Oracle® Communications Session Border Controller and Session Router

Release Notes

Release S-Cz10.0.0
G25344-03
June 2025

ORACLE

Oracle Communications Session Border Controller and Session Router Release Notes, Release S-Cz10.0.0

G25344-03

Contents

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.

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	Description
March 2025	• Initial release.
April 2025	• Adds Account Servers over IPv6 to New Features • Adds upgrade/downgrade caveat about session translation • Adds 6400
June 2025	• Adds Azure rx-queues limitation. • Adds DoS limitations to AWS shapes. • Adds New Features for S-Cz10.0.0p2.

1

Introduction to S-Cz10.0.0

The Oracle Communications Session Border Controller *Release Notes* provides the following information about the S-Cz10.0.0 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-Cz10.0.0 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-Cz10.0.0 release of the Session Router supports the following platforms:

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

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 (4.1.12-124)
  - QEMU (2.9.0_16)
  - libvirt (3.9.0_14)
- VMware: vSphere ESXi (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, nnSCZ1000p1_HOT.tar.gz, and follow the OpenStack Heat Template instructions.

The nnSCZ1000p1_HOT.tar.gz file contains two files:

- nnSCZ1000p1_HOT_pike.tar
- nnSCZ1000p1_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

Shape	OCPUs/ VCPUs	vNICs	Tx/Rx Queues	Max Forwarding Cores	DoS Protection	Memory
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 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
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 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:

- 23.11

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
- (2*Memory +12GB) 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, 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	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

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.

> **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

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

For release S-Cz10.0.0, 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: `nnSCZ1000p1.bz`
- Bootloader file: `nnSCZ1000p1.boot`

Virtual Platforms

This S-Cz10.0.0 release includes distributions suited for deployment over hypervisors. Download packages contain virtual machine templates for a range of virtual architectures. Use the following distributions to the Session Border Controller as a virtual machine:

- `nnSCZ1000p1-img-vm_kvm.tgz`—Compressed image file including SBC VNF for KVM virtual machines, Oracle Cloud Infrastructure (OCI), AWS EC2, and GCP instances.
- `nnSCZ1000p1-img-vm_vmware.ova`—Open Virtualization Archive (.ova) distribution of the SBC VNF for ESXi virtual machines.
- `nnSCZ1000p1-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:

- `nnSCZ1000p1_HOT.tar.gz`—The Heat Orchestration Templates used with OpenStack (Newton or Pike).
- `nnSCZ1000p1_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: `nnSCZ1000p1-img-usb.exe`
- Through ILOM: `nnSCZ1000p1-img.iso`
- Bootloader file: `nnSCZ1000p1.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-Cz9.1.0p14 (or higher) to S-Cz10.0.0
- S-Cz9.2.0p11 (or higher) to S-Cz10.0.0

- S-Cz9.3.0p5 (or higher) to S-Cz10.0.0

In addition, the SBC and Session Router support the following out-of-service upgrade and rollback paths (For the SBC, this support extends to all platforms except for the Acme Packet 3950 and 4900):

- S-Cz8.4.0p13 to S-Cz10.0.0
- S-Cz9.0.0p12 to S-Cz10.0.0

In addition, the Enterprise SBC supports the following out-of-service upgrade and rollback paths (For the Enterprise SBC, this support extends to all platforms except for the Acme Packet 3950 and 4900):

- S-Cz8.3.0m1p14 to S-Cz10.0.0
- S-Cz9.0.0p12 to S-Cz10.0.0

> **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.

Acme Packet 3900 Platform

When you upgrade software, if the session-capacity is configured to a value greater than the 8000 supported sessions on the AP3900, an upgrade from 8.4 to 9.0 (and above) may cause an outage as the session-capacity is reset to 0 (not 8000).

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.

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.

SSH Host Key Algorithms

The SBC offers `rsa-sha2-512` 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 SHA2 host key algorithms.

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.

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.

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.

Upgrading Transcoding Jitter Settings to S-Cz10.0.0

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.

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.

Removed TLS Ciphers

Release S-Cz9.3.0p3 and later removes support for TLS1.0 and TLS1.1. The option parameter in security-config is reset to "sslmin=tls1.2" if it was previously set to either "sslmin=tls1.0" or "sslmin=tls1.1". You can no longer select either "tlsv1" or "tlsv11" for **tls-version** in the **tls-profile** element.

Release S-Cz9.3.0p3 and later removes support for the following weak ciphers:

- 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
- TLS_AES_128_CCM_8_SHA256
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_NULL_SHA256
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_NULL_MD5

The ALL value is also removed, and DEFAULT is now the only cipher list. As a result, the cipher-list in a tls-profile is reset to DEFAULT if it was previously set to ALL.

Updated SRTP Cryptographic Lists

Release S-Cz9.3.0p3 updates the **crypto-list** attribute in the **sdes-profile** element. The **crypto-list** attribute supports the following ciphers on the Acme Packet 6350, Acme Packet 6400, and Acme Packet 4600:

- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32
- ARIA_CM_192_HMAC_SHA1_80
- ARIA_CM_192_HMAC_SHA1_32

The **crypto-list** attribute supports the following ciphers on the Acme Packet 3900, Acme Packet 4900, Acme Packet 1100, and virtual platforms:

- AES_CM_128_HMAC_SHA1_80
- AES_CM_128_HMAC_SHA1_32
- AES_256_CM_HMAC_SHA1_80
- AEAD_AES_256_GCM

Removed IKE Algorithms

Release S-Cz9.3.0p3 and later includes the following IKE-related changes:

- Removes **hmac-md5-96** from the **auth-alg-list** attribute in the **ims-aka-profile** element.
- Removes **des-ede3-cbc** from the **encr-alg-list** attribute in the **ims-aka-profile** element.
- Removes the following values from the **auth-algo** attribute in the **ike-sainfo** element:
  - xcbc
- Removes the following values from the **auth-algo** attribute in the **manual** element:
  - aes-xcbc-mac

Certificates Signature Algorithm

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

HMR Regex Matching

An upgrade to Lua 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.

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 (including in S-Cz10.0.0), 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-Cz10.0.0 from S-Cz9.1.0 or earlier, 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-Cz10.0.0 to two separate translation rules: one that modifies the To header and one that modifies the Request URI.

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
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

Feature	Type
ANSII R226 Compliance	Enabled or Disabled

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
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 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

On virtual platforms, the number of static ACL entries 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 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

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 • G722 • G723 • G726 • G726-16 • G726-24 • G726-32 • G726-40 • G729 • G729A • iLBC • opus • PCMA • PCMU • SILK • telephone-event [2] • T.38OFD*[3] • G711OFD* • OFDFB* 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 **A telephone-event requires DTMF tone generator and detector.**

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

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. If your software version does not support the new memory, the TCM3 cards with the new memory do not boot, and the system shows their state as BOOT FAILURE. Furthermore, system behavior when you use older software with this new memory is unpredictable.

