Oracle® Communications Session Border Controller and Session Router

Release Notes

Release S-Cz9.2.0

F74369-07

April 2024

Oracle Communications Session Border Controller and Session Router Release Notes, Release S-Cz9.2.0

F74369-07

Contents

2 New Features

3 Interface Changes

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

The following table provides the revision history for this document.

Date	Revision
Mar 2023	• Initial release.
May 2023	• Clarifies the new Stir Shaken FQDN TTL Expiry feature. • Corrects Header Customization feature title. • Adds support for iavf driver for intel x7xx series cards. • Adds content for S-Cz9.2.0p1. • Adds TDM support for Digium cards. • Adds Session Router entitlement tables
August 2023	• Adds new caveat and behavioral change for upgrade to host key algorithms. • Adds S-Cz9.2.0p2 features.
October 2023	• Adds S-Cz9.2.0p3 feature.
December 2023	• Adds Intel limitation for software transcoding. • Adds verstat-delimiter as feature, valid from S-Cz9.2.0p1. • Adds S-Cz9.2.0p4 feature. • Clarifies XSD copy in Co-Product Support. • Adds Upgrade Caveat on certificate regeneration for wancom interfaces.
February 2024	• Adds new features at S-Cz9.2.0p5. • Adds interface change introduced in S-Cz9.2.0p3. • Updates ACLI Configuration Element Changes to include "Updates to the STI Server Group".
April 2024	• Insert limitation for AP4900 and EVS. • Adds behavioral change about SSH keys in HA. • Adds new features at S-Cz9.2.0p6. • Clarifies session translation Upgrade/ Downgrade caveat.

1

Introduction to S-Cz9.2.0

The Oracle Communications Session Border Controller *Release Notes* provides the following information about the S-Cz9.2.0 release:

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

Summaries of known issues, caveats, and limitations are found in the companion *Known Issues & Caveats* document.

Supported Platforms

The Oracle Communications Session Border Controller (SBC) can run on a variety of physical and virtual platforms. You can also run the SBC in public cloud environments. The following topics list the supported platforms and high level requirements.

Supported Physical Platforms

You can run the Oracle Communications Session Border Controller (SBC) on the following hardware platforms.

The S-Cz9.2.0 version of the SBC 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

The S-Cz9.2.0 version of the SR supports the following platforms:

- Acme Packet 4600
- Acme Packet 6100
- Acme Packet 6300
- Oracle Server X7-2
- Oracle Server X8-2
- Oracle Server X9-2

> **Note:**
>
> This is the last release that supports the following platforms:
>
> - Acme Packet 6100
> - Acme Packet 6300
> - Dual 10GbE NIU on Acme Packet 6350

Supported Private Virtual Infrastructures and Public Clouds

You can run the SBC 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 the SBC on the following hypervisors:

- KVM: Linux kernel version (4.1.12-124 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)
- Microsoft Hyper-V: Microsoft Server (2012 R2 or later)

Compatibility with OpenStack Private Virtual Infrastructures

Oracle distributes Heat templates for the Newton and Pike versions of OpenStack. Download the source, nnSCZ920_HOT.tar.gz, and follow the OpenStack Heat Template instructions.

The nnSCZ920_HOT.tar.gz file contains two files:

- nnSCZ920_HOT_pike.tar
- nnSCZ920_HOT_newton.tar

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

You can run the SBC 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	Memory
VM.Standard2.4	4/8	4	2	2	Y	60
VM.Standard2.8	8/16	8	2	2	Y	120
VM.Standard2.16	16/32	16	2	2	Y	240
VM.Optimized3.Flex-Small	4/8	4	8	6[1]	Y	16
VM.Optimized3.Flex-Medium	8/16	8	15	14[2]	Y	32
VM.Optimized3.Flex-Large	16/32	16	15	15	Y	64

[1] This maximum is 5 when using DoS Protection
[2] This maximum is 13 when using DoS Protection

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

> **Note:**
>
> Although the VM.Optimized3.Flex OCI shape is flexible, allowing you to choose from 1-18 OCPUs and 1-256GB of memory, the vSBC requires a minimum of 4 OCPUs and 16GB of memory per instance on these Flex shapes.

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

Instance Type	vNICs	RAM	vCPUs	Max Forwarding Cores	DOS Protection
c5.xlarge	4	8	4	1	N
c5.2xlarge	4	16[1]	8	2	Y
c5.4xlarge	8	32	16	6	Y
c5n.xlarge	4	8	4	1	N
c5n.2xlarge	4	16*	8	2	Y
c5n.4xlarge	8	32	16	6	Y

[1] "It is observed that the 16GB AWS instances, effectively provide around 15GB system memory for the SBC. For MSRP, 16GB system memory is minimum requirement. Due to this AWS behavior AWS, customer was not able to use MSRP with AWS - 16GB instance.

To address this behavior, the minimum system memory requirement is reduced to 14GB for vSBC instances over AWS with reduced MSRP capacity."

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)	vNICs	RAM	vCPUs	DOS Protection
Standard_F4s	4	8	4	N
Standard_F8s	8	16	8	Y
Standard_F16s	8	32	16	Y

Size	vNICs	RAM	vCPUs	DOS Protection
Standard_F8s_v2	4	16	8	Y
Standard_F16s_v2	4	32	16	Y

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

For higher performance and capacity on media interfaces, use the Azure CLI to create a network interface with accelerated networking. 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:**
>
> Azure v2 instances have hyperthreading enabled.

- Google Cloud Platform
The following table lists the GCP instance sizes that you can use for the SBC.

Table 1-1 GCP Machine Types

Machine Type	vCPUs	Memory (GB)	vNICs	Egress Bandwidth (Gbps)	Max Tx/Rx queues per VM
n2-standard-4	4	16	4	10	4
n2-standard-8	8	32	8	16	8
n2-standard-16	16	64	8	32	16

Use the n2-standard-4 machine type if you're deploying an SBC that requires one management interface and only two or three media interfaces. Otherwise, use the n2-standard-8 or n2-standard-16 machine types for an SBC that requires one management interface and four media interfaces. Also use the n2-standard-4, n2-standard-8, or n2-standard-16 machine types if deploying the SBC in HA mode.

Before deploying your SBC, check the Available regions and zones to confirm that your region and zone support N2 shapes.

On GCP the SBC must use the **virtio** network interface card. The SBC will not work with the GVNIC

Platform Hyperthreading Support

Some supported platforms support and enable and expose SMT capability by default. Others may not support SMT, require that you enable it, or have support that is specific to machine size/shape:

- Of the supported hypervisors, only VMware does not expose SMT capability to the SBC.
- Of the supported clouds:
  - AWS—Supports SMT and enables it by default.
  - OCI—Supports SMT and enables it by default.
  - GCP—Supports SMT and enables it by default.
  - Azure—Supports SMT, but requires that you enable it. The exception is the FxS_v2, which enables SMT by default.

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:

- 21.11

The DPDK version used in this release is uplifted at S-Cz9.2.0p2 to:

- 22.11

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 vCPU 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 / XXV710	i40e, i40en[1], iavf[2]	M	M
Mellanox Connect X-4	mlx5	M	M
Mellanox Connect X-5[3]	mlx5 [4]	M	NA

1 This driver is supported on VMware only.

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

3 KVM only

4 Device Part number: 7603662 Oracle Dual Port 25 Gb Ethernet Adapter, Mellanox (for factory installation)

Validated with 10G Speed using SFP- Fibre cables with 7604269 Oracle 10/25 GbE Dual Rate SFP28 Short Range (SR) Transceiver is used during validation.

> **Note:**
>
> Although the OCI VM.Optimized3.Flex shapes provide three launch options to select networking modes, always select Option 3, Hardware-assisted (SR-IOV), for the SBC.

For PV mode (default, all supported hypervisors), the following virtual network interface types are supported. You can use any make or 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
VMware (PV)	VMXNET3	W/M

Virtual Network Interface	Driver	W/M
KVM (PV)	virtio	W/M
KVM (PV)	mlx5	W

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

Virtual SBCs for this release 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.

Session Router Recommendations

Oracle recommends the following resources when operating the SR or ESR, release S-Cz9.2.0 over Oracle servers.

Recommendations for Oracle Server X7-2

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

Recommendations for Oracle Server X8-2

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

Recommendations for Oracle Server X9-2

Processor	Memory
2x 32-core Intel Platinum 8358	64GB DDR4 SDRAM

Image Files and Boot Files

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

Acme Packet Platforms

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

- Image file: `nnSCZ920.bz`
- Bootloader file: `nnSCZ920.boot`

Virtual Platforms

This S-Cz9.2.0 release includes distributions suited for deployment over hypervisors. Download packages contain virtual machine templates for a range of virtual architectures. Use the following distributions to the Session Border Controller as a virtual machine:

- `nnSCZ920-img-vm_kvm.tgz`—Compressed image file including SBC VNF for KVM virtual machines, Oracle Cloud Infrastructure (OCI), AWS EC2, and GCP instances.
- `nnSCZ920-img-vm_vmware.ova`—Open Virtualization Archive (.ova) distribution of the SBC VNF for ESXi virtual machines.
- `nnSCZ920-img-vm_vhd.tgz`—Compressed image file including SBC for Hyper-V virtual machine on Windows and Azure.
- `nnSCZ920_HOT.tar.gz`—The Heat Orchestration Templates used with OpenStack.
- `nnSCZ920_tfStackBuilder.tar.gz`—The Terraform templates used to create an AWS AMI and for deployment via the OCI resource manager.

