Oracle® Enterprise Session Border Controller

Release Notes

S-Cz8.2.0

F20172-02

July 2020

Oracle Enterprise Session Border Controller Release Notes, S-Cz8.2.0

F20172-02

Contents

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 table describes the documentation set for this release.

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

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

Related Documentation

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

Document Name	Document Description
Acme Packet 3900 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 3900.
Acme Packet 4600 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4600.
Acme Packet 6100 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6100.
Acme Packet 6300 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6300.
Acme Packet 6350 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6350.
Release Notes	Contains information about the current documentation set release, including new features and management changes.
ACLI Configuration Guide	Contains information about the administration and software configuration of the Service Provider Oracle® Enterprise Session Border Controller.
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Maintenance and Troubleshooting Guide	Contains information about Oracle® Enterprise Session Border Controller logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
MIB Reference Guide	Contains information about Management Information Base (MIBs), Oracle Communication's enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Accounting Guide	Contains information about the Oracle® Enterprise Session Border Controller's accounting support, including details about RADIUS and Diameter accounting.
HDR Resource Guide	Contains information about the Oracle® Enterprise Session Border Controller's Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Administrative Security Essentials	Contains information about the Oracle® Enterprise Session Border Controller's support for its Administrative Security license.

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

Revision History

December 2018	Initial Release
January 2019	• Updated for S-Cz8.2.0p2. • Updated the "Small Footprint VNF" New Feature with the correct spec for required RAM.
February 2019	• Updates "Transcoding Support" for accuracy. • Updates the "Provisioning Transcode Codec Sessions Capacities" caveat for clarity. • Updates "Virtual Network Function (VNF) Limitations".
March 2019	• Adds "Maintain DSA-Based HDR and CDR Push Behavior" to "Upgrade and Downgrade Caveats". • Updates "Default VNF Resources" for accuracy. • Removes T.140-Baudot Relay from the list of features unsupported with Pooled Transcoding. • Updates processor specification requirements for VNFs • Updates VNF Caveats with IXGBE driver limitation.
April 2019	• Updated for S-Cz8.2.0p3. • Corrected the list of platforms supported for virtual MSRP. • Updates Transcoding caveats with Local Media Playback incompatibility. • Corrects "Transcoding Support" table. • Adds explanation of change in HMR matching.

May 2019	• Updates minimum vSBC signaling core requirement to 2 • Adds MSRP to list of features in the "Encryption for Virtual SBC" table. • Adds Performance Enhancements section to New Features list.
June 2019	• Adds OCOM incompatibility with IPv6 to known issues.
October 2019	• Updates the Known Issues table.
November 2019	• Adds trace tool limitations to "Trace Tools" caveats. • Adds VLAN tagging caveat to "Virtual Network Function (VNF) Caveats."
December 2019	• Updates closed Known Issues
February 2020	• Adds telephone-event to supported codecs list for VNF
July 2020	• Moves bug# 22322673 to Non-present Known Issues table. • Repairs confusing known issue on IPv6 and VLANs

1 Introduction to S-Cz8.2.0

The Oracle® Enterprise Session Border Controller *Release Notes* provides the following information about S-Cz8.2.0 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 S-Cz8.2.0 software supports the following platforms.

Acme Packet Platforms

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

Qualified Hypervisors

Oracle qualified the following components for deploying version S-Cz8.2.0 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
  - LIBVIRT
    - 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 Cloud Computing Platforms

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

> **Note:**
>
> For information about deploying Heat, see the README in the TAR file that contains the Heat templates.

Public Cloud Support

- Microsoft Azure: The E-SBC can run in stand-alone mode in Microsoft Azure with version S-Cz8.2.0p3 and later. Customers must contact Oracle support prior to using this platform for important information and approval.

