Oracle® Communications Session Border Controller and Session Router

Release Notes

Release S-Cz9.1.0

F51849-12

June 2024

Oracle Communications Session Border Controller and Session Router Release Notes, Release S-Cz9.1.0

F51849-12

Contents

About this Guide

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

Documentation Set

The following table lists related documentation.

Document Name	Document Description
Acme Packet 3900 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 3900.
Acme Packet 4600 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4600.
Acme Packet 4900 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 3950 and Acme Packet 4900.
Acme Packet 6100 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6100.
Acme Packet 6300 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6300.
Acme Packet 6350 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6350.
Release Notes	Contains information about the current documentation set release, including new features and management changes.
Known Issues & Caveats	Contains known issues and caveats
Configuration Guide	Contains information about the administration and software configuration of the Service Provider Session Border Controller (SBC).
ACLI Reference Guide	Contains explanations of how to use the ACLI, as an alphabetical listings and descriptions of all ACLI commands and configuration parameters.
Maintenance and Troubleshooting Guide	Contains information about SBC logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
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.

Document Name	Document Description
Accounting Guide	Contains information about the SBC's accounting support, including details about RADIUS and Diameter accounting.
HDR Guide	Contains information about the SBC's Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Admin Security Guide	Contains information about the SBC's support for its Administrative Security license.
Security Guide	Contains information about security considerations and best practices from a network and application security perspective for the SBC family of products.
Platform Preparation and Installation Guide	Contains information about upgrading system images and any pre-boot system provisioning.
Call Traffic Monitoring Guide	Contains information about traffic monitoring and packet traces as collected on the system. This guide also includes WebGUI configuration used for the SIP Monitor and Trace application.
HMR Guide	Contains information about configuring and using Header Manipulation Rules to manage service traffic.
REST API	Contains information about the supported REST APIs and how to use the REST API interface.

Documentation Accessibility

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

My Oracle Support

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

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

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

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

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

Emergency Response

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

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

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

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

Locate Product Documentation on the Oracle Help Center Site

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

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

Access to Oracle Support

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

Revision History

This section provides a revision history for this document.

Date	Revision
March 2022	• Initial release.
August 2022	• Updated New Features section to include resetting local account passwords. • Adds DH key size upgrade caveat. • Adds surrogate-agent upgrade caveat. • Adds New Features and updates for the S-Cz9.1.0p2 software release. • Corrects Ethernet Controller model XXV710 in "Supported Platforms."
October 2022	• Updates "Supported Private Virtual Infrastructures and Public Clouds" and "Supported Ethernet Controller, Driver, and Traffic Type based on Input-Output Modes" with a note about media interface support. • Clarifies the requirement for media-policy for setting all DSCP codes on egress • Adds New Features and updates for the S-Cz9.1.0p3 software release.
December 2022	• Updates HOT and Terraform boot files for S-Cz9.1.0p2.
February 2023	• Adds the Reason Attestation and SIP to HTTP Header Mapping features at S-Cz9.1.0p5.
May 2023	• Corrects Header Customization feature title. • Adds PSAP callback and Pooled transcoding features at S-Cz9.1.0p6. • Adds support for iavf driver for intel x7xx series cards. • Corrects transcodable codec list for vSBCs. • Updates Upgrade Information for accuracy.
July 2023	• Adds TDM support for Digium cards. • Adds SDM Upgrade Caveat. • Adds TCM-3 update content at S-Cz9.1.0p7 • Adds Session Router entitlement tables.
September 2023	• Adds steering pool feature at S-Cz9.1.0p8.

Date	Revision
November 2023	• Adds VMWare upgrade details. • Adds Intel limitation for software transcoding. • Adds the httpclient-cache-size-multiplier parameter at S-Cz9.1.0p9. • Adds verstat-delimiter as feature, valid from S-Cz9.1.0p6. • Clarifies XSD copy in Co-Product Support. • Adds Upgrade Caveat on certificate regeneration for wancom interfaces.
February 2024	• Adds new features at S-Cz9.1.0p10.
April 2024	• Updates ACLI Configuration Element Changes to include "Updates to the STI Server Group". • Adds EVS limitation for AP4900. • Adds behavioral change about SSH keys in HA.
June 2024	• Adds Acme Packet 3900 Platform to Upgrade and Downgrade Caveats.

1

Introduction to S-Cz9.1.0

The Oracle Communications Session Border Controller *Release Notes* provides the following information about the S-Cz9.1.0 release:

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

Supported Platforms

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

Supported Physical Platforms

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

The S-Cz9.1.0 version of the OCSBC supports the following platforms:

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

The S-Cz9.1.0 version of the OCSR supports the following platforms:

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

Supported Private Virtual Infrastructures and Public Clouds

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

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

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

Supported Hypervisors for Private Virtual Infrastructures

Oracle supports installation of the SBC on the following hypervisors:

- KVM: Linux kernel version (3.10.0-123 or later), with KVM/QEMU (2.9.0_16 or later) and libvirt (3.9.0_14 or later)
- VMware: vSphere ESXi (Version 6.5 or later)
- 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, nnSCZ910_HOT.tar.gz, and follow the OpenStack Heat Template instructions.

You extract two files from this source, including:

- nnSCZ910_HOT_pike.tar
- nnSCZ910_HOT_newton.tar

Use the Newton template when running either the Newton or Ocata versions of OpenStack. Use the Pike template when running Pike or a later version of OpenStack.

Supported Public Cloud Platforms

You can run the SBC on the following public cloud platforms.

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

Shape	OCPUs/ VCPUs	vNICs	Tx/Rx Queues	Max Forwarding Cores	DoS Protection	Memory
VM.Standard2.4	4/8	4	2	2	Y	60
VM.Standard2.8	8/16	8	2	2	Y	120

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

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

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

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

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

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

  Driver support detail includes:

  – ENA is supported on C5/C5n family only.

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

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

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

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

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

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

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

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

Platform Hyperthreading Support

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

DPDK Reference

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

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

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

The DPDK version used in this release is:

- 20.11

As of version S-Cz9.1.0p2, the DPDK version used in this release is:

- 21.11

Requirements for Machines on Private Virtual Infrastructures

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

Default vSBC Resources

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

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

Interface Host Mode for Private Virtual Infrastructures

The SBC VNF supports interface architectures using Hardware Virtualization Mode - Paravirtualized (HVM-PV):

- ESXi - No manual configuration required.
- KVM - HVM mode is enabled by default. Specifying PV as the interface type results in HVM plus PV.

Supported Interface Input-Output Modes for Private Virtual Infrastructures

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

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

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

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

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

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

1 This driver is supported on VMware only.

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

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

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

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

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

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

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

CPU Core Resources for Private Virtual Infrastructures

Virtual SBCs for this release requires an Intel Core i7 processor or higher, or a fully emulated equivalent including 64-bit SSSE3 and SSE4.2 support.

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

PCIe Transcoding Card Requirements

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

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

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

Oracle Communications Session Router Recommendations for Oracle Servers

Oracle recommends the following resources when operating the OCSR, release S-Cz9.1.0 over Oracle Platforms.

Hardware recommendations for Oracle Server X7-2

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

Hardware recommendations for Oracle Server X8-2

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

Image Files and Boot Files

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

Acme Packet Platforms

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

- Image file: `nnSCZ910.bz`

- Bootloader file: `nnSCZ910.boot`

Virtual Platforms

This S-Cz9.1.0 release includes distributions suited for deployment over hypervisors. Download packages contain virtual machine templates for a range of virtual architectures. Use the following distributions to the Session Border Controller as a virtual machine:

- `nnSCZ910-img-vm_kvm.tgz`—Compressed image file including SBC VNF for KVM virtual machines, Oracle Cloud Infrastructure (OCI), EC2, EC2 Nitro, and AWS C4 and C5 instances.
- `nnSCZ910-img-vm_vmware.ova`—Open Virtualization Archive (.ova) distribution of the SBC VNF for ESXi virtual machines.
- `nnSCZ900-img-vm_vhd.tgz`—Compressed image file including SBC for Hyper-V virtual machine on Windows and Azure.
- `nnSCZ910p2_HOT.tar.gz`—The Heat Orchestration Templates used with OpenStack.
- `nnSCZ910p2_tfStackBuilder.tar.gz`—The Terraform templates used to create an AWS AMI and for deployment via the OCI resource manager.

Each virtual machine package includes:

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

Oracle Platforms for Session Router and Enterprise Session Router

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

- Image file: `nnSCZ910.bz`
- Bootloader file: `nnSCZ910.boot`

Image Files for Customers Requiring Lawful Intercept

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

All subsequent patches follow naming conventions with the LI modifier.

