

Oracle® Communications

Service Provider and Session Router Release Notes



S-Cz8.2.0

F20268-04

June 2021

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

ORACLE®

F20268-04

Copyright © 2004, 2021, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software" or "commercial computer software documentation" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

Contents

About this Guide

1 Introduction to S-Cz8.2.0

Platform Support	1-1
Virtual Machine Platform Resources	1-3
PCIe Transcoding Card Requirements	1-4
Oracle Communications Session Router Recommendations for Netra and Oracle Servers	1-4
Image Files and Boot Files	1-4
Image Files for LI Customers	1-6
Boot Loader Requirements	1-6
Upgrade Information	1-6
Upgrade Checklist	1-6
Upgrade and Downgrade Caveats	1-7
Self-Provisioned Entitlements	1-9
Encryption for Virtual SBC	1-10
System Capacities	1-10
Transcoding Support	1-10
Coproduct Support	1-12
TLS Cipher Updates	1-12
Deprecated Features	1-13
Documentation Changes	1-16
Behavioral Changes	1-16
Patches Included in This Release	1-17
Supported SPL Engines	1-18

2 New Features

3 Interface Changes

ACL Command Changes	3-1
---------------------	-----

ACLI Configuration Element Changes	3-1
Diameter	3-3
Alarms	3-4

4 Caveats and Known Issues

Known Issues	4-1
Caveats and Limitations	4-8

About this Guide

The Oracle Communications Session Border Controller (OCUSM) Release Notes document provides the following information when applicable:

- An introduction to the full release
- An overview of the new features available
- An overview of the interface enhancements
- A summary of known issues, caveats, and behavioral changes

If any of these sections does not appear in the document, then there were no changes to summarize in that category for that specific release.

Documentation Set

The following table describes the documentation set for this release:

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.

Document Name	Document Description
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.
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.

Revision History

This section contains a revision history for this document.

Date	Description
December 2018	<ul style="list-style-type: none"> Initial Release
February 2019	<ul style="list-style-type: none"> Updates "Transcoding Support" for accuracy.

Date	Description
March 2019	<ul style="list-style-type: none"> • Adds "Maintain DSA-Based HDR and CDR Push Behavior" to "Upgrade and Downgrade Caveats". • Updates "Default VNF Resources" for accuracy. • Removes T.140 Baudot Relay from the list of unsupported features with pooled transcoding. • Updates processor specification requirements for VNFs • Updates VNF Caveats with IXGBE driver limitation.
April 2019	<ul style="list-style-type: none"> • Updates for S-Cz8.2.0p3. • Corrects "Transcoding Support" table. • Adds explanation of change in HMR matching.
May 2019	<ul style="list-style-type: none"> • Updates minimum vSBC signaling core requirement to 2 • Adds MSRP to list of features in the "Encryption for Virtual SBC" table. • Adds Performance Enhancements section to New Features list.
June 2019	<ul style="list-style-type: none"> • Adds OCOM incompatibility with IPv6 to known issues.
October 2019	<ul style="list-style-type: none"> • Updates the Known Issues table.
November 2019	<ul style="list-style-type: none"> • Adds trace tool limitations to "Trace Tools" caveat. • Adds FIPS support to coincide with the S-Cz8.2.0p5 release.
December 2019	<ul style="list-style-type: none"> • Adds MSRP caveat • Updates closed Known Issues
February 2020	<ul style="list-style-type: none"> • Adds telephone-event to supported codecs list for VNF
July 2020	<ul style="list-style-type: none"> • Moves bug# 22322673 to Non-present Known Issues table. • Corrects product name in book title. • Repairs confusing known issue on IPv6 and VLANs
August 2020	<ul style="list-style-type: none"> • Updates "PCIe Transcoding Card Requirement" with bullet about the maximum forwarding core.
June 2021	<ul style="list-style-type: none"> • Adds MSRP and Transcoding caveats. • Adds caveat on toggling sip-interfaces with TCP

1

Introduction to S-Cz8.2.0

The Oracle Communications Session Border Controller *Release Notes* provides the following information about S-Cz8.2.0 release:

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

Platform Support

The S-Cz8.2.0 software supports the following platforms.

Acme Packet Platforms

The following platforms are supported by the S-Cz8.2.0 version of the OCSBC:

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

The following platforms are supported by the S-Cz8.2.0 version of the OCSR:

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

Qualified Hypervisors

Oracle qualified the following components for deploying version S-Cz8.2.0 as a Virtual Network Function.

