Oracle® Enterprise Session Border Controller

Release Notes

Release E-CZ8.1.0
F20165-01
December 2019

ORACLE

Oracle Enterprise Session Border Controller Release Notes, Release E-CZ8.1.0

F20165-01

Contents

5 Caveats, Limitations, and Known Issues

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 following list describes the documents included in the E-CZ8.1.0 documentation set.

ACLI Configuration Guide	Contains conceptual and procedural information for configuring, administering, and troubleshooting the E-SBC.
Administrative Security Guide	Contains conceptual and procedural information for supporting the Admin Security, Admin Security with ACP, and JITC feature sets on the E-SBC.
Call Traffic Monitoring Guide	Contains conceptual and procedural information for configuration using the tools and protocols required to manage call traffic on the E-SBC.
FIPS Compliance Guide	Contains conceptual and procedural information about FIPS compliance on the E-SBC.
HMR Guide	Contains conceptual and procedural information for header manipulation. Includes rules, use cases, configuration, import, export, and examples.
Installation and Platform Preparation Guide	Contains conceptual and procedural information for system provisioning, software installations, and upgrades.
Release Notes	Contains information about this release, including platform support, new features, caveats, known issues, and limitations.
Time Division Multiplexing Guide	Contains the concepts and procedures necessary for installing, configuring, and administering Time Division Multiplexing (TDM) on the Acme Packet 1100 and the Acme Packet 3900.
Web GUI User Guide	Contains conceptual and procedural information for using the tools and features of the E-SBC Web GUI.

Related Documentation

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

Accounting Guide	Contains information about the E-SBC accounting support, including details about RADIUS accounting.

ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Acme Packet 1100 Hardware Installation Guide	Contains information about the hardware components and features of the Acme Packet 1100, as well as conceptual and procedural information for installation, start-up, operation, and maintenance.
Acme Packet 3900 Hardware Installation Guide	Contains information about the hardware components and features of the Acme Packet 3900, as well as conceptual and procedural information for installation, start-up, operation, and maintenance.
Acme Packet 4600 Hardware Installation Guide	Contains information about the hardware components and features of the Acme Packet 4600, as well as conceptual and procedural information for installation, start-up, operation, and maintenance.
Acme Packet 6300 Hardware Installation Guide	Contains information about the hardware components and features of the Acme Packet 6300, as well as conceptual and procedural information for installation, start-up, operation, and maintenance.
HDR Resource Guide	Contains information about the E-SBC Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Installation and Platform Preparation Guide	Contains conceptual and procedural information for system provisioning, software installations, and upgrades.
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

April 2018	• Initial release
May 2018	• Removes DTMF Detection limitation on VNF. • Updates the "SIPREC Support for SRTP" item in New Features.

May 2018	• Adds Caveat stating no 'packet trace remote' on the Acme Packet 3900 • Moves 26321175 to caveats .
May 2018	• Adds the High Availability issue and workaround to Caveats.
June 2018	• Removes H.323 and SIP-H.323 IWF support as VNF Caveats. • Adds the Time Division Multiplexing bullet to the"Upgrade and Downgrade Caveats" section of the "Upgrade Information" topic. • Adds the Supported Ethernet Controller table to the "Platform Support" topic. • Adds the Pooled Transcoding Caveat. • Adds the Pooled Transcoding Known Issues.
September 2018	• Adds the Acme Packet 3900 IPSec Limitations Caveat. • Adds the Known Issue about getting IPSec support for the Acme Packet 3900 and VNF. • Adds the IPSec license display on VNF Known Issue. • Adds the Oracle accessibility statement to "About This Guide." • Moves QoS transcoded calls caveat to "Older Caveats Fixed in This Release." • Removes VNF limitation on DTMF generation. • Updates typographical error within the Known Issues table. • Updates location in full doc set of new features. • Adds the VM initial boot Known Issue.
October 2018	• TLS1.0 not supported, by default, in compatibility mode.
November 2018	• Updates the cipher list for tls-profile.
December 2018	• Updates the table in "SRTP Support for SRTP."
March 2019	• Adds "Maintain DSA-Based HDR and CDR Push Behavior" to "Upgrade and Downgrade Caveats". • Removes T.140-Baudot Relay from the list of unsupported features with Pooled Transcoding.
April 2019	• Updates Transcoding caveats with Local Media Playback incompatibility. • Adds explanation of change in HMR matching.

May 2019	• Updates the Known Issues table for accuracy.
June 2019	• Adds Daylong Transcoding Session Cleanup feature to New Features chapter. • Adds OCOM incompatibility with IPv6 to known issues.
August 2019	• Adds an MSRP Known Issue to the Known Issues table.
October 2019	• Updates "Behavioral Changes" and "Deprecated Features" to account for MIB object deprecation.
November 2019	• Adds trace tool limitations to "Trace Tools" caveats. • Adds VLAN tagging caveat to "Virtual Network Function (VNF) Caveats."
December 2019	• Updates Known Issues list

1
Introduction to E-CZ8.1.0

The Oracle® Enterprise Session Border Controller *Release Notes* provides the following information about E-CZ8.1.0 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

Platform Support

The E-CZ8.1.0 software supports the following platforms.

Acme Packet Engineered Hardware

- Acme Packet 1100
- Acme Packet 3900
- Acme Packet 4600
- Acme Packet 6300
- Acme Packet 6350

Qualified Hypervisors

Oracle qualified the following components for deploying version E-CZ8.1.0 as a Virtual Network Function.

