Oracle® Communications Session Border Controller and Session Router
Release Notes

Release S-Cz8.4.0

ORACLE®

Oracle Communications Session Border Controller and Session Router Release Notes, Release S-Cz8.4.0

F30570-18

Contents

About this Guide

Revision History

1   Introduction to S-Cz8.4.0

2 New Features

3 Interface Changes

4 Caveats and Known Issues

About this Guide

The Oracle Session Border Controller (SBC) family of products are designed to increase security when deploying Voice over IP (VoIP) or Unified Communications (UC) solutions. Properly configured, Oracle's SBC family helps protect IT assets, safeguard confidential information, and mitigate risks—all while ensuring the high service levels which users expect from the corporate phone system and the public telephone network.

Documentation Set

The following table lists related documentation.

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 Session Border Controller (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.
Maintenance and Troubleshooting Guide	Contains information about SBC logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
MIB Reference Guide	Contains information about Management Information Base (MIBs), 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 SBC's accounting support, including details about RADIUS and Diameter accounting.

Document Name	Document Description
HDR Resource Guide	Contains information about the SBC's Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Administrative Security Essentials	Contains information about the SBC's support for its Administrative Security license.
SBC Family Security Guide	Contains information about security considerations and best practices from a network and application security perspective for the SBC 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.
FIPS Compliance Guide	Contains conceptual and procedural information for configuration using the tools and protocols required to manage call traffic on the SBC.
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 SBC.
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 section provides a revision history for this document.

Date	Revision
June 2020	• Initial release
June 2020	• Corrects product name in book title • Updates EVS/HW transcoding note • Updates Known Issue list for p1 • Updates ethernet controller list for virtual machines • Corrects format error in fixed known issues table
July 2020	• Updates Caveats and Limitations section • Updates SDM Version Support
Sept 2020	• Updates for release S-Cz8.4.0p2 • Updates Oracle Communications Session Monitor compatibility
Oct 2020	• Updates for S-Cz8.4.0p3 release. • Adds note in Co-Product Support section for new XSD requirement. • Removes SILK from Pooled Transcoding caveats list. • Adds conditional logging upgrade caveat.
Nov 2020	• Adds IKE caveat. • Notes behavioral changes with Acme-User-Class VSA. • Adds "Connection Failures with SSH/SFTP Clients" in the Upgrade and Downgrade Caveats
Dec 2020	• Removes Small Footprint VNF note. • Adds alarm on core config change in HA environments
March 2021	• Updates document, including "New Features" chapter and "Caveats and Known Issues" for S-Cz8.4.0p4 release. • Adds G.723 to vSBC list. • Adds MSRP and Transcoding caveats.
April 2021	• Updates the "New Features" topic for the S-Cz8.4.0p5 release. • Updates the "Known Issues" topic for the S-Cz8.4.0p5 release.

ORACLE®

Date	Revision
June 2021	• Adds STIR/SHAKEN feature development for S-Cz8.4.0p5 • Adds verify-config warnings • Updates Trace Tools caveat • Adds Note on upgrade path • Corrects an upgrade path • Updates "Upgrade and Downgrade Caveats" to remove "Conditional Logging With auth-invite Call Flows (401/407). • Updates the Known Issues table. • Includes additionally supported Azure machine sizes • Removes datapath limitation for virtual MSRP • Adds caveat on toggling sip-interfaces with TCP • Updates Upgrade Caveats with SSH authentication methods offered by SBC • Adds 'reset tacacs-stats' command • Adds S-Cz8.4.0p6 fixed diameter defects • Adds media policing caveat
August 2021	• Adds MS-Teams roaming new feature for S-Cz8.4.0p7 • Updates the "Configuration Assistant Operations" chapter in the *ACLI Configuation Guide* to reflect changes in the Configuration Assistant work flow for SC-z8.4.0p7.
October 2021	• Updates Known Issuses.
November 2021	• Updates Known Issues, Resolved Known Issues, and Caveats and Limitations. • Updates notes in Upgrade information section. • Adds new features for S-Cz840p8.
February 2022	• Adds caveat on performing acquire-config • Corrects ESXi version support • Adds entitlement changes during upgrade in upgrade checklist section. • Adds KI about IPv4 and IPv6.

Date	Revision
March 2022	• Removes H.323 signaling or H.323-SIP inter-working from Virtual Network Function (VNF) Limitations. • Adds KI about running SIPREC on the Acme Packet 4600. • Adds verify-config warning. • Adds strip-restored-sdp option in behavioral changes. • Adds Acme Packet Platform Monitoring Caveats. • Adds a resolved KI related to local-port-match. • Adds IPSec trunking tunnel caveat. • Adds content-length related behavioral change. • Updates Known Issues for S-Cz840p10.

1

Introduction to S-Cz8.4.0

The Oracle Communications Session Border Controller *Release Notes* provides the following information about S-Cz8.4.0 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 Communications Session Border Controller (OCSBC) 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 Communications Session Border Controller can be run on the following hardware platforms.

Acme Packet Platforms

The S-Cz8.4.0 version of the OCSBC supports the following platforms:

- Acme Packet 3900
- Acme Packet 4600
- Acme Packet 6100
- Acme Packet 6300
- Acme Packet 6350
- Virtual Platforms

The S-Cz8.4.0 version of the OCSR supports the following platforms:

- Acme Packet 4600
- Acme Packet 6100
- Acme Packet 6300
- Netra Server X5-2
- Oracle Server X7-2
- Oracle Server X8-2

- Virtual Platforms

Supported Private Virtual Infrastructures and Public Clouds

The OCSBC can be run on the following Private Virtual Infrastructures, which include private server/hypervisor platforms as well as private clouds based on architectures such as VMware or Openstack.

> **Note:**
>
> The OCSBC does not support automatic, dynamic disk resizing.

Supported Hypervisors for Private Virtual Infrastructures

Oracle supports installation of OCSBC 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 6.5 or later)
- XEN: Release 4.4 or later

Compatibility with OpenStack Private Virtual Infrastructures

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-Cz8.4.0 the OCSBC can be run on the following public cloud platforms. For more information, see "New Features".

- Oracle Cloud Infrastructure (OCI) - After deployment, you can change the shape of your machine by, for example, adding disks and interfaces. OCI Cloud Shapes and options validated in this release are listed in the table below.

Shape	OCPUs/ VCPUs	vNICs	Tx/Rx Queues	Max Forwarding Cores	DoS Protection
VM.Standard1.4	4/8	4	2	2	Y
VM.Standard1.8	8/16	8	2	2	Y
VM.Standard1.16	16/32	16	2	2	Y
VM.Standard2.4	4/8	4	2	2	Y
VM.Standard2.8	8/16	8	2	2	Y
VM.Standard2.16	16/32	16	2	2	Y

Networking using image mode [SR-IOV mode - Native] is supported on OCI. PV and Emulated modes are not currently supported.

- Amazon Web Services (EC2) - This table lists the AWS (ECs) instance sizes that apply to the OCSBC. Enhanced networking [SR-IOV mode – i82599 VF] is supported for the VM shapes listed below. ENA is not currently supported.

Instance Type	vCPUs	Memory (GB)	Max NICs
c4.xlarge	4	7.5	4
c4.2xlarge	8	15	4
c4.4xlarge	16	30	8
c4.8xlarge	36	60	8
m4.xlarge	4	16	4
m4.2xlarge	8	32	4
m4.4xlarge	16	64	8

- Microsoft Azure - Size types define architectural differences and cannot be changed after deployment.
  During deployment you choose a size for the OCSBC, based on pre-packaged Azure sizes. After deployment, you can change the detail of these sizes to, for example, add disks or interfaces. Azure presents multiple size options for multiple size types.

  For higher performance and capacity on media interfaces, use the Azure CLI to create a network interface with accelerated networking.

This following table lists the Azure instance sizes that you can use for the OCSBC.

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

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

> **Note:**
>
> v2 instances have hyperthreading enabled.

DPDK Reference

The OCSBC 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

- NIC firmware 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.

The DPDK version used in this release is:

- 19.11
- 19.11.2 (S-Cz8.4.0p2 and later)

Requirements for Machines on Private Virtual Infrastructures

A Virtual Session Border Controller (VSBC) 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 VSBC 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 for Private Virtual Infrastructures

The OCSBC 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 for Private Virtual Infrastructures

- Para-virtualized
- SR-IOV
- PCI Passthrough
- Emulated - Emulated is supported for management interfaces only.

Supported Ethernet Controller, Driver, and Traffic Type based on Input-Output Modes

The following table lists supported Ethernet Controllers (chipset families) and their supported driver that Oracle supports for Virtual Machine deployments. Reference the host hardware specifications, where you run your hypervisor, to learn the Ethernet controller in use. The second table provides parallel information for virtual interface support. Refer to the separate platform benchmark report for example system-as-qualified performance data.

For KVM and VMware, accelerated media/signaling using SR-IOV and PCI-pt modes are supported for the following card types.

Ethernet Controller	Driver	SR-IOV	PCI Passthrough
Intel 82599 / X520 / X540	ixgbe	M	M
Intel i210 / i350	igb	M	M
Intel X710 / XL710	i40e	M	M
Mellanox Connect X-4	mlx5	M	M

For PV mode (default, all supported hypervisors), the following virtual network interface types are supported. You can use any make/model NIC card on the host as long as the hypervisor presents it to the VM as one of these vNIC types.

Virtual Network Interface	Driver	W/M
Emulated	e1000	W
KVM (PV)	virtio	W/M
Hyper-V (PV)	NetVSC	M
VMware (PV)	VMXNET3	W/M

Emulated NICs do not provide sufficient bandwidth/QoS, and are suitable for use as management only.

- W - wancom (management) interface
- M - media interface

> **Note:**
>
> Accelerated media/signaling using SR-IOV (VF) or PCI-pt (DDA) modes are not currently supported for Hyper-V or XEN when running on Private Virtual Infrastructures.

CPU Core Resources for Private Virtual Infrastructures

The OCSBC S-Cz8.4.0 VNF requires an Intel Core i7 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.

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-Cz8.4.0 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

Hardware recommendations for Oracle Server X8-2

Processor	Memory
2x 24-core Intel Platinum 8260	32GB DDR4 SDRAM

Image Files and Boot Files

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

For Acme Packet Platforms

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

- Image file: `nnSCZ840.bz`

- Bootloader file: `nnSCZ840.boot`

For Virtual Machines

This S-Cz8.4.0 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:

- `nnSCZ840-img-vm_ovm.ova`—Open Virtualization Archive (.ova) distribution of the SBC VNF for Oracle (XEN) virtual machines and Amazon EC2 .

- `nnSCZ840-img-vm_kvm.tgz`—Compressed image file including SBC VNF for KVM virtual machines and Oracle Cloud Infrastructure (OCI).

- `nnSCZ840-img-vm_vmware.ova`—Open Virtualization Archive (.ova) distribution of the SBC VNF for ESXi virtual machines.

- `nnSCZ840_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.

For Oracle Platforms supporting the Session Router

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

- Image file: `nnSCZ840.bz`
- Bootloader file: `nnSCZ840.boot`

Image Files for Customers Requiring Lawful Intercept

Deployments requiring Lawful Intercept (LI) functionality must use the LI-specific image files. These image files are available in a separate media pack on MOS and OSDC. LI-specific image files can be identified by the "LI" notation before the file extension. For example, the inventory of files for the initial GA release is:

- `nnSCZ840-img-usb.LI.exe`

- `nnSCZ840-img-vm_kvm.LI.tgz`

- `nnSCZ840-img-vm_vmware.LI.ova`

- `nnSCZ840-img.LI.iso`

- `nnSCZ840.LI.bz`

All subsequent patches will follow naming conventions with the LI modifier.

Boot Loader Requirements

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

Setup Product

The following procedure shows how to setup the product. Once you have setup the product, you must setup entitlements. For information on setting up entitlements, see "Feature Entitlements".

> **Note:**
>
> The availability of a particular feature depends on your entitlements and configuration environment.

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 Communications 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 (OCSBC and OCSR)

Both the OCSBC and the OCSR support the following in-service (hitless) upgrade and rollback paths:

- S-CZ8.3.0m1p8 to S-CZ8.4.0

  > **Note:**
  >
  > If upgrading from S-CZ8.3.0m1p10, the only hitless path is to S-Cz8.4.0p5C.

- S-CZ8.2.0p3 to S-CZ8.4.0
- S-CZ8.1.0m1p25 to S-CZ8.4.0 - See consideration below
- S-CZ7.4.1m1p9 to S-CZ8.4.0
- S-CZ7.4.0m2p4 to S-CZ8.4.0

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

Consideration when Upgrading to S-Cz8.4.0

This consideration applies to deployments that do not use LI images or are not configured for LI.