Supported Interface Input-Output Modes

- Para-virtualized
- SR-IOV
- PCI Passthrough

Supported Ethernet Controller, Driver, and 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	NA	NA
Broadcom BCM57417	bnxt	WM	NA	NA
Mellanox ConnectX-4	mlx5	NA	M	M
Mellanox ConnectX-5	mlx5	NA	M	M

- W - wancom interface
- M - media interface
- NA - not applicable

Virtual Machine Platform Resources

A Virtual Network Function (VNF) requires the CPU core, memory, disk size, and network interfaces specified for operation. Deployment details, such as the use of distributed DoS protection, dictate resource utilization beyond the defaults.

Default VNF Resources

VM resource configuration defaults to the following:

- 4 CPU Cores
- 8 GB RAM
- 20 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 S-Cz8.2.0 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) - You 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 S-Cz8.2.0 VNF requires an Intel Core7 processor or higher, or a fully emulated equivalent including 64-bit SSSE3 and SSE4.2 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.

PCIe Transcoding Card Requirements

For virtual SBC deployments, you can install an Artesyn SharpMedia™ PCIe-8120 media processing accelerator with either 4, 8, or 12 DSPs in the server chassis in a full-height, full-length PCI slot to provide high density media transcoding.

Compatibility between the PCIe-8120 card and the SBC is subject to these constraints:

- VMWare and KVM are supported
- PCIe-pass-through mode is supported
- Each vSBC can support 2 PCIE 8120 cards and the server can support 4 PCIE 8120 cards.
- Each PCIe-8120 card can be devoted to only one vSBC instance
- Transcoding cores for software-based transcoding may not be configured in conjunction with PCIe media card use

Image Files and Boot Files

This software version distribution provides multiple products, based on your **setup product** configuration.

> **Note:**
>
> Starting with this release, the naming convention for the Enterprise Session Border Controller image file and boot file changes from "`nnECZ<release>.bz`" to "`nnSCZ<release>.bz`." (SCZ replaces ECZ.) The naming convention for the boot file changes from "`nnECZ<release>.boot`" to "`nnSCZ<release>.boot>`." In S-CZ8.2.0, the image and boot file names are the same for both Service Provider and Enterprise.

For Acme Packet Platforms

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

- Image file: `nnSCZ820.bz`
- Bootloader file: `nnSCZ820.boot`

For Virtual Machines

This S-Cz8.2.0 release includes distributions suited for deployment over hypervisors. Download packages contain virtual machine templates for a range of virtual architectures. Use the following distributions to the Session Border Controller as a virtual machine:

- `nnSCZ820-img-vm_ovm.ova`—Open Virtualization Archive (.ova) distribution of the SBC VNF for Oracle (XEN) virtual machines.
- `nnSCZ820-img-vm_kvm.tgz`—Compressed image file including SBC VNF for KVM virtual machines.
- `nnSCZ820-img-vm_vmware.ova`—Open Virtualization Archive (.ova) distribution of the SBC VNF for ESXi virtual machines.
- `nnSCZ820-img-vm_vhd.tgz`—Compressed image file including SBC for Hyper-V virtual machine.
- `nnSCZ820_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.

Setup Product

1. Type **setup product** at the ACLI. If this is the first time running the command on this hardware, the product will show as Uninitialized.
2. Type **1 <Enter>** to modify the uninitialized product.
3. Type the number followed by **<Enter>** for the product type you wish to initialize.
4. Type **s <Enter>** to commit your choice as the product type of this platform.
5. Reboot your Oracle® Enterprise Session Border Controller.

```
ORACLE# setup product

--------------------------------------------------------------
WARNING:
Alteration of product alone or in conjunction with entitlement
changes will not be complete until system reboot

Last Modified
--------------------------------------------------------------
 1 : Product        : Uninitialized

Enter 1 to modify, d' to display, 's' to save, 'q' to exit. [s]: 1

  Product
    1 - Session Border Controller
    2 - Session Router - Session Stateful
    3 - Session Router - Transaction Stateful
    4 - Subscriber-Aware Load Balancer
    5 - Enterprise Session Border Controller
    6 - Peering Session Border Controller
  Enter choice     : 1

Enter 1 to modify, d' to display, 's' to save, 'q' to exit. [s]: s
save SUCCESS
```

Note:

When configuring an HA pair, you must provision the same product type and features on each system.

setup product

The setup product command is used to assign a product type to this instance of software and hardware combination. By executing this command, you will be faced with a list of valid products, based on platform, that you may provision this system as. Choose the appropriate product and hit the <Enter> key to accept.