For unsupported TCM3 cards, the system generates a notification for each unsupported card on the console showing its incompatibility. Contact support if you need to verify your hardware.

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.

Session Border Controller

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

- Session Delivery Manager: 9.0.2.0.2, 9.0.3, 9.0.3.0.1 and later
- Oracle Session Delivery Manager Cloud: 25.2 and later
- Oracle Communications Operations Monitor: 5.2 and 6.0
- Subscribe-Aware Load Balancer: 9.2.0, 9.3.0, 10.0
- Session Router: 9.1.0, 9.2.0, 9.3.0, 10.0

> **Note:**
>
> To manage S-Cz10.0.0 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-Cz9.1.0
- S-Cz9.2.0
- S-Cz9.3.0
- S-Cz10.0.0

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

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

Session Router

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

- Session Delivery Manager: 9.0.3.0.1, 9.0.3 and 9.0.2.0.2
- Oracle Session Delivery Manager Cloud: 25.2 and later
- Oracle Communications Operations Monitor: 5.2 and 6.0

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, 9.0.3 and 9.0.2.0.2
- Oracle Session Delivery Manager Cloud: 25.2 and later
- Session Border Controller: S-Cz9.2.0, S-Cz9.3.0 and S-Cz10.0 on the Acme Packet 4600, 4900, and 6350 platforms, and for virtualized deployment.
- Enterprise Session Border Controller: S-Cz9.2.0, S-Cz9.3.0 and S-Cz10.0 on the Acme Packet 4600, 4900, and 6350 platforms, and for virtualized deployment.

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.

TLS 1.0 and TLS 1.1 are not supported in release S-Cz10.0.0.

Unsupported TLS Ciphers

Support for the following ciphers, which were available in S-Cz9.3.0 GA but removed in S-Cz9.3.0p3, are not supported in this release:

- 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

- TLS_AES_128_CCM_8_SHA256
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_NULL_SHA256
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_NULL_MD5

Documentation Changes

The following information describes structural changes to the documentation for the S-Cz10.0.0 release.

Alarm Documentation

This version of the SBC adds the same alarm tables to both the MIB Guide and the Maintenance and Troubleshooting Guide. Both these tables are enhanced to include the following columns:

- Alarm Name
- Alarm ID
- Alarm Severity
- Cause
- Example Log Message
- Actions to diagnose the fault
- Trap Name (if any)

STIR/SHAKEN Client Chapter

The STIR/SHAKEN Client chapter in the ACLI Configuration Guide has been re-organized by grouping the information into a smaller number of higher level topics. This was done to simplify chapter navigation, generated by an increasing number of features. These high level topics now include:

- HTTP Client Operating Mode
- Number Authentication Mechanism Standards Compliance Features
- STIR/SHAKEN Servers
- STIR/SHAKEN Functions
- Additional Administrative Features
- STIR/SHAKEN Reporting

Behavioral Changes

The following information describes behavioral changes to the Oracle Communications Session Border Controller (SBC) for version S-Cz10.0.0.

Preconditions Handling

The SBC now handles preconditions at the dialog level. Previously, the SBC supported preconditions at the session level. This allows the SBC to support confirmation requests coming from different dialogs within a session.

HMR Regex Matching

An upgrade to Lua 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.

Patches Included in This Release

The following information assures you that when upgrading, the S-Cz10.0.0 release includes defect fixes from neighboring patch releases.

Neighboring Patches Included

- S-Cz9.1.0p14
- S-Cz9.2.0p10
- S-Cz9.3.0p4

Supported SPL Engines

The S-Cz10.0.0 release supports the following SPL engine versions:

- C4.0.0 and later

2
New Features

The S-Cz10.0.0 release of the Oracle Communications Session Border Controller (SBC) software supports the following new features.

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

> **Note:**
>
> TEMPLATE - See the Caveats and Limitations Chapter of the S-Cz10.0.0 Known Issues and Caveats Guide for functional limitations of this feature that apply to this software release.

Expanded DNS Functions and Tools

With this release, the SBC allows you to fetch additional DNS statistics and extract DNS resolution information using the **show dns** command on the ACLI. In addition to basic DNS statistics, using the ACLI **show dns** command, new arguments provide more specific statistics, resolutions and information.

See the DNS Statistics section in the ? chapter of the *Maintenance and Troubleshooting Guide* for detailed information.

OCOM Filtering

With this release, you can configure the SBC to filter the data it sends to a monitor collector to simplify your system monitoring and troubleshooting. You do this by configuring one or more **filter-profile** elements within the **comm-monitor** elements.

See the Filtering Data for Operations Monitor section in the ? chapter of the *Maintenance and Troubleshooting Guide* for detailed information. Additional supporting information is available in the *ACLI Reference Guide*.

Sending SIP Pings from Multiple Realms to Global Session Agents

With this release, you can configure the SBC to send SIP OPTION pings to multiple physical agents through multiple realms using a global **session-agent** (SA). This feature monitors status of global SA targets on the system, supporting applicable deployments including UCaaS topologies that include multiple tenancies. You enable this feature by setting the **egress-realm-id** attribute of a **session-agent** to multiple realm names.

See the SIP Pings from Multiple Realms to Global SAs section in the "Session Routing and Load Balancing" chapter of the *ACLI Configuration Guide* for detailed information.

Enhancement to Early Media Gating Functionality

With this release, you can configure the SBC to bypass gating and forward early media to untrusted domains. This feature resolves early media problems for situations including PEM gating when an UPDATE goes from the trusted side towards the untrusted side and the system prevents an early media announcement to play through the subsequent 18x. In this case, the default SBC behavior would be to gate the early media. To configure this feature, you enable the **pass-pem-in-update** option on the ingress **sip-interface**.

See the Bypassing Early Media Gating section in the SIP chapter of the *ACLI Configuration Guide* for detailed information.

STIR/SHAKEN MAN Compliance

With this release, you can configure the SBC to include compliance behaviors for the Number Authentication Mechanism 2.0 operations standards by enabling the **man-compliance** option in the **sti-config**. The Number Authentication Mechanism 2.0 standard, often referenced as MAN 2, is a French standard for CLI anti-spoofing. It was developed via a collaborative effort between the French Telecoms Federation (that unifies telco operators in France) along with ARCEP (Regulatory Authority) and the APNF (French association of standardization platforms for inter-operator flows).

