Oracle® Enterprise Session Border Controller

Release Notes

Release S-Cz8.3.0

F20179-09

August 2021

Oracle Enterprise Session Border Controller Release Notes, Release S-Cz8.3.0

F20179-09

Contents

About This Guide

Revision History

1 Introduction to S-Cz8.3.0

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.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request.
2. Select 3 for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
   - For technical issues such as creating a new Service Request (SR), select 1.
   - For non-technical issues such as registration or assistance with My Oracle Support, select 2.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click **Industries**.
3. Under the Oracle Communications sub-header, click the **Oracle Communications documentation** link.
   The Communications Documentation page appears. Most products covered by these documentation sets appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."
4. Click on your Product and then Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Revision History

This table provides the revision history for this document.

January 2019	• Initial Release
February 2019	• Updates "Image Files and Boot Files" for accuracy.
April 2019	• Updated for S-Cz8.3.0p2 and S-Cz8.3.0p3.
May 2019	• Updates the "Known Issues" table. • Adds Performance Enhancements section to New Features list.
June 2019	• Fixed broken link in Behavioral Changes. • Updates the "Known Issues" table for S-Cz8.3.0p5.
July 2019	• Adds Daylong Transcoding Session Cleanup feature to New Features chapter. • Adds Multiple Contact Handling in Redirect Action for LRT to New Features chapter. • Adds OCOM incompatibility with IPv6 to known issues.
August 2019	• Updates the Known Issues table.
October 2019	• Updated for the S-Cz8.3.0m1 release. • Updated Caveats And Limitations section. • Adds "SNMP-MIB Changes" to "Interface Changes" chapter. • Updates "Behavioral Changes" and "Deprecated Features" to account for MIB object deprecation. • Modifies content to describe as the WebGUI feature is currently supported. • Restores missing content in New Features chapter. • Moves 8.3.0M1 chapter after Interface changes chapter.
November 2019	• Adds trace tool limitations to "Trace Tools" caveats. • Adds VLAN tagging caveat to "Virtual Network Function (VNF) Caveats."
December 2019	• Updates for the S-Cz8.3.0m1p2 release. • Corrects MSRP Supported Platforms. • Updates Resolved Known Issues table.
February 2020	• Adds telephone-event to supported codecs list for VNF
March 2020	• Updates for the S-Cz8.3.0m1p7 release.

June 2020	• Updates for the S-Cz8.3.0m1p8 release. • Moves defect 22322673 to Resolved Known Issues list • Updates Transcoding Support table for EVS
July 2020	• Updates "Virtual Machine Requirements" with new DPDK version • Updated for S-Cz8.3.0m1p9.
August 2020	• Removes SIP/SIPI feature description because it is not supported in this product.
November 2020	• Updates with cloud infrastructure information from Installation Guide • Clarifies "Linux version" is actually Linux kernel version
December 2020	• Updates the "Upgrade Caveats" with warning about disabling authentication-over-ipsec.
June 2021	• Adds MSRP and Transcoding caveats. • Updates the Known Issues table. • Adds caveat on toggling sip-interfaces with TCP.
August 2021	• Adds media policing caveat

1

Introduction to S-Cz8.3.0

The Oracle® Enterprise Session Border Controller *Release Notes* provides the following information about S-Cz8.3.0 release:

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

Supported Platforms

The Oracle® Enterprise Session Border Controller can run on a variety of physical and virtual platforms. It can also be run in public cloud environments. This section lists all supported platforms and high level requirements.

Supported Physical Platforms

The Oracle® Enterprise Session Border Controller can be run on the following hardware platforms.

Acme Packet Platforms

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

Supported Virtual Platforms (and Public Clouds)

The Oracle® Enterprise Session Border Controller can be run on the following virtual platforms.

Supported Hypervisors

Oracle supports installation of Oracle® Enterprise Session Border Controller on the following hypervisors:

- KVM: Linux kernel version 3.10.0-123 or later, with KVM/QEMU (2.9.0_16 or later) and libvirt (3.9.0_14 or later)

- VMware: vSphere ESXi Version 6.x or later (Version 6.5 or later is recommended)
- XEN: Release 4.4 or later
- Microsoft Hyper-V: Microsoft Server 2012 R2 or later

OpenStack Compatibility

Oracle distributes Heat templates for the Newton and Pike versions of OpenStack. Use the Newton template when running either the Newton or Ocata versions of OpenStack. Use the Pike template when running Pike or a later version of OpenStack.

Supported Public Cloud Platforms

In S-Cz8.3.0 the Oracle® Enterprise Session Border Controller can be run on the following public cloud platforms. For more information, see "New Features".

- Oracle Cloud Infrastructure (OCI)

Shape	OCPUs/ VCPUs	vNICs	Tx/Rx Queues	Max Forwarding Cores	DoS Protection
VM.Standard 1.2	2/4	2	2	1	N
VM.Standard 1.4	4/8	4	2	2	Y
VM.Standard 1.8	8/16	8	2	2	Y
VM.Standard 1.16	16/32	16	2	2	Y
VM.Standard 2.2	2/4	2	1	2	N
VM.Standard 2.4	4/8	4	1	2	Y
VM.Standard 2.8	8/16	8	1	2	Y
VM.Standard 2.16	16/32	16	1	2	Y

- Amazon Web Services (EC2)

Shape	vCPUs	Memory (GB)	Max NICs
c4.xlarge	4	7.5	4
c4.2xlarge	8	15	4
c4.4xlarge	16	30	8
c4.8xlarge	32	60	8
m4.xlarge	4	16	4
m4.2xlarge	8	32	4
m4.4xlarge	16	64	8

- Microsoft Azure
  Azure size types include:
  - F(x)—Does not support premium storage
  - FS(x)—Supports premium storage

- FS(x)_v2—Supports premium storage and hyperthreading.

This following tables lists the Azure instance sizes that you can use for the E-SBC. The selection of a Azure instance sizes with less than 8 NICs may require that you use the E-SBC interface mapping tools to adjust your interface to MAC address mapping.