- XEN 4.4: Specifically using Oracle Virtual Machine (OVM) 3.4.2
- KVM: Using version embedded in Oracle Linux 7 with RHCK3.10
Note the use of the following KVM component versions:

- QEMU
 - * 2.9.0-16.el7_4.13.1 for qemu-img-ev, qemu-kvm-ev
 - * 3.9.0-14.el7_5.2 for libvirt-daemon-driver-qemu
- LIBVIRT
 - * 3.90-14-el7_5.2 for all components except -
 - * 3.2.0-3.el7_4.1 for libvirt-python
- VMware: Using ESXI 6.5 u1 on VMware vCenter Server

Supported Cloud Computing Platforms

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

Note:

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

Public Cloud Support

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

Supported Interface Input-Output Modes

- Para-virtualized
- SR-IOV
- PCI Passthrough

Supported Ethernet Controller, Driver, and Input-Output Modes

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

Ethernet Controller	Driver	PV	SR-IOV	PCI Passthrough
Intel 82599 / X520 / X540	ixgbe	WM	M	M
Intel i210 / i350	igb	WM	M	M
Intel X710 / XL710	i40e	WM	M	M
Broadcom (Qlogic Everest)	bnx2x	WM	NA	NA
Broadcom BCM57417	bnxt	WM	NA	NA
Mellanox ConnectX-4	mlx5	NA	M	M

Ethernet Controller	Driver	PV	SR-IOV	PCI Passthrough
Mellanox ConnectX-5	mlx5	NA	M	M

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

Virtual Machine Platform Resources

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

Default VNF Resources

VM resource configuration defaults to the following:

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

Interface Host Mode

The OCSBC S-Cz8.2.0 VNF supports interface architectures using Hardware Virtualization Mode - Paravirtualized (HVM-PV):

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

Note:

When deploying the OCSBC over VMware and using PV interface mode, the number of forwarding cores you may configure is limited to 2, 4, or 8 cores.

CPU Core Resources

The OCSBC S-Cz8.2.0 VNF requires an Intel Core7 processor or higher, or a fully emulated equivalent including 64-bit SSSE3 and SSE4.2 support .

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

PCIe Transcoding Card Requirements

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

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

- VMWare and KVM are supported
- PCIe-pass-through mode is supported
- Each vSBC can support 2 PCIE 8120 cards and the server can support 4 PCIE 8120 cards.
- Each PCIe-8120 card can be devoted to only one vSBC instance
- Transcoding cores for software-based transcoding may not be configured in conjunction with PCIe media card use
- The maximum forwarding core on VMWare and KVM with artesyn card max is 8.

Oracle Communications Session Router Recommendations for Netra and Oracle Servers

Oracle recommends the following resources when operating the OCSR, release S-Cz8.2.0 over Netra and Oracle Platforms.

Hardware recommendations for Netra Server X5-2

Processor	Memory
2 x Intel Xeon E5-2699 v3 CPUs	32GB (16 x 16 GB DIMM) DDR4-2133

Hardware recommendations for Oracle Server X7-2

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

Image Files and Boot Files

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

 **Note:**

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

For Acme Packet Platforms

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

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

For Virtual Machines

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

- nnSCZ820-img-vm_ovm.ova—Open Virtualization Archive (.ova) distribution of the SBC VNF for Oracle (XEN) virtual machines.
- nnSCZ820-img-vm_kvm.tgz—Compressed image file including SBC VNF for KVM virtual machines.
- nnSCZ820-img-vm_vmware.ova—Open Virtualization Archive (.ova) distribution of the SBC VNF for ESXi virtual machines.
- nnSCZ820_HOT.tar.gz—The Heat Orchestration Templates used with OpenStack.

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

- Product software—Bootable image of the product allowing startup and operation as a virtual machine. This disk image is in either the vmdk or qcow2 format.
- usbc.ovf—XML descriptor information containing metadata for the overall package, including identification, and default virtual machine resource requirements. The .ovf 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: nnSCZ820.bz.
- Bootloader file: nnSCZ820.boot.
- Alternate Bootloader file: EFI/BOOT/BOOTX64.EFI—New installations and upgrades on COTS platforms that support 64-bit Unified Extensive Firmware Interface (UEFI) mode. UEFI systems locate this file, provided in the Oracle distribution, when applicable.

Image Files for LI Customers

Customers requiring Lawful Intercept (LI) functionality must use the LI-specific image files, starting in S-CZ8.2.0. 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. The inventory of files for the initial GA release is:

- nnSCZ820-img-usb.LI.exe
- nnSCZ820-img-vm_kvm.LI.tgz
- nnSCZ820-img-vm_vmware.LI.ova
- nnSCZ820-img.LI.iso
- nnSCZ820.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*.

Upgrade Information

This section provides key information about upgrading to this software version.

Supported Upgrade Paths (OCSBC and OCSR)

The following in-service (hitless) upgrade and rollback paths are supported by both the OCSBC and the OCSR:

- S-CZ8.0.0 to S-CZ8.2.0
- S-CZ8.1.0 to S-CZ8.2.0
- S-CZ7.4.0 to S-CZ8.2.0
- S-CZ7.4.1 to S-CZ8.2.0

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

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.

Upgrade and Downgrade Caveats

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

License Keyed Feature Reactivation

On the Acme Packet 1100 and Acme Packet 3900 platforms, the software TLS and software SRTP features no longer require license keys. After you upgrade to S-Cz8.2.0, you must run the **setup product** command to re-activate the features that formerly depended on license keys.

Reset the `rsa_ssh.key`

After you upgrade from 7.x to S-Cz8.2.0, you must manually reset the `rsa_ssh.key` when the host OpenSSH client version is 7.6 or newer. Applies to all platforms.

