Oracle® Enterprise Session Border Controller and Enterprise Session Router

Release Notes

Release S-Cz9.3.0
F92210-08
April 2025

Oracle Enterprise Session Border Controller and Enterprise Session Router Release Notes, Release S-Cz9.3.0

F92210-08

Contents

About this Guide

My Oracle Support vi

Revision History

1 Introduction to S-Cz9.3.0

Supported Platforms 1-1
- Supported Physical Platforms 1-1
- Supported Private Virtual Infrastructures and Public Clouds 1-2
- Requirements for Machines on Private Virtual Infrastructures 1-5
- PCIe Transcoding Card Requirements 1-8
- Enterprise Session Router Recommendations 1-8

Image Files and Boot Files 1-9
- Image Files for Customers Requiring Lawful Intercept 1-10
- Boot Loader Requirements 1-10
- Setup Product 1-10

Upgrade Information 1-11
- Upgrade Checklist 1-12
- Upgrade and Downgrade Caveats 1-12
- Fraud Protection File Rollback Compatibility 1-16
- HA Upgrade Procedure for Deprecated Ciphers 1-17

Feature Entitlements 1-20
- Encryption for Virtual SBC 1-21

System Capacities 1-22
Transcoding Support 1-22
Coproduct Support 1-24
TLS Cipher Updates 1-25
Documentation Changes 1-27
Behavioral Changes 1-27
Patches Included in This Release 1-27
Supported SPL Engines 1-27

2 New Features

3 Interface Changes

ACLI Configuration Element Changes 3-1
ACLI Command Changes 3-5
Accounting Changes 3-6
SNMP/MIB Changes 3-6
Alarms 3-8
HDR 3-8
Errors and Warnings 3-9

About this Guide

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

Documentation Set

The following table lists related documentation.

Document Name	Document Description
Acme Packet 3900 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 3900.
Acme Packet 4600 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4600.
Acme Packet 4900 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 3950 and Acme Packet 4900.
Acme Packet 6100 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6100.
Acme Packet 6350 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6350.
Release Notes	Contains information about the current documentation set release, including new features and management changes.
Known Issues & Caveats	Contains known issues and caveats
Configuration Guide	Contains information about the administration and software configuration of the Service Provider Session Border Controller (SBC).
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Maintenance and Troubleshooting Guide	Contains information about SBC logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
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 shows the dates and descriptions of revisions to the Release Notes.

Date	Revision
March 2024	• Initial release.
July 2024	• Adds Acme Packet 3900 Platform to Upgrade and Downgrade Caveats. • Adds S-Cz9.3.0p2 features.
October 2024	• Adds features for S-Cz9.3.0p3. • Adds TDM parameter caveat to Upgrade and Downgrade Caveats.
December 2024	• Adds features for S-Cz9.3.0p4.
February 2025	• Adds features for S-Cz9.3.0p5. • Adds support for Mellanox X-5. • Adds upgrade caveat about certificate signature algorithm.
April 2025	• Adds downgrade caveat on central CA certificate store feature. • Adds features for S-Cz9.3.0p6. • Corrects PCI Passthrough support for Intel 810 interfaces. • Adds upgrade and downgrade caveat for session translation.

1

Introduction to S-Cz9.3.0

The Oracle® Enterprise Session Border Controller *Release Notes* provides the following information about the S-Cz9.3.0 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® Enterprise Session Border Controller (ESBC) can run on a variety of physical and virtual platforms. You can also run the ESBC in public cloud environments. The following topics list the supported platforms and high level requirements.

Supported Physical Platforms

You can run the Oracle® Enterprise Session Border Controller on the following hardware platforms.

The S-Cz9.3.0 release of the ESBC supports the following platforms:

- Acme Packet 1100
- Acme Packet 3900
- Acme Packet 3950
- Acme Packet 4600
- Acme Packet 4900
- Acme Packet 6350 (Quad 10GbE NIU only)

The following platforms are no longer supported:

- Acme Packet 6100
- Acme Packet 6300
- Acme Packet 6350 (Dual port NIU only)

The S-Cz9.3.0 release of the Enterprise Session Router supports the following platforms:

- Acme Packet 4600
- Acme Packet 4900 (S-Cz9.3.0p2 and newer)
- Oracle Server X9-2

- Oracle Server X8-2

The following platform is no longer supported:

- Oracle Server X7-2

Supported Private Virtual Infrastructures and Public Clouds

You can run the ESBC 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 ESBC does not support automatic, dynamic disk resizing.

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

Supported Hypervisors for Private Virtual Infrastructures

Oracle supports installation of the ESBC on the following hypervisors:

- KVM (the following versions or later)
  - Linux kernel version: 3.10.0-1127
  - Library: libvirt 4.5.0
  - API: QEMU 4.5.0
  - Hypervisor: QEMU 1.5.3
- VMware: vSphere ESXi (Version 7.0)
  As of S-Cz9.3.0p2, the vSBC supports VMware: vSphere ESXi (Version 8.0)
- 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, nnSCZ930_HOT.tar.gz, and follow the OpenStack Heat Template instructions.

The nnSCZ930_HOT.tar.gz file contains two files:

- nnSCZ930_HOT_pike.tar
- nnSCZ930_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 ESBC on the following public cloud platforms.

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

Shape	OCPUs/ VCPUs	vNICs	Tx/Rx Queues	Max Forwarding Cores	DoS Protection	Memory
VM.Standard2.4	4/8	4	2	2	Y	60
VM.Standard2.8	8/16	8	2	2	Y	120
VM.Standard2.16	16/32	16	2	2	Y	240
VM.Optimized3.Flex-Small	4/8	4	8	6[1]	Y	16
VM.Optimized3.Flex-Medium	8/16	8	15	14[2]	Y	32
VM.Optimized3.Flex-Large	16/32	16	15	15	Y	64

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

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

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

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

Instance Type	vNICs	RAM	vCPUs	Max Forwarding Cores	DOS Protection
c4.xlarge	4	7.5	4		
c4.2xlarge	8	15	4		
c4.4xlarge	16	30	8		
c5.xlarge	4	8	4	1	N
c5.2xlarge	4	16	8	2	Y
c5.4xlarge	8	32	16	6	Y
c5n.xlarge	4	10.5	4	1	N
c5n.2xlarge	4	21	8	2	Y
c5n.4xlarge	8	42	16	6	Y

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 ESBC.

Size (Fs series)	vNICs	RAM	vCPUs	DOS Protection
Standard_F4s	4	8	4	N
Standard_F8s	8	16	8	Y
Standard_F16s	8	32	16	Y

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

Size types define architectural differences and cannot be changed after deployment. During deployment you choose a size for the ESBC, 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 ESBC 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 ESBC.

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 ESBC 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 ESBC 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 ESBC in HA mode.

