Oracle® Enterprise Session Border Controller

Known Issues and Caveats

Release S-Cz9.1.0
F51853-12
June 2024

ORACLE

Oracle Enterprise Session Border Controller Known Issues and Caveats, Release S-Cz9.1.0

F51853-12

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.

Revision History

The following table shows the dates and descriptions of revisions to the Known Issues and Caveats Guide.

Date	Revision
March 2022	• Initial release
May 2022	• Updates for S-Cz9.1.0p1. • Corrects a typographical error in caveats.
August 2022	• Corrects the book title. • Updates for S-Cz9.1.0p2.
October 2022	• Updates for S-Cz9.1.0p3. • Adds a Known Issue for local help files.
December 2022	• Adds the "VNF in HA Mode" caveat. • Adds the "View Configuration" Caveat.
May 2023	• Re-adds H.323 to VNF limitations. • Adds the T.39 caveat. • Adds the "SBC Generates RTCP Towards the PSTN" caveat. • Adds content for S-Cz9.1.0p6. • Updates hide-egress-media-update known issue.
July 2023	• Update trace tools caveat to point to Call Monitoring Guide. • Moved "Fax over IP on Acme Packet 3950/4900" caveat to fixed Known Issue.
September 2023	• Updates for S-Cz9.1.0p8
November 2023	• Updates for S-Cz9.1.0p9 • Adds Intel limitation for software transcoding. • Adds caveat about playback headers and hairpin calls.
February 2024	• Updates for S-Cz9.1.0p10
April 2024	• Updates for S-Cz9.1.0p11. • Removes KI 35575147.
June 2024	• Updates for S-Cz9.1.0p12. • Adds Caveat regarding inactivity in the WebGUI. • Creates Resolved Known Issues topic, moving that content from the Known Issues topic.

1

Known Issues and Caveats

The following topics list the known issues and caveats for this release. Oracle updates this document to distribute issue status changes. Check the latest revisions of this document to stay informed about these issues.

Known Issues

The following table lists the known issues in version S-Cz9.1.0. You can reference known issues by Service Request number and you can identify the issue, any workaround, when the issue was found, and when it was fixed using this table. Issues not carried forward in this table from previous Release Notes are not relevant to this release. You can review delivery information, including defect fixes in the S-Cz9.1.0 Build Notes.

ID	Description	Severity	Found In
33600407	When IPv4 and IPv6 addresses are added consecutively on the hip-ip-list and icmp-address of same network-interface, followed by save/activate, the configuration change is eventually activated but the ESBC will get into unsteady state, followed by below events on the console: unregister_netdevice: waiting for <interface:id> to become free.Usage count = 1 Workaround: Add IPv4 and IPv6 address on the hip-ip-list and icmp-address separately and activate them individually i.e. activate the first config change/addition and then add and activate the second config change.	2	S-Cz8.4.0
33190562	On the AP3950 and AP4900, in < 0.1% of reboots, the platform gets stuck and does not reach the ACLI prompt. Workaround: Perform a power cycle to successfully reboot the system.	2	S-Cz9.0.0p1
32742216	The Acme Packet 1100, 3900, and 4600 as well as all software-only deployments do not support any Media Policing configuration.	3	S-Cz8.4.0
32077115	For Hairpin and Spiral call scenarios, the hide-egress-media-update parameter under media-sec-policy is not supported. In addition, you must reboot the SBC when you change the hide-egress-media-update parameter under the media-sec-policy, inbound subelement. This parameter is not RTC supported. Oracle recommends you use the hide-egress-media-update parameter under the realm-config only.	3	S-Cz9.0.0

ID	Description	Severity	Found In
32565921	The acquire-config process fails if your configuration includes an acp-tls-profile. The system does, however, successfully synch this profile after HA is established. Workaround: Disable your acp-tls-profile on the active system before performing an aquire-config procedure. Re-enable this profile after aquire-config completes successfully.	3	S-Cz9.0.0
26790731	Running commands with very long output, such as the "show support-info" command, over an OVM virtual console might cause the system to reboot. Workaround: You must run the "show support-info" command only over SSH.	2	S-Cz8.0.0
None	The system does not support SIP-H323 hairpin calls with DTMF tone indication interworking.	N/A	S-CZ720
None	The ESBC stops responding when you configure an H323 stack supporting SIP-H323-SIP calls with the **max-calls** parameter set to a value that is less than the **q931-max-calls** parameter. Workaround: For applicable environments, configure the H323 stack **max-calls** parameter to a value that is greater than its **q931-max-calls** parameter.	N/A	S-CZ7.4.0
26316821	When configured with the 10 second QoS update mechanism for OCOM, the ESBC presents the same codec on both sides of a transcoding call in the monitoring packets. You can determine the correct codecs from the SDP in the SIP Invite and 200 OK.	3	S-Cz8.0.0p1
	The ESBC dead peer detection does not work with IKEv1.	3	S-Cz8.4.0
28539190	When operating as a VNF and using Mellanox interface cards, the OCSBC does not use the Host In Path (HIP) configuration to restrict management traffic, Instead the system allows any traffic over the interface.	3	S-Cz8.2.0
28617865	This version of the OCSBC is not supported as a VNF over VMware using Mellanox interface cards.	3	S-Cz8.2.0
286588.1.0		3	
29170419	In long call scenarios, the SBC is not sending the expected refresh before the Session-Expires: header value time is up for SUBSCRIBE messages.	2	S-Cz8.2.0
34267143	No left-side Index/search in the browser for local help files.	4	S-CZ9.1.0

Resolved Known Issues

The following table provides a list of previous Known Issues that are now resolved.