Boot Loader Requirements

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

Setup Product

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

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

1. Type **setup product** at the ACLI.

   If this is the first time running the command on this hardware, the product will show as Uninitialized.
2. Select **1** to modify the product.
3. Select the number next to the product you wish to initialize.
4. Type **s** to save your choice as the product type of this platform.
5. Reboot your system.

```
ORACLE# setup product

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

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

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

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

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

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

Upgrade Information

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

Supported Upgrade Paths

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

- SCZ830m1p15B to S-Cz9.1.0
- S-Cz8.4.0p9 to S-Cz9.1.0
- S-Cz9.0.0 to S-Cz9.1.0

You can upgrade the OCSBC, OESBC and the OCSR using the following upgrade and rollback paths, but these paths are not hitless:

- S-Cz8.1.0 to S-Cz9.1.0
- S-Cz8.2.0 to S-Cz9.1.0
- SCZ830m1p10 and patches up to SCZ830m1p15B, to S-Cz9.1.0
  If you require a hitless upgrade for an HA deployment running SCZ830 or later SCZ830 patches to S-Cz9.1.0, you must first upgrade to SCZ830m1p15B. Standalone deployments of these versions do not require this interim upgrade.
- S-Cz8.4.0 and patches up to S-Cz8.4.0p9 to S-Cz9.1.0
  If you require a hitless upgrade for an HA deployment running between SCZ840 and S-Cz840p8 to S-Cz9.1.0, you must first upgrade to S-Cz8.4.0p9. Standalone deployments of these versions do not require this interim upgrade.

> **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 X5-2 to Oracle Server X7-2.

When upgrading to this release from a release older than the previous release, read all intermediate *Release Notes* for notification of incremental changes.

Upgrade Checklist

Before upgrading the Oracle Communications Session Border Controller software:

1. Obtain the name and location of the target software image file from either Oracle Software Delivery Cloud, https://edelivery.oracle.com/, or My Oracle Support, https://support.oracle.com, as applicable.
2. Provision platforms with the Oracle Communications Session Border Controller image file in the boot parameters.

3. Run the **check-upgrade-readiness** command and examine its output for any recommendations or requirements prior to upgrade.
4. Verify the integrity of your configuration using the ACLI **verify-config** command.
5. Back up a well-working configuration. Name the file descriptively so you can fall back to this configuration easily.
6. Refer to the Oracle Communications Session Border Controller Release Notes for any caveats involving software upgrades.
7. Do not configure an entitlement change on the Oracle Communications Session Border Controller while simultaneously performing a software upgrade. These operations must be performed separately.

Upgrade and Downgrade Caveats

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

Acme Packet 3900 Platform

When you upgrade software, if the session-capacity is configured to a value greater than the 8000 supported sessions on the 3900, an upgrade from 8.4 to 9.0 (and above) may cause an outage as the session-capacity is reset to 0 (not 8000).

Acme Packet 4900 and 3950 Platforms

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

Upgrading from releases earlier than S-Cz8.4.0

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

Upgrading to S-Cz9.1.0 with IKEv2 LI Tunnels

An HA upgrade to S-Cz9.1.0, when configured with LI Tunnels using IKEv2, can cause IPSec tunnels to fail if an IPsec rekey initiated from a peer has resulted in the IPSec SAs being out of sync across the HA pair. After an upgrade with these conditions, these LI tunnels do not function on the Active node.

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

- If they are in sync, proceed with the upgrade.
- If the IPsec SA's are not in sync across the HA nodes, perform the following procedure:
  1. If enabled, disable **x2-keep-alive** from the LI shell. (See procedures in LI documentation.)
  2. Upgrade the Standby node to S-Cz9.1.0.
  3. Wait until the pair reaches HA state.

4. Configure the Active node to boot to S-Cz9.1.0. (Do not reboot this device yet.)
5. Delete tunnels on the Active node, which is still running the older software version, using one of the following commands from the CLI root.

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

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

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

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

7. Reboot the Active node.
8. If the IKE interface is in INITIATOR mode, execute the **ping** command to the applicable IPSec endpoints on the newly Active (S-Cz9.1.0) node to establish new tunnels.
   If the IKE interface is in RESPONDER mode, have peers restart tunnels instead of executing the **ping** command.
9. Upon completion of boot cycle of the standby node, verify HA state and proper tunnel synchronization.

Two downgrade procedures are presented below.

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

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

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

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

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

   f. Reboot the Active node.
   g. If the IKE interface is in INITIATOR mode, execute the ping command to the applicable IPSec endpoints on the newly Active (Downgraded) node to establish new tunnels.
   If the IKE interface is in RESPONDER mode, have peers restart tunnels instead of executing the ping command.
   h. Upon completion of boot cycle verify HA state and proper tunnel synchronization.
2. Rollback after Upgrading the active node only:

a. HA pair is in highly available state with Active node 9.1.0 and Standby node with old version
b. Configure boot table on Active node with rollback version
c. Delete tunnels on the Active node using one of the following commands from the CLI root.

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

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

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

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

e. Reboot the Active node.
f. If the IKE interface is in INITIATOR mode, execute the ping command to the applicable IPSec endpoints on the newly Active node to establish new tunnels.
If the IKE interface is in RESPONDER mode, have peers restart tunnels instead of executing the ping command.
g. Upon completion of boot cycle of verify HA state and proper tunnel synchronization

Connection Failures with SSH/SFTP Clients

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

TSCF Configurations from Prior Software Versions

A TSCF configuration that was present on your system before upgrade to this S-Cz9.1.0 release and above, which do not support TSM, may still be present in the configuration file if you do not remove it manually before upgrade. The system does not apply these TSCF configurations on a non-TSM release.

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

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

Acme Packet 3950/4900 Slots

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

Diffie-Hellman Key Size

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

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

Encrypting the Surrogate Agent Password

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

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

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

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

5. Upgrade the release on the new standby SBC.

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

Upgrade Version Caveat from Session Delivery Manager

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

VMWare Virtual Machines

In versions prior to S-Cz9.0.0, VMWare virtual machines used the e1000 driver for management interfaces and the VmxNet3 driver for media interfaces. Versions S-Cz9.0.0 and later use VmxNet3 driver for all interfaces.

New Keys Required for High Availability

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

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

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

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

Fraud Protection File Rollback Compatibility

As of the S-Cz9.1.0 release, Oracle changed some of the Oracle Communications Session Border Controller (SBC) Fraud Protection file list type names to eliminate certain culturally undesirable terms and replace them with more acceptable terms. The changes impact your Fraud Protection file with consequences in rollback scenarios.

As of the S-Cz9.1.0 release, the upgrade process automatically changes the former Fraud Protection list types named call-whitelist and call-blacklist to call-allowlist and call-blocklist.

In a rollback scenario, Fraud Protection does not support the call-allowlist and call-blocklist list types in previous versions of the software. 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-Cz 9.1.0, and use it for previous versions of the software in a rollback scenario.
- Perform the upgrade to S-Cz9.1.0, 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 again. The upgrade process makes the changes automatically.

Fraud Protection File Upgrade Compatibility

As of the S-Cz9.1.0 release, Oracle changed some of the Oracle Communications Session Border Controller (SBC) Fraud Protection file list type names to eliminate certain culturally undesirable terms and replace them with more acceptable terms.

Previous versions of the Fraud Protection file included list types named call-whitelist and call-blacklist. The upgrade process automatically modifies the Fraud Protection file by changing the former names to call-allowlist and call-blocklist. The file is located in /code/fpe/directory with file extensions .xml. .gz, or .gzip.