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

On GCP the ESBC must use the **virtio** network interface card. The ESBC 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 ESBC 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, up to S-Cz9.3.0p5, is:

- 22.11

The DPDK version used as of the S-Cz9.3.0p5 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 ESBC image files is as follows:

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

Small Footprint vSBC

Minimum resources for a small footprint ESBC, typically used for SIP trunking to a PBX for non-transcoded, low-volume traffic, should be configured with the following resources:

- 2 vCPU Cores
- 4 GB RAM
- 20 GB hard disk (pre-formatted)
- 2 interfaces as follows:
  - 1 for management (wancom0)
  - 1 for media

The Small Footprint ESBC does not support the following:

- IMS-AKA Feature
- Transcoding
- IP-Sec Tunnels
- MSRP

Interface Host Mode for Private Virtual Infrastructures

The ESBC 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 ESBCs do not support media interfaces when media interfaces of different NIC models are attached. Media Interfaces are supported only when all media interfaces are of the same model, belong to the same Ethernet Controller, and have the same PCI Vendor ID and Device ID.

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

Ethernet Controller	Driver	SR-IOV	PCI Passthrough
Intel 82599 / X520 / X540	ixgbe	M	M
Intel i210 / i350	igb	M	M
Intel X710 / XL710 / XXV710	iavf (i40e, i40en)[1][2][3], iavf[4]	M	M
Validated with E810-XXVDA4 at 10GB switch speeds.[5]	iavf [6]	M	N/A
Mellanox Connect X-4	mlx5	M	M
Mellanox Connect X-5[7][8]	mlx5 [9][10]	M	N/A

1 This driver is supported on VMware only.
2 ESXi 7.0 deployments utilizing VLANs require the 1.14.1.0 version of this driver (or newer).
3 ESXi 8.0 deployments utilizing VLANs require the 2.6.5.0 version of this driver (or newer)
4 iavf driver is support in SR-IOV n/w mode.
5 Intel E810-XXVDA2, E810-XXVDA4, E810-XXVDA4T all use the same driver.
6 iavf driver is supported in SR-IOV n/w mode over KVM and VmWare
7 KVM only.
8 Supported as of S-Cz9.3.0p5.
9 Device Part number: 7603662 Oracle Dual Port 25 Gb Ethernet Adapter, Mellanox (for factory installation) .
10 Validated with 10G Speed using SFP- Fibre cables with 7604269 Oracle 10/25 GbE Dual Rate SFP28 Short Range (SR) Transceiver 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 ESBC.

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
Hyper-V (PV)	hv_netvsc	W
Hyper-V (PV)	failsafe	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 ESBCs 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 ESBC (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 ESBC 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.

Enterprise Session Router Recommendations

Oracle recommends the following resources when operating the SR or ESR, release S-Cz9.3.0 over Oracle servers.

Supported Platforms

The Session Router and Enterprise Session Router support the same Virtual Platforms as the ESBC. 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: `nnSCZ930.bz`
- Bootloader file: `nnSCZ930.boot`

Virtual Platforms

This S-Cz9.3.0 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:

- `nnSCZ930-img-vm_kvm.tgz`—Compressed image file including SBC VNF for KVM virtual machines, Oracle Cloud Infrastructure (OCI), AWS EC2, and GCP instances.
- `nnSCZ930-img-vm_vmware.ova`—Open Virtualization Archive (.ova) distribution of the SBC VNF for ESXi virtual machines.
- `nnSCZ930-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:

- `nnSCZ930_HOT.tar.gz`—The Heat Orchestration Templates used with OpenStack (Newton or Pike).
- `nnSCZ930_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: `nnSCZ930-img-usb.exe`
- Through ILOM: `nnSCZ930-img.iso`
- Bootloader file: `nnSCZ930.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 ESBC 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.

   If you want to setup the Enterprise Session Router, select **2 - Session Router - Session Stateful**.
4. Type **s** to save your choice as the product type of this platform.

5. Reboot your system.

```
ORACLE# setup product

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

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

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

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

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

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

Upgrade Information

When you perform a software upgrade, you need to follow the paths presented in these Release Notes and use the same image types to achieve a hitless upgrade. This applies to both HA and non-HA deployments. The paths are presented below.

An example of different image types is upgrading a non-LI deployment with an LI image. Such non-hitless upgrades require that you reboot devices per your upgrade procedure, and then reboot all upgraded devices again to establish the new deployment type.

Supported Upgrade Paths

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

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

- S-Cz9.0.0p12 (or higher) to S-Cz9.3.0
- S-Cz9.1.0p10 (or higher) to S-Cz9.3.0
- S-Cz9.2.0p4 (or higher) to S-Cz9.3.0

> **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® Enterprise 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® Enterprise 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® Enterprise Session Border Controller Release Notes for any caveats involving software upgrades.
7. Do not configure an entitlement change on the Oracle® Enterprise 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.

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 ESBC along with their corresponding certificate-records. To remove these certificates from your system, you must manually delete each certificate-record from your configuration.

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 3900, an upgrade from 8.4 to 9.0 (and above) may cuase an outage as the session-capacity is reset to 0 (not 8000).

Platform-Specific Downgrade Limitations

Do not attempt to downgrade your ESBC 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 ESBC, upgrade your client.

SSH Host Key Algorithms

The ESBC 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 ESBC 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.
- Release S-Cz9.3.0 does 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-Cz9.3.0

Most customers should benefit from this new 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 ESBC retains these settings in the new S-Cz9.3.0 configuration. 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 ESBC 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 S-Cz9.3.0 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 S-Cz9.3.0 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 ESBC 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, the ESBC 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 ESBC 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 ESBC version prior to version S-Cz9.3.0, and are upgrading to S-Cz9.3.0, 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 ESBC ACLI Configuration Guide.

Entitlement Caveat for MSRP B2BUA Sessions Entitlement

Before upgrading the Acme Packet 3900 platform to S-Cz9.3.0, 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.

Upgrade Configuration to Correct TON in TDM Deployments

The **calling-type-of-number** parameter in your **tdm-config** specifies the Type of Number (TON) the ESBC should specify within its signaling.

When upgrading from any version prior to 920p6 to any version after, the ESBC begins to include an incorrect type of number (TON) label in "prilocaldialplan" attribute when you have configured the value of the **calling-type-of-number** attribute in your **tdm-config** to **unknown**. Specifically, the ESBC begins to provide the value "national" instead of "unknown" as the TON. This issue occurs regardless of other configuration.

To resolve this issue, you configure the ESBC with the **default-tdm-calling-ton=unknown** option in the **system-config**.