Perform online upgrades from deployments running software versions S-Cz8.1.0m1p25 or earlier to S-Cz8.1.0m1p25 before upgrading to S-Cz8.4.0 if your deployments include High Availability configuration. Upgrades from these earlier versions may cause outages if you are receiving REGISTER messages with IMSI/IMEI headers during the upgrade.

High-level workaround steps, which skip the interim image, include:

1. Change the boot parameters of both HA OCSBCs to boot to S-Cz8.4.0.
2. Reboot the standby.
3. Wait for the standby to boot to S-Cz8.4.0.
4. Reboot the active.

After this procedure both the active and standby OCSBCs should be upgraded to S-Cz8.4.0 without any system or customer impact.

If you wish to revert to the older image:

1. Change the boot parameters of both HA OCSBCs to boot to your previous release.
2. Reboot the standby.
3. Wait for the standby to boot to S-Cz8.4.0.

ORACLE®

4. Reboot the active.

After this procedure both the active and standby OCSBCs should be downgraded to the original version.

Remote access to /boot filesystem

See the section on SFTP Access in the Behavioral Changes for important information related to file access that you may need during your upgrade.

Upgrade Checklist

Before upgrading the Oracle Communications 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 Communications 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 Communications Session Border Controller Release Notes for any caveats involving software upgrades.

7. Do not configure an entitlement change on the Oracle Communications Session Border Controller while simultaneously performing a software upgrade. These operations must be performed separately.

Upgrade and Downgrade Caveats

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

Web Server Config

During an upgrade to S-Cz8.4.0 where the former web-server-config element was enabled *and* no system-config configuration element existed, the web-server-config element will not be configured. This results in a non-enabled web server, as used by REST and WebGUI.

Workarounds include:

• Activate the **system-config** before the upgrade - or

• Configure the **http-server** after the upgrade.

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-Cz8.4.0, you must run the **setup product** command to re-activate the features that formerly depended on license keys.

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 OCSBC 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 or later, 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 software using the new encryption strength from version using the former strength until you are sure that you will not need to downgrade. If you do not change any local account passwords after upgrading to these newer version, downgrading is not affected.

> ⚠ **Caution:**
>
> If you change the local passwords after you upgrade to S-Cz8.4.0, 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 OCSBC first, and then force a switchover. Repeat steps 1-10 on the newly active OCSBC. During the procedure, the OCSBC powers down and you must be present to manually power up the OCSBC.

> ⚠ **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 OCSBC.

1. Log on to the console of the standby OCSBC 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 OCSBC.

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 OCSBC.

vSBC License Keys

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

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-Cz8.4.0, 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.

Connection Failures with SSH/SFTP Clients

If you upgrade and your older SSH or SFTP client stops working, check that the client supports the mimumum ciphers required in the `ssh-config` element. The current default HMAC algorithm is `hmac-sha2-256`; the current key exchange algorithm is `diffie-hellman-group-exchange-sha256`. If a verbose connection log of an SSH or SFTP client shows that it cannot agree on a cipher with the OCSBC, upgrade your client.

Authentication Methods

Prior to 8.4.0, the OCSBC offered three SSH authentication methods: `publickey`, `password`, and `keyboard-interactive`. 8.4.0 and later dropped support for the `password` method in favor of `keyboard-interactive`. The `keyboard-interactive` method offers a similar user experience to `password`, but it also supports two-factor authentication. If your SSH or SFTP client fails to connect after upgrading, confirm that your client uses the `keyboard-interactive` authentication method.

Update known_hosts File

While there are no usability changes to SSH and SFTP, the OCSBC will regenerate its SSH host certificate after upgrading to S-Cz8.4.0 from a previous version or downgrading from S-Cz8.4.0 to a previous version. Existing keys from prior releases will not work after the upgrade. To avoid warnings about mismatched fingerprints,

remove the old host keys from the known_hosts file of a system that wants to connect to the OCSBC.

Entitlement Configurations for MSRP on Virtualized Platforms

To support 500 or more MSRP sessions on virtualized SBCs, in some cases you must reconfigure the entitlements. When the existing entitlements show IMS-AKA Endpoints set to non-zero value, do the following:

1. With the **setup entitlements** command, set IMS-AKA Endpoints to 0.
2. Perform a system reboot.
3. With the **setup entitlements** command, set MRSP B2BUA sessions to a number greater than 499.

R226 Upgrades

When upgrading an OCSBC with the R226 entitlement enabled, you will first need to set the 0x01000000 bootflag during boot so that you can SFTP a boot image to the OCSBC.

Upgrading to S-Cz8.4.0p1 with IKEv1 or IKEv2 Tunnels

Problem Statement: Upgrading to S-Cz8.4.0p1 with IKEv1 or IKEv2 Tunnels from specific releases, listed below, can cause IPSec tunnels to fail. This procedure is not necessary if upgrading to S-Cz8.4.0p2 or above.

- S-Cz8.1.0m1p23
- S-Cz8.1.0m1p24
- S-Cz8.2.0p7
- S-Cz8.3.0m1p5
- S-Cz8.3.0m1p6
- S-Cz8.3.0m1p7
- S-Cz8.3.0m1p8
- S-Cz8.3.0m1p8A
- S-Cz8.3.0m1p8B
- S-CZ8.4.0

Impact: These tunnels do not automatically recover after the upgrade.

Work Around: To avoid this problem, you need to delete these tunnels before the upgrade as outlined in the procedure below.

1. If enabled, disable **x2-keep-alive** from the LI shell. (See procedures in LI documentation.)
2. Upgrade the Standby node to S-Cz8.4.0p1 .
3. Wait until the pair reaches HA state.
4. Configure the Active node to boot to S-Cz8.4.0p1. (Do not reboot this device yet.)

5. Delete tunnels on the Active node, which is still running the older software version, using one of the following commands from the CLI root.

```
security ipsec delete ike-interface <ike-interface IP address> all
```

```
security ipsec delete tunnel destIP <ipsec tunnels destination ip>
spi <inbound spi>
```

6. Ensure that tunnel(s) were deleted from both nodes. (If necessary run this command one more time for any new spi.)

```
show security ipsec sad <network interface name> detail
```

7. Reboot the Active node.

8. If the IKE interface is in INITIATOR mode, execute the **ping** command to the applicable IPSec endpoints on the newly Active (S-Cz8.4.0p1) node to establish new tunnels.
   If the IKE interface is in RESPONDER mode, have peers restart tunnels instead of executing the **ping** command.

9. Upon completion of boot cycle of the standby node, verify HA state and proper tunnel synchronization.

Two downgrade procedures are presented below.

Rollback after full Upgrade

1. HA pair is in highly available state with 840p1 version

2. Reboot Standby node with downgraded version

3. Wait until highly available state established

4. Delete tunnels on the Active node using one of the following commands from the CLI root.

```
security ipsec delete ike-interface <ike-interface IP address> all
```

```
security ipsec delete tunnel destIP <ipsec tunnels destination ip>
spi <inbound spi>
```

5. Ensure that tunnel(s) were deleted from both nodes. (If necessary run this command one more time for any new spi.)

```
show security ipsec sad <network interface name> detail
```

6. Reboot the Active node.

7. If the IKE interface is in INITIATOR mode, execute the ping command to the applicable IPSec endpoints on the newly Active (Downgraded) node to establish new tunnels.
   If the IKE interface is in RESPONDER mode, have peers restart tunnels instead of executing the ping command.

8. Upon completion of boot cycle verify HA state and proper tunnel synchronization.

Rollback after half way Upgrade

1. HA pair is in highly available state with Active node 840p1 and Standby node with old version

2. Configure boot table on Active node with rollback version

3. Delete tunnels on the Active node using one of the following commands from the CLI root.

   ```
   security ipsec delete ike-interface <ike-interface IP address> all
   ```

   ```
   security ipsec delete tunnel destIP <ipsec tunnels destination ip> spi
   <inbound spi>
   ```

4. Ensure that tunnel(s) were deleted from both nodes. (If necessary run this command one more time for any new spi.)

   ```
   show security ipsec sad <network interface name> detail
   ```

5. Reboot the Active node.

6. If the IKE interface is in INITIATOR mode, execute the ping command to the applicable IPSec endpoints on the newly Active node to establish new tunnels.
   If the IKE interface is in RESPONDER mode, have peers restart tunnels instead of executing the ping command.

7. Upon completion of boot cycle of verify HA state and proper tunnel synchronization

Old SSH Keys

Before upgrading, delete any imported public keys using the `ssh-pub-key delete <key-name>` command. Because the commands for SSH key management have changed from 8.3 to 8.4, you will not be able to delete old 8.3-type SSH keys using 8.4 commands. After upgrading, re-import any required public keys. See "Manage SSH Keys" in the *Configuration Guide*.

SSH Keys and Push Receivers

The OCSBC acts as an SFTP client when push-receivers are configured. If you use push-receivers and upgrade to 8.4.0 or later:

1. Because the OCSBC generates a new host key during an upgrade, the OCSBC's new host key needs to be copied to the authorized_keys file on the SFTP server.
   Use the command `show security public-host-key rsa` to view the OCSBC's new host key.

2. Reimport the SFTP server's host key as a known-host into the OCSBC.
   See "SSH Key Management" in the Configuration Guide for importing a known-host key.

3. In the **push-receiver** element, verify the **public-key** attribute is empty.

If you downgrade from 8.4.0 to a previous release, copy the public host key to the authorized_keys file of the SFTP server and reset the value of **public-key** in the **push-receiver** configuration element.

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
Accounting	boolean
Admin Security	boolean
ANSSI R226 Compliance	boolean
BFD	boolean
IMS-AKA Endpoints	Integer
IPSec Trunking Sessions	Integer
IPv4 - IPv6 Interworking	boolean
IWF (SIP-H323)	boolean
Load Balancing	boolean
MSRP B2BUA Sessions	Integer
Policy Server	boolean
Quality of Service	boolean
Routing	boolean
SIPREC Session Recording	boolean
STIR/SHAKEN Client[1]	boolean
SRTP Sessions	Integer
Transcode Codec AMR Capacity	Integer
Transcode Codec AMRWB Capacity	Integer
Transcode Codec EVRC Capacity	Integer
Transcode Codec EVRCB Capacity	Integer
Transcode Codec EVS Capacity	Integer
Transcode Codec OPUS Capacity	Integer
Transcode Codec SILK Capacity	Integer
TSCF Tunnels	Integer

[1] This feature is available in S-Cz8.4.0p2 and above.

The following table lists the features you enable by installing 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.

Feature	Type
Lawful Intercept	boolean
R226 SIPREC	boolean

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
IMS-AKA Endpoints	IPSec
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 S-Cz8.4 From Previous Releases

When upgrading from a previous release to S-Cz8.4.0, 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 Communications 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 • G722 • G723 • G729 • G729A • iLBC • Opus • SILK • PCMU • PCMA • telephone-event Note that the pooled transcoding feature on the VNF uses external transcoding OCSBC, as defined in "Co-Product Support," for supported OCSBC for the Transcoding-SBC (T-SBC) role.

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

Coproduct Support

The following products and features run in concert with the Oracle Communications Session Border Controller for their respective solutions. Contact your Sales representative for further support and requirement details.

Oracle Communications Operations Manager

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

- 4.0.0
- 4.1.0
- 4.2.0
- 4.3.0

Oracle Communications Session Delivery Manager

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

- 8.2.2 and later

> **Note:**
>
> Customers who wish to run release S-Cz8.4.0p3 and higher need to load an updated XSD into OCSDM. This file can be found by searching My Oracle Support for ID: 32063608.

Oracle Communications Subscriber Aware Load Balancer

This release can interoperate as a cluster member with the following versions of the Subscriber Aware Load Balancer:

- S-Cz7.3.10
- S-Cz8.1.0
- S-Cz8.3.0

Oracle Communications TSM SDK

This release can interoperate with the following versions of the TSM SDK:

- 1.6
- 2.0

Pooled Transcoding

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

- Acme Packet 4500: S-CZ7.4.0
- Acme Packet 4600: S-CZ7.4.0, S-CZ8.1.0, S-CZ8.2.0, S-CZ8.3.0

- Acme Packet 6300: S-CZ7.4.0, S-CZ8.1.0, S-CZ8.2.0, S-CZ8.3.0

- Acme Packet 6350: S-CZ7.4.0, 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: S-CZ7.4.0

- 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

Oracle continuously updates the documentation to deliver the latest information about the Session Border Controller. The following information describes the updates.

Oracle updated the following documentation for S-Cz8.4.0

- *Oracle Communications Session Border Controller Configuration Guide*
- *Oracle Communications Session Border Controller ACLI Reference Guide*
- *Oracle Communications Session Border Controller Platform Preparation and Installation Guide*
- *Oracle Communications SLB Essentials*
- *Oracle Communications Accounting Guide*
- *Oracle Communications Call Monitoring Guide*

Oracle updated the following documentation for S-Cz8.4.0:

- *Web GUI User's Guide*
- Web GUI online Help system

The following information lists and describes the changes made to the Oracle Communications Session Border Controller (OCSBC) documentation set for S-Cz8.4.0.