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

Reset Local Passwords for Downgrades

Oracle delivers increased encryption strength for internal password hash storage for the S-Cz8.2.0 release. This affects downgrades to the E/SC-z7.x and E/SC-z8.0.0 releases because the enhanced password hash algorithm is not compatible with those earlier SBC software versions. The change does not affect downgrades to E/SCz8.1.0. If you change any local account passwords after upgrading to S-Cz8.2.0, local authentication does not work and the system locks. Unlocking the system requires a factory reset. Oracle recommends that you do not change any local account passwords after upgrading to S-Cz8.2.0 from a prior release, until you are sure that you will not need to downgrade. If you do not change any local account passwords after upgrading to S-Cz8.2.0, downgrading is not affected.

Caution:

If you change the local passwords after you upgrade to S-Cz8.2.0, and then later want to downgrade to a previous release, reset the local user passwords with the following procedure before you downgrade because the system locks you out until all passwords are cleared. If you get locked out, you must contact Oracle support to clear the passwords.

Perform the following procedure on the standby SBC first, and then force a switchover. Repeat steps 1-10 on the newly active SBC. During the procedure, the SBC powers down and you must be present to manually power up the SBC.

▲ Caution:

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

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

```
*****  
WARNING: All system-specific data will be permanently  
erased and unrecoverable.  
  
Are you sure [y/n]
```

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

vSBC License Keys

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

Maintain DSA-Based HDR and CDR Push Behavior

To maintain your existing DSA key-based CDR and HDR push behavior after upgrading from 7.x to S-Cz8.2.0, perform the following procedure:

1. Navigate to the **security, ssh-config, hostkey-algorithms** configuration element and manually enter the DSA keys you want to use.

2. Save and activate your configuration.
3. Execute the **reboot** command from the ACLI prompt.

Self-Provisioned Entitlements

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

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

Feature	Type
Accounting	boolean
Admin Security	boolean
ANSSI R226 Compliance	boolean
BFD	boolean
Data integrity (FIPS)	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
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

You enable the following features 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

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

Feature	License
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 8.2 From Previous Releases

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

System Capacities

System capacities vary across the range of platforms that support the Oracle 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)
<ul style="list-style-type: none"> • Acme Packet physical platforms • Hardware-based transcoding for virtual platforms (PCIe Media Accelerator) 	<ul style="list-style-type: none"> • AMR • AMR-WB • CN • EVRC0 • EVRC • EVRC1 • EVRCB0 • EVRCB • EVRCB1 • EVS • G711FB • G722 • G723 • G726 • G726-16 • G726-24 • G726-32 • G726-40 • G729 • G729A • GSM • iLBC • Opus • SILK • PCMU • PCMA • T.38 • T.38OFD • telephone-event • TTY, except on the Acme Packet 1100
<ul style="list-style-type: none"> • Virtual Platforms (with 1+ transcoding core) 	<ul style="list-style-type: none"> • AMR • AMR-WB • EVS • G729 • G729A • iLBC • Opus • 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.

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.

Pooled Transcoding

The pooled transcoding feature enables a non-transcoding OCSBC to access the resources of a transcoding OCSBC (T-SBC) to perform transcoding on its behalf. When running S-Cz8.2.0 software, the following hardware/software combinations may be used as a T-SBC in a pooled transcoding scenario:

- Acme Packet 4500: S-CZ7.4.0
- Acme Packet 4600: S-CZ7.4.0, S-CZ8.0.0, S-CZ8.1.0, S-CZ8.2.0
- Acme Packet 6300: S-CZ7.4.0, S-CZ8.0.0, S-CZ8.1.0, S-CZ8.2.0
- Acme Packet 6350: S-CZ7.4.0, S-CZ8.0.0, S-CZ8.1.0, S-CZ8.2.0

Oracle Communications Session Load Balancer

This release of the OCSBC can interoperate with:

- The S-Cz7.3.10 OCSLB as a cluster controller running on the Acme Packet 6100 platform.
- The S-Cz8.1.0 OCSLB as a VNF cluster controller.

Oracle Communications TSM SDK

Oracle Communications Software Development Kit (TSM SDK) versions 1.5 and 1.6 support this GA release of the OCSBC.

Oracle Communications Operations Manager

Oracle Communications Operations Manager (OCOM) versions 4.0 and later support this GA release of the OCSBC.

Oracle Communications Session Delivery Manager

Oracle Communications Session Deliver Manager (OCSDM) versions 8.1.1 and later will support this GA release of the OCSBC.

TLS Cipher Updates

Note the following changes to the DEFAULT cipher list.

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

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

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

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Oracle supports the following ciphers for debugging purposes only:

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

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

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

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

 **WARNING:**

When you set **tls-version** to either **tlsv1** or **tlsv1.1** and you want to use ciphers that Oracle considers not secure, you must manually add them to the **cipher-list** attribute.

 **Note:**



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

Deprecated Features

The features listed in this section are removed from the Oracle Communications Session Border Controller beginning with the version stated.

