Oracle® Communications Session Border Controller and Session Router

Release Notes

Release S-Cz8.1.0

F20255-02

July 2020

ORACLE

Oracle Communications Session Border Controller and Session Router Release Notes, Release S-Cz8.1.0

F20255-02

Contents

About this Guide

The Oracle Communications Session Border Controller (OCSBC) and Oracle Communications Session Router (OCSR) 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.

Related Documentation

The following table lists the members that comprise the documentation set for this release:

Document Name	Document Description
Acme Packet 4600 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4600.
Acme Packet 6100 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6100.
Acme Packet 6300 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6300.
Acme Packet 6350 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6350.
Release Notes	Contains information about the current documentation set release, including new features and management changes.
ACLI Configuration Guide	Contains information about the administration and software configuration of the Service Provider Oracle Communications Session Border Controller.
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Maintenance and Troubleshooting Guide	Contains information about Oracle Communications Session Border Controller 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 Oracle Communications Session Border Controller's accounting support, including details about RADIUS and Diameter accounting.
HDR Resource Guide	Contains information about the Oracle Communications Session Border Controller's Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Administrative Security Essentials	Contains information about the Oracle Communications Session Border Controller's support for its Administrative Security license.
Security Guide	Contains information about security considerations and best practices from a network and application security perspective for the Oracle Communications Session Border Controller family of products.
Installation and Platform Preparation Guide	Contains information about upgrading system images and any pre-boot system provisioning.
Call Traffic Monitoring Guide	Contains information about traffic monitoring and packet traces as collected on the system. This guide also includes WebGUI configuration used for the SIP Monitor and Trace application.
Header Manipulation Rule Guide	Contains information about configuring and using Header Manipulation Rules to manage service traffic.

Revision History

This section contains a revision history for this document.

Date	Description
April 2018	• Initial Release
May 2018	• Removes DTMF Detection limitation on VNF • Updates the "SIPREC Support for SRTP" item in New Features
May 2018	• Adds Caveat stating no 'packet trace remote' on the Acme Packet 3900 • Moves ACMECSBC-26311 to caveats • Removes ACMECSBC-28444 • Adds the High Availability issue and workaround to Caveats.

Date	Description
June 2018	• Adds Supported Ethernet Controller table to Platform Support section. • Removes known issue on ims-aka option • Updates HDR, MIB and ACLI element with pre-alerting feature in 810M1. • Adds Pooled Transcoding Caveat. • Adds Pooled Transcoding Known Issues.
July 2018	• Adds the Acme Packet 3900 IPSec Limitations Caveat. • Adds the Known Issue about getting IPSec support for the Acme Packet 3900 and VNF • Adds the IPSec license display on VNF Known Issue. • Updates the Pooled Transcoding list of supported hardware/software combinations.
September 2018	• Updates for SCZ810M1 • Corrects KVM component version list • Removes outdated caveat on monitoring KVM Kernel development for additional NIC support • Moves QoS for transcoded calls caveat to "Older Caveats Fixed in This Release" • Removes VNF limitation on DTMF generation • Adds "New Features in 8.1.0M1" chapter. • Updates typographical error within the Known Issues table. • Updates location in full doc set of new features. • Adds the VM initial boot Known Issue.
October 2018	• TLS1.0 not supported by default in compatibility mode
November 2018	• Updated cipher list for tls-profile.
March 2019	• Adds "Maintain DSA-Based HDR and CDR Push Behavior" to "Upgrade and Downgrade Caveats". • Removes T.140-Baudot Relay from the list of features unsupported with pooled transcoding.
April 2019	• Adds explanation of change in HMR matching.
May 2019	• Updates SIPREC Support for SRTP section to indicate full support. • Updates "TLS Cipher Updates" to remove TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA384. • Updates the Known Issues table for accuracy.

Date	Description
June 2019	• Adds Daylong Transcoding Session Cleanup feature to New Features chapter. • Adds OCOM incompatibility with IPv6 to known issues.
July 2019	• Adds TSM SDK section to "Coproduct Support."
October 2019	• Adds MSRP Known Issue to Known Issues table. • Updates "Behavioral Changes," "Deprecated Features," and "SNMP/MIB Changes" to account for MIB object deprecation.
November 2019	• Clarifies generic upgrade path statement • Adds trace tool limitations to "Trace Tools" caveat.
December 2019	• Updates Known Issues list
July 2020	• Repairs confusing known issue on IPv6 and VLANs • Updated for S-Cz8.1.0M1P24.

1
Introduction to S-CZ8.1.0

The Oracle Communications Session Border Controller *Release Notes* provides the following information about S-CZ8.1.0 release:

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

Platform Support

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

Acme Packet Engineered Hardware

The following platforms are supported by the S-CZ8.1.0 version of the OCSBC:

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

The following platforms are supported by the S-CZ8.1.0 version of the OCSR:

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

Qualified Hypervisors

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

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

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

Supported Ethernet Controller/Driver/Input-Output Modes

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

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

- W - wancom interface
- M - media interface

Supported Cloud Computing Platforms

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

Virtual Machine Platform Resources

A Virtual Network Function (VNF) requires the CPU core, memory, disk size, and network interfaces specified for operation. The Oracle Communications Session Border Controller (OCSBC) uses the Intel Data Plane Development Kit (DPDK) for datapath design, which imposes specific VNF resource requirements for CPU cores. Deployment details, such as the use of distributed DoS protection, dictate resource utilization beyond the defaults.

You configure CPU core utilization from the ACLI based on your deployment. You can also define memory and hard disk utilization based on your deployment. You must configure the hypervisor with the appropriate settings prior to startup, if you need settings other than the machine defaults set by the machine template (OVA).