In addition to this support, this release extends upon STIR/SHAKEN support to include:

- Accepting Non-Standard verstat
- Bypass STI-AS Signature and STI-VS Verification Requests
- Media Policy within the http-server element
- TLS Session Key Logging
- Remove the verstat from Incoming Requests
- Extract verifyResults Content from div Passports for 3GPP
- Managing Curl within HTTP Server Interactions

See the Number Authentication Mechanism Standards Compliance Features section in the STIR/SHAKEN chapter of the *ACLI Configuration Guide* for detailed information on STIR/SHAKEN MAN Compliance. Additional feature support is also documentation in the STIR/SHAKEN chapter of the *ACLI Configuration Guide*.

TACACS+ support by SBC REST API

This release of the SBC adds support for TACACS+ users to access the SBC from the REST interface, restricting their actions via TACACS+ authorization and recording those actions with TACACS+ accounting.

This functionality is documented in the *ACLI Configuration Guide* and *ACLI Reference Guide* including:

1. In the SBC Configuration Guide, the "User Accounts" > "TACACS+ Authorization" section has a new section called "TACACS+ Authorization for the REST API".
2. In the REST API documentation, a link to the previous topic is added to the Authenticate topic.
3. The authentication reference topic in the ACLI Reference Guide is updated to add the **rest-authorization-accounting** attribute.

Egress Enhancement to the Separate Clock Rates on Audio and 2833 Feature

Release 9.0.0p3 introduced a feature that provided support for different codec and telephone-event rates in the SDP. This feature allows you to configure the SBC to support flows when using different clock rates for audio and telephone events. This allows the SBC to adapt to environments that do not follow the recommendation for the same rates in RFC 4733. This feature, however, was limited to ingress interfaces. This release of the SBC adds this same support for egress interfaces.
See the Separate Clock Rates for Audio and Telephone Events section in the Transcoding chapter of the *ACLI Configuration Guide* for detailed information.

Software FAX Transcoding on virtual SBC

This release of the SBC removes the limitation that excluded software FAX transcoding on virtual SBCs, including those running on AMD CPUs. Verification of the removal of this limitation is provided in the *Known Issues and Caveats Guide*.

Expanded Transcoding Support for virtual SBC

This release of the SBC removes the limitation that excluded transcoding on some virtual SBCs, including those running on AMD CPUs. Verification of the removal of this limitation is provided in the *Known Issues and Caveats Guide*.

Resource Monitoring

In addition to specific function and operation monitoring, the SBC provides you with the ability to monitor overall system resource utilization to protect against undesirable behavior caused by the cumulative utilization of resources. You configure this feature using the **resource-monitoring-profile** element. This monitoring function operates independently on HA pairs, protecting the standby from resource over utilization independently from the active.

See the System Resource Monitoring section in the System chapter of the *ACLI Configuration Guide* for detailed information. SNMP information related to this feature is also available in the *MIB Guide*

System CPU Load Limiting

With this release, the SBC supports better management of overall CPU usage. Specifically, the system can manage overall percent CPU utilization and reject calls regardless of the thread utilization managed by your SIP Limiting configuration. This establishes a second level of limiting, protecting against issues with CPU usage beyond usage of a given thread. Call rejection follows the same logic as SIP Limiting:

- Begins rejecting SIP requests when the CPU reaches its throttling threshold
- Rejects all SIP requests when the CPU reaches its maximum utilization

See the SMP-Aware Task Load Limiting section in the System Management chapter of the *Maintenance and Troubleshooting Guide* for detailed information.

Monitoring Wancom1 and Wancom2 Using SNMP

With this release, you can configure the SBC to trigger alarms and traps when your HA wancom interfaces, including wancom1 and/or wancom2, go down. This allows you to more quickly recognize disruptions and re-establish your HA deployment's functionality.

See the Alarms and Traps for Wancom1 and 2 Interfaces section in the High Availability Notes chapter of the *ACLI Configuration Guide* for detailed information.

Additional Commands in Show support-info

With this release, the SBC includes additional commands in its output when you run the **show support-info** command.

See the Included Data section in the Fault Management chapter of the *Maintenance and Troubleshooting Guide* for a complete list of the commands displayed in the **show support-info** output.

Archiving support-info and Logfiles

With this release, the SBC, you can configure the SBC to include **show support-info** and Log Files with using the same mechanism is uses to archive configuration file backups. The SBC can also raises an alarm and issue a simultaneous SNMP trap to notify you each time access to a push-receiver fails.

See the Scheduled External Backups section in the System chapter of the ACLI Configuration Guide for detailed information.

Re-Registering Surrogate-agents After Switchover over TCP

You can configure the SBC to re-register all of its surrogate agents immediately after an HA switchover. This behavior is valid for all surrogate agent, regardless of transport, but is limited to 10,000 surrogate agent registrations to prevent a registration avalanche. If the system has more than 10,000 surrogate agent registrations to perform, the remaining agents re-register normally.

See the Surrogate Agents Re-Register after Switchover section in the SIP chapter of the ACLI Configuration Guide for detailed information.

Removal of the AMR-NB Entitlement

You can now configure the SBC to use this codec without setting an entitlement, and there is no longer a licensed capacity limit. When observed from HDR, the REST API or SNMP, the limit displays as 0, which means no limit.

Account Servers over IPv6

You can configure the SBC to use IPv6 over the RF interface in addition to IPv4 to support Diameter Accounting Servers. This allows you to support ACR exchanges between the system and CRF servers using IPv6. In addition, you can configure your account-server elements to perform A and AAAA DNS lookups for servers using IPv4 or IPv6 addressing.

See the Diameter Accounting chapter of the *Accounting Guide* and the *ACLI Reference Guide* for information confirming this feature.

Intel 800 Series Support - IAVF

With this release, Oracle has extended upon the support available on the SBC.

See the Requirements for Machines on Private Virtual Infrastructures section in the Introduction Chapter of these Release Notes to see details about the platforms and applications wherein you can use the Intel 800 Series network interfaces.

Acme Packet 6400 Platform

With release S-Cz10.0.0p1, you can deploy the SBC on the Acme Packet 6400 platform.

> **Note:**
>
> Make sure your software image is S-Cz10.0.0p1 or later.

See the Acme Packet 6400 Appendix in the *Platform Preparation and Installation Guide* for information about deploying on this platform. Also see the *Acme Packet 6400 Installation Guide* for detailed physical installation information about this hardware platform.

New PLMN-ID Insertion Cases

In addition to REGISTRATION scenarios, the SBC can use the latest PVNI header with the latest PLMN information in the INVITE/REINVITE/MESSAGE sip request's 200 OK response towards the core. This occurs after S8HR inter-PLMN handover. These scenarios include those that generate a 200 OK toward the core during SIP MO INVITE signaling.