- XEN 4.4: Specifically using Oracle Virtual Machine (OVM) 3.4.2
- KVM: Using version embedded in Oracle Linux 7 with RHCK3.10
  Note the use of the following KVM component versions:
  - QEMU
    - 2.9.0-16.el7_4.13.1 for qemu-img-ev, qemu-kvm-ev
    - 3.9.0-14.el7_5.2 for libvirt-daemon-driver-qemu
  - LIBVERT
    - 3.90-14-el7_5.2 for all components except -
    - 3.2.0-3.el7_4.1 for libvirt-python
- VMware: Using ESXI 6.5 u1 on VMware vCenter Server
- Hyper-V Windows Server 2012 R2 (Generation 1)

Supported Ethernet Controller/Driver/Input-Output Modes

The following table lists supported Ethernet Controllers (chipset families) and their supported driver. Reference the host hardware specifications where you run your hypervisor to learn the Ethernet controller in use.

Ethernet Controller	Driver	PV	SR-IOV	PCI Passthrough
Intel 82599 / X520 / X540	ixgbe	WM	M	M
Intel i210 / i350	igb	WM	M	M
Intel X710 / XL710	i40e	WM	M	M
Broadcom (Qlogic Everest)	bnx2x	WM	-	-
Broadcom BCM57417	bnxt	WM	-	-

- W - wancom interface
- M - media interface

Supported Cloud Computing Platforms

- OpenStack (including support for Heat template versions "Mitaka" and "Newton")

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 Intel 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, dictate 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
- 16 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-CZ8.1.0 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.

> **Note:**
>
> When deploying the E-SBC over VMware and using PV interface mode, the number of forwarding cores you may configure is limited to 2, 4, or 8 cores.

CPU Core Resources

The E-SBC E-CZ8.1.0 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: `nnECZ810.bz`.
- Bootloader file: `nnECZ810.boot`.

For Virtual Machines

The E-SBC E-CZ8.1.0 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:

- `nnECZ810-img-vm_ovm.ova`—Open Virtualization Archive (.ova) distribution of the E-SBC VNF for Oracle (XEN) virtual machines.
- `nnECZ810-img-vm_kvm.tgz`—Compressed image file including E-SBC VNF for KVM virtual machines.
- `nnECZ810-img-vm_vmware.ova`—Open Virtualization Archive (.ova) distribution of the E-SBC VNF for ESXi virtual machines.
- `nnECZ810-img-vm.vhd`—Virtual Hard Drive (.vhd) distribution of the E-SBC VNF for Hyper-V virtual machines.
- `nnECZ810_HOT.tar.gz`—The Heat Orchestration Templates used with OpenStack.

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.

Boot Loader Requirements

All platforms require the Stage 3 boot loader that accompanies the Oracle® Enterprise Session Border Controller image file, as distributed. Install the boot loader according to the instructions in the *Installation and Platform Preparation Guide*.

Upgrade Information

The E-CZ8.1.0 release supports the following online upgrade paths.

Upgrade Paths

Acme Packet 1100, Acme Packet 3900, Acme Packet 4600, and Acme Packet 6300 Upgrade Paths

- E-CZ7.5.0x to E-CZ8.1.0
- E-CZ8.0.0 to E-CZ8.1.0

For systems running E-CZ7.4.0GA to E-CZ7.4.0p3, you must upgrade to E-CZ7.4.0M1 and perform a dual reboot before upgrading to E-CZ.8.0. If you previously upgraded to E-CZ7.4.0m1, E-CZ7.5.0, or E-CZ8.0.0 and performed the dual reboot, you do not need to perform the dual reboot when upgrading to E-CZ8.0.0. Refer to the E-CZ7.4.0 Release Notes for information about upgrading to E-CZ7.4.0M1.

When upgrading to this release from a release older than the previous release, read all of the intermediate *Release Notes* for notification of incremental changes.

Upgrade and Downgrade Caveats

The following items provide key information about upgrading and downgrading with this software version.

License Keyed Feature Reactivation

On the Acme Packet 1100 and VNF platforms, the software TLS and software SRTP features no longer require license keys. After you upgrade either platform to E-CZ8.1.0, you must run the **setup product** command to re-activate the features that formerly depended on license keys.

Set the New FIPS Boot File Name

Typically, you change the name of the boot file to the name of the new release by editing the file name. You cannot edit the boot file name when upgrading from E-CZ7.5.0 to E-CZ8.1.0 on the Acme Packet 1100, Acme Packet 3900, and VNF. You must use the **set-boot-file** command to set the new boot file name.

Reset the rsa_ssh.key

After you upgrade from 7.x to Cz8.1.0, you must manually reset the rsa_ssh.key when the host OpenSSH client version is 7.6 or newer. Applies to all platforms.

1. Delete the old ssh_rsa.key in the /code/ssh directory in the shell environment.
2. Reboot the E-SBC, using reboot from the ACLI prompt.

Reset Local Passwords for Downgrades

Oracle increased the encryption strength for internal password storage as of the Cz8.1.0 release, which affects downgrading to a previous release because the enhanced password encryption is not compatible with earlier SBC software versions. If you change any local account passwords after upgrading to Cz8.1.0, you cannot directly downgrade to a previous release. Oracle recommends that you do not change any local account passwords after upgrading to Cz8.1.0 from a prior release, until you are sure that you will not need to downgrade. If you do not change any local account passwords after upgrading to Cz8.1.0, downgrading is not affected.

> **Caution:**
>
> If you change the local passwords after you upgrade to Cz8.1.0, and then later want to downgrade to a previous release, you must reset the local user passwords with the following procedure before you downgrade or the system will lock you out until all passwords are cleared. If you get locked out, you must contact Oracle support to clear the passwords.

Perform the following procedure on the standby SBC first, and then force a switchover. Repeat steps1-10 on the newly active SBC. During the procedure, the SBC powers down and you must be present to manually power up the SBC.