Feature	Description	First Deprecated
MSRP Stitching	This feature, which supported peer-to-peer TCP connections for peers behind NATs, enabling Message Session Relay Protocol (MSRP) clients to communicate with one another, is not supported. Note that you can still accomplish this function using MSRP B2BUA.	SCZ8.0.0
Telnet	Telnet is not supported. Use SSH for network access to OCSBC management. Note that references to Telnet and FTP are still present in the S-CZ8.0.0 documentation set because those terms are still used in the ACLI. For example, the telnet-timeout parameter persists in the guide because it persists in system-config . In the absence of Telnet support, the telnet-timeout parameter now sets the SSH timeout.	SCZ8.0.0
ACLI "management" Command	The management command is not supported, and removed from the ACLI.	SCZ8.0.0
The dynamic-trusted-drop-threshold Feature	The media-manager-config's dynamic-trusted-drop-threshold feature is not supported, and the parameter is removed from the ACLI.	SCZ8.0.0
Acme Packet 3820 and 4500	This version of software does not support the Acme Packet 3820 and the Acme Packet 4500 platforms.	SCZ8.0.0
The phy-link redundancy Feature	The phy-interface's phy-link redundancy feature, which was available on the Acme Packet 3820 and 4500 platforms, is not supported. The parameter is also removed from the ACLI.	SCZ8.0.0
The minimum-reserved-bandwidth Feature	The access-control's minimum-reserved-bandwidth feature, which was available on the Acme Packet 3820 and 4500 platforms, is not supported.	SCZ8.0.0
TLS Ciphers	<ul style="list-style-type: none"> • TLS_DHE_RSA_WITH_DES_CBC_SHA • TLS_RSA_WITH_DES_CBC_SHA • TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA 	SCZ8.1.0
secure-traps	Within the context of the OCSBC's comprehensive SNMPv3 support, the secure-traps value is removed from the snmp-agent-mode parameter. In addition, the elimination of secure-traps means that the following protocols are deprecated for use by SNMP: <ul style="list-style-type: none"> • DES privacy protocol • MD5 and SHA authentication protocols 	SCZ8.1.0

For your information, the following table carries forward the list of deprecated features noted in previous Release Notes.

Feature	Description	First Deprecated
DES-CBC Ciphers	<p>The OCSBC deprecates the following ciphers, adhering to recent OpenSSL changes intended to eliminate weak ciphers:</p> <ul style="list-style-type: none"> • All DES-CBC ciphers, including: <ul style="list-style-type: none"> – TLS_DHE_RSA_WITH_DES_CBC_SHA – TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA <p>The user should remove any prior Oracle Communications Session Border Controller version configuration that used these ciphers, and not configure a security profile with the expectation that these ciphers are available. Note also that TLS profiles using the ALL (default) value to the cipher-list parameter no longer use these ciphers.</p>	SCZ740m1
	<div style="border-left: 2px solid #0070C0; border-right: 2px solid #0070C0; border-bottom: 2px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>Your version of the ACLI may still display these ciphers within the tls-profile, cipher-list parameter. Despite displaying them in ACLI output, the system does not support them.</p> </div>	
FTP Support	<p>The OCSBC's FTP Server is not supported.</p> <p>Only FTP client services are supported. For example, FTP client service for HDR/CDR push is supported.</p> <p>Note that both the SFTP client and server are supported.</p>	SCZ7.3.0
MGCP Signaling Support	MGCP Signaling is not supported.	SCZ7.1.2
SIP Monitor and Trace / WebGUI	The SIP Monitor & Trace and WebGUI features are not supported.	SCZ7.2.0
Source-based Routing	<p>The source routing feature as configured by system-config, source-routing is not supported.</p> <p>Please review the HIP information in the Network Interface section in the System Configuration chapter of the ACLI Configuration guide for background on accessing OCSBC Administrative Applications over media Interfaces.</p>	SCZ7.1.2
	<div style="border-left: 2px solid #0070C0; border-right: 2px solid #0070C0; border-bottom: 2px solid #0070C0; padding: 10px; background-color: #E6F2FF;"> <p> Note:</p> <p>Despite deprecation, the parameter is still present in the system-config.</p> </div>	
H.248	The Border Gateway and H.248 functionality are not supported.	SCZ7.1.2
HMR action on Call-ID	HMR operations on the Call-ID: header are not supported.	Prior to SCZ7.1.2

Feature	Description	First Deprecated
Session Replication for Recording	Session Replication for Recording is not supported.	Prior to SCZ7.1.2
MIKEY key management protocol	Multimedia Internet KEYing (MIKEY) for SRTP	SCZ7.1.2
Lawful Intercept Features	The following LI features are deprecated: <ul style="list-style-type: none"> • VERINT support • P-DCS-LAES support • LI complex call flow support - SS8 & Verint • SDP and CCC IP address and Port number matching for SS8/Verint variants 	SCZ7.1.2
FIPS Certification	Federal Information Processing Standards (FIPS) Certification is not available in the OCSBC. (Note that it is available in the Oracle Enterprise Session Border Controller.)	SCZ7.1.2
IWF	Interworking Features <ul style="list-style-type: none"> • DTMF IWF for H.323 • Media hairpinning involving H.323 and SIP 	
SRTP	Linksys SRTP is not supported.	SCZ6.4.0

Documentation Changes

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

DTMF IWF Documentation

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

Transcoding Chapter

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

Trunk Group Documentation

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

Behavioral Changes

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

Minimum Signaling Core Requirement

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

TLS1.0

TLS1.0 is no longer advertised by default during session negotiation when the **tls-version** parameter is set to **compatibility**. To advertise TLS1.0 during session negotiation, navigate to the **security-config** element and set the **options** parameter to **+sslmin=tls1.0**. Note that the current default is TLSv1.2.