ID	Description	Severity	Found In	Fixed In
35947232	The ESBC was terminating SIPREC sessions to attended transfer targets if the call flow included refer with replaces. There was no call recording after the transfer completed. Now, the ESBC terminates recording sessions to attended transfer targets after it has replaced the first call leg with the second call leg and initiated a new recording session to session recording server.	4	S-Cz9.1.0	S-Cz9.1.0p11
35614646	Certain RFC2833/ telephone-event sequences generated by customer endpoints may not be properly detected, reported, or re-transmitted by the SBC, resulting in missing DTMF digits.	2	S-Cz9.1.0p8	S-Cz9.1.0p10
33896116	HDR data files are not being replicated from the Active to Standby node. This only affects versions 8.4 and forward.	3	S-Cz8.4.0p9	S-Cz9.1.0p9
34789990	When deployed on the Acme Packet 4600, enabling the Elin-Ignore-PSAP-Source spl-option may impact the number of supported calls per second by approximately 50 CPS, reducing it to 500 CPS.	3	S-Cz9.1.0p6	S-Cz9.1.0p9

ID	Description	Severity	Found In	Fixed In
34458541	During Upgrade of an HA Pair from SCZ840 (any patch up to and including SCZ840p12) to SCZ910 (all releases), the Standby SBC running the SCZ840 release crashes as soon as one of the systems is upgraded to 910p2 and made Active. This crash occurs for the “radd” module which is responsible for CDR generation. Scenario/Condition in which issue is observed: • SBC running with Stir/ Shaken call flows • Protocol is set to RADIUS in account-config configuration attribute • cdr-output-redundancy is set to enabled (this is enabled by default) With the above configuration, once the first SBC is upgraded and made Active on the SCZ910 release, there is a chance that the standby SBC (on SCZ840) release may experience a radd crash. This is due to an issue in the SCZ840 release in which standby SBC decodes radius CDR incorrectly resulting in corruption of the buffer received from Active SBC	2	S-Cz9.1.0	S-Cz9.1.0p3

ID	Description	Severity	Found In	Fixed In
	which results in crash.			

> **Note:** This is only occurs when all three of the above conditio

ID	Description	Severity	Found In	Fixed In
		nsaremetanddoesnotapplyifonly#2and#3areenabledandtherear		

ID	Description	Severity	Found In	Fixed In
	enoStir/Shakencallflows. Workaround: The below steps can be taken as a workaround to perform an HA upgrade from SCZ840 to SCZ910 successfully without experiencing the radd crash described above. **Please note this will stop radius CDR replication to standby briefly during the upgrade.** Once the secondary box is upgraded to the SCZ910 release, perform the following steps before triggering switchover to make the upgraded box as Active: 1. Set “cdr-output-redundancy”			

ID	Description	Severity	Found In	Fixed In
	config attribute under account-config to disabled and perform save/ activate config on the active SBC (which is still on 840 release). 2. Run “notify berpd force” to make the SCZ910 upgraded SBC active. 3. Perform steps to start upgrading the second SBC. 4. While the standby system comes up after reboot, enable “cdr-output-redundancy” config attribute under account-config again on 910 SBC which is currently active. If a roll-back to SCZ840 is required, the same process must be performed.			
26497348	When operating in HA mode, the ESBC may display extraneous "Contact ID" output from the **show sipd endpoint-ip** command. You can safely ignore this output.	3	S-Cz8.0.0	S-Cz9.1.0p3

ID	Description	Severity	Found In	Fixed In
28658810	When operating as a VNF and using Mellanox interface cards, the OCSBC does not support any other type of card for media interfaces. (If any media interface uses a Mellanox card, all media interfaces must use a Mellanox card.)	3	S-Cz8.2.0	S-Cz9.1.0
26323802	The 10s QoS interim feature includes the wrong source IP address as the incoming side of a call flow. The issue does not prevent successful call and QoS monitoring. For monitoring and debugging purposes, you can find the source IP in the SIP messages (INVITE/ 200OK).	3	S-Cz8.0.0p1	S-Cz9.0.0p5
32181987	Do not copy and paste characters into a configuration menu and attempt to edit the copied text. This applies to both console and SSH sessions. Workaround: Edit the data before copy and paste.	3	S-Cz8.4.0	S-Cz9.0.0

ID	Description	Severity	Found In	Fixed In
33434641	If local-port-match value is set under security-policy, and local-port-match-max is not set, then SBC processes traffic considering full port range. SBC considers the default value of local-port-match-max (i.e. 65535) and applies the specific action mentioned under security-policy to full port range. Configure the local-port-match-max or remote-port-match-max value to set a new port range or set same value for local-port-match and remote-port-match-max to configure a single port.	2	S-Cz8.4.0p4	S-Cz8.4.0p9
32535426	The show temperature output will display different values compared to releases older than S-Cz8.3.0. Starting with S-Cz8.3.0, the temperature queries through the ACLI and SNMP are reporting more accurate values. • Similar components may not correspond between different platforms due to physical differences in each system.	3	S-Cz8.1.0	S-Cz8.3.0

ID	Description	Severity	Found In	Fixed In
33059603	On the AP3900, AP3950, and AP4900, when performing quickly successive switchovers, an active system system may not synchronize and go OOS after a failover. Workaround: Set the gateway heartbeat interval timeout value to 10 seconds with 3 gateway heartbeat retries.	3	S-Cz9.0.0p1	S-Cz9.0.0p2
31344292	The ESBC does not support HA replication of a Wildcard PAU.	3	S-Cz9.0.0	S-Cz9.0.0p1

