0

---

```
SIP Inbound TCP Sockets
```

	Active	-- Period --		----- Lifetime -----		
		High	Total	Total	PerMax	High
All States	50	50	100	100	100	50
TCP_INITIAL	0	0	0	0	0	0
TCP_STARTING	0	0	0	0	0	0
TCP_AVAILABLE	0	1	50	50	50	1
TCP_BOUND	0	0	0	0	0	0
TCP_CONNECTED	50	50	50	50	50	50
TCP_CONNECTING	0	0	0	0	0	0
TCP_LISTENING	0	0	0	0	0	0
TCP_DISCONNECT	0	0	0	0	0	0
TCP_CLOSED	0	0	0	0	0	0

---

```
SIP Outbound TCP Sockets
```

	Active	-- Period --		----- Lifetime -----		
		High	Total	Total	PerMax	High
All States	1	1	4	4	4	1
TCP_INITIAL	0	0	0	0	0	0
TCP_STARTING	0	0	0	0	0	0
TCP_AVAILABLE	0	1	1	1	1	1
TCP_BOUND	0	1	1	1	1	1
TCP_CONNECTED	1	1	1	1	1	1
TCP_CONNECTING	0	1	1	1	1	1
TCP_LISTENING	0	0	0	0	0	0
TCP_DISCONNECT	0	0	0	0	0	0
TCP_CLOSED	0	0	0	0	0	0

---

```
SIP Listen TCP Sockets
```

	Active	-- Period --		----- Lifetime -----		
		High	Total	Total	PerMax	High
All States	2	2	4	4	4	2
TCP_INITIAL	0	0	0	0	0	0
TCP_STARTING	0	0	0	0	0	0



```
TCP_AVAILABLE      0      0      0      0      0      0
TCP_BOUND          0      1      2      2      2      1
TCP_CONNECTED      0      0      0      0      0      0
TCP_CONNECTING     0      0      0      0      0      0
TCP_LISTENING      2      2      2      2      2      2
TCP_DISCONNECT     0      0      0      0      0      0
TCP_CLOSED         0      0      0      0      0      0
```

-----

IMS-AKA portion of show sipd tcp command:

```
ORACLE# show sipd tcp
15:28:51-197
[...]
```

```
SIP IMSAKA In TCP Sockets  -- Period --  ----- Lifetime -----
                          Active  High  Total      Total  PerMax  High
All States                0      0      0          0      0      0
TCP_INITIAL               0      0      0          0      0      0
TCP_STARTING              0      0      0          0      0      0
TCP_AVAILABLE            0      0      0          0      0      0
TCP_BOUND                 0      0      0          0      0      0
TCP_CONNECTED             0      0      0          0      0      0
TCP_CONNECTING            0      0      0          0      0      0
TCP_LISTENING             0      0      0          0      0      0
TCP_DISCONNECT            0      0      0          0      0      0
TCP_CLOSED                0      0      0          0      0      0
```

```
-----
SIP IMSAKA Out TCP Sockets -- Period --  ----- Lifetime -----
                          Active  High  Total      Total  PerMax  High
All States                0      0      0          0      0      0
TCP_INITIAL               0      0      0          0      0      0
TCP_STARTING              0      0      0          0      0      0
TCP_AVAILABLE            0      0      0          0      0      0
TCP_BOUND                 0      0      0          0      0      0
TCP_CONNECTED             0      0      0          0      0      0
TCP_CONNECTING            0      0      0          0      0      0
TCP_LISTENING             0      0      0          0      0      0
TCP_DISCONNECT            0      0      0          0      0      0
TCP_CLOSED                0      0      0          0      0      0
```

```
-----
SIP IMSAKA Listen TCP Sockets -- Period --  ----- Lifetime -----
                          Active  High  Total      Total  PerMax  High
All States                1      1      0          2      2      1
TCP_INITIAL               0      0      0          0      0      0
TCP_STARTING              0      0      0          0      0      0
TCP_AVAILABLE            0      0      0          0      0      0
TCP_BOUND                 0      0      0          1      1      1
TCP_CONNECTED             0      0      0          0      0      0
TCP_CONNECTING            0      0      0          0      0      0
TCP_LISTENING             1      1      0          1      1      1
TCP_DISCONNECT            0      0      0          0      0      0
TCP_CLOSED                0      0      0          0      0      0
```

## Updated Show Commands

### show ip

#### Syntax

```
show ip <arguments>
```

Displays IP statistics for the Oracle Enterprise Session Border Controller.

#### Arguments

The following is a list of valid show ip arguments:

- `statistics` —Display detailed IP statistics
- `connections` —Display all TCP and UDP connections
- `setp`—Display all SCTP statistics, including a list of current connections per SCTP state and systemwide counts.
- `tcp` —Display all TCP statistics, including a list of current connections per TCP state and differentiated by inbound, outbound, listen and IMS-AKA connections as well as systemwide counts. (Although the Oracle Enterprise Session Border Controller (E-SBC) displays the IMS-AKA statistics fields, the E-SBC does not support providing the corresponding values.)
- `udp` —Display all UDP statistics

Executing the **show ip** command with no arguments returns the equivalent of the **show ip statistics** command.

### show sipd

#### Syntax

```
show sipd <arguments>
```

The show sipd command displays SIP statistics on your Oracle Enterprise Session Border Controller.



#### Note:

(Although the Oracle Enterprise Session Border Controller (E-SBC) displays the IMS-AKA statistics fields, the E-SBC does not support providing the corresponding values.)

#### Arguments

`status`—Display information about SIP transactions. These statistics are given for the Period and Lifetime monitoring spans. This display also provides statistics related to SIP media events. The following statistics are displayed when using the show sipd status command.