```
ORACLE(system=config)#options +default-tdm-calling-ton=unknown
```

This change requires a reboot. You can satisfy this reboot requirement by setting the option before you upgrade, or by upgrading, setting the option, then rebooting.

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 6300, Acme Packet 6350, 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 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

Certificate Signature Algorithm

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

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-Cz9.3.0), 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-Cz9.3.0 from S-Cz9.1.0 or earlier, the ESBC converts the older **translation-rules** and **session-translation** configuration elements to their new format. Translation rules and session translations will continue to work as before. A rules-called translation rule in release S-Cz9.1.0 and earlier will be upgraded in S-Cz9.3.0 to two separate translation rules: one that modifies the To header and one that modifies the Request URI.

Fraud Protection File Rollback Compatibility

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

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

- Back up of your existing Fraud Protection configuration file before upgrading to S-Cz9.1.0 or later, and use it for previous versions of the software in a rollback scenario.

- Perform the upgrade to S-Cz9.1.0 or later, which automatically changes call-whitelist and call-blacklist to call-allowlist and call-blocklist. Before you rollback, edit your S-Cz9.1.0 Fraud Protection file by replacing call-allowlist and call-blocklist with call-whitelist and call-blacklist, respectively.

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

HA Upgrade Procedure for Deprecated Ciphers

The S-Cz9.3.0 ESBC release includes a Mocana version upgrade that generates important changes to the ciphers you should use with the ESBC. The latest Mocana 7.0 software code disables weak ciphers/algorithms used by IKE-based IPsec tunnels. Removal of these weak ciphers is mandated by Oracle Security standards. If in use, you should consider replacing deprecated ciphers in your configuration.

You use this upgrade procedure to upgrade HA nodes to S-Cz9.3.0 software image when your ESBC deployment has active IKE-based IPsec established tunnels operating with deprecated ciphers. If you have not set an entitlement for **IPsec Trunking Sessions** or if there are no **ike-config** or **ike-interface** configurations on your ESBC, then you can safely ignore this upgrade procedure. Note also that IPsec tunnels established as part of IMS-AKA feature are not affected by this deprecation and should work as it is without any service disruption.

The following ciphers are deprecated for IKE-based IPsec tunnels:

- dh-group2—Configurable under **ike-config**, **phase1-dh-mode** and **phase2-exchange-mode**
- md5 and sha—Configurable under **ike-sainfo**, **auth-algo**
- 3des and null—Configurable under **ike-sainfo**, **encryption-algo**
- esp-null—Configurable under **ike-sainfo**, **security-protocol**

Assume that HA nodes A and B are running a pre-S-Cz9.3.0 software image. Assume that node A is active and node B is a standby. Follow the steps below to perform this upgrade:

1. On the Active node (assume A), identify the IKE-based IPsec tunnels that are using the weak ciphers. You can use the **show security ike sad ike-interface <ike-interface-ip>** ACLI command for this purpose.
   Consider the following example output.

```
ORACLE#show security ike sad ike-interface 172.16.175.51
Displaying the total (1) number of entries may take long and could affect
system performance.
Continue? [y/n]?: y
Peer: 172.16.251.38:500 (NAT: No) Host: 172.16.175.51 State: Up
IKEv2 Cookies: 0x9c840a66a6225f5e[I] 0x51829548c0e451df[R] rekeying in 179
seconds
Child Peer IP: 172.16.251.38:0 Child SPI: 3487269395[I] 3402270211[O]
Protocol: ESP TUNNEL Mode rekeying in 219 seconds
```

2. From the above output, using the child SA's SPI, execute the **show security ipsec sad <network-interface:vlan> detail spi <child-SA-SPI>** command. Example, partial output is shown below.