> **Note:**
>
> The E-SBC does not support Data Disks deployed over any Azure instance sizes.

Size (F series)	vCPUs	Memory	Max NICs
Standard_F4	4	8	4
Standard_F8	8	16	8
Standard_F16	16	32	8

Size (Fs series)	vCPUs	Memory	Max NICs
Standard_F4s	4	8	4
Standard_F8s	8	16	8
Standard_F16s	16	32	8

Size	vCPUs	Memory	Max NICs
Standard_F8s_v2	8	16	4
Standard_F16s_v2	16	32	4
Standard_F32s_v2	32	64	8

Virtual Machine Requirements

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-Cz8.3.0 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.

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 / 5	mlx5	NA	M	M

- W - wancom (management) interface
- M - media interface
- NA - not applicable

CPU Core Resources

The E-SBC S-Cz8.3.0 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 (for example, qemu), Oracle recommends that you set the deployment to pass the full set of host CPU features to the VM.

DPDK Reference

The E-SBC relies on DPDK for packet processing and related functions. You may reference the Tested Platforms section of the DPDK release notes available at https://

doc.dpdk.org. This information can be used in conjunction with this Release Notes document for you to set a baseline of:

- CPU
- Host OS and version
- NIC driver and version

> **Note:**
>
> Oracle only qualifies a specific subset of platforms. Not all the hardware listed as supported by DPDK is enabled and supported in this software. You must use this document in conjunction with DPDK release notes to gain a full picture of supported devices.

The DPDK version used in this release is:

- 17.11.4
- 18.11 (starting in S-Cz8.3.0M1)

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 supports only one vSBC instance
- Do not configure transcoding cores for software-based transcoding when using a PCIe media card.

Oracle Communications Session Router Recommendations for Netra and Oracle Servers

Oracle recommends the following resources when operating the OCSR, release S-Cz8.3.0 over Netra and Oracle Platforms.

Hardware recommendations for Netra Server X5-2

Processor	Memory
2 x Intel Xeon E5-2699 v3 CPUs	32GB DDR4-2133

Hardware recommendations for Oracle Server X7-2

Processor	Memory
2 x 18-core Intel Xeon 6140	32GB DDR4 SDRAM

Image Files and Boot Files

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

> **Note:**
>
> In S-Cz8.3.0, 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: `nnSCZ830.bz`
- Bootloader file: `nnSCZ830.boot`

For Virtual Machines

This S-Cz8.3.0 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:

- `nnSCZ830-img-vm_ovm.ova`—Open Virtualization Archive (.ova) distribution of the SBC VNF for Oracle (XEN) virtual machines and Amazon EC2 .
- `nnSCZ830-img-vm_kvm.tgz`—Compressed image file including SBC VNF for KVM virtual machines and Oracle Cloud Infrastructure (OCI).
- `nnSCZ830-img-vm_vmware.ova`—Open Virtualization Archive (.ova) distribution of the SBC VNF for ESXi virtual machines.
- `nnSCZ830-img-vm_vhd.tgz`—Compressed image file including SBC for Hyper-V virtual machine on Windows and Azure.
- `nnSCZ830_HOT.tar.gz`—The Heat Orchestration Templates used with OpenStack.

Each virtual machine package includes:

- 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*.

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.

Upgrade Information

Supported Upgrade Paths

The S-Cz8.3.0 release supports the following paths for in-service software upgrades and rollbacks on existing Enterprise Session Border Controller installations.

- S-Cz8.2.0p2 to S-Cz8.3.0
- E-Cz8.1.0m1p11 to S-Cz8.3.0

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.

Remote access to /boot filesystem

For 8.4 and later, only the local administrator account (i.e. logging in as ‘admin’) will be able to write files into /boot via SFTP. Supplementary administrators (e.g. TACACS+/RADIUS users with administrative privileges) do not have write access via SFTP.

Oracle recommends you use of /code/images directory as the storage area for system bz images, instead of /boot. This is supported on all platforms as an alternative to /boot, except for systems which are configured in FIPS mode.FIPS requires that the file be written to /boot only. This change is compatible with FIPS operation, as the local admin account is already designated for use by the “FIPS Security Officer”.

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.

Upgrade and Downgrade Caveats

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

Reactivate License Key Features

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-

Cz8.3.0, 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. If FIPS mode is enabled, you cannot edit the boot file name when upgrading from E-CZ7.5.0 to E-CZ8.3.0 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-Cz8.3.0, 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-Cz8.3.0 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 or E/SCz8.2.0.

If you change any local account passwords after upgrading to S-Cz8.3.0, then you attempt to downgrade to the earlier release, local authentication does not succeed and the system becomes inaccessible.

Oracle recommends that you do not change any local account passwords after upgrading to S-Cz8.3.0 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-Cz8.3.0, downgrading is not affected.

> ⚠ **Caution:**
>
> If you change the local passwords after you upgrade to S-Cz8.3.0, and then later want to downgrade to a previous release, reset the local user passwords with the following procedure while running the newer version, before attempting the downgrade.

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-Cz8.3.0, 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.

Errors for authentication-over-ipsec

When upgrading from a previous release to S-Cz8.3.0m1p7 or later, the **authentication-over-ipsec** attribute of the **authentication** element is enabled by default. This may cause **verify-config** to repot the error:

```
ERROR: authentication-over-ipsec is enabled, but x.x.x.x tacacs server
does not match any of the security-policy's remote-ip-addr-match/mask subnet
```

To remove these errors, set **authentication-over-ipsec** to disabled.

Feature Entitlements

You enable the features that you purchased from Oracle, either by self-provisioning using the **setup entitlements** command, or installing a license key at the **system, license** configuration element.

This release uses the following self-provisioned entitlements and license keys to enable features.

The following table lists the features you enable with the **setup entitlements** command.