> **Caution:**
>
> Be aware that the following procedure erases all of your local user passwords, as well as, the log files and CDRs located in the /opt directory of the SBC.

1. Log on to the console of the standby SBC in Superuser mode, type `halt sysprep` on the command line, and press ENTER.
   The system displays the following warning:

   ```
   ******************************************
   WARNING: All system-specific data will be permanently
   erased and unrecoverable.

   Are you sure [y/n]
   ```

2. Type y, and press ENTER.
3. Type your Admin password, and press ENTER.
   The system erases your local passwords, log files, and CDRs and powers down.
4. Power up the standby SBC.

5. During boot up, press the space bar when prompted to stop auto-boot so that you can enter the new boot file name.
   The system displays the boot parameters.
6. For the Boot File parameter, type the boot file name for the software version to which you want to downgrade next to the existing version. For example,`nnECZ800.bz`.
7. At the system prompt, type `@`, and press ENTER.
   The standby reboots.
8. After the standby reboots, do the following:
   a. Type `acme`, and press ENTER.
   b. Type `packet`, and press ENTER.
9. Type and confirm the password that you want for the User account.
10. Type and confirm the password that you want for the Superuser account.
11. Perform a **notify berpd force** on the standby to force a switchover.
12. Repeat steps 1-10 on the newly active SBC.

Time Division Multiplexing

Do not set the **replace-uri** action when routing to a TDM interface.

Set IPSec Support for Acme Packet 3900 and VNF

IPSec is not supported on the Acme Packet 3900 and VNF in the CZ8.1.0 release. You must upgrade to CZ8.1.0p1 to get this support. After you upgrade to CZ8.1.0p1, do the following:

1. Run **setup entitlements**, again.
2. Select **advanced** to enable advanced entitlements, which then provides support for IPSEC on Acme Packet 3900 and VNF systems.

Maintain DSA-Based HDR and CDR Push Behavior

To maintain your existing DSA key-based CDR and HDR push behavior after upgrading from 7.x to E-CZ8.1.0, perform the following procedure:

1. Navigate to the **security**, **ssh-config**, **hostkey-algorithms** configuration element and manually enter the DSA keys you want to use.
2. Save and activate your configuration.
3. Execute the **reboot** command from the ACLI prompt.

Self-Provisioned Entitlements

You enable the features that you purchased from Oracle by way of self-provisioning. Using the **setup entitlements** command, you provision the feature by either entering "enabled" or by setting the number of sessions allowed.

Self-Provisioned Features

The following table lists the features that you can self-provision, and the corresponding type of enablement required.

Feature	Type
Administrative security	Enabled or Disabled
Advanced	Enabled or Disabled
SIP sessions	Number of sessions
Data integrity (FIPS)	Enabled or Disabled
Advanced Security Suite (JITC)	Enabled or Disabled
Transcode AMR-NB	Number of sessions
Transcode AMR-WB	Number of sessions
Transcode EVRC	Number of sessions
Transcode EVRC-B	Number of sessions
Transcode EVS	Number of sessions
Transcode Opus	Number of sessions
Transcode SILK	Number of sessions

Use the **show entitlements** command to see a list of provisioned features and their session capacities.

Use the **show features** command to see a list of all enabled features and the total session capacity.

System Capacities

System capacities vary across the range of platforms that support the Oracle® Enterprise Session Border Controller. To query the current system capacities for the platform you are using, execute the **show platform limit** command.

Transcoding Support

All current platforms, except Virtual Platforms, support the same list of codecs for transcoding. VNF platforms support transcoding when you configure one or more transcoding cores.

Platform	Supported Codecs (by way of codec-policy in the add-on-egress parameter)
All Acme Packet platforms	• AMR • AMR-WB • CN • EVRC0 • EVRC • EVRC1 • EVRCB0 • EVRCB • EVRCB1 • EVS • G729 • G729A • G711FB • G726 • G726-16 • G726-24 • G726-32 • G726-40 • G723 • G722 • GSM • iLBC • Opus • PCMU • PCMA • SILK • T.38 • Telephone-event • T.38OFD • TTY, except on the Acme Packet 1100
Virtual Platforms (with transcoding core)	• AMR • AMR-WB • G729 • G729A • PCMU • PCMA Note that the pooled transcoding feature on the VNF uses external transcoding E-SBC, as defined in "Co-Product Support," for supported E-SBC for the Transcoding-SBC (T-SBC) role.

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-CZ8.0.0 software, you can use the following hardware as a T-SBC in a pooled transcoding scenario:

- Acme Packet 4500 (E-CZ7.5.0, only)
- Acme Packet 4600 (E-CZ7.5.0, E-CZ8.0.0, and E-CZ8.1.0)
- Acme Packet 6300 (E-CZ7.5.0E-CZ8.0.0, and E-CZ8.1.0)

Oracle Communications Session Router

The E-SBC supports the Oracle Communications Session Router.

TLS Cipher Updates

Note the following changes to the DEFAULT cipher list.

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

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

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

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

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

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Oracle supports the following ciphers for debugging purposes only:

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

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

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

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

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

Deprecated Features

Oracle recommends that you review the following information about deprecated features and functions before using the E-CZ8.1.0 release

New Deprecations

Feature	Description	Release Deprecated
Ciphers	• TLS_DHE_RSA_WITH_DES_CBC_SHA • TLS_RSA_WITH_DES_CBC_SHA • TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA	E-CZ8.1.0
apEnvMonVoltageStatusEntry MIB object	The apEnvMonVoltageStatusEntry objects have been deprecated. Voltage monitoring is still available using the command in the ACLI.	S-Cz8.1.0m1p6

Previous Deprecations

Feature	Description	Release Deprecated
Platforms	The E-CZ8.1.0 release does not support either the Acme packet 3820 or the Acme Packet 4500.	E-CZ8.0.0
Telnet	Telnet is not supported. Use SSH for network access to E-SBC management. Note that references to Telnet and FTP are still present in the E-CZ8.1.0 documentation set because those terms are still used in the ACLI. For example, the **telnet-timeout** parameter persists in the guide because it persists in **system-config** where the parameter now specifies the SSH timeout.	E-CZ7.5.0

Documentation Changes

Note the following changes to the documentation for this release.

