Oracle® Session Border Controller

Known Issues and Caveats

Release S-Cz9.3.0

F92219-18

June 2026

Oracle Session Border Controller Known Issues and Caveats, Release S-Cz9.3.0

F92219-18

Copyright © 2024, 2026, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about content, products, and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services unless otherwise set forth in an applicable agreement between you and Oracle. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services, except as set forth in an applicable agreement between you and Oracle.

ADD THE FIRST PARAGRAPH HERE.

ADD THE NEXT PARAGRAPH HERE.

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.

Contents

About this Guide

Revision History

1 Known Issues and Caveats

Known Issues 1
Resolved Known Issues 3
Caveats 53
Limitations 60
Limitations Removed 65

Copyright © 2024, 2026, Oracle and/or its affiliates.

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.

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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Revision History

This section provides a revision history for this document.

Date	Revision
March 2024	• Initial release
March 2024	• Adds KI regarding TCP and UDP usage.
April 2024	• Removes KI 35575147; not a software defect.
May 2024	• Adds Caveat regarding inactivity in the WebGUI. • Creates Resolved Known Issues topic, moving that content from the Known Issues topic.
July 2024	• Updates for S-Cz9.3.0p2.
October 2024	• Updates for S-Cz9.3.0p3. • Adds DTLS-SRTP cipher limitation on HWDP platforms
November 2024	• Adds LI Known Issue. • Adds TLS handshake failure Known Issue.
December 2024	• Updates for S-Cz9.3.0p4.
February 2025	• Removes RTCP limitations on vSBC. • Updates for S-Cz9.3.0p5.
April 2025	• Updates for S-Cz9.3.0p6. • Corrects caveat on certificates not supported by IKEv2. • Adds Known Issue on restore-backup-config command.
June 2025	• Updates for S-Cz9.3.0p7.
August 2025	• Updates for S-Cz9.3.0p8. • Adds caveat on HDR push issues, based on the use of an insecure cipher. • Adds memory-usage limitation for AP4900. • Clarifies fragmented SIP message limitations.
November 2025	• Updates for S-Cz9.3.0p9.
January 2026	• Updates for S-Cz9.3.0p10. • Adds caveat regarding Encryption and FAX Transcoding on the same call.
June 2026	• Updates for S-Cz9.3.0p13. • Moves load-limit to resolved known issues. • Cleaned up closed defects.

Copyright © 2024, 2026, Oracle and/or its affiliates.

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 this release. You can reference known issues by Service Request ID 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-Cz9.3.0 Build Notes.

ID	Description	Severity	Found In
33600407	When you add IPv4 and IPv6 addresses consecutively on the hip-ip-list and icmp-address of the same network-interface, followed by save and activate, the system eventually activates the configuration change but the SBC goes into an unsteady state with the following 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. For example, activate the first config change or addition and then add and activate the second configuration change.	2	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
32565921	The acquire-config process is unsuccessful when your configuration includes an acp-tls-profile. The system does successfully synch the profile after establishing HA. Workaround: Disable your acp-tls-profile on the active system before performing an aquire-config procedure. Re-enable the profile after aquire-config completes successfully.	3	S-Cz9.0.0

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In
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	Re-balancing is unavailable on the OCSLB when running an Acme Packet 6300 as a cluster member. Set the SLB **cluster-config**, **auto-rebalance** parameter to **disabled** to use an Acme Packet 6300 as a cluster member from that SLB.	N/A	S-Cz730
None	The system does not support SIP-H323 hairpin calls with DTMF tone indication interworking.	N/A	S-CZ720
None	The SBC 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
None	The system does not support HA Redundancy for H.323 calls.	N/A	N/A
27699451	Oracle qualified the QSFP interface for the OCSR operating over the Oracle X9-2 platforms for a single QSFP port operating in 4-port mode. Specifically, 4 media interfaces successfully map to the second port of the QSFP interface using a Hydra cable as physical connections to 10G switch ports.	3	S-Cz8.1.0
	The SBC 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
29170419	In long call scenarios, the SBC does not send the expected refresh before the Session-Expires: header value time is up for SUBSCRIBE messages.	2	S-Cz8.2.0
30643522	Starting with S-Cz8.3.0m1p2, Lawful Intercept users cannot modify LI configuration with the Session Delivery Manager. Workaround: LI Configuration must be performed through the ACLI.	4	S-Cz8.3.0m1p2
34267143	No left-side Index and search in the browser for local Help files.	4	S-CZ9.1.0