See the VPLMN-ID Management Support topic in the IMS Support chapter of the *ACLI Configuration Guide* for detailed information about this feature.

> **Note:**
>
> This new feature support begins with S-Cz10.0.0p2.

Managing IOI for Peering Endpoints

You can configure the SBC to manage P-Charging-Vector (PCV) headers and populate standard AVPs and CDRs with Originating and Terminating IOIs for peering deployments. This is separate from IOI management within access and P-CSCF applications. Configurations that apply to this feature include the **ioi-for-unregistered** option in the applicable **account-config**, and the **charging-vector-mode** settings on the applicable **sip-interface** elements.

See the Managing IOI for Peering Endpoints topic in the Diameter Accounting chapter of the *Accounting Guide* for detailed information about this feature.

> **Note:**
>
> This new feature support begins with S-Cz10.0.0p2.

Sending SIP Pings from Multiple Realms to Global Session Agents for Session Router

This feature, introduced for the SBC at S-Cz10.0.0 is now supported on the Session Router.

With this release, you can configure the SBC to send SIP OPTION pings to multiple physical agents through multiple realms using a global **session-agent** (SA). This feature monitors status of global SA targets on the system, supporting applicable deployments including UCaaS topologies that include multiple tenancies. You enable this feature by setting the **egress-realm-id** attribute of a **session-agent** to multiple realm names.

See the SIP Pings from Multiple Realms to Global SAs section in the "Session Routing and Load Balancing" chapter of the *ACLI Configuration Guide* for detailed information.

> **Note:**
>
> This new feature support for the Session Router begins with S-Cz10.0.0p2.

3
Interface Changes

The following topics summarize ACLI, SNMP, HDR, Alarms, Accounting, and Error/Warning changes for S-Cz10.0.0. 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-Cz10.0.0 release.

Security Configuration Element

Modified Element	Description
security, **authentication**, **radius-servers**	This element is only available when FIPS is not enabled.
security, **authentication**, **tacacs-servers**	This element is only available when FIPS is not enabled.
security, **authentication**	When FIPS is enabled, the following attributes are not configurable: **source-port**, **protocol**, **tacacs-authentication-only**, **tacacs-authorization**, **tacacs-accounting**, **server-assigned-privilege**, **allow-local-authorization**, **management-strategy**, **ike-radius-params-name**, and **management-servers**.
security, **authentication**, **type**	When FIPS is enabled, this attribute is always **local**.
security, **authentication**, **tacacs-authorization-arg-mode**	A new value **enabled-include-show** is added to include show commands in the arg-mode of TACACS authorization requests.
security, **authentication**, **rest-authorization-accounting**	Enable TACACS+ accounting for REST users.
security, **certificate-record**, **key-size**	When FIPS is enabled, you cannot set this attribute to **1024**.
security, **certificate-record**, **digest-algor**	When FIPS is enabled, you cannot set this attribute to **sha1**.
security, **certificate-record**, **key-algor**	Adds the value **rsapss**.
security, **ike**, **ike-key-id**	Adds a new attribute **id-type**.
security, **ike**, **ike-sainfo**	Adds new attributes **local-id-profile** and **remote-id-profile**. When FIPS is enabled, the option **any** is not available for either **auth-algo** or **encryption-algo**.
security, **ike**, **ike-sainfo**, **auth-algo**	Removes the value **aes-xcbc**.
security, **ike**, **ike-sainfo**, **encryption-algo**	When FIPS is enabled, the option **any** is not available.
security, **certificate-record**, **key-algor**	Adds the value **rsapss**.
security, **ike**, **ike-config**, **phase1-dh-mode**	When FIPS is enabled, you cannot select the value **dh-group5**.

Modified Element	Description
security, **ike**, **ike-config**, **phase2-exchange-mode**	When FIPS is enabled, you cannot select the value **dh-group5**.
security, **ike**, **ike-config**, **eap-protocol**	Removes the value **eap-md5**.
security, **ike**, **ike-interface**, **eap-protocol**	Removes the value **eap-md5**.
security, **ims-aka-profile**, **auth-alg-list**	Removes the value **hmac-md5-96**.
security, **ims-aka-profile**, **encr-alg-list**	Removes the value **des-ede3-cbc**.
security, **ipsec**, **security-association**, **manual**, **auth-algo**	Removes the value **aes-xcbc-mac**. When FIPS is enabled, you cannot select **null**.
security, **ipsec**, **security-association**, **manual**, **encr-algo**	When FIPS is enabled, you cannot select **null**.
security, **media-profile**, **sdes-profile**, **crypto-list**	When FIPS is enabled, you cannot select AES_CM_128_HMAC_SHA1_32.
security, **ssh-config**, **keyex-algorithms**	When FIPS is enabled, you cannot select: • diffie-hellman-group-exchange-sha256 • diffie-hellman-group-exchange-sha1 • diffie-hellman-group1-sha1 • diffie-hellman-group14-sha1
security, **tls-global**, **diffie-hellman-key-size**	When FIPS is enabled, this value must be DH_KeySize_2048.

Media Manager Configuration Element

Modified Element	Description
media-manager, **codec-policy**	Adds support for the following codecs: **T.38**, **G711FB**, **T.38OFD**, **G711OFD** and **OFDFB**. On most platforms, removes ptime 90 from the G723 codec and adds ptime 60 to G722.
media-manager, **codec-policy**, **tone-detection**	This attribute is now available on software platforms.
media-manager, **codec-policy**, **fax-single-m-line**	This attribute is now available on software platforms.
media-manager, **media-manager**	Removed the attributes **home-realm-id**, **percent-sub**, and **pss-wd-key**.
media-manager, **realm-config**	Adds new attributes **interim-qos-enable** and **multi-tenancy-fqdn**. The **auth-attribute** attribute is renamed **auth-attributes**.

System Configuration Element

Modified Element	Description
system, **system-config**, **collect**, **group-settings**, **group-name**	Adds the value **latest-peak-license-usage**.
system, **system-config**	Adds a new attribute **peak-concurrent-license**.
system, **system-config**, **comm-monitor**	Adds the **filter-profile** configuration element.
system, **system-config**, **comm-monitor**, **monitor-collector**	Adds the attribute **filter-profile-list**.
system, **http-client**	Adds the **media-policy** attribute.
system, **redundancy**	Adds attributes **wancom-ping-interval** and **wancom-ping-retry**.

