Oracle® Communications Session Border Controller and Session Router

Release Notes

Release S-Cz9.0.0
F41583-11
December 2023

ORACLE

Oracle Communications Session Border Controller and Session Router Release Notes, Release S-Cz9.0.0

F41583-11

Copyright © 2004, 2023, 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, software documentation, data (as defined in the Federal Acquisition Regulation), 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," "commercial computer software documentation," or "limited rights data" 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®, Java, MySQL and NetSuite 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

My Oracle Support vi

Revision History

1 Introduction to S-Cz9.0.0

Supported Platforms 1-1
- Supported Physical Platforms 1-1
- Supported Private Virtual Infrastructures and Public Clouds 1-2
- Requirements for Machines on Private Virtual Infrastructures 1-4
- PCIe Transcoding Card Requirements 1-6
- Oracle Communications Session Router Recommendations for Netra and Oracle Servers 1-7

Image Files and Boot Files 1-7
- Image Files for Customers Requiring Lawful Intercept 1-8
- Boot Loader Requirements 1-8
- Setup Product 1-8

Upgrade Information 1-10
- Upgrade Checklist 1-10
- Upgrade and Downgrade Caveats 1-10

Feature Entitlements 1-14
- Encryption for Virtual SBC 1-16

System Capacities 1-16
Transcoding Support 1-16
Coproduct Support 1-18
TLS Cipher Updates 1-19
Documentation Changes 1-20
Behavioral Changes 1-21
Patches Included in This Release 1-21
Supported SPL Engines 1-22

2 New and Deprecated Features

3 Interface Changes

ACLI Configuration Element Changes 3-1
ACLI Command Changes 3-3
Accounting Changes 3-4
SNMP/MIB Changes 3-4
Alarms 3-7
HDR 3-8
Errors and Warnings 3-11

About this Guide

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

Documentation Set

The following table lists related documentation.

Document Name	Document Description
Acme Packet 3900 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 3900.
Acme Packet 4600 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4600.
Acme Packet 4900 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 3950 and Acme Packet 4900.
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.
Known Issues & Caveats	Contains known issues and caveats
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 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 Guide	Contains information about the SBC's Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Admin Security Guide	Contains information about the SBC'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 SBC family of products.
Platform Preparation and Installation Guide	Contains information about upgrading system images and any pre-boot system provisioning.
Call Traffic Monitoring Guide	Contains information about traffic monitoring and packet traces as collected on the system. This guide also includes WebGUI configuration used for the SIP Monitor and Trace application.
HMR Guide	Contains information about configuring and using Header Manipulation Rules to manage service traffic.
REST API	Contains information about the supported REST APIs and how to use the REST API interface.

Documentation Accessibility

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

My Oracle Support

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

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

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

- For non-technical issues such as registration or assistance with My Oracle Support, select 2.

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

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

Emergency Response

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

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

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

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

Locate Product Documentation on the Oracle Help Center Site

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

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

Access to Oracle Support

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

Revision History

This section provides a revision history for this document.

Date	Revision
June 2021	• Initial release. • Adds AWS machine shapes. • Adds 'reset tacacs-stats' command. • Updates Known Issues table.
August 2021	• Update for the S-Cz9.0.0p1 patch. • Updates Pooled Transcoding support in "Co Product Support".
December 2021	• Updates for the S-Cz9.0.0p2 patch. • Adds "OCI Resource Manager" to "New Features". • Updates "Documentation Changes" to include the Platform Preparation and Installation Guide updates.
April 2022	• Updates for the S-Cz9.0.0p3 patch. • Corrects ESXi version support • Removes OVM platform support • Adds STIR/SHAKEN implementation update to New Features • Adds entitlement changes during upgrade in upgrade checklist section. • Updates Amazon Web Services instance sizes in Supported Public Cloud Platforms. • Adds support for the i40en driver with VMware • Adds surrogate-agent upgrade caveat
September 2022	• Corrects Ethernet Controller model XXV710 in "Supported Platforms." • Clarfies that known-host keys must be re-imported after an upgrade. • Updates "Supported Private Virtual Infrastructures and Public Clouds" and "Supported Ethernet Controller, Driver, and Traffic Type based on Input-Output Modes" with a note about media interface support. • Clarifies the requirement for media-policy for setting all DSCP codes on egress.
November 2022	• Updates HOT and Terraform boot files to 900p4.
February 2023	• Updates for OCSP feature.
May 2023	• Adds support for iavf driver for intel x7xx series cards.

Date	Revision
August 2023	• Adds SR entitlements. • Adds SDM upgrade caveat. • Adds new feature content at S-Cz9.0.0p10.
December 2023	• Adds Intel limitation for software transcoding.

1

Introduction to S-Cz9.0.0

The Oracle Communications Session Border Controller *Release Notes* provides the following information about S-Cz9.0.0 release:

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

Supported Platforms

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

Supported Physical Platforms

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

Acme Packet Platforms

The S-Cz9.0.0 version of the OCSBC supports the following platforms:

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

The S-Cz9.0.0 version of the OCSR supports the following platforms:

- Acme Packet 4600
- Acme Packet 6100
- Acme Packet 6300
- Netra Server X5-2

- Oracle Server X7-2
- Oracle Server X8-2
- Virtual Platforms

Supported Private Virtual Infrastructures and Public Clouds

The SBC can be run on the following Private Virtual Infrastructures, which include individual hypervisors as well as private clouds based on architectures such as VMware or Openstack.

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

> **Note:**
>
> Virtual SBCs do not support media interfaces when media interfaces of different NIC models are attached. Media Interfaces are supported only when all media interfaces are of the same model, belong to the same Ethernet Controller, and have the same PCI Vendor ID and Device ID.

Supported Hypervisors for Private Virtual Infrastructures

Oracle supports installation of SBC on the following hypervisors:

- KVM: Linux kernel version 3.10.0-123 or later, with KVM/QEMU (2.9.0_16 or later) and libvirt (3.9.0_14 or later)
- VMware: vSphere ESXi (Version 6.5 or later)

Compatibility with OpenStack Private Virtual Infrastructures

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

Supported Public Cloud Platforms

The SBC can be run on the following public cloud platforms.

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

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

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

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

- Amazon Web Services (EC2) - This table lists the AWS (ECs) instance sizes that apply to the SBC.