Syntax

```
setup product
```

Mode

Superuser

```
ORACLE# setup product

--------------------------------------------------------------
WARNING:
Alteration of product alone or in conjunction with entitlement
changes will not be complete until system reboot

Last Modified
--------------------------------------------------------------
 1 : Product       : Uninitialized

Enter 1 to modify, d' to display, 's' to save, 'q' to exit. [s]: 1

  Product
    1 - Session Border Controller
    2 - Session Router - Session Stateful
    3 - Session Router - Transaction Stateful
    4 - Subscriber-Aware Load Balancer
    5 - Enterprise Session Border Controller
    6 - Peering Session Border Controller
  Enter choice     : 1

Enter 1 to modify, d' to display, 's' to save, 'q' to exit. [s]: s
save SUCCESS
```

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 SC-z8.2.0 release supports the following paths for in-service software upgrades and rollbacks on existing Enterprise Session Border Controller installations.

- E-Cz8.1.0 to S-Cz8.2.0

- E-Cz8.0.0 to S-Cz8.2.0
- E-Cz7.5.0 to S-Cz8.2.0

For systems running E-Cz7.4.0GA to E-CZz.4.0p3, you must upgrade to E-Cz7.4.0M1 and perform a dual reboot before upgrading to S-Cz.8.2.0. 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 S-Cz8.2.0. 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 Acme Packet 3900 platforms, the software TLS and software SRTP features no longer require license keys. After you upgrade to S-Cz8.2.0, 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 in the boot parameters. You cannot edit the boot file name when upgrading from E-CZ7.5.0 to E-CZ8.2.0 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 S-Cz8.2.0, 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 delivers increased encryption strength for internal password hash storage for the S-Cz8.2.0 release. This affects downgrades to the E/SC-z7.x and E/SC-z8.0.0 releases because the enhanced password hash algorithm is not compatible with those earlier SBC software versions. The change does not affect downgrades to E/SCz8.1.0. If you change any local account passwords after upgrading to S-Cz8.2.0, local authentication does not work and the system locks. Unlocking the system requires a factory reset. Oracle recommends that you do not change any local account passwords after upgrading to S-Cz8.2.0 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 S-Cz8.2.0, downgrading is not affected.

Caution:

If you change the local passwords after you upgrade to S-Cz8.2.0, and then later want to downgrade to a previous release, reset the local user passwords with the following procedure before you downgrade because the system locks 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 steps 1-10 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.

vSBC License Keys

See "Encryption for Virtual SBC" under "Self-Provisioned Entitlements" for important information about licensing changes for virtual SBCs.

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 S-Cz8.2.0, 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.

Upgrade Checklist

Before upgrading the Oracle® Enterprise Session Border Controller software:

1. Obtain the name and location of the target software image file from either Oracle Software Delivery Cloud, https://edelivery.oracle.com/, or My Oracle Support, https://support.oracle.com, as applicable.
2. Provision platforms with the Oracle® Enterprise Session Border Controller image file in the boot parameters.
3. Run the **check-upgrade-readiness** command and examine its output for any recommendations or requirements prior to upgrade.
4. Verify the integrity of your configuration using the ACLI **verify-config** command.
5. Back up a well-working configuration. Name the file descriptively so you can fall back to this configuration easily.
6. Refer to the Oracle® Enterprise Session Border Controller Release Notes for any caveats involving software upgrades.

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.

Encryption for Virtual SBC

Starting with the S-Cz8.2.0 release, you must enable encryption for virtualized deployments with a license key. The following table lists which licenses are required for various encryption use cases.