```
Outbound SPI: 1416790526
Mirror SPI : 3719925232
source-address : 192.168.209.219
destination-address : 192.168.209.209
source-port : 0
destination-port : 0
trans-proto : any
vlan_id : 33
ipsec-protocol : ESP
** encr-algo : 3des
** auth-algo : SHA-1
sa-installation-time : 2023-11-10 01:23:40.208
sa-duration : 7838925
sa-installation-complete : 0
sa-installed-on-active : 0
tunnel-source : 192.168.209.219
tunnel-destination : 192.168.209.209
byte count limit -
hard ms: 0xFFFFFFFF, hard ls: 0xFFFFFFFF
soft ms: 0xFFFFFFFF, soft ls: 0xFFFFFFFF
time limit -
hard ms: 0x 0, hard ls : 0xFFFFFFFF
soft ms: 0x 0, soft ls: 0xFFFFFFFF
sequence number -
ms: 0x 0, ls: 0x 0
packets -
0x 0
```

From the above output, you can identify the IPsec SA's that use weak ciphers by looking at the auth-algo and encr-algo parameters, denoted with two asterisks above (**).

Once the tunnels using the weak ciphers are identified, make note of the following information such as the **ike-interface** IP of the ESBC used for the tunnel, peer IP and port, IPsec SA source and destination IP, SPI (Security Policy Identifier) and so forth.

> **Note:**
>
> Tunnels already established using stronger ciphers should not have any impact during the upgrade.

3. Load node B with the S-Cz9.3.0 image, reboot and let the node come up as a standby node.
The standby node loaded with S-Cz9.3.0 software can now show **verify-config** errors for **ike-sainfo** and **ike-config** configurations that have weak ciphers configured. You can also run the **check-upgrade-status** command to show the IKE/IPsec specific configurations that use weak ciphers. Applicable error messages from the **check-upgrade-status** or **verify-config** commands include:

   - ERROR: Security-policy [sec-pol4500] has ike-sainfo-name [ike-sainfo] which contains the following removed authentication algorithm(s): sha1

- ERROR: Security-policy [sec-pol4500] has ike-sainfo-name [ike-sainfo] which contains the following removed encryption algorithm(s): 3des
- ERROR: Security-policy [second4500] has ike-sainfo-name [secondikesa] which contains the following removed authentication algorithm(s): sha1
- ERROR: Security-policy [second4500] has ike-sainfo-name [secondikesa] which contains the following removed encryption algorithm(s): 3des

4. From the previous step, update the weaker algorithms to the stronger ones in your **ike-sainfo** and **ike-config** configurations.
   - ike-sainfo updates the IPsec SA algorithms
   - ike-config updates the IKE DH (Diffie Hellman) algorithms

   Verify your updates using the following methods:
   - Ensure that the errors reported in the **check-upgrade-status** or the **verify-config** command go away after you have updated the configurations.
   - Identify the peer node, identified in Step 1, involved in the tunnel and ensure that the peer endpoint is configured with stronger algorithms (not the ciphers deprecated at the ESBC) to avoid potential failures during the tunnel re-establishment in step 6.
   - Run the **show running-configuration ike-interface** command to identify the list of IKE interfaces configured as initiators by looking at the ike-mode parameter and identify all the tunnels used by the initiator-mode IKE interfaces from the information gathered from Step 1
5. From the information gathered from Step 1 that identifies the tunnel using weaker ciphers, on node A, execute any of the following ACLI commands to delete the existing tunnel:
   - **security ipsec delete tunnel ike-interface <ike-interface-ip> ike-peer <PeerIP:port>**
   - **security ipsec delete userId <userId> [<peer-ip-address[:Port]>]**
   - **security ipsec delete tunnel ike-interface <ip> all** (Beware this command may delete multiple tunnels)
   - **security ipsec delete tunnel destIP <ip> spi <spi>**

   Ensure that the specific tunnel using the weak ciphers is deleted on both HA nodes. This can be done by running **show security ike sad ike-interface <ike-interface-ip>** and/or the **show security ipsec sad <network-interface:vlan> detail** commands.

   > **Note:**
   >
   > When you delete the Active tunnel of weaker algorithms on node A, then incoming calls on this tunnel will fail until node B becomes the Active node using stronger algorithms.
6. Load node A with S-Cz9.3.0 and reboot. Node B becomes the Active node.
7. On the active node, perform this step only for the tunnels that have IKE interfaces configured in initiator mode using the information collected from step 3. Establish the deleted tunnels from step 4 using either of the following commands:
   - **ping <peer-ip> <network-interface:vlan> <source-ike-interface-ip>**
   - **ping <peer-ip>**

8. Verify that the new tunnel is up by executing the **show security ike sad ike-interface <ike-interface-ip>** command and/or the **show security ipsec sad <network-interface:vlan> detail** command to verify that IPsec traffic is passing through the established tunnel. For IKE interfaces that are configured as responder mode, the peer endpoint initiates the tunnel towards the ESBC.

Once node A comes up as a standby node, the system synchronizes the new tunnel(s) (with stronger algorithms) information from the Active node to the standby node. You can ensure that any tunnel is present by executing the **show security ike sad ike-interface <ike-interface-ip>** command.

Also ensure that the tunnel is properly replicated on both nodes by comparing the output of the **show security ike sad ike-interface <ike-interface-ip>** and/or the **show security ipsec sad <network-interface:vlan> detail** commands.

Optional Step

If you did not perform steps 3 through 7, here is the expected behavior:

1. The concerned IKEv2/IPsec tunnel that uses weak ciphers will work until the next (IKE or IPsec) rekey happens.
2. Once the IKE or IPsec rekey negotiation starts, it is likely that the tunnel establishment will fail during the rekey negotiation because ESBC or the peer node will attempt to negotiate weaker algorithms used during the original tunnel establishment.

You should be aware of this situation, and later update your ESBC configuration (**ike-sainfo**, **ike-config**) and, if needed, the peer configuration. Then re-establish applicable tunnels following steps 3 through 8 at your convenience.

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
Admin security	Enabled or Disabled
Advanced	Enabled or Disabled
Advanced Security Suite (JITC)	Enabled or Disabled
Data integrity (FIPS)	Enabled or Disabled
Session Capacity	Number of sessions
STIR/SHAKEN Client	Enabled or Disabled
Transcode AMR-NB	Enabled or Disabled
Transcode AMR-WB	Enabled or Disabled
Transcode EVRC	Enabled or Disabled
Transcode EVRC-B	Enabled or Disabled
Transcode EVS	Enabled or Disabled
Transcode OPUS	Enabled or Disabled
Transcode SILK	Enabled or Disabled

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

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

Feature	Type
Session Capacity	Number of sessions
Accounting	Enabled or Disabled
Load Balancing	Enabled or Disabled
Policy Server	Enabled or Disabled
STIR/SHAKEN Client	Enabled or Disabled
Admin security	Enabled or Disabled
ANSII R226 Compliance	Enabled or Disabled

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

Feature	Type
MPS Capacity	Number of sessions
Admin security	Enabled or Disabled
ANSII R226 Compliance	Enabled or Disabled
Load Balancing	Enabled or Disabled

Encryption for Virtual SBC

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

Feature	License Key
IPSec Trunking	IPSec
SRTP Sessions	SRTP
Transport Layer Security Sessions	TLS [1]
MSRP	TLS

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

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

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

Upgrading To S-Cz9.3.0 From Previous Releases

When upgrading from a previous release to S-Cz9.3.0, 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 ESBC. 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 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) - only supported on Intel CPUs	• AMR • AMR-WB • CN • EVS • G722 • G723 • G726 • G726-16 • G726-24 • G726-32 • G726-40 • G729 • G729A • iLBC • opus • PCMA • PCMU • SILK • telephone-event Note that the pooled transcoding feature on the VNF uses external transcoding ESBC, as defined in "Co-Product Support," for supported ESBC for the Transcoding-SBC (T-SBC) role.

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

TCM3 and System Software Compatibility

As of April 2023, Oracle has begun supporting new memory components for the TCM3. These components are dependent on ESBC 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 ESBC software release.