Instance Type	vCPUs	Memory (GB)	Max NICs
c5.xlarge	4	8	4
c5.2xlarge	8	16	4
c5.4xlarge	16	32	8
c5.9xlarge	36	72	8
c5.12xlarge	48	96	8
c5.18xlarge	72	144	15
c5n.xlarge	4	10.5	4
c5n.2xlarge	8	21	4
c5n.4xlarge	16	42	8
c5n.9xlarge	36	96	8
c5n.18xlarge	72	192	15

Driver support detail includes:

– ENA is supported on C5/C5n family only.

> **Note:**
>
> C5 instances use the Nitro hypervisor.

- Microsoft Azure - The following table lists the Azure instance sizes that you can use for the SBC.

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

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

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

Azure sizes that support and expose hyperthreading to the user includes the version 2, F series.

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

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

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

Platform Hyperthreading Support

Of the supported hypervisors, only VMware does not expose SMT capability to the SBC. Of the supported clouds, OCI, AWS, and, for their FS-v2 sized, Azure enable SMT by default and expose it to the SBC.

DPDK Reference

The SBC relies on DPDK for packet processing and related functions. You may reference the Tested Platforms section of the DPDK release notes available at https://doc.dpdk.org. This information can be used in conjunction with this Release Notes document for you to set a baseline of:

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

> **Note:**
>
> Oracle only qualifies a specific subset of platforms. Not all the hardware listed as supported by DPDK is enabled and supported in this software.

The DPDK version used in this release is:

- 20.11

Requirements for Machines on Private Virtual Infrastructures

In private virtual infrastructures, you choose the compute resources required by your deployment. This includes CPU core, memory, disk size, and network interfaces. Deployment details, such as the use of distributed DoS protection, dictate resource utilization beyond the defaults.

Default VSBC Resources

The default compute for the SBC image files is as follows:

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

Interface Host Mode for Private Virtual Infrastructures

The SBC 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.

Supported Interface Input-Output Modes for Private Virtual Infrastructures

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

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

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

> **Note:**
>
> Virtual SBCs do not support media interfaces when media interfaces of different NIC models are attached. Media Interfaces are supported only when all media interfaces are of the same model, belong to the same Ethernet Controller, and have the same PCI Vendor ID and Device ID.

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

Ethernet Controller	Driver	SR-IOV	PCI Passthrough
Intel 82599 / X520 / X540	ixgbe	M	M
Intel i210 / i350	igb	M	M
Intel X710 / XL710	i40e	M	M
Intel X710 / XL710 / XXV710	i40e, i40en[1], iavf[2]	M	M
Mellanox Connect X-4	mlx5	M	M

1 This driver is not supported on KVM.

2 iavf driver is support in SR-IOV n/w mode

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

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

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

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

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

CPU Core Resources for Private Virtual Infrastructures

The SBC S-Cz9.0.0 VNF requires an Intel Core i7 processor or higher, or a fully emulated equivalent including 64-bit SSSE3 and SSE4.2 support.

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

PCIe Transcoding Card Requirements

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

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

- VMWare and KVM are supported
- PCIe-pass-through mode is supported
- Each vSBC can support 2 PCIE 8120 cards and the server can support 4 PCIE 8120 cards.
- Each PCIe-8120 card supports only one vSBC instance
- Do not configure transcoding cores for software-based transcoding when using a PCIe media card.

Oracle Communications Session Router Recommendations for Netra and Oracle Servers

Oracle recommends the following resources when operating the OCSR, release S-Cz9.0.0 over Netra and Oracle Platforms.

Hardware recommendations for Netra Server X5-2

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

Hardware recommendations for Oracle Server X7-2

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

Hardware recommendations for Oracle Server X8-2

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

Image Files and Boot Files

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

For Acme Packet Platforms

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

- Image file: `nnSCZ900.bz`
- Bootloader file: `nnSCZ900.boot`

For Virtual Platforms

This S-Cz9.0.0 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:

- `nnSCZ900-img-vm_ovm.ova`—Open Virtualization Archive (.ova) distribution of the SBC VNF for Amazon EC2.

- `nnSCZ900-img-vm_kvm.tgz`—Compressed image file including SBC VNF for KVM virtual machines, Oracle Cloud Infrastructure (OCI), EC2 Nitro, and AWS C4 and C5 instances.
- `nnSCZ900-img-vm_vmware.ova`—Open Virtualization Archive (.ova) distribution of the SBC VNF for ESXi virtual machines.
- `nnSCZ900p4_HOT.tar.gz`—The Heat Orchestration Templates used with OpenStack.
- `nnSCZ900p4_tfStackBuilder.tar.gz`—The Terraform templates used to create an AWS AMI.

Each virtual machine package includes:

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

For Oracle Platforms supporting the Session Router

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

- Image file: `nnSCZ900.bz`
- Bootloader file: `nnSCZ900.boot`

Image Files for Customers Requiring Lawful Intercept

Deployments requiring Lawful Intercept (LI) functionality must use the LI-specific image files. These image files are available in a separate media pack on MOS and OSDC. LI-specific image files can be identified by the "LI" notation before the file extension.

All subsequent patches follow naming conventions with the LI modifier.