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In
34991934	Do not upgrade any device licensed to use FIPS to S-Cz9.1.0, S-Cz9.2.0, S-Cz9.3.0, or S-Cz10.0.0. These releases disable FIPS mode on the SBC. Attempting to use FIPS mode on these releases can lead to call failures and unstable system behavior.	3	S-Cz9.2.0

Resolved Known Issues

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

ID	Description	Severity	Found In	Fixed In
36001121	The **suppress-hold-resume-reinvite** feature does not work if the applicable Hold and Resume Re-INVITEs do not include SDP.	3	S-Cz9.3.0	S-Cz9.3.0p1
37522199	ACLI is allowing the configuration of **max-signaling-packets** under **media-manager** to exceed the actual **max-signaling-rate** a system capacity allows.			

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
35641698	When supporting IPSEC tunnels using IKEv1 in initiator mode, and when the endpoint initiates an Security Association renewal sequence (rekey/refresh) over the connection, the SBC can lose connectivity to that endpoint after an HA switchover. This behavior can be considered rare because the SBC is configured as the initiator. Workaround: An example scenario that causes this behavior is when connection rekey requests come from the endpoint. This can occur because the rekey timing configuration on the endpoint is shorter than that of the SBC. A workaround for this scenario is to manually configure rekey timing such that the SBC always issues the rekey request.	3	S-Cz9.3.0	S-Cz9.1.0p1
35038085	If an exiting audio stream is interrupted by a stray SSRC within the flow's packets, this interruption may trigger one-way audio wherein the audio towards the called party fails. You can confirm this condition by locating RTP packets in the flow with stray SSRC.	2	S-Cz9.1.0	S-Cz9.2.0

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
35815496	With Virtual SBCs, registration and calls work fine initially when running IMS-AKA, however, they may stop accepting registrations over TCP after multiple refresh registrations.	2	S-Cz9.2.0p2	S-Cz9.3.0
36195612	When generating RADIUS CDRs, the Acme-TerminatingTrunk-Group and Acme-TerminatingTrunk-Context fields are missing in the Start, Interim-Update, and Stop CDRs.	3	S-Cz9.2.0p5	S-Cz9.3.0p1
36344739	When deployed as a vSBC in HA mode and processing transcoding calls, the SBC, after a reboot or an HA switchover, may enter a state wherein a single core begins to process all calls rather than load balance them. Workaround: Perform a manual HA switchover making the affected system the new stand-by. Next, reboot the new standby to get back it into the correct state. Finally, perform a second manual HA switchover to make the new standby active again. This last step is required because the original standby may have synchronized itself with incorrect data.	3	S-Cz9.3.0	S-Cz9.3.0p1

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
37135255	On large scale VMs with 12 forwarding cores, the last 2 cores do not take any traffic. Traffic is thus balanced between the first 10 forwarding cores.	2	S-Cz9.3.0	S-Cz9.3.0p4
37431006	After running the restore-backup-config command, you must reboot your system to make sure all the non-RTC configurations are applied properly. After this reboot, traffic can be started.	3	S-Cz9.3.0	S-Cz10.0.0p2
37431251	When operating over the Acme Packet 4600, 6300 and 6350 platforms in HA mode and using BFD, the primary BFD interface on the active will not come up. Note that the virtual interface on the active and the secondary interface on the standby do come up. But this is not useful for BFD until the primary session on the active SBC comes up. Due to this, BFD can't be used to perform switchover between active and standby, as switchover happens only when primary session of BFD goes down. It is recommended not use BFD when operating HA deployments over the ACME Packet 4600, 6300 and 6350.	3	S-Cz9.3.0	S-Cz9.3.0p7

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
37677691	When upgrading vSBCs running over KVM, Vmware or cloud deployments to release S-Cz930p5 or later, spaces in the **interface-mapping** labels can corrupt the **interface-mapping** list and cause some media interfaces to fail after the upgrade. Workaround: If you have configured labels to your **interface-mapping** list entries, remove any blank spaces from them before you upgrade. If you have already upgraded, you can edit your **interface-mapping** labels so that there are no blank spaces in the label and reboot.	2	S-Cz9.3.0p5	S-Cz9.3.0p6