ID	Description	Severity	Found In	Fixed In
32939208	You cannot set the ESBC **ikev2-ipsec-wancom0-params** parameters using SDM due to issues with the configuration of the **rekeyfuzz** and **localip** parameters. Note these parameters have defaults or "0" and "empty" respectively. You can, however, configure these values from the ESBC . You cannot set the OCSBC ikev2-ipsec-wancom0-params via SDM due to issues in configuration of parameters rekeyfuzz and localip, which have defaults or "0" and "empty" respectively, using OCSDM. Furthermore, if you change the values for **rekeyfuzz** and **localip**, you cannot change them back to their defaults. Workaround for changing these parameters' values back to their defaults: 1. remove the **ikev2-ipsec-wancom0-params** element from your configuration. 2. Add the element again and set your values.	3	S-Cz9.0.0	S-Cz9.0.0p1

ID	Description	Severity	Found In	Fixed In
24574252	The **show interfaces brief** command incorrectly shows **pri-util-addr** information in its output.	3	S-Cz7.4.0	S-Cz9.0.0
ACMECSBC-38270	Do not configure STIR over TLS. This configuration causes the system to crash.	3	S-Cz9.0.0	S-Cz9.0.0p1
32939113	Do not configure the **auth-user-lookup** parameter within the **local-policy**, **policy-attribute** without already having: • A configured **sip-interface** or, • If that **sip-interface** does not point to a configured **realm** If either of these conditions are true, the ESBC crashes when you perform a **save-config** or a **verify-config**. Workaround: Configure the applicable **sip-interface** and associated realms before you configure the **local-policy**, **policy-attribute**, **auth-user-lookup** parameter.	3	S-Cz9.0.0	S-Cz9.0.0p1
29439964	ACLI Users will receive an error on the output of the show registration sipd by-user command.	4	S-Cz8.2.0	S-Cz8.4.0

ID	Description	Severity	Found In	Fixed In
32534935	Media is not resumed after RBT playback for transcoded calls on vSBC. Avoid upgrading to releases where this bug is open if your deployment uses a vSBC with Transcoding and is configured to use Ringback-Trigger values.	3	S-Cz8.4.0M0P4	S-Cz9.0.0
31163030	In VOLTE deployments with registration refreshes, you may see unusually large numbers in the **alloc** and **usage** count fields while executing the **show buffers** command. This is a known statistics accounting issue.	4	S-Cz8.3.0	S-Cz9.0.0

ID	Description	Severity	Found In	Fixed In
31315823	When running IMS-AKA over UDP on virtual ESBCs, IMS-AKA registrations may not succeed. Registration failure can also cause associated calls to fail. Oracle has observed this only happens after a system reboot. Oracle has also observed that performing a Save and Activate command sequence after a reboot ensures these registrations are successful. If you are running IMS-AKA over UDP on virtual ESBCs, perform a Save and Activate command sequence after system reboot to ensure successful IMS-AKA registrations.	3	S-Cz8.4.0	S-Cz9.0.0
31828563	While using STIR/SHAKEN, Acme Packet 4600 performance is capped at 330 CPS, and Acme Packet 6350 performance is capped at 1200 CPS for both dual and quad NIU cards.	3	S-Cz8.4.0M0P2	S-Cz9.0.0

ID	Description	Severity	Found In	Fixed In
	Do not upgrade to S-Cz9.0.0 directly from S-Cz8.4.0p4, S-Cz8.4.0p5 or any S-Cz8.4.0p5 OOC patches up to S-Cz8.4.0p5B. If running these versions, upgrade to S-Cz8.4.0p5C before upgrading to S-Cz9.0.0. Upgrading directly from these versions may cause the system to crash. When upgrading from these versions, upgrade to S-Cz8.4.0p5C first.	3	S-Cz8.4.0M0P4	S-Cz8.4.0M0P5
29881449	The DSP used by the OCSBC has a vendor firmware defect that causes failures with the T.38 codec. If you are using the T.38 codec, you may experience minimal media losses on those calls. This problem may also cause the OCSBC to reboot.	3	S-Cz8.1.0m1p9	S-Cz8.4.0p4
32517222	Media is not resumed after RBT playback for transcoded calls on vSBC. Avoid upgrading to releases where this bug is open if your deployment uses a vSBC with Transcoding and is configured to use Ringback-Trigger values.	3	S-Cz8.4.0M0P4	S-Cz8.4.0P4A

ID	Description	Severity	Found In	Fixed In
30794993	Please see the section on Upgrades For Configurations that Include Signaled IPSec Tunnels and LI Configurations in Upgrade Downgrade Caveats in this document for an explanation of this issue.	3	S-Cz8.4.0	S-Cz9.0.0
28618563	The system is not populating the Username AVP in Accounting Requests (ACRs) correctly. When triggered by an INVITE, these AVPs contain only the "@" sign. They do not include the username and domain name portion of the URL.	3	CZ8.1.0m1	S-Cz8.4.0
31726575	Do not configure sip-advanced-logging if you expect any auth-invite call flows (401/407). If you are upgrading to S-Cz8.4.0p2 or later, and your configuration includes conditional logging (session-router, sip-advanced-logging, state=enabled), you must first remove sip-advanced-logging from the config, otherwise calls will fail. • Setting the state to disabled does not work and removing it is required.	2	S-Cz8.4.0p2	S-Cz8.4.0p4

ID	Description	Severity	Found In	Fixed In
32049267	Do not configure AEAD_AES_256_GCM cipher in the sdes-profile, crypto-list parameter, or the system will crash.	3	S-Cz8.4.0p3	S-Cz8.4.0p4
30794993	The ESBC might display an excessive number of debug messages after an HA switchover, if you configured both X123 LI and IKEv2/IPSec with IPv6 security policies. You can safely ignore these messages.	4	S-Cz8.4.0	S-Cz8.4.0p2