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.
-

Oracle Platforms for Session Router and Enterprise Session Router

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

- Through USB: `nnSCZ920-img-usb.exe`
- Through ILOM: `nnSCZ920-img.iso`
- Bootloader file: `nnSCZ920.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 SBC 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. Select **1** to modify the product.
3. Select the number next to the product you wish to initialize.
4. Type **s** to save 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

When you perform a software upgrade, you need to follow the paths presented in these Release Notes and use the same image types to achieve a hitless upgrade. This applies to both HA and non-HA deployments. The paths are presented below. An example of different image types is upgrading a non-LI deployment with an LI image. Such non-hitless upgrades require that you reboot devices per your upgrade procedure, and then reboot all upgraded devices again to establish the new deployment type.

Supported Upgrade Paths

Always start the upgrade process with the latest patch version of your current release.

The SBC, ESBC, and SR support the following in-service (hitless) upgrade and rollback paths:

- S-Cz8.4.0p13 (or higher) to S-Cz9.2.0
- S-Cz9.0.0p5 (or higher) to S-Cz9.2.0
- S-Cz9.1.0p3 (or higher) to S-Cz9.2.0

You can upgrade the SLB using the following in-service upgrade and rollback paths:

- S-Cz9.0.0p6 (or higher) to S-Cz9.2.0
- S-Cz9.1.0p4 (or higher) to S-Cz9.2.0

> **Note:**
>
> This support pertains to software upgrades of nodes in existing HA clusters. It does not pertain to upgrade scenarios when the hardware is being upgraded, such as scenarios that include an upgrade from Netra Server X5-2 to Oracle Server X7-2.

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.

Systems with FIPs Licensing

Do not upgrade any device licensed to use FIPS to S-Cz9.2.0. This causes the system to fail, preventing successful boot.

Platform-Specific Downgrade Limitations

Do not attempt to downgrade your SBC to a release not supported by your platform. See the Platform Support table for which platforms support which releases.

Acme Packet 4900 and 3950 Platforms

There is no upgrade on the Acme Packet 3950/4900 platforms from any SBC software version prior to S-Cz9.0.0. This is because S-Cz9.0.0 is the first version these platforms support.

Acme Packet 3950/4900 Slots

If upgrading to the new Acme Packet 3950/4900 hardware, review the slot numbering in the appendix of the Installation Guide in order to configuration the phy-interface elements.

Connection Failures with SSH/SFTP Clients

If you upgrade and your older SSH or SFTP client stops working, check that the client supports the mimumum ciphers required in the `ssh-config` element. The current default HMAC algorithm is `hmac-sha2-256`; the current key exchange algorithm is `diffie-hellman-group14-sha256`. If a verbose connection log of an SSH or SFTP client shows that it cannot agree on a cipher with the SBC, upgrade your client.

Upgrading from releases earlier than S-Cz8.4.0

The S-Cz8.4.0 release included significant changes that hardened the security of the SBC. These changes require your careful evaluation regarding functionality when upgrading to S-Cz8.4.0 or newer. 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

TSCF Configurations from Prior Software Versions

Release S-Cz9.1.0 and later no longer supports TSM. 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*.

Diffie-Hellman Key Size

In the context of TLS negotiations on SIP interfaces, the default Diffie-Hellman key size offered by the SBC is 1024 bits. The key size is set in the diffie-hellman-key-size attribute within the tls-global configuration element.

While the key size can be increased, setting the key size to 2048 bits significantly decreases performance.

Session Translations

Both **translation-rules** and **session-translation** elements have significantly changed in release S-Cz9.2.0. A backup configuration from release S-Cz9.1.0 or earlier will not be compatible with S-Cz9.2.0 or later, and vice versa. Create a backup of the existing configuration before performing an upgrade as the changes to the **translation-rules** and **session-translation** elements are not backward compatible, during a downgrade.

When upgrading to S-Cz9.2.0, the SBC converts the older **translation-rules** and **session-translation** configuration elements to their new format. Translation rules and session translations will continue to work as before. A rules-called translation rule in release S-

Cz9.1.0 and earlier will be upgraded in S-Cz9.2.0 to two separate translation rules: one that modifies the To header and one that modifies the Request URI.

Default TLS Version

When downgrading from S-Cz9.2.0 to an earlier release, the `tls-version` attribute within a tls-profile will be changed from `tlsv13` to `compatibility`. Earlier releases do not support `tlsv13` as a value for `tls-version`.

Downgrade Caveat for NTP Configurations using an FQDN

If you create a **realm-config** for providing resolution of FQDNs for NTP servers through the wancom0 interface, Oracle recommends that you remove this wancom0 **realm-config** before downgrading to a version that does not support FQDNs for NTP servers. If you retain this configuration, you lose SSH and GUI access after the downgrade.

To recover from this issue, use console access to remove the wancom0 **realm-config**. Also remove the wancom0 **phy-interface** and **network-interface**.

If you configure FQDN resolution for NTP servers through a media interface, you can downgrade to a version that does not support this resolution without removing that configuration.

Upgrade Version Caveat from Session Delivery Manager

The Session Delivery Manager cannot direct upgrades from S-Cz9.1.0p6, S-Cz9.0.0p8 or S-Cz9.0.0p9 for HA deployments. See Knowledge Document # 2952935.1 for a detailed explanation.

SSH Host Key Algorithms

If you upgrade to release S-Cz9.2.0p2 or later, the SBC offers `rsa-sha2-512` as the default host key algorithm. Connecting with a client that only offers a SHA1 hash algorithm, like `ssh-rsa`, is no longer supported; your SSH client must offer a SHA2 hash algorithm. If you receive a "no matching host key type found" error message, make sure your client supports SHA2 host key algorithms.

This changes affects only the algorithms offered by the client, not the host key of the SBC.

New Keys Required for High Availability

If you replace a peer in HA from a system running software prior to S-Cz9.1.0p9 running this version or higher, the old keys become irrelevant resulting in SFTP failures using the old keys on the new peer. High Availability collect operations fail unless the old keys are manually deleted on the active peer. This situation is rare. This issue also occurs if you copy an old configuration into any new peer.

This issue does not occur unless you change a system in an HA pair running software prior to S-Cz9.1.0p9 to a different SBC running this version or higher. To replace keys:

1. Check to see if this issue applies to your deployment. Applicable system have keys using **key-name** parameters named **backup-sbc1** and **backup-sbc2**.
2. Prior to replacing your previous system with a new system, delete the authorized public-keys for the HA systems.
3. Replace your previous system with the new system.

4. Reboot both systems.
   At this point, the SBC generates the new keys automatically, allowing the HA pairs to communicate over the wancom interface(s).

Fraud Protection File Rollback Compatibility

In the S-Cz9.1.0 release and later, the upgrade process automatically changes the former Fraud Protection list types named call-whitelist and call-blacklist to call-allowlist and call-blocklist. This change impacts rollback scenarios.

Previous versions of the software expect the list types formerly named call-whitelist and call-blacklist. Use either of the following methods to make older versions support the Fraud Protection file, which is stored in XML format in a file with an extension of .xml, .gz, or .gzip in the /code/fpe/ directory.

- Back up of your existing Fraud Protection configuration file before upgrading to S-Cz9.1.0 or later, and use it for previous versions of the software in a rollback scenario.
- Perform the upgrade to S-Cz9.1.0 or later, which automatically changes call-whitelist and call-blacklist to call-allowlist and call-blocklist. Before you rollback, edit your S-Cz9.1.0 Fraud Protection file by replacing call-allowlist and call-blocklist with call-whitelist and call-blacklist, respectively.

> **Note:**
>
> You do not need to reverse this method when you upgrade to S-Cz9.1.0 or later. The upgrade process makes the changes automatically.

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

Feature	Type
Quality of Service	boolean
Routing	boolean
Session Capacity	integer
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
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
STIR/SHAKEN Client	Enabled or Disabled
Admin security	Enabled or Disabled
ANSII R226 Compliance	Enabled or Disabled

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
Load Balancing	Enabled or Disabled

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-Cz9.2.0 From Previous Releases

When upgrading from a previous release to S-Cz9.2.0, your encryption entitlements carry forward and you do not need to install new license keys.

System Capacities

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

SIP Interface and Realm Limits for vSBC

The number of Realms and SIP interfaces that you can configure on a vSBC is limited by the amount of VM memory. A maximum of 1500 Realms and SIP interfaces can be configured for every 1GB of system memory.

> **Note:**
>
> These limits also apply to the SR.

Static Trusted and Untrusted ACL Limits for vSBC

When deployed as a virtual SBC or a virtual SR, the SBC supports static ACL entry counts based on virtual machine memory. Deployments under 8GB of memory support 8K trusted and 4K untrusted entries. When memory is:

- Between 8GB and 64GB, supported entries include:
  - Trusted static ACLs is 1024 per GB
  - Untrusted static ACLs is 512 per GB

- Greater than 64GB, supported entries include:
  - Trusted static ACLs is 65536
  - Untrusted static ACLs is 32768

Dynamic ACL entries are independent of this support.

> **Note:**
>
> These limits also apply to the SR.