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

Encryption for Virtual SBC

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 8.3 From Previous Releases

When upgrading from a previous release to S-Cz8.3.0, 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 [1] • 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
• Virtual Platforms (with 1+ transcoding core)	• AMR • AMR-WB • EVS • G729 • G729A • iLBC • Opus • SILK • 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.

[1] Hardware-based EVS transcoding is supported for decode-only.

Coproduct Support

The following products and features run in concert with the Oracle® Enterprise Session Border Controller (E-SBC) for their respective solutions. Contact your Sales representative for further support and requirement details.

Oracle Communications Enterprise Operations Manager

This release can interoperate with the following versions of the Oracle Enterprise Operations Monitor:

- 4.0.0
- 4.1.0

Oracle Communications Session Delivery Manager

This release can interoperate with the following versions of the Oracle Communications Session Delivery Manager:

- 8.1 and later

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-Cz8.3.0, as a device in the Device Manager.

Oracle Communications Session Router

The E-SBC supports the Oracle Communications Session Router.

Pooled Transcoding

This release acting as an A-SBC can interoperate with T-SBCs on the following hardware/software combinations :

- Acme Packet 4500: E-CZ7.5.0
- Acme Packet 4600: S-CZ8.1.0, S-CZ8.2.0, S-CZ8.3.0
- Acme Packet 6300: S-CZ8.1.0, S-CZ8.2.0, S-CZ8.3.0
- Acme Packet 6350: S-CZ8.1.0, S-CZ8.2.0, S-CZ8.3.0
- Virtual Platforms with Artesyn SharpMedia™: S-CZ8.2.0, S-CZ8.3.0

This release acting as a T-SBC can interoperate with A-SBCs on the following hardware/software combinations:

- Acme Packet 4500: E-CZ7.5.0
- All other platforms supported on the following releases: S-Cz8.1.0, S-Cz8.2.0, S-Cz8.3.0

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_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
- 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. TLS 1.0 is planned to be deprecated in the next release.

Documentation Changes

The following information lists and describes the changes made to the Oracle® Enterprise Session Border Controller (E-SBC) documentation set for S-Cz8.3.0.

MSRP

The "RCS Services" chapter is added to the *ACLI Configuration Guide* to explain MSRP support, which is new to Enterprise.

SIP ISUP Interworking using HMR

The information used to explain how to configure HMRs within the context of SIP ISUP interworking is moved from the SIP chapter of the *ACLI Configuration Guide* to the *HMR Guide*.

RFC2833 to KPML Interworking

Information on RFC2833 to KPML Interworking is now centralized in the *DTMF Interworking* chapter of the *ACLI Configuration Guide*. A former section on this subject in the *SIP* chapter is removed.

Transcoding Resources

The Transcoding chapter has been reorganized to clearly present the three types of transcoding resources. See the *Transcoding* chapter in the *ACLI Configuration Guide*.

Behavioral Changes

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

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-Cz8.3.0 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.)

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-Cz8.3.0 and later, apEnvMonVoltageStatusValue in the ap-env-monitor.mib file is not supported. Voltage can still be monitored through the ACLI **show voltage** command.

Patches Included in This Release

The following information assures you that when upgrading, the S-Cz8.3.0 release includes defect fixes from neighboring patch releases.

Baseline

Cz8.2.0p3 is the patch baseline, which is the most recent build from which Oracle created S-Cz8.3.0.

Neighboring Patches Also Included

- S-Cz8.1.0m1p11
- E-Cz7.5.0p13
- E-Cz8.0.0p5

Supported SPL Engines

The S-Cz8.3.0 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-Cz8.3.0 release.

- The S-Cz8.3.0 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-Cz8.3.0, the OCSBC gains support for:

- Telephony fraud prevention

2

S-Cz8.3.0m1

The following topics provide descriptions, explanations, and configuration information for the contents of Maintenance Release S-Cz8.3.0m1. Unless otherwise stated, requirements and other release information is identical to S-Cz8.3.0 GA, noted in the first chapter of this document.

Patches Included in This Release

The following information assures you that when upgrading, the S-Cz8.3.0m1 release includes defect fixes from neighboring patch releases.

Baseline

The patch baseline is S-Cz8.3.0p8, the most recent build from which Oracle created S-Cz8.3.0m1.

Neighboring Patches Also Included

- E-Cz8.1.0m1p12
- E-Cz7.5.0p15
- E-Cz8.0.0p6

Virtual Machine Requirements for Release S-Cz8.3.0m1

DPDK Reference

The S-Cz8.3.0m1 release supports the DPDK version 18.11.2.

Upgrade Information

Supported Upgrade Paths

The S-Cz8.3.0 release supports the following paths for in-service software upgrades and rollbacks on existing Enterprise Session Border Controller installations.

- S-Cz8.2.0p4 to S-Cz8.3.0
- E-Cz8.1.0m1p11 to S-Cz8.3.0

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.

Documentation Changes

The following books have been updated for S-Cz8.3.0m1:

- Oracle Enterprise Session Border Controller ACLI Configuration Guide
- Oracle Enterprise Session Border Controller Web GUI User Guide

The following information lists and describes the changes made to the Oracle® Enterprise Session Border Controller (E-SBC) documentation set for S-Cz8.3.0m1.

My Oracle Support

Each book in the Oracle® Enterprise Session Border Controller documentation set now contains the "My Oracle Support" topic. This topic contains information on contacting product support, accessing emergency help in the case of a critical emergency, and locating product documentation.

ACLI Reference Guide

The A-M section of the *ACLI Reference Guide* includes the following new elements.

- Authentication Profile
- HTTP Client
- HTTP Server

> **Note:**
>
> These elements are reserved for future use.

Web GUI User Guide

The contents of the *Web GUI User Guide* are significantly revised to reflect the major update to the look and behavior of the Web GUI for S-Cz8.3.0m1.

New Features

The S-Cz8.3.0m1 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.

