

Oracle® Enterprise Session Border Controller

Release Notes



Release E-CZ7.5.0

F19883-01

November 2019

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

ORACLE®

Oracle Enterprise Session Border Controller Release Notes, Release E-CZ7.5.0

F19883-01

Copyright © 2014, 2019, 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	Introduction to E-CZ7.5.0	
	Supported Platforms and Components	1-1
	Virtual Machine Platform Resources	1-3
	Image Files and Boot Files	1-3
	Platform Boot Loaders	1-4
	Upgrade Information	1-5
	Patches Included in This Release	1-5
	CPU Support for the Acme Packet 4500	1-5
	NIU and Feature Group Requirements	1-6
	QoS NIU Version Requirement for Acme Packet 4500	1-7
	System Capacities	1-7
	Transcoding Support	1-8
	Co-Product Support	1-9
	Supported SPL Engines	1-9
	Deprecated Features	1-10
	E-SBC 7.x Features Not Available in SBC 7.x Releases	1-11
2	New Features	
	FIPS 140-2 and JITC Compliance	2-1
	Security	2-1
	Transcoding	2-1
	RTCP	2-2
	Session Recording	2-2
	VNF for the E-SBC	2-2
	SPLs	2-2
3	Caveats, Known Issues, and Limitations	
	Caveats	3-1

Known Issues
Limitations

3-3
3-6

About This Guide

The *Release Notes* describe new features, enhancements, supported platforms, upgrade paths, limitations, known issues, resolved issues, and caveats for the Oracle® Enterprise Session Border Controller (E-SBC).

Documentation Set

The E-CZ7.5.0 documentation set differs from previous releases with the addition of separate guides for installation, call traffic monitoring, and header manipulation rules. The content for the new guides was previously located in the *ACLI Configuration Guide*, which no longer contains such information. The documentation set also includes new guides for Federal Information Processing Standard (FIPS) compliance and the Admin Security licenses.

The following table describes the documents included in the E-SBC E-CZ7.5.0 documentation set.

Document Name	Document Description
ACLI Configuration Guide	Contains conceptual and procedural information for configuring, administering, and troubleshooting the E-SBC.
Administrative Security Guide	Contains conceptual and procedural information for supporting the Admin Security license, the Admin Security ACP license, and JITC on the E-SBC.
Call Traffic Monitoring Guide	Contains conceptual and procedural information for configuration using the tools and protocols required to manage call traffic on the E-SBC.
FIPS Compliance Guide	Contains conceptual and procedural information about FIPS compliance on the E-SBC.
HMR Guide	Contains conceptual and procedural information for header manipulation. Includes rules, use cases, configuration, import, export, and examples.
Installation and Platform Preparation Guide	Contains conceptual and procedural information for system provisioning, software installations, and upgrades.
Release Notes	Contains information about the E-Cz7.5.0 release, including platform support, new features, caveats, known issues, and limitations.
Web GUI User Guide	Contains conceptual and procedural information for using the tools and features of the E-SBC Web GUI.

Related Documentation

The following table lists other documentation related to using the E-SBC. You can find the listed documents on <http://docs.oracle.com/en/industries/communications/> in the "Session Border Controller Documentation" and "Acme Packet" libraries.

Document Name	Document Description
Accounting Guide	Contains information about the E-SBC accounting support, including details about RADIUS accounting.
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Acme Packet 1100 Hardware Installation Guide	Contains information about the hardware components and features of the Acme Packet 1100, as well as conceptual and procedural information for installation, start-up, operation, and maintenance.
Acme Packet 3900 Hardware Installation Guide	Contains information about the hardware components and features of the Acme Packet 3900, as well as conceptual and procedural information for installation, start-up, operation, and maintenance.
Acme Packet 4500 Hardware Installation Guide	Contains information about the hardware components and features of the Acme Packet 4500, as well as conceptual and procedural information for installation, start-up, operation, and maintenance.
Acme Packet 4600 Hardware Installation Guide	Contains information about the hardware components and features of the Acme Packet 4600, as well as conceptual and procedural information for installation, start-up, operation, and maintenance.
Acme Packet 6300 Hardware Installation Guide	Contains information about the hardware components and features of the Acme Packet 6300, as well as conceptual and procedural information for installation, start-up, operation, and maintenance.
HDR Resource Guide	Contains information about the E-SBC Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Maintenance and Troubleshooting Guide	Contains information about E-SBC logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
MIB Reference Guide	Contains information about Management Information Base (MIBs), Acme Packet's enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Security Guide	Contains information about security considerations and best practices from a network and application security perspective for the E-SBC family of products.