Boot Loader Requirements

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

Setup Product

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

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

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

```
ORACLE# setup product

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

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

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

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

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

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

Upgrade Information

Supported Upgrade Paths (OCSBC, OESBC and OCSR)

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

- S-Cz8.2.0 to S-Cz9.0.0
- S-Cz8.3.0 to S-Cz9.0.0
- S-Cz8.4.0 to S-Cz9.0.0
- S-Cz8.4.0p3 to S-Cz9.0.0
- S-Cz8.4.0p5C (and newer) to S-Cz9.0.0

> **Note:**
>
> Do not upgrade to S-Cz9.0.0 directly from S-Cz8.4.0p4, S-Cz8.4.0p5 or any S-Cz8.4.0p5 OOC patches up to S-Cz8.4.0p5B. If running these versions, upgrade to S-Cz8.4.0p5C before upgrading to S-Cz9.0.0.

When upgrading to this release from a release older than the previous release, read all intermediate *Release Notes* 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.
7. Do not configure an entitlement change on the Oracle Communications Session Border Controller while simultaneously performing a software upgrade. These operations must be performed separately.

Upgrade and Downgrade Caveats

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

> **Note:**
>
> Upgrading to this Release from releases earlier than S-Cz8.4.0:
> The S-Cz8.4.0 release included significant changes that hardened the security posture of the SBC. These changes required your careful evaluation regarding functionality when upgrading to S-Cz8.4.0. These changes are also applicable to customers upgrading from releases prior to S-Cz8.4.0 to this release. Take care to review this information in the S-Cz8.4.0 Release Notes: Upgrade and Downgrade Caveats

Upgrading to S-Cz9.0.0 with IKEv2 LI Tunnels

An HA upgrade to S-Cz9.0.0, when configured with LI Tunnels using IKEv2, can cause IPSec tunnels to fail if an IPsec rekey initiated from a peer has resulted in the IPSec SAs being out of sync across the HA pair. After an upgrade with these conditions, these LI tunnels do not function on the Active node.

Prior to upgrading these deployments determine whether the IKEv2/IPsec SA's are in sync on the Active and Standby node by running the ACLI command **show security ipsec sad <network-interface>:vlan detail** and check whether the SPI's are same on both the Active and standby node.

- If they are in sync, proceed with the upgrade.
- If the IPsec SA's are not in sync across the HA nodes, perform the following procedure:
  1. If enabled, disable **x2-keep-alive** from the LI shell. (See procedures in LI documentation.)
  2. Upgrade the Standby node to S-Cz9.0.0.
  3. Wait until the pair reaches HA state.
  4. Configure the Active node to boot to S-Cz9.0.0. (Do not reboot this device yet.)
  5. Delete tunnels on the Active node, which is still running the older software version, using one of the following commands from the CLI root.

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

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

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

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

  7. Reboot the Active node.
  8. If the IKE interface is in INITIATOR mode, execute the **ping** command to the applicable IPSec endpoints on the newly Active (S-Cz9.0.0) node to establish new tunnels.
     If the IKE interface is in RESPONDER mode, have peers restart tunnels instead of executing the **ping** command.

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

Two downgrade procedures are presented below.

1. Rollback after full Upgrade:
   a. HA pair is in highly available state with 840p1 version
   b. Reboot Standby node with downgraded version
   c. Wait until highly available state established
   d. Delete tunnels on the Active node using one of the following commands from the CLI root.

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

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

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

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

   f. Reboot the Active node.
   g. If the IKE interface is in INITIATOR mode, execute the ping command to the applicable IPSec endpoints on the newly Active (Downgraded) node to establish new tunnels.
      If the IKE interface is in RESPONDER mode, have peers restart tunnels instead of executing the ping command.
   h. Upon completion of boot cycle verify HA state and proper tunnel synchronization.
2. Rollback after Upgrading the active node only:
   a. HA pair is in highly available state with Active node 9.0.0 and Standby node with old version
   b. Configure boot table on Active node with rollback version
   c. Delete tunnels on the Active node using one of the following commands from the CLI root.

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

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

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

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

e. Reboot the Active node.

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

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

SSH Keys

Before upgrading from a pre-8.4 release to this release, delete any imported public keys using the `ssh-pub-key delete <key-name>` command. Because the commands for SSH key management changed between 8.3 and 8.4, you will not be able to delete old 8.3-type SSH keys using 8.4 (or later) commands. After upgrading, re-import any required public keys. For example, if your SBC pushes records to an SFTP server, import that server's public key as a known host.

If you're upgrading from 8.4 and you didn't previously import the public keys of your SFTP server, import them as a known-host key. Any public keys imported in 8.4 will be available in 9.0.

See "Manage SSH Keys" in the *Configuration Guide*.

TSCF Configurations from Prior Software Versions

A TSCF configuration that was present on your system before upgrade to this S-Cz9.0.0 release and above, which do not support TSM, may still be present in the configuration file if you do not remove it manually before upgrade. The system does not apply these TSCF configurations on a non-TSM release.

If you subsequently downgrade to a TSM supported release, however, the system applies the TSCF configuration.

Although there is no operational impact, Oracle recommends that you manually remove the TSCF configuration before you upgrade to a non-TSM supported release. If working with an HA pair, be sure your TSM configuration and feature setup is synchronized across the pair during an upgrade. Refer to the procedures in “Setting Up Product-Type, Features and Functionality” and “Setup Features on an HA Pair" in the *ACLI configuration Guide*.

Acme Packet 3950/4900 Slots

The Acme Packet 3950 and Acme Packet 4900 support:

- 4 media interfaces: s0p0, s0p1, s0p2, and s0p3
- 2 10G interfaces: s0p4 and s0p5
- The optional TDM interface: s2p0

Because there is no slot 1, do not copy over a configuration which contains a phy-interface element that uses slot 1 unless you delete and reconfigure the phy-interfaces.

Encrypting the Surrogate Agent Password

If upgrading from any version prior to S-CZ8.4.0p5, run the `spl save acli encr-surrogate-passwords` command to save the surrogate-agent passwords in an encrypted format. Later versions do not require this command.