ID	Description	Severity	Found In	Fixed In
31384643	During the testing of this release Oracle identified a pre-existing issue in the code where adding an LI warrant during a period of heavy SIP load may cause the system to stop responding, which results in a switchover. This issue exists in prior releases and will be addressed in an upcoming 8.4 patch. If you have not encountered this issue in the past, it is unlikely that you will encounter it now. System Impact: If you add an LI warrant while the ESBC is under heavy load from SIP traffic, a mid-call intercept operation may not occur after the addition (causing the ESBC to stop responding). If the ESBC stops responding a switchover will occur, but the warrant will have been added correctly. The issue can be mitigated by performing addition of LI warrants during off-peak times, such as maintenance windows.	3	S-Cz8.4.0	S-Cz8.4.0p2

ID	Description	Severity	Found In	Fixed In
30364057	Do not use DNS for multiple services on the OCSBC simultaneously. DNS service operates on the OCSBC normally when you configure it for a single purpose. When you configure it for multiple purposes, however, lookups do not complete correctly. Workaround: An example of this would be configuring DNS for both PCRF and ENUM services. You can mitigate this issue by configuring the local routing table with ENUM lookups.	3	S-Cz8.3.0p7	S-Cz8.3.0m1p5
29862440	When transcoding from T.38 to G711FB, the OCSBC includes multiple (for example 2) m-lines in the SDP when there are multiple (for example 2) c-lines in the source SDP. This happens even if you have set the fax-single-m-line parameter in the applicable codec-policy to present a single m-line. Workaround: Configure an ingress HMR to remove all but 1 c-line from the incoming SDP.	3	S-Cz7.4.0m1p8	S-Cz8.3.0m1p3

ID	Description	Severity	Found In	Fixed In
30158557	Under high media loads that include AMR/AMR-WB to PCMA transcoding, the 10G port on the Acme Packet 6300 is experiencing packet loss and, therefore media MOS degradation.	2	S-Cz8.1.0m1p16	S-Cz8.4.0
30444535	When configured for the minimum TCP disconnect time, the default for network-parameters, the OCSBC takes an unexpectedly long time before attempting to create a socket and connect. When using the defaults to create and connect using the minimum amount of time, this process takes 18 seconds instead of 9.	3	N/A	S-Cz8.3.0m1p3
29846828	The OCSBC stops generating registration refreshes after 12 hours for Surrogate Agents. After a reboot, the OCSBC attends to registration and refreshes correctly using the new Call ID for 12 more hours.	2	E-Cz8.1.0m1p8	S-Cz8.1.0m1p22

ID	Description	Severity	Found In	Fixed In
30330778	The OCSBC cannot forward a call that uses a TEL-URI and includes the routing number (rn) parameter. Depending on your routing configuration, the OCSBC may reject these call with a 404 Not Found/No Route to Destination. The OCSBC forwards these portability scenarios properly when they present an R-URI.	1	S-Cz7.4.0m2p4;8.1.0m1p18	S-Cz8.1.0m1p23
29779932	The OCSBC uses a Diffie Hellman algorithm that conflicts with that of the 10.4 Solaris SFTP server. As a result, both CDR and HDR transfers to these servers fail. Do not use the Solaris 10.4 SFTP server with the OCSBC.	1	S-Cz8.1.0m1p9, S-Cz8.3.0p7	S-Cz8.3.0m1p4
29403076	When generating HDR reports and SNMP output on resource utilization that includes threads, the OCSBC omits the thread name, leaving the applicable field and OID empty.	3	S-Cz8.1.0M1P9	S-Cz825p3
310398.2.0	When mid-call Lawful Intercept is enabled, and the SBC has not started intercepting particular sessions, those sessions will not be replicated on the standby. If a switchover occurs, affected calls could be dropped.	3	S-Cz8.3.0m1p2	S-Cz8.4.0

ID	Description	Severity	Found In	Fixed In
26432028	On the Acme Packet 1100, Acme Packet 3900, and VME un-encrypted SRTP-SDES calls result in one-way audio.	3	E-Cz7.5.0	S-Cz8.0.0
28157960	When setting up a SIPREC session, the SBC sets up 1-way audio if the far end offers an odd port number in the m line.	2	S-Cz8.0.0	S-Cz8.3.0m1p8
26669090	The ESBC dead peer detection does not work with IPv4.	3	S-Cz8.0.0	Could not reproduce - S-Cz8.4.0
22322673	When running in an HA configuration, the secondary ESBC might go out of service (OoS) during upgrades, switchovers, and other HA processes while transitioning from the "Becoming Standby" state. Oracle observes such behavior in approximately 25% of these circumstances. You can verify the issue with log.berpd, which can indicate that the media did not synchronize. Workaround: Reboot the secondary until it successfully reaches the "Standby" state.	3	S-Cz7.3.0P1	S-Cz8.0.0
29931732	The embedded communications monitor probe does not send IPv6 traffic to the Oracle Communications Operations Monitor's mediation engine.	3	S-Cz8.0.0	S-Cz8.3.0m1p4

ID	Description	Severity	Found In	Fixed In
30375697	Infrequently during race conditions, the number of SIP registration entries on the active and standby SBCs differs, with the standby SBC containing fewer entries. When this happens and a switchover occurs, some endpoints are unable to receive calls until the endpoint re-registers. Increase Journal index size and optimize the Journal management code to avoid this.	2	S-Cz8.1.0m1p18	S-Cz8.1.0m1p18b
30544663	When a session add action is executed and the session is not found in the sipProxy, a new Sip Session and two Sip Dialogs are created and cross referenced and the buffer from the active is loaded. If the load fails, the update function exits and the SipSession and SipDialogs are left dangling and create a memory leak. Workaround: To avoid this memory leak, successfully load the buffer BEFORE creating the session and dialogs. Monitor the standby SBC's memory usage and reboot as needed.	3	S-Cz8.1.0m1	S-Cz8.1.0m1p18b