Modified Element	Description
system, **resource-monitor-profile**	Adds the attribute **processName**. Adds the subelements **minor-config**, **major-config**, and **critical-config**. Moves the attributes *-threshold and *-precaution-action into their respective *-config subelements. Each subelement also has its own **healthscore-decrement-value** attribute.
system, **system-config**, **schedule-backup**	Adds a new attribute **logs-backup**.
system, **system-config**	Adds new attribute **peak-concurrent-license**, **ldap-trace**, and **log-curl-tls-key**

Session Router Configuration Element

Modified Element	Description
The **account-servers** element is found under **session-router**, **account-group**; or **session-router**, **account-config**.	Adds a new attribute **dns-query-type** to specify A or AAAA records.
session-router, **sti-config**	Adds new attribute **sti-reason-header-config-name** to identify the name of the STI Reason Header config configured under **sti-reason-header-config**.
session-router, **sti-server**	Adds new attribute **sti-reason-header-config-name** to identify the name of the STI Reason Header config configured under **sti-reason-header-config**.
session-router, **session-agent**	The **auth-attribute** attribute is renamed **auth-attributes**.
session-router, **sip-config**	Adds new attribute **surrogate-reg-switchover**.
session-router, **sti-config**	Adds attributes **sti-reason-header-config-name**, **stop-adding-verstat-towards-caller**, **stivs-bypass-header**, and **stias-bypass-header**
session-router, **sti-server**	Adds attributes **sti-reason-header-config-name** and **sti-reason-header-config-name**

ACLI Command Changes

The following table summarizes the ACLI command changes in the Oracle Communications Session Border Controller S-Cz10.0.0 release.

This table lists and describes changes to ACLI commands that are available in the S-Cz10.0.0 release.

Modified Commands	Description
ssh-key	The ssh-key command no longer allows you to import DSA keys.
request collection [purge | restart | start | status | stop] [args]	Adds a new argument **latest-peak-license-usage**.
reset [args]	Adds a new argument **resourceMonitor**.
generate-key	Removes the values **3des** and **hmac-md5**.
show dns stats [args]	Adds a new argument **dns-servers**.
show dns query <realm> <type> <domain> [args]	Adds a new argument **server-ip-addr**

Modified Commands	Description
show redundancy [args]	Adds a new argument **xserv**
show ip connections [args]	Adds new arguments: **srcip**, **srcport**, **dstip**, **dstport**
show resourcemonitor	Adds new show options: **resourcemonitor**, **system-overload**.
test-stir	New command.

Accounting Changes

The following information summarizes the accounting changes in the Oracle Communications Session Border Controller S-Cz10.0.0 release.

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

The following accounting AVPs have been added in this release:

- Stir-VS-Attest
- Stir-Div-VS-Reason
- Stir-Div-VS-Verstat

SNMP/MIB Changes

The following information summarizes the SNMP MIB changes in the Oracle Communications Session Border Controller S-Cz10.0.0 release.

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

MIBs

The following new MIBs are added in this release:

- apNetNet6400 / 1.3.6.1.4.1.9148.1.5.4
- apWancomSyncNotificationsGroupCap / 1.3.6.1.4.1.9148.2.1.20.9
- apAppsPushReceiverNotificationGroupTrapCap / 1.3.6.1.4.1.9148.2.1.20.10
- apResourceMonitoringCapabilities / 1.3.6.1.4.1.9148.2.1.34
- apResMonitoringPpmGroupCap / 1.3.6.1.4.1.9148.2.1.34.1
- apResMonitoringResourceTrapCap / 1.3.6.1.4.1.9148.2.1.34.2
- apLatestPeakLicenseUsageMibCapabilities / 1.3.6.1.4.1.9148.2.2.6
- apLatestPeakLicenseUsageCap / 1.3.6.1.4.1.9148.2.2.6.1
- apAppsLatestPeakLicenseUsageMIBObjects / 1.3.6.1.4.1.9148.3.16.1.2.7
- apAppsLatestPeakLicenseUsageTable / 1.3.6.1.4.1.9148.3.16.1.2.7.1
- apAppsLatestPeakLicenseUsageEntry / 1.3.6.1.4.1.9148.3.16.1.2.7.1.1
- apLatestPeakLicenseUsageSessionType / 1.3.6.1.4.1.9148.3.16.1.2.7.1.1.1
- apLatestPeakLicenseUsageHighCount / 1.3.6.1.4.1.9148.3.16.1.2.7.1.1.2
- apLatestPeakLicenseUsageTimeStamp / 1.3.6.1.4.1.9148.3.16.1.2.7.1.1.3
- apPushReceiverNotifObj / 1.3.6.1.4.1.9148.3.16.2.1.1

- apPushReceiverType / 1.3.6.1.4.1.9148.3.16.2.1.1.1
- apPushReceiverAddressType / 1.3.6.1.4.1.9148.3.16.2.1.1.2
- apPushReceiverAddress / 1.3.6.1.4.1.9148.3.16.2.1.1.3
- apPushReceiverFailureReasonCode / 1.3.6.1.4.1.9148.3.16.2.1.1.4
- apAppsWancomNotif / 1.3.6.1.4.1.9148.3.16.2.2.7
- apAppsWancomNotifications / 1.3.6.1.4.1.9148.3.16.2.2.7.0
- apWancomSyncFailTrap / 1.3.6.1.4.1.9148.3.16.2.2.7.0.1
- apWancomSyncFailClearTrap / 1.3.6.1.4.1.9148.3.16.2.2.7.0.2
- apPushReceiverNotif / 1.3.6.1.4.1.9148.3.16.2.2.8
- apPushReceiverNotifications / 1.3.6.1.4.1.9148.3.16.2.2.8.0
- apPushReceiverFailureTrap / 1.3.6.1.4.1.9148.3.16.2.2.8.0.1
- apAppsLatestPeakLicenseUsageGroup / 1.3.6.1.4.1.9148.3.16.3.1.13
- apWancomNotificationGroups / 1.3.6.1.4.1.9148.3.16.3.2.8
- apWancomSyncNotificationsGroup / 1.3.6.1.4.1.9148.3.16.3.2.8.1
- apPushReceiverNotificationGroups / 1.3.6.1.4.1.9148.3.16.3.2.9
- apPushReceiverNotificationsGroup / 1.3.6.1.4.1.9148.3.16.3.2.9.1
- apAppsWancomObjects / 1.3.6.1.4.1.9148.3.16.9
- apWancomSyncObjects / 1.3.6.1.4.1.9148.3.16.9.1
- apWancomName / 1.3.6.1.4.1.9148.3.16.9.1.1
- apResourceMonitoringModule / 1.3.6.1.4.1.9148.3.22
- apRMPPMObjects / 1.3.6.1.4.1.9148.3.22.1
- apNatPpmDebugStatsTable / 1.3.6.1.4.1.9148.3.22.1.1
- apNatFlowDebugEntry / 1.3.6.1.4.1.9148.3.22.1.1.1
- apNatFlowDebugStatsIndex / 1.3.6.1.4.1.9148.3.22.1.1.1.1
- apNatFlowDebugStats / 1.3.6.1.4.1.9148.3.22.1.1.1.2
- ap2833PpmDebugStatsTable / 1.3.6.1.4.1.9148.3.22.1.2
- ap2833FlowDebugEntry / 1.3.6.1.4.1.9148.3.22.1.2.1
- ap2833FlowDebugStatsIndex / 1.3.6.1.4.1.9148.3.22.1.2.1.1
- ap2833FlowDebugStats / 1.3.6.1.4.1.9148.3.22.1.2.1.2
- apHmuDebugStatsTable / 1.3.6.1.4.1.9148.3.22.1.3
- apHmuFlowDebugEntry / 1.3.6.1.4.1.9148.3.22.1.3.1
- apHmuFlowDebugStatsIndex / 1.3.6.1.4.1.9148.3.22.1.3.1.1
- apHmuFlowDebugStats / 1.3.6.1.4.1.9148.3.22.1.3.1.2
- apQosPpmDebugStatsTable / 1.3.6.1.4.1.9148.3.22.1.4
- apQosFlowDebugEntry / 1.3.6.1.4.1.9148.3.22.1.4.1
- apQosFlowDebugStatsIndex / 1.3.6.1.4.1.9148.3.22.1.4.1.1
- apQosFlowDebugStats / 1.3.6.1.4.1.9148.3.22.1.4.1.2
- apSrtpEPpmStatsDebugTable / 1.3.6.1.4.1.9148.3.22.1.5