Revision History

The following table describes the history of updates to this guide.

Date	Description
August 2017	Initial release
September 2017	<ul style="list-style-type: none"> • Adds a limitation regarding the packet-trace remote command. • Updates the "Fixed In" column in the "Known Issues" topic for items fixed in ECZ750p1.
October 2017	<ul style="list-style-type: none"> • Adds qualified VNF interface firmware revisions, based on DPDK version • Adds the following Caveat <ul style="list-style-type: none"> – Interface Utilization Support
January 2018	<ul style="list-style-type: none"> • Correctly refers users to the <i>Administrative Security Guide</i> for information on the JITC feature.
March 2018	<ul style="list-style-type: none"> • Adds the Comm Monitor Caveat.
May 2018	<ul style="list-style-type: none"> • Clarifies the media hairpinning Caveat.
June 2018	<ul style="list-style-type: none"> • Adds the High Availability Configuration Caveat. • Removes H323 and SIP/H323 IWF support as VNF caveat • Adds Pooled Transcoding Caveat. • Adds Pooled Transcoding Known Issue. • Adds the Acme Packet 3900 to "Upgrade Caveats" for software TLS licensing.
July 2018	<ul style="list-style-type: none"> • Updates the "Upgrade Information" topic about dual rebooting the Acme Packet 3900 in certain circumstances.
December 2018	<ul style="list-style-type: none"> • Adds "Ciphers" to the "Deprecated Features" table.
May 2019	<ul style="list-style-type: none"> • Updates Transcoding caveats with Local Media Playback incompatibility.
November 2019	<ul style="list-style-type: none"> • Adds trace tool limitations to "Trace Tools" caveats.

1

Introduction to E-CZ7.5.0

The Oracle® Enterprise Session Border Controller *Release Notes* provides the following information about E-CZ7.5.0 release:

- Specifications of supported platforms, virtual machine resources, and hardware requirements
- Overviews of the new features and enhancements
- Summaries of known issues, caveats, limitations, and behavioral changes
- Details about upgrades and patch equivalency
- Notes about documentation changes, behavioral changes, and interface changes

Supported Platforms and Components

The following platforms support the Oracle® Enterprise Session Border Controller (E-SBC).

Acme Packet Engineered Hardware

- Acme Packet 1100
- Acme Packet 3900
- Acme Packet 4500
- Acme Packet 4600
- Acme Packet 6300

Oracle qualified the following components for deploying version E-CZ7.5.0 as a Virtual Network Function.

Qualified Hypervisors

- XEN 4.4: Specifically using Oracle Virtual Machine (OVM) 3.4.2
- KVM: Using version embedded in Oracle Linux 7 with RHCK.
Note the use of the following KVM component versions:
 - Compiled against library: libvirt 2.0.0
 - Using library: libvirt 2.0.0
 - Using API: QEMU 2.0.0
 - Running hypervisor: QEMU 1.5.3
- VMware: Using ESXI 6.0 u2 on VMware vCenter Server

Qualified hardware platforms for hypervisors:

- Netra X5-2
- Oracle X5-2

Qualified interface chipsets

- Intel x540/82599
- Intel i350
- Intel X710 / XL710

Firmware version information from dpdk.org is also presented, based on the DPDK version used in this release.

Intel x540/82599

- (Intel(R) Ethernet Controller X540-AT2)
- Firmware version: 0x80000389
- Device id (pf): 8086:1528
- Driver version: 3.23.2 (ixgbe)
- Intel(R) 82599ES 10 Gigabit Ethernet Controller
- Firmware version: 0x61bf0001
- Device id (pf/vf): 8086:10fb / 8086:10ed
- Driver version: 4.0.1-k (ixgbe)

Intel i350 (On Acme Packet 1100 and Acme Packet 3900 platforms:

- Intel(R) Corporation I350 Gigabit Network Connection
- Firmware version: 1.48, 0x800006e7
- Device id (pf/vf): 8086:1521 / 8086:1520
- Driver version: 5.2.13-k (igb)