Platform Preparation and Installation Guide

Oracle moved the instance sizes for public platforms from the *Platform Preparation and Installation Guide* to the *Oracle® Enterprise Session Border Controller Release Notes* and the *Oracle® Communications Session Border Controller Release Notes*. The moves improve per-version visibility to supported instance sizes.

Call Monitoring Guide

Oracle updated the *Call Monitoring Guide* to reflect the availability of **packet-trace remote** on DPDK-based platforms.

ACLI Configuration Guide

Oracle consolidated information about P-Early Media (PEM) in the "SIP Signaling Services" chapter, which included moving PEM Header information from its previous location into the "SIP Signaling" chapter.

Release Notes

Oracle moved known issues about the Web GUI out of the general Known Issues section into a new, separate section called "Web GUI Known Issues."

Behavioral Changes

The following information documents the behavioral changes to the Oracle Communications Session Border Controller (OCSBC) in this software release.

SSH Access

Starting in S-Cz8.4.0 and later, and as a result of the change of SSH stack vendor, host certificates and stored keys will be regenerated / updated on first boot. You cannot use previous keys after upgrade. Specifically, any host keys which were cached in a client's "known hosts" file do not match the new fingerprint, so manual steps are required to remove the stale entry and accept the new key.

SFTP Access

Supplementary administrators such as TACACS+ or RADIUS administrators no longer have write access to the `/boot` directory via SFTP. If a supplementary administrator needs to upload a boot image, use the `/code/images` directory and update the boot parameters to point to the uploaded file.

SFTP Access with R226 Entitlement

When the R226 entitlement is enabled, no user (not even the local admin user) can read, write, or list the contents of the `/boot` directory with SFTP. To upload to the `/boot` directory with SFTP, the `0x01000000` bootflag must be passed to the bootloader during boot.

SSH Cipher Mapping

In S-Cz8.4.0 and later, the rijndael ciphers in the **encr-algorithm** attribute of the **ssh-config** element are mapped to their AES counterparts. Selecting **rijndael128-cbc** results in **aes128-cbc**. Selecting **rijndael192-cbc** results in **aes192-cbc**. Selecting **rijndael256-cbc** results in **aes256-cbc**.

REST API Response Headers

The Server header in the REST API response headers changed because the backend Appweb web server was replaced with nginx.

Importing External SSH Host Keys

The OCSBC no longer supports importing externally generated SSH keys for use as the host key. If you want to regenerate the SSH host keys, you may use the command **ssh-key private-key generate [rsa | dsa]**.

Ring Back Tone

When receiving P-Early-Media: inactive , the OCSBC no longer prevents Ring Back Tone from playing. Furthermore, the OCSBC does not create a playback stream if:

- The initial INVITE or the SIP reply contains the proprietary SIP header "P-Acme-RBT: no".

- The SIP reply contains a P-Early-Media with the value sendonly/sendrecv.

Data Partitions

Oracle recommends creating a single mount-point for data partitions, such as `/mnt/app`, and then using subfolders for specific purposes, such as `/mnt/app/HDR` or `/mnt/app/CDR`.

> ⚠️ **Caution:**
>
> Creating a folder directly under `/mnt` without first formatting a partition is not supported and likely to result in data loss. Use the `format` command to create mount points.

Minidump

The minidump file is no longer created during a crash. This change makes the other crash files more useful for debugging.

RADIUS Acme-User-Class

When the OCSBC uses RADIUS authentication in S-CZ8.4.0 and later, the Acme-User-Class VSA no longer supports the value `SystemAdmin`.

The value of Acme-User-Class must be lowercase: `admin` or `user`. Following the standard, the OCSBC rejects values with capitalization like `Admin` or `User`.

strip-restored-sdp option

The **strip-restored-sdp** option is disabled by default starting S-Cz8.4.0 and above. You may enable this option from **sip-config** to prevent insertion of SDP into messaging that was set up for P-Early Media(PEM).

Content-length header in OPTIONS message

Content-length is not mandatory for UDP messages by default. OCSBC sends content-length header in OPTIONS message to Session Agent that has HMR configured starting SC-z8.4.0p8 and above

Patches Included in This Release

The following information assures you that when upgrading, the S-Cz8.4.0 release includes defect fixes from neighboring patch releases.

Baseline

S-Cz8.3.0m1p8 - is the patch baseline, which is the most recent build from which Oracle created S-Cz8.4.0.

Neighboring Patches Also Included

- S-8.3.0m1p8
- S-Cz8.2.0p6
- S-Cz8.1.0m1p18c
- S-Cz8.1.0m1p23
- S-Cz8.0.0p11
- S-Cz7.4.0m2p7
- S-Cz7.4.1m1p8

Supported SPL Engines

The S-Cz8.4.0 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, C3.1.13, C3.1.14, C3.1.15, C3.1.16, C3.1.17, C3.1.18, C3.1.19, C3.1.20.

2
New Features

The S-Cz8.4.0 release of the Oracle Communications Session Border Controller 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.

Mid-Call Location Change Support for MS-Teams

The OCSBC supports mid-call end station changes between internal and external locations, and any associated OCSBC interface change. With this feature, the OCSBC provides support for the X-MS-UserLocation, and X-MS-UserSite headers, which supports traffic flow based on tenant administrator configuration.

> **Note:**
>
> The availability of this Mid-Call Location Change Support for MS-Teams feature begins with the S-cZ840p7 release.

The Configuration Assistant

When you first log on to the OCSBC, the system requires you to set the configuration parameters necessary for basic operation. To help you set the initial configuration with minimal effort, the OCSBC provides the Configuration Assistant. The Configuration Assistant asks you questions and uses your answers to set parameters for managing and securing call traffic. You can use the Configuration Assistant for the initial set up as well as for subsequent changes that you want to make to the basic configuration. See "Configuration Assistant Operations" in the *ACLI Configuration Guide*.

> **Note:**
>
> Configuration Assistant availability begins with the S-cZ840p5 release.

The Configuration Assistant

The S-cZ840p7 release adds more Configuration Templates to the template download package and enhances the work flow. See "Configuration Templates" at https://www.oracle.com/technical-resources/documentation/acme-packet.html. See "Configuration Assistant Operations" in the *ACLI Configuration Guide*.

Early Media Support

The OCSBC supports early media features, including SIP early media suppression, the Private Early Media (PEM) header, and multiple dialog management. This support complies with 3GPP TS 24.628, TS 24.182 and RFC 5009 behavior for sessions supporting early media.

Early media can be unidirectional or bidirectional, and can be generated by the caller, the callee, both, or by interim AS components. Important early media concepts for which the OCSBC provides feature support includes:

- Early Media Suppression
- Early Media Support for Multiple Early Dialog Scenarios
- Private Early Media (PEM) Header Support
- Selecting SDP within Multi-Dialog Call Scenarios

See Early Media in the *ACLI Configuration Guide*.

Use of the AF-Requested-Data AVP to Obtain EPC Identity for Emergency Calls

You can configure the OCSBC to get EPC-level identities from the PCRF through the Rx interface. When triggered, the feature issues an AAR that includes the AF-Requested-Data AVP set to the value, EPC-level identities required, as described in TS 29.214, during emergency calls. Within this context, the OCSBC is the Application Function (AF). Target deployment scenarios include supporting emergency call for native, multi-SIM subscribers. These subscribers may use multiple terminals with the same IMS-level MSISDN, such as a smart phone and a wearable device, that are in different locations. You can use this feature to populate the INVITE with the terminal identity retrieved by the EPC.

See Use of the AF-Requested-Data AVP to Obtain EPC Identity for Emergency Calls in the *ACLI Configuration Guide*.

Enhancements to NPLI Support

The OCSBC now can restrict sending NPLI AVP's only in first AAR for that session. In Invite call flow, when first AAR is sent to PCRF first AAR will have NPLI AVP's AVP, and any more AAR's going to PCRF for this session, will not have NPLI AVP's present in them. This will help achieve location optimization in outgoing AAR's. Similarly in after this feature, PANI header will be sent to core only once

See Network Provided Location Information in the *ACLI Configuration Guide*.

Diversion Info and History-Info Header Mapping Enhancement

This version of the OCSBC provides updates to Diversion and History-Info header interworking include support for later RFCs 7044 and 7544. This new support also generates several operational enhancements, including:

- Hist-to-Div enhancements
- Div-to-Hist enhancements
- 380 Cause conversion
- Tel-URI support enhancements
- Cause parameter support

- Header anonymization

The OCSBC also supports configuration to revert to former operational support.

See Diversion Info and History-Info Header Mapping in the *ACLI Configuration Guide*.

Enhancement to SIP Refer with Replaces

This version of the OCSBC provides an option configuration that allows you to enhance existing Reger with Replaces functionality. Generically, these enhancements include:

- Supports call resume between the Transferer and Transferee if the call transfer fails.
- Sets the SDP o-line in compliance with RFC 4566 and 5234.
- Accommodates the new SDP provided by a Transferee in SDP negotiations during an attended transfer.

See SIP REFER with Replaces in the *ACLI Configuration Guide*.

SIP-ISUP Inter-working Function Enhancement

This version of the OCSBC supports the Interworking function (IWF) between SIP and SIP-I networks by including ISUP message information in the body of SIP messages, and formatting SIP message information for SIP-I, from which subsequent devices use for ISUP. The OCSBC supports ITU Specifications Q.1912.5, which defines SIP-I. This specification defines ISUP message encapsulation and the mapping between SIP headers and ISUP parameters. This ITU specification is considered a super set of the IETF's SIP-T specification. The OCSBC also complies with IETF specifications on the use of MIME within SIP messages.

Enhancement development to this support has been implemented over three sequential releases, with this being the last.

See SIP ISUP Interworking in the ACLI Configuration Guide

Secure DTMF Enhancements

This version of the OCSBC enhances the existing DTMF suppression feature by providing cancellation of inband DTMF, specifically when there is a corresponding RFC2833 event. This cancellation is at the onset of inband DTMF tones, when tones partially canceled by the endpoint still allow some DTMF signal to be present in the media flow.

See Secure DTMF Cancellation in the *ACLI Configuration Guide*.

EVS Codec Enhancements

This version of the OCSBC supports two new scenarios when receiving EVS SWB codecs without requiring header manipulation rules, including:

- Pass EVS SWB media within end-to-end scenarios
- Transcode in the event of a SRVCC handover

See EVS Codec Transcoding Support in the *ACLI Configuration Guide*.

IKEv2 Implementation for Signaling and Media

This version of the OCSBC provides IKE version 2 for signaling and media traffic. Key elements of this IKEv2 support include:

- Peering/SIP Trunking solutions and access-side use cases

- Mutual authentication between the OCSBC and its peers, including:
  - IKE rekey
  - Dead Peer Detection (DPD)
  - Initiator mode
  - Responder mode
- Per-interface IKEv2 configuration
- Simultaneous support of IKEv1 and IKEv2 protocols
- Either tunnel or transport mode supported per IKE interface
- Transcoding
- Separate interfaces and IP addressing for SIP and IKE for related traffic
- Certificate-based authentication during IKEv2 tunnel establishment
- Multiple endpoints beyond tunnel remote address

See IKEv2 Protocol in the *ACLI Configuration Guide*.

SMS and VoLTE CDR Support

This version of the OCSBC adds SMS and VoLTE Session Attributes. Session attribute information presents data about the protocol type, ingress and egress realms used. With this version, the OCSBC adds SIP reporting on specific information for Short Message Service (SMS) traffic, defined within the OCSBC as message events reported using CDR STOP records. New SIP reporting also includes detail on VoLTE sessions to support management within IMS constructs.

See *VoLTE and SMS VSAs* as well as *VoLTE Call and SMS AVPs for Diameter* in the *Accounting Guide*.

Heat Template Updates

Two additional parameters have been added to the properties file of the Heat template:

- enableRestInterface—When set to true, the OCSBC generates a self-signed certificate and enables the HTTPS port during instantiation. This allows users to finish configuring the OCSBC from the REST interface.

  > **Note:**
  >
  > The self-signed certificate should be replaced with a CA-signed certificate before being deployed in a production environment.

- licenseKeys—You can pass license keys to the Heat template so that OpenStack instantiates the OCSBC with the license installed.

MSRP Enhancements

Re-creation of an MSRP Session After a TCP Disconnect—The Oracle Session Border Controller (SBC) supports the re-creation of a Message Session Relay Protocol (MSRP) session after a connection interruption, as specified in section 5.4 of RFC 4975. A User Agent engaged in an MSRP session with the SBC can send a reINVITE to the SBC to set up a new MSRP session to replace the existing MSRP session when the TCP connection is interrupted, disconnected, or otherwise unresponsive.