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

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

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

VNF Licensing

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

Lawful Intercept Customers

Refer to the topic about new images files for LI customers only: [Image Files for LI Customers](#).

HMR Regex Matching Changes

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

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

Patches Included in This Release

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

Baseline

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

Neighboring Patches Also Included

- S-Cz7.4.0m1p6

- S-Cz8.0.0p2

Supported SPL Engines

The S-Cz8.2.0 release supports the following SPL engine versions: C2.0.0, C2.0.1, C2.0.2, C2.0.9, C2.1.0, C2.1.1, C2.2.0, C2.2.1, C2.3.2, C3.0.0, C3.0.1, C3.0.2, C3.0.3, C3.0.4, C3.0.6, C3.0.7, C3.1.0, C3.1.1, C3.1.2, C3.1.3, C3.1.4, C3.1.5, C3.1.6, C3.1.7, C3.1.8, C3.1.9, C3.1.10, C3.1.11, C3.1.12.

2

New Features

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



Note:

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

Telephony Fraud Protection

You can configure the Oracle Communications Session Border Controller (OCSBC) to protect against fraudulent calls by enabling telephony fraud protection and creating lists of phone numbers to block, allow, redirect, and rate-limit. The lists reside together in a single XML file that you create and then specify as the source file in the **fraud-protection** configuration under **system**. The source file can contain any combination of the list types, but the system limits the total file size to 100,000 entries. You can also configure the OCSBC to enforce an order of precedence among the lists and among the dial patterns.

See "Telephony Fraud Protection" in the *ACLI Configuration Guide*.

MSRP Support for VNF

The CZ8.2.0 release adds support for Message Session Relay Protocol (MSRP) to the Oracle Virtual Machine (OVM), Kernel-based Virtual Machine (KVM), and VMware. Note that the system requires 16GB of RAM.

Multimedia Priority Service for VoLTE Access

The Oracle Communications Session Border Controller (OCSBC) supports Multimedia-priority services (MPS) to prioritize communications by emergency personnel within VoLTE networks. Specifically, the OCSBC supports emergency service authorization and resource allocation for an MPS call. You enable support for MPS by enabling **mps-volte** in the **sip-config**. You configure this support in conjunction with your **net-management-control** and **rph-profile** configurations.

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

S8HR Roaming Compatibility

The Oracle Communications Session Border Controller (OCSBC) allows you to configure support for S8 Home Routing (S8HR) routing architecture. S8 is the 3GPP-defined Packet Data Network (PDN) Gateway to Serving Gateway (S-GW) interface used when a UE is roaming. S8HR is described in full by 3GPP TR 23.749. The OCSBC feature provides support for UE connectivity, sec-agree and emergency call services.

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

Bidirectional Forwarding Detection

The Oracle Communications Session Border Controller (OCSBC) supports Bidirectional Forwarding Detection (BFD) over network interfaces. BFD is a network protocol used to detect faults between two forwarding engines connected by a link. It provides low-overhead detection of faults, even on physical media that doesn't support failure detection of any kind, such as Ethernet, virtual circuits, tunnels and MPLS Label Switched Paths. You configure BFD for functions, including gateway path verification.

BFD platform support for this release:

- OCSBC — Acme Packet 4600, Acme Packet 6100, Acme Packet 6300, and Acme Packet 6350.

This release does not support BFD on the Oracle Communications Session Recorder (OCSR) and the Oracle Communications Session Load Balancer (OCSLB).

See "High Availability Nodes" in the *ACLI Configuration Guide*.

RTP TTL

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

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

Upgrade Information

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

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

Mellanox® Support

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

Simultaneous DTMF and Audio Payload Mapping

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

Software-Based Transcoding Support

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

- EVS (Service Provider, only)

- OPUS
- iLBC

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

REST API

The Oracle Communications Session Border Controller (OCSBC) includes a REST API that accepts Create, Read, Update, and Delete (CRUD) operations over HTTPS. For a description of the supported REST API endpoints, see the [REST API documentation](#).

OpenStack Heat Template

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

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

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

Product and Entitlement Provisioning from the Heat template

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

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

Performance Enhancements

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

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

FIPS Support for Service Provider SBC

As of release S-Cz8.2.0p5, the OCSBC supports FIPS.

See the *FIPS Compliance Guide* for complete information about FIPS support.

3

Interface Changes

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

ACLI Command Changes

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

Command	Description
check-upgrade-readiness	New command providing you with summary or comprehensive system state. Information reported is filtered to assist with or prevent upgrade to new system software.
show mps-stats	New command that presents MPS session count for period and lifetime timeframes.
show registration	Existing command modified to include r-value information on a per-user basis.
show bfd-stats	New command that displays status information on active BFD sessions.
show media	Existing command modified to include packet counts for BFD sessions.