Intel X710 / XL710

- Intel(R) Ethernet Converged Network Adapter X710-DA4 (4x10G)
- Firmware version: 5.05
- Device id (pf/vf): 8086:1572 / 8086:154c
- Driver version: 1.5.23 (i40e)
- Intel(R) Ethernet Converged Network Adapter X710-DA2 (2x10G)
- Firmware version: 5.05
- Device id (pf/vf): 8086:1572 / 8086:154c
- Driver version: 1.5.23 (i40e)

Qualified interface input-output modes

- PV (VIF on XEN)
- SR-IOV
- PCI Passthrough

Virtual Machine Platform Resources

A Virtual Network Function (VNF) requires the CPU core, memory, disk size, and network interfaces specified for operation. The Oracle® Enterprise Session Border Controller (E-SBC) uses the Data Plane Development Kit (DPDK) for datapath design, which imposes specific VNF resource requirements for CPU cores. Deployment details, such as the use of distributed DoS protection, specify resource utilization beyond the defaults.

You configure CPU core utilization from the ACLI based on your deployment. You can also define memory and hard disk utilization based on your deployment. You must configure the hypervisor with the appropriate settings prior to startup, if you need settings other than the machine defaults set by the machine template (OVA).

Default VM Resources

VM resource configuration defaults to the following:

- 4 CPU Cores - specific to deployment
- 8 GB RAM
- 40 GB hard disk (pre-formatted)
- 8 interfaces as follows:
 - 1 for management (wancom0)
 - 2 for HA (wancom1 and 2)
 - 1 spare
 - 4 for media

Interface Host Mode

The E-SBC E-CZ7.5.0 VNF supports interface architectures using Hardware Virtualization Mode - Paravirtualized (HVM-PV):

- ESXi - No manual configuration required.
- KVM - HVM mode is enabled by default. Specifying PV as the interface type results in HVM plus PV.
- XEN (OVM) - The user must configure HVM+PV mode.

CPU Core Resources

The E-SBC E-CZ7.5.0 VNF requires an Intel Core2 processor or higher, or a fully emulated equivalent including 64-bit SSSE3 and TSC support.

If the hypervisor uses CPU emulation (qemu etc), Oracle recommends that you set the deployment to pass the full set of host CPU features to the VM.

Image Files and Boot Files

For Engineered Hardware

Use the following files for new installations and upgrades on Acme Packet platforms.

- Image file: `nnECZ750.bz`.
- Bootloader file: `nnECZ750.boot`.

For Virtual Machines

The E-SBC E-CZ7.5.0 version includes distributions suited for deployment over hypervisors. Download packages contain virtual machine templates for a range of virtual architectures. Use the following distributions to deploy the E-SBC as a virtual machine:

- `nnECZ750-img-vm_ovm.ova`—Open Virtualization Archive (.ova) distribution of the E-SBC VNF for Oracle (XEN) virtual machines.
- `nnECZ750-img-vm_kvm.tgz`—Compressed image file including E-SBC VNF for KVM virtual machines.
- `nnECZ750-img-vm_vmware.ova`—Open Virtualization Archive (.ova) distribution of the E-SBC VNF for ESXi virtual machines.

The Oracle (XEN) Virtual Machine, KVM, and ESXi packages include:

- Product software—Bootable image of the product allowing startup and operation as a virtual machine. This disk image is in either the `vmdk` or `qcow2` format.
- `usbc.ovf`—XML descriptor information containing metadata for the overall package, including identification, and default virtual machine resource requirements. The `.ovf` file format is specific to the supported hypervisor.
- `legal.txt`—Licensing information, including the Oracle End-User license agreement (EULA) terms covering the use of this software, and third-party license notifications.

Platform Boot Loaders

Oracle® Enterprise Session Border Controller (E-SBC) platforms require a boot loader to load the operating system and application software. New software releases include the corresponding boot loader, which the E-SBC launches during application installation. Note that software upgrades do not update the boot loader. You must manually set the compatibility. For example, suppose you want to install the software image with the filename `nnECZ750.bz`. Use the corresponding boot loader file named `nnECZ750.boot`. From the command line, use the **show version boot** command to view the boot loader version. You must install the boot loader file as `/boot/bootloader` on the target system.