SIP Header Automation for Microsoft Teams

The E-SBC can manipulate SIP message headers in the format required by Microsoft Teams, rather than with custom Header Manipulation Rules. The following parameters are used for this function:

- **session-agent**, **ping-response**
- **realm-config**, **teams-fqdn-uri**
- **realm-config**, **sdp-active-only**

See the Configuring the Oracle ESBC to Microsoft Teams Direct Routing Media Bypass - Enterprise Model Document for details.

SIP to SIP-I Interworking Enhancement

Oracle plans to enhance SIP to SIP-I interworking over the course of several releases. For the S-Cz8.3.0m1 release, this interworking now supports populating of IAM parameters based on SIP INV, support for REL/RLC messages, reason code mapping from 4xx, 5xx, 6xx final responses into REL and vice versa, support for supplementary services, and support for parsing of SPIROU.

See "SIP ISUP Interworking" in the *ACLI Configuration Guide*.

Registration Event Subscription Counters

This release provides new counters for registration event subscriptions.

See "SIP Registration Event Package Support" in the *ACLI Configuration Guide*.

HA Deployments over Oracle Cloud Infrastructure

This release supports HA deployments over Oracle Cloud Infrastructure (OCI).

See the *Platform Preparation and Installation Guide*.

MSRP Statistics

This release provides MSRP byte and packet counters at the end of each MSRP call.

See "MSRP Statistics" in the *ACLI Configuration Guide*.

IMS-AKA Subscriber Support

The OCSBC supports up to 400,000 IMS-AKA subscribers, but is dependent on configuration. For example, Oracle recommends at least 2 forwarding cores and 52GB to support 400,000 subscribers. In addition, the OCSBC allocates resources for IMS-AKA based on your setting for the IMS-AKA endpoint entitlement. This means that you must also set the entitlement prior to IMS-AKA operation so that the system correctly allocates resource utilization.

Thresholds to consider when you set the entitlement include:

- 1 Forwarding core:
  - Less that 8GB memory support only 500 IMS-AKA subscribers
  - 8GB memory supports 48,000 IMS-AKA subscribers
  - 10GB memory supports 80,000 IMS-AKA subscribers
  - 16GB memory supports 104,000 IMS-AKA subscribers
- 2 Forward cores:
  - 16GB memory supports 112,000 IMS-AKA subscribers
  - 20GB memory supports 144,000 IMS-AKA subscribers
  - 24GB memory supports 176,000 IMS-AKA subscribers
  - 32GB memory supports 240,000 IMS-AKA subscribers
  - 48GB memory supports 368,000 IMS-AKA subscribers
  - 52GB memory supports 400,000 IMS-AKA subscribers

See "IMS Support" in the *ACLI Configuration Guide*.

OCSR Platform Support

The OCSR is supported over the X8-2 platform, beginning with version S-cZ8.3.0m1p2.

See "Oracle Server X8-2 Platform Preparation" in the *Platform Preparation and Installation Guide*.

Interface Changes

The following topics summarize ACLI, SNMP, HDR, Alarms, and RADIUS changes for S-Cz8.3.0m1. The additions, removals, and changes noted in these topics occurred 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-Cz8.3.0m1 release.

Command	Description
show sipd status	This command now displays counters for SIP registration event subscriptions.
request collection	This command now accepts msrp-stats as a collection-object value.

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-Cz8.3.0m1 release.

Elements Reserved for Future Use

The following table lists and describes new configuration elements that display in the S-Cz8.3.0m1 release, but are reserved for future use.

New Elements	Description
authentication-profile	For creating an authentication scheme profile. Other configurations, such as HTTP Client and HTTP Server, require the authentication profile.
http-client	For providing a way for the E-SBC to communicate with a remote server.
http-server	For provisioning the E-SBC for mid-call updates.

SIP to SIP-I Interworking

This table lists and describes new configuration elements that display in the S-Cz8.3.0m1 release.

New Elements	Description
session-router, **session-translation**, **rules-isup-cdpn**	Manipulates the ISUP Called Party Number parameter
session-router, **session-translation**, **rules-isup-cgpn**	Manipulates the ISUP Calling Party Number parameter
session-router, **session-translationrules-isup-gn**	Manipulates the ISUP Generic Number parameter
session-router,**session-translation**, **rules-isup-rdn**	Manipulates the ISUP Redirecting Number parameters
session-router,**session-translation**, **rules-isup-ocn**	Manipulates the ISUP Original Called Number
session-router,**sip-isup-profile**, **isup-version**	Adds the spirou value to the **isup-version** parameter
session-router,**sip-isup-profile**, **country-code**	Specifies the text string to use for country code interworking
session-router,**sip-isup-profile**, **portability-method**	Set this parameter to **concatenate** if you want to perform interworking for Number Portability Support within the IAM

MSRP Statistics

This table lists and describes new configuration elements that display in the S-Cz8.3.0m1 release.

Elements	Description
system-config, **collect**, **group-settings**	Adds msrp-stats value to group-name parameter

SIP Header Automation for Microsoft Teams

This table lists and describes new configuration elements that display in the S-Cz8.3.0m1p4 release.

Elements	Description
session-agent, **ping-response**	Reserved for use with Microsoft Teams only.
realm-config, **teams-fqdn-uri**	Reserved for use with Microsoft Teams only. **Note:** This parameter uses the hostname configured under **network-interface**.
realm-config, **sdp-active-only**	Reserved for use with Microsoft Teams only.

SNMP/MIB Changes

This section summarizes the SNMP/MIB changes that appear in the Oracle Communications Session Border Controller version S-Cz8.3.0m1.

MIB Changes for MSRP Statistics

A new object-group apSipMSRPStatsGroup will be added to ap-sip.mib for the MSRP statistics.

Diameter

This section summarizes the accounting changes that appear in the Oracle Communications Session Border Controller version S-Cz8.3.0m1.

New Diameter Rf ACR AVPs

The following AVPs are available in "Acme-Packet-Specific-Extension-Rf AVP:"

- MSRP-Calling-Packets-Received
- MSRP-Calling-Octets-Received
- MSRP-Calling-Packets-Transmitted
- MSRP-Calling-Octets-Transmitted
- MSRP-Called-Packets-Received
- MSRP-Called-Octets-Received
- MSRP-Called-Packets-Transmitted
- MSRP-Called-Octets-Transmitted

Accounting

This section summarizes the accounting changes that appear in the Oracle Communications Session Border Controller version S-Cz8.3.0m1.