ACLI Configuration Element Changes

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

VoLTE Features

New Parameters	Description
session-router, sip-config, mps-volte	Allows you to enable and disable the MPS for VoLTE feature.
session-router, s8hr-profile	Allows you to configure S8HR profiles.
session-router, s8hr-profile, name	Specifies the name for the S8HR profile.
session-router, s8hr-profile, register-hold-for-plmn-info	Specifies the time to hold registers for the S8HR profile.
session-router, s8hr-profile, plmn-id-prefix s8hr	Specifies the prefix the system uses to build P-Visited-Network-ID header for the S8HR profile.
session-router, s8hr-profile, emergency-reject-on-ident-error	Causes the system to reject an emergency session if the user identification validation does not respond.
session-router, s8hr-profile, local-mnc	Specifies the Mobile Network Code wherein the SBC resides.

New Parameters	Description
session-router, s8hr-profile, local-mcc	Specifies the Mobile Country Code wherein the SBC resides.

SIP Interface Features

New Parameters	Description
session-router, sip-interface, s8hr-profile	Allows you to apply an S8HR profile to a sip-interface .

External Policy Features

New Parameters	Description
session-router, external-policy-server, specific-action-subscription	Adds the plmn-change value to the specific-action-subscription parameter

Network Interface Features

New Parameters	Description
system, network-interface, bfd-config	Provides access to the BFD configuration element, its parameters and the BFD session sub-element.
system, network-interface, bfd-config, state	Specifies whether BFD is operational for this network interface.
system, network-interface, bfd-config, health-score	Specifies the health score decrement when any BFD session goes down.
system, network-interface, bfd-config, options	Provides the user with the ability to set any BFD options for this network interface.
system, network-interface, bfd-config, bfd-session	Provides access to BFD session sub-element.
system, network-interface, bfd-config, bfd-session, bfd-sess-type	Specifies whether this BFD session is for gateway health checking or VIP support.
system, network-interface, bfd-config, bfd-session, admin-state	Specifies whether this specific session is enabled.
system, network-interface, bfd-config, bfd-session, admin-session-state	Specifies whether this specific session is in admin-down state.
system, network-interface, bfd-config, bfd-session, min-tx-interval	Specifies the min-tx-interval in milliseconds. Refer to RFC 5880 for more details.
system, network-interface, bfd-config, bfd-session, min-rx-interval	Specifies the min-rx-interval in milliseconds. Refer to RFC 5880 for more details.
system, network-interface, bfd-config, bfd-session, detect-multiplier	Specifies the integer to use as the BFD detect multiplier, which impacts the system's BFD state transition timing calculations. Refer to RFC 5880 for more details.
system, network-interface, bfd-config, bfd-session, hold-down-time	Specifies the time in milliseconds after a session has gone down that before which the system reports the BFD protocol state transition to Up.
system, network-interface, bfd-config, bfd-session, local-discriminator	Specifies the integer used by the system to identify this session.

Media Features

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

System Features

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

Security Features

New Parameters	Description
security, ike, ike-interface, ike-version	Setting ike-version to 2 is only supported for X2/X3 connections over a media interface.

Diameter

This section summarizes the accounting changes that appear in the Oracle Communications Session Border Controller version S-Cz8.2.0.

AAR AVPs

The Oracle Communications Session Border Controller includes the **MPSIdentifier AVP** and **Reservation-Priority AVPs** in the AAR command towards the PCRF.

Alarms

This topic summarizes the Alarm changes that appear in the Oracle Communications Session Border Controller version S-Cz8.2.0.

VIP Down Alarm

If a BFD VIP session fails, the OCSBC sends out the following alarm prior to failover.

ID	Task	Severity	First Occurred	Last Occurred
327724	117	5	2017-12-13 05:31:09	2017-12-13 05:31:09
Count	Description			
1	1 VIP BFD session down !!!			

The OCSBC does not issue traps on VIP session status.

4

Caveats and Known Issues

This chapter lists the caveats and known issues for this release. Oracle updates this Release Notes document to distribute issue status changes. Check the latest revisions of this document to stay informed about these issues.

Known Issues

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

ID	Description	Severity	Found In
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	SCZ740
24574252	The show interfaces brief command incorrectly shows pri-util-addr information in its output.	3	SCZ740
26790731	Running commands with very long output, such as the "show support-info" command, over an OVM virtual console might cause the system to reboot. Workaround: You must run the "show support-info" command only over SSH.	2	SCZ800
26338219	The packet-trace remote command does not work with IPv6.	2	SCZ740
26497348	When operating in HA mode, the OCSBC may display extraneous "Contact ID" output from the show sipd endpoint-ip command. You can safely ignore this output.	3	SCZ800
26258705	The show sipd srvc command does not display the correct number of unsuccessful aSRVCC calls.	3	SCZ800
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	SCZ800