- `Dialogs`—Number of end-to-end SIP signaling connections
- `CallID Map`—Total number of successful session header Call ID mappings
- `Sessions`—Number of sessions established by an INVITE

- Subscriptions—Number of sessions established by SUBSCRIPTION
- Rejections—Number of rejected INVITEs
- ReINVITEs—Number of ReINVITEs
- Media Sessions—Number of successful media sessions
- Media Pending—Number of media sessions waiting to be established
- Client Trans—Number of client transactions
- Server Trans—Number of server transactions that have taken place on the Oracle Enterprise Session Border Controller
- Resp Contexts—Number of current response contexts
- Saved Contexts—Total number of saved contexts
- Sockets—Number of active SIP sockets
- Req Dropped—Number of requests dropped
- DNS Trans—Number of DNS transactions
- DNS Sockets—Number of DNS Sockets
- DNS Results—Number of dns results
- Session Rate—The rate, per second, of SIP invites allowed to or from the Oracle Enterprise Session Border Controller during the sliding window period. The rate is computed every 10 seconds
- Load Rate—Average Central Processing Unit (CPU) utilization of the Oracle Enterprise Session Border Controller during the current window. The average is computed every 10 seconds. When you configure the load-limit in the SIPConfig record, the system computes the average every 5 seconds

errors —Display statistics for SIP media event errors. These statistics are errors encountered by the SIP application in processing SIP media sessions, dialogs, and session descriptions (SDP). Errors are only displayed for the lifetime monitoring span.

- SDP Offer Errors—Number of errors encountered in setting up the media session for a session description in a SIP request or response which is an SDP Offer in the Offer/Answer model (RFC 3264)
- SDP Answer Errors—Number of errors encountered in setting up the media session for a session description in a SIP request or response which is an SDP Answer in the Offer/Answer model (RFC 3264)
- Drop Media Errors—Number of errors encountered in tearing down the media for a dialog or session that is being terminated due to: a) non-successful response to an INVITE transaction; or b) a BYE transaction received from one of the participants in a dialog or session; or c) a BYE initiated by the system due to a timeout notification from MBCD
- Transaction Errors—Number of errors in continuing the processing of the SIP client transaction associated with setting up or tearing down of the media session
- Missing Dialog—Number of requests received by the SIP application for which a matching dialog count not be found
- Application Errors—Number of miscellaneous errors in the SIP application that are otherwise uncategorized
- Media Exp Events—Flow timer expiration notifications received from MBCD

- Early Media Exps—Flow timer expiration notifications received for media sessions that have not been completely set up due to an incomplete or pending INVITE transaction
  - Exp Media Drops—Number of flow timer expiration notifications from the MBCD that resulted in the termination of the dialog/session by the SIP application
  - Multiple OK Drops—Number of dialogs terminated upon reception of a 200 OK response from multiple UASs for a given INVITE transaction that was forked by a downstream proxy
  - Multiple OK Terms—Number of dialogs terminated upon reception of a 200 OK response that conflicts with an existing established dialog on the Oracle Enterprise Session Border Controller
  - Media Failure Drops—Number of dialogs terminated due to a failure in establishing the media session
  - Non-ACK 2xx Drops—Number of sessions terminated because an ACK was not received for a 2xx response
  - Invalid Requests—Number of invalid requests; an unsupported header for example
  - Invalid Responses—Number of invalid responses; no Via header for example
  - Invalid Messages—Number of messages dropped due to parse failure
  - CAC Session Drop—Number of call admission control session setup failures due to user session count exceeded
  - Expired Sessions—Number of sessions terminated due to the session timer expiring
  - CAC BW Drop—Number of call admission control session setup failures due to insufficient bandwidth
- Lifetime displays show information for recent, total, and period maximum error statistics:
- Recent—Number of errors occurring in the number of seconds listed after the time stamp
  - Total—Number of errors occurring since last reboot
  - PerMax—Identifies the highest individual Period Total over the lifetime of the monitoring
- policy—Display SIP local policy / routing statistics for lifetime duration
- Local Policy Lookups—Number of Local policy lookups
  - Local Policy Hits—Number of successful local policy lookups
  - Local Policy Misses—Number of local policy lookup failures
  - Local Policy Drops—Number of local policy lookups where the next hop session agent group is H323
  - Agent Group Hits—Number of successful local policy lookups for session agent groups
  - Agent Group Misses—Number of successful local policy lookups where no session agent was available for session agent group
  - No Routes Found—Number of successful local policy lookups but temporarily unable to route; session agent out of service for instance
  - Missing Dialog—Number of local policy lookups where the dialog is not found for a request addressed to the Oracle Enterprise Session Border Controller with a To tag or for a NOTIFY-SUBSCRIBE sip request
  - Inb SA Constraints—Number of successful local policy lookups where inbound session agent exceeded constraints

- Outb SA Constraints—Number of successful outbound local policy lookups where session agent exceeded constraints
- Inb Reg SA Constraints—Number of successful inbound local policy lookups where registrar exceeded constraints
- Out Reg SA Constraints—Number of successful outbound local policy lookups where registrar exceeded constraints
- Requests Challenged—Number of requests challenged
- Challenge Found— Number of challenges found
- Challenge Not Found—Number of challenges not found
- Challenge Dropped—Number of challenges dropped

server—Display statistics for SIP server events when the Oracle Enterprise Session Border Controller acts as a SIP server in its B2BUA role. Period and Lifetime monitoring spans for SIP server transactions are provided.

- All States—Number of all server transactions
- Initial—Number of times the “initial” state was entered after a request was received
- Queued—Number of times the “queued” state is entered because resources are temporarily unavailable
- Trying—Number of times the “trying” state was entered due to the receipt of a request
- Proceeding—Number of times a server transaction has been constructed for a request
- Cancelled—Number of INVITE transactions that received a CANCEL
- Established—Number of times the server sent a 2xx response to an INVITE
- Completed—Number of times the server received a 300 to 699 status code and entered the “completed” state
- Confirmed—Number of times that an ACK was received while the server was in “completed” state and transitioned to “confirmed” state
- Terminated—Number of times that the server received a 2xx response or never received an ACK in the “completed” state, and transitioned to the “terminated” state

client —Display statistics for SIP client events when the Oracle Enterprise Session Border Controller is acting as a SIP client in its B2BUA role. Period and Lifetime monitoring spans are displayed.