Feature	License
IPSec Trunking	IPSec
SRTP Sessions	SRTP
Transport Layer Security Sessions	TLS [1]
MSRP	TLS

[1] The TLS license is only required for media and signaling. TLS for secure access, such as SSH, HTTPS, and SFTP is available without installing the TLS license key.

To enable the preceding features, you install a license key at the **system, license** configuration element. Request license keys at the License Codes website at http://www.oracle.com/us/support/licensecodes/acme-packet/index.html.

After you install the license keys, you must reboot the system to see them.

Upgrading To 8.2 From Previous Releases

When upgrading from a previous release to S-Cz8.2.0, your encryption entitlements carry forward and you do not need to install a new license key.

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 limits** command.

Transcoding Support

Based on the transcoding resources available, which vary by platform, different codecs may be transcoded from- and to-.

Platform	Supported Codecs (by way of codec-policy in the add-on-egress parameter)
• Acme Packet physical platforms • Hardware-based transcoding for virtual platforms (PCIe Media Accelerator)	• AMR • AMR-WB • CN • EVRC0 • EVRC • EVRC1 • EVRCB0 • EVRCB • EVRCB1 • EVS • G711FB • G722 • G723 • G726 • G726-16 • G726-24 • G726-32 • G726-40 • G729 • G729A • GSM • iLBC • Opus • SILK • PCMU • PCMA • T.38 • T.38OFD • telephone-event • TTY, except on the Acme Packet 1100

Platform	Supported Codecs (by way of codec-policy in the add-on-egress parameter)
• Virtual Platforms (with 1+ transcoding core)	• AMR • AMR-WB • EVS • G729 • G729A • iLBC • Opus • PCMU • PCMA • telephone-event 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.

Coproduct 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-Cz8.2.0 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, E-Cz8.1.0, and E-Cz8.2.0)
- Acme Packet 6300 (E-Cz7.5.0, E-Cz8.0.0, E-Cz8.1.0, and E-Cz8.2.0)

Oracle Communications Session Router

The E-SBC supports the Oracle Communications Session Router.

Oracle Communications Session Delivery Manager

Oracle Communications Session Deliver Manager (OCSDM) versions 8.1.1 and later support this GA release of the Enterprise SBC. You must do the following:

1. Setup the Enterprise SBC system using the **setup product** command.
2. Install the Service Provider Edge and Core plug-in v 2.0 in OCSDM.
3. Add the Enterprise SBC, running S-Cz8.2.0, as a device in the Device Manager.

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_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_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_AES_128_CBC_SHA256
- 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.

Note:

The default is TLSv1.2. Oracle supports TLS1.0 and TLS1.1 for backward compatibility, only, and they may be deprecated in the future.

Deprecated Features

Oracle recommends that you review the following information about deprecated features and functions before using the S-Cz8.2.0 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	ECZ8.1.0
secure-traps	Within the context of the E-SBC's comprehensive SNMPv3 support, the **secure-traps** value is removed from the **snmp-agent-mode** parameter. The elimination of **secure-traps** means that the following protocols are deprecated for use by SNMP: • DES privacy protocol • MD5 and SHA authentication protocols	SCZ8.1.0

Previous Deprecations

Feature	Description	Release Deprecated
Platforms	The S-Cz8.2.0 release does not support either the Acme Packet 3820 or the Acme Packet 4500.	E-CZ8.0.0

Feature	Description	Release Deprecated
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 S-Cz8.2.0 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

The following information lists and describes the changes made to the Oracle® Enterprise Session Border Controller (E-SBC) documentation set for S-Cz8.2.0.

ACLI Reference Guide

The *ACLI Reference Guide* now includes commands for both Service Provider and Enterprise software.

Documentation Set

The following guides were formerly listed as Related Documentation because they were oriented to Service Provider customers, but might occasionally interest the Enterprise customer. Due to changes in the way Oracle builds the session border controller software, the content in these guides is no longer predominately useful to Service Provider customers. Much of the content now applies to Enterprise, as well, making them useful additions to the Enterprise documentation set.