- apSrtpEFlowDebugEntry / 1.3.6.1.4.1.9148.3.22.1.5.1
- apSrtpEFlowDebugStatsIndex / 1.3.6.1.4.1.9148.3.22.1.5.1.1
- apSrtpEFlowDebugStats / 1.3.6.1.4.1.9148.3.22.1.5.1.2
- apSrtpDPpmDebugStatsTable / 1.3.6.1.4.1.9148.3.22.1.6
- apSrtpDFlowDebugEntry / 1.3.6.1.4.1.9148.3.22.1.6.1
- apSrtpDFlowDebugStatsIndex / 1.3.6.1.4.1.9148.3.22.1.6.1.1
- apSrtpDFlowDebugStats / 1.3.6.1.4.1.9148.3.22.1.6.1.2
- apRMResourceObjects / 1.3.6.1.4.1.9148.3.22.2
- apRmCommandQueueUtil / 1.3.6.1.4.1.9148.3.22.2.1
- apRmNatFlowPpmUtil / 1.3.6.1.4.1.9148.3.22.2.2
- apRmQosPpmUtil / 1.3.6.1.4.1.9148.3.22.2.3
- apRm2833PpmUtil / 1.3.6.1.4.1.9148.3.22.2.4
- apRmMbcdSrtpSessionsUtil / 1.3.6.1.4.1.9148.3.22.2.5
- apRmHmuPpmUtil / 1.3.6.1.4.1.9148.3.22.2.6
- apRmSrtpEPpmUtil / 1.3.6.1.4.1.9148.3.22.2.7
- apRmSrtpDPpmUtil / 1.3.6.1.4.1.9148.3.22.2.8
- apRmAtcpdTcpTlsSessions / 1.3.6.1.4.1.9148.3.22.2.9
- apRMNotificationObjects / 1.3.6.1.4.1.9148.3.22.3
- apRmTrapType / 1.3.6.1.4.1.9148.3.22.3.1
- apRmTrapValue / 1.3.6.1.4.1.9148.3.22.3.2
- apRMNotificationPrefix / 1.3.6.1.4.1.9148.3.22.4
- apRMNotifications / 1.3.6.1.4.1.9148.3.22.4.0
- apRmResourcesGroupTrap / 1.3.6.1.4.1.9148.3.22.4.0.1
- apRmResourcesGroupClearTrap / 1.3.6.1.4.1.9148.3.22.4.0.2
- apResObjectGroups / 1.3.6.1.4.1.9148.3.22.5
- apResMonitoringPpmGroup / 1.3.6.1.4.1.9148.3.22.5.1
- apResMonitoringResourceTrapGroup / 1.3.6.1.4.1.9148.3.22.5.2
- apResMonitoringNotificationGroup / 1.3.6.1.4.1.9148.3.22.5.3

The following MIBS are not supported in SBC. Earlier releases supported these MIBs for customers using Oracle EMS and NNC products.

- apEMSModule / 1.3.6.1.4.1.9148.3.8
- apEMSMIBObjects / 1.3.6.1.4.1.9148.3.8.1
- apEMSNotificationObjects / 1.3.6.1.4.1.9148.3.8.2
- apEMSDiscoveryMode / 1.3.6.1.4.1.9148.3.8.2.1
- apEMSNodeID / 1.3.6.1.4.1.9148.3.8.2.2
- apEMSStartTime / 1.3.6.1.4.1.9148.3.8.2.3
- apEMSDateTime / 1.3.6.1.4.1.9148.3.8.2.4
- apEMSUser / 1.3.6.1.4.1.9148.3.8.2.5