Default VM Resources

VM resource configuration defaults to the following:

- 4 CPU Cores
- 16 GB RAM

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

Interface Host Mode

The OCSBC S-CZ8.1.0 VNF supports interface architectures using Hardware Virtualization Mode - Paravirtualized (HVM-PV):

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

> **Note:**
>
> When deploying the 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-CZ8.1.0 VNF requires an Intel Core2 processor or higher, or a fully emulated equivalent including 64-bit SSSE3 and TSC support.

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

Image Files and Boot Files

For Engineered Hardware

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

- Image file: `nnSCZ810.bz`.
- Bootloader file: `nnSCZ810.boot`.

For Virtual Machines

The OCSBC S-CZ8.1.0 version includes distributions suited for deployment over hypervisors. Download packages contain virtual machine templates for a range of virtual architectures. Use the following distributions to deploy the OCSBC as a virtual machine:

- `nnSCZ810-img-vm_ovm.ova`—Open Virtualization Archive (.ova) distribution of the OCSBC VNF for Oracle (XEN) virtual machines.
- `nnSCZ810-img-vm_kvm.tgz`—Compressed image file including OCSBC VNF for KVM virtual machines.

- `nnSCZ810-img-vm_vmware.ova`—Open Virtualization Archive (.ova) distribution of the OCSBC VNF for ESXi virtual machines.
- `nnSCZ810_HOT.tar.gz`—The Heat Orchestration Templates used with OpenStack.

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

- Product software—Bootable image of the product allowing startup and operation as a virtual machine. This disk image is in either the vmdk or qcow2 format.
- `usbc.ovf`—XML descriptor information containing metadata for the overall package, including identification, and default virtual machine resource requirements. The .ovf file format is specific to the supported hypervisor.
- `legal.txt`—Licensing information, including the Oracle End-User license agreement (EULA) terms covering the use of this software, and third-party license notifications.

For COTS Platforms

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

- Image file: `nnSCZ810.bz`.
- Bootloader file: `nnSCZ810.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.

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

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

- S-CZ7.4.0 -> S-CZ8.1.0
- S-CZ8.0.0 -> S-CZ8.1.0

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 and Downgrade Caveats

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

License Keyed Feature Reactivation

On the Acme Packet 1100 and VNF platforms, the software TLS and software SRTP features no longer require license keys. After you upgrade either platform to S-CZ8.1.0, 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 Cz8.1.0, you must manually reset the rsa_ssh.key when the host OpenSSH client version is 7.6 or newer. Applies to all platforms.

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

Upgrading Systems Running IMS-AKA DDoS

When upgrading an OCSBC running IMS-AKA DDoS and HA from S-CZ7.4.0 and later to S-CZ8.1.0, you must upgrade and simultaneously reboot both the active and secondary nodes. This properly clears ACLs built by the earlier version, allowing the system to instantiate new, operational ACLs.

IMS-AKA DDoS is not supported in releases prior to S-Cz7.3.0M1. Upgrades from those versions to S-Cz8.0.0 do not require this simultaneous reboot.