Stage 1 and Stage 2 Boot Loaders

The Acme Packet 4500 uses the Stage 1 and Stage 2 boot loaders, which must be dated July 3, 2013 (MOS patch #1815632) or later. Network booting for release 7.x by way of FTP and TFTP on the Acme Packet 4500 requires the November 2013 or later boot loader.

Stage 3 Boot Loader

Every new software release contains a system software image and the Stage 3 boot loader. All platforms require the Stage 3 boot loader, and the Stage 3 boot loader is compatible with previous releases. Oracle recommends that you upgrade the Stage 3 boot loader before booting the new system image.

 **Note:**

The E-SBC does not support uploading the boot loader by way of the Web GUI.

Upgrade Information

Oracle recommends that you review the following information before upgrading to the E-Cz7.5.0 release.

Upgrade Paths

You can upgrade directly to E-CZ.5.0, with the exceptions noted for the Acme Packet 1100, Acme Packet 3900, and VME platforms.

- E-C[xz]6.4.0 to E-CZ7.5.0
- E-CZ7.x to E-CZ7.5.0

Upgrade the Acme Packet 1100 and VME Platforms

The software TLS and software SRTP features no longer require license keys. The change affects the upgrade process for the Acme Packet 1100 platform and the Virtual Machine Edition (VME) platform. After you upgrade either platform from E-Cz7.3.0 to E-Cz7.5.0, you must run the `setup product` command to re-activate the features that formerly depended on license keys.

Upgrade from the Acme Packet 3820 hardware to the Acme Packet 3900 Hardware

Oracle supports only an offline upgrade, when upgrading from the Acme Packet 3820 to the Acme Packet 3900.

Upgrade the Acme Packet 3900 Software

Upgrade from E-CZ7.4.0GA to E-CZ7.4.0p3—The system requires a dual reboot on the initial upgrade to E-CZ7.5.0.

Upgrade from E-CZ7.4.0m1 to E-CZ7.5.0—In-service upgrade is supported. Use the E-CZ7.5.0 boot loader. If you performed the dual reboot when you upgraded to E-CZ7.4.0m1, you do not need to perform the dual reboot after upgrading to E-CZ7.5.0. It is required only once during the first upgrade to a release after E-CZ7.4.0p3.

Patches Included in This Release

The following list shows the software patches merged into the E-CZ7.5.0 release.

E-CZ730m2p11

E-CZ740M1

CPU Support for the Acme Packet 4500

The following requirements for CPU support apply to the Acme Packet 4500.

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

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). In the tables, the ✓ character indicates the feature set that requires the supported NIU.

Table 1-1 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 1-2 Acme Packet 3900 NIU and Feature Group Support Matrix

NIU	IPSec	SRTP	QoS	Transcoding	ISDN PRI
4x1Gig	✗	✓	✓	✓ (requires transcoding module)	✗
Quad-Span TDM interface	Not applicable	Not applicable	Not applicable	Not applicable	✓

Table 1-3 Acme Packet 4500 NIU and Feature Group Support Matrix

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

Table 1-4 Acme Packet 4600 NIU and Feature Group Support Matrix

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

Table 1-5 Acme Packet 6300 NIU and Feature Group Support Matrix

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

Table 1-6 Virtual Machine and Feature Group Support Matrix

	IPSec	SRTP	QoS	Transcoding
Virtual Machine	✗	✓	✓	✓ (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 4500

A Network Interface Unit (NIU) that supports the Quality of Service (QoS) feature group on the Acme Packet 4500, except the two Enhanced Traffic Control (ETC) cards, requires QoS Field Programmable Gate Array (FPGA) revision 2.22 or higher for the E-CZ7.5.0. The *Acme Packet 4500/3820 V2.22 QOS FPGA Upgrade 24369382* image is available at My Oracle Support, <https://support.oracle.com/>, with a customer account.

System Capacities

System capacities vary across the range of Oracle® Enterprise Session Border Controller (E-SBC) platforms. You can query the system for the capacities of a particular platform by executing the **show platform limit** command.

Transcoding Support

The Oracle® Enterprise Session Border Controller supports different sets of codecs and transcoding functions depending upon the platform on which it runs. Virtual platforms, the Acme Packet 1100, and the Acme Packet 3900 support one set of codecs. The Acme Packet 4500 adds a second set of codecs with transcoding hardware. The Acme Packet 4600 and Acme Packet 6300 add a third set of codecs with transcoding hardware. VNF platforms support transcoding when you configure one or more transcoding cores.