- All States—Number of all client transactions
- Initial—State when initial server transaction is created before a request is sent
- Trying—Number of times the “trying” state was entered due to the sending of a request
- Calling—Number of times that the “calling” state was entered due to the receipt of an INVITE request
- Proceeding—Number of times that the “proceeding” state was entered due to the receipt of a provisional response while in the “calling” state
- Early Media—Number of times that the “proceeding” state was entered due to the receipt of a provisional response that contained SDP while in the “calling” state
- Completed—Number of times that the “completed” state was entered due to the receipt of a status code in the range of 300-699 when either in the “calling” or “proceeding” state

- SetMedia—Number of transactions in which the Oracle Enterprise Session Border Controller is setting up NAT and steering ports
- Established—Number of situations when client receives a 2xx response to an INVITE, but cannot forward it because it NAT and steering port information is missing
- Terminated—Number of times the “terminated” state was entered after a 2xx message

acls—Display ACL information for Period and Lifetime monitoring spans

- Total entries—Total ACL Entries, including both trusted and blocked
- Trusted—Number of trusted ACL entries
- Blocked—Number of blocked ACL entries
- Blocked NATs—Number of blocked entries that are behind NATs  
Lifetime monitoring span is displayed for SIP ACL Operations.
- ACL Requests—Number of ACL requests
- Bad Messages —Number of bad messages
- Promotions—Number of ACL entry promotions
- Demotions—Number of ACL entry demotions
- Trust->Untrust—Number of ACL entries demoted from trusted to untrusted
- Untrust->Deny—Number of acl entries demoted from untrusted to deny

sessions—Display the number of sessions and dialogs in various states for the Period and Lifetime monitoring spans, in addition to the current Active count:

- Sessions—Identical to the identically named statistic on the show sipd status command
- Initial—Displays sessions for which an INVITE or SUBSCRIBE is being forwarded
- Early—Displays sessions for which the first provisional response (1xx other than 100) is received
- Established—Displays sessions for which a success (2xx) response is received
- Terminated—Displays sessions for which the session is ended by receiving or sending a BYE for an “Established” session or forwarding an error response for an “Initial” or “Early” session. The session will remain in the “Terminated” state until all the resources for the session are freed.
- Dialogs—Identical to the identically named statistic on the show sipd status command
- Early—Displays dialogs that were created by a provisional response
- Confirmed—Displays dialogs that were created by a success response. An “Early” dialog will transition to “Confirmed” when a success response is received
- Terminated—Displays dialogs that were ended by receiving/sending a BYE for an “Established” session or receiving/sending error response “Early” dialog. The dialog will remain in the “Terminated” state until all the resources for the session are freed.

sessions all—Display all SIP sessions currently on the system

sessions by-agent <agent name>—Display SIP sessions for the session agent specified; adding iwf to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

sessions by-ip <endpoint IP address>—Display SIP sessions for the specified IP address for an endpoint; adding iwf to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

sessions by-user <calling or called number>—Display SIP sessions for the specified user; adding iwf to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

sessions by-callid <call ID>—Display SIP sessions for the specified call ID; adding iwf to the end of the command shows sessions for the IWF; adding detail to the end of the command expands the displayed information

redundancy—Display sipd redundancy statistics. Executing the show sipd redundancy command is the equivalent to the show redundancy sipd command.

agents [hostname][method][-t]—Display statistics related to defined SIP session agents. Entering this command without any arguments list all SIP session agents. By adding the IP address or hostname of a session agent as well as a specified method at the end of the command, you can display statistics for that specific session agent and method. For a specific session agent, identified by IP address, the show sipd agents command lists:

- session agent state
    - D—disabled
    - I—in-service
    - O—out-of-service
    - S—transitioning from out-of-service to in-service
  - inbound and outbound statistics
  - average and maximum latency for each session agent
  - maximum burst rate for each session agent as total number of session invitations sent to or received from the session agent within the amount of time configured in the burst-rate-window field
- Inbound Statistics:
- Active—Number of active sessions sent to each session agent listed
  - Rate—Average rate of session invitations (per second) sent to each session agent listed
  - ConEx—Number of times the constraints have been exceeded
- Outbound Statistics:
- Active—Number of active sessions sent from each session agent
  - Rate—Average rate of session invitations (per second) sent from each session agent listed
  - ConEx—Number of times the constraints have been exceeded
- Latency:
- Avg—Average latency for packets traveling to and from each session agent
  - Max—Maximum latency for packets traveling to and from each session agent listed
- t—Append to the end of the command to specify the current time period for the max-burst value.

interface [interface-id][method]—Display SIP interface statistics. By adding the optional interface-id and method arguments you can narrow the display to view just the interface and method you want to view.

ip-cac <IP address>—Display CAC parameters for an IP address

publish—Display statistics related to incoming SIP PUBLISH messages

agent <agent>—Display activity for the session agent that you specify

- Inbound Sessions:
  - Rate Exceeded—Number of times session or burst rate was exceeded for inbound sessions
- Num Exceeded—Number of times time constraints were exceeded for inbound sessions
- Outbound Sessions:
  - Rate Exceeded—Number of times session or burst rate was exceeded for outbound sessions
  - Num Exceeded—Number of times time constraints were exceeded for inbound sessions
  - Burst—Number of times burst rate was exceeded for this session agent
  - Out of Service—Number of times this session agent went out of service
  - Trans Timeout—Number of transactions timed out for this session agent
  - Requests Sent—Number of requests sent by way of this session agent
  - Requests Complete—Number of requests that have been completed for this session agent
  - Messages Received—Number of messages received by this session agent

realm—Display realm statistics related to SIP processing

routers—Display status of Oracle Enterprise Session Border Controller connections for session router functionality

directors—Display the status of Oracle Enterprise Session Border Controller connections for session director functionality

<message>—Add one of the following arguments to the end of a show sipd command to display information about that type of SIP message:

- INVITE—Display the number of SIP transactions including an INVITE method
- REGISTER—Display the number of SIP transactions including a REGISTER method
- OPTIONS—Display the number of SIP transactions including an OPTIONS method
- CANCEL—Display the number of SIP transactions including a CANCEL method
- BYE—Display the number of SIP transactions including a BYE method
- ACK—Display the number of SIP transactions including an ACK method
- INFO—Display the number of SIP transactions including an INFO method
- PRACK—Display the number of SIP transactions including a PRACK method
- SUBSCRIBE—Display the number of SIP transactions including a SUBSCRIBE method
- NOTIFY—Display the number of SIP transactions including a NOTIFY method
- REFER—Display the number of SIP transactions including a REFER method
- UPDATE—Display the number of SIP transactions including an UPDATE method
- other—Display the number of SIP transactions including non-compliant methods and protocols used by specific customers



The following lists information displayed for each individual SIP message statistic. Some or all of the following messages and events may appear in the output from a show sipd command.