Reset Local Passwords for Downgrades

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

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

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

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

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

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

   Are you sure [y/n]
   ```

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

Time Division Multiplexing

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

Set IPSec Support for Acme Packet 3900 and VNF

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

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-CZ8.1.0, perform the following procedure:

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

Self-Provisioned Entitlements

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
Admin Security	boolean
Accounting	boolean
IPv4 - IPv6 Interworking	boolean
IWF (SIP-H323)	boolean
Load Balancing	boolean
Policy Server	boolean
Quality of Service	boolean
Routing	boolean
SIPREC Session Recording	boolean
Advanced Security Suite (JITC)	boolean
ANSSI R226 Compliance	boolean
IMS-AKA Endpoints	Integer
IPSec Trunking Sessions	Integer
MSRP B2BUA Sessions	Integer
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

The following features are enabled 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

Feature	Type
R226 SIPREC	boolean

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 limit** command.

Transcoding Support

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

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

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

Oracle Communications Session Router Platform Requirements

The Oracle Communications Session Router, release S-CZ8.1.0 supports the following platforms:

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

Coproduct Support

The products/features listed in this section run in concert with the Oracle Communications Session Border Controller for their respective solutions.

Oracle Communications TSM SDK

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

- 1.5

- 1.6

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 the A-SBC/P-CSCF function is based on S-CZ8.1.0 software, the following hardware/software combinations may be used as a T-SBC in a pooled transcoding scenario:

- Acme Packet 4600, with transcoding hardware (TM2): S-CZ7.4.0+, S-CZ8.0.0+, S-CZ8.1.0+
- Acme Packet 6300, with transcoding hardware (TM2): S-CZ7.4.0+, S-CZ8.0.0+, S-CZ8.1.0+
- Acme Packet 6350, with transcoding hardware (TM2): S-CZ8.0.0+, S-CZ8.1.0+

Oracle Communications Session Element Manager

Oracle Communications Session Element Manager (SEM) versions 8.1 and later, with the SD-plugin 2.0 and later, will be required to support this GA release of the Oracle Communications Session Border Controller due to the R226 features supported. Previous SDM releases and plugin versions are not able to support this GA release. Contact your Sales representative for further support and requirement details.

TLS Cipher Updates

Note the following changes to the DEFAULT cipher list.

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

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

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

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256

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

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA

- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Oracle supports the following ciphers for debugging purposes only:

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

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

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

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

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

Deprecated Features

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 your 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

Feature	Description	First Deprecated
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	• 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: • DES privacy protocol • MD5 and SHA authentication protocols	SCZ8.1.0
apEnvMonVoltageStatusEntry MIB object	The apEnvMonVoltageStatusEntry objects have been deprecated. Voltage monitoring is still available using the **show voltage** command in the ACLI.	SCZ8.1.0m1p6

The following features were deprecated prior to this release.

Feature	Description	First Deprecated
DES-CBC Ciphers	The OCSBC deprecates the following ciphers, adhering to recent OpenSSL changes intended to eliminate weak ciphers: • All DES-CBC ciphers, including: – TLS_DHE_RSA_WITH_DES_CBC_SHA – TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA 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. **Note:** Your version of the ACLI may still prints these ciphers when you run **cipher-list ?**. Despite printing them in ACLI output, the system does not support them within service operations.	SCZ740m1
FTP Support	The OCSBC's FTP Server is not supported. Only FTP client services are supported. For example, FTP client service for HDR/CDR push is supported. Note that both the SFTP client and server are supported.	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	The source routing feature as configured by **system-config**, **source-routing** is not supported. 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. **Note:** Despite deprecation, the parameter is still present in the **system-config**.	SCZ7.1.2
H.248	The Border Gateway and H.248 functionality are not supported.	SCZ7.1.2

Feature	Description	First Deprecated
HMR action on Call-ID	HMR operations on the Call-ID: header are not supported.	Prior to SCZ7.1.2
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: • 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 • DTMF IWF for H.323 • Media hairpinning involving H.323 and SIP	
SRTP	Linksys SRTP is not supported.	SCZ6.4.0

Documentation Changes

Note the following changes to the documentation for this release.

Entitlement and License Documentation

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

SNMP and MIB Documentation

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

Behavioral Changes

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

NAPTR Follow-Up Queries for A Records

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

External Policy Server Unreachable Alarm

The OCSBC issues an alarm when a connection to an external policy server configured for RACF or CLF fails. The OCSBC assigns these policy servers with a status of **Inactive** when:

- The TCP connection is closed by a RST or FIN.
- The Diameter CER/CEA exchange is not successful.
- The number of Diameter message timeouts exceeds the configured value.

Prior to this software version, the system raised an alarm only when all external policy servers in an HA cluster became unreachable. With this software version, the OCSBC issues this alarm when a connection to any member of a cluster fails. The OCSBC establishes an HA cluster when it receives multiple address as resolution to an FQDN request for a single **external-policy server** configured with an FQDN from a DNS server.