If performing an upgrade from any version prior to S-CZ8.4.0p5 in an HA environment:

1. Run `backup-config` on both the active and standby SBC.
2. Upgrade the release on the standby SBC.
3. Perform a failover so that the standby becomes the active.
4. Encrypt surrogate-agent passwords on the new active SBC with the command:

   ```
   spl save acli encr-surrogate-passwords
   ```

5. Upgrade the release on the new standby SBC.

You do not need to run the same `spl` command on the new standby SBC because it will sync with the new active SBC.

Upgrade Version Caveat from Session Delivery Manager

The Session Delivery Manager cannot direct upgrades from SCZ910p6, SCZ900p8 or SCZ900p9 for HA deployments. See Knowledge Document # 2952935.1 for a detailed explanation.

Feature Entitlements

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

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

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

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

Feature	Type
Transcode Codec EVRCB Capacity	Integer
Transcode Codec EVS Capacity	Integer
Transcode Codec OPUS Capacity	Integer
Transcode Codec SILK Capacity	Integer

The following table lists the features you enable by installing a license key at the **system, license** configuration element. Request license keys at the License Codes website at http://www.oracle.com/us/support/licensecodes/acme-packet/index.html.

Feature	Type
Lawful Intercept	boolean
R226 SIPREC	boolean

The following tables lists the features for the Oracle Communications' Session Router (SR) you enable with the **setup entitlements** command. When setting up an SR, you choose between either the Session Stateful or the Transaction Stateful Session Routers. The Enterprise Session Router entitlements are the same.

This first SR table lists entitlements for the Session Stateful Session Router.

Feature	Type
Session Capacity	Number of sessions
Accounting	Enabled or Disabled
Load Balancing	Enabled or Disabled
Policy Server	Enabled or Disabled
Admin security	Enabled or Disabled
ANSII R226 Compliance	Enabled or Disabled
Data Integrity (FIPS 140-2)	Enabled or Disabled

Note:

Do not enable the FIPS entitlement for the Oracle Session Router, service provider product.

This second SR table lists entitlements for the Transaction Stateful Session Router.

Feature	Type
MPS Capacity	Number of sessions
Admin security	Enabled or Disabled
ANSII R226 Compliance	Enabled or Disabled
Data Integrity (FIPS 140-2)	Enabled or Disabled
Load Balancing	Enabled or Disabled

> **Note:**
>
> Do not enable the FIPS entitlement for the Oracle Session Router, service provider product.

Encryption for Virtual SBC

You must enable encryption for virtualized deployments with a license key. The following table lists which licenses are required for various encryption use cases.

Feature	License Key
IMS-AKA Endpoints	IPSec
IPSec Trunking	IPSec
SRTP Sessions	SRTP
Transport Layer Security Sessions	TLS [1]
MSRP	TLS

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

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

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

Upgrading To S-Cz9.0.0 From Previous Releases

When upgrading from a previous release to S-Cz9.0.0, your encryption entitlements carry forward and you do not need to install a new license key.

System Capacities

System capacities vary across the range of platforms that support the Oracle Communications Session Border Controller. To query the current system capacities for the platform you are using, execute the **show platform limits** command.

Transcoding Support

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

Platform	Supported Codecs (by way of codec-policy in the add-on-egress parameter)
• Acme Packet physical platforms • Hardware-based transcoding for virtual platforms (PCIe Media Accelerator)	• AMR • AMR-WB • CN • EVRC0 • EVRC • EVRC1 • EVRCB0 • EVRCB • EVRCB1 • EVS[1] • G711FB • G722 • G723 • G726 • G726-16 • G726-24 • G726-32 • G726-40 • G729 • G729A • GSM • iLBC • Opus • SILK • PCMU • PCMA • T.38 • T.38OFD • telephone-event • TTY, except on the Acme Packet 1100
• Virtual Platforms (with 1+ transcoding core) - only supported on Intel CPUs	• AMR • AMR-WB • EVS • G722 • G723 • G729 • G729A • iLBC • Opus • SILK • PCMU • PCMA • telephone-event Note that the pooled transcoding feature on the VNF uses external transcoding SBC, as defined in "Co-Product Support," for supported SBC for the Transcoding-SBC (T-SBC) role.

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

Coproduct Support

The following products and features run in concert with the Oracle Communications Session Border Controller (SBC) for their respective solutions. Oracle Communications Session Router support is also provided below. Contact your Sales representative for further support and requirement details.

Oracle Communications Operations Manager

This S-Cz9.0.0 SBC release can interoperate with the following versions of the Oracle Communications Session Monitor:

- 4.2.0
- 4.3.0
- 4.4.0

Oracle Communications Session Delivery Manager

This S-Cz9.0.0 SBC release can interoperate with the following versions of the Oracle Communications Session Delivery Manager:

- 8.2.3

> **Note:**
>
> Customers who wish to run release S-Cz9.0.0 and higher need to load an updated XSD into OCSDM. This file can be found by searching My Oracle Support for Patch ID 32887468, which is the NNC-OCSDM XSD file for SCz9.0.0 with SDM 8.2.2/8.2.3.

Oracle Communications Subscriber Aware Load Balancer

This S-Cz9.0.0 SBC release can interoperate as a cluster member with the following versions of the Subscriber Aware Load Balancer:

- Acme Packet 6100: S-Cz8.3.0
- v-SLB: S-Cz8.4.0, S-Cz9.0.0

Pooled Transcoding

This S-Cz9.0.0 SBC release acting as an A-SBC can interoperate with T-SBCs on the following hardware/software combinations :

- Acme Packet 4500: S-Cz7.4.0
- Acme Packet 4600: S-Cz8.3.0, S-Cz8.4.0
- Acme Packet 6300: S-Cz8.3.0, S-Cz8.4.0
- Acme Packet 6350: S-Cz8.3.0, S-Cz8.4.0
- Virtual Platforms with Artesyn SharpMedia™: S-Cz8.2.0, S-Cz8.3.0, S- Cz8.4.0, S-Cz9.0.0

This S-Cz9.0.0 SBC release acting as a T-SBC can interoperate with A-SBCs on the following hardware/software combinations:

- All platforms supported by the following releases: S-Cz8.2.0, S-Cz8.3.0, S-Cz8.4.0
- Acme Packet 4500 running S-Cz7.4.0

Oracle Communications Session Router and SDM

This S-Cz9.0.0 release of the OCSR can interoperate with the following versions of the Oracle Communications Session Delivery Manager:

- 8.2.3

Oracle Communications Session Router and Operations Manager

This S-Cz9.0.0 release of the OCSR can interoperate with the following versions of the Oracle Communications Operations Manager:

- 4.2.0
- 4.3.0
- 4.4.0

TLS Cipher Updates

Note the following changes to the DEFAULT cipher list.

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

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

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

- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

Oracle supports the following ciphers for debugging purposes only:

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

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

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

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

WARNING:

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

Note:

The default is TLSv1.2. Oracle supports TLS1.0 and TLS1.1 for backward compatibility, only, and they may be deprecated in the future. TLS 1.0 is planned to be deprecated in the next release.