HA for MSRP After a TCP Disconnect—Upon a switchover, the first MSRP packet arriving at the newly active SBC triggers a TCP RST to be sent back immediately because the newly active does not have the TCP connection to receive the packet. This timely response allows the UA that sends the packet to quickly detect the connection interruption and send a reINVITE to set up a replacement session.

Platform Support for MSRP—The Acme Packet 3900 supports MSRP.

Increased Capacities for MSRP on a Virtual Oracle Session Border Controller—The improvements apply to total Transport Layer Security (TLS) subscribers and total concurrent Message Session Relay Protocol (MSRP) sessions. Contact Oracle for more information.

Two-Factor Authentication

Two-factor authentication (2FA) adds an extra layer of security when authenticating to the OCSBC by requiring a key, such as an SSH public key or X.509 certificate, as well as a username and password. 2FA can be enabled on either the web interface, the SSH interface, or both.

2FA requires the Admin Security entitlement. See the *Admin Security Guide* for details.

Logging HTTP Headers

The **audit-logging** element has a new **audit-http** attribute that enables logging HTTP requests. See the *Admin Security Guide* for details.

SIPREC Enhancements

The configuration parameter for session recording servers in the Session Agent, SIP Interface, and Realm objects has been enhanced to accept an input of up to four SRGs, or SRS', or a combination of both.

Global Match Intercept

When using lawful intercept, the global match intercept feature has been enhanced to no longer report duplicate sessions. To enable this feature, set **sip-sess-intercept-mode** to **report-sessions-swap-match**. Using **global-match-intercept** is now deprecated.

Media Path Optimization for Microsoft Teams

Media Path Optimization is a Microsoft TEAMS feature that supports optimized media paths from a TEAMS client to the PSTN. The OCSBC receives media path information in Microsoft proprietary headers. A proxy OCSBC and a location specific OCSBC perform pass-through media or media anchoring depending on this information.

TEAMS clients could be in different locations, but they can all follow the same SIP signaling path from the DR to an SBC-proxy to a downstream OCSBC using an optimized media path from which the DR is excluded. Depending on the routing decision made at the DR, media flows directly from TEAMS to the downstream OCSBC or from TEAMS to an SBC-proxy to the downstream OCSBC. This feature keeps the media path as local and/or as short as possible.

You use the following parameters to control this function:

- **realm-config**, **user-site**
- **realm-config**, **media-realm-list**
- **realm-config**, **teams-fqdn-in-uri**

- **realm-config**, **sdp-inactive-only**
- **ice-profile**, **mode**
- **session-agent**, **ping-response**

See Oracle SBC with Local Media OptimizationFor Microsoft Teams Direct Routing for more information.

Accounting Enhancement

This version of the OCSBC enhances the accounting functionality that allows you to force accounting processes on the egress realm in addition to the ingress realm.

This support is available in software versions S-Cz8.4.0p2 and above. See the Per Realm Accounting Control section in the *Accounting Guide*.

Ring Back Tone Enhancement

This version of the OCSBC enhances the RBT functionality to include delaying RBT media until after a successful SDP response when the OCSBC a session update with a new SDP offer.

This support is available in software versions S-Cz8.4.0p2 and above. See the Ring Back Tone chapter in the *ACLI Configuration Guide*.

STIR/SHAKEN Framework Support

This version of the OCSBC adds a STIR/SHAKEN client. STIR/SHAKEN is a framework of interconnected standards the OCSBC can use for authenticating calling parties in VoIP calls. To support STIR/SHAKEN, the OCSBC implements a STIR/SHAKEN REST Client, which, upon receiving an initial out-of-dialog SIP INVITE, sends a REST request to a STIR server for attestation or verification of the calling party identification. You configure the OCSBC to perform the associated functions. You can make these configurations when you enable the STIR/SHAKEN Client entitlement.

This support is available in software versions S-Cz8.4.0p2 and above. See the new STIR/SHAKEN chapter in the *ACLI Configuration Guide*.

Stir/Shaken Enhancement

This version of the OCSBC adds the following functionality to its Stir/Shaken feature:

- Handling of the verstat parameter when no Identity Header is received
- STI-VS reasoncode support in SIP responses
- Support for multiple STI Application and Verification Servers including load balancing controls
- Addition of ACP and REST configurable objects for SDM, third party and direct OSDMC support
- Alarms for STI server connection failure and failed REST responses
- Statistics to provide visibility to counts of REST queries and responses to and from the STI AS and VS
- CDR enhancements to capture calling party authentication

This support is available in software versions S-Cz8.4.0p5 and above. See the *STIR/SHAKEN Client* chapter in the *ACLI Configuration Guide*.

REST TLS Certificates

With 8.4.0p3 and later, you can use a REST client to create a certificate-record configuration element, generate a Certificate Signing Request, and upload a CA-signed certificate to the OCSBC.

BFD Platform Support

Starting with the Oracle Communications Session Border Controller S-Cz8.4.0 release, you can use BFD functionality on the OCSBC when it is running on virtual platforms as well as the Acme Packet 3900.

New Ciphers for SDES Profile

The Acme Packet 1100, Acme Packet 3900, and virtual platforms running 8.4.0p3 or later support two new ciphers in the sdes-profile configuration element:

• AES_256_CM_HMAC_SHA1_80

• AEAD_AES_256_GCM

Local Accounts

The OCSBC now supports creating local accounts in either the admin class or the user class. After you create a second admin-class local account, you may disable the default factory accounts.

Additional Diameter Compliance for the Rx Interface

When handling some Register and Message flows, the OCSBC default behavior does not include strict compliance with Diameter session tear down rules. Typically, the environment can proceed without issue, but the OCSBC provides an **ext-policy-server** option, called **diam-rx-strict-compliance**, that provides better compliance with Diameter session tear down rules.

This support is available in software versions S-Cz8.4.0p4 and above. See the new External Policy Server chapter in the *ACLI Configuration Guide*.

Analyze IPv6 Traffic with OCOM

The OCSBC can encapsulate and send IPv6 traffic to OCOM for analysis.

This support is available in software versions S-Cz8.4.0p4 and above. See the *Call Monitoring Guide*.

Support for Azure Accelerated Networking

The OCSBC supports accelerated networking when deployed on Azure.

This support is available in software versions S-Cz8.4.0p4 and above. See the *Installation Guide*, the "Public Cloud Platform" chapter.

AWS Image Optimization

The *Installation Guide* includes a new scalable process for deploying the OCSBC on AWS with Terraform when using software versions S-Cz8.4.0p4 and above.

Enhancement for Boot Loader Upgrade

For streamlining boot loader upgrades, the **set-boot-loader**, **backup-boot-loader**, and **delete-boot-file** commands are available. This feature enhances the upgrade procedure for R226 users, and can also be used for all other deployments. These commands are available in software versions S-Cz8.4.0p4 and above. See the following documents:

- *Configuration Guide*, R226 chapter
- *ACLI Reference Guide*, Commands chapter
- *Installation and Platform Preparation Guide*, the "Update the Stage3 Boot Loader" section

Emergency Registrations Based on Roaming Status

The OCSBC IMEI/IMSI validation for Emergency registration from an S8HR roaming user utilizes the epc-id-required parameter to determine its authentication behavior based on input from the REGISTER and the PCRF. Using epc-id-required within the context of emergency registration feature for S8HR Roaming station, the OCSBC provides the VPLMN identity to IMS entities in the HPLMN and supports the HPLMN, which must ensure that IMS layer signaling and media confidentiality protection is not activated in order to enable the VPLMN to meet the local regulatory requirements.

This feature is available beginning with the S-cZ840p5 release. See the *ACLI Configuration Guide*.

Including P-Visited Network Identifier and History-Info Headers in CDRs

You can configure the OCSBC to add fully compliant P-Visited Network Identifier (PVNI) and History-Info (HI) headers in CDRs. You configure this by adding the pcscf-cdr-compliance option to the account-config, specifying whether you want to include PVNI (PVNI-pref), HI (HI-pref), or both. The behavior is dependent on the type of call, including Mobile Terminating (MT) and Mobile Originating (MO), information provided by SIP, and whether you are also using an S8HR profile.

This feature is available beginning with the S-cZ840p5 release. See the *ACLI Configuration Guide*.

SIP Method Event Rate Statistics

When you enable the **extra-method-stats** parameter, the OCSBC can display success, timeout and failure rates for both client and server statistics on recent and cumulative (lifetime) requests and responses for the SUBSCRIBE, NOTIFY and MESSAGE methods in addition to the other statistics enabled by this parameter.

This support is available in software versions S-Cz8.4.0p8 and above. See the *Troubleshooting and Maintenance Guide*.

Negotiating Message Connection Roles using actpass

When you configure the **preferred-setup-role** parameter to **passive**, the OCSBC negotiates with the end station using the a=setup:actpass parameter. This allows the OCSBC to comply with RFC 4145 and RFC 4975, and to assume the correct roles when connecting to remote peers.

This support is available in software versions S-Cz8.4.0p8 and above. See the *ACLI Configuration Guide*.

3

Interface Changes

The following topics summarize ACLI, SNMP, HDR, Alarms, Accounting, and Web GUI changes for S-Cz8.4.0. The additions, removals, and changes noted in these topics occured since the previous major release of the Oracle Communications Session Border Controller.

ACLI Configuration Element Changes

The following tables describe the ACLI configuration element changes for the Oracle Communications Session Border Controller (OCSBC) S-Cz8.4.0 release and subsequent patch releases.

Configuration Assistant

New Elements	Description
run configuration-assistant	Use to launch the Configuration Assistant from the Acme Command Line Interface (ACLI). Available as of the S-Cz-8.4.0p5 release,.

telnet-timeout

> **Note:**
>
> The following configuration parameter has been deprecated. Although it is still present in the ACLI, it is not functional. Any value set here is ignored.

Removed Elements	Description
system-config, **telnet-timeout**	Deprecated. Although the parameter is present, it is not functional. Any value set here is ignored.

Public Key

> **Note:**
>
> The following configuration element has been removed.

Removed Elements	Description
security, **public-key**	Removed. Use the **ssh-key** command instead.

SSH Configuration

> **Note:**
>
> The following attributes have been removed from the **ssh-config** element.

Element with Removed Attributes	Description
security, **ssh-config**	• Removed **keep-alive-enable** attribute. • Removed **keep-alive-idle-timer** attribute. • Removed **keep-alive-interval** attribute. • Removed **keep-alive-retries** attribute.

The following configuration attributes have been added.

New Elements	Description
security, **ssh-config**	• Adds **client-idle-timeout** parameter. • Adds **tcp-keep-alive** parameter

Certificate Records

> **Note:**
>
> The following attributes have been removed from the **certificate-record** element.

Element with Removed Attributes	Description
security, **certificate-record**	The **key-size** attribute no longer accepts 512 as a value.

SIP to SIP-I Interworking

This table lists and describes new configuration elements that display in the S-Cz8.4.0 release.

New Elements	Description
session-router,**sip-isup-profile**, **iwf-for-183**	Adds the pem-controlled value to the **iwf-for-183** parameter
session-router,**sip-isup-profile**, **extract-isup-params**	Specifies the ISUP parameters to interwork to SIP
session-router,**sip-isup-profile**, **remove-isup-params**	Removes the specified ISUP parameter from the list of parameters previously added using the `extract-isup-param` configuration parameter. Allowed values include generic-number | location-number | user-to-user | calling-party-number | inband-announcement

Early Media Support

This table lists and describes new configuration elements that display in the S-Cz8.4.0 release.

New Elements	Description
session-router,**sip-interface**	Adds the support value to the **p-early-media-header** parameter
media-manager,**realm-config**	Adds the **merge-early-dialogs** parameter

Use of the AF-Requested-Data AVP to Obtain EPC Identity for Emergency Calls

This table lists and describes new configuration elements that display in the S-Cz8.4.0 release.

New Elements	Description
session-router, **ext-policy-server**	Adds the **use-epc-level-msisdn** parameter

NPLI Support

This table lists and describes new configuration elements that display in the S-Cz8.4.0 release.

New Elements	Description
session-router,**npli-profile**	Adds this new parameter to allow you to define, then apply augmented NPLI management behavior
session-router,**sip-interface**	Adds the **npli-profile** parameter

Diversion and History-Info Interworking

This table lists and describes new configuration elements that display in the S-Cz8.4.0 release.

New Elements	Description
session-router, **sip-interface**	Adds the **anonymize-history-for-untrusted** parameter
session-router, **sip-interface**	Adds the **hist-to-div-for-cause-380** parameter

SMS and VoLTE CDR Support

This table lists and describes new configuration elements that display in the S-Cz8.4.0 release.

New Elements	Description
system, **account-config**, **generate-event**	Add the **message** value
system, **account-config**, **options**	Adds the **realm-as-ioi** value
session-router,**sip-config**	Adds the **sms-report-timeout** parameter
media-manager, **ext-policy-server**, **specific-action-subscription**	Adds the **ip-can-change** value

IKEv2 Support

This table lists and describes new configuration elements that display in the S-Cz8.4.0 release.