- apEMSDeviceAddress / 1.3.6.1.4.1.9148.3.8.2.6
- apEMSFunction / 1.3.6.1.4.1.9148.3.8.2.7
- apEMSNotifications / 1.3.6.1.4.1.9148.3.8.3
- apEMSConfigNotificationsPrefix / 1.3.6.1.4.1.9148.3.8.3.1
- apEMSConfigNotifications / 1.3.6.1.4.1.9148.3.8.3.1.0
- apEMSDiscoveryFailure / 1.3.6.1.4.1.9148.3.8.3.1.0.1
- apEMSSaveFailure / 1.3.6.1.4.1.9148.3.8.3.1.0.2
- apEMSActivateFailure / 1.3.6.1.4.1.9148.3.8.3.1.0.3
- apEMSInvalidConfigDiscovered / 1.3.6.1.4.1.9148.3.8.3.1.0.4
- apEMSInvalidConfigInventory / 1.3.6.1.4.1.9148.3.8.3.1.0.5
- apEMSDeviceHealthNotificationsPrefix / 1.3.6.1.4.1.9148.3.8.3.2
- apEMSDeviceHealthNotifications / 1.3.6.1.4.1.9148.3.8.3.2.0
- apEMSNodeUnreachable / 1.3.6.1.4.1.9148.3.8.3.2.0.1
- apEMSNodeUnreachableClear / 1.3.6.1.4.1.9148.3.8.3.2.0.2
- apEMSModuleConformance / 1.3.6.1.4.1.9148.3.8.4
- apEMSGroups / 1.3.6.1.4.1.9148.3.8.4.1
- apEMSNotificationsGroups / 1.3.6.1.4.1.9148.3.8.4.2
- apEMSConfigNotificationsGroup / 1.3.6.1.4.1.9148.3.8.4.2.1
- apEMSDeviceHealthNotificationsGroup / 1.3.6.1.4.1.9148.3.8.4.2.2
- apEMSNotificationObjectsGroups / 1.3.6.1.4.1.9148.3.8.4.3
- apEMSNotificationObjectsGroup / 1.3.6.1.4.1.9148.3.8.4.3.1
- apNNCModule / 1.3.6.1.4.1.9148.3.8.5
- apNNCMIBObjects / 1.3.6.1.4.1.9148.3.8.5.1
- apNNCNotificationObjects / 1.3.6.1.4.1.9148.3.8.5.2
- apNNCServerAddressRemote / 1.3.6.1.4.1.9148.3.8.5.2.1
- apNNCServerNameRemote / 1.3.6.1.4.1.9148.3.8.5.2.2
- apNNCServerAddressLocal / 1.3.6.1.4.1.9148.3.8.5.2.3
- apNNCServerNameLocal / 1.3.6.1.4.1.9148.3.8.5.2.4
- apNNCFailureReason / 1.3.6.1.4.1.9148.3.8.5.2.5
- apNNCAggregationTimePercent / 1.3.6.1.4.1.9148.3.8.5.2.6
- apNNCAggregationLagPercent / 1.3.6.1.4.1.9148.3.8.5.2.7
- apOCSDMServerMasterAddress / 1.3.6.1.4.1.9148.3.8.5.2.8
- apOCSDMServerMasterName / 1.3.6.1.4.1.9148.3.8.5.2.9
- apOCSDMServerTrapInterval / 1.3.6.1.4.1.9148.3.8.5.2.10
- apEMPluginNameLocal / 1.3.6.1.4.1.9148.3.8.5.2.11
- apEMPluginRestPrefixName / 1.3.6.1.4.1.9148.3.8.5.2.12
- apNNCReportingUser / 1.3.6.1.4.1.9148.3.8.5.2.13
- apNNCReportingPswdExpiryDate / 1.3.6.1.4.1.9148.3.8.5.2.14

- apNNCFraudProtectionListName / 1.3.6.1.4.1.9148.3.8.5.2.15
- apNNCFraudProtectionListSizeLimit / 1.3.6.1.4.1.9148.3.8.5.2.16
- apNNCNotifications / 1.3.6.1.4.1.9148.3.8.5.3
- apNNCServerHealthNotificationsPrefix / 1.3.6.1.4.1.9148.3.8.5.3.1
- apNNCServerHealthNotifications / 1.3.6.1.4.1.9148.3.8.5.3.1.0
- apNNCServerUnreachable / 1.3.6.1.4.1.9148.3.8.5.3.1.0.1
- apNNCServerUnreachableClear / 1.3.6.1.4.1.9148.3.8.5.3.1.0.2
- apNNCTrapRelayNotAliveNotification / 1.3.6.1.4.1.9148.3.8.5.3.1.0.3
- apNNCTrapRelayAliveNotification / 1.3.6.1.4.1.9148.3.8.5.3.1.0.4
- apOCSDMSeverHeartbeatReachable / 1.3.6.1.4.1.9148.3.8.5.3.1.0.5
- apEMPluginFailedInstall / 1.3.6.1.4.1.9148.3.8.5.3.1.0.6
- apEMPluginFailedInstallClear / 1.3.6.1.4.1.9148.3.8.5.3.1.0.7
- apEMPluginFailedUninstall / 1.3.6.1.4.1.9148.3.8.5.3.1.0.8
- apEMPluginFailedUninstallClear / 1.3.6.1.4.1.9148.3.8.5.3.1.0.9
- apEMPluginDuplicatedRestPrefixName / 1.3.6.1.4.1.9148.3.8.5.3.1.0.10
- apNNCReportingNotificationsPrefix / 1.3.6.1.4.1.9148.3.8.5.3.2
- apNNCReportingNotifications / 1.3.6.1.4.1.9148.3.8.5.3.2.0
- apNNCReportingHdrDetectionFailure / 1.3.6.1.4.1.9148.3.8.5.3.2.0.1
- apNNCReportingHdrAggregationFailure / 1.3.6.1.4.1.9148.3.8.5.3.2.0.2
- apNNCReportingHdrAggregationFailureClear / 1.3.6.1.4.1.9148.3.8.5.3.2.0.3
- apNNCReportingHdrAggregationLagFailure / 1.3.6.1.4.1.9148.3.8.5.3.2.0.4
- apNNCReportingHdrAggregationLagFailureClear / 1.3.6.1.4.1.9148.3.8.5.3.2.0.5
- apNNCReportingPswdExpiration / 1.3.6.1.4.1.9148.3.8.5.3.2.0.6
- apNNCReportingPswdExpirationClear / 1.3.6.1.4.1.9148.3.8.5.3.2.0.7
- apOCSDMFraudProtectionNotificationsPrefix / 1.3.6.1.4.1.9148.3.8.5.3.3
- apOCSDMFraudProtectionNotifications / 1.3.6.1.4.1.9148.3.8.5.3.3.0
- apOCSDMFPLSizeExceedLimit / 1.3.6.1.4.1.9148.3.8.5.3.3.0.1
- apNNCModuleConformance / 1.3.6.1.4.1.9148.3.8.5.4
- apNNCGroups / 1.3.6.1.4.1.9148.3.8.5.4.1
- apNNCNotificationsGroups / 1.3.6.1.4.1.9148.3.8.5.4.2
- apNNCServerHealthNotificationsGroup / 1.3.6.1.4.1.9148.3.8.5.4.2.1
- apNNCReportingNotificationsGroup / 1.3.6.1.4.1.9148.3.8.5.4.2.2
- apNNCReportingAggrNotifsGroup / 1.3.6.1.4.1.9148.3.8.5.4.2.3
- apNNCReportingAggregationNotificationGroup / 1.3.6.1.4.1.9148.3.8.5.4.2.4
- apNNCServerHealthbeatNotificationsGroup / 1.3.6.1.4.1.9148.3.8.5.4.2.5
- apNNCPluginNotificationsGroup / 1.3.6.1.4.1.9148.3.8.5.4.2.6
- apOCSDMFraudProtectionNotificationsGroup / 1.3.6.1.4.1.9148.3.8.5.4.2.7
- apNNCNotificationObjectsGroups / 1.3.6.1.4.1.9148.3.8.5.4.3

- apNNCServerHealthObjectsGroup / 1.3.6.1.4.1.9148.3.8.5.4.3.1
- apNNCFailureObjectsGroup / 1.3.6.1.4.1.9148.3.8.5.4.3.2
- apNNCTimePercentObjectsGroup / 1.3.6.1.4.1.9148.3.8.5.4.3.3
- apNNCTimePercentObjGroup / 1.3.6.1.4.1.9148.3.8.5.4.3.4

Alarms

The following information summarizes the alarm changes in the Oracle Communications Session Border Controller S-Cz10.0.0 release.