ID	Description	Severity	Found In	Fixed In

30498837	A sipd process crash occurs with a signature containing the following:
	
	`ZNSt8_Rb_tree ISsSt4pairIKS s4SptrI10SipC ontactEESt10* _Select*1stIS 5_ESt4lessIS sE SaIS5_EE11equ al_rangeERS1_ (+ 0x67) - sp = 0x7f334938d38 0, ip = 0x1f1b117`
	
	The SBC can leak File Descriptors in cases where there are certain process errors. For example:
	
	`[MINOR] (0) Selector::do_ select() - epoll_ctl(DEL , 409) failed with errno=9:Bad file descriptor)`
	
	This does not trigger proper closure of sockets. This is avoided by closing the socket that was opened and then setting an error identifying exact error code.
		2	S-Cz8.1.0m1p18	S-Cz8.1.0m1p18b

ID	Description	Severity	Found In	Fixed In
29403076	The "thread-event" and "thread-usage" HDR categories are displaying incorrectly due to MBCD and SIPD thread names not properly writing into the files and OID output. MBCD and SIPD now properly assign and pass the proper names.	3	S-Cz8.1.0m1p9	S-Cz8.1.0m1p18b
29633588	During certain configuration activities, the SBC restarts due to an issue caused by improper configuration steps being processed in the **sip-manipulation**, **header-rules**. The SBC now returns an error message stating "Invalid Selection" instead of failing.	3	S-Cz8.1.0m1p11	S-Cz8.1.0m1p18b
29937232	GW unreachable and NetBufCtrl MBUFF errors - This can result in system instability including crash, gw-unreachable and redundancy issues. System will switchover if in HA. Show Buffers output will normally show an increase of errors reported in the NetBufCtrl field due to mbuf's not being freed.	2	S-Cz8.3.0	S-Cz8.3.0p6

ID	Description	Severity	Found In	Fixed In
288.2.0258	On VNF platforms, when running TLS Chat on VMware-PV 4core (SSFD) + 16GB, TLS Chat sessions are gradually decreasing. When looking in Wireshark at EXFO, EXFO forwards a wrong TLS MSRP Chat payload to EXFO UAS. TCP Chat does not have this error.	3	S-Cz8.0.0	S-Cz8.3.0m1p2
	For Advanced Media Termination deployments using the 4600, 6300, 6350 platforms, the SBC is generating RTP and RTCP on the ports 20000 and 20001, instead of generating both on the same port 20000.	3	S-Cz8.3.0	S-Cz8.3.0m1p2
29522609	Some calls that are configured to generate ring back tones result in one-way audio.	2	S-Cz8.3.0	S-Cz8.3.0m1p2
29607573	The SBC is unable to successfully initiate a TCP connection to configured Diameter Accounting (Rf) servers.	2	S-Cz8.3.0	S-Cz8.3.0m1p2
30114764	When presenting the content type for SPIROU during SIP to SIPI interworking, the SBC is displaying the text **base=spirou**. Based on relevant standards, it should display **base=itu-92+** as the content type.	4	S-CZ8.3.0m1	S-Cz8.3.0m1p2

ID	Description	Severity	Found In	Fixed In
30127762	When performing SIP to SIPI interworking, the SBC is not including an ISUP REL in the interworked body of its **400 Missing CSeq** message when it rejects applicable calls from the SIPI side.	4	S-CZ8.3.0m1	S-Cz8.3.0m1p2
30240798	The OCSBC closes connections when using some SFTP clients, including WinSCP and MOBA, to upload files over 200KB. Workaround - Use the Linux or Filezilla SFTP client when uploading files greater than 200k.	3	S-CZ8.3.0p6	S-Cz8.3.0m1p2
30289027	Azure does not always properly reset media interfaces after the OCSBC reboots. Instead, Azure sometimes tries to process a non-existent packet as soon as the OCSBC comes back up, resulting in a kernel panic. Workaround - If you experience a kernel panic after OCSBC reboot, stop and restart the vSBC from the Azure UI.	3	S-Cz8.3.0	S-Cz8.3.0m1p2

ID	Description	Severity	Found In	Fixed In
28617938	The **anonymize-invite** option for CommMonitor is not RTC. To see a change, you must either reboot or toggle the admin state. The following is a general admin state toggle procedure: 1. Set admin state to disabled. 2. Save and activate. 3. Set admin state to enabled. 4. Save and activate.	4	CZ8.1.0m1	S-Cz8.3.0
29556215	The SBC does not send SIPREC data to a remote call server.	2	S-Cz8.3.0	S-Cz8.3.0p5
29608499	In all documents except for the Release Notes and Installation guide, the printed version of this release (S-Cz8.3.0) is incorrectly displayed as S-Cz8.2.0.	4	S-Cz8.3.0	S-Cz8.3.0p3
28539155	When operating as a VNF and using Mellanox interface cards, the OCSBC does not support ICMP over IPv6.	3	S-Cz8.2.0	S-Cz8.3.0
28526228	Maximum SRTP capacity on VNF platforms is 25% lower than in the S-Cz8.1.0 release. Expected capacity will be restored in a follow up patch.	3	S-Cz8.2.0	S-Cz8.3.0