The pooled transcoding feature on the VNF uses an external transcoding Session Border Controller (SBC), as defined in "Co-Product Support," for supported Oracle Communications SBCs for the Transcoding-SBC (T-SBC) role.

Table 1-7 E-CZ7.5.0 Supported Codecs Per Platform

Platform	Supported Codecs (by way of valid codec-policy > add-on-egress parameter)
Virtual Platforms (with transcoding core)	<ul style="list-style-type: none"> • PCMU • PCMA • G729 • G729A
Acme Packet 1100, Acme Packet 3900, Acme Packet 4500 add:	<ul style="list-style-type: none"> • G711FB • G726 • G726-16 • G726-24 • G726-32 • G726-40 • G723 • G722 • GSM • AMR • AMR-WB • iLBC • T.38 • CN • Telephone-event
Acme Packet 4600 and Acme Packet 6300 add:	<ul style="list-style-type: none"> • EVRC0 • EVRC • EVRC1 • EVRCB0 • EVRCB • EVRCB1 • T.38OFD • Opus • SILK

Co-Product Support

The following products and features run in concert with the Oracle® Enterprise Session Border Controller (E-SBC).

Pooled Transcoding

The E-SBC supports pooled transcoding to conserve resources. Pooled transcoding requires an Access-Session Border Controller (A-SBC) that uses transcoding resources provided by at least one Transcoding-Session Border Controller (T-SBC). When the A-SBC uses the E-CZ7.5.0 software, you can use the following hardware with E-CZ7.5.0 as a T-SBC in a pooled transcoding scenario:

- Acme Packet 4500
- Acme Packet 4600
- Acme Packet 6300

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
- C3.1.7
- C3.1.8
- C3.1.9

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

Deprecated Features

Oracle recommends that you review the following deprecated features before using the E-CZ7.5.0 release.

Feature	Description	First Deprecated
Telnet	<p>Telnet is not supported. Use SSH for network access to E-SBC management.</p> <p>Note that references to Telnet and FTP are still present in the E-CZ7.5.0 documentation set because those terms are still used in the ACLI.</p> <p>For example, the telnet-timeout parameter persists in the guide because it persists in system-config where the parameter now specifies the SSH timeout.</p>	ECZ7.5.0
Ciphers	<p>The system deprecates the following ciphers, adhering to recent OpenSSL changes intended to eliminate weak ciphers:</p> <ul style="list-style-type: none"> • All DES-CBC ciphers, including: <ul style="list-style-type: none"> – TLS_DHE_RSA_WITH_DES_CBC_SHA – TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA <p>The user should remove any prior system version configuration that used these ciphers, and not configure a security profile with the expectation that these ciphers are available. Note also that TLS profiles using the ALL (default) value to the cipher-list parameter no longer use these ciphers.</p>	

Note:

Your version of the ACLI may still print these ciphers when you run **cipher-list ?**. Despite printing them in ACLI output, the system does not support them within service operations.

E-SBC 7.x Features Not Available in SBC 7.x Releases

The Oracle® Enterprise Session Border Controller (E-SBC) 7.x releases support certain features that the Oracle® Communications Session Border Controller (SBC) 7.x releases do not support.

The following list identifies the features that are unique to the E-SBC 7.x releases.

- Support for Acme Packet 1100 and 3900 platforms
- LDAP support (Active Directory based call routing)
- Secure access for SDM over TLS
- Dual Network Address Translation (NAT)
- Telephony fraud prevention
- Microsoft Lync & Skype for Business certification
- Enterprise SPL plug-ins
 - SIPREC Extension Data SPL
 - Local Media Playback SPL
 - Configuration Import and Export SPL
 - Lync Emergency Call SPL
 - Universal Call Identifier SPL
 - Comfort Noise Generation SPL
 - Emergency Location Identification Number Gateway SPL
 - Avaya Session Manager Redundancy SPL
- Web GUI Capabilities
 - SIP monitoring tool
 - ISBC
 - Dashboard
 - Basic and Expert configuration modes
 - Configuration wizard
- FIPS certification
- H.323 routing enhancements
- Suite B cryptography
- PKCS 12 container import and export
- Avaya enhancements
 - Personal Profile Manager (PPM) support
 - Dual registrations

2

New Features

The E-CZ7.5.0 release includes the following new features and enhancements for the Oracle® Enterprise Session Border Controller (E-SBC).

