Oracle® Communications Session Border Controller and Session Router

Release Notes

Release S-Cz10.1.0
G49668-02
April 2026

ORACLE

Oracle Communications Session Border Controller and Session Router Release Notes, Release S-Cz10.1.0

G49668-02

Contents

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 6350 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6350.
Acme Packet 6400 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6400.
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.
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.

Document Name	Document Description
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.

Revision History

The following table provides the revision history for this document.

Date	Description
April 2026	• Initial release.

1

Introduction to S-Cz10.1.0

The Oracle Communications Session Border Controller *Release Notes* provides the following information about the S-Cz10.1.0 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 on the following hardware platforms.

The S-Cz10.1.0 release of the SBC supports the following platforms:

- Acme Packet 3900
- Acme Packet 3950
- Acme Packet 4600
- Acme Packet 4900
- Acme Packet 6350 (Quad 10GbE NIU only)
- Acme Packet 6400

The S-Cz10.1.0 release of the Session Router supports the following platforms:

- Acme Packet 4600
- Acme Packet 4900
- Oracle Server X8-2
- Oracle Server X9-2

Release S-Cz10.1.0 is the last Session Router release that will support the Oracle Server X8-2.

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, have the same PCI Vendor ID and Device ID, and share the same network IO mode (SRIOV, PV, or PCI-PT).

Supported Hypervisors for Private Virtual Infrastructures

Oracle supports installation of the SBC on the following hypervisors:

- KVM (the following versions or later)
  - Linux kernel (5.14.0-162)
  - QEMU (6.1.1-3)
  - libvirt (7.10.0-2)
- VMware: vSphere ESXi (7.x 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, nnSCZ1010_HOT.tar.gz, and follow the OpenStack Heat Template instructions.

The nnSCZ1010_HOT.tar.gz file contains two files:

- nnSCZ1010_HOT_pike.tar
- nnSCZ1010_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.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
VM.Standard.E5. Flex-Small	4/8	4	8	6	Y	16
VM.Standard.E5. Flex-Medium	8/16	8	10	8	Y	32
VM.Standard.E5. Flex-Large	16/32	16	10	8	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 OCI VM.Optimized3.Flex shapes provide three launch options to select networking modes, always select Option 3, Hardware-assisted (SR-IOV), for the SBC.

> **Note**
>
> Although the VM.Optimized3.Flex OCI shape is flexible, allowing you to choose from 1-18 OCPUs and 1-256GB of memory, the virtual SBC 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 when the **use-sibling-core-datapath** attribute is disabled and DoS protection is enabled.

> **Note**
>
> The Subscriber-Aware Load Balancer is not supported on any c4 shape.

Instance Type	vNICs	RAM	vCPUs	Max Forwarding Cores (with DoS protection)	DoS Protection
c4.xlarge	4	7.5	4	1[1]	N[2]
c4.2xlarge	4	15	8	2	Y
c4.4xlarge	8	30	16	6	Y

Instance Type	vNICs	RAM	vCPUs	Max Forwarding Cores (with DoS protection)	DoS Protection
c5.xlarge	4	8	4	1	Y[3]
c5.2xlarge	4	16	8	2	Y
c5.4xlarge	8	32	16	6	Y
c5n.xlarge	4	10.5	4	1	Y[4]
c5n.2xlarge	4	21	8	2	Y
c5n.4xlarge	8	42	16	6	Y

1 2 forwarding cores if use-sibling-core-datapath is enabled and no DoS core is configured.

2 Enable use-sibling-core-datapath to support DoS protection. If a DoS core is configured, only 1 forwarding core can be used.

3 Only supported when use-sibling-core-datapath is enabled.

4 Only supported when use-sibling-core-datapath is enabled.

For the x4.xlarge instance, you can have:

- 2 forwarding cores, if use-sibling-core-datapath is enabled and no DoS core is configured
- 1 forwarding core, if use-sibling-core-datapath is enabled and a DoS core is configured
- 1 forwarding core and no DoS core, if use-sibling-core-datapath is disabled

For the c4.2xlarge instance, you can have:

- 6 forwarding cores, if use-sibling-core-datapath is enabled and no DoS core is configured
- 5 forwarding cores, if use-sibling-core-datapath is enabled and a DoS core is configured
- 3 forwarding cores, if use-sibling-core-datapath is disabled and no DoS core is configured
- 2 forwarding cores, if use-sibling-core-datapath is disabled and a DoS core is configured

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	Y
Standard_F8s	8	16	8	Y
Standard_F16s	8	32	16	Y

> **Note**
>
> The Subscriber-Aware Load Balancer is not supported on any Standard_F(x)s shape.

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

> **Note**
>
> The Subscriber-Aware Load Balancer is not supported on any Standard_F(x)s_v2 shape.

An Azure virtual SBC deployed with accelerated networking only supports a number of rx-queues that is a power of 2. When rebooting or redeploying, an Azure VM may be deployed on hardware with a different model of Mellanox as its physical NIC (MLX4 or MLX5).

Size types define architectural differences and cannot be changed after deployment. During deployment you choose a size for the SBC, 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 [1]
n2-standard-4	4	16	4	10	4
n2-standard-8	8	32	8	16	8
n2-standard-16	16	64	8	32	16

[1] Using virtIO or a custom driver, the VM is allocated 1 queue for each vCPU with a minimum of 1 queue and maximum of 32 queues.
Next, each NIC is assigned a fixed number of queues calculated by dividing the number of queues assigned to the VM by the number of NICs, then rounding down to the closest whole number.
For example, each NIC has five queues if a VM has 16 vCPUs and three NICs.
It is also possible to assign a custom queue count. To create a VM with specific queue counts for NICs, you use API/Terraform. There is no provision on the GCP console yet.