Coproduct Support

The following products and features run in concert with the ESBC 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.

Enterprise Session Border Controller

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

- Session Delivery Manager: 9.0 and later

> **Note:**
>
> To manage S-Cz9.3.0 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.

- Oracle Session Delivery Manager Cloud: 24.1 and later
- Enterprise Operations Monitor: 5.0, 5.1 and 5.2
- Interactive Session Recorder: 6.4
- Enterprise Communications Broker: 4.0, 4.1
- Security Shield

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

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

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

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

Enterprise Session Router

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

- Session Delivery Manager: 9.0 and later
- Oracle Session Delivery Manager Cloud: 24.1 and later
- Enterprise Operations Monitor: 5.0, 5.1 and 5.2

TLS Cipher Updates

Note the following changes to the DEFAULT cipher list.

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

- TLS_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_CCM_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

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

- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256

Oracle supports the following ciphers, but considers them not secure. They are not included in the DEFAULT cipher-list, but they are included when you set the **cipher-list** attribute to **ALL**. The **verify-config** command returns a warning if these ciphers are used.

- TLS_AES_128_CCM_8_SHA256 (demoted to weak in 9.3.0)
- 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

Oracle supports the following ciphers for debugging purposes only:

- TLS_RSA_WITH_NULL_SHA256
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_WITH_NULL_MD5

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

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

S-Cz9.3.0p3 TLS Cipher Updates

Release S-Cz9.3.0p3 and later removes support for weak ciphers and for previously allowed ciphers. Oracle includes only the following ciphers in the DEFAULT cipher list:

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_AES_256_GCM_SHA384
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_SHA256
- TLS_CHACHA20_POLY1305_SHA256

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

TLS 1.0 and TLS 1.1 are not supported in release S-CZ9.3.0p3 and later.

Documentation Changes

The following information describes structural changes to the documentation for the S-Cz9.3.0 release.

Behavioral Changes

The following information describes behavioral changes to the Oracle® Enterprise Session Border Controller (ESBC) for version S-Cz9.3.0.

Preconditions Handling

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

Patches Included in This Release

The following information assures you that when upgrading, the S-Cz9.3.0 release includes defect fixes from neighboring patch releases.

Neighboring Patches Included

- S-Cz900p10
- S-Cz910p9
- S-Cz920p4

Supported SPL Engines

The S-Cz9.3.0 release supports the following SPL engine versions: C2.0.0, C2.0.1, C2.0.2, C2.0.9, C2.1.0, C2.1.1, C2.2.0, C2.2.1, C2.3.2, C3.0.0, C3.0.1, C3.0.2, C3.0.3, C3.0.4, C3.0.6, C3.0.7, C3.1.0, C3.1.1, C3.1.2, C3.1.3, C3.1.4, C3.1.5, C3.1.6, C3.1.7, C3.1.8, C3.1.9, C3.1.10, C3.1.11, C3.1.12, C3.1.13, C3.1.14, C3.1.15, C3.1.16, C3.1.17, C3.1.18, C3.1.19, C3.1.20, C3.1.21.

2
New Features

The S-Cz9.3.0 release of the Oracle® Enterprise Session Border Controller (ESBC) software supports the following new features.

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

Preconditions and Multiple Early Dialog

You can configure the ESBC with the enhancement described here to overcome limitations in Multiple Early Dialogs (MED) call flows. To support the use of MED with preconditions, the ESBC implements preconditions processing at the dialog level.

See the Preconditions and Multiple Early Dialog section in the SIP Signaling Services chapter of the *ACLI Configuration Guide* for detailed information.

> **Note:**
>
> See the Caveats and Limitations Chapter of the S-Cz9.3.0 Known Issues and Caveats Guide for functional limitations of this feature that apply to this software release.

Reject Non-Emergency Traffic using Emergency DSCP

You can configure the ESBC to reject traffic that uses emergency DSCP codes to designate itself as emergency traffic. This function applies to calls from both registered and unregistered endpoints and for both UDP and TCP traffic.

See the Reject Non-Emergency Traffic using Emergency DSCP section in the SIP Signaling Services chapter of the *ACLI Configuration Guide* for detailed information.

Realm Based SIP Method Statistics for SNMP

You can configure the ESBC to generate SIP method statistics for SUBSCRIBE, NOTIFY, and MESSAGE requests on a realm basis by enabling the **snmp-sipmethod-stats** parameter in the applicable **realm-config**. These statistics are only available when you perform an SNMP WALK, GET or SNMPGETNEXT from you SNMP manager.

See the Realm Based SIP Method Statistics section in the SNMP Configuration chapter of the *MIB Guide* for detailed information.

Supporting IOI AVPs for Unregistered Endpoints

You can configure the ESBC to include the Originating-IOI and Terminating-IOI AVPs within ACRs and Diameter based CDRs for unregistered endpoints in addition to registered endpoints. Support for registered endpoints is available without special configuration. For

unregistered endpoints, you enable the **ioi-for-unregistered** option within the **account-config** element.

See the Supporting IOI AVPs for Unregistered Endpoints section in the Diameter Accounting chapter of the *Accounting Guide* for detailed information.

Suppressing Re-INVITEs for Call Hold/Resume Dialogs

You can configure the ESBC to suppress Re-INVITEs for Call Hold/Resume dialogs and REPLACES dialogs to reduce excess signaling traffic. From the perspective of the ESBC, a re-INVITE on one side of a session does not necessarily need to be forwarded to other side. When the ESBC receives a Re-INVITE that triggers, for example, a call hold, it can suppress that message from being sent out the egress and handle the transaction locally, between itself and the endstation that sent the re-INVITE. For this feature to work correctly, the applicable Hold and Resume Re-INVITEs must include SDP.

See the Suppressing Re-INVITEs for Call Hold/Resume Dialogs section in the SIP Signaling chapter of the *ACLI Configuration Guide* for detailed information.

Support of Adaptive HNT for TCP endpoints

The ESBC supports Adaptive Host NAT Traversal (AHNT) over TCP in addition to UDP. TCP AHNT configuration and behavior is largely the same as for UDP. You use **sip-interface** parameters that are equivalent to, but separate from the UDP parameters to configure Adaptive HNT for TCP.

See the Adaptive HNT over TCP section in the SIP Signaling chapter of the *ACLI Configuration Guide* for detailed information.

Incoming Request Validation

You can configure the ESBC to validate a specific set of requests and respond to these requests with the behaviors presented here when you enable the **ntt-request-valid** SPL option. This validation works using Surrogate Register SPL options within SurrogateRegister.spl and in conjunction with other NTT Message Converter SPL options. This processing compares values within the request, and only processes the call if they match. If they do not match, the ESBC replies with responses specific to each scenario.

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

Mapping SIP to HTTP Parameters

You can configure the ESBC with static mapping of signaling information to and from SIP INVITEs and HTTP requests or responses. This mapping provides a means of conveying SIP header and parameter information, including ICID information within HTTP headers and vice-versa. The HTTP exchanges can be during authentication and verification procedures. This feature applies to both ATIS and 3GPP modes.

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

> **Note:**
>
> See the Caveats and Limitations Chapter of the S-Cz9.3.0 Known Issues and Caveats Guide for functional limitations of this feature that apply to this software release.

Suppression of Subsequent 18x Messages