The upgrade process does not delete the existing file and replace it with a new one. The upgrade changes only the list type names within the existing file.

Note that previous versions of the Fraud Protection software do not support the new list type names and you must take action to ensure compatibility in a rollback scenario. See Fraud Protection File Rollback Compatibility for information about what to do in a rollback scenario.

Feature Entitlements

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

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

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

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

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

Feature	Type
Lawful Intercept	boolean
R226 SIPREC	boolean

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

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

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

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

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

Encryption for Virtual SBC

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

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

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

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

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

Upgrading To S-Cz9.1.0 From Previous Releases

When upgrading from a previous release to S-Cz9.1.0, your encryption entitlements carry forward and you do not need to install a new license key.

System Capacities

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

SIP Interface and Realm Limits for vSBC

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

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

Static Trusted and Untrusted ACL Limits for vSBC

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

- Between 8GB and 64GB, supported entries include:
  - Trusted static ACLs is 1024 per GB
  - Untrusted static ACLs is 512 per GB
- Greater than 64GB, supported entries include:
  - Trusted static ACLs is 65536
  - Untrusted static ACLs is 32768

Dynamic ACL entries are independent of this support.

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

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 • EVRC0 • EVRC • EVRC1 • EVRCB0 • EVRCB • EVRCB1 • EVS[1] • G711FB • G722 • G723 • G726 • G726-16 • G726-24 • G726-32 • G726-40 • G729 • G729A • GSM • iLBC • Opus • SILK • PCMU • PCMA • T.38 • T.38OFD • telephone-event • TTY, except on the Acme Packet 1100

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 • SILK • PCMU • PCMA • telephone-event Note that the pooled transcoding feature on the VNF uses external transcoding SBC, as defined in "Co-Product Support," for supported SBC for the Transcoding-SBC (T-SBC) role.

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

Coproduct Support

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

Oracle Communications Session Delivery Manager

This S-Cz9.1.0 SBC GA release can interoperate with the following versions of the Oracle Communications Session Delivery Manager:

- 8.2.4

> **Note:**
>
> Customers wishing to manage S-Cz9.1.0 patches in conjunction with Oracle's Session Delivery Manager must review the build notes to determine if an XSD file is required. In addition, please review the readme file in the XSD file for confirmation. XSD files may work with older OCSDM releases, though not guaranteed.

Oracle Session Delivery Manager Cloud

This S-Cz9.1.0 SBC release can interoperate with the following versions of the Oracle Session Delivery Manager Cloud:

- 20.5.0 and higher

Oracle Communications Operations Manager

This S-Cz9.1.0 SBC release can interoperate with the following versions of the Oracle Communications Session Monitor:

- 4.3.0
- 4.4.0
- 5.0.0

Oracle Communications Subscriber Aware Load Balancer

This S-Cz9.1.0 SBC release can interoperate as a cluster member with the following versions of the Subscriber Aware Load Balancer (SLB):

- S-Cz8.4.0
- S-Cz9.0.0
- S-Cz9.1.0

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

Oracle Communications Session Router

This S-Cz9.1.0 SBC release can interoperate with the following versions of the Session Router:

- S-Cz8.3.0
- S-Cz8.4.0
- S-Cz9.0.0
- S-Cz9.1.0

Pooled Transcoding

This S-Cz9.1.0 SBC release acting as an A-SBC can interoperate with T-SBCs on the following hardware/software combinations :

- Acme Packet 4500: S-Cz7.4.0
- Acme Packet 4600: S-Cz8.3.0, S-Cz8.4.0, S-Cz9.0.0 , S-Cz9.1.0
- Acme Packet 6300: S-Cz8.3.0, S-Cz8.4.0, S-Cz9.0.0 , S-Cz9.1.0
- Acme Packet 6350: S-Cz8.3.0, S-Cz8.4.0, S-Cz9.0.0 , S-Cz9.1.0
- Virtual Platforms with Artesyn SharpMedia™: S-Cz8.2.0, S-Cz8.3.0, S- Cz8.4.0, S-Cz9.0.0 , S-Cz9.1.0

This S-Cz9.1.0 SBC release acting as a T-SBC can interoperate with A-SBCs on the following hardware/software combinations:

- All platforms supported by the following releases: S-Cz8.3.0, S-Cz8.4.0, S-Cz9.0.0 , S-Cz9.1.0
- Acme Packet 4500 running S-Cz7.4.0

Session Routers and SDM

This S-Cz9.1.0 release of the Oracle Communications Session Router and Enterprise Session Router can interoperate with the following versions of the Oracle Communications Session Delivery Manager:

- 8.2.4 and above

Session Routers and Operations Manager

This S-Cz9.1.0 release of the Oracle Communications Session Router and Enterprise Session Router can interoperate with the following versions of the Oracle Communications Operations Manager:

- 4.3.0
- 4.4.0
- 5.0.0

TLS Cipher Updates

Note the following changes to the DEFAULT cipher list.

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

- TLS_ECDHE_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_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_AES_128_GCM_SHA256

Oracle supports the following ciphers for debugging purposes only:

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

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

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA

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

WARNING:

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

Note:

The default is TLSv1.2. Oracle supports TLS1.0 and TLS1.1 for backward compatibility only and they may be deprecated in the future.

Documentation Changes

The following information describes structural changes to the documentation for the S-Cz9.1.0 release.

Service Provider Session Border Controller

The Service Provider documentation contains no notable changes.

Behavioral Changes

This section presents behavioral changes to the SBC for version S-Cz9.1.0.

TOS Configuration

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

NPLI for Unregistered Emergency VoLTE Calls

With the 'NPLI for Unregistered Emergency VoLTE Calls' feature, new in this version, the SBC adds a new behavior when configured with the **location-optimization-on-aar** option. Specifically, the SBC adds NPLI AVP's only to the first AAR for volte unregistered emergency MO calls. This is the same behavior the SBC previously used for registered subscriber flows only.

See the NPLI section in the External Policy Servers chapter in the *ACLI Configuration Guide*.

STIR/SHAKEN Implementation Enhancements

With the new 'STIR/SHAKEN Implementation Enhancements' feature in this version, the SBC, by default, only sends signing and verification requests if there is a TN in the FROM header or PAI headers of the SIP request.

See the STIR/SHAKEN Client chapter in the *ACLI Configuration Guide* for detail on these enhanced processes.

SSH Keys for HA

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

An example of the known-host keys:

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

An example of the authorized-keys:

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

Patches Included in This Release

The following information assures you that when upgrading, the S-Cz9.1.0 release includes defect fixes from neighboring patch releases.

Neighboring Patches Included

- S-Cz830m1p15
- S-Cz840p8
- S-Cz900p2

Supported SPL Engines

The S-Cz9.1.0 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-Cz9.1.0 release of the Oracle Communications Session Border Controller (SBC) software supports the following new features.

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

OCI Resource Manager

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

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

Listing Available Boot and Code Images from the ACLI

With this release, the SBC can list local bootloader and code images in the output of the boot process. To do this, the SBC reads and prints all files with the .bz extension in the /boot and /code/images directories to the ACLI. The system does not display this list when configured for FIPs.

See Displaying Files from Boot and Images directory section in Boot Management chapter in the *Platform Preparation and Installation Guide*.

Display Disabled Sip-Interfaces

With this release, the SBC now labels a disabled **sip-interface** in the output of the **show sipd interface** command using a capital "D". The system labels each **sip-interface** this way when you set the **sip-interface**, **state** parameter to **disabled**.

See Viewing SIP Interface Statistics section in Performance Management chapter in the *Maintenance and Troubleshooting Guide*.

See show sipd section in ACLI Commands N-Z chapter in the *ACLI Reference Guide*.

Configuration Assistant Enhancements

This release includes assorted enhancements to the configuration assistant function.

See the Configuration Assistant Operations section in the Getting Started chapter in the *ACLI Configuration Guide*.

NPLI for Unregistered Emergency VoLTE Calls

Despite the absence of a SIP contact within the context of an unregistered user, the SBC manages network provided location information (NPLI) within call flows for unregistered emergency calls using the same controls it uses for registered flows. There is no additional configuration required to support unregistered calls. Common behavior for registered and unregistered emergency calls include the SBC managing NPLI AVP's in AARs and using the same timing controls to fine tune this management.