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 platforms support SMT and enable it by default; others support SMT but don't enable it by default; others support SMT only for certain machine shapes; and others don't support SMT. Check your platform documentation to determine its level of SMT support.

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 . 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:

- 24.11.1

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 Virtual Resources

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

- 4 vCPU Cores
- 8 GB RAM
- 28 GB hard disk (pre-formatted)
  The hard disk size should be twice the RAM plus 12 GB: (2 * RAM) + 12 GB.
- 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, have the same PCI Vendor ID and Device ID, and share the same network IO mode (SRIOV, PV, or PCI-PT).

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 X710 / XL710 / XXV710 Intel E810-XXV / E810-XXVDA4 / E810-CQDA	i40e i40en[1] iavf[2]	M	M
E810-XXVDA4 (at 10GB switch speeds)[3]	iavf [4]	M	NA
Mellanox Connect X-4 [5]	mlx5	M	M
Mellanox Connect X-5[6]	mlx5 [7][8]	M	NA
Mellanox ConnectX-6 Dx	mlx5_pci PMD	M/W	M/W

1 This driver is supported on VMware only. ESXi 7.0 deployments utilizing VLANs require the 1.14.1.0 version of this driver (or newer). ESXi 8.0 deployments utilizing VLANs require the 2.6.5.0 version of this driver (or newer).
2 iavf driver is support in SR-IOV n/w mode
3 Intel E810-XXVDA2, E810-XXVDA4, E810-XXVDA4T all use the same driver.
4 iavf driver is supported in SR-IOV n/w mode over KVM and VmWare
5 Not tested for media interfaces
6 KVM only
7 Device Part number: 7603662 Oracle Dual Port 25 Gb Ethernet Adapter, Mellanox (for factory installation)
8 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.

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
KVM (PV)	virtio	W/M
VMware (PV)	VMXNET3	W/M

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

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

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

CPU Core Resources for Private Virtual Infrastructures

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.

Session Router Recommendations

For release S-Cz10.1.0, Oracle recommends the following resources when operating the Session Router or Enterprise Session Router over Oracle servers.

Supported Platforms

The Session Router and Enterprise Session Router support the same Virtual Platforms as the SBC. Please see the Supported Private Virtual Infrastructures and Public Clouds section for these platform lists.

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: `nnSCZ1010.bz`
- Bootloader file: `nnSCZ1010.boot`

Virtual Platforms

This S-Cz10.1.0 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:

- `nnSCZ1010-img-vm_kvm.tgz`—Compressed image file including SBC VNF for KVM virtual machines, Oracle Cloud Infrastructure (OCI), AWS EC2, and GCP instances.
- `nnSCZ1010-img-vm_vmware.ova`—Open Virtualization Archive (.ova) distribution of the SBC VNF for ESXi virtual machines.
- `nnSCZ1010-img-vm_vhd.tgz`—Compressed image file including SBC for Hyper-V virtual machine on Windows and Azure, as well as the `legal.txt` file.

Each virtual machine package includes:

- Product software—Bootable image of the product allowing startup and operation as a virtual machine. Example formats include vmdk (for VMware) and qcow2 (for KVM).
- OVF File—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` (KVM only)—Licensing information, including the Oracle End-User license agreement (EULA) terms covering the use of this software, and third-party license notifications.

Additional image packages include:

- `nnSCZ1010_HOT.tar.gz`—The Heat Orchestration Templates used with OpenStack (Newton or Pike).
- `nnSCZ1010_tfStackBuilder.tar.gz`—The Terraform templates used to create an AWS AMI and for deployment via the OCI resource manager.

Oracle Platforms for Session Router and Enterprise Session Router

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

- Through USB: `nnSCZ1010-img-usb.exe`
- Through ILOM: `nnSCZ1010-img.iso`
- Bootloader file: `nnSCZ1010.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 set up the product. Once you have set up the product, you must set up 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, Enterprise SBC, and Session Router support the following in-service (hitless) upgrade and rollback paths:

- S-Cz9.2.0p13 (or higher) to S-Cz10.1.0
- S-Cz9.3.0p9/S-Cz9.3.0p11 (or higher) to S-Cz10.1.0

  > **Note**
  >
  > S-Cz9.3.0p10 is not a supported upgrade path.

- S-Cz10.0.0p5 (or higher) to S-Cz10.1.0

The SBC, Enterprise SBC, and Session Router support the following out-of-service upgrade and rollback paths:

- S-Cz9.0.0p12 to S-Cz10.1.0
- S-Cz9.1.0p14 to S-Cz10.1.0

The Subscriber-Aware Load Balancer supports the following in-service (hitless) upgrade and rollback paths:

- S-Cz9.3.0p9/S-Cz9.3.0p11 (or higher) to S-Cz10.1.0

> **Note**
>
> S-Cz9.3.0p10 is not a supported upgrade path.

- S-Cz10.0.0p5 to S-Cz10.1.0

> **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 Oracle Server X7-2 to Oracle Server X9-2.

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.

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.

Syslog Transport Protocol

SCZ10.1.0 introduces TLS as a transport protocol for syslog messages. If you downgrade from 10.1 to a previous release, the transport protocol for syslog messages is set to UDP.

HMR Regex Matching

An upgrade to Lua in S-Cz10.0.0 affects how the SBC adds headers on outgoing messages. When the header contains multiple values, the order of the values cannot be guaranteed. As a result, your regex patterns must not assume any specific order to the values of a header.