New RADIUS VSAs

- Acme-Extended-Attributes: The VSAs available are the following:
  - Acme-MSRP-Calling-Packets
  - Acme-MSRP-Calling-Octets
  - Acme-MSRP-Calling-Packets-Transmitted
  - Acme-MSRP-Calling-Octets-Transmitted
  - Acme-MSRP-Called-Packets
  - Acme-MSRP-Called-Octets
  - Acme-MSRP-Called-Packets-Transmitted
  - Acme-MSRP-Called-Octets-Transmitted

See "Acme-Extended-Attributes Explanation" in the *Accounting Guide* for more information.

HDR

This section summarizes the HDR changes that appear in the Oracle Communications Session Border Controller version S-Cz8.3.0m1.

New HDR Groups

This release adds the following new HDR groups. This group is documented in this release's *HDR Guide*.

- **msrp-stats**: displays identical information as **show msrp stats** CLI command.

Web GUI Changes

Ensure you are running releases prior to S-Cz8.3.0M1, or releases S-Cz8.3.M1p2 and later to experience supported WebGUI functionality.

3
New Features

The S-Cz8.3.0 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.

Cloud Platform Support - Microsoft Azure

This E-SBC software version supports deployment over the Microsoft Azure public cloud in Standalone mode.

See Cloud Platform Installation in the *Platform Preparation and Installation Guide*.

Cloud Platform Support - Amazon EC2

This E-SBC software version supports deployment over the Amazon EC2 public cloud in both Standalone and High Availability mode.

See Cloud Platform Installation in the *Platform Preparation and Installation Guide*.

Cloud Platform Support - OCI

This E-SBC software version supports deployment over the Oracle Cloud Infrastructure (OCI) public cloud in Standalone mode.

See Cloud Platform Installation in the *Platform Preparation and Installation Guide*.

Local Media Playback

The Oracle® Enterprise Session Border Controller (E-SBC) can generate media locally based on end station signaling, local media playback configuration, and other E-SBC configuration.
See Local Media Playback the *ACLI Configuration Guide*.

MSRP Support

The Oracle Enterprise Session Border Controller supports Message Relay Protocol (MSRP) sessions initiated by Session Description Protocol (SDP) messages exchanged through the Session Initiation Protocol (SIP) offer/answer model on all Enterprise platforms except the Acme Packet 1100 and the Acme Packet 3900. MSRP usage with SDP and SIP is described in Section 8 of RFC 4975, The Message Relay Protocol. The SBC functions as a Back-to-Back User Agent (B2BUA) for MSRP sessions, terminating incoming MSRP, proxying for the MSRP session originator, initiating outgoing MSRP to the endpoint peer, and providing Network Address Translation (NAT) services.

See the new RCS Services chapter in the *ACLI Configuration Guide*.

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

> **Note:**
>
> These optimization and performance enhancements were first introduced in S-Cz8.2.0 and apply to SBC components in this release as well.

Notifications for Certificate Expiration

The E-SBC supports setting an alarm when a TLS certificate is about to expire.

See Notifications for Certificate Expiration in the *ACLI Configuration Guide*.

Quad-Port 10GbE NIU

The Acme Packet 6350 supports the Quad 10 GbE Network Interface Unit (NIU). The Quad 10 GbE NIU contains four 10G interfaces to provide greater session scaling capacity and Packet Processing Module (PPM) support. The Quad 10 GbE NIU also includes an internal network processor to allow for more flexible traffic loading to the multi-core processor.

See "Acme Packet 6350" in the *Platform Preparation and Installation Guide*.

Rest API Enhancements

Version 1.1 of the REST API adds support for the following features:

- Discover the supported versions of the REST API (REST API)
- Execute an HA switchover (REST API, feature documentation)
- Load a Fraud Protection file into the running configuration (REST API, feature documentation)
- Load a Local Route Table file into the running configuration (REST API, feature documentation)
- Delete the current configuration (REST API)
- Retrieve the list of saved backup configuration files (REST API, feature documentation)
- Delete saved backup configuration files (REST API, feature documentation)
- Retrieve the list of supported metrics (REST API)
- Retrieve system metrics (REST API)
- Start, stop, or restart HDR collection (REST API, feature documentation)
- Get the current HDR collection status (REST API, feature documentation)
- Purge collected HDR files (REST API, feature documentation)

- Add a license (REST API, feature documentation)
- Delete a license (REST API, feature documentation)
- Retrieve system information like hardware, storage space, and version (REST API)
- Set product type and entitlements (REST API, feature documentation)

See the REST API documentation for more information.

RFC2833 and KPML Inter-working Function for Hairpin Calls

The E-SBC supports RFC 2833-KPML interworking scenarios that include forwarded calls that hairpin to an endpoint out the original interface. If the initial callee supports one of these digit encapsulation methods, and the caller and final callee support the other, the default E-SBC behavior of preferring RFC 2833 may block the KPML digit tranmission. You can configure the E-SBC to support interworking within these hairpin scenarios in the egress direction.
See RFC2833 and KPML Interworking the *ACLI Configuration Guide*.

Virtual Network Function Enhancements

This version of the E-SBC supports the following functionality on Virtual Network Function deployments:

- Comfort Noise Transcoding
- RTCP Generation

Advanced Media Termination

The Oracle® Enterprise Session Border Controller (E-SBC) supports VoIP calls through the browser-based, real-time communication known as Advanced Media Termination. Using W3C and IETF standards, Advanced Media Termination supports cross-browser video calls and data transfers, such as browser-based VoIP telephony and video streaming. Advanced Media Termination allows users to make and receive calls from within a web browser, relieving the need to install a softphone application. With Advanced Media Termination, the E-SBC can enable users to communicate concurrently with one or more peers through various browsers and devices to stream voice and data communications in real-time through a variety of web applications. Advanced Media Termination also supports communications through end-user clients such as mobile phones and SIP User Agents.
Advanced Media Termination supports clients:

- connected to networks with different throughput capabilities.
- on variable media quality networks (wireless).
- on firewalled networks that do not allow UDP.
- on networks with NAT or IPv4 translation devices using any type of mapping and filtering behaviors (RFC 4787).