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	SCZ800
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	SCZ730
21805139	RADIUS stop records for IWF calls may display inaccurate values.	2	SCZ730b6
24809688	Media interfaces configured for IPv6, and using different VLANs that operate over different infrastructures, including VoLTE and 3GPP, are not supported.	3	SCZ730
None	The system does not support SIP-H323 hairpin calls with DTMF tone indication interworking.	N/A	S-CZ720
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-CZ740
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
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.	2	SCZ730M2
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	SCZ810

ID	Description	Severity	Found In
27911939	<p>When running the OCSBC over the KVM hypervisor and using SR-IOV interface mode, the system fails over when all of following conditions are in effect:</p> <ul style="list-style-type: none"> • 4 forwarding cores • 8 signaling cores • IMS-AKA in use • High call traffic load 	3	SCZ810
28617938	<p>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:</p> <ol style="list-style-type: none"> 1. Set admin state to disabled. 2. Save and activate. 3. Set admin state to enabled. 4. Save and activate. 	4	CZ810m1
28618563	<p>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.</p>	3	CZ810m1
26316821	<p>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.</p> <p>You can determine the correct codecs from the SDP in the SIP Invite and 200 OK.</p>	3	SCZ8.0.0p1
26323802	<p>The 10s QoS interim feature includes the wrong source IP address as the incoming side of a call flow.</p> <p>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).</p>	3	SCZ8.0.0p1
26669090	<p>The OCSBC dead peer detection does not work with IPv4.</p>	3	SCZ8.0.0

ID	Description	Severity	Found In
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.	3	SCZ8.0.0p1
28539155	When operating as a VNF and using Mellanox interface cards, the OCSBC does not support ICMP over IPv6.	3	SCZ820
28539190	When operating as a VNF and using Mellanox interface cards, the OCSBC does not use the Host In Path (HIP) configuration to restrict management traffic. Instead the system allows any traffic over the interface.	3	SCZ820
28617865	This version of the OCSBC only is not supported as a VNF over VMware using Mellanox interface cards.	3	SCZ820
28639227	When operating as a VNF and using Mellanox interface cards, the OCSBC does not support SCTP transport.	3	SCZ820
28658810	When operating as a VNF and using Mellanox interface cards, the OCSBC does not support any other type of card for media interfaces. (If any media interface uses a Mellanox card, all media interfaces must use a Mellanox card.)	3	SCZ820
28748784	When operating as a VNF and using Mellanox interface cards, the OCSBC does not support outbound ICMP.	3	SCZ820
28819431	For TSM use case, the ETC CPU load increased 40% over the previous release.	2	SCZ820
28906914	For transcoding use cases, the G711/ G729 codec pair might experience unstable performance when each DSP has greater than 500 transcoding sessions.	3	SCZ820
29005944	On engineered hardware in an HA configuration, with a large number of IMS-AKA endpoints, the standby is unable to synchronize, and when rebooted goes OOS.	3	SCZ820
28999116	IWF (SIP-H323) appears at the setup entitlements prompt on virtual platforms when H.323 is not supported.	3	SCZ820
28770472	ACLI Users will receive an error on the output of the show registration sipd by-user command.	4	SCZ820

ID	Description	Severity	Found In
29170419	In long call scenarios, the SBC is not sending the expected refresh before the Session-Expires: header value time is up for SUBSCRIBE messages.	2	SCZ820
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	SCZ820
29931732	The embedded communications monitor probe does not send IPv6 traffic to the Oracle Communications Operations Monitor's mediation engine.	3	SCZ800
28820258	On PNF platforms, when running TLS Chat on VMware-PV 4core (SSFD) + 16GB, TLS Chat sessions are gradually decreasing. When looking in Wireshark at EXFO, EXFO forwards a wrong TLS MSRP Chat payload to EXFO UAS. TCP Chat does not have this error.	3	SCZ800

Resolved Known Issues

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

ID	Description	Severity	Found In	Fixed In
29937232	GW unreachable and NetBufCtrl MBUFF errors - This can result in system instability including crash, gw-unreachable and redundancy issues. System will switchover if in HA. Show Buffers output will normally show an increase of errors reported in the NetBufCtrl field due to mbuf's not being freed.	2	SCZ820	SCZ830p6
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	SCZ800	SCZ820p4
28526228	Maximum SRTP capacity on VNF platforms is 25% lower than in the SCZ8.1.0 release. Expected capacity will be restored in a follow up patch.	3	SCZ820	SCZ830
26313330	In some early media call flows, the OCSBC may not present the correct address for RTP causing the call to terminate.	3	SCZ800	SCZ820