Certificates Signature Algorithm

If you previously created a certificate using a weak signature algorithm or message digest like MD5 or SHA1, you must create a new certificate using SHA256. Use **show security certificates** to view which signature algorithm is used.

Downgrade Caveat on Central Certificate Authority Store Feature

The central CA certificate store feature was added to S-Cz9.3.0p5. When downgrading from a version that supports this feature to one that does not, any CA-certificates that you imported from the certificate-bundle remain in the SBC along with their corresponding certificate-records. To remove these certificates from your system, you must manually delete each certificate-record from your configuration.

SSH Host Key Algorithms

The SBC uses `rsa-sha2-256` as the default host key algorithm. SSH clients that offer only a SHA1 hash algorithm, like `ssh-rsa`, are not supported; your SSH client must offer a SHA2 hash algorithm. If you receive a "no matching host key type found" error message, upgrade your SSH client to one that supports connecting to hosts with SHA2 host keys.

NPLI Sync During Upgrades

During an HA pair upgrade, when a switchover activates the standby which uses a newer image, the cached NPLI (Network Provided Location Information) will be deleted from the newly active SBC before it actively expires. If configured, the default-location-string will be sent in subsequent messages. This issue persists until both HA nodes use the new image.

TLS Secure Renegotiation

In release S-Cz9.3.0 and later, the SBC requires the use of TLS Secure Renegotiation as described in RFC 5746 in order to counter the prefix attack described in CVE-2009-3555. If the devices attempting a TLS connection to the SBC don’t support TLS Secure Renegotiation, the TLS handshake fails. Oracle recommends updating such devices to support TLS Secure Renegotiation.

SuppressAdditionalProvisional SPL Upgrade Caveat

If you are using the SuppressAdditionalProvisional SPL loaded on an SBC version prior to version S-Cz9.3.0, and are upgrading to S-Cz9.3.0 or later, remove this suppression SPL manually and reboot your system before you perform this upgrade. Instruction and explanation on removing an SPL is documented in the SBC Processing Language (SPL) Chapter of the SBC *Configuration Guide*.

Entitlement Caveat for MSRP B2BUA Sessions Entitlement

Before upgrading the Acme Packet 3900 platform to S-Cz9.3.0 or later, set your MSRP B2BUA Sessions entitlement on that system to zero. After the upgrade is complete, reset your MSRP B2BUA Sessions entitlements back to your desired value. That platform is not supporting this entitlement properly during upgrades.

Default TLS Version

- Releases prior to S-Cz9.2.0 do not support TLS1.3.
- Releases S-Cz9.3.0 and S-Cz10.0.0 do not support TLS 1.0 or TLS1.1.
- If you are downgrading from this release to a release prior to S-Cz9.2.0, set your `tls-version` to `compatibility`.

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.

Upgrading Transcoding Jitter Settings to S-Cz10.0.0 or later

Most customers should benefit from the dynamic adaptive feature, and require no intervention. However, if you have customized the previous **xcode-jitter-buffer-min** and **xcode-jitter-buffer-max** jitter buffer options settings, the SBC retains these settings in the new configurations. Specifically:

- **xcode-jitter-buffer-min**—mapped to **xcode-jitter-buffer-low-min** and **xcode-jitter-buffer-high-min**
- **xcode-jitter-buffer-max**—mapped to **xcode-jitter-buffer-low-max** and **xcode-jitter-buffer-high-max**

This mapping results in the same transcoding jitter buffer behavior performed in versions prior to S-Cz9.3.0. These behaviors do not make full use of the new adaptive feature. Also, the SBC performs this mapping during boot-up in a way that does not permanently alter your configuration.

For a proper long-term migration, remove any previous **xcode-jitter-buffer-min** and **xcode-jitter-buffer-max** jitter buffer options settings from your configuration prior to your upgrade. This allows the new adaptive features to take effect.

If needed, you can then modify the new options settings from their default values. Oracle recommends, however, that you use the adaptive transcoding jitter buffer feature with the default settings, and only change those settings under the direction of Oracle support.

Connection Failures with SSH/SFTP Clients

If you upgrade and your older SSH or SFTP client stops working, check that the client supports the minimum 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 SSH client.

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
Certificate Management Protocol (CMP)	boolean
IMS-AKA Endpoints	Integer
IPSec Trunking Sessions	Integer
IPv4 - IPv6 Interworking	boolean
IWF (SIP-H323)	boolean
Load Balancing	boolean
Policy Server	boolean
Quality of Service	boolean
Routing	boolean
Session Capacity	integer
SIPREC Session Recording	boolean
SRTP Sessions	Integer
STIR/SHAKEN Client	boolean
Transcode Codec AMRWB	boolean
Transcode Codec AMRWB Capacity	Integer
Transcode Codec EVS	boolean
Transcode Codec EVS Capacity	Integer
Transcode Codec OPUS	boolean
Transcode Codec OPUS Capacity	Integer
Transcode Codec SILK	boolean
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 Session Router you enable with the **setup entitlements** command. When setting up an Session Router, you choose between either the Session Stateful or the Transaction Stateful Session Routers. The Enterprise Session Router entitlements are the same.

This first Session Router 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
Certificate Management Protocol (CMP)	Enabled or Disabled
Data Integrity (FIPS 140-3)	Enabled or Disabled
IPSec Trunking Sessions	Number of sessions

This second Session Router 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
Certificate Management Protocol (CMP)	Enabled or Disabled
Data Integrity (FIPS 140-3)	Enabled or Disabled
Load Balancing	Enabled or Disabled

Encryption for Virtual SBC

You must enable encryption for virtual 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 From Previous Releases

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

System Capacities

System capacities vary across the platforms that support the SBC. Use the **show platform limits** command to query your system's capacities.