FIPS 140-2 and JITC Compliance

The E-CZ7.5.0 release includes the following support for Federal Information Processing Standards (FIPS) and Joint Interoperability Test Command (JITC) compliance.

FIPS 140-2 Compliance

The Acme Packet 1100, Acme Packet 3900, and VME support FIPS 140-2 compliance. See the *FIPS Compliance Guide*.

JITC Compliance

All Acme Packet E-SBCs support JITC compliance. See the *Administrative Security Guide*.

Security

The E-CZ7.5.0 release includes the following security enhancements.

Two-Factor Authentication

Two-factor authentication provides an extra level of security for the E-SBC by requiring users to enter a Passcode during login, in addition to their Username and Password credentials. Two-factor authentication applies to the Superuser for both local and SSH login to the ACLI, and for HTTPS login to the Web GUI. The two-factor authentication option requires the Admin Security license, and you must enable the option by setting **login-auth-method** to "two-factor" and saving the configuration. After you set "two-factor" and save the configuration, the E-SBC prompts you to set the Passcode.

4096 Key Support

The E-SBC supports 4096-bit RSA keys for SIP TLS on all Acme Packet platforms. The 4096-bit support enables you to import root certificates for SIP communications secured with TLS into the E-SBC. Use the **key-size** parameter in the certificate-record configuration to set the key size.

Transcoding

The E-CZ7.5.0 release includes the following enhancements to Transcoding.

Pooled Transcoding

In the pooled transcoding model, the Access E-SBC (A-SBC) sits between realms or between user endpoints that require transcoding between their preferred codecs. This deployment model

conserves resources on both the A-SBC and the Transcoding E-SBC (T-SBC). While the A-SBC serves as the access function with encryption support, the T-SBC supports on-demand transcoding in a tunneling gateway configuration to meet high-density transcoding requirements with greater efficiency.

Comfort Noise Transcoding

The E-SBC supports transcoding the Comfort Noise (CN) codec into in-band RTP packets when you add CN on egress, resulting in low-level noise during periods of silence.

Secure Dual-tone Multi-frequency (DTMF) Suppression

For security and privacy reasons, you can remove all DTMF sensitive information that the E-SBC processes by enabling **secure-dtmf-cancellation** within the codec-policy. In contrast to standard DTMF cancellation, which leaves some residual signal energy at the beginning and ending of each DTMF digit, **secure-dtmf-cancellation** removes all signal energy from the media stream. The result is silence.

RTCP

The E-CZ7.5.0 release includes the following RTCP enhancement.

RTCP Receiver Report Generation

When you want to make the system generate a Real-Time Transport Control Protocol (RTCP) Receiver Report separately from the default combined Sender-Receiver Report, for example to encapsulate the receiver statistics differently, you can add the **xcode-gratuitous-rtcp-report-generation** option in the media-manager configuration and the system will generate a report of receiver statistics only.

Session Recording

The E-CZ7.5.0 release includes the following session recording enhancement.

Simultaneous Session Recording Group Maximum

The maximum number of simultaneous session recording servers increases from 3 to 10.

VNF for the E-SBC

The E-CZ7.5.0 release includes the following new deployment capability.

VNF Deployment

You can deploy the E-CZ7.5.0 version of the E-SBC as a Virtual Network Function (VNF). See the *Installation and Platform Preparation Guide*.

SPLs

The E-CZ7.5.0 release includes the following change to SPL distribution.

The following SPLs were formerly distributed separately.

- Survivability

- Comfort Noise
- Header NAT

The E-CZ750 software includes these SPLs as part of the standard installation. You no longer need to get them separately.

3

Caveats, Known Issues, and Limitations

Oracle recommends that you review the following information about caveats, known issues, and limitations, before using the E-CZ7.5.0 release.

Caveats

Oracle recommends that you review the following caveats before using the E-CZ7.5.0 release.

Interface Utilization Support

The Interface Utilization: Graceful Call Control, Monitoring, and Fault Management feature is unsupported for this release.

DTMF Interworking

The system does not support RFC 2833 interworking with H.323.

The system does not support SIP-KPML to RFC2833 conversion for transcoded calls.

Fragmented Ping Support

The system does not respond to inbound fragmented ping packets.