Documentation Changes

The following information lists and describes the changes made to the Oracle Communications Session Border Controller (SBC) documentation set for S-Cz9.0.0.

TSM Documentation

All TSM documentation is removed due to the feature being deprecated.

Platform Preparation and Installation Guide

The vSBC configuration and operation descriptions are moved from the *Platform Preparation and Installation Guide* to the *System Configuration* chapter of the *ACLI Configuration Guide*. This consolidates vSBC information.

An appendix has been added with reference information for users who want to deploy Heat templates on versions of OpenStack newer than Pike.

A new section has been added with reference to deploying on Azure with accelerated networking in Public Cloud Platforms chapter.

Accounting Guide

The *Accounting Guide* is re-organized to present the same content it presented before more clearly and effectively.

Security Guide

The DDoS recommendations have been removed from the Security Guide. Refer to the following documents for DDoS recommendations:

- DDoS Prevention Configuration for SIP Peering Environments
- DDoS Prevention Configuration for SIP Access Environments

Known Issues and Caveats

Oracle has moved the Known Issues and Caveats section from the Release Notes to its own publication titled *Oracle Communications Session Border Controller Known Issues S-Cz9.0.0.*

Behavioral Changes

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

SSH Keys

A new **ssh-key** command was introduced in 8.4. We recommended customers use this command to import public keys. In 9.0, however, customers must use the **ssh-key** command to manage SSH keys. For example, if you have an SFTP server that you push logs to, you must import your logging server's public key as a known host on the SBC.

TOS Configuration

By default, the SBC no longer passes DSCP codes in ingress packets to egress packets. You must configure a **media-policy** with desired TOS changes and affix those policies to the realms on which you want to define egress types of service. Without a **media-policy**, the SBC includes the default DSCP code, CS0 (Hex 0x00), as the DSCP code to all egress media packets.

Patches Included in This Release

The following information assures you that when upgrading, the S-Cz9.0.0 release includes defect fixes from neighboring patch releases.

Neighboring Patches Included

- S-Cz740m2p9
- S-Cz800p10
- S-Cz810m1p25B
- S-Cz810m1p26
- S-Cz810m1p18D
- S-Cz820p8
- S-Cz830m1p11

- S-Cz840p3
- S-Cz840p4
- S-Cz840p5

Supported SPL Engines

The S-Cz9.0.0 release supports the following SPL engine versions: C2.0.0, C2.0.1, C2.0.2, C2.0.9, C2.1.0, C2.1.1, C2.2.0, C2.2.1, C2.3.2, C3.0.0, C3.0.1, C3.0.2, C3.0.3, C3.0.4, C3.0.6, C3.0.7, C3.1.0, C3.1.1, C3.1.2, C3.1.3, C3.1.4, C3.1.5, C3.1.6, C3.1.7, C3.1.8, C3.1.9, C3.1.10, C3.1.11, C3.1.12, C3.1.13, C3.1.14, C3.1.15, C3.1.16, C3.1.17, C3.1.18, C3.1.19, C3.1.20, C3.1.21.

2
New and Deprecated Features

The S-Cz9.0.0 release of the Oracle Communications Session Border Controller (SBC) supports the following new features and enhancements. Deprecated features are listed at the end of this section.

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

DoS Counters

The SBC provides ACL and DDOS statistics that track events for ARP, trusted, and untrusted traffic. These statistics include notifications about ARP watermarks and trusted and untrusted queue metrics to provide visibility into traffic management rates, based on traffic patterns in normal and peak times. You configure these thresholds as a percentage of the configured traffic rates within the media-manager configuration element. This provides you with early notification of traffic congestion so you can better tune the global media settings for DDOS. The SBC does not drop the packets affected through threshold events. Instead, it forwards them to a traffic manager for making permit/drop decisions prior to sending it to the host. In addition to host bound events, the SBC generates SMNP traps and alarms for TCAs that monitor ARP, trusted, untrusted and max-signaling rates. You can collect statistics on related traffic using the ACLI, SNMP walks, HDR and REST.

See the *Security* chapter in the *ACLI Configuration Guide*.

Hyperthreading Support

You can configure the SBC to utilize hyperthreading (SMT) support for datapath cores, including forwarding, DoS and transcoding cores. This configuration allows datapath CPUs to utilize two virtual CPUs (vCPUs) as "siblings" on the same physical CPU when the platform host supports hyperthreading. Refer to your software version's Release Notes to determine platforms that support this feature.

See the *System Configuration* chapter in the *ACLI Configuration Guide*.

Surrogate Registration for Diverse Realms

The SBC uses an authentication attribute element in realms to support surrogate agent authentication requests initiated from other realms. This is a multi-instance element that supports the authentication of non-REGISTER traffic to surrogate agents with different authentication detail. The key for these lookups is the combination of the authentication realm and the authentication user lookup configurations. If you do not configure authentication attribute element in the realm, the SBC handles surrogate agent authentication using the authentication table setup on the (softswitch) session agent, which supports this traffic in a single realm only.

See the *SIP Signaling Services* chapter in the *ACLI Configuration Guide*.

Multi-Tiered Local Route Tables

When routing though an LRT, the SBC normally attempts to reach next-hops using LRT entries in the order that they appear in the XML file. If a next-hop is unsuccessful, the SBC tries the next-hop on the list. You can, however, configure entries in LRTs that cause the SBC to gradually increase traffic for specific routes and control the distribution, while also monitoring usage. You can specify priorities and weights to favor route entries and use a preferred route instead of following the list order.

See the *Session Routing and Load Balancing* chapter in the *ACLI Configuration Guide*.

Support for RFC 5939

You can configure the SBC to support RFC 5939-based SDP capability negotiation. This support overrides the supported RFC 3264-based mechanism for generating mixed RTP/SRTP offers to better support secure and non-secure flows in the same realm. Within the RFC 3264 model, both the offer and answer contain actual configurations, but separate capabilities and potential configurations are not supported. The RFC 5939 implementation on the SBC is backward compatible and uses the RFC 3264-based model by default.

See the *SIP Signaling Services* chapter in the *ACLI Configuration Guide*.

Session Translation Enhancement

This version of the SBC adds an option to allow CDR generation to reflect values that have been modified by translations rules, and the ability to enable history-info header manipulation to its support for using session translation rules to manage SIP-SIPI interworking.

See the *SIP Signaling Services* chapter in the *ACLI Configuration Guide*.

Transcoding Free Operation and Ring Back Tone

You can configure the SBC to avoid using transcoding resources within certain local media playback scenarios. After establishing a RBT call that includes transcoding, the SBC can trigger this Transcoding Free Operation (TrFO) feature if the P-Acme-TrFO header is present. Having determined that the call can proceed without transcoding, the SBC originates a reINVITE towards the calling party containing the called side codec. Once the reINVITE is completed, the call can continue without transcoding. In addition, the negotiated codec on the called party side must have been included in the calling party's original offer (after ingress codec-policy execution).