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) The Acme Packet 4900 does not support 40 and 60 packetization times for the EVS codec.	• AMR • AMR-WB • CN • EVRC • EVRC0 • EVRC1 • EVRCB • EVRCB0 • EVRCB1 • EVS[1] • G711FB • G711OFD • G722 • G723 • G726 • G726-16 • G726-24 • G726-32 • G726-40 • G729 • G729A • GSM • iLBC • OFDFB • opus • PCMA • PCMU • SILK • T.38 • T.38OFD • telephone-event • TTY, except on the Acme Packet 1100

Platform	Supported Codecs (by way of codec-policy in the add-on-egress parameter)
• Virtual Platforms (with 1+ transcoding core) - only supported on Intel CPUs	• AMR • AMR-WB • CN • EVS • G722 • G723 • G726 • G726-16 • G726-24 • G726-32 • G726-40 • G729 • G729A • iLBC • opus • PCMA • PCMU • SILK • 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.

TCM3 and System Software Compatibility

As of April 2023, Oracle has begun supporting new memory components for the TCM3. These components are dependent on SBC software version. Newer Oracle software releases, starting with SCz9.2.0p1, provide you with multiple means of verifying TCM3 memory compatibility. Software versions prior to SCz9.2.0p1 do not operate properly with this new memory, but does allow the TCM3 cards to boot. Furthermore, system behavior when you use older software with this new memory is unpredictable.

If you need to verify the hardware you have, use the **show-prom-info all** command to display the TCU card part number. The applicable part numbers include:

- TCM3 card with old memory—8202681
- TCM3 card with new memory—8213881

See *Minimum TCM3 Versions on the Acme Packet 3950/4900* in the *Transcoding* chapter for explanation about verifying TCM3 memory compatibility with this SBC software release.

Coproduct Support

The following products and features run in concert with the SBC for their respective solutions. Support for Session Router and Enterprise Session Router is also provided below. Contact your Sales representative for further support and requirement details.

Oracle Communications Session Delivery Manager

This S-Cz9.2.0 SBC GA release can interoperate with the following versions of the Oracle Communications Session Delivery Manager:

- 8.2.5

> **Note:**
>
> Customers wishing to manage S-Cz9.2.0 patches in conjunction with Oracle's Session Delivery Manager must review the build notes to determine if an XSD file is required. In addition, please review the readme file in the XSD file for confirmation. XSD files may work with older OCSDM releases, though not guaranteed.

Oracle Session Delivery Manager Cloud

This S-Cz9.2.0 SBC release can interoperate with the following versions of the Oracle Session Delivery Manager Cloud:

- 22.1.0 and higher

Oracle Communications Operations Manager

This S-Cz9.2.0 SBC release can interoperate with the following versions of the Oracle Communications Session Monitor:

- 4.4.0
- 5.0.0
- 5.1.0

Oracle Communications Subscriber Aware Load Balancer

This S-Cz9.2.0 SBC release can interoperate as a cluster member with the following versions of the Subscriber Aware Load Balancer (SLB):

- S-Cz9.0.0
- S-Cz9.1.0
- S-Cz9.2.0

> **Note:**
>
> SLB is not supported with OCOM

Oracle Communications Session Router

This S-Cz9.2.0 SBC release can interoperate with the following versions of the Session Router:

- S-Cz8.4.0
- S-Cz9.0.0

- S-Cz9.1.0
- S-Cz9.2.0

Pooled Transcoding

This S-Cz9.2.0 SBC release acting as an A-SBC can interoperate with T-SBCs on the following hardware/software combinations :

- All platforms supported by the following releases: S-Cz8.4.0, S-Cz9.0.0 , S-Cz9.1.0, S-Cz9.2.0
- Acme Packet 4500 running S-Cz7.4.0
- Virtual Platforms with Artesyn SharpMedia™: S-Cz8.4.0, S-Cz9.0.0 , S-Cz9.1.0, S-Cz9.2.0

This S-Cz9.2.0 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-Cz8.4.0, S-Cz9.0.0 , S-Cz9.1.0, S-Cz9.2.0
- Acme Packet 4500 running S-Cz7.4.0

Session Routers and SDM

This S-Cz9.2.0 release of the Oracle Communications Session Router and Enterprise Session Router can interoperate with the following versions of the Oracle Communications Session Delivery Manager:

- 8.2.4 and above

Session Routers and Operations Manager

This S-Cz9.2.0 release of the Oracle Communications Session Router and Enterprise Session Router can interoperate with the following versions of the Oracle Communications Operations Manager:

- 4.4
- 5.0
- 5.1

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_AES_128_GCM_SHA256 (new in 9.2.0)
- TLS_AES_256_GCM_SHA384 (new in 9.2.0)
- TLS_CHACHA20_POLY1305_SHA256 (new in 9.2.0)
- TLS_AES_128_CCM_SHA256 (new in 9.2.0)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256

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

- TLS_AES_128_CCM_8_SHA256 (new in 9.2.0)
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256

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**. The **verify-config** command returns a warning if these ciphers are used.

- TLS_RSA_WITH_3DES_EDE_CBC_SHA (demoted to weak in 9.2.0)
- 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

Oracle supports the following ciphers for debugging purposes only:

- TLS_RSA_WITH_NULL_SHA256
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_NULL_MD5

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

> **WARNING:**
>
> When you set **tls-version** to either **tlsv1**, **tlsv11**, **tlsv12** or **tlsv13**, and you want to use ciphers that Oracle considers not secure, you must manually add them to the **cipher-list** attribute.

Documentation Changes

The following information describes structural changes to the documentation for the S-Cz9.2.0 release.

ACLI Configuration Guide

Renamed the "Number Translation" chapter as "Session Translation".

ACLI Reference Guide

Removed the duplicate **dtls-srtp-profile** topic. See the **media-security > dtls-srtp-profile** topic for documentation about the **dtls-srtp-profile** configuration element.

Enterprise ACLI Configuration Guide

Removes the STIR/SHAKEN Client chapter.

Behavioral Changes

The following information describes behavioral changes to the Oracle Communications Session Border Controller (SBC) for version S-Cz9.2.0.

Default TLS Version

When creating a tls-profile, the default tls-version is **tlsv13** rather than **tlsv12**. See "TLS Cipher Updates" to determine which ciphers are included in the new default cipher list.

IKE Interface Precedence

Prior to S-Cz9.2.0, if you had an invalid certificate configured in ike-interface but a valid certificate in ike-config, the SBC would accept the ike-config certificate rather than the ike-interface certificate. In release S-Cz9.2.0, ike-interface attributes take precedence over ike-config attributes. Verify your certificates in ike-interface are valid to ensure that the SBC establishes IPsec tunnels properly.

HTTP Client Management

By default, the SBC stops creating TCP connections to servers configured as an **http-client** when it reaches 500 connections, or CPU utilization reaches 70%. The system does this to reduce the impact of these clients traffic on the overall system. You can change these values or disable this function using the **httpclient-max-total-conn** and **httpclient-max-cpu-load** parameter in the **system-config**.

SSH Host Key Algorithms

If you upgrade to release S-Cz9.2.0p2 or later, the SBC offers `rsa-sha2-512` as the default host key algorithm. Connecting with a client that only offers a SHA1 hash algorithm, like `ssh-rsa`, is no longer supported; your SSH client must offer a SHA2 hash algorithm. If you receive a "no matching host key type found" error message, make sure your client supports SHA2 host key algorithms.

This changes affects only the algorithms offered by the client, not the host key of the SBC.

SSH Keys for HA

When deploying the SBC in an HA environment, the SBC adds SSH keys to the active and standby configuration to support switchovers and HDR replication.

An example of the known-host keys:

```
ssh-key
        name                                    169.254.1.1
        size                                    2048
ssh-key
        name                                    169.254.1.2
        size                                    2048
ssh-key
        name                                    169.255.1.1
        size                                    2048
ssh-key
        name                                    169.255.1.2
        size                                    2048
```

An example of the authorized-keys:

```
ssh-key
        name                                    backup-sbc1
        type                                    authorized-key
        size                                    2048
ssh-key
        name                                    backup-sbc2
        type                                    authorized-key
        size                                    2048
```

Patches Included in This Release

The following information assures you that when upgrading, the S-Cz9.2.0 release includes defect fixes from neighboring patch releases.

Neighboring Patches Included

- S-Cz840p14
- S-Cz900p6
- S-Cz910p4

Supported SPL Engines

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

The S-Cz9.2.0 release of the Oracle Communications Session Border Controller (SBC) software includes the following new features.

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

Session Translation Enhancements

In the *Configuration Guide*, the Number Translation chapter is renamed Session Translation. The **number-translation** element has been redesigned to support regular expressions that match predefined input headers and populate predefined output headers. The **session-translation** element is enhanced to more easily group and rearrange number translations. And finally, the **realm-config** and **session-agent** elements are enhanced to support grouping and rearranging session translations.

Update an Existing Certificate Record with a New Certificate

When you need to renew a certificate on the Session Border Controller, you no longer need to create a new certificate record. You can go to the existing record and import the renewed certificate. The imported certificate overwrites the existing one. See "Update a Certificate" in the *Web GUI Guide* and the *Configuration Guide*.

Alarm Enhancement

This release adds three alarms to help monitor system status, especially suited for notifying you of issues before they become operational problems. The new alarms include The Session Agent Out of Service Alarm, The Steering Pool Threshold Alarm, and The Internal 503 Threshold Alarm.

See the sections using the same titles as the alarms in the Fault Management chapter of the *Maintenance and Troubleshooting Guide* for detailed information.