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 workaround 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.

Media Hairpinning

The system does not support media hairpinning for hair-pin and spiral call flows for H.323-SIP calls. (The system does support hair-pinning for SIP-SIP calls.)

Physical Interface RTC Support

You must reboot the system after changing any Physical Interface configuration.

Comm Monitor

Problem: When running SIP Monitor & Trace and Comm-Monitor simultaneously, while the system is passing TLS over TCP calls on a system with high load, the ESBC may fall-over and not reboot. The issue affects all platforms.

Workaround: Run SIP Monitor & Trace or Comm-Monitor individually, not simultaneously.

Packet-trace command

- The Acme Packet 1100, Acme Packet 3900, and VNF deployments do not support the **packet-trace remote** command.
- Output from the **packet-trace local** command on hardware platforms running the E-CZ7.5.0 software version may display invalid MAC addresses for signaling packets.

Trace Tools

You may only use one of these trace tools at a time:

- **packet-trace** command
- The **communications-monitor** as an embedded probe with the Enterprise Operations Monitor
- SIP Monitor and Trace

RTCP Generation

The system does not support video flows in realms with RTCP generation enabled.

Security

The Acme Packet 4500 with an SSM card does not support the 4096-bit RSA key size. Without the SSM card, the Acme Packet 4500 supports the 4096-bit RSA key size.

SRTP Caveats

MIKEY key negotiation - not supported.

The ARIA cipher - not supported by virtual machine deployments.

Linksys SRTP - not supported.

For hold and resume SRTP calls, if the rollover counter increments, upon a subsequent hold and resume action without an SRTP rekey or SSRC change an SRTP rekey, the media portion of the call will be lost. This Caveat only applies to systems running Encryption or QoS & Encryption NIUs.

Transcoding -General

Only SIP signaling is supported with transcoding.

Codec policies can only be used with realms associated with SIP signaling.

SIPREC may not be performed on a transcoded call.

Local Media Playback feature is incompatible with any transcoding functionality.

Transcoding - T.38 Fax

Pooled Transcoding for Fax is unsupported.

The G711 leg of a fax relay call supports only 10ms, 20ms, and 30ms ptime values. The T.38 leg generates packets asynchronously at 30ms multiples.

Pooled Transcoding

The following media-related features are not supported in pooled transcoding scenarios:

- Lawful intercept
- 2833 IWF
- Fax scenarios
- RTCP generation for transcoded calls
- T.140-Baudot Relay
- OPUS/SILK codecs
- SRTP and Transcoding on the same call
- Asymmetric DPT in SRVCC call flows
- Media hairpinning
- QoS reporting for transcoded calls
- Multiple SDP answers to a single offer
- PRACK Interworking
- Asymmetric Preconditions

Virtual Network Function (VNF)

The following caveats apply to VNF deployments:

- The OVM server 3.4.2 does not support the virtual back-end required for para-virtualized (PV) networking. VIF emulated interfaces are supported but have lower performance. Consider using SR-IOV or PCI-passthru as an alternative if higher performance is required.
- Default levels for scalability and are set to ensure appropriate throttling based on platform capacity factors such as hypervisor type, number and role of CPU cores, available host memory and I/O bandwidth. In some cases, those defaults may not be appropriate and throttling may occur at lower or higher call rates than expected. Please contact Oracle Technical Support for details on how to override the default throttles, if required.
- To support HA failover, MAC anti-spoofing must be disabled for media interfaces on the host hypervisor/vSwitch/SR-IOV_PF.

Known Issues

The following table describes known issues in the E-CZ7.5.0 release. You can reference the issues by Service Request ID and learn about any workaround, when the issue occurred, and when Oracle resolved the issue. Issues from previous releases that do not appear here do not apply to this release. You can also find information about resolved issues in the Build Notes for this release.