Virtual platforms include the following limitations.

SIP Interface and Realm Limits

On virtual platforms, the number of realms and SIP interfaces is limited by the amount of VM memory. You can configure a maximum of 1500 realms and SIP interfaces for every 1GB of system memory.

Static Trusted and Untrusted ACL Limits

Hardware and virtual platforms support a maximum of 1024 static ACL entries that contain IP address ranges (such as /8, /16, or /24).

On virtual platforms, the number of static ACL entries that contain exact IP addresses is limited by the amount of VM 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.

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 and the Acme Packet 6400 do not support 40 and 60 packetization times for the EVS codec.	• AMR • AMR-WB • CN • EVRC • EVRC0 • EVRC1 • EVRCB • EVRCB0 • EVRCB1 • EVS[1] • G711AOMD • G711FB • G711OFD • G711UOMD • 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

Platform	Supported Codecs (by way of codec-policy in the add-on-egress parameter)
• Virtual Platforms (with 1+ transcoding core)	• AMR • AMR-WB • CN • EVS • G711AOMD • G711FB • G711OFD • G711UOMD • G722 • G723 • G726-16 • G726-24 • G726-32 • G726-40 • G726 • G729A • G729 • iLBC • OFDFB • opus • PCMA • PCMU • SILK • T.38 • T.38OFD[2] • telephone-event[3] 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.

2 *** These codecs require Fax Tone Detection.**

3 **A telephone-event requires DTMF tone generator and detector.**

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.

Session Border Controller

This release of the Session Border Controller interoperates with the following product releases:

- Session Delivery Manager: 9.0.3.0.1, 9.0.4, 9.0.4.0.1 and later
- Oracle Session Delivery Manager Cloud: 26 and later
- Oracle Communications Operations Monitor: 6.0 and 6.1
- Subscribe-Aware Load Balancer: 9.3.0, 10.0.0, and 10.1.0
- Session Router: 9.2.0, 9.3.0, 10.0.0, 10.1.0

> **Note**
>
> To manage S-Cz10.1.0 patches in conjunction with Oracle's Session Delivery Manager, review the build notes to determine if an XSD file is required and review the readme file in the XSD file. XSD files may work with older SDM releases, though it is not guaranteed.

When acting as an A-SBC, this release of the SBC can interoperate with T-SBCs running the following versions:

- S-Cz9.2.0
- S-Cz9.3.0
- S-Cz10.0.0
- S-Cz10.1.0

When acting as a T-SBC, this release of the SBC can interoperate with A-SBCs running the following versions:

- S-Cz9.2.0
- S-Cz9.3.0
- S-Cz10.0.0
- S-Cz10.1.0

Session Router

This release of the Session Router interoperates with the following product releases:

- Session Delivery Manager: 9.0.3.0.1, 9.0.4, 9.0.4.0.1 and later
- Oracle Session Delivery Manager Cloud: 26 and later
- Oracle Communications Operations Monitor: 6.0 and 6.1

The Session Delivery Manager offers only configuration support using XSD.

Subscriber-Aware Load Balancer

This release of the Subscriber-Aware Load Balancer interoperates with the following product releases:

- Session Delivery Manager: 9.0.3.0.1, 9.0.4, 9.0.4.0.1 and later
- Oracle Session Delivery Manager Cloud: 26 and later
- Session Border Controller: S-Cz9.3.0, S-Cz10.0.0, and S-Cz10.1.0 on the Acme Packet 4600, 4900, 6350, and 6400 platforms, and for virtual deployments.
- Enterprise Session Border Controller: S-Cz9.3.0, S-Cz10.0.0, and S-Cz10.1.0 on the Acme Packet 4600, 4900, 6350, and 6400 platforms, and for virtual deployments.

Cipher Updates

Note the changes to the TLS ciphers and IKE ciphers.

TLS Cipher Updates

The following ciphers may be selected for the **cipher-list** attribute in the **tls-profile** configuration element:

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_AES_128_CCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256
- 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

In addition to these options, you may select **DEFAULT**, which includes all of the ciphers in this list.

IKE Cipher Updates

In the context of IKE negotiations, the SBC offers the following ciphers with key lengths of 128, 192, and 256:

- ENCR-AES-CCM_12
- ENCR_AES-CCM_8
- ENCR-AES-CCM_16
- ENCR_AES_CBC
- ENCR_AES_CTR

Documentation Changes

The following information describes structural changes to the documentation for the S-Cz10.1.0 release.

Updates to SIP REFER Method Call Transfer Topics

The documentation for the SIP REFER method in the SIP Signaling Services chapter of the *SBC Configuration Guide* has been condensed. The content from the previous REFER-Initiated Call Transfer and 180 & 100 NOTIFY in REFER Call Transfers topics has been integrated into the SIP REFER Method Call Transfer topic.

A single SIP REFER Method Configuration topic now includes all three options for **refer-call-transfer**, the **dyn-refer-term** and **refer-notify-provisional** parameters, and the policy lookup configuration for source routing.

This was done to remove redundancy and now covers related concepts in a single topic and related configurations in a single procedure.

Updates to Secure Real-Time Transport Protocol Topics

The Secure Real-Time Transport Protocol and Secure Real-Time Transport Protocol (SRTP) for Software topics in the Security chapter of the *SBC Configuration Guide* has been condensed. The content was redundant and has been combined into a single topic.