The ANSSI R226 Compliance and SIPREC Entitlements

The OCSBC supports self-entitlement for most product features. Be aware that the new ANSSI R226 Compliance entitlement interacts with the SIPREC entitlement to perform an ANSSI R226 function. When you enable ANSSI R226 Compliance, the OCSBC removes the SIPREC entitlement and any associated configuration.

The use of SIPREC is against ANSSI R226 Compliance. If, subsequently, you want to use SIPREC, you must obtain and install a SIPREC license.

You cannot simply disable the ANSSI R226 Compliance entitlement. After enabling ANSSI R226 Compliance the only way to remove it is to "zeroize" the OCSBC. See the Factory Reset section in the *Administrative Security Essentials Guide*.

The ANSSI R226 Compliance Entitlement and Boot Parameter Security

When the ANSSI R226 Compliance entitlement is set, the OCSBC ignores attempts to modify security related boot flags from the ACLI. The OCSBC still supports changing security related bootflags through the bootloader.

After enabling ANSSI R226 Compliance, the only way to remove the entitlement is to "zeroize" the OCSBC.

SNMPv3

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

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

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

- DES privacy protocol
- MD5 and SHA authentication protocols

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

TLS1.0

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

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

HMR Regex Matching Changes

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

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

Voltage Monitoring

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

Patch Equivalency

Patch equivalency indicates which patch content in neighbor releases is included in this release. This assures you that in upgrading, defect fixes in neighbor stream releases are included in this release.

Patch Equivalency for SCZ810

Neighbor Release Patch Equivalency for S-Cz8.1.0 GA:

- S-Cz7.4.0m1p6

The patch baseline, the most recent build from which the GA build was created, is SCZ800p2.

Patch Equivalency for SCZ810M1

Neighbor Release Patch Equivalency for S-Cz8.1.0M1

- S-CZ8.0.0p4
- S-Cz7.4.0m1p9

The patch baseline, the most recent build from which the GA build was created, is SCZ810p1.

Supported SPL Engines

The following SPL engine versions are supported by this software:

- C2.0.0
- C2.0.1
- C2.0.2
- C2.0.9
- C2.1.0
- C2.1.1
- C2.2.0
- C2.2.1
- C2.3.2
- C3.0.0
- C3.0.1
- C3.0.2
- C3.0.3
- C3.0.4
- C3.0.6
- C3.0.7
- C3.1.0
- C3.1.1
- C3.1.2
- C3.1.3
- C3.1.4
- C3.1.5
- C3.1.6
- C3.1.7
- C3.1.8
- C3.1.9

2

New Features in OCSBC Release S-CZ8.1.0

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

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

Software Transcoding

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

- AMR
- AMR-WB

DNS A Record Queries

Based on response messaging from DNS queries, the system can now generate A record queries.

Non-recursive DNS Query Support

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

DTMF IWF for VNF

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

Restricting Logons to TACACS

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

UEFI Boot Loader Support

The Oracle Communications Session Border Controller (OCSBC) supports 64-bit Unified Extensive Firmware Interface (UEFI) mode in addition to BIOS mode. This allows support over applicable platforms, including the Oracle X7-2 server where it exists as a bare metal platform.
See the *Platform Preparation and Installation Guide*.

FAX Support for UEs that Do Not Support Multiple M Lines

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

Load Balancing for the Rx Interface

The Oracle Communications Session Border Controller (OCSBC) allows you to configure load balancing for DIAMETER Rx traffic across multiple Diameter Routing Agents (DRAs) using the **external-policy-server** configuration. When configured for TCP transport, this load balancing is available in addition to standard, DNS-based redundancy, where the OCSBC uses fully qualified domain names (FQDNs) to cycle through the multiple DRAs that DNS resolves to a single FQDN. For SCTP transport, the OCSBC simply substitutes the first address provided by a DNS lookup as the DRA connection address, and only uses **policy-group**s for load balancing.
See "External Policy Servers" in the *ACLI Configuration Guide*.

SCTP Support for the Rx Interface

The OCSBC now allows you to communicate over the Rx Interface using SCTP transport.

See "External Policy Servers" in the *ACLI Configuration Guide*.

New AVPs for the Rx Interface

The OCSBC now supports the service-info-status and rx-request-type AVPs. The OCSBC uses these AVPs to clarify signaling status.

See "External Policy Servers" in the *ACLI Configuration Guide*.

Oracle X7-2 Platform Support for the Oracle Communications Session Router

The OCSR can now run on the Oracle X7-2 platform.

See "Software Installation - Oracle X7-2 Platforms" in the *Platform Preparation and Installation Guide*.

Call Duration Counters

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

Local and Remote Call Termination Counters

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

Common Codec Support for Transcoded SIPREC Calls

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

SIPREC Support for SRTP

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

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

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

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

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

Provisioning Transcode Codecs

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

disables the codec for transcoding. Note that the system allows you to enable only the codecs supported for the platform that you are configuring.

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

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

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

Other applicable commands work as follows:

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

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

SNMPv3 Support

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

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

Import SSH Keys as Host Keys

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

Import a Private SSH Key

As an alternative to relying on the SSH keys generated by the Oracle Communications Session Border Controller, customers may import externally generated SSH keys for any configured **public-key** element. Because the OCSBC derives the public key from the private key, only the private key needs to be imported, and any previously generated keys for this **public-key** element will be overwritten. The OCSBC uses