System CPU Usage

This feature introduces 1 alarm on the SBC.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
SYSTEM_CPU_UTIL_OVER_THRESHOLD_BASE	131342	Minor, Major and Critical	System CPU utilization has exceeded configured thresholds	System CPU is at 92 percent, over minor/ major/critical threshold of 85 percent	Monitor and decrease CPU utilization, if necessary	NA

Wancom1 and Wancom2 monitoring using SNMP

This feature introduces 2 alarms on the SBC.

Table 3-1 Alarms Table

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
APP_WANCOM1_SYNC_FAILURE	327752	MAJOR	Synchronization across WANCOM1 has failed	Sync failure for Wancom1	Troubleshoot the network connection between the WANCOM1 interfaces	apWancomSyncFailTrap
APP_WANCOM2_SYNC_FAILURE	327753	MAJOR	Synchronization across WANCOM2 has failed	Sync failure for Wancom2	Troubleshoot the network connection between the WANCOM2 interfaces	apWancomSyncFailTrap

Scheduled External Log and Support-Info Backup

This feature introduces 1 alarm on the SBC.

Alarm Name	Alarm ID	Alarm Severity	Cause(s)	Example Log Message	Action to diagnose the fault	Trap Name
APP_ALARM_SCHBKP_LOGS_PUSH_FAIL	327760	WARNING	SBC failed to upload the current logs of the one (or more) configured push-receivers.	Some or all of the scheduled-backup's push receivers are down	Troubleshoot the network connection between the SBC and the scheduled-backup's push receivers interfaces	apPushReceiverFailureTrap

Resource Monitoring

This feature introduces 9 alarms on the SBC.

AlarmName	Alarm-ID	Severity	Causes	Example Log Message	Action	TrapName
MEM_UTIL_OVER_THRESHOLD	131100	minor major critical	High memory usage	Resource monitoring module raising alarm - Resource task id = TASK_ID, threshold = 80%, current value = 82%, processName = theap , resourceName = HEAP	Ensure calls are managed in a way that resource usage stays within the specified threshold	apRmResourcesGroupTrap
COMMAND_QUEUE_OVER_THRESHOLD	131426	minor major critical	High command Queue usage	Resource monitoring module raising alarm - Resource task id = TASK_ID, threshold = 80%, current value = 82%,process Name = sipd1 , resourceName = COMMAND_QUEUE	Ensure calls are managed in a way that resource usage stays within the specified threshold	apRmResourcesGroupTrap

NAT_OVER_THRESHOLD	131427	minor major critical	High calls / media sessions	Resource monitoring module raising alarm - Resource task id = TASK_ID, threshold = 80%, current value = 82%,process Name = tPpmEntry, resourceName = NAT_FLOWS	Ensure calls are managed in a way that resource usage stays within the specified threshold	apRmResourcesGroupTrap
DTMF_2833_OVER_THRESHOLD	131429	minor major critical	High DTMF calls usage	Resource monitoring module raising alarm - Resource task id = TASK_ID, threshold = 80%, current value = 82%,process Name = tPpmEntry , resourceName = 2833	Ensure calls are managed in a way that resource usage stays within the specified threshold	apRmResourcesGroupTrap
HMU_OVER_THRESHOLD	131431	minor major critical	High calls with HMU usage	Resource monitoring module raising alarm - Resource task id = TASK_ID, threshold = 80%, current value = 82%,process Name = tPpmEntry , resourceName = HMU	Ensure calls are managed in a way that resource usage stays within the specified threshold	apRmResourcesGroupTrap

QOS_OVER_THRESHOLD	131430	minor major critical	High calls with QOS usage	Resource monitoring module raising alarm - Resource task id = TASK_ID, threshold = 80%, current value = 82%,process Name = tPpmEntry, resourceName = QOS	Ensure calls are managed in a way that resource usage stays within the specified threshold	apRmResourcesGroupTrap
SRTPE_OVER_THRESHOLD	131432	minor major critical	High calls with SRTP_E usage	Resource monitoring module raising alarm - Resource task id = TASK_ID, threshold = 80%, current value = 82%,process Name = tPpmEntry , resourceName = SRTP_E	Ensure calls are managed in a way that resource usage stays within the specified threshold	apRmResourcesGroupTrap
SRTD_OVER_THRESHOLD	131433	minor major critical	High calls with SRTP_D usage	Resource monitoring module raising alarm - Resource task id = TASK_ID, threshold = 80%, current value = 82%,process Name = tPpmEntry, resourceName = SRTP_D	Ensure calls are managed in a way that resource usage stays within the specified threshold	apRmResourcesGroupTrap

SRTP_SESSIONS_OVER_THRESHOLD	131428	minor major critical	High calls of SRTP_SESSIONS	Resource monitoring module raising alarm - Resource task id = TASK_ID, threshold = 80%, current value = 82%,process Name = tmbcd, resourceName = SRTP_SESSIONS	Ensure calls are managed in a way that resource usage stays within the specified threshold	apRmResourcesGroupTrap
TCP_OVER_THRESHOLD	131434	minor major critical	High TCP/TLS calls.	Resource monitoring module raising alarm - Resource task id = TASK_ID, threshold = 80%, current value = 82%,process Name = tPpmEntry , resourceName = TCP/TLS	Ensure calls are managed in a way that resource usage stays within the specified threshold	apRmResourcesGroupTrap

HDR

The following information summarizes the accounting changes in the Oracle Communications Session Border Controller S-Cz10.0.0 release.

New HDR Objects for STIR/SHAKEN

STIR/SHAKEN development for this release generated 2 new HDR objects, including:

- AS Bypass - Total number of calls that bypassed the STI-AS server signature request based on message contents
- VS Bypass - Total number of calls that bypassed the STI-VS server verification request based on message contents

This version of the SBC uses these new HDR variables to collect data within 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

There are no new errors and warnings in this release.