Updates to the Changing the STI-VS Trigger Topic

Previously, when you enabled **man-compliance**, STI-VS processing automatically happened after checking for session constraints. Now, the new **sti-vs-post-check** option lets you control whether STI-VS processing happens before or after checking for session constraints.

The Changing the STI-VS Trigger Topic topic in the STIR/SHAKEN Client chapter of the *SBC Configuration Guide* has been updated to reflect this.

Removal of the ssh-password Topic

The **ssh-password** topic has been removed from the *SBC ACLI Reference Guide*. This command was deprecated and replaced with the **local-accounts** command in a previous release.

Behavioral Changes

The following information describes behavioral changes to the Oracle Communications Session Border Controller (SBC) for version S-Cz10.1.0.

Patches Included in This Release

The S-Cz10.1.0 release includes defect fixes from neighboring patch releases.

- S-Cz9.2.0p13
- S-Cz9.3.0p10
- S-Cz10.0.0p5

Supported SPL Engines

The S-Cz10.1.0 release supports the following SPL engine versions:

- C4.0.0 and later

Release S-Cz10.0.0 and later use sipShield v1.11. If downgrading to a previous software release, also downgrade sipShield to version 1.9.

2

New Features

The S-Cz10.1.0 release of the Oracle Communications Session Border Controller (SBC) software supports the following new features.

Certificate Automation

You can enable the SBC to perform key X.509 certificate related tasks automatically, including certificate renewals. These functions, based on the Certificate Management Protocol (CMP) defined within RFC 4210 and RFC 4211, make the SBC a CMP client, which interacts with a CMP server managed by a Certificate Authority (CA).

This feature requires the **Certificate Management Protocol (CMP)** entitlement.

See the Certificate Automation topic in the Security chapter of the *Configuration Guide* for more information.

Hiding Session Updates

You can configure the SBC to simplify call flows by hiding session updates that do not impact the ongoing call flow. Instead of sharing renegotiations with the opposite leg, the SBC responds locally with 200 OK for reINVITE and UPDATE renegotiations. This also ensures that SDP versions and sequence numbers (CSeq) are handled properly.

You configure this on the **hsu-policy** configuration element on the **session-router**, then apply **hsu-policy** to an interface, realm, or session agent.

See the Hiding Session Updates topic in the SIP Signaling Services chapter of the *Configuration Guide* for more information.

Continuing Calls in Failed REFER Call Transfers when Advanced Media Termination Clients send Music on Hold

In scenarios where Advanced Media Termination clients (such as Microsoft Teams) sending music on hold when referring calls, you can now configure whether the SBC ends the original call automatically when the REFER transfer fails, or lets it continue.

See the Continuing Calls in Failed REFER Call Transfers topic in the SIP Signaling Services chapter of the *Configuration Guide* for more information.

Custom Diameter ACR AVPs for SIP

When using diameter accounting, you can populate reserved ACR AVPs for SIP calls with SIP headers by using header manipulation rules (HMR). Previously, you could only use HMR with VSAs in RADIUS accounting.

See the Custom Diameter ACR AVPs for SIP topic in the Diameter Accounting chapter of the *Accounting Guide* for more information.

STIR/SHAKEN Client Updates

The STIR/SHAKEN client has been enhanced as follows:

- In ATIS deployments, you can configure a list of scenarios for which to bypass STI-AS requests and, optionally, configure a static token to use for bypassed requests.

- You can reject calls based on the verstat and reasonCode in the STI-VS server response for 200 OK responses in 3GPP deployments. This builds on the existing call rejection functionality.
- You can configure the following for the STI server heartbeat mechanism:
  - You can now configure the SBC start performing heartbeat checks as soon as the STI server is configured.
  - The heartbeat check can include a dummy identity header.
  - The SBC can verify if the response to the heartbeat check contains valid JSON and specific reason codes before adding the server to the rotation.
- You can see new statistics for calls that did not trigger STI-AS/VS requests, calls that did but received no response, and calls that bypasses STI-AS/VS.
- You can monitor CPU usage for the curld process by using the **show processes** command.

See the STIR/SHAKEN Client chapter of the *Configuration Guide* for more information about these enhancements.

SAN/CN Validation for TLS SIP Calls

You can now configure the SBC to validate the Subject Alternative Name (SAN) and Common Name (CN) from an incoming TLS certificate against a session agent during the TLS handshake, before SIP data is exchanged, in compliance with RFC 5922, sections 7.3 and 7.4.

See the SAN/CN Validation topic in the Security chapter of the *Configuration Guide* for more information.

Diameter Manipulation Rule Enhancements

You can now use diameter manipulation rules to copy AVPs at different levels and within different grouped AVPs. Previously, you could only act on AVPs at the same level within the same grouped AVP.

See the Manipulating Grouped AVPs topic in the External Policy Servers chapter of the *Configuration Guide* for more information.

New Number-Portability-Routing-Information AVP

A new AVP, Number-Portability-Routing-Information (2024), has been introduced. This AVP contains the routing number (rn) received from a mobile number portability (MNP) request and is grouped in the IMS-Information group AVP.

See the Including Number Portability Routing Information in ACRs and CDRs topic in the Diameter Accounting chapter of the *Accounting Guide*.

CDR Updates for Modem Tone Detection

When modem tone detection is configured and modem tones are detected on a call, the CDR now logs the name, family, and direction of modem tones detected on the call.

See the Accounting for Modem Tone Detection topic in the Transcoding chapter of the *Configuration Guide* and *Accounting Guide* for more information.

Real Time Configuration Support for SIPREC

You no longer need to reboot the SBC to apply SIPREC configurations on the **session-recording-server** configuration element. This helps prevent service disruption when enabling

SIPREC on active networks. It is also helpful in HA environments, where you previously had to reboot both standby and active node to apply the configuration.