Entitlement and License Documentation

All of the entitlement and licensing documentation is consolidated into the "Setting Up Product-Type, Features, and Functionality" section of the *ACLI Configuration Guide*. For a list of current entitlements and license keys, see "Self-Provisioned Entitlements and License Keys" in the *Release Notes*.

SNMP and MIB Documentation

The SNMP configuration documentation that was formerly located in the *ACLI Configuration Guide* is moved into the *MIB Reference Guide*.

Local Media Playback

In the *ACLI Configuration Guide*, all of the "Local Media Playback" topics that were previously located in the "Session Plug-in Language" chapter are now located in the newly created "Local Media Playback" chapter.

Behavioral Changes

The following information documents the behavioral changes to the Oracle® Enterprise Session Border Controller (E-SBC) in this software release.

Provisioning FIPS

To downgrade to a previous release that does not support SHA-2 hashing, use the **show version boot** command to get the serial number of your E-SBC and contact Oracle Support.

In previous releases, you needed a license key to enable the FIPS feature set. As of E-CZ8.1.0, you enable the FIPS feature set by way of self-provisioned entitlements using **setup entitlements**, You must use this method when adding FIPS on a new system.

NAPTR Follow-Up Queries for A Records

The E-SBC can issue a query for either S or A records, based on the response to an E-SBC request within a NAPTR resource record. This happens if the E-SBC needs more information to reach its target FQDN. Previously, the system always issued queries for S records.

SNMPv3

With this software version, you configure SNMP traps within the context of the E-SBC's comprehensive SNMPv3 support.

The **secure-traps** value is removed from the **snmp-agent-mode** parameter, which is part of the **system-config**.

In addition, the elimination of **secure-traps** means that the following protocols are deprecated for use by SNMP:

- DES privacy protocol
- MD5 and SHA authentication protocols

To configure traps, refer to SNMP configuration information in the *MIB Reference Guide*.

TLS1.0

TLS 1.0 sessions fail to negotiate when the **tls-version** parameter is set to **compatibility**. To advertise TLS1.0 during session negotiation, navigate to the **security-config** element and set the **options** parameter to **+sslmin=tls1.0**.

```
ORACLE(security-config)# options +sslmin=tls1.0
```

HMR Regex Matching Changes

The PCRE (Perl Compatible Regular Expression) engine was updated in 8.1 and consequently the `match-value` value of `\,` is no longer valid. In previous releases, the PCRE engine used `\,` to match any character, including a NUL character. The newer PCRE engine does not support `\,`.

Separate from the PCRE, the SBC supports the non-standard `\,+` to match one or more characters, including NUL characters. If your HMR rule for 8.0 or earlier depends on `\,` (for example, `\,*`), use either the standard `.*` to match any character zero or more times, excluding NUL characters, or use `\,+` to match any character, including NUL characters, one or more times.

Voltage Monitoring

Starting in S-Cz8.1.0m1p6 and later, apEnvMonVoltageStatusValue in the ap-env-monitor.mib file is not supported. Voltage can still be monitored through the ACLI **show voltage** command.

Patch Equivalency

Patch equivalency indicates which neighboring patch releases the E-CZ8.1.0 release includes. This information assures you that when upgrading, the E-CZ8.1.0 release includes defect fixes from neighboring patch releases.

E-CZ7.5.0p5

E-CZ8.0.0p2

Supported SPL Engines

The following SPL engine versions are supported by this software:

- C2.0.0
- C2.0.1
- C2.0.2
- C2.0.9
- C2.1.0
- C2.1.1
- C2.2.0
- C2.2.1
- C2.3.2
- 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

FIPS and JITC Compliance

Oracle recommends that you review the following information about compliance with Federal Information Processing Standards (FIPS) and Joint Interoperability Certification and Assessment (JITC) before using the E-CZ8.1.0 release.

- The E-CZ8.1.0 release is FIPS and JITC compliant, but is not certified by the National Institute of Standards and Technology (NIST) and the Defense Information Systems Agency (DISA). To verify certification, go to https://csrc.nist.gov/Projects/Cryptographic-Module-Validation-Program/Validated-Modules/Search .
- FIPS and JITC certification does not include Message Session Relay Protocol (MSRP).

The E-SBC supports FIPS and JITC on the following platforms.

- Acme Packet 1100
- Acme Packet 3900
- Acme Packet 4600
- Acme Packet 6300
- VMWare

NIU and Feature Group Requirements

The following tables list the feature groups for all Oracle® Enterprise Session Border Controller (E-SBC) hardware and virtual platforms that require a specific Network Interface Unit (NIU). The left column lists the supported NIUs. The other columns represent feature sets. In the table cells, the check mark character (✓) indicates a feature set that requires the corresponding NIU listed in the left column. The x character in a table cell indicates a feature set that does not require the NIU. Some cells contain text that says, "Not applicable."