See the NPLI section in the External Policy Servers chapter in the *ACLI Configuration Guide*.

5G NR location support

The SBC provides 5G NR Location support, which enables interoperability with 5G core elements in 5G systems. This allows the SBC to operate as an Application Function and in its role as a P-CSCF in the 5G core. Many carriers deploy a separate 5G with the N26 interface in parallel with their older architectures. This newer architecture continues to use the Rx diameter interface to interwork with the PCF/PCRF and route diameter messages via the DRA. As an A-SBC, the SBC supports this architecture, further enabling operation within 5G. The SBC achieves this support through the ext-policy-server, specific-action-subscription, access-network-info-report configuration, which enables it to support additional 5G objects and behaviors, including objects that provide location information. No additional configuration is required to support NR location support for 5G.

See the NPLI section in the External Policy Servers chapter in the *ACLI Configuration Guide*.

TrFO for Asymmetric Preconditions

You can configure the SBC to avoid using transcoding resources while supporting call flows with asymmetric preconditions. After establishing a call that includes transcoding, the SBC can trigger this Transcoder Free Operation (TrFO) feature if the asymmetric preconditions parameter is present in the caller's SDP and a compatible codec can still be identified. Having determined that the call can proceed without transcoding, the SBC originates a reINVITE towards the calling party containing the called side codec. Once the reINVITE is completed, the call can continue without transcoding. The negotiated codec on the called party side must have been included in the calling party's original offer (after ingress codec-policy execution).

See the TrFO section in the Transoding chapter in the *ACLI Configuration Guide*.

STIR/SHAKEN Implementation Enhancements

This version of the SBC enhances the STIR/SHAKEN implementation to include new attestation behaviors and additional traffic statistics that report on STIR/SHAKEN traffic on per-interface, agent, realm and system-wide bases.These statistics are now available using the ACLI, SNMP and HDR.

See the STIR/SHAKEN chapter in the *ACLI Configuration Guide*.

DSCP marking for WPS

This feature provides you with the ability to configure the OCSBC to mark media packets for NSEP calls with DSCP codes on a realm-specific basis. This allows you to use DSCP to classify and set this traffic's priority differently for each realm.

See the Multimedia Priority Service for VoLTE Access section in the IMS Support chapter in the *ACLI Configuration Guide*.

WPS Session Reservation

This feature allows you to configure the SBC to reserve resources from the overall session pool for NSEP sessions only.

See the Multimedia Priority Service for VoLTE Access section in the IMS Support chapter in the *ACLI Configuration Guide*.

Forcing Port Parity for SRS

You can configure the SBC to enforce media port number parity on flows between the SBC and the SRS, as discussed in RFC 4566. By default, the SBC does not consider port number parity when assigning or recognizing RTP and RTCP flows in SDP session descriptions. This can result in signaling issues, including one-way audio recording, when the recording server and the SBC establish flows that have a port number conflict.

See the Session Recording Server section in the Selective Call Recording chapter in the *Call Traffic Monitoring Guide*.

SIP Transaction KPIs

This version of the SBC includes three new KPIs for measuring success-rate, timeout-rate and failure rate. These new parameters are displayed for SIP SUBSCRIBE, NOTIFY and MESSAGE messages only

See the SIP Method Counters section in the Performance Management chapter in the *Maintenance and Troubleshooting Guide*.

Increased Support of Static Trusted and Untrusted ACL Entries for vSBC and vSR

When deployed as a Virtual SBC or a Virtual SR, the SBC supports static ACL entry counts based on virtual machine memory. Deployments under 8GB of memory support 8000 trusted and 4000 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 64G, supported entries include:
  - Trusted static ACLs is 65536
  - Untrusted static ACLs is 32768

> **Note:**
>
> Dynamic ACL entries are independent of this support.

Reason Header AVP

This version of the SBC includes the Reason-Header AVP (code 3401) in STOP/EVENT ACRs when it receives a BYE/CANCEL (or SIP error response 4xx, 5xx, 6xx) with the Reason header in the SIP message.

See the Reason Header AVP section in the External Policy Server chapter of the *ACLI Configuration Guide*.

Reset Local Account Passwords

The local-accounts command has a new option to reset the password of a local user account. You must be logged in as an administrator to use this feature.

See the Manage Local Accounts section in the Getting Started chapter of the *Configuration Guide*.

STIR/SHAKEN Functionality on the OCSR

This release provides the same STIR/SHAKEN Functionality on the OCSR that is available on the SBC.

See the STIR/SHAKEN Client chapter in the *ACLI Configuration Guide* for documentation on STIR/SHAKE support on these session delivery products.

> **Note:**
>
> STIR/SHAKEN Functionality on the OCSR begins with S-Cz9.1.0p2.

MSRP KPIs

This release allows your to configure the SBC to present additional statistics on MSRP traffic using the ACLI and SNMP. These statistics include a filter for viewing realm-specific statistics, and allow you to extend reported data to include SEND and REPORT statistics.

See the Extended MSRP Statistics section in the *ACLI Configuration Guide* for explanation on this feature. See the *Maintenance and Troubleshooting Guide* and the *MIB Guide* for reference information about these statistics.

> **Note:**
>
> This new MSRP KPI support begins with S-Cz9.1.0p2.

OCI Shapes supported on Intel X9 processor

This version of the SBC supports the use of VM.Optimized3.Flex Machine Shapes over the OCI public cloud platform.

See the Create and Deploy on OCI section in the Public Cloud Platforms chapter of the *Platform Preparation and Installation Guide* for detail on using this platform. See the Supported Private Virtual Infrastructures and Public Clouds section in the Introduction chapter of these *Platform Preparation and Installation Guide* for shape and specification support of this OCI machine type for this software version release.

> **Note:**
>
> The availability of this vSBC Support on OCI for VM.Optimized3.Flex Machine Shapes feature begins with the S-Cz910p2 release.

DPDK Version Support

This release adds support for the DPDK version 21.11 at S-Cz9.1.0p2.

This change is reflected in the Supported Private Virtual Infrastructures and Public Clouds section in these *Release Notes*.

Matching Source Addressing for Authentication by a Surrogate Agent

Adds the **source-ip-prefix** parameter within the **surrogate-agent** element to specify the source addressing of endpoints for which the system can authenticate calls using this surrogate-agent. This configuration provides a means of matching mulitple source addresses, which defines a list of addresses for which the system can perform surrogate agent authentication.

This support is available in software versions S-Cz9.1.0p3 and above. See the *ACLI Configuration Guide*.

Authenticating Surrogate Agent Registrations across Realms

This release allows you to use **surrogate-agent** and **realm-config** configuration to configure surrogate-agent authentication. This method is considered robust, supporting multi-tenant, diverse IP-IPXs, and intra-realm registration support.

See the SIP chapter in the *ACLI Configuration Guide* for explanation on this feature. See the *ACLI Reference Guide* for reference information on the applicable configuration parameters and values.

> **Note:**
>
> This new intra-realm surrogate-agent authentication feature support begins with S-Cz9.1.0p3.

Changing the Precedence for Handling orig and verstat Values

This release allows you to change the header the system focuses on to populate orig and verstat values, Some regions require that the FROM header be the first source of this information. To accommodate these deployments, you can configure the SBC to use the FROM as the primary caller id source for information used to determine a SHAKEN orig claim and the verstat value.

See the Stir/Shaken Client chapter in the *ACLI Configuration Guide* for explanation on this feature. See the *ACLI Reference Guide* for reference information on the applicable configuration parameters and values.

> **Note:**
>
> This new TN Flip feature support begins with S-Cz9.1.0p3.

Configurable PAI and FQDN Manipulations

You can configure the system to manipulate the content of egress messages, including PAI headers and FQDNs, using realm parameters instead of HMR. By setting these parameters,

you cause the system to perform these manipulations on specific SIP methods that egress the realm.

See the Realms and Nested Realms chapter in the *ACLI Configuration Guide* for explanation on this feature. See the *ACLI Reference Guide* for reference information on the applicable configuration parameters and values.

> **Note:**
>
> This new manipulation feature support begins with S-Cz9.1.0p3.

TOS Passthrough Configuration

As stated above, the SBC does not passthrough received DSCP values transparently. If this is the desired behavior, no config change is required. This is the default behavior. Packets sent by SBC show DSCP value 0x00.

If passthrough support is desires, you can enable the **sip-config** option called **use-recvd-dscp-marking** which enables passthrough support. With this option enabled, the SBC passes the DSCP value which was received through to egress. To enable this option in **sip-config**, set the option as shown below.