The E-SBC now supports Advanced Media Termination media handling. When deployed with an associated Advanced Media Termination signaling application receiving Advanced Media Termination signaling from endpoints (using SIP over Websockets or JSON over Multiple Transports signaling), this combination allows users to communicate concurrently with one or more peers through various browsers and devices to stream voice and data communications in real-time through a variety of web applications, as well as end-user clients such as mobile phones and SIP User Agents. Finally, the E-SBC can interwork between Advanced Media Termination media and more traditional VoIP media, allowing customers to connect Advanced Media Termination endpoints to legacy VoIP systems and the PSTN.

Specifically, the E-SBC supports the following services and functions for Advanced Media Termination.:

- ICE-STUN (Lite mode) - Interactive Connectivity Establishment - Session Traversal Utility for NAT (ICE-STUN) enables an Advanced Media Termination client to perform connectivity checks. Use ICE to provide several STUN servers to the browser by way of the application. ICE processing chooses which candidate to address. Other benefits include support for IPv4, load balancing, and redundancy. ICE-STUN support requires configuring an **ice-profile** and specifying the profile in **realm-config**. See "Configure ice-profile" and "Configure Advanced Media Termination in realm-config."
- RTP-RTCP multiplexing - Enables Real-Time Protocol (RTP) and Real-Time Control Protocol (RTCP) packets to use the same media port numbers. RTP is used for real-time multimedia applications, such as internet audio and video streaming, VoIP, and video conferencing. RTCP is used to monitor data transmission statistics and QoS, and helps to synchronize multiple streams. RTP-RTCP support requires enabling **rtcp-mux** in **realm-config**. See "Configure Advanced Media Termination in realm-config."
- SIP services including codec renegotiation, late media, early media, PACK interworking, attended and unattended call transfer, call forking, music on hold, transcoding, and High Availability.

> **Note:**
>
> The E-SBC Advanced Media Termination feature supports Advanced Media Termination media handling only and does not support SIP over WebSocket or JSON signaling. For most Advanced Media Termination use cases involving the E-SBC, you need an associated Advanced Media Termination signaling application to convert SIP over Websocket or JSON signaling to standard SIP signaling. See "Advanced Media Termination Support" 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 S-Cz830p7 and later.

Multiple Contact Handling in Redirect Action for LRT

When performing a redirect action triggered by local policy lookups, the Oracle® Enterprise Session Border Controller (E-SBC) typically issues a 305 (Use Proxy) message with a single contact derived from the local policy. In some cases, however, it is preferred to issue a 300 (Multiple Choices) message and provide multiple contacts, providing the endpoint with, for example, fallback contacts. For these scenarios, you can configure the E-SBC with a **sip-interface** option that supercedes the lookup configuration's compliance with the RFC 3261 standard for issuing a proxy, and respond based on the number of local policy contacts.

See "Session Routing" in the *ACLI Configuration Guide*.

4
Interface Changes

The following topics summarize ACLI, SNMP, HDR, Alarms, and RADIUS changes for S-Cz8.3.0. 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-Cz8.3.0 release.

There are no command changes or additions in this release.

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-Cz8.3.0 release.

RCS Services (MSRP)

New Parameters	Description
media-manager, **media-policy**, **rtp-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**	Enables the system to negotiate Connection Establishment for Media Anchoring (CEMA) support with parties in a given realm.
media-manager, **tcp-media-profile**, **msrp-sessmatch**	Determines whether or not the URI comparison of the To-Path header in the MSRP messages received from the respective realm includes the authority part.
media-manager, **tcp-media-profile**, **msrp-message-size-enforce**	Enables the system to reject messages that exceed the negotiated maximum size or to stop file transfers that exceed the maximum negotiated size.
media-manager, **tcp-media-profile**, **msrp-message-size**	Sets the maximum size negotiated for MSRP messages.
media-manager, **tcp-media-profile**, **msrp-message-size-file**	Sets the maximum size negotiated for the MSRP file transfer.

Advanced Media Termination Features

New Parameters	Description
media-manager, **realm-config**, **ice-profile**	Specifies ICE-STUN Lite mode (Interactive Connectivity Establishment - Session Traversal Utility for NAT) support that enables a WebRTC client to perform connectivity checks, and provide several STUN servers to the browser.
media-manager, **realm-config**, **rtcp-mux**	Enables RTCP multiplexing support for monitoring data transmission statistics and QoS, and synchronizing multiple data streams.
security, **media-security**, **dtls-srtp-profile**	Defines the key exchange and DTLS handshake for a media session, the role the SBC negotiates when offered alternatives, and the crypto suite that you want to use. Enter the name of the **dtls-srtp-profile** in the **webrtc-profile**.

Interworking Features

New Parameters	Description
sip-isup-profile, **iwf-for-183**	Instructs the OCSBC to exclude interworking of 183 messages to ACMs during SIP to ISUP interworking.
session-agent, **kpmlRFC2833-iwf-on-hairpin**	Enables the OCSBC to present the correct digit encapsulation (KPML or RFC2833) when hairpinned back to the original interface.
sip-interface, **kpmlRFC2833-iwf-on-hairpin**	Enables the OCSBC to present the correct digit encapsulation (KPML or RFC2833) when hairpinned back to the original interface.

Ringback Features

New Parameters	Description
realm-config, **ringback-trigger**	Specifies the trigger upon which the OCSBC starts to play the configured ringback audio file. Parameters include: • disabled • 180-force • 180-no-sdp
realm-config, **ringback-file**	Specifies the audio file to play when initiated by the **ringback-trigger**.