these keys when it functions as an SFTP client. See " Import a Private SSH Key for the OCSBC as an SFTP Client" in the *ACLI Configuration Guide*.

Delete an SSH Key

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

Daylong Transcoding Session Cleanup

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

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

3

New Features in OCSBC Release S-CZ8.1.0M1

The following information lists and describes features newly developed or newly released for S-CZ8.1.0M1.

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

The Subscriber Aware Load Balancer as a Virtual Machine

The S-CZ8.1.0M1 software version supports the Oracle Communications Subscriber Aware Load Balancer (OCSLB) deployed as a Virtual Network Function.

Full information about the OCSLB is available in th Oracle Communications SLB Essentials Guide.

SRVCC in the Pre-Alerting Phase

In addition to other SRVCC support, the Oracle Communications Session Border Controller (OCSBC) supports procedures to manage the handover from 4G to 3G/2G of sessions in pre-alerting phase. The conditions by which a session is defined as in the pre-alerting phase include the calling party has not yet received a 180 RINGING message.

This feature description is found in the *ACLI Configuration Guide*, IMS Support chapter.

SIP-Forking-Indication AVP

When handling access VoLTE sessions with multiple early dialogs, the Oracle Communications Session Border Controller (OCSBC), acting as A-SBC or P-CSCF, includes the **SIP-Forking-Indication** AVP in the Rx request sent to the PCRF. This occurs when the OCSBC receives several responses (provisional or not) with different To-Tag identifiers and different SDP.

This feature description is found in the *ACLI Configuration Guide*, External Policy Servers chapter.

4
Inherited Features

Feature descriptions found in this chapter are inherited (forward merged) from the following Oracle Communications Session Border Controller releases:

- S-CZ7.3.0M3
- S-CZ7.4.1

The S-CZ8.1.0 GA documentation set does not include the following features:

Bootparameter Security for R226

An Oracle Communications Session Border Controller ignores attempts to modify security related boot flags from the ACLI. The OCSBC still supports changing security related boot flags through the bootloader.
See the "R226 Security Recommendation Compliance" chapter in the *ACLI Reference Guide*.

SHA2 Password Hashing

The Oracle Communications Session Border Controller supports SHA-2 hashing of user login passwords. The OCSBC hashes passwords using a randomly generated salt with 65532 iterations of the SHA-512 algorithm.
See the "R226 Security Recommendation Compliance" chapter in the *ACLI Reference Guide*.

SFTP Access Restrictions for R226

In the default restricted mode, the normal user and admin user are restricted from adding, deleting, renaming, or modifying sensitive system files when accessing the file system with SFTP. Although setting the boot flag to `0x01000000` allows access to sensitive files, if the **ANSSI R226 Compliance** entitlement is enabled, all boot flags are reset to zero during a reboot and can only be set through the bootloader.
See the "R226 Security Recommendation Compliance" chapter in the *ACLI Reference Guide*.

Import SSH Keys as Host Keys

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

Import a Private SSH Key

As an alternative to relying on the SSH keys generated by the Oracle Communications Session Border Controller, customers may import externally generated SSH keys for any configured **public-key** element. Because the OCSBC derives the public key

from the private key, only the private key needs to be imported, and any previously generated keys for this **public-key** element will be overwritten. The OCSBC uses these keys when it functions as an SFTP client.
See "Import a Private SSH Key for the OCSBC as an SFTP Client" in the *ACLI Configuration Guide*.

Delete an SSH Key

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

Secure the ACP Comm Link with TLS

You can use the Transport Layer Security (TLS) protocol to secure the communications link between the Oracle Communications Session Border Controller (OCSBC) and the Oracle Communications Session Delivery Manager (SDM). Note that the systems use Acme Control Protocol (ACP) for this messaging.
See "Securing Communications Between the OCSBC and SDM with TLS" in the *ACLI Configuration Guide*.

AAA Authentication for ACP

To authenticate SDM by way of an external AAA server connected to the OCSBC, the OCSBC supports ACP authentication using the HTTP Basic Authentication Scheme. By using ACP over TLS, the OCSBC exchanges RADIUS or TACACS+ encrypted passwords and shared keys securely.
See the *Administrative Security Guide*.

5

Interface Changes

This chapter summarizes ACLI, SNMP, HDR, Alarms, and RADIUS changes (where applicable) for S-CZ8.1.0. Additions, removals, and changes appearing in this chapter are since the previous major release of the Oracle Communications Session Border Controller.

ACLI Command Changes

This section summarizes the ACLI command changes that first appear in the Oracle Communications Session Border Controllerrelease S-CZ8.1.0

Command	Description
show policy-server connections	Modified to add information about the current connections/associations. The command displays the active path in the stats.
show policy-server <server name>	Modified to add application stats about that particular server, as well as summary stats
request collection start (and stop)	Adds new collection groups, including traffic counters for: • sip-method • sip-realm-method • sip-interface-method • sip-agent-method Single radio voice call continuity counter • sip-srvcc External policy server counter: • ext-rx-policy-server Security related counters, including: • sa-ike • sa-imsaka • sa-srtp Transcoding related counters, including: • xcode-session-gen-info • xcode-codec-util • xcode-tcm-util
show sessions	Adds new counter row to SIP statistics section for Messaging Sessions.
show sipd status	Adds new counter row for SMS Messages. Also adds 2 new counter rows that display Local and Normal call drops. Also adds new counter row that displays call duration times.
show sipd agents	Adds 2 new counter rows that display Local and Normal call drops. Also adds new counter rows that display inbound and outbound call duration times.

Command	Description
show sipd realms	Adds 2 new counter rows that display Local and Normal call drops. Also adds new counter rows that display inbound and outbound call duration times.
show sipd interface	Adds 2 new counter rows that display Local and Normal call drops. Also adds new counter rows that display inbound and outbound call duration times.
show sipd codecs	Modified to add **EVS Count**.
show sipd transcode	Modified to add **EVS**.
show xcode load	Modified to add **EVS**
show xcode codecs	Modified to add **EVS-AMR-WB** sessions.

ACLI Configuration Element Changes