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

NIU	IPSec	SRTP	QoS	Transcoding	ISDN PRI	ISDN BRI	Analog POTS
Acme Packet 1100 Ethernet interface	✗	✓	✓	✓ (requires transcoding module)	✗	✗	✗
Acme Packet 1100 TDM interface (single port and quad port)	Not applicable	Not applicable	Not applicable	Not applicable	✓	✗	✗
Acme Packet 1100 Euro ISDN BRI interface	Not applicable	Not applicable	Not applicable	Not applicable	✗	✓	✗
Acme Packet 1100 Analog POTS 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 4600 NIU and Feature Group Support Matrix

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

Table 1-4 Acme Packet 6300 NIU and Feature Group Support Matrix

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

Table 1-5 Virtual Machine and Feature Group Support Matrix

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

OESBC Features Not Available for the OCSBC

The Oracle® Enterprise Session Border Controller (OESBC) supports certain features that the Oracle® Communications Session Border Controller (OCSBC) does not support.

The following list identifies the features that are unique to the OESBC.

- Support for the Acme Packet 1100
- LDAP support (Active Directory based call routing)
- Dual Network Address Translation (NAT)
- Telephony fraud prevention
- Microsoft Lync and 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 in OCSBC Release S-CZ8.1.0

The following information lists and describes features newly developed or enhanced for E-CZ8.1.0.

> **Note:**
>
> System session capacity and performance are subject to variations between various use cases and major software releases.

Software Transcoding

The system supports the following new codecs for software transcoding, when deployed as a Virtual Network Function VNF:

- AMR
- AMR-WB

Non-recursive DNS Query Support

By default, the Oracle® Enterprise Session Border Controller (E-SBC) requests DNS query with recursive searches. The Telecommunication Technology Committee's Standard JJ-90.31 specifies that ENUM DNS queries be performed iteratively. The E-SBC complies with this requirement when remote (server) recursive searches are disabled. You can disable recursive searches on a per **enum-config** basis.
See "Routing" in the *ACLI Configuration Guide*.

DTMF IWF for VNF

The E-SBC supports DTMF interworking when deployed as a VNF. The functionality works the same as on other platforms. See "Graceful DTMF Conversion Call Processing" in the *ACLI Configuration Guide*.

Restricting Logons to TACACS

For deployments that include TACACS authentication, the Oracle® Enterprise Session Border Controller (E-SBC) allows the user to configure a restriction that prevents users from logging into the system using mechanisms other than TACACS. The function that manages this restriction evaluates the availability of TACACS infrastructure and allows alternate login mechanisms if TACACS servers are unavailable due to either network or server issues.
See "Getting Started" in the *ACLI Configuration Guide*.

FAX Support for UEs that Do Not Support Multiple M Lines

The Oracle® Enterprise Session Border Controller (E-SBC) sometimes supports FAX transcoding scenarios using a Re-INVITE that includes two m-lines in the SDP. Some end stations, however, do not support multiple m-lines, causing the FAX setup to fail. You can configure the E-SBC to resolve this problem on a per realm basis via transcoding policy.
See "Transcoding" in the *ACLI Configuration Guide*.

Call Duration Counters

The Oracle® Enterprise Session Border Controller maintains aggregate call duration in seconds for the current period, lifetime total and the lifetime-period-maximum. These counters are maintained for each session agent, realm, SIP Interface, and globally across the system. The call duration counter can count up to a 32 bit value, after which time it rolls over.
See the *Maintenance and Troubleshooting Guide*.

Local and Remote Call Termination Counters

The E-SBC maintains counters of gracefully terminated calls for cases where the BYE is generated both locally within the system and call is terminated externally, as expected. Each case is maintained in a unique counter. These counters are maintained for each session agent, realm, SIP Interface, and globally.
See "Local and Remote Call Termination Counters" in the *Maintenance and Troubleshooting Guide*.

Common Codec Support for Transcoded SIPREC Calls

The E-SBC supports SIPREC on all transcoded call flows by capturing the same codec type from the "called" party side of the session on both legs of the call.

SIPREC Support for SRTP

With the exception noted in the following table, the E-SBC supports SIPREC on all media flows with any combination of SRTP-RTP call legs on ingress and egress for all Acme Packet platforms. The E-SBC also supports SRTP on the interface between the E-SBC and the SIPREC server.

Caller A	Caller B	SRS	Supported or Not Supported
RTP	RTP	RTP	Supported
RTP	SRTP	RTP	Supported
SRTP	RTP	RTP	Supported
SRTP	SRTP	RTP	Supported
RTP	RTP	SRTP	Supported*
RTP	SRTP	SRTP	Supported
SRTP	RTP	SRTP	Supported
SRTP	SRTP	SRTP	Supported

* Not supported in the S-CZ8.1.0 GA release. Support begins with the S-CZ8.1.0p1 release.

- The supported combinations apply to transcoded and non-transcoded calls.
- The supported combinations apply to recording and requires either the disabled mode or the enabled mode.
- The SDES profile that you use for in the media-security-policy configuration must include both the AES_CM_128_HMAC_SHA1_80 and AES_CM_128_HMAC_SHA1_32 ciphers in the crypto-list. Apply this media security policy to each realm where you want SRTP traffic.

See the *Call Traffic Monitoring Guide* and the *ACLI Configuration Guide* for complete information about SIPREC support.

Provisioning FIPS and JITC

In previous releases, you needed a license key to enable the FIPS and JITC feature sets. As of E-CZ8.1.0, you enable both FIPS and JITC feature sets by way of self-provisioned entitlements using **setup entitlements**.

Provisioning Transcode Codecs

You no longer need to use a license key to provision transcode codecs. Use the **setup entitlements** command. Provisioning means enabling one or more codec types for transcoding by setting the number of sessions allowed for each codec type that you use. A value higher than zero enables the codec for transcoding. A value of zero (0) disables the codec for transcoding. Note that the system allows you to enable only the codecs supported for the platform that you are configuring.

You can provision transcoding for the following codecs with the **setup entitlements** command:

- AMR
- AMR-WB
- EVRC
- EVRCB
- EVS
- Opus
- SILK

When you enable or disable transcoding for a codec or change the session capacity through **setup entitlements**, the system immediately recognizes and reports the action in "show sipd transcode" and "show xcode load."