New Elements	Description
security, **ike**, **ike-interface**	• Adds the **access-control-name** parameter • Adds the **tunnel-orig-name-list** parameter
security, **ike**, **ike-config**	• Adds the **overload-threshold** parameter • Adds the **overload-interval** parameter • Adds the **overload-action** parameter • Adds the **overload-critical-threshold** parameter • Adds the **overload-critical-interval** parameter

SIP REFER with Replaces

This table lists and describes new configuration elements that display in the S-Cz8.4.0 release.

New Elements	Description
session-router, **sip-config**	Adds the **refer-reinvite-no-sdp** parameter

Transcoding Free Operation

This table lists and describes new configuration elements that display in the S-Cz8.4.0 release.

New Elements	Description
realm-config	Adds the **srvcc-trfo** parameter.

HTTP Server

New Elements	Description
system, **http-server**	Replaces **web-server-config**.

Two-Factor Authentication

New Elements	Description
security, **authentication**, **two-factor-authentication**	Allows users to configure 2FA.

Chapter 3
ACLI Configuration Element Changes

Audit HTTP Headers

New Elements	Description
security, **admin-security**, **audit-logging**	A new attribute called **audit-http** was added which logs HTTP headers

Unsupported Configuration

New Elements	Description
system, **system-config**	Adds the **enable-snmp-tls-srtp-traps** parameter. ✎ **Note:** Unsupported. Do not enable this parameter.

SIPREC Enhancements

Modified Elements	Description
SRG: <srg name>, or**<srsname>**	Modifies configuration parameter to accept to take as input a list of up to four SRGs or SRS' or a combination of both.

Teams Integrations

New Elements	Description
realm-config, **user-site**	Lists the user-site names corresponding to the user-site configuration set at the DR. The OCSBC uses this name to select the realm for allocating media IP. The match for user-site is case insensitive.
realm-config, **media-realm-list**	Lists media realm names the OCSBC searches to match a user-site and select a media realm for allocating media IP. The first realm in the media-realm-list is the default realm for fall back functionality.
ice-profile, **mode**	Specifies the OCSBC functionality as Downstream or Proxy for media path optimization. The default, None, avoids this specification.

SSH Client Timeout

The inactivity timeout for SSH clients is set in the **client-idle-timeout** attribute in the **ssh-config** element. In S-Cz8.4.0p3 and later, the maximum timeout value changed from 1440 to 59.

MSRP Connection Delay Timer

In S-Cz8.4.0p3 and later, you can alleviate the risk of failed sessions by configuring the **conn-setup-delay-timer** parameter under the **msrp-config** element to wait the configured number of milleseconds before initiating an outbound connection.

ACLI Command Changes

The following table summarizes the ACLI command changes that first appear in the Oracle Communications Session Border Controller S-Cz8.4.0 release.

This table lists and describes changes to ACLI commands that are available in the S-Cz8.4.0 release.

New Commands	Description
ssh-key	Replaces both **ssh-pub-key** and **ssh-priv-key** commands.
show processes <process>	The following <process> arguments have been removed: • acliSSH0 • acliSSH1 • acliSSH2 • acliSSH3 • acliSSH4 • acliTelnet0 • acliTelnet1 • acliTelnet2 • acliTelnet3 • acliTelnet4 • acliConsole • cliWorker • monitor • pusher
local-accounts	Manage local accounts. In 840p3 and later, the local-accounts command replaces the ssh-password command.
set-boot-loader	Set the bootloader. Available in 8.4.0p4 and later.
delete-boot-file	Delete an unused boot file. Availabe in 8.4.0p4 and later.
backup-boot-loader	Copy the bootloader to `/code/images`. Availabe in 8.4.0p4 and later.
ssh-password	Deprecated in 840p3 and replaced by local-accounts command.
show-stir stats	Display STIR/SHAKEN statistics in 840p5 and later.
reset tacacs-stats	Reset the TACACS+ statistics

Accounting Changes

This section summarizes the accounting changes that appear in the Oracle Communications Session Border Controller version S-Cz8.4.0.

SMS and VoLTE CDR Support

With this version, the OCSBC adds SIP reporting on specific information for Short Message Service (SMS) traffic, defined within the OCSBC as message events reported using STOP records. New SIP reporting also includes detail on VoLTE sessions to support management within IMS constructs. This development has generated multiple new VSAs and AVPs provided in reports that are specific to these flows.

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
Acme-Access-Network-Information	Extracted from Access-Network-Information field from P-Access-Network-Info headers. For MO calls it should be the PANI headers of the outgoing INVITE (after the NPLI procedure). For MT calls it should be the PANI headers of the outgoing 18x response (after the NPLI procedure).	248	SMS and VoLTE	Start Interim-Update Stop
Acme-P-GW IP Address	Obtained from PCRF RAR/AAA in Access-Network-Charging-Address (501) AVP.	249, ext 1	VoLTE call	Start Interim-Update Stop
Acme-S-GW IP Address	Obtained from PCRF AAA/RAR in AN-GW-Address (1050) AVP	249, ext 2	VoLTE call	Start Interim-Update Stop
Acme-Originating-IOI	Extracted from the Originating-IOI field in the P-Charging-Vector header. For MT, MO (MESSAGE/INVITE) calls, the field is extracted from SIP reply(20X).	249, ext 3	SMS and VoLTE call	Start Interim-Update Stop
Acme-Terminating-IOI	Extracted from the Terminating-IOI field in the P-Charging-Vector header. For MT, MO (MESSAGE/INVITE) calls, the field is extracted from SIP reply(20X).	249, ext 4	SMS and VoLTE call	Start Interim-Update Stop
Acme-IMEI	Extracted from the registration cache or Initial request. (The Initial request takes priority.)	249, ext 5	SMS and VoLTE call	Start Interim-Update Stop

Attribute Name	Attribute Description	Attribute Value	Attribute Value Type	Messages
Acme-Node-Functionality	Configured with a single, global Node Functionality value. This is done in the SIP config's node functionality parameter. However, if the node functionality parameter is also configured in a realm config, the ingress realm's node functionality value supersedes the global value.	249, ext 6	SMS and VoLTE call	Start Interim-Update Stop
Acme-SMS Message Type	Extracted from initial SIP MESSAGE.	249, ext 7	SMS	Stop
Acme-SMS Calling party number	Extracted from initial SIP MESSAGE. For MO, from the P-Asserted-Identity header. For MT, from the TP-Originating-Address	249, ext 8	SMS	Stop
Acme-SMS Called party number	Extracted from initial SIP MESSAGE. For MO, from the TP-Destination-Address. For MT, from the To header of the SIP MESSAGE	249, ext 9	SMS	Stop
Acme-Message Length	Extracted from SIP MESSAGE field TP-User-Data-Length	249, ext 10	SMS	Stop
Acme-History-Info	Extracted from History-Info sip headers, ingress interface and it taken from initial message. In case of multiple History-Info headers, concatenated into a single header values in CDR.	250	VoLTE call	Start Interim-Update Stop
Acme-Visited-Network-Identifier	Extracted from Visited-Network-Identifier field from P-Visited-Network-Id headers. For MO calls, the field is extracted from initial request, or from the ingress sip-interface if the PVNI is not received in the initial request. For MT calls, the field is extracted from the initial request.	251	SMS and VoLTE call	Start Interim-Update Stop
Acme-IMSI	Extracted from the registration cache or Initial request. (The Initial request takes priority.)	252	SMS and VoLTE call	Start Interim-Update Stop

See *VoLTE and SMS VSAs* as well as *VoLTE Call and SMS AVPs for Diameter* in the *Accounting Guide*.

Diameter AVPs for VoLTE Calls

The OCSBC sends an ACR to the PCRF for call accounting with the following VoLTE-specific AVPs. The table shows all mandatory and optional AVP's. If there is data, the OCSBC includes Optional AVPs. If not the OCSBC does not include them.

AVP Name	AVP Code	Is grouped ? Group hierarchy	Type
Access-Network-Information	1263	Yes [ACR] | [Service-Information] | [IMS Information] | [Access-Network-Information]	String
IMS-Visited-Network-Identifier	2713	Yes [ACR] | [Service-Information] | [IMS Information] | [IMS-Visited-Network-Identifier]	String
Originating-IOI	839	Yes [ACR] | [Service-Information] | [IMS Information] | [Inter-Operator-Identifier] | [Originating-IOI]	String
Terminating-IOI	840	Yes [ACR] | [Service-Information] | [IMS Information] | [Inter-Operator-Identifier] | [Terminating-IOI]	String

In addition, the OCSBC sends the following fields as custom AVP's in the ACR.

AVP	ACME Diameter Attribute	AVP Type
IMSI	98	UTF8String
IMEI	97	UTF8String
History-Info	99	UTF8String
PGW-IP Address	95	UTF8String
SGW-IP Address	96	UTF8String

The table below identifies AVPs specific to VoLTE and SMS traffic.

AVP	ACME Diameter Attribute	Start	Interim	Stop	Event = MESSAGE	AVP Type
Pgw-IP	95	Y	Y	Y	N	UTF8String
Sgw-IP	96	Y	Y	Y	N	UTF8String
IMEI	97	Y	Y	Y	Y	UTF8String
IMSI	98	Y	Y	Y	Y	UTF8String
History-Info	99	Y	Y	Y	N	UTF8String

AVP	ACME Diameter Attribute	Start	Interim	Stop	Event = MESSAGE	AVP Type
Sms-Msg-Type	100	N	N	N	Y	UTF8String
Sms-called party-Number	101	N	N	N	Y	UTF8String
Sms-calling party-Number	102	N	N	N	Y	UTF8String
Sms-Msg-Length	103	N	N	N	Y	Unsigned32

SNMP/MIB Changes

This section summarizes the SNMP/MIB changes that appear in the Oracle Communications Session Border Controller version S-Cz8.4.0.

MIB Changes for TLS and SRTP Failures

When the SRTP and TLS Encryption/Decryption Failure Alarms feature is enabled and a failure occurs during TLS/SRTP encryption and decryption, the following traps in `ap.security.mib` are sent:

Trap Name	Description
apSecurityTlsEncryptionFailureNotification 1.3.6.1.4.1.9148.3.9.3.10.0.1	These notifications are sent when there is a failure during TLS packet encryption.
apSecurityTlsDecryptionFailureNotification 1.3.6.1.4.1.9148.3.9.3.10.0.2	These notifications are sent when there is a failure during TLS packet decryption.
apSecuritySrtpEncryptionFailureNotification 1.3.6.1.4.1.9148.3.9.3.11.0.1	These notifications are sent when there is a failure during SRTP packet encryption.
apSecuritySrtpDecryptionFailureNotification 1.3.6.1.4.1.9148.3.9.3.11.0.2	These notifications are sent when there is a failure during SRTP packet decryption.

The following objects get sent with the traps, depending on the failure condition:

Object Name	MIB File
apSecuritySrcAddressFamily 1.3.6.1.4.1.9148.3.9.2.23	`ap-security.mib`
apSecuritySrcAddress 1.3.6.1.4.1.9148.3.9.2.24	`ap-security.mib`
apSecuritySrcPort 1.3.6.1.4.1.9148.3.9.2.32	`ap-security.mib`
apSecurityDstAddressFamily 1.3.6.1.4.1.9148.3.9.2.25	`ap-security.mib`

Object Name	MIB File
apSecurityDstAddress 1.3.6.1.4.1.9148.3.9.2.26	`ap-security.mib`
apSecurityDstPort 1.3.6.1.4.1.9148.3.9.2.33	`ap-security.mib`
apSecurityTlsEncryptionFailureCause 1.3.6.1.4.1.9148.3.9.2.38	`ap-security.mib`
apSecurityTlsCipherSuite 1.3.6.1.4.1.9148.3.9.2.36	`ap-security.mib`
apSecurityTlsSessionId 1.3.6.1.4.1.9148.3.9.2.34	`ap-security.mib`
apSecurityTlsPacketFailureCount 1.3.6.1.4.1.9148.3.9.2.35	`ap-security.mib`
apSecurityTlsDecryptionFailureCause 1.3.6.1.4.1.9148.3.9.2.37	`ap-security.mib`
apSecuritySrtpEncrAlgorithm 1.3.6.1.4.1.9148.3.9.2.41	`ap-security.mib`
apSecuritySrtpAuthAlgorithm 1.3.6.1.4.1.9148.3.9.2.42	`ap-security.mib`

MIB Changes for STIR/SHAKEN

The S-Cz8.4.0p5 release includes new MIB objects within ap-apps.mib for the STIR/SHAKEN application.