```
ORACLE(sip-config)#options +use-recvd-dscp-marking
```

> **Note:**
>
> This new feature support begins with S-Cz9.1.0p3.

Creating a Reason Header During Verification

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

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

> **Note:**
>
> This new feature support begins with S-Cz9.1.0p5.

HTTP Header Customization for STIR/SHAKEN

You can configure the OCSBC with static mapping to and from SIP INVITEs and HTTP requests or responses within the context of STIR/SHAKEN authentication or verification procedures. This mapping provides a means of conveying SIP header information within HTTP headers and vice-versa. This feature adds headers and their new parameters in the rules'

targets or modifies existing headers with the new parameters presented by the rule. This feature applies to both ATIS and 3GPP modes.

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

> **Note:**
>
> This new feature support begins with S-Cz9.1.0p5.

Pooled Transcoding for MS-Team Deployments

You can configure the SBC to support pooled transcoding for most call flows, including incoming calls, outgoing calls, call forwarding and call transfers within MS Teams environments.

See the Pooled Transcoding for MS-Team Deployments section in the Transcoding chapter of the *ACLI Configuration Guide* for detailed information.

> **Note:**
>
> This new feature support begins with S-Cz9.1.0p6.

PSAP Callback Enhancement

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

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

> **Note:**
>
> This new feature support begins with S-Cz9.1.0p6.

New Memory Support for TCM-3

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

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

> **Note:**
>
> This new feature support begins with S-Cz9.1.0p7.

Allocation Strategies for Steering Pools

This version of the SBC allows you to configure three types of steering pools to allocate network ports for specific types of network traffic. These pool types include audio/video, MSRP and mixed media types. Establishing these pool types provides more efficient use of media ports. The SBC provides you with a means of monitoring port usage by type to troubleshoot and refine these configurations.

See the Allocation Strategies for Steering Pools section in the Realms chapter of the *ACLI Configuration Guide* for detailed information about this feature.

> **Note:**
>
> This new feature support begins with S-Cz9.1.0p8.

HTTP Client Cache Size Configuration

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

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

> **Note:**
>
> This new feature support begins with S-Cz9.1.0p9.

Verstat Delimiter

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

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

> **Note:**
>
> This new feature support begins with S-Cz9.1.0p6.

Session-Level DoS Protection

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

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

> **Note:**
>
> This new feature support begins with S-Cz9.1.0p10.

Subscription-Id-Data AVP

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

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

> **Note:**
>
> This new feature support begins with S-Cz9.1.0p10.

Supporting HA with STIR SHAKEN over TCP

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

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

> **Note:**
>
> This new feature support begins with S-Cz9.1.0p10.

3
Interface Changes

The following topics summarize ACLI, SNMP, HDR, Alarms, Accounting, and Error/Warning changes for S-Cz9.1.0. The additions, removals, and changes noted in these topics occurred since the previous major release of the Oracle Communications Session Border Controller.

ACLI Configuration Element Changes

The following tables summarize the ACLI configuration element changes that first appear in the Oracle Communications Session Border Controller (SBC) S-Cz9.1.0 release.

TrFO for Asymmetric Preconditions

Modified Elements	Description
media-manager, **realm-config**, **feature-trfo**, supports the new value **asymmetric-preconditions**	This release adds this new value to the feature-trfo parameter that sets the system to support transcoding-free operation within call flows that use asymmetric-preconditions.

STIR/SHAKEN Implementation Enhancements

Modified Elements	Description
session-router, **sti-config**, **sti-signaling-attest-info-mandatory**	Enables the system to require that the received INVITE contain the P-Attestation-Info and/or Attestation-Info header, and the P-Origination-Id and/or Origination-Id header, for the system to send a signing request to STI-AS.
session-router, **sti-config**, **anonymous-uri-add-verstat-to-hostpart**	Enables the system to place the verstat parameter after the hostpart when the received INVITE does not contain a P-Asserted-Identity header, but does contain a Privacy header and an anonymous URI in the FROM.
system-config, **collect group-settings** supports the new value **stir-stats**	Enables STIR/SHAKEN authentication and verification statistics on a per-server basis.
system-config, **collect group-settings** supports the new value **stir-stats-session-agent**	Enables STIR/SHAKEN authentication and verification statistics on a per-session-agent basis.
system-config, **collect group-settings** supports the new value **stir-stats-sip-interface**	Enables STIR/SHAKEN authentication and verification statistics on a per-sip-interface basis.
system-config, **collect group-settings** supports the new value **stir-stats-realm**	Enables STIR/SHAKEN authentication and verification statistics on a per-realm basis.
system-config, **collect group-settings** supports the new value **stir-stats-system**	Enables STIR/SHAKEN authentication and verification statistics on a global system basis.

Realm-Specific DSCP Marking for NSEP Traffic

Modified Elements	Description
media-manager, **realm-config**, **nsep-media-policy**	Enables the system to specify a media policy to perform DSCP marking of media on a realm-specific basis.

WPS Session reservation

Modified Elements	Description
system, **system-config**, **reserved-nsep-session-capacity**	Enables the system to reserve resources from the overall session pool for NSEP sessions only.
system, **system-config**, **alarm-threshold**, **type** supports the new value **reserved-nsep-sessions**	This release adds this new value, which allows you to set thresholds for alarms related to the pool of sessions reserved for NSEP traffic.

Enabling Parity of RTC and RTCP Ports within SRS

Modified Elements	Description
session-router, **session-recording-server**, **force-parity**	Enables the system to require port number parity for RTC and RTCP ports within SRS-related calls.

Update in media-profile parameters for SD5 platforms - 4600,6300 and 6350

Modified Elements	Description
session-router, **media-profile**, **average-rate-limit**	The minimum value is changed from 0 to 8192 bytes/sec on SD5 platforms (AP4600, AP6300, AP6350) to support the media-policy feature.
session-router, **media-profile**, **peak-rate-limit**	The minimum value is changed from 0 to 8192 bytes/sec on SD5 platforms (AP4600, AP6300, AP6350) to support the media-policy feature.
session-router, **media-profile**, **max-burst-size**	The minimum value is changed from 0 to 8192 bytes/sec on SD5 platforms (AP4600, AP6300, AP6350) to support the media-policy feature.

Updates in the global TLS Settings

Added Element	Description
security, **tls-global**, **diffie-hellman-key-size**	The size of the Diffie-Hellman key offered by the SBC during TLS negotiations on SIP interfaces. The default is 1024. Setting to 2048 significantly decreases performance.

Updates to the STI Server Group

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

ACLI Command Changes

The following table summarizes the ACLI command changes that first appear in the Oracle Communications Session Border Controller S-Cz9.1.0 release.

This table lists and describes changes to ACLI commands that are available in the S-Cz9.1.0 release.

New Commands	Description
show stir agents < agent_id >	STIR/SHAKEN Session Agents Statistics
show stir interface < interface_id >	STIR/SHAKEN Sip Interface Statistics
show stir realm < realm_id >	STIR/SHAKEN Realm Statistics
show stir stats <sti-server>	STIR/SHAKEN Server Statistics
show stir all	STIR/SHAKEN System Wide Statistics
show sessions	This command output is modified to display NSEP session reservation capacity and current NSEP inbound session counts.
bootparam	The l (small letter L) option is added to view the list of image files (.bz files) from /boot and /code/ images directories.
local-accounts reset <user>	The local-accounts command has a new option to reset the password of a local user account.

Accounting Changes

This section summarizes the accounting changes that appear in the Oracle Communications Session Border Controller version S-Cz9.1.0.

STIR/SHAKEN CDR Support

The SBC sends an ACR to the PCRF for call accounting with the following VoLTE-specific AVPs. The table shows all mandatory and optional AVP's. If there is data, the SBC includes Optional AVPs. If not the SBC does not include them.

The SBC sends the following fields as RADIUS extended attributes for the Call.

AVP	VSA ID	Extended Attribute Value
Stir-Signed- Request	249	11
Stir-Signed- Request- Exception-Id	249	12
Stir-Verified- Request	249	13
Stir-Verified- Request- Exception-Id	249	14

The SBC sends the following fields as custom AVP's in the Diameter ACR.

AVP	ACME Diameter Attribute	Start	Interim	Stop	Message Type = INVITE	AVP Type
Stir-Signed-Request	104	NA	Yes	Yes	Yes	String

AVP	ACME Diameter Attribute	Start	Interim	Stop	Message Type = INVITE	AVP Type
Stir-Signed-Request-Exception-Id	105	NA	Yes	Yes	Yes	String
Stir-Verified-Request	106	Yes	Yes	Yes	Yes	String
Stir-Verified-Request-Exception-Id	107	Yes	Yes	Yes	Yes	String

See *STIR/SHAKEN* in the *Accounting Guide*.

STIR/SHAKEN Attributes for Local CDRs

This table lists the new STIR/SHAKEN attributes placed into local CDR files when the protocol is Diameter and generate-event is START.

AVP	CSV Placement	Value Type
Destination-Host	164	ACME
Stir-Signed- Request	165	ACME
Stir-Signed- Request- Exception-Id	166	ACME
Stir-Verified- Request	167	ACME
Stir-Verified- Request- Exception-Id	168	ACME

This table lists the new STIR/SHAKEN attributes placed into local CDR files when the protocol is Diameter and generate-event is INTERIM.

AVP	CSV Placement	Value Type
Destination-Host	206	ACME
Stir-Signed- Request	207	ACME
Stir-Signed- Request- Exception-Id	208	ACME
Stir-Verified- Request	209	ACME
Stir-Verified- Request- Exception-Id	210	ACME

This table lists the new STIR/SHAKEN attributes placed into local CDR files when the protocol is Diameter and generate-event is STOP.

AVP	CSV Placement	Value Type
Destination-Host	230	ACME
Stir-Signed- Request	231	ACME
Stir-Signed- Request- Exception-Id	232	ACME
Stir-Verified- Request	233	ACME
Stir-Verified- Request- Exception-Id	234	ACME

This table lists the new STIR/SHAKEN attributes placed into local CDR files when the protocol is RADIUS and generate-event is START.

AVP	CSV Placement	Value Type
CDR Sequence Number	136	ACME
Stir-Signed- Request	137	ACME
Stir-Signed- Request- Exception-Id	138	ACME
Stir-Verified- Request	139	ACME
Stir-Verified- Request- Exception-Id	140	ACME

This table lists the new STIR/SHAKEN attributes placed into local CDR files when the protocol is RADIUS and generate-event is INTERIM.