- INVITE Requests—Number of times method has been received or sent
- Retransmissions—Information regarding sipd message command requests received by the Oracle Enterprise Session Border Controller
- 100 Trying—Number of times some unspecified action is being taken on behalf of a call (e.g., a database is being consulted), but user has not been located
- 180 Ringing—Number of times called UA identified a location where user has registered recently and is trying to alert the user
- 200 OK—Number of times request has succeeded
- 408 Request Timeout—Number of times server could not produce a response before timeout
- 481 Does Not Exist—Number of times UAS received a request not matching existing dialog or transaction
- 486 Busy Here—Number of times callee's end system was contacted successfully but callee not willing to take additional calls
- 487 Terminated—Number of times request was cancelled by a BYE or CANCEL request
- 4xx Client Error—Number of times the 4xx class of status code appeared for cases where the client seems to have erred
- 503 Service Unavail—Number of times server was unable to handle the request due to a temporary overloading or maintenance of the server
- 5xx Server Error—Number of times the 5xx class of status code appeared
- Response Retrsns—Number of response retransmissions sent and received
- Transaction Timeouts— Number of times a transaction timed out. The timer related to this transaction is Timer B, as defined in RFC 3261
- Locally Throttled—Number of locally throttled invites. Does not apply to a server. show sipd <message> output is divided in two sections: Server and Client, with information for recent, total, and period maximum time frames. This command also displays information about the average and maximum latency. For each type of SIP message, only those transactions for which there are statistics are shown. If there is no data available for a certain SIP message, the system displays the fact that there is none and specifies the message about which you inquired.

groups—Display cumulative information for all session agent groups on the Oracle Enterprise Session Border Controller. This information is compiled by totaling the session agent statistics for all of the session agents that make up a particular session agent group. While the show sipd groups command accesses the sub-commands described in this section, the main show sipd groups command (when executed with no arguments) displays a list of all session agent groups.

groups -v—Display statistics for the session agents that make up the session agent groups that are being reported. The -v (meaning “verbose”) executed with this command must be included to provide verbose detail.

groups <specific group name>— Display statistics for the specified session agent group

endpoint-ip <phone number> —Displays registration information for a designation endpoint entered in the <phone number> argument; also show IMS-AKA data

all—Display all the show sipd statistics listed above

sip-endpoint-ip—See show sipd endpoint-ip

sa-nsep-burst—Display NSEP burst rate for all SIP session agents

subscriptions-by-user—Display data for SIP per user subscribe dialog limit

rate—Displays the transaction rate of SIP messages

codecs—Displays codec usage per realm, including counts for codecs that require a license such as SILK and opus.

pooled-transcoding—Pooled transcoding information for the client and server User Agents on the P-CSCF

srvc—Displays EATF Session information

tcp—Displays TCP connection state information for the following

- inbound
- outbound
- listen
- IMS-AKA
- total

tcp connections—Dump TCP connections for analysis. Options include:

- sip-interface—Optional parameter that limits output to sockets in the specified sip-interface
- start start—Integer indicating which connection to start display. This can be a negative number. If the number selected for the start variable is greater than the number of TCP connections, nothing will be displayed
- start-count start—Integer as per above plus the count integer, specifying how many TCP connections to display from the start.
- all—Dump all of the sipd tcp connections. Exercise caution due to the possibility of consuming all CPU time; preferably use during a maintenance window

### Example

```
ORACLE# show sipd errors
```

## 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.

The screenshot shows the Oracle Configuration interface for the 'login-config' page. The left sidebar lists various objects, with 'login-config' selected. The main content area displays the following configuration parameters:

Parameter	Value	Range
Enable login banner:	<input checked="" type="checkbox"/>	
Concurrent session limit:	3	(Range: 1..10)
Max login attempts:	3	(Range: 2..100)
Login attempt interval:	30	(Range: 4..60)
Lockout interval:	30	(Range: 30..300)
Send alarm:	<input checked="" type="checkbox"/>	
Login auth method:	single-factor	

**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.

The screenshot shows the Oracle Configuration interface for the 'password-policy' page. The left sidebar lists various objects, with 'password-policy' selected. The main content area displays the following configuration parameters:

Parameter	Value	Range
Min secure pwd len:	8	(Range: 8..64)
Expiry interval:	30	(Range: 1..65535)
Expiry notify period:	2	(Range: 1..90)
Grace period:	3	(Range: 1..90)
Grace logins:	3	(Range: 1..10)
Password history count:	5	(Range: 3..10)
Password change interval:	24	(Range: 1..24)

### Enhanced Security Requirements

**HTTPS**—The system requires an HTTPS connection to access the Web GUI. Oracle recommends that you configure HTTPS on the Web server before installing the Admin Security License. If the Web server is configured for HTTP when you install the Admin Security License, the system displays an error message when you attempt to Save. Note that after 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