You can configure the ESBC to suppress some provisional 180 or 183 messages from a UAS within call-setup transactions to reduce excess signaling traffic. The system forwards only the first 180 or 183 and suppresses all of the subsequent 180 and 183 messages until it receives a 200 OK from the UAC. You configure this feature using an SPL option within the SuppressAdditionalProvisional SPL.

See the Suppression of Subsequent 18x Messages section in the SIP Signaling chapter of the *ACLI Configuration Guide* for detailed information.

Additional STUN Candidate for RTCP

You can configure the ESBC to establish a collapsed flow between itself and any STUN endpoint by enabling the **rtcp-stun** parameter in the applicable **ice-profile**. The system uses this flow for both RTP and RTCP, collapsing this traffic from two ports. As such, this configuration only applies when you have a realm supporting STUN with **rtcp-mux** disabled.

See the Additional STUN Candidate for RTCP section in the Advanced Media Termination Support chapter of the *ACLI Configuration Guide* for detailed information.

IPv4/IPv6 MSRP Packet Trace Remote Support

You can use the ESBC remote capture feature to analyze MSRP traffic, including the TCP handshake to set up connections and support MSRP traffic as well as IPv6 traffic.

See the Packet Trace Remote section in the *Monitoring Guide* for detailed information.

Disabling GARP and ND for out-of-subnet Addresses

You can configure the ESBC to limit its use of Gratuitous Address Resolution Protocol (GARP) or Network Discovery (ND). Specifically, you can prevent the system from performing this function for each **sip-interface** that is not in the same subnet as the **network-interface** on which they operate. External systems typically reach these addresses through static routes or other routing configurations, making the use of GARP and ND unnecessary for them.

See the Disabling GARP and ND for out-of-subnet Addresses section in the System Configuration chapter of the *ACLI Configuration Guide* for detailed information.

Adaptive Jitter Buffers for Transcoding Flows on vSBCs

The processing of transcoded flows on the ESBC uses an adaptive jitter buffer. This feature allows the transcoding function to adapt to changes in network conditions and packet jitter. But if necessary, the jitter buffer feature (on virtual SBC platforms only) can also be adjusted to better align to specific network conditions.

See the Adaptive Jitter Buffers for Transcoding Flows on vSBCs section in the Transcoding chapter of the *ACLI Configuration Guide* for detailed information.

Critical Memory Switchover

You can configure a high availability deployment of the ESBC to switch to the standby when the system detects memory utilization that is persistently high. Over-utilization of memory can trigger a system crash. This function reduces the risk of those crashes.

See the Critical Memory Switchover section in the System Configuration chapter of the *ACLI Configuration Guide* for detailed information.

Scheduled External Configuration Backup

You can configure the ESBC to automatically back up its current backup configuration file dataDoc.gz, which is available at /code/gzConfig/, to an external SFTP server. This feature enhances system reliability by maintaining an off-system copy of your configuration and by making restoration processes faster.

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

Oracle Enterprise Session Router Platform Support

The Acme Packet 4900 supports the Oracle Enterprise Session Router. This support begins with S-Cz9.3.0p2.

ESXI Version Support

The ESBC supports operation with ESXI version 8. This support begins with S-Cz9.3.0p2.

See the Supported Private Virtual Infrastructures and Public Clouds section in the Introduction chapter of these *Release Notes* for confirmation of this feature.

TACACS ARG Mode

When sending the Authorization query to the TACACS+ server, by default the ESBC sends everything typed at the ACLI in the cmd parameter. For commands, this includes the command plus all of its arguments (for example, cmd=show interfaces brief). For configurations, this includes the full path of the configuration element plus its attributes and values (for example, cmd=configure terminal security authentication type tacacs). In the TACACS+ query, the cmd-arg parameter is set to <cr>.

This support begins with S-Cz9.3.0p2.

See the Supported Private Virtual Infrastructures and Public Clouds section in the Introduction chapter of the *ACLI Configuration Guide* for detailed information about this feature.

Bypassing Early Media Gating

You can configure the ESBC 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 ESBC 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**.

This support begins with S-Cz9.3.0p3.

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

Concurrent Session License Usage

This feature allows the ESBC to track the maximum values of it's licensed session usage over time. Specific 'high water marks' that the system stores includes total sessions, SRTP sessions, and transcoding Sessions on a rolling 365-day period with timestamps for auditing purposes. This can inform the customer and Oracle if and when it has exceeded its licensed session usage over specific windows for up to one year. You configure this feature by setting the **peak-concurrent-license** parameter within the **system-config**.

This support begins with S-Cz9.3.0p3.

See the Concurrent Session License Usage section in the Getting Started chapter of the *ACLI Configuration Guide* for detailed information about this feature.

Account Servers over IPv6

You can configure the ESBC 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.

This support begins with S-Cz9.3.0p4.

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

AVP for the TO Header

You can configure the ESBC to support the Acme-SipHdr-TO AVP. This AVP conveys the value of TO headers in Rf deployments. The system uses this AVP to populate the string in the sipHdrTO from SIP methods into ACRs and CDRs. Enabling this feature causes the system record the SIP TO header in ACRs for all endpoints.

This support begins with S-Cz9.3.0p4.

See the Including the To Header in ACRs and CDRs section in the Getting Started chapter of this *Accounting Guide* for detailed information about this feature.

Configurations for non-Standard PT Cases

This feature adds Support for two configuration options you can use to support rare call flow issues associated with payload types. The first scenario includes non-transcoded call flow wherein a UAC presents an unexpected payload type (PT) within the context of a re-INVITE. This flow requires additional logic for the ESBC to handle the re-INVITE. The second scenario includes the ESBC handling payload types within the context of matching a **codec-policy** with traffic even though the **sub-names** are not the same. Both of these scenarios become supported when you enable their respective configuration options.

This support begins with S-Cz9.3.0p4.

See the Configurations for non-Standard PT Cases section in the Transcoding chapter of the *ACLI Configuration Guide* for detailed information about this feature.

Certificate Bundles with the REST API

Release S-Cz9.3.0p5 introduces two new APIs to manage certificate bundles:

- Import certificate bundles with the `/configuration/certificates/caBundle` endpoint.
- Get the details of certificate bundles with the `/configuration/certificates/displayBundle` endpoint.

See the REST API documentation for details.

Central Certificate Authority Management

The ESBC allows you to create trusted root Certificate Authority (CA) lists that serve as global sets of certificates for multiple TLS profiles to reference. These lists consist of **certificate-record** names representing respective CA certificates on the ESBC and can simplify certificate management by allowing you to manage these individual trusted root CA stores instead of multiple **tls-profile** elements. When you create a new certificate record, import a root CA, or when a root CA linked to a certificate record expires or is compromised, you only need to

update the applicable global trusted CA list instead of manually updating every applicable TLS profile.

This support begins with S-Cz9.3.0p5.

See the Central Certificate Authority Management section in the Security chapter of the *ACLI Configuration Guide* for detailed information about this feature.

Managing IOI for Peering Endpoints

You can configure the ESBC 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-Cz9.3.0p6.

3
Interface Changes