Creating a Reason Header During Verification

You can configure the SBC to create and insert SIP reason headers into applicable SIP INVITEs based on information received from an STI-VS during verification attempts. These headers provide insight into the reason the STI-VS could not or did not verify the request. You can use this feature to provide visibility into the reasoncode, reasontext and the verstat parameters downstream within the SIP INVITE and in CDRs. This feature applies to both ATIS and 3GPP modes.

See the Creating a Reason Header During Verification section in the STIR/SHAKEN chapter of the*ACLI Configuration Guide* for detailed information.

HTTP Header Customization for STIR/SHAKEN

You can configure the SBC with static mapping to and from SIP INVITEs and HTTP requests or responses within the context of STIR/SHAKEN authentication or verification procedures. This mapping provides a means of conveying SIP header information within HTTP headers and conversely. This feature adds headers and their new parameters in the rules targets or modifies existing headers with the new parameters presented by the rule. This feature applies to both ATIS and 3GPP modes.

See the HTTP Header Manipulation section in the STIR/SHAKEN chapter of the *ACLI Configuration Guide* for detailed information.

Please review the Caveats and Limitations Chapter of the S-Cz9.2.0 Known Issues and Caveats Guide for functional limitations of this feature that apply to this software release.

CALEA in Authentication Requests

You can configure the OCSBC to include Communications Assistance for Law Enforcement Act (CALEA) information in SHAKEN and DIV PASSporT authentication requests. This feature applies to both ATIS and 3GPP operation modes.

See the Including CALEA in Authentication Requests section in the STIR/SHAKEN chapter of the*ACLI Configuration Guide* for detailed information.

DTLS-SRTP Server Mode

The SBC supports Datagram Transport Layer Security (DTLS) to establish SRTP media traffic over UDP in server mode. The SBC uses DTLS within the context of SRTP (DTLS-SRTP) per RFC 5764. This DTLS-SRTP feature provides for secure media, supports the same transfer scenarios supported for SDES-SRTP, and supports unattended transfer, and music on hold scenarios.

This feature is not supported on the SLB.

See the DTLS-SRTP section in the Security chapter of the *ACLI Configuration Guide* for detailed information.

Please review the Caveats and Limitations Chapter of the S-Cz9.2.0 Known Issues and Caveats Guide for functional and platform limitations of this feature that apply to this software release.

Flowtype AVPs

This release of the SBC adds 5 AVPs that the system includes in CDRs to better identify and track media flows. These AVPs include, Acme-FlowIDFS1-R, Acme-FlowIDFS2-F, Acme-FlowIDFS2-R, Acme-FlowType-FS2-F, and Acme-FlowType-FS2-R.

See the sections using the same titles as the AVPs in Appendix C of the *Accounting Guide* for detailed information.

NTP Servers Configured with an FQDN

You can configure the SBC with an FQDN for establishing communications with NTP time servers. This feature supports FQDN resolution through a DNS query over wancom or media interfaces. Having received DNS resolution for the query, the SBC

uses its standard selection process for DNS results to request time synchronization from one of multiple, redundant NTP servers.

See the FQDNs for Time Servers on the SBC section in the Diameter Accounting Chapter of the *Accounting Guide* for detailed information.

Using FQDNs to Access CCFs over Diameter

You can configure the SBC with a primary and, if wanted, a secondary FQDN to access CCF servers over Diameter. You do this by configuring the diameter account-server with an FQDN. The SBC uses DNS to resolve the FQDN into an IP list and, if provided, route the traffic based on DNS-provided priority and weight. The SBC supports resolution of CCF FQDNs from SRV, and A records.
See the Using FQDNs to Access CCFs over Diameter section in the Diameter Accounting Chapter of the *Accounting Guide* for detailed information.

STI Server Status Timer Changes

This release changes the values you can configure to the STI server circuit breaker window timers to enhance the ability of the SBC to manage STI server status.

See the STIR/SHAKEN chapter of the *ACLI Configuration Guide* and the circuit-breaker-retry-time and circuit-breaker-half-open-frequency parameters in the *ACLI Reference Guide* for the new values.

Enhanced Reporting on NSEP Traffic Statistics

The SBC provides you with NSEP traffic statistics from the ACLI and SNMP. You can access system wide NSEP traffic reports when you configure the system for applicable network management controls (NMC). In addition, you can now configure the system to provide realm-specific reporting on a per-realm basis by configuring the nsep-stats-profile on the session-router and enabling nsep-stats on the applicable realms.

See the Reporting on NSEP Traffic Statistics section in the SIP Signaling Services Chapter of the *ACLI Configuration Guide* for detailed information.

Parallel Call Forking

You can configure the SBC to direct calls to multiple targets simultaneously using parallel forking. You establish parallel forking behavior by enabling the parallel-forking parameter on one or more local-policy elements and configuring the cost within each applicable policy-attribute.

See the Parallel Call Forking section in the Routing Chapter of the *ACLI Configuration Guide* for detailed information.

Please review the Caveats and Limitations Chapter of the S-Cz9.2.0 Known Issues and Caveats Guide for functional limitations of this feature that apply to this software release.

Enhancements to Preconditions Processing

You can configure the SBC to extend its support of preconditions with dynamic preconditions, which allows the SBC to determine whether and where to support preconditions for a given call. When you configure the system for the above, you also:

- Configure the SBC to manipulate the PEM header within both static asymmetric and dynamic preconditions call flows to change the direction attributes.

- Establish system behavior changes for certain preconditions call flows wherein the SBC changes the direction value of the SDP media attribute to prevent issues.
- Establish support for all of the strength tag values within all preconditions attributes. In addition, the SBC inserts strength tags under certain conditions.

See the Enhanced Preconditions section in the SIP Signaling Chapter of the *ACLI Configuration Guide* for detailed information.

Allocation Strategies for Steering Pools

You can configure the SBC with three types of steering pools to allocate network ports for specific types of network traffic. These pool types include audio/video, MSRP and mixed media types. Establishing these pool types provides more efficient use of media ports.

See the Allocation Strategies for Steering Pool section in the Realms and Nested Realms Chapter of the *ACLI Configuration Guide* for detailed information.

3GPP Mode for STIR Shaken Deployments

This version of the SBC adds support for the 3GPP mode of STIR/SHAKEN operation. 3GPP supports verifying DIV passports in addition to SHAKEN passports. The DIV category refers to passports generated for diverted calls.

See the STIR/SHAKEN chapter of the *ACLI Configuration Guide* for detailed information. This feature creates changes in multiple sections of that chapter.

STIR SHAKEN FQDN TTL Expiry

You can configure the SBC to use FQDNs for STI-AS and STI-VS server to establish STIR/SHAKEN server pools using DNS. This new feature includes TTL expiry as a trigger to DNS queries.

See the Server Names as FQDNs section in the STIR/SHAKEN chapter of the *ACLI Configuration Guide* for detailed information.

SDP Compliance Enforcement

You can configure the SBC to enforce SDP compliance on incoming messages and reject non-compliant messages and change the non-compliant SDP in ensuing messages. By default, the SBC forwards response message even if the Content-Length is greater than the SDP size and the SDP does not have mandatory parameters. You enable the **sip-strict-compliance** option when the SBC is operating in environments where it is expected to monitor and validate these aspects of SDP.

See the SDP Compliance Enforcement section in the SIP chapter of the *ACLI Configuration Guide* for detailed information.

Managing HTTP Connections

By default, the SBC limits system impact caused by HTTP client behavior using the **httpclient-max-total-conn** and **httpclient-max-cpu-load** parameters in the **system-config**. These parameters, respectively, allow you to change the number of TCP connections and the amount of CPU resources consumed by traffic between the SBC and all types of HTTP servers.

See the Managing HTTP Connections section in the System Configuration chapter of the *ACLI Configuration Guide* for detailed information.

TLS 1.3 Support

This release supports TLS 1.3 by default. See the **tls-profile** topic in the ACLI Configuration Guide and the "Configure a TLS Profile" section in the Security chapter of the Configuration Guide.

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 Troubleshooting section of these *Release Notes* for specific software/hardware compatibility for this version of the SBC software.

> **Note:**
>
> This new feature support begins with S-Cz9.2.0p1.

STIR/SHAKE Support on the Session Router

This version of the SBC updates the Session Router support for STIR/SHAKEN functionality to be the same as the SBC.

> **Note:**
>
> This new feature support begins with S-Cz9.2.0p1.

DTLS/SRTP Support on the Acme Packet 6350

This version of the SBC adds DTLS/SRTP support on the Acme Packet 6350.

> **Note:**
>
> This new feature support begins with S-Cz9.2.0p1.

Enhanced Restricted Latching

You can now configure the SBC to latch all media flows within a realm to both the externally provided address and port when you set the restricted-latching mode to sdp-ip-port. When configured to this setting, the system latches to media based on the IP Address received in the SDP c= connect address line, and the port in the mline in the offer and answer. This differs from standard latching in that the port is left unassigned by the SBC. This feature allows the SBC to better support multiple RTP streams from different ports using the same IP address, such as within forking scenarios.

See the Restricted Latching section in the Realms chapter of the *ACLI Configuration Guide* for detailed information.

> **Note:**
>
> This new feature support begins with S-Cz9.2.0p2.

DPDK Uplift

This version of the SBC uplifts the DPDK version to 22.11.