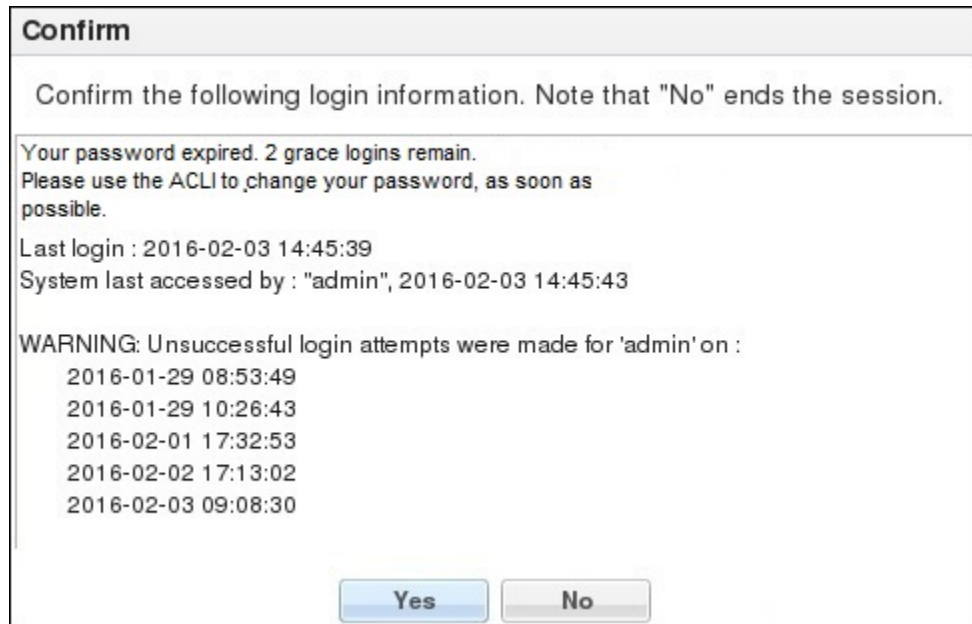
**Concurrent Sessions Limit**—In login-config, you can specify the maximum number of concurrent sessions allowed. When the limit is reached, the system allows no more logins until the number of active sessions falls below the maximum.

**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.

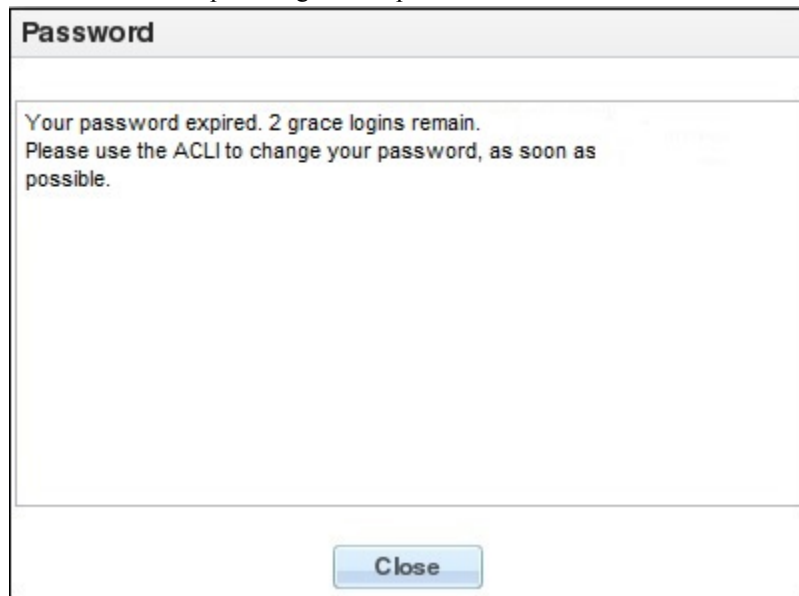


**Password Expiry Notification**—You can configure password-policy to notify the user up to 90 days in advance of password expiry. The system provides the notification in the following ways.

- 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:

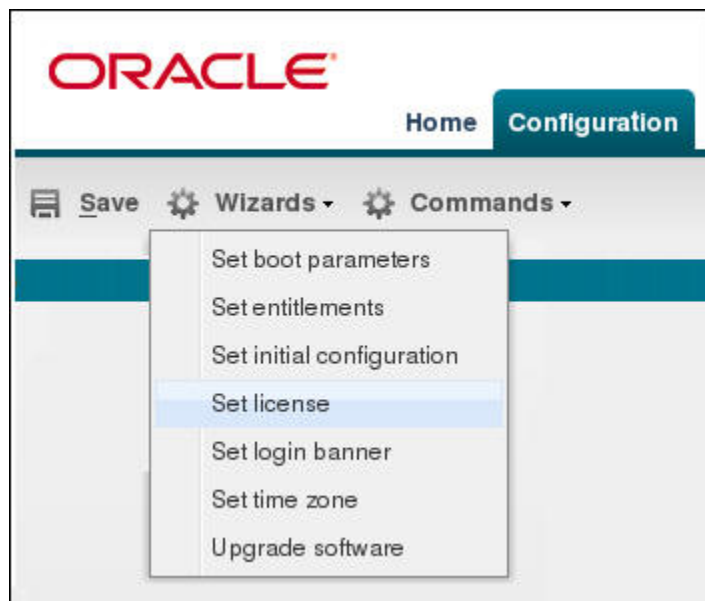
- The local Admin and User can login by way of the E-SBC console, the Web GUI, SSH or SFTP, and the system performs the local user authentication process.

- 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.

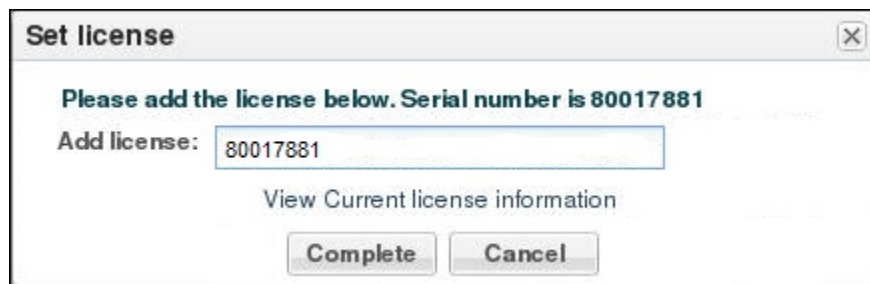
Two-Factor Authentication. When enabled, the system prompts the user for a passcode in addition to the User Name and Password. Change the default passcode upon the first login attempt. The length and strength requirements that apply to passwords also apply to passcodes. Other policy mandates such as 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.