ID	Description	Severity	Found In	Fixed In
26313330	In some early media call flows, the ESBC may not present the correct address for RTP causing the call to terminate.	3	S-Cz8.0.0	S-Cz8.2.0
26281599	The system feature provided by the **phy-interfaces overload-protection** parameter and **overload-alarm-threshold** sub-element is not functional. Specifically, enabling the protection and setting the thresholds does not result in trap and trap-clear events based on the interface's traffic load. The applicable ap-smgmt.mib SNMP objects include: • apSysMgmtPhyUtilThresholdTrap • apSysMgmtPhyUtilThresholdClearTrap	3	S-Cz720	S-Cz8.2.0
27539750	When trying to establish a connection between the SBC and your network, while using TLS version 1.2, the SBC may reject the connection. Workaround: You may need to adjust your cipher list.	3	S-Cz8.1.0	S-Cz8.1.0

ID	Description	Severity	Found In	Fixed In
28062411	Calls that require SIP/PRACK interworking as invoked by the 100rel-interworking option on a SIP interface do not work in pooled transcoding architectures.	2	S-Cz7.4.0	S-Cz8.2.0
None	The CZ8.1.0 release does not support IPSec on the Acme Packet 3900 and VNF. You must upgrade to CZ8.1.0p1 to get this support. After you upgrade to CZ8.1.0p1, do the following: 1. Run **setup entitlements**, again. 2. Select **advanced** to enable advanced entitlements, which then provides support for IPSEC on Acme Packet 3900 and VNF systems.	N/A	S-Cz8.1.0	S-Cz8.2.0
28.3.05575	On VNFs, the system erroneously displays the IPSEC entitlement under "Keyed (Licensed) Entitlements." The error does not affect any functionality and you do not need to do anything.	4	S-Cz8.1.0	S-Cz8.2.0

ID	Description	Severity	Found In	Fixed In
28659469	When booting CZ8.1.0M1 on any virtual platform, not all system processes start. This known issue only occurs on initial boot, and not in an upgrade scenario. Workaround: Reboot the ESBC a second time, after it initially starts.	3	SCz8.1.0m1	S-Cz8.2.0
27240195	The **cpu-load** command does not display the correct value under **show-platforms**.	3	E-Cz8.0.0	S-Cz8.2.0
	If you configured the ims_aka option, you must also configure sip-interfaces with an ims-aka-profile entry.	3	E-Cz7.4.0	E-Cz7.4.0m1
27795586	When running E-Cz8.1.0 over Hyper-V, and you set the process-log level to DEBUG, the system can become unstable or stop responding. The system requires a reboot. Workaround: Do not enable process-log level DEBUG.	3	E-Cz8.1.0	S-Cz8.2.0
28475320	When running E-Cz8.1.0M1 on the Acme Packet 3900, IPSec functionality is not available.	2	S-Cz8.1.0	S-Cz8.2.0
32849192	The Data Integrity entitlement does not work properly, sometimes introducing system instability. Do not enable the Data Integrity entitlement.	2	S-Cz9.0.0	S-Cz9.0.0p1

ID	Description	Severity	Found In	Fixed In
34233796	T.38 transcoding is not available on the Acme Packet 3950 and Acme Packet 4900 platforms.	2	S-Cz9.1.0 GA	S-Cz9.1.0p3

The following Known Issues and Caveats do not occur in this release. They are listed here for tracking purposes.

ID	Description
36200606	The SBC stops processing calls from other IP addresses coming into the realm if the realm is marked with trust level high and there is a static ACL configured for the realm. When operating over the Azure platform, the ESBC displays an inordinate number of kernel messages during the bootup process. You can safely ignore these messages.
23756306	When you configure the session-router with an operation-mode of session, it does not correctly clear sessions.
25954122	Telephony Fraud Protection does not blocklist calls after a switchover. Workaround: Activate the fraud protection table on the newly active server.
31162394	Running SIPREC on the Acme Packet 4600 over 1G interfaces may result in system instability. Workaround : Do not egress traffic out of a physical interface that exceeds the bandwidth of the physical media capacity. You should determine the amount of egress media traffic and the amount of intercepted traffic on that interface. The intercepted traffic could be any recorded traffic on the interface like (SIPREC, LI, and remote packet trace).
26260953	Enabling and adding Comm Monitor config for the first time can create a situation where the monitoring traffic (IPFIX packets) does not reach the Enterprise Operations Monitor. Workaround: Reboot the system.
33751575	Deployments must not signal any SILK codec with 12000 or 24000 clock rate in SDP to the ESBC. Furthermore, the ESBC must not use any SILK media profile with 12000 or 24000 Hz clock rate. Under these conditions, there is a risk of system memory corruption that can potentially lead to a transcoding core crashing.
26598075	When running on the Acme Packet 4600, the OCSBC sends a 200OK with IPv4 media address for call flows with offerless INVITES and the OCSBC configured with add-sdp-invite=invite and ALTC configured for IPv6 on the egress.