- ACLI Reference Guide
- Installation and Platform Preparation Guide
- SBC Family Security Guide

DTMF IWF Documentation

The RFC 2833 Dual Tone Multi Frequency (DTMF) Inter-working Function (IWF) information moves from the "IWF Services" chapter in the *ACLI Configuration Guide* to the "DTMF Transfer and Support" chapter.

Transcoding Chapter

In the *ACLI Configuration Guide*, the "Transcoding" chapter is reorganized and edited for clarity.

Trunk Group Documentation

The "Trunk Group URIs" information is removed from the "IWF Services" chapter in the *ACLI Configuration Guide*. This information, previously duplicated, is retained in the "SIP Signaling" chapter.

Patches Included in This Release

The following information assures you that when upgrading, the S-Cz8.2.0 release includes defect fixes from neighboring patch releases.

Baseline

Cz8.1.0m1p5 is the patch baseline, which is the most recent build from which Oracle created S-Cz8.2.0.

Neighboring Patches Also Included

- E-Cz7.5.0p5
- E-Cz8.0.0p2

Behavioral Changes

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

Minimum Signaling Core Requirement

The minimum number of signaling cores for a vSBC is changed to 2. The exceptions to this requirement are deployments on the Acme Packet 1100 and small footprint deployments.

TLS1.0

TLS1.0 is no longer advertised by default during session negotiation 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**. Note that the current default is TLSv1.2.

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

Licensing IPSec / TLS / SRTP / IMS-AKA on vSBC

For new configurations on virtual platforms, you must enter a license key that enables certain encryption-oriented features before setting entitlements. See: Encryption for Virtual SBC for more information.

VNF Licensing

The S-Cz8.2.0 release reverts to the pre-S-Cz8.1.0 behavior where VNF once again requires a license key. (The S-Cz8.1.0 release did not require a license key for VNF.)

Image File Name Change

Starting with this release, the naming convention for the Enterprise Session Border Controller image and boot files changes. See Image Files and Boot Files for the new file names.

> **Note:**
>
> This change also affects Session Delivery Manager support. See the Coproduct Support topic for details.

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.

Supported SPL Engines

The S-Cz8.2.0 release supports the following SPL engine versions: 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, C3.1.10, C3.1.11, C3.1.12.

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 S-Cz8.2.0 release.

- The S-Cz8.2.0 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).

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)
- 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 and JITC certification
- H.323 routing enhancements
- Several Suite B ciphers across the product
- Avaya enhancements
  - Personal Profile Manager (PPM) support
  - Dual registrations

Note the following changes in support. As of S-Cz8.2.0, the OCSBC gains support for:

- Telephony fraud prevention
- PKCS 12 container import and export

2

New Features

The S-Cz8.2.0 release supports the following new features and enhancements.

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

Small Footprint VNF

Oracle® Enterprise Session Border Controller (E-SBC) customers who want to reduce the size of their SBC deployment footprints or who may not need the maximum number of cores and amount of memory available can deploy the SBC virtually with fewer cores and memory requirements. For smaller scale deployments, the VNF software supports a minimum deployment of 2 virtual cores, 4GB RAM, and 20GB storage. In this way, Oracle provides a flexible solution that you can tailor to your requirements.

RTP TTL

The Oracle® Enterprise Session Border Controller (E-SBC) allows you to set, on a per media-policy basis, the number of hops RTP packets can traverse before they should be dropped.

See "Realms and Nested Realms" in the *ACLI Configuration Guide*.

Upgrade Information

The Oracle® Enterprise Session Border Controller (E-SBC) includes the **check-upgrade-readiness** ACLI command, which presents system information arranged to clearly tell you if you need to perform any tasks before you upgrade.

See "Upgrading Software" in the *Platform Preparation and Installation Guide*.

Mellanox® Support

SCZ8.2.0 supports interface card from Mellanox® for VNF deployments. Refer to "Platform Support" in these Release Notes for details on specific cards, drivers, interface modes, and functional support.