AVP	CSV Placement	Value Type
CDR Sequence Number	182	ACME
Stir-Signed- Request	183	ACME
Stir-Signed- Request- Exception-Id	184	ACME
Stir-Verified- Request	185	ACME
Stir-Verified- Request- Exception-Id	186	ACME

This table lists the new STIR/SHAKEN attributes placed into local CDR files when the protocol is RADIUS and generate-event is STOP.

AVP	CSV Placement	Value Type
CDR Sequence Number	205	ACME
Stir-Signed- Request	206	ACME
Stir-Signed- Request- Exception-Id	207	ACME
Stir-Verified- Request	208	ACME
Stir-Verified- Request- Exception-Id	209	ACME

See Appendix B in the *Accounting Guide*.

SNMP/MIB Changes

This section summarizes the SNMP/MIB changes that appear in the SBC version S-Cz9.1.0.

MIB Changes for STIR/SHAKEN Statistics

When the STIR/SHAKEN feature is enabled, the SBC uses the apAppsStirMIBObjects table, within the `ap.apps.mib`, to monitor feature statistics. The system assembles this table by nesting the objects in the following SNMP tables.

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

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.1.2.4.2.1.4.x + (except apStirServerName)	Description
apStirServerName	1.3.6.1.4.1.9148.3.16.1.2.4.1.1.2	Server name as configured on the SBC
apStirServerStats.recent.asQueries	1.1	Recent queries made to the named AS server
apStirServerStats.recent.asSuccessResponses	1.2	Recent successful responses received from the named AS server
apStirServerStats.recent.asFailResponses	1.3	Recent failed responses received from the named AS server
apStirServerStats.recent.asFailServiceException	1.4	Recent failed responses received from the named AS server caused by a service exception
apStirServerStats.recent.asFailPolicyException	1.5	Recent failed responses received from the named AS server caused by a policy exception
apStirServerStats.recent.vsQueries	1.6	Recent queries made to the named VS server
apStirServerStats.recent.vsSuccessResponses	1.7	Recent successful responses received from the named VS server
apStirServerStats.recent.vsFailResponses	1.8	Recent failed responses received from the named VS server
apStirServerStats.recent.vsSuccessVerification	1.9	Recent successful verifications received from the named VS server
apStirServerStats.recent.vsFailVerification	1.10	Recent failed responses received from the named VS server indicating verification failure
apStirServerStats.recent.vsFailServiceException	1.11	Recent failed responses received from the named VS server caused by a service exception
apStirServerStats.recent.vsFailPolicyException	1.12	Recent failed responses received from the named VS server caused by a policy exception
apStirServerStats.recent.serverUnreachable	1.13	Number of times a server could not e reached within the recent window.
apStirServerStats.total.asQueries	2.1	Total queries made to the named AS server
apStirServerStats.total.asSuccessResponses	2.2	Total successful responses received from the named AS server
apStirServerStats.total.asFailResponses	2.3	Total failed responses received from the named AS server
apStirServerStats.total.asFailServiceException	2.4	Total failed responses received from the named AS server caused by a service exception
apStirServerStats.total.asFailPolicyException	2.5	Total failed responses received from the named AS server caused by a policy exception
apStirServerStats.total.vsQueries	2.6	Total queries made to the named VS server

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.1.2.4.2.1.4.x + (except apStirServerName)	Description
apStirServerStats.total.vsSuccessResponses	2.7	Total successful responses received from the named VS server
apStirServerStats.total.vsFailResponses	2.8	Total failed responses received from the named VS server
apStirServerStats.total.vsSuccessVerification	2.9	Total successful verifications received from the named VS server
apStirServerStats.total.vsFailVerification	2.10	Total failed responses received from the named VS server indicating verification failure
apStirServerStats.total.vsFailServiceException	2.11	Total failed responses received from the named VS server caused by a service exception
apStirServerStats.total.vsFailPolicyException	2.12	Total failed responses received from the named VS server caused by a policy exception
apStirServerStats.total.serverUnreachable	2.13	Total number of times a server could not be reached.
apStirServerStats.permax.asQueries	3.1	Permax queries made to the named AS server
apStirServerStats.permax.asSuccessResponses	3.2	Permax successful responses received from the named AS server
apStirServerStats.permax.asFailResponses	3.3	Permax failed responses received from the named AS server
apStirServerStats.permax.asFailServiceException	3.4	Permax failed responses received from the named AS server caused by a service exception
apStirServerStats.permax.asFailPolicyException	3.5	Permax failed responses received from the named AS server caused by a policy exception
apStirServerStats.permax.vsQueries	3.6	Permax queries made to the named VS server
apStirServerStats.permax.vsSuccessResponses	3.7	Permax successful responses received from the named VS server
apStirServerStats.permax.vsFailResponses	3.8	Permax failed responses received from the named VS server
apStirServerStats.permax.vsSuccessVerification	3.9	Permax successful responses received from the named VS server
apStirServerStats.permax.vsFailVerification	3.10	Permax failed responses received from the named VS server
apStirServerStats.permax.vsFailServiceException	.3.11	Permax failed responses received from the named VS server caused by a service exception
apStirServerStats.permax.vsFailPolicyException	3.12	Permax failed responses received from the named VS server caused by a policy exception
apStirServerStats.permax.serverUnreachable	3.13	Permax number of times a server could not be reached.

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

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.1.2.4.4.1.4.x + (except apStirAgentName)	Description
apStirAgentName	1.3.6.1.4.1.9148.3.16.1.2.4.1.1.2	Session-agent hostname name as configured on the SBC
apStirAgentStats.recent.asQueries	1.1	Recent queries made to the named AS server
apStirAgentStats.recent.asSuccessResponses	1.2	Recent successful responses received from the named AS server
apStirAgentStats.recent.asFailResponses	1.3	Recent failed responses received from the named AS server
apStirAgentStats.recent.asFailServiceException	1.4	Recent failed responses received from the named AS server caused by a service exception
apStirAgentStats.recent.asFailPolicyException	1.5	Recent failed responses received from the named AS server caused by a policy exception
apStirAgentStats.recent.vsQueries	1.6	Recent queries made to the named VS server
apStirAgentStats.recent.vsSuccessResponses	1.7	Recent successful responses received from the named VS server
apStirAgentStats.recent.vsFailResponses	1.8	Recent failed responses received from the named VS server
apStirAgentStats.recent.vsSuccessVerification	1.9	Recent successful verifications received from the named VS server
apStirAgentStats.recent.vsFailVerification	1.10	Recent failed responses received from the named VS server indicating verification failure
apStirAgentStats.recent.vsFailServiceException	1.11	Recent failed responses received from the named VS server caused by a service exception
apStirAgentStats.recent.vsFailPolicyException	1.12	Recent failed responses received from the named VS server caused by a policy exception
apStirAgentStats.total.asQueries	2.1	Recent queries made to the named AS server
apStirAgentStats.total.asSuccessResponses	2.2	Total successful responses received from the named AS server
apStirAgentStats.total.asFailResponses	2.3	Total failed responses received from the named AS server
apStirAgentStats.total.asFailServiceException	2.4	Total failed responses received from the named AS server caused by a service exception
apStirAgentStats.total.asFailPolicyException	2.5	Total failed responses received from the named AS server caused by a policy exception
apStirAgentStats.total.vsQueries	2.6	Total queries made to the named VS server

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.1.2.4.4.1.4.x + (except apStirAgentName)	Description
apStirAgentStats.total.vsSuccessResponses	2.7	Total successful responses received from the named VS server
apStirAgentStats.total.vsFailResponses	2.8	Total failed responses received from the named VS server
apStirAgentStats.total.vsSuccessVerification	2.9	Total successful verifications received from the named VS server
apStirAgentStats.total.vsFailVerification	2.10	Total failed responses received from the named VS server indicating verification failure
apStirAgentStats.total.vsFailServiceException	2.11	Total failed responses received from the named VS server caused by a service exception
apStirAgentStats.total.vsFailPolicyException	2.12	Total failed responses received from the named VS server caused by a policy exception
apStirAgentStats.permax.asQueries	3.1	Permax queries made to the named AS server
apStirAgentStats.permax.asSuccessResponses	3.2	Permax successful responses received from the named AS server
apStirAgentStats.permax.asFailResponses	3.3	Permax failed responses received from the named AS server
apStirAgentStats.permax.asFailServiceException	3.4	Permax failed responses received from the named AS server caused by a service exception
apStirAgentStats.permax.asFailPolicyException	3.5	Permax failed responses received from the named AS server caused by a policy exception
apStirAgentStats.permax.vsQueries	3.6	Permax queries made to the named VS server
apStirAgentStats.permax.vsSuccessResponses	3.7	Permax successful responses received from the named VS server
apStirAgentStats.permax.vsFailResponses	3.8	Permax failed responses received from the named VS server
apStirAgentStats.permax.vsSuccessVerification	3.9	Recent successful verifications received from the named VS server
apStirAgentStats.permax.vsFailVerification	3.10	Permax failed responses received from the named VS server indicating verification failure
apStirAgentStats.permax.vsFailServiceException	.3.11	Permax failed responses received from the named VS server caused by a service exception
apStirAgentStats.permax.vsFailPolicyException	3.12	permax failed responses received from the named VS server caused by a policy exception

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

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.1.2.4.6.1.4.x + (except apStirSipInterfaceName)	Description
apStirSipInterfaceName	1.3.6.1.4.1.9148.3.16.1.2.4.1.1.2	Server name as configured on the SBC
apStirSipInterfaceStats.recent.asQueries	1.1	Recent queries made to the named AS server
apStirSipInterfaceStats.recent.asSuccessResponses	1.2	Recent successful responses received from the named AS server
apStirSipInterfaceStats.recent.asFailResponses	1.3	Recent failed responses received from the named AS server
apStirSipInterfaceStats.recent.asFailServiceException	1.4	Recent failed responses received from the named AS server caused by a service exception
apStirSipInterfaceStats.recent.asFailPolicyException	1.5	Recent failed responses received from the named AS server caused by a policy exception
apStirSipInterfaceStats.recent.vsQueries	1.6	Recent queries made to the named VS server
apStirSipInterfaceStats.recent.vsSuccessResponses	1.7	Recent successful responses received from the named VS server
apStirSipInterfaceStats.recent.vsFailResponses	1.8	Recent failed responses received from the named VS server
apStirSipInterfaceStats.recent.vsSuccessVerification	1.9	Recent successful verifications received from the named VS server