> **Note:**
>
> This new feature support begins with S-Cz9.2.0p2.

DPDK Uplift

This version of the SBC allows you to configure the SBC to use a static TCP port when connecting to a **session-agent** instead of an ephemeral port.

See the About Session Agents section in the Session Routing and Load Balancing chapter of the *ACLI Configuration Guide* for detailed information.

> **Note:**
>
> This new feature support begins with S-Cz9.2.0p3.

PSAP Callback Enhancement

You can configure the SBC to support Public Safety Answering Point (PSAP) callback handling to numbers that are not in the PSAP callback list, which includes 911, 112 and any number you have added. You can also configure the SBC to replace the request-URI in a PSAP callback to resolve routing issues.

See the PSAP Callback Option section in the SBC Processing Language (SPL) chapter of the *ACLI Configuration Guide* for detailed information.

> **Note:**
>
> This new feature support begins with S-Cz9.2.0p4.

Verstat Delimiter

This version of the SBC allows you to configure the **verstat-delimiter** option in the applicable **sti-server**. You use this delimiter to refine the specific text of the verstat during verstat retrieval processes.

See the STIR/SHAKEN chapter of the *ACLI Configuration Guide* for detailed information about this parameter.

> **Note:**
>
> This new feature support begins with S-Cz9.2.0p1.

HTTP Client Cache Size Configuration

This version of the SBC allows you to configure the **httpclient-cache-size-multiplier** parameter in the **system-config** to adjust the size of the HTTP connection cache.

See the HTTP Connection Management section in the System Configuration chapter of the *ACLI Configuration Guide* for detailed information about this parameter.

> **Note:**
>
> This new feature support begins with S-Cz9.2.0p4.

Session-Level DoS Protection

You can configure the SBC to implement DoS protection when any individual session appears to be conducting an attack. You can configure this protection on a **realm-config** or a **session-agent**, with the **session-agent** configuration taking precedence when applicable.

See the DoS Protection section in the Security chapter of the *ACLI Configuration Guide* for detailed information about this feature.

> **Note:**
>
> This new feature support begins with S-Cz9.2.0p5.

Subscription-Id-Data AVP

When applicable, the SBC can send a Subscription-Id-Data AVP (444) to an external policy server. This AVP is contained within the grouped Subscription-Id AVP (443) and carries the user's identifier. You can configure the SBC to refine this data so it gets this information from the SBC and uses your configured value for the **subscription-id-type** parameter to determine which user identifier it sends.

See the Subscriber Information AVP section in the External Policy Server chapter of the *ACLI Configuration Guide* for detailed information about this feature.

> **Note:**
>
> This new feature support begins with S-Cz9.2.0p5.

RFC 6733 Compliance for the Vendor-Specific-Application-Id

You can configure the SBC to perform CER and LIR transactions over the Cx interface in compliance with RFC 6733 with respect to the contents of the Vendor-Specific-Application-Id AVP (260). You do this by setting the **rfc6733compliant** option under the applicable **home-subscriber-server**. RFC 6733 compliance consists of several behaviors, including limiting

the number of Vendor-Ids present in the CER and LIR diameter messages to one. By default, the system aligns with RFC 3588 and sends out both Vendor-IDs in the diameter messages.

See the Compliance for the Vendor-Specific-Application-Id section in the IMS chapter of the *ACLI Configuration Guide* for detailed information about this feature.

> **Note:**
>
> This new feature support begins with S-Cz9.2.0p5.

Supporting HA with STIR SHAKEN over TCP

You can configure the SBC with the **exclusive-http-client-port-range** option within the **system-config** to support an HA Pair running STIR SHAKEN to use the different set of ports between Primary and Secondary machine for establishing TCP connection with HTTP server.

See the Supporting HA with STIR SHAKEN over TCP section in the STIR SHAKEN chapter of the *ACLI Configuration Guide* for detailed information about this feature.

> **Note:**
>
> This new feature support begins with S-Cz9.2.0p5.

Create a Dictionary File for Decoding AVPs

You can generate an AVP dictionary from the SBC to install and use for decoding Oracle-specific Rf AVPs in messages using Wireshark. After generating this dictionary, you include it within your Wireshark deployment and configure a Wireshark resource file. This allows Wireshark to decode standalone and grouped AVPs identified with the ACME_DIAM_VENDOR_ID label.

See the Create a Dictionary File for Decoding AVPs task in the Diameter Accounting chapter of the *Accounting Guide* for detailed information about this feature.

> **Note:**
>
> This new feature support begins with S-Cz9.2.0p5.

Support for the Mellanox C5 Interface

The SBC supports the Mellanox C5 interface for use as a media interface. For this release, Oracle is supporting this interface on the vSBC over KVM in SRIOV mode.

> **Note:**
>
> This new feature support begins with S-Cz9.2.0p6.

SPL for Skipping the INVITE Validation for KDDI

You can configure an SPL option on the SBC to disable incoming INVITE validation. This feature makes use of the Control-Surr-Reg SPL, requiring the applicable configuration. When you configure this feature, the SBC does not attempt to match the incoming R-URI against the random user part received while performing the Surrogate Registration SPL feature processing for KDDI deployments.

> **Note:**
>
> This new feature support begins with S-Cz9.2.0p6.

REFER Handling Enhancement

The SBC may stop sending its configured ring back tone (RBT) to the caller when operating within some transfer scenarios. Applicable scenarios include the presence of network infrastructure that issues a BYE from the callee to the SBC while the transfer is underway. You can configure the SBC to persist with RBT for the duration of the transfer process so the caller does not unexpectedly lose RBT.

> **Note:**
>
> This new feature support begins with S-Cz9.2.0p6.

3
Interface Changes

The following topics summarize ACLI, SNMP, HDR, Alarms, Accounting, and Error/Warning changes for S-Cz9.2.0. The additions, removals, and changes noted in these topics occurred since the previous major release of the Oracle Communications Session Border Controller.

ACLI Configuration Element Changes

The following tables summarize the ACLI configuration element changes in the Oracle Communications Session Border Controller S-Cz9.2.0 release.

SIP Config

New Attributes	Description
session-router, **sip-config**, **precondition-enhancement**	Enables preconditions behaviors, including Dynamic Preconditions, PEM Gating, Changing the Media Direction Attribute, and the Optional Strength Tag Support

Realm Config

Modified Elements	Description
media-manager, **realm-config**, **in-translationid**	This attribute has been removed.
media-manager, **realm-config**, **out-translationid**	This attribute has been removed.
media-manager, **realm-config**, **in-session-translations**	This element has been added. Use this element to configure ingress session translations.
media-manager, **realm-config**, **in-session-translations**, **in-session-translation-id**	Identify the session translation id to apply to ingress headers.
media-manager, **realm-config**, **in-session-translations**, **state**	Enable or disable this session translation.
media-manager, **realm-config**, **in-session-translations**, **move**	Change the order of execution of the session translation rules.
media-manager, **realm-config**, **out-session-translations**	This configuration element has been added. Use this element to configure egress translations.
media-manager, **realm-config**, **out-session-translations**, **out-session-translation-id**	Identify the session translation id to apply to egress headers.
media-manager, **realm-config**, **out-session-translations**, **state**	Enable or disable this session translation.
media-manager, **realm-config**, **out-session-translations**, **move**	Change the order of execution of the session translation rules.
media-manager, **realm-config**, **fqdn-hostname**	The FQDN hostname to be used in messages.
media-manager, **realm-config**, **fqdn-hostname-in-header**	The headers where the FQDN hostname can be applied.
media-manager, **realm-config**, **P-Asserted-Identity**	The string you want to use to set the identity within PAI headers for this realm's egress traffic

Modified Elements	Description
media-manager, **realm-config**, **P-Asserted-Identity-For**	The method header to match for inserting PAI headers.

Session Agent

Modified Elements	Description
session-router, **session-agent**, **in-translationid**	This attribute has been removed.
session-router, **session-agent**, **out-translationid**	This attribute has been removed.
session-router, **session-agent**, **in-session-translations**	This element has been added. Use this element to configure ingress session translations.
session-router, **session-agent**, **in-session-translations**, **in-session-translation-id**	Identify the session translation id to apply to ingress headers.
session-router, **session-agent**, **in-session-translations**, **state**	Enable or disable this session translation.
session-router, **session-agent**, **in-session-translations**, **move**	Change the order of execution of the session translation rules.
session-router, **session-agent**, **out-session-translations**	This configuration element has been added. Use this element to configure egress translations.
session-router, **session-agent**, **out-session-translations**, **out-session-translation-id**	Identify the session translation id to apply to egress headers.
session-router, **session-agent**, **out-session-translations**, **state**	Enable or disable this session translation.
session-router, **session-agent**, **out-session-translations**, **move**	Change the order of execution of the session translation rules.
session-router, **session-agent**, **fax-servers**	Add a fax server group.

System Config

Modified Elements	Description
system, **system-config**, **collect**	This element is no longer visible when the product is SLB.
system, **system-config**, **link-redundancy-state**	Attribute is not present in 9.2.
system, **system-config**, **log-tls-key**	Enable logging TLS keys
system, **system-config**, **httpclient-max-total-conn**	The total number of TCP connections allowed by HTTP clients.
system, **system-config**, **httpclient-max-cpu-load**	The maximum CPU percentage for HTTP clients.