See the Configuring SIPREC topic in the Selective Call Recording SIPREC chapter of the *Call Monitoring Guide* for more information about configuring SIPREC.

New Commands for vSBC, vSLB, and PNF Included in show support-info

The **show support-info** command now includes additional commands to support virtual SBCs, virtual Subscriber-Aware Load Balancers, and PNF platforms.

See the System Support Information for Troubleshooting topic in the Fault Management chapter of the *Maintenance and Troubleshooting Guide* for a list of all commands included in **show support-info**.

New Argument for backup-config

You can now use the **all** argument with the **backup-config** command to include files for LRT, media playback, fraud protection, SBC Processing Language, and Peak license data (in addition to all other backed up files).

The documentation has also been updated to include the **saved** argument, and to specify which arguments the **standard** and **non-standard** options apply to.

See the backup-config topic in the *ACLI Reference Guide* for information about the specific directories included in the backup with this new argument.

TLS for Syslog

You can now encrypt syslog messages with TLS as they flow across your network. In syslog-servers configuration element, set the **transport-protocol** attribute to TLS and set the **tls-profile** attribute to the name of the TLS profile you want to use.

System Resource Monitoring Enhancements

You can now use the Resource Monitoring feature to monitor utilization for additional resources:

- Platform-level CPU usage and core memory utilization
- Application-level CPU usage (for SIPD, MBCD, ATCPD)
- Application-level file descriptor (FD) usage
- PAC buffer usage

New statistics, alarms, and MIBs have been added to support these new resources.

See the System Resource Monitoring topic in the System Configuration chapter of the *Configuration Guide* and the Resource Monitor MIBs section of the Enterprise SNMP GET Requests chapter of the *MIB Guide* for more information.

3
Interface Changes

The following topics summarize ACLI, SNMP, HDR, Alarms, Accounting, and Error/Warning changes for S-Cz10.1.0. 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-Cz10.1.0 release.

Modified Element	Description
system, and then **system-config**, and then **schedule-backup**, and then **config-backup** , and then **push-receiver**	The default value for the **address** attribute is now empty instead of 0.0.0.0.
security, and then **certificate-record**, and then **cmp-profile**	This new attribute is available if you have installed a CMP license.
media-manager, and then **codec-policy**	Adds a new attribute **tone-detection-xcode-only**
media-manager, and then **codec-policy**, and then **add-codecs-on-egress**	Adds new values: G711AOMD, G711UOMD
media-manager, and then **codec-policy**, and then **tone-detection**	Adds new values: modem-ans, modem-orig
system, and then **system-config**, and then **collect**, and then **group-settings**, and then **group-name**	Adds new value **sip-invites-detail**.
system, and then **system-config** , and then **comm-monitor**, and then **monitor-collector**	The default value for the **address** attribute is now empty instead of 0.0.0.0.
system, and then **system-config** , and then **comm-monitor**	Adds the new attribute **http-enable**.
system, and then **system-config** , and then **comm-monitor**, and then **filter-profile**	Adds the new attribute **session-agents**.
system, and then **system-config** , and then **comm-monitor**, and then **filter-profile**, and then **type**	Adds the new values **HTTP-STIR**.
session-router, and then **diameter-manipulation**, and then **diameter-manip-rules**	Adds new attribute **avp-path**.
session-router, and then **http-profile**, and then **tcp-conn-idle-max-age**	This attribute's new default value is 118.
security, and then **ike**, and then **ike-config**, and then **ike-version**	When FIPS is enabled, this value is always set to 2.
security, and then **ike**, and then **ike-interface**, and then **ike-version**	When FIPS is enabled, this value is always set to 2.
security, and then **ike**, and then **ike-sainfo**, and then **security-protocol**	When FIPS is enabled, this value is always set to esp-auth.

Modified Element	Description
security, and then **ims-aka-profile**, and then **auth-alg-list**	Adds new values: • aes-gmac • hmac-sha2-512-256 • hmac-sha2-256-128 • null
security, and then **ims-aka-profile**, and then **encr-alg-list**	Adds new value aes-gcm.
session-router, and then **lbp-config**	Adds new attribute **vlan-based-routing**.
session-router, and then **media-profile**	The attributes **average-rate-limit** , **peak-rate-limit**, and **max-burst-size** all support values from 0 to 125000000 on supported platforms.
media-manager, and then **msrp-config**	This element is not supported when FIPS is enabled.
session-router, and then **net-management-control**	Adds the attribute **notify-on-emergency**.
media-manager, and then **realm-config**	Adds the attributes **default-teams-realm**, **refer-fail-resume**, **hsu-policy**, and **emergency-notify-for-tpm**
security, and then **security-config**, and then **local-cert-exp-warn-period**	The default value is now 30.
session-router, and then **session-agent**	Adds the following attributes: **reroute-servers**, **hsu-policy**, **session-recording-server**, **session-recording-required**, **sti-as**, **sti-vs**, **sti-orig-id**, **sti-attest**, and **sti-signaling-attest**
session-router, and then **sip-config**	Adds new attributes: **reroute-try-threshold-value**, **retry-after-enhancement**, **response-code-and-phrase-config-name**
session-router, and then **sip-interface**	Adds attribute **hsu-policy**.
session-router, and then **sti-config**	Adds the attributes **sti-static-bypass-token** and **sti-bypass-token-scenarios**
session-router, and then **sti-heartbeat-config**	Adds the attributes **sti-identity**, **sti-json-mandate**, **mode**, and **sti-in-service-response-code**.
system, and then **system-config**, and then **syslog-servers**	Adds attributes **transport-protocol** and **tls-profile**
system, and then **system-config**	Removes attribute **http-clearDead-conn-timer** and **log-curl-tls-key**. Adds attributes **fault-recovery**, , **domain-validation**, **gui-audit-trail**, and **secure-certificate-mode**
security, and then **tls-profile**	Adds the attributes **global-trusted-ca-lists** and **domain-validation**.