Simultaneous DTMF and Audio Payload Mapping

In addition to enabling audio payload type mapping for AMR and AMR-WB and enabling EVS AMR-WB IO payload type mapping, the **audio-payload-type-mapping** option, within the **media-manager**, configures the Oracle® Enterprise Session Border Controller (E-SBC) to support simultaneous payload type mapping for audio and DTMF RFC-2833 for AMR, AMR -WB, and EVS in AMR wideband IO mode. Payload type mapping requires fully compatible SDP, with the exception of the payload type number. Simultaneous audio and DTMF RFC 2833 payload type mapping also requires that the payload type numbers for audio and DTMF be different.

Software-Based Transcoding Support

SCZ8.2.0 adds support for software transcoding of the following codecs for VNF deployments.

- EVS (Service Provider, only)
- OPUS
- iLBC

Refer to "Transcoding Support" in these Release Notes for complete lists of transcoding codecs, based on Acme Packet and VNF platforms.

REST API

The Oracle® Enterprise Session Border Controller (E-SBC) includes a REST API that accepts Create, Read, Update, and Delete (CRUD) operations over HTTPS. For a description of the supported REST API endpoints, see the REST API documentation.

OpenStack Heat Template

The following new parameters are available for configuration in the environmental file.

- diskPartitions—Specify the percentage of disk space that will be allocated for each partition.
- applyBaseConfiguration—Enable or disable the base configuration, which is suitable for minimal Standalone or HA-pair functionality.
- configuration—If applyBaseConfiguration is set to true, specify the input parameters for the base configuration. Sub-parameters include:
  - dosCores—Specify the number of CPU cores dedicated for denial-of-service protection.
  - forwardingCores—Specify the number of CPU cores dedicated for forwarding frames.
  - transcodingCores—Specify the number of CPU cores dedicated for transcoding media.
  - ntpServer1—Specify the IP address of an NTP server to use for time synchronization.
  - ntpServer2—Specify the IP address of an NTP server to use for time synchronization.
  - snmpCommunityName—Specify the name of the SNMPv2 community to use for SNMP management.
  - snmpIpAddress—Specify the IP address to add to the SNMPv2 community for SNMP management.
- wancom0VLAN—(Only available on Pike and newer) Specify the bootparameter VLAN value for the wancom0 interface.
- vnicBinding—Specify the virtual NIC binding type for each media interface.

For a list of all supported parameters, see the *The Platform Preparation and Installation Guide*.

Secure RADIUS Connection

The E-SBC can connect to a RADIUS server over a secure IPSec/IKEv2 connection over a media interface.

> **Note:**
>
> You must install the IPSec license to enable RADIUS over a secure IPSec/IKEv2 connection.

See "Secure RADIUS Connection" in the *Administrative Security Guide*.

Product and Entitlement Provisioning from the Heat template

This release supports provisioning both the product and any of its entitlements when deploying virtual machines from a Heat template.

For more details, see the "Virtual Machine Platforms" chapter in *The Platform Preparation and Installation Guide*. For examples, see the README file located in the Heat Orchestration Template .tar.gz file.

Performance Enhancements

Optimization and performance enhancements have been made to SBC components. These include:

- SIPd, Radd, and MBCD enhancements that increase performance
- Improved SSM card utilization
- File descriptor monitoring

3

Interface Changes

The following topics summarize ACLI, SNMP, HDR, Alarms, and RADIUS changes for S-Cz8.2.0. The additions, removals, and changes noted in these topics occured since the previous major release of the Oracle® Enterprise Session Border Controller.

ACLI Command Changes

The following table summarizes the ACLI command changes that first appear in the Oracle® Enterprise Session Border Controller S-Cz8.2.0 release.

Command	Description
check-upgrade-readiness	New command providing you with summary or comprehensive system state. Information reported is filtered to assist with or prevent upgrade to new system software.

ACLI Configuration Element Changes

The following tables summarize the ACLI configuration element changes that first appear in the Oracle® Enterprise Session Border Controller (E-SBC) S-Cz8.2.0 release.