This section summarizes the ACLI configuration element changes that first appear in release Oracle Communications Session Border ControllerS-CZ8.1.0

Security Features

New Parameters	Description
security, **authentication**, **tacacs-authentication-only**	Adds the **tacacs-authentication-only** parameter to restrict login authentication to TACACS if it is available.
security, **ssh-config**	Element that provides access to global SSH configuration settings.
security, **ssh-config**, **keyex-algorithms**	Allows you to specify which key exchange algorithms are offered during SSH session negotiation
security, ssh-config, **hostkey-algorithms**	Allows you to specify which host key algorithms are offered during SSH session negotiation
security, **ssh-config**, **encr-algorithms**	Allows you to specify which encryption algorithms are offered during SSH session negotiation
security, **ssh-config**, **hmac-algorithms**	Allows you to specify which HMAC algorithms are offered during SSH session negotiation
security, **tls-profile**, **cipher-list**	The default value has changed from **all** to **default**.
security, **tls-profile**, **tls-version**	The **SSLv3** option is no longer supported.
security, **ike**, **tls-config**, **ike-version**	The parameter now accepts version 2 as a value. Although version 2 is available for configuration, it is supported only for LI interfaces. Available in S-CZ8.1.0M1

ENUM Features

New Parameters	Description
session-router, **enum-config**, **remote-recursion**	Adds the **remote-recursion** parameter to allow the user to disable ENUM server

VoLTE Features

New Parameters	Description
session-router, **sip-interface**, **charging-vector-mode**	Adds the **conditional-insert** parameter to specify header insertion behavior based on original message content.
session-router, **sip-interface**, **charging-function-address-mode**	Adds the **conditional-insert** parameter to specify header insertion behavior based on original message content.
session-router, **sip-feature-caps**	Adds the **pre-alerting** parameter to enable SRVCC support during the pre-alerting phase. Released with S-CZ8.1.0M1

External Policy Server Features

New Parameters	Description
media-manage, **policy-group**	Defines a group of policy servers for load balancing. Parameters include: • group-name—policy server group name • description— • state—administrative state • policy-agents— • strategy—strategy for rotating destinations • max-recursions—Max number of recursions • stop-recurse—Response codes that stop recursion • recursion-timeout—DIAMETER transaction expiration timer (secs)

New Parameters	Description
media-manager, **policy-group**, **policy-agent**	Defines the policy servers for load balancing within the context of the policy group. Parameters include: • name—policy agent name • description— • state—administrative state • address—FQDN/IP Address address of external bandwidth manager • port—port • realm—name of realm to send requests on • watch-dog-ka-timer—watchdog/keep-alive msg interval • transport-protocol—transport protocol • local-multi-addr-list—Multihomed IP Address • remote-multi-addr-list—Multihomed IP Address • sctp-send-mode—SCTP message delivery mode ordering
media-manager, **ext-policy-server**, **transport-protocol**	Select a specified protocol or the special value all that specifies transport-protocol based matching criteria for inbound and outbound traffic. • Default: TCP • Values: SCTP | TCP
media-manager, **ext-policy-server**, **local-multi-homing**	if the remote primary address is not reachable, the SCTP association fails even if an alternate path is possible. Assigns the local address that the remote station can use for multi-homing redundancy.
media-manager, **ext-policy-server**, **remote-multi-homing**	Assigns the remote address that the local station can use for multi-homing redundancy.
media-manager, **ext-policy-server, sctp-send-mode**	Leave this parameter set to its default (unordered) so data delivery can occur without regard to stream sequence numbering. If data delivery must follow stream sequence number, change this parameter to ordered. • Default: unordered • Values: ordered | unordered

Transcoding Features

New Parameters	Description
media-manager, **codec-policy**, **fax-single-m-line**	Set this parameter to the preferred FAX media type for Re-INVITEs to endstations that do not support multiple m-lines. The system issues Re-INVITEs using the configured media type only. Should the negotiation fail, the system issues another Re-INVITE that offers the other media type.

Message Counter Features

The following new components appear within the following **session-router** elements, using the listed order to define configuration precedence:

1. **session-agent**
2. **sip-interface**
3. **realm-config**

New Parameters	Description
sm-icsi-match-for-invite	<pattern> (i.e. Large Message Mode Standalone message). E.g: urn:urn-7:3gpp-service.ims.icsi.oma.cpm.largemsg (as per ABNF mentioned in RFC-6050) match icsi value for INVITE
sm-icsi-match-for-message	<pattern> (i.e. Pager mode Standalone message). E.g: urn:urn-7:3gpp-service.ims.icsi.oma.cpm.msg (as per ABNF mentioned in RFC-6050) match icsi value for MESSAGE

HDR Features

New Parameters	Description
system, **system-config**, **collect**, **group-settings**, **group-name**	Adds new collection groups, including traffic counters for: • sip-method • sip-realm-method • sip-interface-method • sip-agent-method Single radio voice call continuity counter • sip-srvcc External policy server counter: • ext-rx-policy-server Security related counters, including: • sa-ike • sa-imsaka • sa-srtp Transcoding related counters, including: • xcode-session-gen-info • xcode-codec-util • xcode-tcm-util SIP traffic counters, including: • sip-method • sip-realm-method • sip-interface-method • sip-agent-method

TLS Features

New Parameters	Description
security, **tls-profile**, **cipher-list**	The default value for this parameter is changed to **Default** in this software version. This prevents the former default of **All** from including ciphers that Oracle has deemed weak. In addition, the cipher list has been updated to the following (for tlsv1, tlsv11, tlsv12 and compatibility): • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA, • TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA • TLS_RSA_WITH_3DES_EDE_CBC_SHA • TLS_RSA_WITH_NULL_SHA256 • TLS_RSA_WITH_NULL_SHA • TLS_RSA_WITH_NULL_MD5 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 • DEFAULT • ALL • NONE

SNMP/MIB Changes

This section summarizes the SNMP/MIB changes that appear in the Oracle Communications Session Border Controller version S-CZ8.1.0.

MIB Changes for EVS

This section presents SNMP changes made to support EVS.

ap-codec.mib

Object Name/OID	Description
apCodecRealmCountEVS 1.3.6.1.4.1.9148.3.7.1.1.1.33	The count of SDP media streams received in the realm which negotiated to the EVS codec.

ap-smgmt.mib

Object Name/OID	Description
apSysXCodeEVSCapacity 1.3.6.1.4.1.9148.3.2.1.1.49	The percentage of licensed EVS transcoding utilization (non pollable).