ACLI Command Changes

The following table summarizes the ACLI command changes in the Oracle Communications Session Border Controller S-Cz10.1.0 release.

This table lists and describes changes to ACLI commands that are available in the S-Cz10.1.0 release.

Modified Commands	Description
global-trusted-ca	This command is new in this release.

Modified Commands	Description
clear-cache	Adds a new argument **dns-cmp**.
backup-config [name]	Adds a new argument **all**.
request collection [start | stop]	Adds a new argument **sip-invites-detail**.
reset	Adds new arguments: **reroute-stats** and **dns-cmp**.
reset sipd	Adds new argument **hsu**.
cmp-keyupdate-request <record-name>	This command is new in this release.
delete-cmp-tlskey-file	This command is new in this release.
show ccd sds <id>	Adds a new argument **tunnels**.
show ccd sds all	Adds a new argument **<size>**.
show ccd rebalance	Adds a new argument **stats**.
show dns	Adds new arguments: **stats-cmp** and **cache-entry-cmp**.
show processes	Adds new arguments: **certd** and **tCurId**
show security certificates	Adds new arguments: **cmp** and **list-names**.
show queues	Adds new argument **certd**.
show stir	Adds a new argument **status**.
show	Adds a new argument **reroute**.
show sipd	Adds a new argument **hsu**.

Accounting Changes

The following information summarizes the accounting changes in the Oracle Communications Session Border Controller S-Cz10.1.0 release.

See the Accounting Guide for descriptions of each new AVP.

The following accounting AVPs have been added:

- Acme-P-VSA-200 through Acme-P-VSA-230
- Acme-Transcoding-Occurred
- Acme-Transrating-Occurred
- Acme-DTMFIW-Occurred
- Acme-FAXIW-Occurred
- Acme-CNIW-Occurred
- Acme-RTCPGen-Occurred
- Acme-T140Baudot-Relay
- Acme-VBDTone-Detected
- Acme-Calling-Jitter-Buffer-Pkt-Loss
- Acme-Called-Jitter-Buffer-Pkt-Loss
- Acme-Calling-Jitter-Buffer-Reset-Count
- Acme-Called-Jitter-Buffer-Reset-Count
- Number-Portability-Routing-Information
- Stir-AS-Bypass-Token

SNMP/MIB Changes

The following information summarizes the SNMP MIB changes in the Oracle Communications Session Border Controller S-Cz10.1.0 release.

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

MIBs

The following new MIBs are added in this release:

- apAppsCurlCPUUsageStatsTable / 1.3.6.1.4.1.9148.3.16.1.2.4.10
- apRmPacBufferPoolUtil / 1.3.6.1.4.1.9148.3.22.2.10
- apRmApplicationFdUtil / 1.3.6.1.4.1.9148.3.22.2.11
- rpRmCpuUtil / 1.3.6.1.4.1.9148.3.22.2.12
- apRmDpwdCpuUtil / 1.3.6.1.4.1.9148.3.22.2.13
- apRmDpwdMemUtil / 1.3.6.1.4.1.9148.3.22.2.14
- apSecurityCMPServerMIBObjects / 1.3.6.1.4.1.9148.3.9.1.16.3.1.2
- apSecurityCmpRealmMIBObjects / 1.3.6.1.4.1.9148.3.9.1.17.2.1.2
- apSecurityCmpMessageFailureCause / 1.3.6.1.4.1.9148.3.9.2.46
- apSecurityCmpCertificateEnrollmentFailureNotification / 1.3.6.1.4.1.9148.3.9.3.12.0.1

Alarms

The following information summarizes the alarm changes in the Oracle Communications Session Border Controller S-Cz10.1.0 release.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
APP_ALARM_SYSLOG_CONNECTION_FAIL	327769	MAJOR	The syslog server got disconnected.	Syslog server 10.0.0.1:514 got disconnected.	Ensure the SBC can access the syslog server, and that syslog is running on the server.	NA
PAC_BUFFER_COMMON_OVER_THRESHOLD	131435	MINOR MAJOR CRITICAL	High common PAC buffer.	Resource monitoring module raising alarm - Resource task id = TASK_ID, threshold = 80%, current value = 82%, processName = theap, resourceName = PAC_BUFFER_COMMON	Ensure calls are managed in a way that resource usage stays within the specified threshold	apRmResourcesGroupTrap

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
PAC_BUFFER_NET_G_OVER_THRESHOLD	131436	MINOR MAJOR CRITICAL	High netlink global PAC buffer.	Resource monitoring module raising alarm - Resource task id = TASK_ID, threshold = 80%, current value = 82%,processName = theap, resourceName = PAC_BUFFER_NET_G	Ensure calls are managed in a way that resource usage stays within the specified threshold	apRmResourcesGroupTrap
PAC_BUFFER_NET_P_OVER_THRESHOLD	131437	MINOR MAJOR CRITICAL	High netlink private PAC buffer.	Resource monitoring module raising alarm - Resource task id = TASK_ID, threshold = 80%, current value = 82%,processName = theap, resourceName = PAC_BUFFER_NET_p	Ensure calls are managed in a way that resource usage stays within the specified threshold	apRmResourcesGroupTrap
DPWD_MON_CPU_OVER_THRESHOLD	131696, incremented by 1 for each subsequent resource	MINOR MAJOR CRITICAL	High platform-level CPU usage	Resource monitoring module raising alarm - Resource task id = TASK_ID, threshold = 80%, current value = 82%,processName = tDpwdMonit, resourceName = DPWD_MON_CPU	Ensure calls are managed in a way that resource usage stays within the specified threshold	apRmResourcesGroupTrap