apStirSipInterfaceStats.recent.vsFailVerification	1.10	Recent failed responses received from the named VS server indicating verification failure
apStirSipInterfaceStats.recent.vsFailServiceException	1.11	Recent failed responses received from the named VS server caused by a service exception
apStirSipInterfaceStats.recent.vsFailPolicyException	1.12	Recent failed responses received from the named VS server caused by a policy exception
apStirSipInterfaceStats.total.asQueries	2.1	Recent queries made to the named AS server
apStirSipInterfaceStats.total.asSuccessResponses	2.2	Total successful responses received from the named AS server
apStirSipInterfaceStats.total.asFailResponses	2.3	Total failed responses received from the named AS server
apStirSipInterfaceStats.total.asFailServiceException	2.4	Total failed responses received from the named AS server caused by a service exception
apStirSipInterfaceStats.total.asFailPolicyException	2.5	Total failed responses received from the named AS server caused by a policy exception
apStirSipInterfaceStats.total.vsQueries	2.6	Total queries made to the named VS server

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.1.2.4.6.1.4.x + (except apStirSipInterfaceName)	Description
apStirSipInterfaceStats.total.vsSuccessResponses	2.7	Total successful responses received from the named VS server
apStirSipInterfaceStats.total.vsFailResponses	2.8	Total failed responses received from the named VS server
apStirSipInterfaceStats.total.vsSuccessVerification	2.9	Total successful verifications received from the named VS server
apStirSipInterfaceStats.total.vsFailVerification	2.10	Total failed responses received from the named VS server indicating verification failure
apStirSipInterfaceStats.total.vsFailServiceException	2.11	Total failed responses received from the named VS server caused by a service exception
apStirSipInterfaceStats.total.vsFailPolicyException	2.12	Total failed responses received from the named VS server caused by a policy exception
apStirSipInterfaceStats.permax.asQueries	3.1	Permax queries made to the named AS server
apStirSipInterfaceStats.permax.asSuccessResponses	3.2	Permax successful responses received from the named AS server
apStirSipInterfaceStats.permax.asFailResponses	3.3	Permax failed responses received from the named AS server
apStirSipInterfaceStats.permax.asFailServiceException	3.4	Permax failed responses received from the named AS server caused by a service exception
apStirSipInterfaceStats.permax.asFailPolicyException	3.5	Permax failed responses received from the named AS server caused by a policy exception
apStirSipInterfaceStats.permax.vsQueries	3.6	Permax queries made to the named VS server
apStirSipInterfaceStats.permax.vsSuccessResponses	3.7	Permax successful responses received from the named VS server
apStirSipInterfaceStats.permax.vsFailResponses	3.8	Permax failed responses received from the named VS server
apStirSipInterfaceStats.permax.vsSuccessVerification	3.9	Permax successful verifications received from the named VS server
apStirSipInterfaceStats.permax.vsFailVerification	3.10	Permax failed responses received from the named VS server indicating verification failure
apStirSipInterfaceStats.permax.vsFailServiceException	.3.11	Permax failed responses received from the named VS server caused by a service exception
apStirSipInterfaceStats.permax.vsFailPolicyException	3.12	Recent failed responses received from the named VS server caused by a policy exception

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

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.1.2.4.8.1.4.x + (except apRealmName)	Description
apStirRealmName	1.3.6.1.4.1.9148.3.16.1.2.4.1.1.2	Server name as configured on the SBC
apStirRealmStats.recent.asQueries	1.1	Recent queries made to the named AS server
apStirRealmStats.recent.asSuccessResponses	1.2	Recent successful responses received from the named AS server
apStirRealmStats.recent.asFailResponses	1.3	Recent failed responses received from the named AS server
apStirRealmStats.recent.asFailServiceException	1.4	Recent failed responses received from the named AS server caused by a service exception
apStirRealmStats.recent.asFailPolicyException	1.5	Recent failed responses received from the named AS server caused by a policy exception
apStirRealmStats.recent.vsQueries	1.6	Recent queries made to the named VS server
apStirRealmStats.recent.vsSuccessResponses	1.7	Recent successful responses received from the named VS server
apStirRealmStats.recent.vsFailResponses	1.8	Recent failed responses received from the named VS server
apStirRealmStats.recent.vsSuccessVerification	1.9	Recent successful verifications received from the named VS server
apStirRealmStats.recent.vsFailVerification	1.10	Recent failed responses received from the named VS server indicating verification failure
apStirRealmStats.recent.vsFailServiceException	1.11	Recent failed responses received from the named VS server caused by a service exception
apStirRealmStats.recent.vsFailPolicyException	1.12	Recent failed responses received from the named VS server caused by a policy exception
apStirRealmStats.total.asQueries	2.1	Recent queries made to the named AS server
apStirRealmStats.total.asSuccessResponses	2.2	Total successful responses received from the named AS server
apStirRealmStats.total.asFailResponses	2.3	Total failed responses received from the named AS server
apStirRealmStats.total.asFailServiceException	2.4	Total failed responses received from the named AS server caused by a service exception
apStirRealmStats.total.asFailPolicyException	2.5	Total failed responses received from the named AS server caused by a policy exception
apStirRealmStats.total.vsQueries	2.6	Total queries made to the named VS server

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.1.2.4.8.1.4. x + (except apRealmName)	Description
apStirRealmStats.total.vsSuccessResponses	2.7	Total successful responses received from the named VS server
apStirRealmStats.total.vsFailResponses	2.8	Total failed responses received from the named VS server
apStirRealmStats.total.vsSuccessVerification	2.9	Total successful verifications received from the named VS server
apStirRealmStats.total.vsFailVerification	2.10	Total failed responses received from the named VS server indicating verification failure
apStirRealmStats.total.vsFailServiceException	2.11	Total failed responses received from the named VS server caused by a service exception
apStirRealmStats.total.vsFailPolicyException	2.12	Total failed responses received from the named VS server caused by a policy exception
apStirRealmStats.permax.asQueries	3.1	Permax queries made to the named AS server
apStirRealmStats.permax.asSuccessResponses	3.2	Permax successful responses received from the named AS server
apStirRealmStats.permax.asFailResponses	3.3	Permax failed responses received from the named AS server
apStirRealmStats.permax.asFailServiceException	3.4	Permax failed responses received from the named AS server caused by a service exception
apStirRealmStats.permax.asFailPolicyException	3.5	Permax failed responses received from the named AS server caused by a policy exception
apStirRealmStats.permax.vsQueries	3.6	Permax queries made to the named VS server
apStirRealmStats.permax.vsSuccessResponses	3.7	Permax successful responses received from the named VS server
apStirRealmStats.permax.vsFailResponses	3.8	Permax failed responses received from the named VS server
apStirRealmStats.permax.vsSuccessVerification	3.9	Permax successful verifications received from the named VS server
apStirRealmStats.permax.vsFailVerification	3.10	Permax failed responses received from the named VS server indicating verification failure
apStirRealmStats.permax.vsFailServiceException	.3.11	Permax failed responses received from the named VS server caused by a service exception
apStirRealmStats.permax.vsFailPolicyException	3.12	Recent failed responses received from the named VS server caused by a policy exception

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

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.1.2.4.9.1.3 +	Description
apStirSystemStats.recent.asQueries	1.1	Recent queries made to the named AS server
apStirSystemStats.recent.asSuccessResponses	1.2	Recent successful responses received from the named AS server
apStirSystemStats.recent.asFailResponses	1.3	Recent failed responses received from the named AS server
apStirSystemStats.recent.asFailServiceException	1.4	Recent failed responses received from the named AS server caused by a service exception
apStirSystemStats.recent.asFailPolicyException	1.5	Recent failed responses received from the named AS server caused by a policy exception
apStirSystemStats.recent.vsQueries	1.6	Recent queries made to the named VS server
apStirSystemStats.recent.vsSuccessResponses	1.7	Recent successful responses received from the named VS server
apStirSystemStats.recent.vsFailResponses	1.8	Recent failed responses received from the named VS server
apStirSystemStats.recent.vsSuccessVerification	1.9	Recent successful responses received from the named VS server indicating verification failure
apStirSystemStats.recent.vsFailVerification	1.10	Recent failed responses received from the named VS server indicating verification failure
apStirSystemStats.recent.vsFailServiceException	1.11	Recent failed responses received from the named VS server caused by a service exception
apStirSystemStats.recent.vsFailPolicyException	1.12	Recent failed responses received from the named VS server caused by a policy exception
apStirSystemStats.total.asQueries	2.1	Recent queries made to the named AS server
apStirSystemStats.total.asSuccessResponses	2.2	Total successful responses received from the named AS server
apStirSystemStats.total.asFailResponses	2.3	Total failed responses received from the named AS server
apStirSystemStats.total.asFailServiceException	2.4	Total failed responses received from the named AS server caused by a service exception
apStirSystemStats.total.asFailPolicyException	2.5	Total failed responses received from the named AS server caused by a policy exception
apStirSystemStats.total.vsQueries	2.6	Total queries made to the named VS server
apStirSystemStats.total.vsSuccessResponses	2.7	Total successful responses received from the named VS server

MIB Object	Object ID 1.3.6.1.4.1.9148.3.16.1.2.4.9.1.3 +	Description
apStirSystemStats.total.vsFailResponses	2.8	Total failed responses received from the named VS server
apStirSystemStats.total.vsSuccessVerification	2.9	Total successful responses received from the named VS server indicating verification failure
apStirSystemStats.total.vsFailVerification	2.10	Total failed responses received from the named VS server indicating verification failure
apStirSystemStats.total.vsFailServiceException	2.11	Total failed responses received from the named VS server caused by a service exception
apStirSystemStats.total.vsFailPolicyException	2.12	Total failed responses received from the named VS server caused by a policy exception
apStirSystemStats.permax.asQueries	3.1	Permax queries made to the named AS server
apStirSystemStats.permax.asSuccessResponses	3.2	Permax successful responses received from the named AS server
apStirSystemStats.permax.asFailResponses	3.3	Permax failed responses received from the named AS server
apStirSystemStats.permax.asFailServiceException	3.4	Permax failed responses received from the named AS server caused by a service exception
apStirSystemStats.permax.asFailPolicyException	3.5	Permax failed responses received from the named AS server caused by a policy exception