apSysMgmtXCodeEVSUtilGroup 1.3.6.1.4.1.9148.3.2.4.2.35	Object to monitor licensed EVS transcoding utilization.

New Traps - New SNMP OID **apSysXCodeEVSCapacity** is added to transcoding utilization statistics as reported in the **apSysMgmtGroupTrap**. When utilization falls below 80%, the **apSysMgmtGroupClearTrap** is sent.

Trap Name (clear trap)	Description
apSysMgmtCPULoadAvgTrap (apSysMgmtCPULoadAvgClearTrap)	The trap will be generated when CPU Load Average Alarm exceeds its minor alarm threshold. The clear trap will be sent when the CPU load average recedes to the minor alarm level.

Capability MIBs

Object Name/OID	MIB file
apSmgmtXCodeEVSUtilCap 1.3.6.1.4.1.9148.2.1.8.59	ap-smgmt.mib
apCodecRealmCodecCap9 1.3.6.1.4.1.9148.2.1.13.11	ap-codec.mib

MIB Changes for Policy Server Objects

This table presents a policy server table miboid that is new to this version.

Object Name/OID	MIB file
apDiamRxPolicyServerStatsTable 1.3.6.1.4.1.9148.3.13.1.1.2.3	ap-diameter.mib

Security-Related MIB Changes

This table lists Session agent counter and SRTP Session Agent counter table miboids that are new to this version.

Object Name/OID	MIB file
apSecuritySAIKEStats 1.3.6.1.4.1.9148.3.9.5.1	ap-security.mib
apSecuritySASRTPStats 1.3.6.1.4.1.9148.3.9.5.3	ap-security.mib

MIB Changes for IMS-AKA

This table presents an IMS-AKA counter table miboid that are new to this version.

Object Name/OID	MIB file
apSipSRVCCStatsobjects 1.3.6.1.4.1.9148.3.15.1.1.3	ap-sip.mib

MIB Changes for Transcoding

This table lists transcoding-related miboids that are new to this version, in this order:

1. Active Transcoding Sessions
2. TCU load counters
3. Codec licensed capacities

Object Name/OID	MIB file
apCodecTranscodingResourceUtilMIBObjects 1.3.6.1.4.1.9148.3.7.2.5	ap-codec.mib
apCodecTranscodingTCULoadStatsTable 1.3.6.1.4.1.9148.3.7.2.6.1	ap-codec.mib
apLicenseEntry 1.3.6.1.4.1.9148.3.5.1.1.1	ap-license.mib

MIB Changes for Licensing

This table presents codec miboids that are new to this version.

Object Name/OID	MIB file
1.3.6.1.4.1.9148.3.5.1.1.1	ap-license.mib

MIB Changes for SRVCC

This table presents SRVCC miboids that are new to this version. These OIDs were released with S-CZ8.1.0M1.

Object Name/OID	MIB file
1.3.6.1.4.1.9148.3.15.1.1.3.13	ap-sip.mib

Object Name/OID	MIB file
1.3.6.1.4.1.9148.3.15.1.1.3.14	ap-sip.mib
1.3.6.1.4.1.9148.3.15.1.1.3.15	ap-sip.mib

MIB Changes for TACACS

Trap Name apSysMgmtTacacsDownLocalAuthUsedTrap (ap-smgmt.mib)Trap OID 1.3.6.1.4.1.9148.3.2.6.0.88

This trap is generated when a user remotely logs into a system configured for TACACS+ authentication and is authenticated locally by the system because all of the configured and enabled TACACS+ servers have become unreachable or unresponsive.

Trap Name apSysMgmtTacacsDownLocalAuthUsedClearTrap (ap-smgmt.mib)Trap OID 1.3.6.1.4.1.9148.3.2.6.0.89

This trap is generated when a user remotely logs into a system configured for TACACS+ authentication and is successfully authenticated (i.e., access accepted or denied) remotely by a configured and enabled TACACS+ server.

MIB Changes for Voltage Monitoring

Starting in S-Cz8.1.0m1p6 and later, apEnvMonVoltageStatusValue MIB objects have been deprecated.

Alarms

This section summarizes the Alarm changes that appear in the Oracle Communications Session Border Controller version S-CZ8.1.0.

EVS

The Licensed EVS Transcoding Capacity Threshold Alarm is a warning triggered when the EVS transcoding utilization exceeds 95% of licensed capacity. This alarm that does not affect the system's health score. The alarm is cleared when the EVS transcoding utilization falls below 80% of licensed capacity.

TACACS-only Authentication

Associated Alarms APP_ALARM_TACACS_DOWN_LOCAL_AUTH_USED (327721)

Accounting

This section summarizes the accounting changes that appear in the Oracle Communications Session Border Controller version S-CZ8.1.0.

RADIUS

Acme-FlowType_FS{1,2}_{F,R} AVPs reflect the use of the EVS codec.

HDR

This section summarizes the HDR changes that appear in the Oracle Communications Session Border Controller version S-CZ8.1.0.

New HDR Groups

This software version adds new HDR groups to the collect, group, group-name These HDR groups are documented in this release's *HDR Guide*.

HDR Features

New Parameters	Description
system, **system-config**, **collect**, **group-settings**, **group-name**	Adds new collection groups, including traffic counters for: • sip-method • sip-realm-method • sip-interface-method • sip-agent-method Single radio voice call continuity counter • sip-srvcc External policy server counter: • ext-rx-policy-server Security related counters, including: • sa-ike • sa-imsaka • sa-srtp Transcoding related counters, including: • xcode-session-gen-info • xcode-codec-util • xcode-tcm-util SIP traffic counters, including: • sip-method • sip-realm-method • sip-interface-method • sip-agent-method
system, **system-config**, **collect**, **group-settings**, **group-name**, **srvcc**	• Adds pre-alerting statistics to **sip-srvcc** group Released with S-CZ8.1.0M1

6
Older Caveats Fixed in This Release

The following caveats have been fixed in SCZ8.1.0:

- QoS reporting is now supported for transcoded calls.

7

Caveats and Limitations

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

Provisioning Transcode Codec Session Capacities

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

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

Virtual Network Function (VNF) Caveats

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

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

Transcoding - general

Only SIP signaling is supported with transcoding.

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

T.38 Fax Transcoding

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

Pooled Transcoding for Fax is unsupported.

Pooled Transcoding

The following media-related features are not supported in pooled transcoding scenarios:

- Lawful intercept
- 2833 IWF
- Fax scenarios
- RTCP generation for transcoded calls
- OPUS/SILK codecs
- SRTP and Transcoding on the same call
- Asymmetric DPT in SRVCC call flows
- Media hairpinning
- QoS reporting for transcoded calls
- Multiple SDP answers to a single offer
- PRACK Interworking
- Asymmetric Preconditions

DTMF Interworking

RFC 2833 interworking with H.323 is unsupported.

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

H.323 Signaling Support

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

Media Hairpinning

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

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 reboot.

SRTP Caveats

The ARIA cipher is not supported by virtual machine deployments.

Packet Trace

- VNF deployments do not support the **packet-trace remote** command.
- The Acme Packet 3900 does not support the **packet-trace remote** command.
- 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.

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.

Virtual Network Function (VNF) Limitations