Other applicable commands work as follows:

- **show entitlements**—displays all provisioned codecs and session capacities
- **show features**—displays all enabled features and total session capacity

For upgrades, the system honors the license keys for transcode codecs from previous releases.

Increased Media Playback Sessions

Beginning with the E-CZ8.1.0 release, the Acme Packet 6300 supports to up to 1,550 concurrent media playback sessions.

Note that all other platforms remain as before, supporting up to 100 concurrent media playback sessions.

SNMPv3 Support

The Oracle® Enterprise Session Border Controller supports SNMPv3 by default. To secure your SNMPv3 system, you must configure SNMP users and groups, SNMP managers, and view access to MIB trees. SNMPv3 provides the SNMP agent and SNMP Network Management System (NMS) with protocol security enhancements used to protect your system against a variety of attacks, such as increased authentication, privacy, MIB object access control and trap filtering capabilities.

See "SNMPv3" in the *MIB Reference Guide*.

SFTP Access Restrictions

In the default restricted mode, the normal user and admin user are restricted from adding, deleting, renaming, or modifying specific system files when accessing the file system with SFTP.

Import SSH Keys as Host Keys

The Oracle® Enterprise Session Border Controller supports importing externally generated SSH keys to replace the internally generated SSH host keys. Because the E-SBC derives the public key from the private key, only the externally generated private key needs to be imported. The E-SBC uses these keys when it functions as an SSH server. The E-SBC supports RSA or DSA key lengths of 1024, 2048, 3072, or 4096 bits. See "Import Private SSH Key to Derive New SSH Host Keys" in the *ACLI Configuration Guide*.

Import a Private SSH Key

As an alternative to relying on the SSH keys generated by the Oracle® Enterprise Session Border Controller, customers may import externally generated SSH keys for any configured **public-key** element. Because the E-SBC derives the public key from the private key, only the private key needs to be imported, and any previously generated keys for this **public-key** element will be overwritten. The E-SBC uses these keys when it functions as an SFTP client. See " Import a Private SSH Key for the E-SBC as an SFTP Client" in the *ACLI Configuration Guide*.

Delete an SSH Key

You can delete private keys from the system individually. See "Delete an SSH Key" in the *ACLI Configuration Guide*.

Daylong Transcoding Session Cleanup

The Oracle® Enterprise Session Border Controller can perform hourly checks for long xcode/DSP sessions. The amount of time that defines these long sessions defaults to 86400 seconds (24 hours), and may be configured to a different number. After finding these long sessions, they will be cleared from the system when the hourly process runs. Freeing up these potentially orphaned sessions ensures that maximum transcoding resources are available for incoming calls.

This feature is available in release E-Cz810m1p16 and later.

3
Configuration Element Changes

The following topics explain changes to configuration elements. The system may process some changes, while others may require you to intervene.

Attribute Name Changes for session-agent Configuration

For PCZ3.0.0, Oracle changed the names of several attributes in the session-agent configuration. Updating the schema resolves the changes, but if you try to upload a .csv file of session-agents with the previous attribute names you will see errors. To avoid errors, update the column header names in the .csv file to match the new attribute names before uploading the .csv file. Note that the order of the attributes in the configuration is different for PCZ3.0.0, but you do not need to re-order the attributes in the .csv file. The following table lists the attribute names prior to PCZ3.0.0 and the corresponding new names.

Prior to PCZ3.0.0	As of PCZ3.0.0
IP-address	ip-address
transport-protocol	transport-method
inbound-header-manipulation	in-manipulationid
outbound-header-manipulation	out-manipulationid
OPTIONS-ping-interval	ping-interval
enable-REFER-termination	refer-call-transfer
Send-NOTIFY-for-REFER-provisional-responses	refer-notify-provisional
enable-constraints	constraints
maximum-sessions	max-sessions
maximum-inbound-sessions	max-inbound-sessions
maximum-outbound-sessions	max-outbound-sessions
maximum-burst-rate	max-burst-rate
maximum-inbound-burst-rate	max-inbound-burst-rate
maximum-outbound-burst-rate	max-outbound-burst-rate
burst-rate-window-size	register-burst-window
maximum-sustain-rate	max-register-sustain-rate
maximum-inbound-sustain-rate	max-inbound-sustain-rate
maximum-outbound-sustain-rate	max-outbound-sustain-rate
sustained-rate-window-size	sustain-rate-window
SPL-options	spl-options

4

Inherited Features

Oracle merged the features available in the following releases into the E-CZ8.1.0 release.

S-CZ8.0.0

E-CZ8.0.0

5

Caveats, Limitations, and Known Issues

Oracle recommends that you review the following information about Caveats, Limitations, and Known Issues before using the E-CZ8.1.0 release. The Caveats and Limitations topics explain certain behaviors and limitations that you can expect. They do not provide workarounds. The Known Issues topic describes issues that Oracle is aware of and may address in a future release. Known Issues contain workarounds, when available.

Older Caveats Fixed in This Release

The following caveats have been fixed in ECZ8.1.0:

- QoS reporting is now supported for transcoded calls

Caveats and Limitations

The following information lists and describes the caveats and limitations for this release. Oracle updates this Release Notes document to distribute issue status changes. Check the latest revisions of this document to stay informed about these issues.

Provisioning Transcode Codec Session Capacities

When you use **setup entitlements** to set the capacity for a transcode codec, the system may or may not require a reboot.

- When a transcode codec is licensed with a license key, a capacity change requires a reboot to take effect.
- When a transcode codec is not licensed with a license key, a capacity change takes effect without a reboot.