Acme Packet 1100

ID	Description	Found In	Fixed In
26432028	Un-encrypted SRTP-SDES calls result in one-way audio. Workaround: None at this time.	E-CZ7.5.0	

Acme Packet 3900

ID	Description	Found In	Fixed In
25852256	The Acme Packet 3900 does not send 10 second Interm-QoS data to the OCOM. Workaround: None at this time.	E-CZ7.5.0	E-CZ7.5.0p1
26432028	Un-encrypted SRTP-SDES calls result in one-way audio. Workaround: None at this time.	E-CZ7.5.0	

Asterisk Behavior

ID	Description	Found in	Fixed in
25874496	The Asterisk interface on the E-SBC becomes unresponsive. Workaround: Issue a ping command to the Asterisk interface from the E-SBC command line.		E-CZ7.5.0p1

Calls from Different Realms, and Route-to-Registrar

ID	Description	Found In	Fixed In
26612880	When the caller and callee are in different realms, and Route-to-Registrar is enabled, and the caller and the callee are registered endpoints, the system cannot route the call.		E-CZ7.5.0p1

Comm Monitor

ID	Description	Found in	Fixed In
26260953	Enabling and adding Comm Monitor config for the first time can create a situation where the monitoring traffic (IPFIX packets) does not reach the Enterprise Operations Monitor. Workaround: Reboot the system.	E-CZ7.5.0	
	Problem: When running SIP Monitor & Trace and Comm-Monitor simultaneously, while the system is passing TLS over TCP calls on a system with high load, the ESBC may fall-over and not reboot. The issue affects all platforms. Workaround: Run SIP Monitor & Trace or Comm-Monitor individually, not simultaneously.	E-CZ7.5.0	E-CZ8.0.0p2

H.323

ID	Description	Found In	Fixed In
	The system stops responding when you configure an H.323 stack supporting SIP-H323-SIP calls with the max-calls parameter set to a value that is less than the q931-max-calls parameter. Workaround: For applicable environments, configure the H.323 stack max-calls parameter to a value that is greater than the q931-max-calls parameter. The system does not support HA Redundancy for H.323 calls.		

IPv6

ID	Description	Found In	Fixed In
	Media interfaces configured for IPv6 do not support multiple VLANs.		

Hairpin calls

ID	Description	Found In	Fixed In
	The system does not support SIP-H323 hairpin calls with DTMF tone indication interworking.		

LDAP Server

ID	Description	Found In	Fixed In
26136553	The E-SBC can incur a system-level service impact while performing a switchover using "notify berpd force" with an LDAP configuration pointing to an unreachable LDAP server. Workaround: Ensure that the E-SBC can reach the LDAP server before performing switchover.		

SCTP

ID	Description	Found In	Fixed In
	E-CZ7.5.0 does not support SCTP.		E-CZ7.5.0p1

SRTP

ID	Description	Found In	Fixed In
24355493 7	When the Acme Packet 4500 reaches approximately 1,600 sessions, the system begins to send 503 responses to messages over SRTP. The system to stops responding and displays a DPWD error.	E-CZ7.5.0	

System Tools

ID	Description	Found In	Fixed In
26338219	The packet-trace remote command does not work with IPv6.	S-CZ7.4.0	

Telephony Fraud Protection

ID	Description	Found in	Fixed In
25954122	Telephony fraud protection does not black list calls after a failover. Workaround: Activate the fraud protection table on the newly active server.	E-CZ7.5.0	

Transcoding

ID	Description	Found In	Fixed In
26498937	QoS is not supported for transcoded calls.	E-CZ7.3.0	E-CZ7.5.0p1

Pooled Transcoding

ID	Description	Found In	Fixed In
28062411	Calls that require SIP/PRACK interworking as invoked by the 100rel-interworking option on a SIP interface do not work in pooled transcoding architectures.	SCZ740	
28071326	Calls that require LMSD interworking as invoked by the lmsd-interworking option on a SIP interface do not work in pooled transcoding architectures. During call establishment, when sending the 200 OK back to the original caller, the cached SDP is not included.	SCZ740	

Limitations

Oracle recommends that you review the following limitations before using the E-CZ7.5.0 release.

Functional Limitations of the Virtual Network Function (VNF)

Oracle® Enterprise Session Border Controller functions not available in VNF deployments of this release:

- Native transcoding for codecs other than G.711 and G.729.
Workaround: For all other codecs, configure your environment and system for pooled transcoding.
- Inband DTMF detection
- DTMF generation
- RTCP generation for G.711 or G.729
- In-service software upgrades for KVM and OVM deployments
- IPSec functionality not available in VNF deployments of this release:
 - IKEv1

- Authentication header (AH)
- The AES-XCBC authentication algorithm
- Dynamic reconfiguration of security-associations
- Hitless HA failover of IPSec connections.