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
DPWD_MON_MEMORY_OVER_THRESHOLD	131728, incremented by 1 for each subsequent resource	MINOR MAJOR CRITICAL	High platform-level memory usage	Resource monitoring module raising alarm - Resource task id = TASK_ID, threshold = 80%, current value = 82%,processName = tDpwdMonit, resourceName = DPWD_MON_MEMORY	Ensure calls are managed in a way that resource usage stays within the specified threshold	apRmResourcesGroupTrap
CPU_OVER_THRESHOLD	131438, incremented by 1 for each subsequent resource	MINOR MAJOR CRITICAL	High application-level CPU usage	Resource monitoring module raising alarm - Resource task id = TASK_ID, threshold = 80%, current value = 82%,processName = sipd1, resourceName = CPU	Ensure calls are managed in a way that resource usage stays within the specified threshold	apRmResourcesGroupTrap
APPLICATION_FD_OVER_THRESHOLD	131856	MINOR MAJOR CRITICAL	High application FD usage	Resource monitoring module raising alarm - Resource task id = TASK_ID, threshold = 80%, current value = 82%,processName = sipd1 , resourceName = APPLICATION_FD	Ensure calls are managed in a way that resource usage stays within the specified threshold	apRmResourcesGroupTrap

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
APP_ALARM_CERT_EXPIRED	327730	CRITICAL	A certificate has expired.	Certificate: tempCert expired on Jan 30 20:58:29 2019 GMT, done	If the certificate is managed manually, take action to update the applicable record with a new, valid certificate. This alarm will not appear for certificates managed by CMP.	apSecurityCertExpiredNotification (1.3.6.1.4.1.9148.3.9.3.6.0.1)
APP_ALARM_CERT_EXPIRE_SOON	327731	WARNING	A certificate will expire in more than fifteen days, but less than or equal to the number of days in **local-cert-exp-warn-period**.	Certificate: tempCert expiring on Jan 30 20:58:29 2019 GMT,done	If the certificate that is expiring is managed by CMP, no action is necessary. If the certificate is managed manually, take action to update the applicable record with a new, valid certificate.	apSecurityCertExpireSoonNotification (1.3.6.1.4.1.9148.3.9.3.6.0.2)
APP_ALARM_CERT_EXPIRE_SOON_1	327761	MINOR	A certificate will expire in fifteen days.	Certificate: tempCert expiring on Jan 30 20:58:29 2019 GMT,done	If the certificate that is expiring is managed by CMP, no action is necessary. If the certificate is managed manually, take action to update the applicable record with a new, valid certificate.	apSecurityCertExpireSoonNotification (1.3.6.1.4.1.9148.3.9.3.6.0.2)
APP_ALARM_CERT_EXPIRE_SOON_2	327762	MAJOR	A certificate will expire in seven days.	Certificate: tempCert expiring on Jan 30 20:58:29 2019 GMT,done	If the certificate that is expiring is managed by CMP, no action is necessary. If the certificate is managed manually, take action to update the applicable record with a new, valid certificate.	apSecurityCertExpireSoonNotification (1.3.6.1.4.1.9148.3.9.3.6.0.2)

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
APP_ALARM_CERT_EXPIRE_SOON_3	327763	CRITICAL	A certificate will expire in one day.	Certificate: tempCert expiring on Jan 30 20:58:29 2019 GMT,done	If the certificate that is expiring is managed by CMP, no action is necessary. If the certificate is managed manually, take action to update the applicable record with a new, valid certificate.	apSecurityCertExpireSoonNotification (1.3.6.1.4.1.9148.3.9.3.6.0.2)

HDR

The following information summarizes the accounting changes in the Oracle Communications Session Border Controller S-Cz10.1.0 release.

New HDR Objects for STIR/SHAKEN

- AS Queries Not Triggered: Number of calls not sent to the STI-AS server for various reasons (server unreachable, overloaded internal services, exceeded admission control, missing or invalid TN, bypass scenarios, missing attestation header, and so on.)
- VS Queries Not Triggered: Number of calls not sent to the STI-VS server for various reasons (server unreachable, overloaded internal services, exceeded admission control, missing or invalid TN, bypass scenarios, missing identity header, and so on.)
- AS Queries Triggered But No Responses: Number of queries made to the STI-AS server that timed out with no response
- VS Queries Triggered But No Responses: Number of queries made to the STI-VS server that timed out with no response
- AS Bypass Token Counter: Number of INVITES sent with the configured bypass token.

These objects appear in each of the following HDR groups:

- ACLI-Group_stir-stats
- ACLI_Group_stir-stats-session-agent
- ACLI_Group_stir-stats-sip-interface
- ACLI_Group_stir-stats-realm
- ACLI_Group_stir-stats-system

Errors and Warnings

IMS AKA Profile

In the **ims-aka-profile** element, when **encr-alg-list** is set to aes-gcm, then **auth-alg-list** must be set to **null**. When **auth-alg-list** is set to aes-gmac, then **encr-alg-list** must be set to **null**.

If you attempt to save some other configuration, warnings are displayed with the **done** command or the **verify-config** command.