TLS 1.3

Modified Elements	Description
security, **tls-profile**, **tls-version**	The **tls-version** attribute has a new default value: **tlsv13**.

Translation Rules

Modified Elements	Description
session-router, **translation-rules**, **type**	This attribute has been removed.
session-router, **translation-rules**, **add-string**	This attribute has been removed.
session-router, **translation-rules**, **add-index**	This attribute has been removed.
session-router, **translation-rules**, **delete-string**	This attribute has been removed.
session-router, **translation-rules**, **delete-index**	This attribute has been removed.
session-router, **translation-rules**, **description**	This attribute has been added. Provide a description of this translation rule.
session-router, **translation-rules**, **input-header-type**	This attribute has been added. Select the ingress header on which to perform a translation rule.
session-router, **translation-rules**, **input-header-value**	This attribute has been added. Enter a regex pattern to identify which part of the ingress header will be manipulated.
session-router, **translation-rules**, **output-header-type**	This attribute has been added. Select the egress header that will contain the previously captured information.
session-router, **translation-rules**, **output-header-value**	This attribute has been added. Enter the regex pattern that will create the value of the egress header.

Session Translation

Modified Elements	Description
session-router, **session-translation**, **rules-calling**	This attribute has been removed.
session-router, **session-translation**, **rules-called**	This attribute has been removed.
session-router, **session-translation**, **rules-asserted-id**	This attribute has been removed.
session-router, **session-translation**, **rules-redirect**	This attribute has been removed.
session-router, **session-translation**, **rules-history-info**	This attribute has been removed.
session-router, **session-translation**, **rules-isup-cdpn**	This attribute has been removed.
session-router, **session-translation**, **rules-isup-cgpn**	This attribute has been removed.
session-router, **session-translation**, **rules-isup-gn**	This attribute has been removed.
session-router, **session-translation**, **rules-isup-rdn**	This attribute has been removed.

Modified Elements	Description
session-router, **session-translation**, **rules-isup-ocn**	This attribute has been removed.
session-router, **session-translation**, **id**	This attribute has been added. Provide a name for this set of translation rules.
session-router, **session-translation**, **session-trans-rule**	This configuration element has been added.
session-router, **session-translation**, **session-trans-rule**, **rule-id**	Identify the id of the translation rule that you want to apply.
session-router, **session-translation**, **session-trans-rule**, **mandatory**	Determine whether this translation-rule is required or not.
session-router, **session-translation**, **session-trans-rule**, **state**	Enable or disable this translation-rule.
session-router, **session-translation**, **session-trans-rule**, **move**	This command has been added. Change the order in which the translation rules are run.

Media Security

New Attributes	Description
security, **media-security**, **media-sec-policy**	Configure a media security policy to apply to inbound or outbound traffic.
security, **media-security**, **sdes-profile**	Configure an SDES profile.
security, **media-security**, **sipura-profile**	Configure a Sipura/Linksys profile.

Home Subscriber Server

New Attributes	Description
session-router, **home-subscriber-server**, **options**	A new options attribute exists in this release.

Local Policy

New Attributes	Description
session-router, **local-policy**, **policy-attributes**, **move**	Move the position of a policy attribute.
session-router, **local-policy**, **parallel-forking**,	Used for forking a call in parallel to policy-attributes

MSRP Config

New Attribute	Description
media-manager, **msrp-config**, **msrp-kpi**	Enable or disable MSRP KPI statistics.

SIP Interface

New Attributes	Description
session-router, **sip-interface**, **allow-diff2833-clock-rate-mode**	Specifies whether and how the SBC can present an SDP answer towards ingress that contains a telephone-event clock rate that is not the same as the audio codec clock rate.

Steering Pool

New Attributes	Description
media-manager, **steering-pool**, **port-allocation-strategy**	Select the appropriate strategy for this steering pool based on media type support in this realm.

STI Header Mapping Rules

New Attributes	Description
session-router, **sti-header-mapping-ruleset**	Multi-instance element allowing you to create header manipulations that target Stir/Shaken traffic.
session-router, **sti-header-mapping-ruleset**, **name**	Specifies a unique identifier for this sti-header-mapping-ruleset. You use this name when you apply the ruleset to either a sti-server or the sti-config.
session-router, **sti-header-mapping-ruleset**, **mapping-rules**	Multi-instance element from which you create rules for manipulating headers within Stir/Shaken traffic.
session-router, **sti-header-mapping-ruleset**, **mapping-rules**, **id**	Specifies a unique identifier for this mapping-rule.
session-router, **sti-header-mapping-ruleset**, **mapping-rules**, **source-header**	Specifies the header within an HTTP request or a SIP INVITE from which you create changes to the target-header. You can use Regex syntax to refine the selection of the header components that you apply to the target-header.
session-router, **sti-header-mapping-ruleset**, **mapping-rules**, **target-header**	Specifies the header you modify, based on this rule's source-header parameter, within an HTTP request or a SIP INVITE. You can use Regex syntax to refine the insertion of the header components that you apply to this header.
session-router, **sti-header-mapping-ruleset**, **mapping-rules**, **direction**	Specifies the direction that this rule affects. Outbound causes the system to modify headers traffic to the applicable sti-server. Inbound affects headers from the sti-server.
session-router, **sti-header-mapping-ruleset**, **mapping-rules**, **role**	Specifies the role, Stir/Shaken authentication or verification, within which this rule applies.

STI Config and STI Server

New Attributes	Description
session-router, **sti-config**, **use-identity-header**	Causes the SBC to add a Reason header to 18x, 19x responses and 3xx, 4xx, 5xx, 6xx final responses that it sends to a callee with a cause value of “428” and the text “Use Identity Header” for all received INVITEs that did not contain an identity header.
session-router, **sti-config**, **check-duplicate-passports**	Enables the system to check for duplicate SHAKEN or DIV passports in a received INVITE.
session-router, **sti-config**, **tn-retargeting**	Enables the system to perform DIV authentication request, based on the received INVITE.
session-router, **sti-config**, **verstat-comparison**	Determines whether and how the system compares the verstat value present in FROM and PAI headers.
session-router, **sti-config**, **dest-comparison**	Specifies whether and on which header the system compares its stored TN.
session-router, **sti-config**, **sti-as-correlation-id**	Adds the SipCallId parameter to REST authentication requests to the STI-AS.
session-router, **sti-config**, **reason-json-sip-translation**	Creates a Reason header from the parameters reasoncode and reasontext, if received from the STI-VS.
session-router, **sti-config**, **sti-header-mapping-ruleset-name**	Name of this STI Header Mapping Ruleset you want to use as default across all sti-servers.
session-router, **sti-config**, **flip-tn-lookup-order**	Prioritize the FROM header over the PAI header as the source from which it retrieves a TN for use during authentication and verification procedures.
session-router, **sti-server**, **role**	The role of the STIR/SHAKEN server.
session-router, **sti-server**, **http-rest-type**	The type of the STIR/SHAKEN implementation.
session-router, **sti-server**, **div-as-server-root**	The STI-AS Server root URL for div authentication requests.
session-router, **sti-server**, **div-vs-server-root**	The STI-VS Server root URL for div verification requests.
session-router, **sti-server**, **options**	A new options parameter.
session-router, **sti-server**, **sti-header-mapping-ruleset-name**	The name of the instance of sti-header-mapping-ruleset to apply.

DTLS-SRTP

New Attributes	Description
security, **media-security** , **dtls-srtp-profile**, **name**	Unique identifier for this DTLS SRTP profile. Use this name when you apply the profile to realms.
security, **media-security** , **dtls-srtp-profile**, **tls-profile**	The name of the tls-profile you want to apply to traffic under this dtls-srtp-profile.

New Attributes	Description
security, **media-security** , **dtls-srtp-profile**, **dtls-completion-timeou**	Specify the number of seconds the system waits for a DLTS handshake to finish before terminating the session.
security, **media-security** , **dtls-srtp-profile**, **preferred-setup-role**	Specify the role the system takes within the client-server context of the DTLS handshake.
security, **media-security** , **dtls-srtp-profile**, **crypto-suite**	Specifies the cryptography suite the system proposes during the DTLS handshake for encrypting media and authentication.
realm-config, **dtls-srtp-profile**	The name of the dtls-srtp-profile you want to apply to DTLS traffic on this realm

NSEP Statistics

New Attributes	Description
session-router, **nsep-stats-profile**, **state**	Enables or disables this nsep-stats-profile, which is a multiple element
session-router, **nsep-stats-profile**, **rvalues**	Lists the rvalues to be considered for per realm statistics.
session-router, **nsep-stats-profile**, **feature-code**	The country code STD to be used to with the dialed numbers on which you want to collect realm-based statistics. This is to be pre-pended to all configured dialed numbers. This value must be configured if any dialed number is configured. You can configure only one feature code.
session-router, **nsep-stats-profile**, **dialed-numbers**	Specifies the dialed numbers to be considered for per realm statistics. Use of this parameter also requires that the feature-code parameter be configured.
media-manager, **realm-config**, **nsep-stats**	Enable NSEP statistics on a realm.