Media Features

New Parameters	Description
media-manager, **media-policy**, **rpt-ttl**	Specifies the number of hops media traffic can take before being dropped.
media-manager, **options +audio-payload-type-mapping**	Adds additional function to the option wherein the system can perform both audio and DTMF RFC-2833 payload type mapping simultaneously on AMR, AMR-WB, and EVS in AMR-WB IO mode calls.
media-manager, **tcp-media-profile**, **msrp-cema-support**	Not supported.
media-manager, **tcp-media-profile**, **msrp-sessmatch**	Not supported.
media-manager, **tcp-media-profile**, **msrp-message-size-enforce**	Not supported.
media-manager, **tcp-media-profile**, **msrp-message-size**	Not supported.
media-manager, **tcp-media-profile**, **msrp-message-size-file**	Not supported.

System Features

New Parameters	Description
system, **fraud-protection**	Specifies the XML file used by the system to categorize endpoints in the white list, blacklist, redirect list, and rate limit list for the fraud protection function.
session-router, **local-response-map**	Adds the **fraud-protection-reject-call** setting to specify the response sent to stations that the system finds on its blacklist.

Security Features

New Parameters	Description
security, **ike**, **ike-interface**, **ike-version**	Setting **ike-version** to **2** is only supported for RADIUS authentication over a media interface when the Advanced Security Suite entitlement is installed.

4

Caveats and Known Issues

This chapter lists the caveats and known issues 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.

Known Issues

This table lists the OCSBC known issues in version CZ8.2.0. You can reference known issues by Service Request number and you can identify the issue, any workaround, when the issue was found, and when it was fixed using this table. Issues not carried forward in this table from previous Release Notes are not relevant to this release. You can review delivery information, including defect fixes in this release's Build Notes.

ID	Description	Severity	Found In
24574252	The **show interfaces brief** command incorrectly shows **pri-util-addr** information in its output.	3	SCZ740
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.	2	SCZ800
26338219	The **packet-trace remote** command does not work with IPv6.	2	SCZ740
26497348	When operating in HA mode, the E-SBC may display extraneous "Contact ID" output from the **show sipd endpoint-ip** command. You can safely ignore this output.	3	SCZ800
The **show sipd srvcc** command does not display the correct number of unsuccessful aSRVCC calls.	3	SCZ800	
21805139	RADIUS stop records for IWF calls may display inaccurate values.	2	SCZ730b6
24809688	Media interfaces configured for IPv6, and using different VLANs that operate over different infrastructures, including VoLTE and 3GPP, are not supported.	3	SCZ730
None	The system does not support SIP-H323 hairpin calls with DTMF tone indication interworking.	N/A	S-CZ720

ID	Description	Severity	Found In
None	The E-SBC stops responding when you configure an H323 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 H323 stack **max-calls** parameter to a value that is greater than its **q931-max-calls** parameter.	N/A	S-CZ740
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.	4	CZ810m1
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.	3	CZ810m1
25954122	Telephony fraud protection does not black list calls after a failover. Workaround: Activate the fraud protection table on the newly active server.	3	E-CZ7.5.0
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.	2	Unknown
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.	3	E-CZ7.5.0

ID	Description	Severity	Found In
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.	3	SCZ8.0.0p1
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).	3	SCZ8.0.0p1
26432028	On the Acme Packet 1100, Acme Packet 3900, and VME un-encrypted SRTP-SDES calls result in one-way audio.	3	E-CZ7.5.0
26669090	The E-SBC dead peer detection does not work with IPv4.	3	SCZ8.0.0
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.	3	SCZ8.0.0p1
28539155	When operating as a VNF and using Mellanox interface cards, the OCSBC does not support ICMP over IPv6.	3	SCZ820
28539190	When operating as a VNF and using Mellanox interface cards, the OCSBC does not use the Host In Path (HIP) configuration to restrict management traffic, Instead the system allows any traffic over the interface.	3	SCZ820
28617865	This version of the OCSBC only is not supported as a VNF over VMware using Mellanox interface cards.	3	SCZ820
28639227	When operating as a VNF and using Mellanox interface cards, the OCSBC does not support SCTP transport.	3	SCZ820