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

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

- RTCP generation for G.711 or G.729
- RTCP detection
- TSCF functionality
- 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.

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.

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.

8
Known Issues

This table lists OCSBC known issues in version S-CZ8.1.0. 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	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.	S-Cz8.1.0	S-Cz8.1.0m1p18
31373813	If upgrading TO any of the following releases FROM any prior release and you have IPSEC or IMS-AKA enabled and are configured in an HA configuration, an In-Service upgrade is not supported. • S-Cz8.1.0m1p23 • S-Cz8.1.0m1p24 • S-Cz830m1p5 • S-Cz830m1p6 • S-Cz830m1p7 • S-Cz830m1p8 You must upgrade both systems in the HA pair and perform a simultaneous reboot for HA synchronization to work in the above upgrade scenario. This also applies to a downgrade FROM the above releases TO prior releases. For example, if you are running S-CZ8.1.0M1P23 and decide to downgrade to S-Cz8.1.0M1P21, you will need to install the prior version (Cz8.1.0M1P21) on both systems in the HA pair and execute a simultaneous reboot. If you are already running one of the above releases and are upgrading between them, this step is unnecessary and in-service upgrades are supported.	3	S-Cz8.1.0m1p23
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.	SCZ740	TBD
24574252	The **show interfaces brief** command incorrectly shows **pri-util-addr** information in its output.	SCZ740	TBD
26790731	Running commands with very long output, such as the "show support-info" command, over an OVM virtual console might cause the system to reboot. Workaround: You must run the "show support-info" command only over SSH.	SCZ800	TBD
26338219	The **packet-trace remote** command does not work with IPv6.	SCZ740	TBD

ID	Description	Found In	Fixed In
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.	SCZ800	TBD
26258705	The **show sipd srvcc** command does not display the correct number of unsuccessful aSRVCC calls.	SCZ800	TBD
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.	SCZ800	TBD
26559988	In call flows that include dual ALTC INVITEs from the callee, and subsequent Re-INVITEs that offer and 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 the video failing.	SCZ800	TBD
26313330	In some early media call flows, the OCSBC may not present the correct address for RTP causing the call to fail.	SCZ800	SCZ800p2, SCZ740m1p6
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	SCZ720	SCZ8.2.0
25144010	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.	SCZ740p1	SCZ810 SCZ740M1
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.	SCZ730	TBD
21805139	RADIUS stop records for IWF calls may display inaccurate values.	SCZ730b6	TBD
24809688	Media interfaces configured for IPv6, and using different VLANs that operate over different infrastructures, including VoLTE and 3GPP, are not supported.	SCZ730	TBD
	SIP-H323 hairpin calls with DTMF tone indication interworking is not supported.	S-CZ720	TBD
	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.	S-CZ740	TBD
None	HA Redundancy is not supported for H.323 calls.		TBD

ID	Description	Found In	Fixed In
21341383	If after upgrading to a S-CZ7.4.0 OCSR software image and its corresponding 7.3 stage3 boot loader, you decide to downgrade to a pre- S-CZ7.3.0 product release, you must install the corresponding 7.2 stage3 boot loader before rebooting with the older image.		TBD
23756306	When the session-router is configured with a operation-mode of session, it does not correctly clear sessions.	S-Cz7.2.0	TBD
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.	SCZ730M2	TBD
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 systems subsequently goes out of service.	SCZ800	SCZ740m1p1, SCZ800p1
21975038	MSRP File Transfer is not supported on the Acme Packet 4600, 6100, 6300, and 6350.	SCZ810	SCZ810p1
27579686	TSM is not supported in this release.	SCZ810	SCZ810p1
27699451	Oracle has 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.	SCZ810	TBD
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.	SCZ810	TBD
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.	SCZ810	TBD
27911939	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: • 4 forwarding cores • 8 signaling cores • IMS-AKA in use • High call traffic load	SCZ810	TBD
28062411	Calls that require SIP/PRACK interworking as invoked by the 100rel-interworking option on a SIP interface do not work in pooled transcoding architectures.	SCZ740	SCZ810m1
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.	SCZ740	SCZ810m1

ID	Description	Found In	Fixed In
None	IPSec is not supported on the Acme Packet 3900 and VNF in the CZ8.1.0 release. You must upgrade to CZ8.1.0p1 to get this support. After you upgrade to CZ8.1.0p1, do the following: 1. Run **setup entitlements**, again. 2. Select **advanced** to enable advanced entitlements, which then provides support for IPSEC on Acme Packet 3900 and VNF systems.	CZ810	CZ810p1
28305575	On VNFs, the system erroneously displays the IPSEC entitlement under "Keyed (Licensed) Entitlements." The error does not affect any functionality and you do not need to do anything.	CZ810	CZ820
28367500	When operating the OCSBC on the Acme Packet 6300, the **traceroute** command does not show hops for an IPv6 traceroute that does not reach the target address. The system successfully displays hops when the traceroute reaches the target and for IPv4 traceroutes.	CZ810	TBD
28617938	The **anonymize-invite** option for CommMonitor is not RTC. To see a change, you must either reboot or toggle the admin state. The following is a general admin state toggle procedure: 1. Set admin state to disabled. 2. Save and activate. 3. Set admin state to enabled. 4. Save and activate.	CZ810m1	TBD
28618563	The system is not populating the Username AVP in Accounting Requests (ACRs) correctly. When triggered by an INVITE, these AVPs contain only the "@" sign. They do not include the username and domain name portion of the URL.	CZ810m1	TBD
28659469	When booting CZ8.1.0M1 on any virtual platform, not all system processes start. This known issue only occurs on initial boot, and not in an upgrade scenario. Workaround: Reboot the OCSBC a second time, after it initially starts.	CZ810m1	TBD
29931732	The embedded communications monitor probe does not send IPv6 traffic to the Oracle Communications Operations Monitor's mediation engine.	SCZ800	TBD
28820258	When running TLS Chat on VMware-PV 4core (SSFD) + 16GB, TLS Chat sessions are gradually decreasing. When looking in Wireshark at EXFO, EXFO forwards a wrong TLS MSRP Chat payload to EXFO UAS. TCP Chat doesn't have this error.	SCZ800	TBC

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
27700607	When recording multiple transcoded streams under load, the recorder may only receive a single stream.	N/A	N/A
N/A	The T.140-Baudot Relay is not excluded from pooled transcoding support.	N/A	N/A