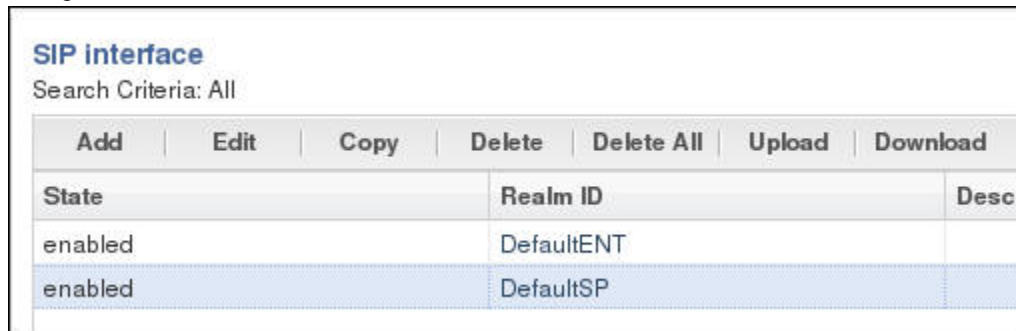
For license installation instructions, see "Set License" in the *WEB GUI User Guide*, and the online Help.

## Web GUI Enhancements

The ECZ7.3.0M2 release includes the following enhancements to the Web GUI.

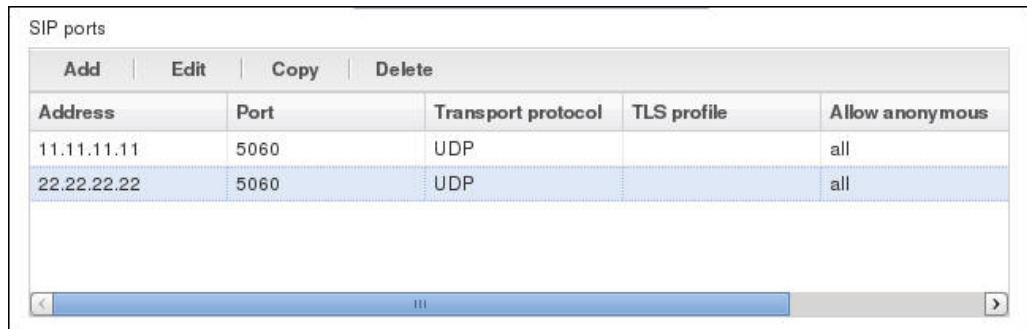
### Configuration Tab

Adds the **Delete all**, **Upload**, and **Download** buttons to the tool bar of all top-level, multi-instance configuration objects. A top-level, multi-instance object is one that includes sub-objects and allows multiple iterations of the configuration. For example, you can configure more than one SIP Interface (top-level object) with more than one SIP Port (sub-object). In contrast, you can configure only one web server with no sub-objects. The SIP Interface page displays the list of configured instances and the additional buttons, but the Web Server Config page does not. The following illustration shows the SIP Interface configuration object with multiple instances and the available buttons.



SIP interface						
Search Criteria: All						
Add	Edit	Copy	Delete	Delete All	Upload	Download
State	Realm ID	Desc				
enabled	DefaultENT					
enabled	DefaultSP					

A sub-object, for example SIP Ports, does not display the **Delete all**, **Upload**, and **Download** buttons. The buttons displayed in the sub-object affect only the items in the sub-object list, and only one list item at a time. For example, when you delete address 22.22.22.22, address 11.11.11.11 remains.



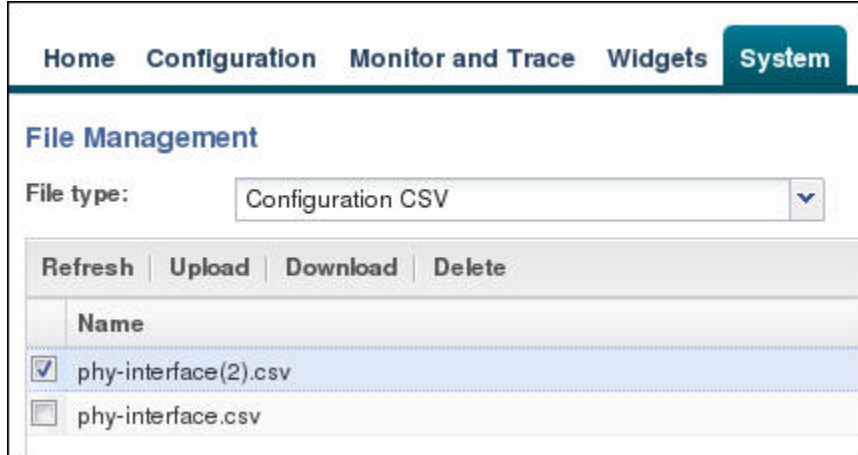
SIP ports				
Add	Edit	Copy	Delete	
Address	Port	Transport protocol	TLS profile	Allow anonymous
11.11.11.11	5060	UDP		all
22.22.22.22	5060	UDP		all

**Delete all** removes all instances in the top-level object along with the corresponding sub-objects. For example, when you click **Delete all** in the preceding SIP Interface illustration, the system deletes DefaultENT and DefaultSP along with all of the SIP Ports associated with both configurations.

Use **Upload** and **Download** to upload and download Comma Separated Values (.csv) files. For example, you might upload a .csv file that contains users, dial plans, and routes or you might download the physical interface configuration as a .csv file to store offline.