ID	Description	Severity	Found In
28658810	When operating as a VNF and using Mellanox interface cards, the OCSBC does not support any other type of card for media interfaces. (If any media interface uses a Mellanox card, all media interfaces must use a Mellanox card.)	3	SCZ820
28748784	When operating as a VNF and using Mellanox interface cards, the OCSBC does not support outbound ICMP.	3	SCZ820
28906914	For transcoding use cases, the G711/G729 codec pair might experience unstable performance when each DSP has greater than 500 transcoding sessions.	3	SCZ820
28770472	ACLI Users will receive an error on the output of the show registration sipd by-user command.	4	SCZ820
29170419	In long call scenarios, the SBC is not sending the expected refresh before the Session-Expires: header value time is up for SUBSCRIBE messages.	2	SCZ820
29931732	The embedded communications monitor probe does not send IPv6 traffic to the Oracle Communications Operations Monitor's mediation engine.	3	SCZ800
28820258	On PNF platforms, 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 does not have this error.	3	SCZ800

Resolved Known Issues

The following table provides a list of previous Known Issues that are now resolved.

ID	Description	Severity	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.	2	SCZ820	SCZ830p6

ID	Description	Severity	Found In	Fixed In
28526228	Maximum SRTP capacity on VNF platforms is 25% lower than in the SCZ8.1.0 release. Expected capacity will be restored in a follow up patch.	3	SCZ820	SCZ830
26313330	In some early media call flows, the E-SBC may not present the correct address for RTP causing the call to terminate.	3	SCZ800	SCZ820
26281599	The system feature provided by the **phy-interfaces 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	3	SCZ720	SCZ820
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.	3	SCZ810	SCZ810
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.	2	SCZ740	SCZ820
None	The CZ8.1.0 release does not support IPSec on the Acme Packet 3900 and VNF. 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.	N/A	CZ810	CZ820
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.	4	CZ810	CZ820
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.	3	CZ810m1	SCZ820
27240195	The **cpu-load** command does not display the correct value under **show-platforms**.	3	ECZ8.0.0	SCZ820

ID	Description	Severity	Found In	Fixed In
	If you configured the ims_aka option, you must also configure sip-interfaces with an ims-aka-profile entry.	3	ECZ7.4.0	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.	3	ECZ8.1.0	SCZ820
28475320	When running ECZ810M1 on the Acme Packet 3900, IPSec functionality is not available.	2	CZ810	SCZ820

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
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.	N/A	N/A
N/A	The T.140-Baudot Relay is not excluded from supported features with pooled transcoding.	N/A	N/A

ID	Description	Found In	Fixed In
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.	N/A	N/A

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 provisioned with a license key, a capacity change requires a reboot to take effect.
- When a transcode codec is self-provisioned, 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 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.
- MSRP support for VNF requires a minimum of 16GB of RAM.

- The system supports only KVM and VMWare for virtual MSRP, and it supports only the 4 core SSFD model.
- CPU load on 2-core systems may be inaccurately reported.
- IXGBE drivers that are a part of default host OS packages do not support VLANs over SR-IOV interfaces.
- Virtual LAN (VLAN) tagging is not supported when deploying the OCESBC over the Hyper-V platform.

Virtual Network Function (VNF) Limitations

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

- FAX Detection
- RTCP generation for G.711 or G.729
- RTCP detection
- 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.

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.

MSRP Support

The Acme Packet 3900 does not support the MSRP feature set.

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.

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".

Diameter Server Timeout during Save/Activate

When saving and activating a configuration, the E-SBC may disconnect from an external policy server. The cause of this disconnect is based on SCTP HEARTBEAT value configured on the Diameter policy server.

Solution: You can work around this issue by setting the policy server's SCTP HEARTBEAT to a value greater than 750ms, which exceeds the amount of time it takes to perform a save/activate on the E-SBC.