ID	Description	Severity	Found In	Fixed In
262815 99	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: <ul style="list-style-type: none"> • apSysMgmtPhyUtilThresholdTrap • apSysMgmtPhyUtilThresholdClearTrap 	3	SCZ720	SCZ820
251440 10	When an OCSBC operating on an Acme Packet 6300 fails over, the secondary can successfully add new ACL entries, but it also retains old ACL entries that it should have deleted.	3	SCZ740p 1	SCZ820
261837 67	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	SCZ800	SCZ820
219750 38	The Acme Packet 4600, 6100, 6300, and 6350 platforms do not support MSRP File Transfer.	3	SCZ810	SCZ820
275796 86	This release does not support TSM.	2	SCZ810	SCZ820
275397 50	When trying to establish a connection between the SBC and your network, while using TLS version 1.2, the SBC may reject the connection. Workaround: You may need to adjust your cipher list.	3	SCZ810	SCZ810
280624 11	Calls that require SIP/PRACK interworking as invoked by the 100rel-interworking option on a SIP interface do not work in pooled transcoding architectures.	2	SCZ740	SCZ820
280713 26	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	SCZ740	SCZ820
None	The CZ8.1.0 release does not support IPsec on the Acme Packet 3900 and VNF. You must upgrade to CZ8.1.0p1 to get this support. After you upgrade to CZ8.1.0p1, do the following: <ol style="list-style-type: none"> 1. Run setup entitlements, again. 2. Select advanced to enable advanced entitlements, which then provides support for IPSEC on Acme Packet 3900 and VNF systems. 	N/A	CZ810	CZ820
283055 75	On VNFs, the system erroneously displays the IPSEC entitlement under "Keyed (Licensed) Entitlements." The error does not affect any functionality and you do not need to do anything.	4	CZ810	CZ820

ID	Description	Severity	Found In	Fixed In
286594 69	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	CZ810m1	SCZ820
	If you configured the <code>ims_aka</code> option, you must also configure sip-interfaces with an <code>ims-aka-profile</code> entry.	3	ECZ7.4.0	ECZ7.4.0 m1
289986 93	For TSM use cases, AP6100 and AP6300 systems do not support data-flow modes.	2	SCZ820	SCZ820p 1
278111 29	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	SCZ810	SCZ820

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

ID	Description	Found In	Fixed In
22322673	When running in an HA configuration, the secondary 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 <code>log.berpd</code> , which can indicate that the media did not synchronize. Workaround: Reboot the secondary until it successfully reaches the "Standby" state.	N/A	N/A
N/A	The T.140-Baudot Relay is not excluded from supported features with pooled transcoding.	N/A	N/A

ID	Description	Found In	Fixed In
28367500	When operating the OCSBC on the Acme Packet 6300, the tracert command does not show hops for an IPv6 traceroute that does not reach the target address. The system successfully displays hops when the traceroute reaches the target and for IPv4 traceroutes.	N/A	N/A

Caveats and Limitations

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

Toggling SIP Interfaces Running TCP

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

Provisioning Transcode Codec Session Capacities

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

- When a transcode codec is provisioned with a license key, a capacity change requires a reboot to take effect.
- When a transcode codec is self-provisioned, a capacity change takes effect without a reboot.

Virtual Network Function (VNF) Caveats

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

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

- When operating as a VNF deployed in an HA configuration, the OCSBC does not support IPSec.
- MSRP support for VNF requires a minimum of 16GB of RAM.
- The system supports only KVM and VMWare for virtual MSRP, and it supports only the 4 core SSFD model.
- CPU load on 2-core systems may be inaccurately reported.
- IXGBE drivers that are a part of default host OS packages do not support VLANs over SR-IOV interfaces.
- Virtual LAN (VLAN) tagging is not supported when deploying the OCESBC over the Hyper-V platform.

Virtual Network Function (VNF) Limitations

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

- FAX Detection
- RTCP generation for G.711 or G.729
- RTCP detection
- TSCF functionality
- LI-PCOM
- H.323 signaling or H.323-SIP inter-working
- Remote Packet Trace
- ARIA Cipher
- IPSec functionality not available in VNF deployments of this release:
 - IKEv1
 - Authentication header (AH)
 - The AES-XCBC authentication algorithm
 - Dynamic reconfiguration of security-associations
 - Hitless HA failover of IPSec connections.

Transcoding - general

Only SIP signaling is supported with transcoding.

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

The T.140 to Baudot Relay transcoding support is not available on vSBC and 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/SILK codecs
- SRTP and Transcoding on the same call
- Asymmetric DPT in SRVCC call flows
- Media hairpinning
- QoS reporting for transcoded calls
- Multiple SDP answers to a single offer
- PRACK Interworking
- Asymmetric Preconditions

DTMF Interworking

RFC 2833 interworking with H.323 is unsupported.

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

H.323 Signaling Support

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

Media Hairpinning

Media hairpinning 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.

IKEv2 interfaces are supported only for X2 and X3 traffic.

 **WARNING:**

No other interfaces support IKEv2.

 **WARNING:**

Customers using IKEv1 should not enable IKEv2.

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.

SRTP Caveats

The ARIA cipher is not supported by virtual machine deployments.

Packet Trace

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

Trace Tools

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

- **packet-trace** command
- The communications-monitor as an embedded probe with the Oracle Communications Operations Monitor

RTCP Generation

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

SCTP

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

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

MSRP Support

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

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 the Oracle 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.

Acme Packet 3900 IPSec Limitations

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

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

Dead Peer Detection

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

Offer-Less-Invite Call Flow

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

Fragmented SIP Message Limitations

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

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

IPv6 On X1 Interface

IPv6 does not work on X1 interface.

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.