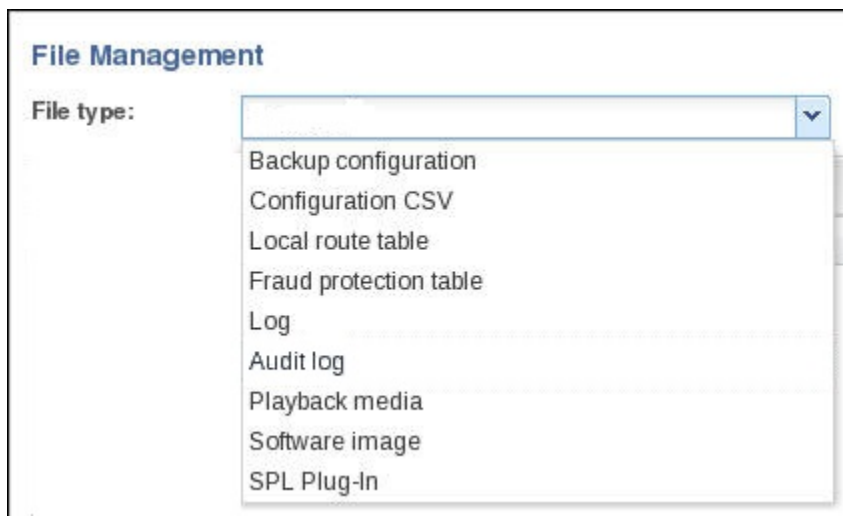
### System Tab

Adds the **Refresh**, **Upload**, **Download**, and **Delete** buttons to the File Management tool bar.



Adds the following file types to the File Type list for File Management:

- Configuration CSV
- Audit log



## Inherited Features

The following features inherited from other releases apply to the E-CZ7.3.0M2 release.

### Link Redundancy

Link redundancy enables the Oracle Enterprise Session Border Controller to run a pair of media interfaces redundantly so that in the event of a network or link failure, the Oracle Enterprise Session Border Controller automatically fails over to the redundant physical link. The Oracle



Enterprise Session Border Controller polls link state on a one-second basis, so the maximum outage time is one second. And if gateway heartbeats are enabled, then gateway timeout alarms will also cause failovers.

This feature is only supported on the Acme Packet 3820 and 4500 on the following NIUs:

- 4-port 10/100/1000 copper
- 4-port 1Gig SFP
- 4-port 1Gig SFP phy card with QoS

The link redundancy feature enables each slot pair (SxP1 and SxP2) on an NIU to behave as only a single port with one port as an active port and the other port as the hot standby simultaneously. Port 0 on Slots 0 and 1 is the master port, and the two Port 1s are the backup ports. The NIU receives and sends all traffic on one port, while the other acts as a standby in the event of failure. When enabled, this feature takes effect system-wide.

Link redundancy is configured by setting the **link-redundancy-state** parameter to **enabled** in **system-config**. To perform a manual switchover from one port to its redundant port, execute the **switchover-redundancy-link** command.

The criteria for port switchover are:

- Link down event on active port
- ARP timeout to the gateway configured on the media interface
- Administratively-forced switchover

Please note the following:

- Physical interface configuration for the standby port must not exist. The network interface for the first port (port 0) should only be configured, and it becomes the preferred active port.
- A critical level ALARM will be issued during operation if both the active and standby ports experience LINK down state.
- Link redundancy is non-revertive; after switching over to the standby, if the formerly-active port recovers link, the Oracle Enterprise Session Border Controller does not switch back.

### Link Redundancy and High Availability Interaction

The Link redundancy feature is a layer 2 feature which handles lower layer physical failure conditions automatically; the failure of one link does not cause health score decrements that result in a system-to-system switchover. However, in the event that both the active and standby ports fail on a single slot, the Oracle Enterprise Session Border Controllers will decrement its health score so that an active-to-standby HA switchover occurs.

The high availability (HA) feature can be considered an application layer feature which depends upon numerous critical conditions including lower layer alarm status (such as double physical link failure) to update the system's health score and determine whether to switchover. HA and LR are independent features, but they can be simultaneously configured to support extensive failover protection. You may treat them as two layers of redundancy protection. One for physical layer switchover on each slot on SBC (LR) and another (HA) as global "system" layer switchover capability.

## Caveats

- Be aware that DoS protection and QoS metrics are not compatible with this feature. However, hostpath DoS protection is still available when you enable phy link redundancy.
- Link redundancy statistics are not mirrored between active and standby nodes in an HA pair.

## Phy Link Redundancy Configuration

This section shows you how to enable phy link redundancy, how to force a switchover, and how to view information about the redundancy links.

Only configure port 0, the redundant port 1 is automatically configured.

1. Access the **system-config** configuration element.

```
ORACLE# configure terminal
ORACLE(configure)# system
ORACLE(system)# system-config
ORACLE(system-config)#
```

2. Type **select** to begin editing the **system-config** object.

```
ORACLE(system-config)# select
ACMEPACKET(system-config)#
```

3. **link-redundancy-state**—Set this parameter to **enabled** if you want to use phy link redundancy for your system with two two-port GigE cards installed. A value of **disabled** turns this feature off. The default is **disabled**. The valid values are:

- enabled | disabled

4. Type **done** to save your configuration.

To view link redundancy state, in Superuser mode, execute the **show redundancy link** command.

```
console# show redundancy link
Active port on Slot 0 is port: 1
Slot 0 Switchover Events: 1
Active port on Slot 1 is port: 0
Slot 1 Switchover Events: 0
```

To force a switchover, in Superuser mode, execute the **switchover-redundancy-link** and a Space and the slot number (0 or 1). This change the roles of the active and the standby ports on the slot you specify. If the command is successful, then no further information will be displayed.

```
ORACLE# switchover-redundancy-link 0
```

The system allows you to switch links only if the newly active link is up. If it is not, then the system displays information that tells you why the operation could not be completed:

```
Switch From Slot 1 Port 1, to Port 0 was not completed
Due to the fact Link State for Slot 1 Port 0 is down
```

## Deprecated Features and Functions

The following deprecated features and functions apply to the E-CZ7.3.0M2 release.

Topic	Deprecation
Configuration	The call-recording-server-id configuration element is deprecated.