SNMP/MIB Changes

This section summarizes the SNMP/MIB changes that appear in the S-Cz8.3.0 release.

Deprecated SNMP Statistics

apEnvMonVoltageStatusValue MIB objects have been deprecated.

5

Caveats and Known Issues

The following topics list 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 known issues in version S-Cz8.3.0. 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
31373813	If upgrading TO any of the following releases FROM any prior release and you have IPSEC or IMS-AKA enabled and are configured in an HA configuration, an In-Service upgrade is not supported. • S-Cz8.1.0m1p23 • S-Cz8.1.0m1p24 • S-Cz830m1p5 • S-Cz830m1p6 • S-Cz830m1p7 • S-Cz830m1p8 You must upgrade both systems in the HA pair and perform a simultaneous reboot for HA synchronization to work in the above upgrade scenario. This also applies to a downgrade FROM the above releases TO prior releases. For example, if you are running S-CZ8.1.0M1P23 and decide to downgrade to S-Cz8.1.0M1P21, you will need to install the prior version (Cz8.1.0M1P21) on both systems in the HA pair and execute a simultaneous reboot. If you are already running one of the above releases and are upgrading between them, this step is unnecessary and in-service upgrades are supported.	3	SCZ830m1p5

ID	Description	Severity	Found In
30611784	When executing a GET ALL procedure using the REST interface, the OCSBC fails over. The GET method does not produce results until the Standby server becomes Active. Customer Impact: Customer will not be able to get any response(including 200 empty response) from OCSBC when he tries to retrieve configuration of any element using GET method.	3	SCZ830m1p2
29403076	When generating HDR reports and SNMP output on resource utilization that includes threads, the OCSBC omits the thread name, leaving the applicable field and OID empty.	3	SCZ810M1P9
29881449	The DSP used by the OCSBC has a vendor firmware defect that causes failures with the T.38 codec. If you are using the T.38 codec, you may experience minimal media losses on those calls. This problem may also, however, cause the OCSBC to reboot. Oracle is acquiring a firmware fix from the DSP vendor.	3	SCZ810m1p9
30330778	The OCSBC cannot forward a call that uses a TEL-URI and includes the routing number (rn) parameter. Depending on your routing configuration, the OCSBC may reject these call with a 404 Not Found/No Route to Destination. The OCSBC forwards these portability scenarios properly when they present an R-URI.	1	SCZ740m2p4;810m1p18
29846828	The OCSBC stops generating registration refreshes after 12 hours for Surrogate Agents. After a reboot, the OCSBC attends to registration and refreshes correctly using the new Call ID for 12 more hours.	2	ECZ810m1p8

ID	Description	Severity	Found In
30444535	When configured for the minimum TCP disconnect time, the default for network-parameters, the OCSBC takes an unexpectedly long time before attempting to create a socket and connect. When using the defaults to create and connect using the minimum amount of time, this process takes 18 seconds instead of 9.	3	
30158557	Under high media loads that include AMR/AMR-WB to PCMA transcoding, the 10G port on the Acme Packet 6300 is experiencing packet loss and, therefore media MOS degradation.	2	SCZ810m1p16
29862440	When transcoding from T.38 to G711FB, the OCSBC includes mutiple (for example 2) m-lines in the SDP when there are multiple (for example 2) c-lines in the source SDP. This happens even if you have set the fax-single-m-line parameter in the applicable codec-policy to present a single m-line. Workaround: Configure an ingress HMR to remove all but 1 c-line from the incoming SDP.	3	SCZ740m1p8
30364057	Do not use DNS for multiple services on the OCSBC simultaneously. DNS service operates on the OCSBC normally when you configure it for a single purpose. When you configure it for multiple purposes, however, lookups do not complete correctly. Workaround: An example of this would be configuring DNS for both PCRF and ENUM services. You can mitigate this issue by configuring the local routing table with ENUM lookups.	3	SCZ830p7
30612465	On Virtual platforms, the OCSBC is not forwarding traffic transcoded to EVS or Opus codecs if you have configured the applicable policy with a forced ptime of 60ms.	3	SCZ830m1p2
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

ID	Description	Severity	Found In
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
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
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
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
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
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

ID	Description	Severity	Found In
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
29546194	The SBC is unable to maintain 400 or more TSM/DTLS tunnels.	2	SCZ830

Resolved Known Issues

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

ID	Description	Severity	Found In	Fixed In
28157960	When setting up a SIPREC session, the SBC sets up 1-way audio if the far end offers an odd port number in the m line.	2	SCZ800	SCZ830m1p8
29779932	The OCSBC uses a Diffie Hellman algorithm that conflicts with that of the 10.4 Solaris SFTP server. As a result, both CDR and HDR transfers to these servers fail. Do not use the Solaris 10.4 SFTP server with the OCSBC.	1	SCZ830p7	SCZ830m1p5
30611784	When executing a GET ALL procedure using the REST interface, the OCSBC fails over. The GET method does not produce results until the Standby server becomes Active. Customer Impact: Customer will not be able to get any response(including 200 empty response) from OCSBC when he tries to retrieve configuration of any element using GET method.	3	SCZ830m1p2	SCZ830m1p5
29931732, 31089996	The embedded communications monitor probe does not send IPv6 traffic to the Oracle Communications Operations Monitor's mediation engine.	3	SCZ800	SCZ830m1p9