See the *Transcoding* chapter in the *ACLI Configuration Guide*.

Support for AWS C5 Machines

You can deploy the SBC on AWS using their C5 family of virtual system shapes.

Unlike C4 and M4 instances, which use Xen as the underlying hypervisor, C5 instances use the KVM hypervisor. Use the following image:

- nnSCZ900-img-vm_kvm.tgz—Compressed image file including SBC VNF for KVM virtual machines from which you create AWS AMIs

See the *Introduction* chapter in the *Release Notes*.

Increased LRT Entry Capacity on the Acme Packet 6350

The Acme Packet 6350 now supports 20 million LRT entries.

See the *Session Routing and Load Balancing* chapter in the *ACLI Configuration Guide* for further information about LRTs.

TACACS+ IKEv2/IPsec over wancom0

You can configure the SBC to connect to a TACACS+ server over an IKEv2/IPsec secured connection. This communication must occur over the management interface wancom0. The **ikev2-ipsec-wancom0-params** element enables this configuration.

See the TACACS+ section in the Getting Started chapter of the *Configuration Guide*.

AWS Image Optimization

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

SPL Plugins

The service provider OCSBC supports the following SPL Plugins:

- Universal Call Identifier, which generates, preserves or removes UCID headers.
- SIPREC Metadata, which provides additional header information in the originating SIP messages metadata sent to the Interactive Session Recorder (ISR).
- HeaderNAT, which can be used for deploying SBCs behind a NAT device

Regex Support for Conditional Logging

Conditional logging has been enhanced to support regex matching. See the Advanced Logging section in the *Maintenance and Troubleshooting Guide*.

SIPREC Enhancements

New ACLI commands have been added to display statistics for session recording servers (SRSs) and session recording groups (SRGs). The new CLI commands:

- Support new show commands to display statistics related to SRS' and SRGs.
- Display message-level statistics to give more clarity about recording sessions.

For more information on the new commands, see ACLI Command Changes .

OCI Resource Manager

OCI Resource Manager automates the process of provisioning your Oracle Cloud Infrastructure resources. The Resource Manager provides stacks to set up OCI resources that runs the virtual SBC using Terraform scripts. However, Terraform scripts cannot be used for complete SBC configuration. Hence, Resource Manager uses two pre-build stacks for deploying environments. The two stacks are - VCN and SBC stack. The VCN stack creates the required network infrastructure to deploy the virtual SBC instance on OCI. The SBC stack instantiates a standalone or HA pair on OCI with all Day-0 configuration. You can run these templates or scripts from CLI, similar to running the Terraform templates from OCI Resource Manager.

See Create and Deploy on OCI using Resource Manager section in Public Cloud Platforms chapter in *Platform Preparation and Installation Guide* .

> **Note:**
>
> Creating and Deploying on OCI using Resource Manager begins with S-Cz9.0.0p2.

Mid-Call Location Change Support for MS-Teams

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

> **Note:**
>
> The availability of this Mid-Call Location Change Support for MS-Teams feature begins with the S-Cz900p2 release.

FAX Detection and Re-Direct

You can configure the SBC to detect fax signaling within a SIP call and redirect those calls directly to a group of one or more fax servers. By default, the SBC sends a reINVITE either to a caller or calling party, based on your setting for the **reverse-fax-tone-detection-reinvite** parameter, when it detects a fax tone from the media stream. There are some call flows, however, that need redirection to the FAX endpoint without using this reINVITE. You can configure this support by setting the **fax-servers** parameter with the name of an applicable **session-agent-group** on the applicable **session-agent**. When enabled, the Fax Redirect feature takes precedence over the above mentioned legacy fax functionality.

> **Note:**
>
> Support for this FAX Detection and Re-Direct feature begins with the S-Cz900p3 release.

Supporting Different Codec and Telephone-Event Rates in the SDP

RFC 4733 recommends that telephone events within an audio stream that use the same synchronization source (SSRC) should use the same timestamp clock rate as the audio channel. As an example, if SILK/16000 is being used as the audio stream then the flow should use telephone-event TE/16000. By default, the SBC complies with this behavior. You can configure the SBC, however, to support flows when using different clock rates for audio and telephone events. This allows the SBC to adapt to environments that do not follow the recommendation.

> **Note:**
>
> Support for Different Codec and Telephone-Event Rates in the SDP begins with the S-Cz900p3 release.

Deprecation of TSM (TSCF) Feature

The TSM feature is removed from this S-Cz9.0.0 release of the SBC.

OCSP Verification of Client X.509 Certificates

When a browser sends an X.509 certificate during authentication, the SBC can verify the X.509 certificate using OCSP. In addition, the **ssh-keys** command has been expanded to import or delete X.509 certificates and their certificate chains. These certificates can be verified using OCSP during the authentication of SSH clients. Customers can configure both the FQDN of the OCSP server as well as the IP address and port of the DNS server which resolves that FQDN.

New Memory Support for TCM-3

This version of the SBC supports TCM-3 cards with new memory. This software is also backwards compatible with cards that include the old memory. Note that older software does not support this new memory.

See the Acme Packet 3950/4900 Minimum Versions section in the Transcoding chapter of the *ACLI Configuration Guide* for detailed information about verifying software/hardware compatibility. See the Platform support information in these *Release Notes* for specific software/hardware compatibility for this version of the SBC software.

> **Note:**
>
> This new feature support begins with S-Cz9.2.0p10.

3
Interface Changes

The following topics summarize ACLI, SNMP, HDR, Alarms, Accounting, and Web GUI changes for S-Cz9.0.0. The additions, removals, and changes noted in these topics occured since the previous major release of the Oracle Communications Session Border Controller.

ACLI Configuration Element Changes

The following tables summarize the ACLI configuration element changes that first appear in the Oracle Communications Session Border Controller (SBC) S-Cz9.0.0 release.

DoS Counters

Modified Elements	Description
media-manager, **media-manager**, **untrusted-minor-threshold**	Specifies the traffic level at which the system triggers minor notifications about DoS traffic in the untrusted queue.
media-manager, **media-manager**, **untrusted-major-threshold**	Specifies the traffic level at which the system triggers major notifications about DoS traffic in the untrusted queue.
media-manager, **media-manager**, **untrusted-critical-threshold**	Specifies the traffic level at which the system triggers critical notifications about DoS traffic in the untrusted queue.