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.1.4.2.1.4.x +	Description
apStirServerName	.1.	Server name as configured on the OCSBC
apStirServerStats.recent.asQueries	.1.1	Recent queries made to the named AS server
apStirServerStats.recent.asSuccessResponses	.1.2	Recent successful responses received from the named AS server
apStirServerStats.recent.asFailResponses	.1.3	Recent failed responses received from the named AS server
apStirServerStats.recent.asFailServiceException	.1.4	Recent failed responses received from the named AS server caused by a service exception
apStirServerStats.recent.asFailPolicyException	.1.5	Recent failed responses received from the named AS server caused by a policy exception
apStirServerStats.recent.vsQueries	.1.6	Recent queries made to the named VS server
apStirServerStats.recent.vsSuccessResponses	.1.7	Recent successful responses received from the named VS server

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.1.4.2.1.4.x +	Description
apStirServerStats.recent.vsFailResponses	.1.8	Recent failed responses received from the named VS server
apStirServerStats.recent.vsFailVerification	.1.9	Recent failed responses received from the named VS server indicating verification failure
apStirServerStats.recent.vsFailServiceException	.1.10	Recent failed responses received from the named VS server caused by a service exception
apStirServerStats.recent.vsFailPolicyException	.1.11	Recent failed responses received from the named VS server caused by a policy exception
apStirServerStats.recent.ServerUnreachable	.1.12	
apStirServerStats.total.asQueries	.2.1	Recent queries made to the named AS server
apStirServerStats.total.asSuccessResponses	.2.2	Total successful responses received from the named AS server
apStirServerStats.total.asFailResponses	.2.3	Total failed responses received from the named AS server
apStirServerStats.total.asFailServiceException	.2.4	Total failed responses received from the named AS server caused by a service exception
apStirServerStats.total.asFailPolicyException	.2.5	Total failed responses received from the named AS server caused by a policy exception
apStirServerStats.total.vsQueries	.2.6	Total queries made to the named VS server
apStirServerStats.total.vsSuccessResponses	.2.7	Total successful responses received from the named VS server
apStirServerStats.total.vsFailResponses	.2.8	Total failed responses received from the named VS server
apStirServerStats.total.vsFailVerification	.2.9	Total failed responses received from the named VS server indicating verification failure
apStirServerStats.total.vsFailServiceException	.2.10	Total failed responses received from the named VS server caused by a service exception
apStirServerStats.total.vsFailPolicyException	.2.11	Total failed responses received from the named VS server caused by a policy exception
apStirServerStats.total.ServerUnreachable	.2.12	
apStirServerStats.permax.asQueries	.3.1	Permax queries made to the named AS server
apStirServerStats.permax.asSuccessResponses	.3.2	Permax successful responses received from the named AS server

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.1.4.2.1.4.x +	Description
apStirServerStats.permax.asFail Responses	.3.3	Permax failed responses received from the named AS server
apStirServerStats.permax.asFail ServiceException	.3.4	Permax failed responses received from the named AS server caused by a service exception
apStirServerStats.permax.asFail PolicyException	.3.5	Permax failed responses received from the named AS server caused by a policy exception
apStirServerStats.permax.vsQue ries	.3.6	Permax queries made to the named VS server
apStirServerStats.permax.vsSuc cessResponses	.3.7	Permax successful responses received from the named VS server
apStirServerStats.permax.vsFail Responses	.3.8	Permax failed responses received from the named VS server
apStirServerStats.permax.vsFail Verification	.3.9	Permax failed responses received from the named VS server indicating verification failure
apStirServerStats.permax.vsFail ServiceException	.3.10	Permax failed responses received from the named VS server caused by a service exception
apStirServerStats.permax.vsFail PolicyException	.3.11	Recent failed responses received from the named VS server caused by a policy exception
apStirServerStats.permax.Server Unreachable	.3.12	

Alarms

This topic summarizes the Alarm changes that appear in this release.

Core Configuration Change in HA Environments

In HA environments, when the primary node's core configuration changes and syncs to the secondary, the secondary node sends the same alarm that the primary sends:

• **1 CPU core configuration changed - Reboot is required**

SRTP and TLS Encryption/Decryption Failure Alarms

When the notifications for TLS and SRTP Failures are enabled, if a failure occurs during SRTP or TLS encryption or decryption, the SBC can trigger the following alarms:

• SRTP Encryption Failed

• TLS Decryption Failed

STIR/SHAKEN Alarms

The OCSBC generates an alarm for STI server connection failure and failed REST responses. The OCSBC raises the trap when the circuit-breaker trips and clears it when the circuit-breaker closes again. Examples of events that would trigger the alarm include:

- Invalid credentials with STI-AS or STI-VS

- Cannot resolve host

- REST API response time out

- Internal REST API query time-out

HDR

This section presents changes to the HDR implementation.

STIR/SHAKEN Statistics

The 840p5 release includes new HDR data for collecting STIR/SHAKEN information. This stir-server-stats group includes the fields in the following table.

Position	Statistic	Description
1	TimeStamp	N/A
2	STI-Server	Server name as configured on the OCSBC
3	AS Queries	Recent queries made to the named AS server
4	AS Success Responses	Recent successful responses received from the named AS server
5	AS Fail Responses	Recent failed responses received from the named AS server
6	AS Fail Service Exception	Recent failed responses received from the named AS server caused by a service exception
7	AS Fail Policy Exception	Recent failed responses received from the named AS server caused by a policy exception
8	VS Queries	Recent queries made to the named VS server
9	VS Success Responses	Recent successful responses received from the named VS server
10	VS Fail Responses	Recent failed responses received from the named VS server

Position	Statistic	Description
11	VS Fail Verification	Recent failed responses received from the named VS server indicating verification failure
12	VS Fail Service Exception	Recent failed responses received from the named VS server caused by a service exception
13	VS Fail Policy Exception	Recent failed responses received from the named VS server caused by a policy exception
14	STI Server Unreachable	The number of times the server has tripped the STI server's 'circuit breaker'

Errors and Warnings

The following errors or warnings have been added in this release.

verify-config Errors and Warnings

Error or Warning	Description
WARNING: [x] and [y] should not be run simultaneously as they may interfere with each other and lead to undefined behavior.	Two or more of these conflicting items have been activated: comm-monitor, packet-trace, call-trace and SIP Monitoring & Trace. At least one needs to be disabled.
WARNING: access-control [x] has trust-level set to [y], while none of the attributes `invalid-signal-threshold[0], maximum-signal-threshold[0], nat-trust-threshold[0], max-endpoints-per-nat[0], nat-invalid-message-threshold[0], cac-failure-threshold[0]` are set	When DDoS is configured in media-manager, the access-control element [x] needs to have additional attributes set.

When misconfigured, a warning will display when running the packet-trace or capture command. For example:

```
ORACLE# packet-trace local start wancom0 "host 192.168.1.1"

WARNING: packet-trace and comm-monitor should not be run simultaneously as
they may interfere with each other and lead to undefined behavior.

Do you want to continue :  [y/n]?:


ORACLE# capture start global *

WARNING: SIP Monitoring & Trace, call-trace and comm-monitor should not be
run simultaneously as they may interfere with each other and lead to
undefined behavior.
```

```
Do you want to continue :  [y/n]?:
```

4

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

The following table lists the known issues in version S-Cz8.4.0. 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 the S-Cz8.4.0 Build Notes.

ID	Description	Severity	Found In
31162394	Running SIPREC on the Acme Packet 4600 over 1G interfaces may result in system instability. Workaround : Do not egress traffic out of a physical interface that exceeds the bandwidth of the physical media capacity. You should determine the amount of egress media traffic and the amount of intercepted traffic on that interface. The intercepted traffic could be any recorded traffic on the interface like (SIPREC, LI, and remote packet trace).	3	S-Cz8.4.0
33600407	When IPv4 and IPv6 addresses are added consecutively on the hip-ip-list and icmp-address of same network-interface, followed by save/activate, the configuration change is eventually activated but the OCSBC will get into unsteady state, followed by below events on the console: unregister_netdevice: waiting for <interface:id> to become free.Usage count = 1 Workaround: Add IPv4 and IPv6 address on the hip-ip-list and icmp-address separately and activate them individually i.e. activate the first config change/addition and then add and activate the second config change.	2	S-Cz8.4.0

ID	Description	Severity	Found In
32939208	You cannot set the OCSBC **ikev2-ipsec-wancom0-params** parameters using SDM due to issues with the configuration of the **rekeyfuzz** and **localip** parameters. Note these parameters have defaults or "0" and "empty" respectively. You can, however, configure these values from the OCSBC . You cannot set the OCSBC ikev2-ipsec-wancom0-params via SDM due to issues in configuration of parameters rekeyfuzz and localip, which have defaults or "0" and "empty" respectively, using OCSDM. Furthermore, if you change the values for **rekeyfuzz** and **localip**, you cannot change them back to their defaults. Workaround for changing these parameters' values back to their defaults: 1. remove the **ikev2-ipsec-wancom0-params** element from your configuration. 2. Add the element again and set your values.	3	S-Cz8.4.0
None	This version's enhancement to SMP-Aware Task Load Limiting, which adds a second parameter to the sip-config load-limit option, is currently not supported.	N/A	S-Cz7.4.0
24574252	The **show interfaces brief** command incorrectly shows **pri-util-addr** information in its output.	3	S-Cz7.4.0
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	S-Cz8.0.0
26497348	When operating in HA mode, the OCSBC may display extraneous "Contact ID" output from the **show sipd endpoint-ip** command. You can safely ignore this output.	3	S-Cz8.0.0
26598075	When running on the Acme Packet 4600, the OCSBC sends a 200OK with IPv4 media address for call flows with offerless INVITES and the OCSBC configured with add-sdp-invite=invite and ALTC configured for IPv6 on the egress.	3	S-Cz8.0.0

ID	Description	Severity	Found In
26559988	In call flows that include dual ALTC INVITEs from the callee, and subsequent Re-INVITEs that offer an ALTC with IPv6 video, the OCSBC may not include the m lines in the SDP presented to the end stations during the Re-INVITE sequence. This results in the call continuing to support audio, but not video.	3	S-Cz8.0.0
None	Re-balancing is unavailable on the OCSLB when running an Acme Packet 6300 as a cluster member. Set the SLB **cluster-config**, **auto-rebalance** parameter to **disabled** to use an Acme Packet 6300 as a cluster member from that SLB.	N/A	S-Cz730
None	The system does not support SIP-H323 hairpin calls with DTMF tone indication interworking.	N/A	S-CZ720
None	The OCSBC 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-CZ7.4.0
None	The system does not support HA Redundancy for H.323 calls.	N/A	N/A
23756306	When you configure the session-router with an operation-mode of session, it does not correctly clear sessions.	3	S-Cz7.2.0
27699451	Oracle qualified the QSFP interface for the OCSR operating over the Oracle X7-2 platform for a single QSFP port operating in 4-port mode. Specifically, 4 media interfaces successfully map to the second port of the QSFP interface using a Hydra cable as physical connections to 10G switch ports.	3	S-Cz8.1.0
26316821	When configured with the 10 second QoS update mechanism for OCOM, the OCSBC 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	S-Cz8.0.0p1

ID	Description	Severity	Found In
26323802	The 10s QoS interim feature includes the wrong source IP address as the incoming side of a call flow. The issue does not prevent successful call and QoS monitoring. For monitoring and debugging purposes, you can find the source IP in the SIP messages (INVITE/200OK).	3	S-Cz8.0.0p1
	The OCSBC dead peer detection does not work with IKEv1.	3	S-Cz8.4.0
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	S-Cz8.2.0
28617865	This version of the OCSBC is not supported as a VNF over VMware using Mellanox interface cards.	3	S-Cz8.2.0
286588.1.0	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	S-Cz8.2.0
28748784	When operating as a VNF and using Mellanox interface cards, the OCSBC does not support outbound ICMP.	3	S-Cz8.2.0
28819431	For TSM use case, the ETC CPU load increased 40% over the previous release.	2	S-Cz8.2.0
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	S-Cz8.2.0
29546194	The SBC is unable to maintain 400 or more TSM/DTLS tunnels.	2	S-Cz8.3.0
30643522	Starting with S-Cz8.3.0m1p2, Lawful Intercept users cannot modify LI configuration with the Session Delivery Manager. Workaround: LI Configuration must be performed through the ACLI.	4	S-Cz8.3.0m1p2