Virtual Network Function (VNF) Caveats

The following functional caveats apply to VNF deployments of this release:

- 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 scenarios, the 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.
- When operating as a VNF deployed in an HA configuration, the OCSBC does not support IPSec.

- Virtual LAN (VLAN) tagging is not supported when deploying the OCESBC over the Hyper-V platform.

Transcoding - general

Only SIP signaling is supported with transcoding.

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

Local Media Playback feature is incompatible with any transcoding functionality.

T.38 Fax Transcoding

T.38 Fax transcoding is available for G711 only at 10ms, 20ms, 30ms ptimes.

Pooled Transcoding for Fax is unsupported.

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
- 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

DTMF Interworking

RFC 2833 interworking with H.323 is unsupported.

SIP-KPML to RFC2833 conversion is not supported for transcoded calls.

H.323 Signaling Support

If you run H.323 and SIP traffic in system, configure each protocol (SIP, H.323) in a separate realm.

Media Hairpinning

Media hairpining is not supported for hair-pin and spiral call flows involving both H.323 and SIP protocols.

Fragmented Ping Support

The Oracle® Enterprise Session Border Controller does not respond to inbound fragmented ping packets.

Physical Interface RTC Support

After changing any Physical Interface configuration, you must reboot the system reboot.

SRTP Caveats

The ARIA cipher is not supported by virtual machine deployments.

Packet Trace

- VNF deployments do not support the **packet-trace remote** command.
- The Acme Packet 3900 does not support the **packet-trace remote** command.
- The Acme Packet 1100 does not support the **packet-trace remote** command.
- Output from the **packet-trace local** command on hardware platforms running this 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

Video flows are not supported in realms where RTCP generation is enabled.

SCTP

SCTP Multihoming does not support dynamic and static ACLs configured in a realm.

SCTP must be configured to use different ports than configured TCP ports for a given interface.

Real Time Configuration Issues

In this version of the E-SBC, the **realm-config** element's **access-control-trust-level** parameter is not real-time configurable.

Workaround: Make changes to this parameter within a maintenance window.

Virtual Network Function (VNF) Limitations

Oracle® Enterprise Session Border Controller (E-SBC) functions not available in VNF deployments of this release include:

- Native transcoding for codecs other than G.711, G.729 and AMR.
  Workaround: For all other codecs, configure your environment and system for pooled transcoding.
- FAX Detection
- RTCP generation for G.711 or G.729
- RTCP detection
- TSCF functionality

- Remote Packet Trace
- ARIA Cipher
- 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.

High Availability

High Availability (HA) redundancy is unsuccessful when you create the first SIP interface, or the first time you configure the Session Recording Server on theOracle® 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.

Acme Packet 3900 IPSec Limitations

The following IPSec functions are not available for the Acme Packet 3900 in this release.

- IKEv1
- Authentication header (AH)
- The AES-XCBC authentication algorithm
- Dynamic reconfiguration of security-associations
- Hitless HA failover of IPSec connections.

Dead Peer Detection

When running on the Acme Packet 6100, the E-SBC's dead peer detection does not work with IPv4.

Offer-Less-Invite Call Flow

Call flows that have "Offer-less-invite using PRACK interworking, Transcoding, and dynamic payload" are not supported in this release.

Fragmented SIP Message Limitations

Fragmented SIP messages are intercepted but not forwarded to the X2 server if IKEv1/IPsec tunnels are configured as transport mode.

Workaround: Configure IKEv1/IPsec tunnels as "tunnel mode".

IPv6 On X1 Interface

IPv6 does not work on X1 interface.

Known Issues

The following list of Known Issues provides the Bug DB number, a description of the issue, and when possible, the workaround, the found-in release, and the fixed-in release.

ID	Description	Found-in	Fixed-in
29937232	GW unreachable and NetBufCtrl MBUFF errors - This can result in system instability including crash, gw-unreachable and redundancy issues. System will switchover if in HA. Show Buffers output will normally show an increase of errors reported in the NetBufCtrl field due to mbuf's not being freed.	E-Cz8.1.0	E-Cz8.1.0m1p18
None	The system does not support SIP-H323 hairpin calls with DTMF tone indication interworking.	SCZ7.2.0	CZ8.1.0
None	The E-SBC stops responding when you configure an H323 stack supporting SIP-H323-SIP calls with its **max-calls** parameter set to a value that is less than its **q931-max-calls** parameter. Workaround: For applicable environments, configure the H323 stack **max-calls** parameter to a value that is greater than its **q931-max-calls** parameter.	SCZ7.4.0	TBD
None	The system does not support HA Redundancy for H.323 calls.		TBD
21805139	RADIUS Stop records for inter-working function (IWF) calls might display inaccurate values.	SCZ7.3.0	TBD

ID	Description	Found-in	Fixed-in
22322673	When running in an HA configuration, the secondary E-SBC might go out of service (OoS) during upgrades, switchovers, and other HA processes while transitioning from the "Becoming Standby" state. Oracle observes such behavior in approximately 25% of these circumstances. You can verify the issue with log.berpd, which can indicate that the media did not synchronize. Workaround: Reboot the secondary until it successfully reaches the "Standby" state.	SCZ7.3.0P1	TBD
24574252	The **show interfaces brief** command incorrectly shows **pri-util-addr** information in its output.	SCZ7.4.0	TBD
24809688	Media interfaces configured for IPv6 do not support multiple VLANs.	SCZ7.3.0	TBD
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	TBD
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.	Unknown	TBD