media-manager, **media-manager**, **trusted-minor-threshold**	Specifies the traffic level at which the system triggers minor notifications about DoS traffic in the trusted queue.
media-manager, **media-manager**, **trusted-major-threshold**	Specifies the traffic level at which the system triggers major notifications about DoS traffic in the trusted queue.
media-manager, **media-manager**, **trusted-critical-threshold**	Specifies the traffic level at which the system triggers critical notifications about DoS traffic in the trusted queue.
media-manager, **media-manager**, **arp-minor-threshold**	Specifies the traffic level at which the system triggers minor notifications about DoS traffic in the arp queue.
media-manager, **media-manager**, **arp-major-threshold**	Specifies the traffic level at which the system triggers major notifications about DoS traffic in the arp queue.
media-manager, **media-manager**, **arp-critical-threshold**	Specifies the traffic level at which the system triggers critical notifications about DoS traffic in the arp queue.

Hyperthreading Support

Modified Elements	Description
system-config, **use-sibling-core-datapath**	Allows the system to support hyperthreading of cores performing datapath functions.

Surrogate Registration for Diverse Realms

Modified Elements	Description
media-manager, **realm-config**, **auth-attributes**	Allows the application of authentication configuration on a realm to support cross-realm surrogate authentication.
media-manager, **realm-config**, **auth-attributes**, **username**	Performs the same authentication function as a session agent's auth-attribute from within a realm.
media-manager, **realm-config**, **auth-attributes**, **auth-user-lookup**	Performs the same authentication function as a session agent's auth-attribute from within a realm.
media-manager, **realm-config**, **auth-attributes**, **password**	Performs the same authentication function as a session agent's auth-attribute from within a realm.
media-manager, **realm-config**, **auth-attributes**, **in-dialog-methods**	Performs the same authentication function as a session agent's auth-attribute from within a realm.

Support for RFC 5939

Modified Elements	Description
sdes-profile, **egress-offer-format**, **rfc5939-compliant**	Allows you to specify RFC 5939 operation for this sdes-profile.

Session Translation for SIP-SIPI Interworking

Modified Elements	Description
session-router, **session-translation**, **rules-redirect**	Allows you to define session translation rules for managing redirect information during SIP-SIPI interworking.
session-router, **session-translation**, **rules-history-info**	Allows you to define session translation rules for managing history-info information during SIP-SIPI interworking.

IKEv2 Support for Wancom0

New Elements	Description
security, **ikev2-ipsec-wancom0-params**	Allows you to define the IP addresses, ports, protocol, and other attrbutes of the IKEv2/IPsec connection.

Regex Support for Advanced Logging

New Elements	Description
session-router, **sip-advanced-logging**, **conditions**, **match-procedure**	Allows you to select whether to perform an exact match or a regex match.

OCSP Verification of Client X.509 Certificates

New Elements	Description
security, **authentication**, **online-certificate-status-protocol**	Allows you to select which interfaces require OCSP verification, the OCSP FQDN, and the IP address and port of the DNS resolver for the OCSP FQDN.

ACLI Command Changes

The following table summarizes the ACLI command changes that first appear in the Oracle Communications Session Border Controller S-Cz9.0.0 release.

This table lists and describes changes to ACLI commands that are available in the S-Cz9.0.0 release.

New Commands	Description
show sipd rbt-trfo	
show lrt route-table <lrt-config-name>	Output enhanced to include information on priority and weight.
show lrt route-entry <lrt-config-name> <user>	Output enhanced to include information on priority and weight.
show dos threshold counters	Displays current statistics on traffic and triggers collected to monitor DoS traffic status.
show security ipsec wancom0 <sad | spd | tunnels>	Displays the IPsec databases and counters for the wancom0 interface
show security ike wancom0 <error-stats | sad>	Displays the IKEv2 error stats or SAD information for the wancom0 interface.
show sipd srs	Lists the current status for all the SRS' configured in the system. The status being: • I (in service) • O (out of service) • S (Transitioning from out of service to in service status.)
show sipd srg	Displays the current status for all the SRGs configured in the system.
show sipd siprec <message>	Lists information about a specific type of SIP message related to all SIPREC sessions towards SRS.
show sipd siprec errors	Shows errors related to SIP media event.
show rec srs <srs_name>	Shows the statistics for a specific SRS.
show rec srg <srg_name>	Shows the statistics for a specific SRG.
reset tacacs-stats	Reset the TACACS+ statistics
ssh-key x509 import <certificate-name> <ocsp-server> <class>	Import a client X.509 certificate that a client can use for authentication, specifying the OCSP server to use for verification.
ssh-key x509 delete <login-name>	Delete an imported X.509 certificate.

Accounting Changes

This section summarizes the accounting changes that appear in the Oracle Communications Session Border Controller version S-Cz9.0.0.

There are no accounting data additions documented for this release.

SNMP/MIB Changes

This section summarizes the SNMP/MIB changes that appear in the SBC version S-Cz9.0.0.

MIB Changes for STIR/SHAKEN Statistics

When the STIR/SHAKEN feature is enabled, the SBC uses the apStirServerStats table, within the `ap.apps.mib`, to monitor feature statistics.

This table contains the new apStirServerStats objects by which the user can monitor STIR/SHAKEN statistics using SNMP.

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.1.4.2.1. 4.x +	Description
apStirServerName	.1.	Server name as configured on the SBC
apStirServerStats.recent.asQueries	.1.1	Recent queries made to the named AS server
apStirServerStats.recent.asSuccessResponses	.1.2	Recent successful responses received from the named AS server
apStirServerStats.recent.asFailResponses	.1.3	Recent failed responses received from the named AS server
apStirServerStats.recent.asFailServiceException	.1.4	Recent failed responses received from the named AS server caused by a service exception
apStirServerStats.recent.asFailPolicyException	.1.5	Recent failed responses received from the named AS server caused by a policy exception
apStirServerStats.recent.vsQueries	.1.6	Recent queries made to the named VS server
apStirServerStats.recent.vsSuccessResponses	.1.7	Recent successful responses received from the named VS server
apStirServerStats.recent.vsFailResponses	.1.8	Recent failed responses received from the named VS server
apStirServerStats.recent.vsFailVerification	.1.9	Recent failed responses received from the named VS server indicating verification failure

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.1.4.2.1.4.x +	Description
apStirServerStats.recent.vsFailServiceException	.1.10	Recent failed responses received from the named VS server caused by a service exception
apStirServerStats.recent.vsFailPolicyException	.1.11	Recent failed responses received from the named VS server caused by a policy exception
apStirServerStats.recent.ServerUnreachable	.1.12	N/A
apStirServerStats.total.asQueries	.2.1	Recent queries made to the named AS server
apStirServerStats.total.asSuccessResponses	.2.2	Total successful responses received from the named AS server