Resolved Known Issues

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

ID	Description	Severity	Found In	Fixed In
31828563	While using STIR/SHAKEN, Acme Packet 4600 performance is capped at 330 CPS, and Acme Packet 6350 performance is capped at 1200 CPS for both dual and quad NIU cards.	3	S-Cz8.4.0p2	S-Cz8.4.0p3
33434641	If local-port-match value is set under security-policy, and local-port-match-max is not set, then SBC processes traffic considering full port range. SBC considers the default value of local-port-match-max (i.e. 65535) and applies the specific action mentioned under security-policy to full port range. Configure the local-port-match-max or remote-port-match-max value to set a new port range or set same value for local-port-match and remote-port-match-max to configure a single port.	2	S-Cz8.4.0p4	S-Cz8.4.0p9
32535426	The show temperature output will display different values compared to releases older than S-Cz8.3.0. Starting with S-Cz8.3.0, the temperature queries via ACLI and SNMP are reporting more accurate values. • Similar components may not correspond between different platforms due to physical differences in each system.	3	S-Cz8.1.0	S-Cz8.3.0
29439964	ACLI Users will receive an error on the output of the show registration sipd by-user command.	4	S-Cz8.2.0	S-Cz8.4.0
	Issue: When upgrading to S-Cz8.4.0p7 from a release prior to S-Cz8.4.0p5, the system does not display templates in Configuration Assistant. Work-around: Run **mkdir /code/configAssistant/** before the upgrade. Or, if upgraded already, run **mkdir /code/configAssistant/ and cp /var/configAssistant/ template-package.tar.gz /code/ configAssistant/** You need to do this only once. The folder persists unless you delete it manually.		SC-z8.4.0p7	SC-z8.4.0p8

ID	Description	Severity	Found In	Fixed In
32688016 32695177	The OCSBC incorrectly exhibits the following 2 incorrect behaviors with the PCRF during Register or Message call flows: 1. Within a register call flow wherein the OCSBC receives an AAA with a 3002 error code from the PCRF after the diameter transaction has timed out, the OCSBC sends an STR to the PCRF during the de-register process. 2. For S8HR emergency registrations wherein the OCSBC receives an AAA containing a 3002 error code from the PCRF, and when the OCSBC does not have an applicable EPC level identity cached, it sends an STR to the PCRF simultaneously with a 403 message. Workaround—You can correct these by setting the **diam-rx-strict-compliance** option to the applicable **ext-policy-server** to **enabled**. When you set this option, you can correct the four issues above so that the OCSBC performs the following: 1. Within a register call flow wherein the OCSBC receives an AAA with a 3002 error code from the PCRF after the diameter transaction has timed out, the OCSBC does not send an STR to the PCRF. 2. Within emergency REGISTER call flows when S8HR is enabled and there are no EPC level identities cached, the OCSBC does not issue an STR simultaneously with a 403 error code if it receives a 3002 error code from the PCRF.	3	S-Cz8.4.0p4	S-Cz8.40p6

ID	Description	Severity	Found In	Fixed In
32524837 32524762 32488834 32502583	The OCSBC incorrectly exhibits the following 4 incorrect behaviors with the PCRF during Register and Message call flows:	3	S-Cz8.4.0	S-Cz8.4.0p5

1. If the OCSBC receives an S8HR emergency registration without an Authorization header, and cannot execute the EPC identities validation either because the Rx interface is not available or the diameter AAR gets an error in the AAA response, the OCSBC is answering with a 403.

2. For registration scenarios that do not include an Authorization header and wherein the EPC identity validation fails, the OCSBC sends a 403 error response with the reason in the MIME XML body.

3. The OCSBC is adding the PVNI header using the wrong syntax.

4. If your configuration does not identify a next-hop the OCSBC sends a 404 response to S8HR roaming emergency registration requests received with Authorization header if the EPC identities verification fails. Also, when there is no authorization header, the OCSBC is sending a 403 error response if the EPC identity verification fails.

Workaround—You can correct these by setting the **diam-rx-strict-compliance** option to the applicable **ext-policy-server** to **enabled**. When you set this option, you can correct the four issues above so that the OCSBC performs the following:

1. If the OCSBC receives an S8HR Emergency Registration, with or without Authorization header, and either the Rx interface is not available or there is an error

ID	Description	Severity	Found In	Fixed In
	in AAA response sent by PCRF, the OCSBC replies with a 5xx response. 2. If the OCSBC receives an S8HR Emergency Registration without an Authorization header and the EPC identities validation fails, the OCSBC sends a 403 error with the SIP reason header. If the OCSBC receives a REGISTER request with the authorization header, it sends a MIME XML body with a reason tag. 3. For S8HR registrations and calls, the OCSBC adds the P-Visited-Network-ID header using the format "plmnIdPrefix.mncxxx.mccxxx.3gppnetwork.org". 4. During an S8HR registration scenario, if the OCSBC receives a REGISTER request with the Authorization header and the next-hop is not configured, the OCSBC sends a 403 response if the EPC identities validation fails.			
32243204	STIR/SHAKEN entitlement is not available when system is set up as a Peering Session Border Controller product.	2	S-Cz8.4.0p2	S-Cz8.4.0p4
32056356	While performing VoLTE Accounting on a 3G-to-4G MT call, the OCSBC incorrectly populates VSA ID 69 with the P-Asserted-Identity (PAI) retrieved from the response. This identifies the called side. Within the context of a mobile terminating call, the OCSBC should be identifying the caller, populating this VSA with the PAI retrieved from the INVITE. Workaround—You can correct this by setting the **unidirectional-p-asserted-id** option in the applicable **account-config** to **yes**.	2	S-Cz8.4.0	S-Cz8.4.0p4

ID	Description	Severity	Found In	Fixed In
31812964 31926021 31918592	The OCSBC incorrectly exhibits the following 3 incorrect behaviors with the PCRF during Register and Message call flows:	3	S-Cz8.4.0	S-Cz8.4.0p4

1. The OCSBC sends an STR to the PCRF in response to a de-register even though PCRF does not consider the session established, having sent an AAA with a 3xxx. 4xxx or 5xxx error in response to the corresponding Register.

2. The OCSBC keeps the hold timer active and holds an SMS message even though the PCRF has sent an ASR telling the OCSBC to abort the diameter session.

3. The OCSBC does not send an STR to the PCRF during Register flows that fail because of an error from the core, even though the Diameter session between the OCSBC and PCRF was established.

Workaround—You can correct this by setting the **diam-rx-strict-compliance** option to the applicable **ext-policy-server** to **enabled**. When you set this option, you can correct the three issues above so that the OCSBC performs the following:

1. For Register flows that do not establish a diameter session with the PCRF due to a 3xxx. 4xxx or 5xxx error from the PCRF, the OCSBC does not send an STR to tear down the session when it receives a De-Register.

2. For Message flows, when the OCSBC receives an ASR from PCRF, it stops the hold timer, forwards the MESSAGE to the core, and sends an ASA with success.

3. For unsuccessful Register flows that include an established diameter session with the PCRF, the

ID	Description	Severity	Found In	Fixed In
	OCSBC sends an STR to tear down the session after the Register has failed due to, for example, responses from the core.			
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	CZ8.1.0m1	S-Cz8.4.0
31163030	In VOLTE deployments with registration refreshes, you may see unusually large numbers in the **alloc** and **usage** count fields while executing the **show buffers** command. This is a known statistics accounting issue.	4	S-Cz8.3.0	S-Cz8.3.0m1p9
31315823	When running IMS-AKA over UDP on virtual OCSBCs, IMS-AKA registrations may not succeed. Registration failure can also cause associated calls to fail. Oracle has observed this only happens after a system reboot. Oracle has also observed that performing a Save and Activate command sequence after a reboot ensures these registrations are successful. If you are running IMS-AKA over UDP on virtual OCSBCs, perform a Save and Activate command sequence after system reboot to ensure successful IMS-AKA registrations.	3	S-Cz8.4.0	S-Cz8.4.0p3
32181987	Do not copy/paste characters into a configuration menu and attempt to edit the copied text. This applies to both console and SSH sessions. Workaround: Edit the data before copy/paste.	3	S-Cz8.4.0	S-Cz8.4.0p3
32534935	Media is not resumed after RBT playback for transcoded calls on vSBC. Avoid upgrading to releases where this bug is open if your deployment uses a vSBC with Transcoding and is configured to use Ringback-Trigger values.	3	S-Cz8.4.0p4	S-Cz8.4.0p5

ORACLE

ID	Description	Severity	Found In	Fixed In
32517222	sipd crash while processing 200 OK of reINVITE. The SIP process can crash (and failover in an HA pair) while processing 200OK on the reINVITE in certain scenarios involving media-sec-policy configurations. See the build notes for more details.	2	S-Cz8.4.0p4	S-Cz8.4.0p5
30794993	Please see the section on Upgrades For Configurations that Include Signaled IPSec Tunnels and LI Configurations in Upgrade Downgrade Caveats in this document for an explanation of this issue.	3	S-Cz8.4.0	S-Cz8.4.0p2
31726575	Do not configure sip-advanced-logging if you expect any auth-invite call flows (401/407). If you are upgrading to S-Cz8.4.0p2 or later, and your configuration includes conditional logging (session-router, sip-advanced-logging, state=enabled), you must first remove sip-advanced-logging from the config, otherwise calls will fail. • Setting the state to disabled does not work and removing it is required.	2	S-Cz8.4.0p2	S-Cz8.4.0p4
32049267	Do not configure AEAD_AES_256_GCM cipher in the sdes-profile, crypto-list parameter, or the system will crash.	3	S-Cz8.4.0p3	S-Cz8.4.0p4
	The Acme Packet 6350 with Quad 10Gbe NIU is unable to maintain 375,000 or more idle TSM/DTLS tunnels.	3	S-Cz8.3.0p2	S-Cz8.4.0p2
30794993	The OCSBC might display an excessive number of debug messages after an HA switchover, if you configured both X123 LI and IKEv2/IPSec with IPv6 security policies. You can safely ignore these messages.	4	S-Cz8.4.0	S-Cz8.4.0p2

ID	Description	Severity	Found In	Fixed In
31384643	During the testing of this release Oracle identified a pre-existing issue in the code where adding an LI warrant during a period of heavy SIP load may cause the system to stop responding, which results in a switchover. This issue exists in prior releases and will be addressed in an upcoming 8.4 patch. If you have not encountered this issue in the past, it is unlikely that you will encounter it now. System Impact: If you add an LI warrant while the OCSBC is under heavy load from SIP traffic, a mid-call intercept operation may not occur after the addition (causing the OCSBC to stop responding). If the OCSBC stops responding a switchover will occur, but the warrant will have been added correctly. The issue can be mitigated by performing addition of LI warrants during off-peak times, such as maintenance windows.	3	S-Cz8.4.0	S-Cz8.4.0p2
30520108	Upon registering 100k or more IMS-AKA user registrations, and handling large numbers of VoLTE calls and registration refreshes, in excess of 8k for example, a vSBC may hang. At this point, you would find the vSBC unresponsive and inaccessible. An example of conditions when this may occur includes: • 100k IMS-AKA registrations with 100 registrations per second and an expiry timer of 18.0.0 seconds. • Forwarding cores at 60% or above utilization. • New calls at 50 registrations per second and 10 second hold timers. Reboot the system from the hypervisor to recover from this issue.			S-Cz8.3.0m1p5

ID	Description	Severity	Found In	Fixed In
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	S-Cz8.3.0p7	S-Cz8.3.0m1p5
29862440	When transcoding from T.38 to G711FB, the OCSBC includes multiple (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	S-Cz7.4.0m1p8	S-Cz8.3.0m1p3
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	S-Cz8.1.0m1p16	S-Cz8.4.0
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		S-Cz8.3.0m1p3
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	E-Cz8.1.0m1p8	S-Cz8.1.0m1p22

ID	Description	Severity	Found In	Fixed In
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	S-Cz7.4.0m2p4;8.1.0m1p18	S-Cz8.1.0m1p23
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	S-Cz8.1.0m1p9, S-Cz8.3.0p7	S-Cz8.3.0m1p4
29913123	NMC causes the Acme Packet 6350 to switchover when NMC gets its first traffic match.	2	S-Cz8.1.0M1P9	S-Cz8.3.0m1p3
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	S-Cz8.1.0M1P9	S-Cz825p3
310398.2.0	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	S-Cz8.3.0m1p2	S-Cz8.4.0
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	S-Cz8.0.0	S-Cz8.3.0m1p8
26669090	The OCSBC dead peer detection does not work with IPv4.	3	S-Cz8.0.0	Could not reproduce - S-Cz8.4.0