ID	Description
26559988	In call flows that include dual ALTC INVITEs from the callee, and subsequent Re-INVITEs that offer an ALTC with IPv6 video, the OCSBC may not include the m lines in the SDP presented to the end stations during the Re-INVITE sequence. This results in the call continuing to support audio, but not video.
28748784	When operating as a VNF and using Mellanox interface cards, the OCSBC does not support outbound ICMP.
30612465	On Virtual platforms, the OCSBC is not forwarding traffic transcoded to EVS or Opus codecs if you have configured the applicable policy with a forced ptime of 60ms.
21805139	RADIUS stop records for IWF calls may display inaccurate values.
26136553	The ESBC can incur a system-level service impact while performing a switchover using "notify berpd force" with an LDAP configuration pointing to an unreachable LDAP server. Workaround: Ensure that the ESBC can reach the LDAP server before performing switchover.
28770472	ACLI Users will receive an error on the output of the show registration sipd by-user command.
29999832 and 30194470	
32062551	Virtual SBC platforms may incorrectly assess link status thereby causing major health degradation and triggering a failover.
30595413	The IKEv2/IPSEC negotiation fails while using TRANSPORT MODE and different IP’s for IKE and SIP interfaces.
23253731	After an HA switchover, the new standby ESBC retains some IMS-AKA subscriber TCP sockets. You can clear these sockets by rebooting the ESBC.
29005944	On Acme Packet hardware in an HA configuration, with a large number of IMS-AKA endpoints, the standby is unable to synchronize, and when rebooted goes OOS.
27031344	When configured to perform SRTP-RTP interworking, the ESBC might forward SRTP information in the SDP body of packets on the core side, causing the calls to terminate. Workaround: Add an appropriately configured media-sec-policy on the RTP side of the call flow. This policy is in addition to the policy on the SRTP side of the call flow.
30520181	When performing large numbers of simultaneous registrations, such as during a registration flood, the OCSBC may become unstable and stop responding when it exceeds 200k IMS-AKA subscriber registrations.

ID	Description
ACMECSBC-23446 24809688	Media interfaces configured for IPv6, and using different VLANs that operate over different infrastructures, including VoLTE and 3GPP, are not supported.
28639227	When operating as a VNF and using Mellanox interface cards, the OCSBC does not support SCTP transport.
28906914	For transcoding use cases, the G711/G729 codec pair might experience unstable performance when each DSP has greater than 500 transcoding sessions.
N/A	The T.140-Baudot Relay is not excluded from supported features with pooled transcoding.
N/A	When operating as a VNF deployed in an HA configuration, the OCSBC does not support IPSec.

Caveats and Limitations

The following information lists and describes the caveats and limitations for this release. Oracle updates this Release Notes document to distribute issue status changes. Check the latest revisions of this document to stay informed about these issues.

Overlap of Data Between Widgets During Periods of Inactivity

When the dashboard is left open for 20 minutes or more without performing any action other than keeping the session alive on the WebGUI, the data between different widgets may overlap occasionally. Workaround: Refresh the page to resolve this issue.

New Keys Required for High Availability

If you replace a peer in HA from a system running software prior to S-Cz9.1.0p9 to 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.

The SBC Generates RTCP Towards the PSTN

Scenario: In a pooled transcoding configuration, the transcoding Session Border Controller (SBC) has a single realm with rtcp-policy enabled. On the MSTeams realm, rtcp-policy is enabled on the signaling SBC and rtcp-policy is disabled on the PSTN realm.

Behavior: Because rtcp-policy is enabled on the transcoding realm, the PSTN will also receive rtcp packets even though rtcp-policy is not enabled on the PSTN realm. MSTeams will receive RTCP packets, as intended.

The Web GUI Shows No Configuration Data After Clicking "View Configuration"

When you set the process level or system log level to DEBUG, the Web GUI may not display any configuration information for large configurations when you click "View Configuration".

Acquire Config and acp-tls-profile

The **acquire-config** process fails if your configuration includes an **acp-tls-profile**. The system does, however, successfully synch this profile after HA is established.

Workaround: Disable your **acp-tls-profile** on the active system before performing an **acquire-config** procedure. Re-enable this profile after **aquire-config** completes successfully.

VNF in HA Mode

When the SBC VNF is running in HA mode, any existing IPSec tunnels do not fail over the standby SBC.

Toggling SIP Interfaces Running TCP

You must reboot the system any time you disable, then enable an active SIP interface that is using TCP.

Provisioning Transcode Codec Session Capacities

When a transcode codec was originally provisioned in an earlier software version with a license key, a capacity change using the **setup entitlements** command requires a reboot to take effect.

Virtual Network Function (VNF) Caveats

The following functional caveats apply to VNF deployments of this release:

- The OVM server 3.4.2 does not support the virtual back-end required for para-virtualized (PV) networking. VIF emulated interfaces are supported but have lower performance. Consider using SR-IOV or PCI-passthru as an alternative if higher performance is required.
- To support HA failover, MAC anti-spoofing must be disabled for media interfaces on the host hypervisor/vSwitch/SR-IOV_PF.
- You may need to enable trust mode on the host PF, when using Intel X/XL7xx [i40e] NICs with SR-IOV, before you can use VLANs or HA virtual MAC on the guest VF. Refer to the Intel X710 firmware release notes for further information.
- MSRP support for VNF requires a minimum of 16GB of RAM.
- The system supports only KVM and VMWare for virtual MSRP.
- CPU load on 2-core systems may be inaccurately reported.
- IXGBE drivers that are a part of default host OS packages do no support VLANs over SR-IOV interfaces.
- Software-based transcoding on vSBCs is not supported on servers with AMD CPUs.

Virtual Network Function (VNF) Limitations

Oracle® Enterprise Session Border Controller (ESBC) functions not available in VNF deployments of this release include:

- FAX Detection
- T.38 FAX IWF
- RTCP detection
- H.323 signaling or H.323-SIP inter-working
- ARIA Cipher

Transcoding - general

Only SIP signaling is supported with transcoding.

Codec policies can be used only with realms associated with SIP signaling.

T.38 Fax Transcoding

T.38 Fax transcoding is available for G711 only at 10ms, 20ms, 30ms ptimes.

Pooled Transcoding for Fax is unsupported.