ID	Description	Severity	Found In	Fixed In
31039820	When mid-call Lawful Intercept is enabled, and the SBC has not started intercepting particular sessions, those sessions will not be replicated on the standby. If a switchover occurs, affected calls could be dropped.	3	SCZ830m1p2	SCZ830m1p9
31188777	The SBC does not provide support for P-Acme-Playback header when 'direction=both'.	3	SCZ830	SCZ830m1p9
30375697	Infrequently during race conditions, the number of SIP registration entries on the active and standby SBCs differs, with the standby SBC containing less entries. When this happens and a failover occurs, some endpoints are unable to receive calls until the endpoint re-registers. Increase Journal index size and optimize the Journal management code to avoid this.	2	S-Cz8.1.0m1p18	S-Cz8.1.0m1p18b
30544663	When a session add action is executed and the session is not found in the sipProxy, a new Sip Session and two Sip Dialogs are created and cross referenced and the buffer from the active is loaded. If the load fails, the update function exits and the SipSession and SipDialogs are left dangling and create a memory leak. Workaround: To avoid this memory leak, successfully load the buffer BEFORE creating the session and dialogs. Monitor the standby SBC's memory usage and reboot as needed.	3	S-Cz8.1.0m1	S-Cz8.1.0m1p18b

ID	Description	Severity	Found In	Fixed In

30498837	A sipd process crash occurs with a signature containing the following:
	`ZNSt8_Rb_treeISsSt4pairIKSs4SptrI10SipContactEESt10*_Select*1stIS5_ESt4lessIS sE SaIS5_EE11equal_rangeERS1_ (+ 0x67) - sp = 0x7f334938d380, ip = 0x1f1b117`
	The SBC can leak File Descriptors in cases where there are certain process errors. For example:
	`[MINOR] (0) Selector::do_select() - epoll_ctl(DEL, 409) failed with errno=9:Bad file descriptor)`
	This does not trigger proper closure of sockets. This is avoided by closing the socket that was opened and then setting an error identifying exact error code.
		2	S-Cz8.1.0m1p18	S-Cz8.1.0m1p18b

29403076	The "thread-event" and "thread-usage" HDR categories are displaying incorrectly due to MBCD and SIPD thread names not properly writing into the files and OID output. MBCD and SIPD now properly assign and pass the proper names.	3	S-Cz8.1.0m1p9	S-Cz8.1.0m1p18b
29633588	During certain configuration activities, the SBC restarts due to an issue caused by improper configuration steps being processed in the **sip-manipulation**, **header-rules**. The SBC now returns an error message stating "Invalid Selection" instead of failing.	3	S-Cz8.1.0m1p11	S-Cz8.1.0m1p18b

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	SCZ830	S-Cz830p6
28820258	On VNF 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	S-CZ830m1p2
	For Advanced Media Termination deployments using the 4600, 6300, 6350 platforms, the SBC is generating RTP and RTCP on the ports 20000 and 20001, instead of generating both on the same port 20000.	3	SCZ830	S-CZ830m1p2
29522609	Some calls that are configured to generate ring back tones result in one-way audio.	2	SCZ830	S-CZ830m1p2
29607573	The SBC is unable to successfully initiate a TCP connection to configured Diameter Accounting (Rf) servers.	2	SCZ830	S-CZ830m1p2
30114764	When presenting the content type for SPIROU during SIP to SIPI interworking, the SBC is displaying the text **base=spirou**. Based on relevant standards, it should display **base=itu-92+** as the content type.	4	S-CZ830m1	S-CZ830m1p2
30127762	When performing SIP to SIPI interworking, the SBC is not including an ISUP REL in the interworked body of its **400 Missing CSeq** message when it rejects applicable calls from the SIPI side.	4	S-CZ830m1	S-CZ830m1p2

ID	Description	Severity	Found In	Fixed In
30240798	The OCSBC closes connections when using some SFTP clients, including WinSCP and MOBA, to upload files over 200KB. Workaround - Use the Linux or Filezilla SFTP client when uploading files greater than 200k.	3	S-CZ830p6	S-CZ830m1p2
30289027	Azure does not always properly reset media interfaces after the OCSBC reboots. Instead, Azure sometimes tries to process a non-existent packet as soon as the OCSBC comes back up, resulting in a kernel panic. Workaround - If you experience a kernel panic after OCSBC reboot, stop and restart the vSBC from the Azure UI.	3	SCZ830	S-CZ830m1p2
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	SCZ830
29556215	The SBC does not send SIPREC data to a remote call server.	2	SCZ830	SCZ830p5
29608499	In all documents except for the Release Notes and Installation guide, the printed version of this release (S-Cz8.3.0) is incorrectly displayed as S-Cz8.2.0.	4	SCZ830	SCZ830p3
28539155	When operating as a VNF and using Mellanox interface cards, the OCSBC does not support ICMP over IPv6.	3	SCZ820	SCZ830

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

ID	Description	Severity	Found In	Fixed In
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
	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
21805139	RADIUS stop records for IWF calls may display inaccurate values.	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.

Media Policing

The Acme Packet 1100, 3900 and 4600 as well as all software-only deployments do not support any Media Policing configuration.

Toggling SIP Interfaces Running TCP

You must reboot the system any time you disable, then enable an active SIP interface that is using TCP.

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.
- 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 no support VLANs over SR-IOV interfaces.
- 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.
- 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
- T.38 FAX IWF
- 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.

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

These platforms do not support the MSRP feature set:

- Acme Packet 3900
- Acme Packet 1100

When running media over TCP (e.g., MSRP, RTP) on the same interface as SIP signaling, TCP port allocation between media and signaling may be incompatible.

- Workaround: Set the **sip-port**, **address** parameter to a different address than where media traffic is sent/received, the **steering-pool**, **ip-address** value.

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".

HA Deployment on Azure

HA deployments on Azure are not supported.

Graphical User Interface

When maximizing and minimizing the browser, the WEB GUI is not currently compensating correctly for display changes in tables that require scrolling. This can corrupt the display of tables in ESBC GUI management dialogs.

Simultaneous Use of Trace Tools

See "Trace Tools" caveat.

A

Deprecated Features

Oracle recommends that you review the following information about deprecated features and functions before using the S-Cz8.3.0 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
apEnvMonVoltageStatusEntry MIB object	The apEnvMonVoltageStatusEntry objects have been deprecated. Voltage monitoring is still available using the **show voltage** command in the ACLI.	SCZ8.3.0

Previous Deprecations

Feature	Description	Release Deprecated
Platforms	The S-Cz8.3.0 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-Cz8.3.0 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