The following topics summarize ACLI, SNMP, HDR, Alarms, Accounting, and Error/Warning changes for S-Cz9.3.0. The additions, removals, and changes noted in these topics occurred since the previous major release of the Oracle® Enterprise Session Border Controller.

ACLI Configuration Element Changes

The following tables summarize the ACLI configuration element changes in the Oracle® Enterprise Session Border Controller S-Cz9.3.0 release.

Online Certificate Status Protocol

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

STUN Support

New Attribute	Description
media-manager, **ice-profile**, **rtcp-stun**	Enable STUN support on RTCP port

IKE/IPsec Encryption

Modified Attribute	Description
security, **ike**, **ike-config**, **phase1-dh-mode**	The value `dh-group2` is removed. The values `dh-group17` and `dh-group18` are added.
security, **ike**, **ike-config**, **phase2-exchange-mode**	The value `dh-group2` is removed. The values `dh-group17` and `dh-group18` are added.
security, **ike**, **ike-sainfo**, **security-protocol**	The value `esp-null` is removed.
security, **ike**, **ike-sainfo**, **auth-algo**	The values of `md5` and `sha1` are removed.
security, **ike**, **ike-sainfo**, **encryption-algo**	The values `null` and `3des` are removed.
security, **ipsec**, **security-association**, **manual**, **auth-algo**	The values of `md5` and `sha1` are removed.
security, **ipsec**, **security-association**, **manual**, **encr-algo**	The value of `3des` is removed.
security, **ikev2-ipsec-wancom0-params**, **ipsec-algorithms**	The value of `null` is removed from allowed ciphers and the value of `sha1` is removed from the allowed hashes.

MSRP Ports

New Attribute	Description
media-manager, **msrp-config**, **double-port-allocation**	Enable or disable using 2 steering pool ports for MSRP calls.

Realm Configuration

New Elements and Attributes	Description
media-manager, **realm-config**, **suppress-hold-resume-reinvite**	A new attribute to enable to suppress reinvites.
media-manager, **realm-config**, **snmp-sipmethod-stats**	A new attribute to enable SNMP retrieval of realm based SIP method statistics for SUBSCRIBE, NOTIFY and MESSAGE methods.
media-manager, **realm-config**, **max-inbound-per-session-burst-rate**	A new attribute to set the maximum inbound burst rate per session.
media-manager, **realm-config**, **burst-rate-window-per-session**	A new attribute to set the burst rate window per session.
media-manager, **realm-config**, **dos-action-at-session**	A new attribute to set the action to take on the session conducting a DoS attack.
media-manager, **realm-config**, **restricted-latching**	A new value of `sdp-ip-port` has been added to use the IP address and port specified in the SDP for latching.

Session Agent Configuration

New Attributes	Description
session-router, **session-agent**, **max-inbound-per-session-burst-rate**	A new attribute to set the maximum inbound burst rate per session.
session-router, **session-agent**, **burst-rate-window-per-session**	A new attribute to set the burst rate window per session.
session-router, **session-agent**, **dos-action-at-session**	A new attribute to set the action to take on the session conducting a DoS attack.
session-router, **session-agent**, **emergency-dscp-profile**	The name of the emergency DSCP profile to apply to this session agent.

SIP Configuration

New Attributes	Description
session-router, **sip-config**, **emergency-dscp-profile**	The name of the emergency DSCP profile to apply to this session agent.
session-router, **sip-config**, **precondition-med-enhancement**	Enables support for multiple early dialogs with preconditions and TrFO.
session-router, **sip-config**, **transcoding-agents**	This element no longer accepts port numbers in its list of agents.

SIP Interface

New Attributes	Description
session-router, **sip-interface**, **tcp-max-nat-interval**	The amount of time in seconds that testing over TCP connections should not exceed for adaptive HNT.
session-router, **sip-interface**, **tcp-nat-int-increment**	The amount of time in seconds to use as the increment in value in the SIP expires header for adaptive HNT testing for TCP connections.
session-router, **sip-interface**, **tcp-nat-test-increment**	The amount of time in seconds that will be added to the test timer for adaptive HNT testing for TCP connections.
session-router, **sip-interface**, **tcp-sip-dynamic-hnt**	Enables dynamic hosted NAT traversal feature for connections using TCP as the transport protocol.
session-router, **sip-interface**, **emergency-dscp-profile**	Specifies the name of the emergency DSCP profile you want to apply to this sip-interface.

Schedule Backups

New Elements and Attributes	Description
system, **system-config**, **schedule-backup**	A new element to configure automatic backups.
system, **system-config**, **schedule-backup**, **admin-state**	A new attribute to enable or disable all automatic backups.
system, **system-config**, **schedule-backup**, **config-backup**	A new element to configure the attributes for an automatic backup.
system, **system-config**, **schedule-backup**, **config-backup**, **admin-state**	A new attribute to enable or disable this specific backup.
system, **system-config**, **schedule-backup**, **config-backup**, **interval**	Set how often the ESBC backs up the configuration.
system, **system-config**, **schedule-backup**, **config-backup**, **retry-interval**	The length in minutes after which the ESBC will retry backing up the configuration if the previous attempt failed.
system, **system-config**, **schedule-backup**, **config-backup**, **retry-count**	The number of times which the ESBC will try to backup the configuration when repeated attempts fail.
system, **system-config**, **schedule-backup**, **config-backup**, **push-failure-alarm**	Enable or disable generating an alarm and trap when the backup attempt failed.
system, **system-config**, **schedule-backup**, **config-backup**, **push-receiver**	The configuration element where you set the connection details of the push receiver. This is a multi-instance configuration element.
system, **system-config**, **schedule-backup**, **config-backup**, **push-receiver**, **address**	The IPv4 address of the SFTP server to which the ESBC will push the backups.
system, **system-config**, **schedule-backup**, **config-backup**, **push-receiver**, **user-name**	The user name that the ESBC will use to log in to the SFTP server.
system, **system-config**, **schedule-backup**, **config-backup**, **push-receiver**, **password**	The password that the ESBC will use to authenticate to the SFTP server.
system, **system-config**, **schedule-backup**, **config-backup**, **push-receiver**, **data-store**	The directory on the SFTP server where the ESBC will copy the backup configuration files.
system, **system-config**, **schedule-backup**, **config-backup**, **push-receiver**, **protocol**	The protocol that the ESBC will use when connecting to the SFTP server.

SSH Configuration

Modified Attributes	Description
security, **ssh-config**, **hostkey-algorithms**	The values of `ssh-rsa` and `ssh-dss` have been replaced with the values of `rsa-sha2-256` and `rsa-sha2-512`.
security, **ssh-config**, **encr-algorithms**	The following values are removed: `aes256-cbc`, `aes192-cbc`, `aes128-cbc`, `rijndael256-cbc`, `rijndael192-cbc`, `rijndael128-cbc`, and `3des-cbc`

STI Configuration

New or Modified Attributes	Description
session-router, **sti-config**, **sti-response-treatment-config-name**	The name of the sti-response-treatment-config to apply to this sti-config.
session-router, **sti-config**, **max-retry-attempts**	The number of attempts the system tries sending a request to a new sti-server within the sti-server-group unless a server responds or sip transaction times out.
session-router, **sti-header-mapping-ruleset**, **mapping-rules**, **source-param**	The SIP or HTTP header parameter based on the source header.
session-router, **sti-header-mapping-ruleset**, **mapping-rules**, **target-param**	The SIP or HTTP header parameter based on the target header.
session-router, **sti-heartbeat-config**	A new element to define operational parameters for the heartbeat that monitors the availability of the STIR/SHAKEN servers.
session-router, **sti-response-treatment-config**	A new element to create containers for response-treatment-entry sub-elements.
session-router, **sti-response-treatment-config**, **sti-response-treatment-entry**	A new element to define global or specific STI server rules.
session-router, **sti-server-group**, **strategy**	The values `LeastBusy` and `PropDist` are deprecated.