Pooled Transcoding

The following media-related features are not supported in pooled transcoding scenarios:

- Lawful intercept
- 2833 IWF
- Fax scenarios
- RTCP generation for transcoded calls
- OPUS codec
- SRTP and Transcoding on the same call
- Asymmetric DPT in SRVCC call flows
- Media hairpinning
- QoS reporting for transcoded calls
- Multiple SDP answers to a single offer
- PRACK Interworking
- Asymmetric Preconditions

DTMF Interworking

RFC 2833 interworking with H.323 is unsupported.

SIP-KPML to RFC2833 conversion is not supported for transcoded calls.

H.323 Signaling Support

If you run H.323 and SIP traffic in system, configure each protocol (SIP, H.323) in a separate realm.

Media Hairpinning

Media hairpining is not supported for hair-pin and spiral call flows involving both H.323 and SIP protocols.

Fragmented Ping Support

The Oracle® Enterprise Session Border Controller does not respond to inbound fragmented ping packets.

Physical Interface RTC Support

After changing any Physical Interface configuration, you must reboot the system.

SRTP Caveats

The ARIA cipher is not supported by virtual machine deployments.

Packet Trace

- Output from the **packet-trace local** command on hardware platforms running this software version may display invalid MAC addresses for signaling packets.
- The **packet-trace remote** command does not work with IPv6.
- If any conflicting applications are enabled, the **packet-trace** command displays a warning. Conflicting applications are comm-monitor, call-trace, and SIP Monitor and Trace.

Trace Tools

See the Monitoring Warning in the Call Monitoring Guide before running any monitoring service like SIPREC, Communications Operation Monitor, Packet Trace, call-trace, or SIP Monitoring and Trace (on the ESBC).

RTCP Generation

Video flows are not supported in realms where RTCP generation is enabled.

SCTP

SCTP Multihoming does not support dynamic and static ACLs configured in a realm.

SCTP must be configured to use different ports than configured TCP ports for a given interface.

MSRP Support

The Acme Packet 1100 platform does not support the MSRP feature set:

When running media over TCP (e.g., MSRP, RTP) on the same interface as SIP signaling, TCP port allocation between media and signaling may be incompatible.

- Workaround: Set the **sip-port**, **address** parameter to a different address than where media traffic is sent/received, the **steering-pool**, **ip-address** value.

Real Time Configuration Issues

In this version of the ESBC, the **realm-config** element's **access-control-trust-level** parameter is not real-time configurable.

Workaround: Make changes to this parameter within a maintenance window.

High Availability

High Availability (HA) redundancy is unsuccessful when you create the first SIP interface, or the first time you configure the Session Recording Server on theOracle® Enterprise Session Border Controller (ESBC). Oracle recommends that you perform the following work around during a maintenance window.

1. Create the SIP interface or Session Recording Server on the primary ESBC, and save and activate the configuration.
2. Reboot both the Primary and the Secondary.

Offer-Less-Invite Call Flow

Call flows that have "Offer-less-invite using PRACK interworking, Transcoding, and dynamic payload" are not supported in this release.

Fragmented SIP Message Limitations

Fragmented SIP messages are intercepted but not forwarded to the X2 server if IKEv1/IPsec tunnels are configured as transport mode.

Workaround: Configure IKEv1/IPsec tunnels as "tunnel mode".

HA Deployment on Azure

HA deployments on Azure are not supported.

Graphical User Interface

When maximizing and minimizing the browser, the WEB GUI is not currently compensating correctly for display changes in tables that require scrolling. This can corrupt the display of tables in ESBC GUI management dialogs.

Simultaneous Use of Trace Tools

See "Trace Tools" caveat.

IKE

ECDSA certificates are not supported with IKEv2 configurations.

Acme Packet 3950/4900 Power Button

When running release 9.0.0 on the Acme Packet 3950 and the Acme Packet 4900, the power button may not function correctly. Upgrade to 9.0p1 or later to correct this.

Acme Packet 3950/4900 Excluded Features

The following features are not supported on the Acme Packet 3950 or Acme Packet 4900:

- VoLTE
- LI-PCOM
- IMS-AKA
- Diameter RX

Acme Packet 3950/4900 Transcoding Module Compatibility

The transcoding modules in the Acme Packet 3950 and Acme Packet 4900 are not compatible with other physical platforms.

IWF

IWF (SIP-H323) appears at the setup entitlements prompt on virtual platforms when H.323 is not supported.

SIPREC Post REFER Processing

For SIPREC calls that use the Universal Call ID SPL and also exercise SIPREC on main call flow, the ESBC does not include UUID in ACK or BYE messages post REFER processing.

Acme Packet 1100 Debug log Level

Do not set log level to DEBUG on the Acme Packet 1100.

Acme Packet Platform Monitoring Caveats

The SFP INSERTED and SFP REMOVED Alarms and corresponding traps are not supported on the following platforms:

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

IPSec Trunking Tunnel Caveat

The **setup entitlements** command allows to set a maximum of 2500 IPSec trunking tunnels. Each IPSec trunking tunnel secures signaling and media traffic for more than one SIP session. You can either set a maximum of 2500 trunking tunnels or less, while configuring the session capacity. Setting a maximum value for trunking tunnel does not limit the configured session capacity.

Playback Headers and Hairpin Calls

Playback headers are not supported in hairpin calls.

Limitations Removed

The limitations listed in this section are no longer applicable on this version of the ESBC.

Remote Packet Trace

Remote packet trace is now supported on the Acme Packet 1100, 3900, and 4900 platforms. It is also now supported over virtual platforms.

IPSec on Virtual Platforms

IPSec functionality including authentication header (AH) support is available on virtual platforms and the Acme Packet 3900.