CCF via FQDN

Modified Elements	Description
session-router, **account-config**, **dns-realm**	The realm where the DNS server from which the system can obtain resolutions to an FQDN hostname for a Diameter server.
session-router, **account-config**, **acr-buffer-upper-threshold**	New attribute. The upper threshold for the ACR buffer after which the SBC will select an alternate server.
session-router, **account-config**, **acr-buffer-lower-threshold**	New attribute. The lower threshold for the ACR buffer which, when reached, the SBC will select the primary server again.
session-router, **account-config**, **maintain-ccf-affinity**	New attribute. Enable an affinity between ACRs and CCFs so that all ACRs within a single session are sent to the same CCF (unless it goes down).
session-router, **account-config**, **send-disconnect-peer-msg**	New attribute. Enable or disable sending the disconnect message to a peer.
session-router, **account-config**, **next-priority-selection-interval**	New attribute. The time interval in minutes between routing the new call session to the next lower priority CCF after the first switch.

Modified Elements	Description
session-router, **account-group**, **account-servers**, **fqdn-pool-type**	New attribute. Identify whether the configured hostname FQDN belongs to the primary pool or the secondary pool.

NTP Sync

New Attribute	Description
ntp-sync, **dns-realm**	The realm on which your NTP server resides.

New Alarms

New Attributes	Description
session-router, **sip-config**, **internal-503-threshold**	The percentage of 503 Service Unavailable responses over the total SBC-generated messages which, once crossed, generates an alarm.
session-router, **sip-config**, **internal-503-lower-threshold**	The percentage of 503 Service Unavailable responses which, once crossed, informs the system that the previously generated alarm is considered resolved.
session-router, **sip-config**, **503-alarm-monitoring-time**	The number of minutes before which the SBC rechecks whether the internal 503 alarm is cleared.
media-manager, **realm-config**, **steering-pool-threshold**	The utilization percentage for steering pools which, once crossed, generates an alarm.
media-manager, **realm-config**, **steering-pool-lower-threshold**	The utilization percentage for steering pools which, once crossed, the previously generated alarm is considered resolved.
media-manager, **realm-config**, **steering-pool-alarm-monitoring-time**	The number of minutes that a steering-pool alarm should be monitored before re-triggering.
session-router, **session-agent**, **trigger-oos-alarm**	Enable or disable the sending of an alarm when a Session Agent is out of service

Surrogate Agent

New Attributes	Description
session-router, **surrogate-agent**, **auth-user-lookup**	Enter the name of an auth-user-lookup in a realm's auth-attributes list so that the SBC uses those credentials to authenticate challenged register requests
session-router, **surrogate-agent**, **proxy-name**	Enter the name of the session agent you have configured as the Registrar that validates this surrogate agent's register requests for the purpose of routing to that session agent.
session-router, **surrogate-agent**, **un-register**	Set the de-registration state
session-router, **surrogate-agent**, **source-ip-prefix**	Enter the list of IP address (with optional prefix) to validate the source IP.

TCP Port for Session Agents

The following change was introduced in S-CZ9.2.0p3.

New Attributes	Description
session-router, **session-agent**, **static-tcp-source-port**	Set the source TCP port for the session agent.

Updates to the STI Server Group

Modified Element	Description
session-router, **sti-server-group**, **strategy**	The following strategy parameter values are not supported: • least-busy • prop-dist

ACLI Command Changes

The following table summarizes the ACLI command changes in the Oracle Communications Session Border Controller S-Cz9.2.0 release.

This table lists and describes changes to ACLI commands that are available in the S-Cz9.2.0 release.

New Commands	Description
clear-cache dns-eas <realm-id> <cache_record_key>	Clear the external accounting server DNS cache
delete-tlskey-files	Deletes the `tlskey.log` file.
reset nsep-stats realms <realm-id> [<rvalue> | dialed-numbers]	Reset the NSEP statistics for a realm.
reset dns-eas	Reset the DNS statistics for the external accounting server.
reset stir header-mapping [<sti-server>]	Reset the header-mapping statistics for a specific STI server or for all STI servers.
show dns stats-eas [<realm> | <interface>]	Show the DNS statistics of all external accounting servers or just those on a specific realm or interface.
show dns cache-entry-eas <realm-id> <cache-record-key>	Show the DNS cache entries for an external accounting server by realm.
show mbcd realms <realm-id> detailed	Show detailed MBCD statistics for a specific realm.
show xcode dsp-resource <dsp-event-id>	The **show xcode dsp-resource** command now has a **dsp-event-id** option.
show xcode session-bitinfo <session-id>	The **show xcode session-bitinfo** command now has a **session-id** option.
show xcode session-byattr <attribute>	The **show xcode session-byattr** command now has a **attribute** option.
show xcode session-byid <session-id>	The **show xcode session-byid** command now has a **session-id** option.
show xcode session-byipp <ip-address> <port>	The **show xcode session-byipp** command now has a **ip-address** and **port** option.

New Commands	Description
show xcode session-config <session-id>	The **show xcode session-config** command now has a **session-id** option.
show nsep-stats realms <realm-id> [<rvalue> | dialed-numbers]	Show the NSEP statistics for a specific realm.
show accounting servers	Show the FQDN and connection details for all accounting servers per pool.
show sockets <process-name> [<options>]	Show socket information.
show transactions <process-name> [<options>]	Show transaction information.
show stir header-mapping [<sti-server>]	The **show stir** command has a new **header-mapping** option to display header mapping statistics for all STI servers or a particular STI server.
show tracker-profiles-running	Show the running memory tracker profiles.
show sipd redEntries [Objectid | RedType | className] [<options>]	Show entries from the EntryById table.
show platform nftables	Display kernel NF tables rules.
show version [boot | image]	The **show version** command as two new options.

Accounting Changes

The following information summarizes the accounting changes in the Oracle Communications Session Border Controller S-Cz9.2.0 release.

See the *Accounting Guide* for descriptions of each new AVP.

The following accounting AVPs have been added in this release:

- Stir-TN-Used-For-AS-VS-Request
- Stir-Div-Signed-Request
- Stir-Div-Verified-Request
- Stir-VS-Verstat
- Stir-VS-Reason
- Acme-FlowID-FS1-R
- Acme-FlowID-FS2-F
- Acme-FlowID-FS2-R
- Acme-FlowType-FS2-F
- Acme-FlowType-FS2-R

New Message Types

The SBC supports the Disconnect-Peer-Request and Disconnect-Peer-Answer messages.

New CDR

A new History-Info2 field has been added to the CDRs. See the *Accounting Guide* for more information.

SNMP/MIB Changes

The following information summarizes the SNMP MIB changes in the Oracle Communications Session Border Controller S-Cz9.2.0 release.

See the *MIB Guide* for a description of each MIB.

The following SNMP objects are included in this release. This list may not include objects included in other patches.

- apSmgmtLDAPServerCap / 1.3.6.1.4.1.9148.2.1.8.61
- apDiamAcctBufferUsageNotifyCap / 1.3.6.1.4.1.9148.2.1.17.7
- apSip503RespThresholdNotificationsGroupCap / 1.3.6.1.4.1.9148.2.1.21.16
- apSipSteeringPoolUtilNotificationsGroupCap / 1.3.6.1.4.1.9148.2.1.21.17
- apMSRPKPIMibCapabilities / 1.3.6.1.4.1.9148.2.2.3
- apMSRPKPIStatsCap / 1.3.6.1.4.1.9148.2.2.3.1
- apNSEPRealmKPIMibCapabilities / 1.3.6.1.4.1.9148.2.2.4
- apNSEPRealmKPIStatsCap / 1.3.6.1.4.1.9148.2.2.4.1
- apNSEPOutboundSessionMibCapabilities / 1.3.6.1.4.1.9148.2.2.5
- apSmgmtNSEPOutboundSession / 1.3.6.1.4.1.9148.2.2.5.1
- apNSEPStatsCurrentActiveSessionsOutbound / 1.3.6.1.4.1.9148.3.2.1.5.9
- apNSEPStatsTotalSessionsOutbound / 1.3.6.1.4.1.9148.3.2.1.5.10
- apNSEPStatsPeriodHighOutbound / 1.3.6.1.4.1.9148.3.2.1.5.11
- apSysMgmtNSEPOutboundStatsGroup / 1.3.6.1.4.1.9148.3.2.4.2.37
- apAcctMsgQueueLowerThreshold / 1.3.6.1.4.1.9148.3.13.1.2.1.11
- apAcctMsgQueueUpperThreshold / 1.3.6.1.4.1.9148.3.13.1.2.1.12
- apDiamACCTBufferUsageNotificationsGroup / 1.3.6.1.4.1.9148.3.13.1.3.2.5
- apSip503RespThresholdNotificationsGroup / 1.3.6.1.4.1.9148.3.15.3.2.5
- apSipSteeringPoolUtilNotificationGroups / 1.3.6.1.4.1.9148.3.15.3.2.6
- apSipSteeringPoolUtilNotificationsGroup / 1.3.6.1.4.1.9148.3.15.3.2.6.1
- apSip503RespThreshold / 1.3.6.1.4.1.9148.3.15.5
- apSip503RespThresholdNotifications / 1.3.6.1.4.1.9148.3.15.5.1
- apSip503RespThresholdNotificationsPrefix / 1.3.6.1.4.1.9148.3.15.5.1.0
- apSip503RespThresholdCrossedNotify / 1.3.6.1.4.1.9148.3.15.5.1.0.1
- apSip503RespThresholdObjects / 1.3.6.1.4.1.9148.3.15.5.1.1
- apSip503ConfiguredThreshold / 1.3.6.1.4.1.9148.3.15.5.1.1.1
- apSip503RespRate / 1.3.6.1.4.1.9148.3.15.5.1.1.2
- apSip503MethodName / 1.3.6.1.4.1.9148.3.15.5.1.1.3
- apSipSteeringPoolUtil / 1.3.6.1.4.1.9148.3.15.6
- apSipSteeringPoolUtilNotifications / 1.3.6.1.4.1.9148.3.15.6.1