apStirSystemStats.permax.vsQueries	3.6	Permax queries made to the named VS server
apStirSystemStats.permax.vsSuccessResponses	3.7	Permax successful responses received from the named VS server
apStirSystemStats.permax.vsFailResponses	3.8	Permax failed responses received from the named VS server
apStirSystemStats.permax.vsSuccessVerification	3.9	Permax failed responses received from the named VS server indicating verification failure
apStirSystemStats.permax.vsFailVerification	3.10	Permax failed responses received from the named VS server indicating verification failure
apStirSystemStats.permax.vsFailServiceException	.3.11	Permax failed responses received from the named VS server caused by a service exception
apStirSystemStats.permax.vsFailPolicyException	3.12	Permax failed responses received from the named VS server caused by a policy exception

Alarms

This section summarizes the alarm changes that appear in the Oracle Communications Session Border Controller version S-Cz9.1.0.

NSEP Session Reservation

When you configure **reserved-nsep-session-capacity** to a non-zero value, the system uses default thresholds to trigger minor, major and critical alarms when session utilization exceeds these thresholds. You can customize these thresholds by configuring the **reserved-nsep-sessions alarm threshold** type:

- **The system is exceeding the minor threshold for sessions reserved for NSEP sessions**
- **The system is exceeding the major threshold for sessions reserved for NSEP sessions**
- **The system is exceeding the critical threshold for sessions reserved for NSEP sessions**

HDR

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

STIR/SHAKEN HDR Groups - stir-stats

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

CSV Position	HDR Column Name	Data Type	Range	Description
1	TimeStamp	N/A	N/A	Time that this data was written to this file.
2	STI-Server	N/A	N/A	Server name as configured on the SBC.
3	AS Queries	Counter	0-2147483647	Total AS server queries made to the named server.
4	AS Success Responses	Counter	0-2147483647	Total successful AS server responses received from the named server.
5	AS Fail Responses	Counter	0-2147483647	Total failed AS server responses received from the named server.
6	AS Fail Service Exception	Counter	0-2147483647	Total AS server responses received from the named server indicating failure caused by a service exception.

CSV Position	HDR Column Name	Data Type	Range	Description
7	AS Fail Policy Exception	Counter	0-2147483647	Total AS server responses received from the named server indicating failure caused by a policy exception.
8	VS Queries	Counter	0-2147483647	Total VS server queries made to the named server.
9	VS Success Responses	Counter	0-2147483647	Total successful VS server responses received from the named server.
10	VS Fail Responses	Counter	0-2147483647	Total failed VS server responses received from the named server.
11	VS Success Verification	Counter	0-2147483647	Total VS server responses received from the named server indicating verification success.
12	VS Fail Verification	Counter	0-2147483647	Total VS server responses received from the named server indicating verification failure.
13	VS Fail Service Exception	Counter	0-2147483647	Total VS server responses received from the named server indicating failure caused by a service exception.
14	VS Fail Policy Exception	Counter	0-2147483647	Total VS server responses received from the named server indicating failure caused by a policy exception.
15	STI Server Unreachable	Counter	N/A	The number of times the server has tripped the STI server's 'circuit breaker'

STIR/SHAKEN HDR Groups - stir-stats-session-agent

The table below lists and describes stir servers statistics and includes HDR position, statistic, type, timer value, range, and description.

CSV Position	HDR Column Name	Data Type	Range	Description
1	TimeStamp	Integer	N/A	Time that this data was written to this file.
2	Session-Agent	ASCII	N/A	Session agent name as configured on the SBC.
3	AS Queries	Counter	0-2147483647	Total AS server queries made via the named session agent.
4	AS Success Responses	Counter	0-2147483647	Total successful AS server responses received via the named session agent.
5	AS Fail Responses	Counter	0-2147483647	Total failed AS server responses received via the named session agent.
6	AS Fail Service Exception	Counter	0-2147483647	Total AS server responses received via the named session agent indicating failure caused by a service exception.
7	AS Fail Policy Exception	Counter	0-2147483647	Total AS server responses received via the named session agent indicating failure caused by a policy exception.
8	VS Queries	Counter	0-2147483647	Total VS server queries made via the named session agent.
9	VS Success Responses	Counter	0-2147483647	Total successful VS server responses received via the named session agent.
10	VS Fail Responses	Counter	0-2147483647	Total failed VS server responses received via the named session agent.
11	VS Success Verification	Counter	0-2147483647	Total VS server responses received via the named session agent indicating verification success.

CSV Position	HDR Column Name	Data Type	Range	Description
12	VS Fail Verification	Counter	0-2147483647	Total VS server responses received via the named session agent indicating verification failure.
13	VS Fail Service Exception	Counter	0-2147483647	Total VS server responses received via the named session agent indicating failure caused by a service exception.
14	VS Fail Policy Exception	Counter	0-2147483647	Total VS server responses received via the named session agent indicating failure caused by a policy exception.

STIR/SHAKEN HDR Groups - stir-stats-sip-interface

The table below lists and describes stir servers statistics and includes HDR position, statistic, type, timer value, range, and description.

CSV Position	HDR Column Name	Data Type	Range	Description
1	TimeStamp	Integer	N/A	Time that this data was written to this file.
2	SIP Interface	ASCII	N/A	SIP interface name as configured on the SBC.
3	AS Queries	Counter	0-2147483647	Total AS server queries made via the named SIP interface.
4	AS Success Responses	Counter	0-2147483647	Total successful AS server responses received via the named SIP interface.
5	AS Fail Responses	Counter	0-2147483647	Total failed AS server responses received via the named SIP interface.
6	AS Fail Service Exception	Counter	0-2147483647	Total AS server responses received via the named SIP interface indicating failure caused by a service exception.

CSV Position	HDR Column Name	Data Type	Range	Description
7	AS Fail Policy Exception	Counter	0-2147483647	Total AS server responses received via the named SIP interface indicating failure caused by a policy exception.
8	VS Queries	Counter	0-2147483647	Total VS server queries made via the named SIP interface.
9	VS Success Responses	Counter	0-2147483647	Total successful VS server responses received via the named SIP interface.
10	VS Fail Responses	Counter	0-2147483647	Total failed VS server responses received via the named SIP interface.
11	VS Success Verification	Counter	0-2147483647	Total VS server responses received via the named SIP interface indicating verification success.
12	VS Fail Verification	Counter	0-2147483647	Total VS server responses received via the named SIP interface indicating verification failure.
13	VS Fail Service Exception	Counter	0-2147483647	Total VS server responses received via the named SIP interface indicating failure caused by a service exception.
14	VS Fail Policy Exception	Counter	0-2147483647	Total VS server responses received via the named SIP interface indicating failure caused by a policy exception.

STIR/SHAKEN HDR Groups - stir-stats-realm

The table below lists and describes stir servers statistics and includes HDR position, statistic, type, timer value, range, and description.

CSV Position	HDR Column Name	Data Type	Range	Description
1	TimeStamp	Integer	NA	Time that this data was written to this file.

CSV Position	HDR Column Name	Data Type	Range	Description
2	Realm	ASCII	N/A	Realm name as configured on the SBC.
3	AS Queries	Counter	0-2147483647	Total AS server queries made via the named realm.
4	AS Success Responses	Counter	0-2147483647	Total successful AS server responses received via the named realm.
5	AS Fail Responses	Counter	0-2147483647	Total failed AS server responses received via the named realm.
6	AS Fail Service Exception	Counter	0-2147483647	Total AS server responses received via the named realm indicating failure caused by a service exception.
7	AS Fail Policy Exception	Counter	0-2147483647	Total AS server responses received via the named realm indicating failure caused by a policy exception.
8	VS Queries	Counter	0-2147483647	Total VS server queries made via the named realm.
9	VS Success Responses	Counter	0-2147483647	Total successful VS server responses received via the named realm.
10	VS Fail Responses	Counter	0-2147483647	Total failed VS server responses received via the named realm.
11	VS Success Verification	Counter	0-2147483647	Total VS server responses received via the named realm indicating verification success.
12	VS Fail Verification	Counter	0-2147483647	Total VS server responses received via the named realm indicating verification failure.
13	VS Fail Service Exception	Counter	0-2147483647	Total VS server responses received via the named realm indicating failure caused by a service exception.

CSV Position	HDR Column Name	Data Type	Range	Description
14	VS Fail Policy Exception	Counter	0-2147483647	Total VS server responses received via the named realm indicating failure caused by a policy exception.

STIR/SHAKEN HDR Groups - stir-stats-system

The table below lists and describes stir servers statistics and includes HDR position, statistic, type, timer value, range, and description.

CSV Position	HDR Column Name	Data Type	Range	Description
1	TimeStamp	N/A	N/A	Time that this data was written to this file.
2	AS Queries	Counter	0-2147483647	Total AS server queries made across the system.
3	AS Success Responses	Counter	0-2147483647	Total successful AS server responses received across the system.
4	AS Fail Responses	Counter	0-2147483647	Total failed AS server responses received across the system.
5	AS Fail Service Exception	Counter	0-2147483647	Total AS server responses received across the system realm indicating failure caused by a service exception.
6	AS Fail Policy Exception	Counter	0-2147483647	Total AS server responses received across the system indicating failure caused by a policy exception.
7	VS Queries	Counter	0-2147483647	Total VS server queries made across the system.
8	VS Success Responses	Counter	0-2147483647	Total successful VS server responses received across the system.
9	VS Fail Responses	Counter	0-2147483647	Total failed VS server responses received across the system.

CSV Position	HDR Column Name	Data Type	Range	Description
10	VS Success Verification	Counter	0-2147483647	Total VS server responses received across the system indicating verification success.
11	VS Fail Verification	Counter	0-2147483647	Total VS server responses received across the system indicating verification failure.
12	VS Fail Service Exception	Counter	0-2147483647	Total VS server responses received across the system indicating failure caused by a service exception.
13	VS Fail Policy Exception	Counter	0-2147483647	Total VS server responses received across the system indicating failure caused by a policy exception.

Errors and Warnings

There are no new errors or warnings added in this release.