ID	Description	Severity	Found In	Fixed In
22322673	When running in an HA configuration, the secondary OCSBC 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.	3	S-Cz7.3.0P1	S-Cz8.0.0
29931732	The embedded communications monitor probe does not send IPv6 traffic to the Oracle Communications Operations Monitor's mediation engine.	3	S-Cz8.0.0	S-Cz8.3.0m1p4
30375697	Infrequently during race conditions, the number of SIP registration entries on the active and standby SBCs differs, with the standby SBC containing fewer entries. When this happens and a switchover 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_treeISsSt4pairI KSs4SptrI10SipContactEES t10*_Select*1stIS5_ESt4l essIS sE SaIS5_EE11equal_rangeERS 1_ (+ 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	S-Cz8.3.0	S-Cz8.3.0p6
288.2.0258	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	S-Cz8.0.0	S-Cz8.3.0m1p2
	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	S-Cz8.3.0	S-Cz8.3.0m1p2
29522609	Some calls that are configured to generate ring back tones result in one-way audio.	2	S-Cz8.3.0	S-Cz8.3.0m1p2
29558827	IMS-AKA calls running over IPv6 networks which utilize VLANs on systems with Mellanox network interfaces may experience one-way audio.	3	S-Cz8.3.0p3	S-Cz8.3.0m1p2
29580506	SBCs running on virtual platforms or the Acme Packet 3900 could switch over when running IMS-AKA calls involving refresh registrations.	2	S-Cz8.3.0p3	S-Cz8.3.0m1p2
29607573	The SBC is unable to successfully initiate a TCP connection to configured Diameter Accounting (Rf) servers.	2	S-Cz8.3.0	S-Cz8.3.0m1p2
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-CZ8.3.0m1	S-Cz8.3.0m1p2

ID	Description	Severity	Found In	Fixed In
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-CZ8.3.0m1	S-Cz8.3.0m1p2
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-CZ8.3.0p6	S-Cz8.3.0m1p2
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	S-Cz8.3.0	S-Cz8.3.0m1p2
30453532	The Web GUI available in the S-Cz8.3.0M1 release cannot adequately be used to configure the Enterprise SBC. Workaround: For Web GUI support, use releases either prior to S-Cz8.3.0M1, or releases S-Cz8.3.M1p2 and later.	2	S-Cz8.3.0m1	S-Cz8.3.0m1p2
26258705	The **show sipd srvcc** command does not display the correct number of unsuccessful aSRVCC calls.	3	S-Cz8.0.0	S-Cz8.3.0
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	CZ8.1.0m1	S-Cz8.3.0
29556215	The SBC does not send SIPREC data to a remote call server.	2	S-Cz8.3.0	S-Cz8.3.0p5

ID	Description	Severity	Found In	Fixed In
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	S-Cz8.3.0	S-Cz8.3.0p3
28539155	When operating as a VNF and using Mellanox interface cards, the OCSBC does not support ICMP over IPv6.	3	S-Cz8.2.0	S-Cz8.3.0
29322490	The SBC intermittently does not process the registration (Event: reg) of a SUBSCRIBE with Expires header=0 that should be created after receiving a NOTIFY with a termination request from a UE.	2	S-Cz8.2.0	S-Cz8.3.0
28526228	Maximum SRTP capacity on VNF platforms is 25% lower than in the S-Cz8.1.0 release. Expected capacity will be restored in a follow up patch.	3	S-Cz8.2.0	S-Cz8.3.0
28679339	When supporting SRVCC roaming calls, the OCSBC is handling SRVCC end-station de-registration events by properly including associated URIs in the 200 OK. It is not, however, saving those associated URIs in its registration cache. This causes the OCSBC to respond to calls to those URIs with 404 not found messages until the end-station re-registers.	2	S-Cz8.0.0	S-Cz8.3.0
26313330	In some early media call flows, the OCSBC may not present the correct address for RTP causing the call to terminate.	3	S-Cz8.0.0	S-Cz8.2.0
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	S-Cz720	S-Cz8.2.0

ID	Description	Severity	Found In	Fixed In
25144010	When an OCSBC operating on an Acme Packet 6300 switches over, the secondary can successfully add new ACL entries, but it also retains old ACL entries that it should have deleted.	3	S-Cz7.4.0p1	S-Cz8.2.0
26183767	When operating in HA mode and handling large traffic loads, the active OCSBC stops responding when you restore large configurations that are different from the configuration the active is currently running. The system subsequently goes out of service.	3	S-Cz8.0.0	S-Cz8.2.0
21975038	The Acme Packet 4600, 6100, 6300, and 6350 platforms do not support MSRP File Transfer.	3	S-Cz8.1.0	S-Cz8.2.0
27579686	This release does not support TSM.	2	S-Cz8.1.0	S-Cz8.2.0
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	S-Cz8.1.0	S-Cz8.1.0
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	S-Cz7.4.0	S-Cz8.2.0
28071326	Calls that require LMSD interworking, as invoked by the lmsd-interworking option on a SIP interface, do not work in pooled transcoding architectures. During call establishment, when sending the 200 OK back to the original caller, the cached SDP is not included.	2	S-Cz7.4.0	S-Cz8.2.0

ID	Description	Severity	Found In	Fixed In
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	S-Cz8.1.0	S-Cz8.2.0
28.3.05575	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	S-Cz8.1.0	S-Cz8.2.0
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 OCSBC a second time, after it initially starts.	3	SCz8.1.0m1	S-Cz8.2.0
	If you configured the ims_aka option, you must also configure sip-interfaces with an ims-aka-profile entry.	3	E-Cz7.4.0	E-Cz7.4.0m1
28998693	For TSM use cases, AP6100 and AP6300 systems do not support data-flow modes.	2	S-Cz8.2.0	S-Cz8.3.0
27811129	When upgrading an OCSBC from a version that uses License Keys to enable CODECs, you must reboot the system after setting any CODEC entitlements to override the License Keys.	3	S-Cz8.1.0	S-Cz8.3.0

ID	Description	Severity	Found In	Fixed In
30152019	Oracle has identified a Potential tSipd crash when configured for a VOLTE w/SRVCC scenario. When the issue is encountered, there is a sipd crash and, if configured, an HA switchover. This is a race condition that is relatively rare, but has been seen in internal testing. System Impact of HA Switchover: • The Registration cache and existing media sessions are replicated to the standby OCSBC. • During the switchover, transient calls/registrations are lost. • After the switchover, TCP connections to and from the UE's must become re-established in order to make a new call out /refresh register /reregister. • The UEs is able to receive calls from the IMS-core because the setup message reestablishes the TCP connection towards the UE.	3	S-Cz8.3.0p7	S-Cz8.3.0m1
28610095	In some circumstances, and with **add-sdp-invite** and **add-sdp-profile** configured, the OCSBC does not include the original SDP in a Re-INVITE that has no SDP. This does not comply with RFC 3264. Instead, the OCSBC inserts the negotiated media information from the last successful negotiation as the ReINVITE's SDP offer and sends this ReINVITE with inserted SDP to the next hop signaling entity. This issue is evident by the contents of the SDP o line.	3	S-Cz7.4.0	S-Cz8.3.0m1
29541242	*Installation and Platform Preparation* guide incorrectly includes information about setting up HA on Oracle Cloud platforms. These platforms do not support HA deployments at this time.	3	S-Cz8.3.0	S-Cz8.3.0m1

The following Known Issues and Caveats do not occur in this release. They are listed here for tracking purposes.

ID	Description
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.
The OCSBC 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 OCSBC can reach the LDAP server before performing switchover.	
28770472	ACLI Users will receive an error on the output of the show registration sipd by-user command.
29999832 and 30194470	When deployed as a vSBC, configured for IMS-AKA, and operating with registrations exceeding 60k, the OCSBC may exhibit performance degradation, exhibited by high CPU load or system crash. Workaround - Oracle has found that disabling the **security-policy sa-lookup-exception** parameter allows IMS-AKA to function correctly while supporting a high number of registrations. This parameter is enabled by default. Disable this parameter within all applicable security policies before running IMS-AKA. This parameter, when enabled on Acme Packet hardware, works as designed.
32062551	Virtual SBC platforms may incorrectly assess link status thereby causing major health degradation and triggering a failover.
30595413	The IKEv2/IPSEC negotiation fails while using TRANSPORT MODE and different IP's for IKE and SIP interfaces.
23253731	After an HA switchover, the new standby OCSBC retains some IMS-AKA subscriber TCP sockets. You can clear these sockets by rebooting the OCSBC.
29005944	On Acme Packet hardware in an HA configuration, with a large number of IMS-AKA endpoints, the standby is unable to synchronize, and when rebooted goes OOS.
27031344	When configured to perform SRTP-RTP interworking, the OCSBC 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.
30520181	When performing large numbers of simultaneous registrations, such as during a registration flood, the OCSBC may become unstable and stop responding when it exceeds 200k IMS-AKA subscriber registrations.

ID	Description
32512333	If managing with Oracle Communications Session Delivery Manager (formerly NNC) there is an updated XSD file required. The following is the patch number on MOS for obtaining the XSD: • **NNC-OCSDM XSD file for SCZ840p4 with SDM 8.2.x**
24809688	Media interfaces configured for IPv6, and using different VLANs that operate over different infrastructures, including VoLTE and 3GPP, are not supported.
28639227	When operating as a VNF and using Mellanox interface cards, the OCSBC does not support SCTP transport.
28906914	For transcoding use cases, the G711/G729 codec pair might experience unstable performance when each DSP has greater than 500 transcoding sessions.
30534173	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 cause the OCSBC to reboot.
N/A	The T.140-Baudot Relay is not excluded from supported features with pooled transcoding.
N/A	When operating as a VNF deployed in an HA configuration, the OCSBC does not support IPSec.
21805139	RADIUS stop records for IWF calls may display inaccurate values.

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.

Acquire Config and acp-tls-profile

The **acquire-config** process fails if your configuration includes an **acp-tls-profile**. The system does, however, successfully synch this profile after HA is established.

Workaround: Disable your **acp-tls-profile** on the active system before performing an **acquire-config** procedure. Re-enable this profile after **aquire-config** completes successfully.

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 a transcode codec was originally provisioned in an earlier software version with a license key, a capacity change using the **setup entitlements** command requires a reboot to take effect.

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.

- You may need to enable trust mode on the host PF, when using Intel X/XL7xx [i40e] NICs with SR-IOV, before you can use VLANs or HA virtual MAC on the guest VF. Refer to the Intel X710 firmware release notes for further information.

- MSRP support for VNF requires a minimum of 16GB of RAM.

- The system supports only KVM and VMWare for virtual MSRP.

- 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.

Virtual Network Function (VNF) Limitations

Oracle Communications Session Border Controller (OCSBC) functions not available in VNF deployments of this release include:

- FAX Detection

- T.38 FAX IWF

- RTCP detection

- TSCF functionality

- LI-PCOM

- ARIA Cipher

Transcoding - general

Only SIP signaling is supported with transcoding.

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

The T.140 to Baudot Relay transcoding support is not available on vSBC or Acme Packet 3900 platforms.

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 codec
- 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.

Lawful Intercept

Lawful Intercept is supported for the X123 and PCOM protocols only. PCOM support for LI is not available on virtual platforms.

Fragmented Ping Support

The Oracle Communications 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

- Output from the **packet-trace local** command on hardware platforms running this software version may display invalid MAC addresses for signaling packets.
- The **packet-trace remote** command does not work with IPv6.

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 Oracle Communications Operations Monitor
- call-trace

The verify-config command displays a warning if more than one of these is enabled.

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

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 OCSBC, 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 Communications Session Border Controller (OCSBC). 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 OCSBC, and save and activate the configuration.

2. Reboot both the Primary and the Secondary.

Offer-Less-Invite Call Flow

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

Fragmented SIP Message Limitations

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

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

IPv6 On X1 Interface

IPv6 does not work on X1 interface.

Diameter Server Timeout during Save/Activate

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

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

HA Deployment on Azure

HA deployments on Azure are not supported.

Simultaneous Use of Trace Tools

See "Trace Tools" caveat.

LI and Rx Interfaces using the same Address

Do not configure an X1, X2, or X3 TCP endpoint with the same address as an Rx interface. These configurations create conflicts between the Linux TCP stack and atcpd.

IKE

ECDSA certificates are not supported with IKEv2 configurations.

IWF

IWF (SIP-H323) appears at the setup entitlements prompt on virtual platforms when H.323 is not supported.

SIPREC Post REFER Processing

For SIPREC calls that use the Universal Call ID SPL and also exercise SIPREC on main call flow, the OCSBC does not include UUID in ACK or BYE messages post REFER processing.

Acme Packet Platform Monitoring Caveats

The SFP INSERTED and SFP REMOVED Alarms and corresponding traps are not supported on the following platforms:

- Acme Packet 3900
- Acme Packet 3950
- Acme Packet 4600
- Acme Packet 4900
- Acme Packet 6100
- Acme Packet 6300
- Acme Packet 6350

IPSec Trunking Tunnel Caveat

The **setup Entitlements** command allows to set a maximum of 2500 IPSec trunking tunnels. Each IPSec trunking tunnel secures signaling and media traffic for more than one SIP session. You can either set a maximum of 2500 trunking tunnels or less, while configuring the session capacity. Setting a maximum value for trunking tunnel does not limit the configured session capacity.

Limitations Removed

The limitations listed in this section are no longer applicable on this version of the OCSBC.

Remote Packet Trace

Remote packet trace is now supported on the Acme Packet 1100, 3900, and 4900 platforms. It is also now supported over virtual platforms.

IPSec on Virtual Platforms

IPSec functionality including authentication header (AH) support is available on virtual platforms and the Acme Packet 3900.