apStirServerStats.total.asFailResponses	.2.3	Total failed responses received from the named AS server
apStirServerStats.total.asFailServiceException	.2.4	Total failed responses received from the named AS server caused by a service exception
apStirServerStats.total.asFailPolicyException	.2.5	Total failed responses received from the named AS server caused by a policy exception
apStirServerStats.total.vsQueries	.2.6	Total queries made to the named VS server
apStirServerStats.total.vsSuccessResponses	.2.7	Total successful responses received from the named VS server
apStirServerStats.total.vsFailResponses	.2.8	Total failed responses received from the named VS server
apStirServerStats.total.vsFailVerification	.2.9	Total failed responses received from the named VS server indicating verification failure
apStirServerStats.total.vsFailServiceException	.2.10	Total failed responses received from the named VS server caused by a service exception
apStirServerStats.total.vsFailPolicyException	.2.11	Total failed responses received from the named VS server caused by a policy exception
apStirServerStats.total.ServerUnreachable	.2.12	N/A
apStirServerStats.permax.asQueries	.3.1	Permax queries made to the named AS server
apStirServerStats.permax.asSuccessResponses	.3.2	Permax successful responses received from the named AS server
apStirServerStats.permax.asFailResponses	.3.3	Permax failed responses received from the named AS server

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.1.4.2.1.4.x +	Description
apStirServerStats.permax.asFailServiceException	.3.4	Permax failed responses received from the named AS server caused by a service exception
apStirServerStats.permax.asFailPolicyException	.3.5	Permax failed responses received from the named AS server caused by a policy exception
apStirServerStats.permax.vsQueries	.3.6	Permax queries made to the named VS server
apStirServerStats.permax.vsSuccessResponses	.3.7	Permax successful responses received from the named VS server
apStirServerStats.permax.vsFailResponses	.3.8	Permax failed responses received from the named VS server
apStirServerStats.permax.vsFailVerification	.3.9	Permax failed responses received from the named VS server indicating verification failure
apStirServerStats.permax.vsFailServiceException	.3.10	Permax failed responses received from the named VS server caused by a service exception
apStirServerStats.permax.vsFailPolicyException	.3.11	Recent failed responses received from the named VS server caused by a policy exception
apStirServerStats.permax.ServerUnreachable	.3.12	N/A

The SBC sends two SNMP traps that alert you when traffic crosses each threshold, and clear when the traffic falls back below the threshold:

- apDosThresholdCrossTrap
- apDosThresholdClearTrap

See the *Security* chapter in the *ACLI Configuration Guide* for further information on how to read these traps.

DoS Counter Statistics

The SBC uses the apStirServerStats table, within the `ap.apps.mib`, to monitor feature statistics.

This table contains the new apDosThresholdCountersGroup objects by which the user can monitor DoS statistics on a per-queue basis using SNMP.

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.5 +	Description
apDosTrustedMinorCounter	.1	Counter incremented, when trusted bandwidth crossed the minor threshold percentage
apDosTrustedMajorCounter	.2	Counter incremented, when trusted bandwidth crossed the major threshold percentage
apDosTrustedCriticalCounter	.3	Counter incremented, when trusted bandwidth crossed the critical threshold percentage
apDosUntrustedMinorCounter	.4	Counter incremented, when untrusted bandwidth crossed the minor threshold percentage
apDosUntrustedMajorCounter	.5	Counter incremented, when untrusted bandwidth crossed the major threshold percentage
apDosUntrustedCriticalCounter	.6	Counter incremented, when untrusted bandwidth crossed the critical threshold percentage
apDosArpMinorCounter	.7	Counter incremented, when ARP bandwidth crossed the minor threshold percentage
apDosArpMajorCounter	.8	Counter incremented, when ARP bandwidth crossed the major threshold percentage
apDosArpCriticalCounter	.9	Counter incremented, when ARP bandwidth crossed the critical threshold percentage

OCSP Verification of Client X.509 Certificates

The following MIB is generated whenever any second-factor authentication fails, including when OCSP verification rejects an X.509 certificate because it is revoked.

MIB Object	Object ID	Description
apSysMgmtAuthenticationFailedTrap	1.3.6.1.4.1.9148.3.2.6.0.16	Generated if an authentication attept fails.

Alarms

This topic summarizes Alarm additions that appear in this release.

DoS Traffic Alarms

Three alarms are implemented to notify the user that DoS traffic has exceeded your thresholds on the applicable queue. These alarms correspond to the SNMP traps:

- DOS THRESHOLD TRUSTED CROSS MEDIA ALARM
- DOS THRESHOLD UNTRUSTED CROSS MEDIA ALARM
- DOS THRESHOLD ARP CROSS MEDIA ALARM

Unlike SNMP, these present type and 'threshold crossed' in a single alarm object.

HDR

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

STIR/SHAKEN HDR Group

This release includes the **stir-stats** HDR group. The table below lists and describes stir servers statistics and includes HDR position, statistic, type, timer value, range, and description.

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

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

DoS Traffic Group

This release includes the **dos-threshold-counters** HDR group. The table below lists and describes counter statistics and includes HDR position, statistic, type, timer value, range, and description.

CSV Position	HDR Column Name	Data Type	Range	Description
1	Trusted Minor Counter	Counter	(0-2^64-1)	Counter incremented, when trusted bandwidth crossed the minor threshold percentage
2	Trusted Major Counter	Counter	(0-2^64-1)	Counter incremented, when trusted bandwidth crossed the major threshold percentage

CSV Position	HDR Column Name	Data Type	Range	Description
3	Trusted Critical Counter	Counter	(0-2^64-1)	Counter incremented, when trusted bandwidth crossed the critical threshold percentage
4	Untrusted Minor Counter	Counter	(0-2^64-1)	Counter incremented, when untrusted bandwidth crossed the minor threshold percentage
5	Untrusted Major Counter	Counter	(0-2^64-1)	Counter incremented, when untrusted bandwidth crossed the major threshold percentage
6	Untrusted Critical Counter	Counter	(0-2^64-1)	Counter incremented, when untrusted bandwidth crossed the critical threshold percentage
7	ARP Minor Counter	Counter	(0-2^64-1)	Counter incremented, when ARP bandwidth crossed the minor threshold percentage
8	ARP Major Counter	Counter	(0-2^64-1)	Counter incremented, when ARP bandwidth crossed the major threshold percentage
9	ARP Critical Counter	Counter	(0-2^64-1)	Counter incremented, when ARP bandwidth crossed the critical threshold percentage

Errors and Warnings

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

verify-config Errors and Warnings

Error or Warning	Description
WARNING: [x] and [y] should not be run simultaneously as they may interfere with each other and lead to undefined behavior.	Two or more of these conflicting items have been activated: comm-monitor, packet-trace, call-trace and SIP Monitoring & Trace. At least one needs to be disabled.

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

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

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

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


ORACLE# capture start global *

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

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