## Known Issues

The following known issues apply to the E-CZ7.3.0M2 release.

ID	Description	Found In	Fixed In
26756453	It is possible to configure a <b>ldap-config &gt; name</b> longer than 24 characters. However, it cannot be assigned as next-hop in the local policy.	ECZ7.3.0 MR-1 Patch 1	
25381270	Can not create more that 285 media interfaces as VLANs.		
23575246	The Media Playback SPL Feature is not working for hairpinned calls.	nnECZ730m1p1	ECZ730m2p17
25603258	TACACS not working when system-access-list > protocol is set to 6/49	ECZ7.3.0 MR-2	ECz730m2p17
27017062	Configured LRT tables will not forward IWF (SIP to H.323) calls.	nnECZ730m2p7	ECz730m2p17
25337203	Some information is omitted from the show running-config command when connected to the management port via Telnet using TeraTerm.	SCZ720m6p8	ECz730m2p17
23706151	Wrong health score is reported in the switchover log portion of the show health command under some conditions. The Redundancy Protocol Process section of the show health command reports the correct health score.	nnSCZ720m6p5	
26281432	One-way audio in SRTP termination scenario after session refresh from the RTP side.	nnECZ740p3	ECz730m2p17
26877552	C-line in SDP refresh has an incorrect IP Address.	Ecz740M1	ECz730m2p17

---

<b>ID</b>	<b>Description</b>	<b>Found In</b>	<b>Fixed In</b>
25799838	When the SBC starts, the SPL file requires extra time to load resulting in graceful fail-over and system restart. This does not occur in later ESBC releases. This behavior occurs sporadically and only on system start-up.	ECZ730m2p17	

---

## Limitations

The following limitations apply to the E-CZ7.3.0M2 release.

---

<b>Topic</b>	<b>Limitation</b>
Expired Password	The Web GUI does not support changing a user password. Use the <code>#secret enable</code> command from the ACLI.
TACACS	The Admin Security License does not support TACACS.


---

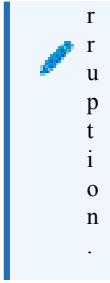
## Caveats

The following caveats apply to the E-CZ7.3.0M2 release.

Issue	Affected Oracle Enterprise Session Border Controller (E-SBC )	Workaround
<p>When upgrading the software, intermittent DSP boot failures occur on some DSP slots. The system displays a DSP failure message such as:</p> <pre>CRITICAL ALARM - DSP#1 Boot Failure!</pre> <p>writing stats to file/opt/logs/ dump.xcode-boot</p> <p>Alternatively, you can use the</p> <pre>show xcode xlist</pre> <p>command to check DSP status.</p> <p>Failure example</p> <pre>TCM DSPs#Sess Load State === ===== 00 2 0 0% 2 Active 01 2 0 0% 2 Active 02 2 0 0% 2 Active 03 2 0 0% 2 Active 04 2 0 0% 2 Active 05 2 0 0% Boot Failure--&gt; failed to load state</pre> <p>When upgrading the software, the standby member of a High Availability (HA) pair goes Out-of-Service and does not sync.</p>	<p>Affects the Acme Packet 4500 and Acme Packet 3820 with DSPs, when upgrading from either the E-CZ7.2.0x or the E-CZ7.3.0m1x releases.</p> <p>Affects the standby member of an HA pair on the Acme Packet 4500 and the Acme Packet 3820 with DSPs, when upgrading from the E-CZ7.2.0x and E-CZ7.3.xx releases.</p>	<p>When the system displays a DSP Failure Message while re-starting, perform a re-start. All of the DSPs will come up, as expected. To confirm that the DSPs are operational, use the</p> <pre>show xcode xlist</pre> <p>command.</p> <p>Success example</p> <pre>TCM DSPs#Sess Load State === ===== 00 2 0 0% 2 Active --&gt; successful 01 2 0 0% 2 Active load state 02 2 0 0% 2 Active 03 2 0 0% 2 Active 04 2 0 0% 2 Active</pre> <p>Change the "becoming-standby-time" value under "redundancy-config" to "360000" before upgrading. You can restore the previous setting after upgrading.</p>

Issue	Affected Oracle Enterprise Session Border Controller (E-SBC )	Workaround
When forcing a switchover, the standby member of a High Availability (HA) pair successfully becomes the active member, but the former active member re-starts before becoming the standby member.	Affects the Acme Packet 4500 and the Acme Packet 3820 with DSPs and LDAP config, when you issue the "notify berpd force" command on either the active member or the standby member of the HA pair.	If you find it necessary to avoid the re-start situation, delete the LDAP configuration and any local policy that references LDAP.

 Note: There is a re-start does not cause session revive incident

Issue	Affected Oracle Enterprise Session Border Controller (E-SBC )	Workaround
 <p data-bbox="446 653 727 821">With SIPREC enabled for all sessions, the E-SBC supports no more than 4,000 sessions with infinite media hold time for the G711 codec.</p>	<p data-bbox="743 653 1122 705">Affects the Acme Packet 4500 with the ETC2.</p>	<p data-bbox="1179 653 1328 680">Not Applicable</p>
<p data-bbox="446 831 727 1001">This release does not support SDM, which affects SDM functionality and the new "Secure the ACP Communications Link with TLS" feature.</p>	<p data-bbox="743 831 1057 858">Affects all Acme Packet ESBCs.</p>	<p data-bbox="1179 831 1328 858">Not Applicable</p>

## Closed Caveats

The following closed caveats apply to the E-CZ7.3.0M2 release.

Topic	Closed Caveat
<p data-bbox="446 1255 683 1283">KPML and Transcoding</p>	<p data-bbox="959 1255 1458 1339">The E-SBC supports KPML with transcoding enabled in the same realm, including when calls are not being transcoded.</p>
<p data-bbox="446 1350 781 1377">KPML to RFC 2833 Interworking</p>	<p data-bbox="959 1350 1360 1402">The E-SBC supports KPML to RFC 2833 Interworking.</p>