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	TBD
26281599	The system feature provided by the **phy-interfaces**'s **overload-protection** parameter and **overload-alarm-threshold** sub-element is not functional. Specifically, enabling the protection and setting the thresholds does not result in trap and trap-clear events based on the interface's traffic load. The applicable ap-smgmt.mib SNMP objects include: • apSysMgmtPhyUtilThresholdTrap • apSysMgmtPhyUtilThresholdClearTrap	SCZ7.2.0	SCZ8.2.0
26313330	In some early media call flows, the E-SBC might not present the correct address for RTP causing the call to terminate.	SCZ8.0.0	SCZ8.0.0p2
26316821	When configured with the 10 second QoS update mechanism for OCOM, the E-SBC presents the same codec on both sides of a transcoding call in the monitoring packets. You can determine the correct codecs from the SDP in the SIP Invite and 200 OK.	SCZ8.0.0p1	TBD

ID	Description	Found-in	Fixed-in
26323802	The 10s QoS interim feature includes the wrong source IP address as the incoming side of a call flow. The issue does not prevent successful call and QoS monitoring. For monitoring and debugging purposes, you can find the source IP in the SIP messages (INVITE/200OK).	SCZ8.0.0p1	TBD
26338219	The **packet-trace remote** command does not work with IPv6.	S-CZ7.4.0	TBD
26432028	On the Acme Packet 1100, Acme Packet 3900, and VME un-encrypted SRTP-SDES calls result in one-way audio. Workaround: None at this time.	E-CZ7.5.0	TBD
26497348	When operating in HA mode, the E-SBC might display extraneous "Contact ID" output from the **show sipd endpoint-ip** command. You can safely ignore such output.	SCZ8.0.0	TBD
26669090	The E-SBC dead peer detection does not work with IPv4.	SCZ8.0.0	TBD
26790731	Running commands with very long output, such as the "show support-info" command, over an OVM virtual console might cause the system to reboot. Workaround: You must run the "show support-info" command only over SSH.	SCZ8.0.0p1	TBD

ID	Description	Found-in	Fixed-in
27031344	When configured to perform SRTP-RTP interworking, the E-SBC might forward SRTP information in the SDP body of packets on the core side, causing the calls to terminate. Workaround: Add an appropriately configured media-sec-policy on the RTP side of the call flow. This policy is in addition to the policy on the SRTP side of the call flow.	SCZ8.0.0p1	TBD
27240195	The cpu-load command does not display the correct value under show-platforms.	ECZ8.0.0	CZ8.1.0
26338219	In some PRACK IWF scenarios, the E-SBC may insert the media address of the core in the 200 OK SDP sent to the caller instead of it's own address. This misdirects the audio causing the call to fail.		CZ8.1.0
	If you configured the ims_aka option, you must also configure sip-interfaces with an ims-aka-profile entry.		ECZ7.4.0m1
27795586	When running E-CZ8.1.0 over Hyper-V, and you set the process-log level to DEBUG, the system can become unstable or stop responding. The system requires a reboot. Workaround: Do not enable process-log level DEBUG.	ECZ8.1.0	CZ810p1
27539750	When trying to establish a connection between the SBC and your network, while using TLS version 1.2, the SBC may reject the connection. Workaround: You may need to adjust your cipher list.	ECZ8.1.0	TBD

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	SCZ810m1
None	IPSec is not supported on the Acme Packet 3900 and VNF in the CZ8.1.0 release. You must upgrade to CZ8.1.0p1 to get this support. After you upgrade to CZ8.1.0p1, do the following: 1. Run **setup entitlements**, again. 2. Select **advanced** to enable advanced entitlements, which then provides support for IPSEC on Acme Packet 3900 and VNF systems.	CZ810	CZ810p1
28305575	On VNFs, the system erroneously displays the IPSEC entitlement under "Keyed (Licensed) Entitlements." The error does not affect any functionality and you do not need to do anything.	CZ810	CZ820
28367500	When operating the OCSBC on the Acme Packet 6300, the **traceroute** command does not show hops for an IPv6 traceroute that does not reach the target address. The system successfully displays hops when the traceroute reaches the target and for IPv4 traceroutes.	CZ810	TBD
28475320	When running ECZ810M1 on the Acme Packet 3900, IPSec functionality is not available.	CZ810	TBD

ID	Description	Found-in	Fixed-in
28617938	The **anonymize-invite** option for CommMonitor is not RTC. To see a change, you must either reboot or toggle the admin state. The following is a general admin state toggle procedure: 1. Set admin state to disabled. 2. Save and activate. 3. Set admin state to enabled. 4. Save and activate.	CZ810m1	TBD
28618563	The system is not populating the Username AVP in Accounting Requests (ACRs) correctly. When triggered by an INVITE, these AVPs contain only the "@" sign. They do not include the username and domain name portion of the URL.	CZ810m1	TBD
28659469	When booting CZ8.1.0M1 on any virtual platform, not all system processes start. This known issue only occurs on initial boot, and not in an upgrade scenario. Workaround: Reboot the E-SBC a second time, after it initially starts.	CZ810m1	TBD
29931732	The embedded communications monitor probe does not send IPv6 traffic to the Oracle Communications Operations Monitor's mediation engine.	SCZ800	TBD

ID	Description	Found-in	Fixed-in
28820258	When running TLS Chat on VMware-PV 4core (SSFD) + 16GB, TLS Chat sessions are gradually decreasing. When looking in Wireshark at EXFO, EXFO forwards a wrong TLS MSRP Chat payload to EXFO UAS. TCP Chat doesn't have this error.	E-CZ800	TBD

The following Known Issues and Caveats have been found not to be present in this release. They are collected here for tracking purposes.

ID	Description	Found In	Fixed In
27700933	The system does not support TSM.	N/A	N/A
27700607	When recording transcoded streams under load, sometimes the recorder might receive only a single stream.	N/A	N/A
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.	N/A	N/A
N/A	The T.140-Baudot Relay is not excluded from pooled transcoding support.	N/A	N/A