- apSipSteeringPoolUtilNotificationsPrefix / 1.3.6.1.4.1.9148.3.15.6.1.0
- apSipSteeringPoolThresholdCrossedNotify / 1.3.6.1.4.1.9148.3.15.6.1.0.1
- apSipSteeringPoolUtilObjects / 1.3.6.1.4.1.9148.3.15.6.1.1
- apSipRealm / 1.3.6.1.4.1.9148.3.15.6.1.1.1
- apSipSteeringPoolThreshold / 1.3.6.1.4.1.9148.3.15.6.1.1.2
- apSipSteeringPoolUtilization / 1.3.6.1.4.1.9148.3.15.6.1.1.3
- apAppsMSRPKPIMIBObjects / 1.3.6.1.4.1.9148.3.16.1.2.5
- apAppsMSRPKPIRealmTable / 1.3.6.1.4.1.9148.3.16.1.2.5.1
- apAppsMSRPKPIRealmEntry / 1.3.6.1.4.1.9148.3.16.1.2.5.1.1
- apMSRPKPIRealmIndex / 1.3.6.1.4.1.9148.3.16.1.2.5.1.1.1
- apMSRPKPIRealmName / 1.3.6.1.4.1.9148.3.16.1.2.5.1.1.2
- apAppsMSRPKPIRealmStatsTable / 1.3.6.1.4.1.9148.3.16.1.2.5.2
- apAppsMSRPKPIRealmStatsEntry / 1.3.6.1.4.1.9148.3.16.1.2.5.2.1
- apMSRPKPIStatsRealmIndex / 1.3.6.1.4.1.9148.3.16.1.2.5.2.1.1
- apMSRPKPIRealmStatsCounterType / 1.3.6.1.4.1.9148.3.16.1.2.5.2.1.2
- apMSRPKPIRealmStatsType / 1.3.6.1.4.1.9148.3.16.1.2.5.2.1.3
- apMSRPKPIRealmStats / 1.3.6.1.4.1.9148.3.16.1.2.5.2.1.4
- apAppsMSRPKPISystemStatsTable / 1.3.6.1.4.1.9148.3.16.1.2.5.3
- apAppsMSRPKPISystemStatsEntry / 1.3.6.1.4.1.9148.3.16.1.2.5.3.1
- apMSRPKPISystemStatsCounterType / 1.3.6.1.4.1.9148.3.16.1.2.5.3.1.1
- apMSRPKPISystemStatsType / 1.3.6.1.4.1.9148.3.16.1.2.5.3.1.2
- apMSRPKPISystemStats / 1.3.6.1.4.1.9148.3.16.1.2.5.3.1.3
- apAppsNSEPRealmMIBObjects / 1.3.6.1.4.1.9148.3.16.1.2.6
- apAppsNSEPRealmTable / 1.3.6.1.4.1.9148.3.16.1.2.6.1
- apAppsNSEPRealmEntry / 1.3.6.1.4.1.9148.3.16.1.2.6.1.1
- apNSEPRealmIndex / 1.3.6.1.4.1.9148.3.16.1.2.6.1.1.1
- apNSEPRealmName / 1.3.6.1.4.1.9148.3.16.1.2.6.1.1.2
- apAppsNSEPRealmRvalueDNTable / 1.3.6.1.4.1.9148.3.16.1.2.6.2
- apAppsNSEPRealmRvalueDNEntry / 1.3.6.1.4.1.9148.3.16.1.2.6.2.1
- apNSEPRealmRvalueDNIndex / 1.3.6.1.4.1.9148.3.16.1.2.6.2.1.1
- apNSEPRvalueDNName / 1.3.6.1.4.1.9148.3.16.1.2.6.2.1.2
- apNSEPRealmRvalueDNStatsTable / 1.3.6.1.4.1.9148.3.16.1.2.6.3
- apAppsNSEPRealmRvalueDNStatsEntry / 1.3.6.1.4.1.9148.3.16.1.2.6.3.1
- apNSEPStatsRealmIndex / 1.3.6.1.4.1.9148.3.16.1.2.6.3.1.1
- apNSEPStatsRvalueDNIndex / 1.3.6.1.4.1.9148.3.16.1.2.6.3.1.2
- apNSEPRealmStatsType / 1.3.6.1.4.1.9148.3.16.1.2.6.3.1.3
- apNSEPRealmStats / 1.3.6.1.4.1.9148.3.16.1.2.6.3.1.4

- apAppsMSRPKPIRealmStatsGroup / 1.3.6.1.4.1.9148.3.16.3.1.10
- apAppsMSRPKPISystemStatsGroup / 1.3.6.1.4.1.9148.3.16.3.1.11
- apNSEPRealmStatsGroup / 1.3.6.1.4.1.9148.3.16.3.1.12

In addition, the following SNMP tables include new objects supporting the STIR/SHAKEN implementation:

- apAppsStirServerTable
- apAppsStirAgentStatsTable
- apAppsStirSipInterfaceStatsTable
- apAppsStirRealmStatsTable
- apAppsStirSystemStatsTable

The applicable MIB objects are nested to appear based on the individual STIR servers, Session Agents, SIP Interfaces, Realms, and system that you have configured on your system. Within those contexts, the applicable MIB objects are further nested in these tables based on count type, which the system identifies using OID prefix, including recent, total, and permax.

These objects include:

- asSentInviteswithShakenPASSportA
- asSentInviteswithShakenPASSportB
- asSentInviteswithShakenPASSportC
- asSentInviteswithdivPASSport
- vsReceivedInviteswithNoPASSport
- vsReceivedInviteswithShakenPASSport
- vsReceivedInviteswithDivPASSport
- vsSentInviteswithTNValidationPassed
- vsSentInviteswithTNValidationFailed
- vsSentInviteswithNoTNValidation

As an example, the full, MIB OID for the apAppsStirServerTable for recent INVITES received from server 6 within the verification context, and with no passport is:

- recent.vsReceivedInviteswithNoPASSport / 1.3.6.1.4.1.9148.3.16.1.2.4.2.1.4.6.1.17

New Traps

The following traps are added in this release:

- apAcctMsgQueueUpperThresholdTrap / 1.3.6.1.4.1.9148.3.13.1.2.2.0.7
- apAcctMsgQueueUpperThresholdClearTrap / 1.3.6.1.4.1.9148.3.13.1.2.2.0.8
- apSip503RespThresholdCrossedNotify / 1.3.6.1.4.1.9148.3.15.5.1.0.1
- apSipSteeringPoolThresholdCrossedNotify / 1.3.6.1.4.1.9148.3.15.6.1.0.1

Alarms

The following information summarizes the alarm changes in the Oracle Communications Session Border Controller S-Cz9.2.0 release.

Connectivity to the CCF by way of FQDN

The following alarms are added in this release:

- **Diameter Accounting Server lost connection**
- **Diameter Accounting Server Returned Error Result Code|<IP-address>:<port>-<error-response>**
- **Buffer Usage (x%) hit Upper Threshold Limit for Diameter Accounting buffer**

Session Agent Alarms

When **trigger-oos-alarm** is enabled, the following alarms may be raised when a session agent goes out of service.

- **One or more Session Agent's state changed from In-Service to OOS | SA Hostname: <hostname>, IP: <ip-address>**

Steering Pool Alarms

When the steering pool utilization is equal or greater than the configured threshold, the following alarm is raised:

- **Steering ports utilization for one or more realm is over configured threshold | <realm name> is at x%, configured threshold: y%.**

Service Unavailable Alarms

When number of 503 Service Unavailable responses crosses the configured threshold within the configured monitoring time, the following alarm is raised:

- **503 Service Unavailable response to <SIP request name> is x%, over configured threshold of y%**.

HDR

The following information summarizes the accounting changes in the Oracle Communications Session Border Controller S-Cz9.2.0 release.

See the *HDR Guide* for descriptions of each new historical data record fields.

The same 9 fields are added to the following HDR output groups:

- stir-stats
- stir-stats-session-agent
- stir-stats-sip-interface
- stir-stats-realm
- stir-stats-system

These fields include:

- AS Shaken Passport A
- AS Shaken Passport B
- AS Shaken Passport C
- AS DIV Passport
- VS Shaken Passport VS
- Div Passport
- VS TN-Validation-Passed
- VS TN-Validation-Failed
- VS No-TN-Validation

Errors and Warnings

The following errors and warnings are new in this release.

Error or Warning	Description
WARNING: tls-profile [x] contains the following weak cipher(s): TLS_AES_128_CCM_8_SHA256, etc	When **tls-version** is set to **compatibility**, the weak cipher TLS_AES_128_CCM_8_SHA256 will be sent along with other weak ciphers.
ERROR: sti-server [serverA] has reference to sti-header-mapping-ruleset [rulesetA] which does not exist	The **sti-header-mapping-ruleset** name parameter of an **sti-server** contains a ruleset name that does not exist.
ERROR: sti-config [configA] has reference to sti-header-mapping-ruleset [rulesetA] which does not exist	The **sti-header-mapping-ruleset** name parameter of an **sti-config** contains a ruleset name that does not exist.