session-router, **sti-server**, **sti-response-treatment-config-name**	A new attribute for the name of the STI response treatment.

System Configuration

Modified Attributes	Description
system, **system-config**, **disable-garp-out-of-subnet**	A new attribute to prevents the system from sending out any GARP or ND query for sip-interfaces that are not in the same subnet of each network-interface.
system, **system-config**, **httpclient-cache-size-multiplier**	A new attribute to store the connection cache multiplier value.
system, **system-config**, **http-clearDead-conn-timer**	The time interval in seconds for clearing dead connections.
system, **system-config**, **resource-monitoring**	A new element for configuring resource monitoring.

S-Cz9.3.0p2 Changes

These changes are present in S-Cz9.3.0p2 and later.

Modified Attributes	Description
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, **ike**, **ike-key-id**	Adds a new attribute **id-type**.
security, **ike**, **ike-sainfo**	Adds a new attribute **remote-id-profile**.
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**.

S-Cz9.3.0p3 Changes

These changes are present in S-Cz9.3.0p3 and later.

Modified Attributes	Description
security, **certificate-record**, **key-algor**	Adds the value **rsapss**.
system, **system-config**, **collect**, **group-settings**, **group-name**	Adds the value **latest-peak-license-usage**.
security, **ike**, **ike-config**, **eap-protocol**	Removes the value **eap-md5**.
security, **ike**, **ike-interface**, **eap-protocol**	Removes the value **eap-md5**.
security, **ike**, **ike-sainfo**, **auth-algo**	Removes the value **aes-xcbc**.
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**.
system, **system-config**	Adds a new attribute **peak-concurrent-license**.

ACLI Command Changes

The following table summarizes the ACLI command changes in the Oracle® Enterprise Session Border Controller S-Cz9.3.0 release.

This table lists and describes changes to ACLI commands that are available in the S-Cz9.3.0 release.

New Commands	Description
clear-cache registration sipd expired-contacts [all | by-aor]	Clear all expired contacts from the cache.
clear-resourcemonitor-actions	Clear the actions taken by the resource monitor.
reset stir heartbeat	Reset the heartbeat statistics for STIR.
show stir heartbeat [sti-server]	Show heartbeat statistics for all or a specified STI server.
show datapath xcode [switch fdb-entries | port-stats-all | port-stats | drop-count | all]	New datapath options
show smt stats	Display SMT statistics

New Commands	Description
show security x509 [brief | detail]	View the X.509 certificates on systems that enabled the Admin Security entitlement.
ssh-key x509 <delete | import> <name>	Manage X.509 certificates on systems that enabled the Admin Security entitlement.
check-upgrade-status	Check the readiness of your system to upgrade to a new version.

SSH Keys

These changes are present in S-Cz9.3.0p3 and later.

Modified Commands	Description
ssh-key	The ssh-key command no longer allows you to import DSA keys.

Accounting Changes

The following information summarizes the accounting changes in the Oracle® Enterprise Session Border Controller S-Cz9.3.0 release.

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

The following accounting AVPs have been added in this release:

- Stir-VS-Invite-State

SNMP/MIB Changes

The following information summarizes the SNMP MIB changes in the Oracle® Enterprise Session Border Controller S-Cz9.3.0 release.

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

MIBs

The following new MIBs are added in this release:

- apAppsSchBkpNotificationGroupTrapCap / 1.3.6.1.4.1.9148.2.1.21.19
- apAppsConfigPushReceiverAddress / 1.3.6.1.4.1.9148.3.15.7.1.1.2
- apAppsConfigPushReceiverAddressType / 1.3.6.1.4.1.9148.3.15.7.1.1.1
- apAppsConfigPushReceiverFailureReasonCode / 1.3.6.1.4.1.9148.3.15.7.1.1.3
- apAppsResrvdNsepSessionCapacity / 1.3.6.1.4.1.9148.3.16.8.1.1
- apAppsResrvdNsepSessUtlObjects / 1.3.6.1.4.1.9148.3.16.8.1
- apAppsResrvdNsepUtlObjects / 1.3.6.1.4.1.9148.3.16.8
- apAppsSchBkpNotifications / 1.3.6.1.4.1.9148.3.15.7.1
- apAppsSchBkpNotificationsPrefix / 1.3.6.1.4.1.9148.3.15.7.1.0
- apAppsSchBkpObjects / 1.3.6.1.4.1.9148.3.15.7.1.1
- apAppsSchBkpUtil / 1.3.6.1.4.1.9148.3.15.7

- apAppsStirNotificationGroups / 1.3.6.1.4.1.9148.3.16.3.2.7
- apAppsStirNotificationsGroup / 1.3.6.1.4.1.9148.3.16.3.2.7.1
- apDosThresholdNotificationObjects / 1.3.6.1.4.1.9148.3.16.6
- apSchBkpNotificationGroups / 1.3.6.1.4.1.9148.3.15.3.2.7
- apSchBkpNotificationsGroup / 1.3.6.1.4.1.9148.3.15.3.2.7.1
- apSipRealmEntry / 1.3.6.1.4.1.9148.3.15.1.2.11.1.1
- apSIPRealmIndex / 1.3.6.1.4.1.9148.3.15.1.2.11.1.1.1
- apSipRealmMethodStatsEntry / 1.3.6.1.4.1.9148.3.15.1.2.11.2.1
- apSipRealmMethodStatsEventCode / 1.3.6.1.4.1.9148.3.15.1.2.11.2.1.4
- apSipRealmMethodStatsEventCount / 1.3.6.1.4.1.9148.3.15.1.2.11.2.1.5
- apSipRealmMethodStatsGroup / 1.3.6.1.4.1.9148.3.15.3.1.13
- apSipRealmMethodStatsGroupCap / 1.3.6.1.4.1.9148.2.1.21.18
- apSipRealmMethodStatsIndex / 1.3.6.1.4.1.9148.3.15.1.2.11.2.1.2
- apSipRealmMethodStatsTable / 1.3.6.1.4.1.9148.3.15.1.2.11.2
- apSipRealmMethodStatsTransType / 1.3.6.1.4.1.9148.3.15.1.2.11.2.1.3
- apSipRealmMIBTabularObjects / 1.3.6.1.4.1.9148.3.15.1.2.11
- apSIPRealmName / 1.3.6.1.4.1.9148.3.15.1.2.11.1.1.2
- apSipRealmStatsIndex / 1.3.6.1.4.1.9148.3.15.1.2.11.2.1.1
- apSipRealmTable / 1.3.6.1.4.1.9148.3.15.1.2.11.1
- hcnumTC / 1.3.6.1.2.1.78

The following MIBs were changed:

- apAppsStirNotificationGroups — The last OID number changed from 5 to 7.
- ApStirStatsType—Added vsInviteRejected as integer 26, and moved apStirStatsTypeMax from 26 to 27.

Traps

The following traps are added in this release:

- apConfigPushReceiverFailureTrap / 1.3.6.1.4.1.9148.3.15.7.1.0.1

The following traps were modified:

- apSysMgmtAuthenticationFailedTrap / 1.3.6.1.4.1.9148.3.2.6.0.16—Added the values of http and https.

SNMP for STIR/SHAKEN

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

- vsInviteRejected / Object available from STIR/SHAKEN SNMP walk tables, including the apAppsStirServerTable, apAppsStirAgentStatsTable, apAppsStirSipInterfaceStatsTable, apAppsStirRealmStatsTable and apAppsStirSystemStatsTable.

For example, the tabular object apStirServerStats instance that has an OID of the form apStirServerStats.x.y.26, where:

- apStirServerStats is 1.3.6.1.4.1.9148.3.16.1.2.4.2.1.4;
- x is the stir server's object ID/index;
- y is the ApCounterStatsType (recent (1), total (2), or permax (3)
- 26 is the data category, (In this example, "vsInviteRejected")

SNMP for Realm Based SIP Method Statistics

The existing SIP Method statistics are available, after configuration, on a per-realm basis. The applicable OIDs use the same prefix as the system-wide statistics, 1.3.6.1.4.1.9148.3.15.1.2 under the package apSipRealmTable. The system nests the realm-based statistics under the package apSipRealmMethodStatsTable, completing each individual OID using the identifier and variables 11.2.1.5.X1.X2.X3.X4, with the variables enumerating specific statistics:

- X1 ranges from 1 to n, where n is the number of configured realms, enumerated within apSIPRealmIndex. Perform an SNMPWALK on 1.3.6.1.4.1.9148.3.15.1.2.11.1.1.2 to list the values of X1.
- X2 values are 9,10 and 13, which enumerate the SIP Method types SUBSCRIBE (9), NOTIFY (10) and MESSAGE (13).
- X3 ranges from 1 to 2, which enumerate the transaction types, including Server Transaction (1) and Client Transaction (2), which are the contents of ApSipMethodTransType.
- X4 ranges from 1 to 57, which enumerates the event code types within ApSipMethodEventCode.

See the Realm Based SIP Method Statistics section in the *MIB Guide* for additional explanation.

Alarms

The following information summarizes the alarm changes in the Oracle® Enterprise Session Border Controller S-Cz9.3.0 release.

Scheduled Backups

This version of the ESBC introduces the **APP_ALARM_SCHBKP_PUSH_FAIL** alarm, which notifies you if a scheduled backup process has failed.

HDR

The following information summarizes the accounting changes in the Oracle® Enterprise Session Border Controller S-Cz9.3.0 release.

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

The following field is added to the **ACLI_Group_sip-errors** and **Group survivability-sip-errors** HDR output groups to support the "Reject Non-Emergency Traffic using Emergency DSCP" feature.

- Drop Unauth NSEP DSCP—Total number of messages dropped because of improper use of DSCP.

Errors and Warnings

The following errors and warnings are new in this release.

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