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
37211703	TLS client and server negotiates EC (elliptic curve) named curves in supported_groups extension. With this fix, SBC uses the blow named curves: • x25519 • secp256r1 • x448 • secp521r1 • secp384r1	2	S-Cz9.3.0p3	S-Cz9.3.0p4

Note

Earlier SBC versions used only secp256r

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
		1.		
36907247	This issue pertains to upgrades to S-Cz930GA and later releases that are configured as HA and have Lawful Intercept enabled. During an upgrade of HA system with LI enabled, after failing over the newly upgraded system (switching over the standby system that has just been upgraded and making it active), the active system (running the upgraded release) crashes. SCZ930p4 includes a work around for this issue, which is detailed in **KM Doc ID 3057846.1.** If upgrading to SCZ930p4 or later, and systems have Lawful Intercept enabled and are configured has HA, please refer to this document prior to upgrading.	2	S-Cz9.2.0	S-Cz9.3.0p4

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
35784723	The system may encounter a dpwd crash or datapath overload errors due to synchronization issues between cavium control core and data core when there is a high traffic in datapath. This issue is applicable to 4600/6300/6350 hardware platforms. This issue was only seen under extremely heavy load and unusual traffic patterns during Oracle stress testing. These conditions are considered highly unlikely in live deployments.	2	S-Cz9.2.0	S-Cz9.3.0 S-Cz9.1.0p10 S-Cz9.2.0p5
34511656	Primary SD runs into a USBC crash after running show scode session-byid command.	3	S-Cz9.1.0	S-Cz9.2.0
35614646	Certain RFC2833/ telephone-event sequences generated by customer endpoints may not be properly detected/ reported/re-transmitted by the SBC, resulting in missing DTMF digit(s).	2	S-Cz9.2.0p3	S-Cz9.2.0p4
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-Cz9.2.0p4

Copyright © 2024, 2026, Oracle and/or its affiliates.

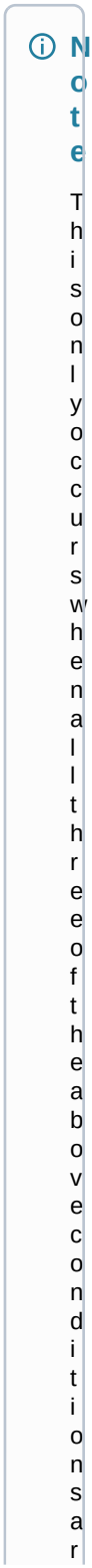
ID	Description	Severity	Found In	Fixed In
35011380	When running Remote Packet Trace on VNF platforms filtered to specific ingress IP addresses, in the PCAP capture you will sometime observe out of filter or wrong IP addresses. Specifically, the ingress flow packet addressing in the PCAP may display as the egress flow addressing and vice-versa. This depends on scheduling of original and captured packets by the NIC in SBC and this behavior is random. If you find packets that have the wrong addressing, you need to analyze them using the content of the payload and ignore any incorrect addressing.	2	S-Cz9.2.0	S-Cz9.2.0p3
34870648	The "show fans" command (a hidden command) is not working on the following SD6 platforms: • Acme Packet 1100 • Acme Packet 3900 • Acme Packet 3950 • Acme Packet 4900	4	S-Cz9.2.0p1	S-Cz9.2.0p2
34593124	Media interfaces configured with Mellanox NICs do not support STIR/SHAKEN.	3	S-Cz9.2.0	S-Cz9.2.0p1

Copyright © 2024, 2026, Oracle and/or its affiliates.

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

Copyright © 2024, 2026, Oracle and/or its affiliates.

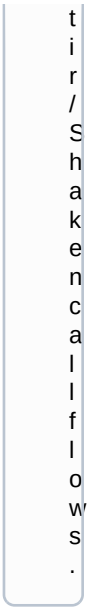
ID	Description	Severity	Found In	Fixed In
	which results in crash.			



Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
		emetanddoesnotapplyifonly#2and#3areenabledandthereareno S		

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
				
	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” config attribute under account-config to			

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
	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 SBC 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

Copyright © 2024, 2026, Oracle and/or its affiliates.

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

Copyright © 2024, 2026, Oracle and/or its affiliates.

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

Copyright © 2024, 2026, Oracle and/or its affiliates.

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 SBC does not support HA replication of a Wildcard PAU.	3	S-Cz9.0.0	S-Cz9.0.0p1

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
32939208	You cannot set the SBC **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 SBC . 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

Copyright © 2024, 2026, Oracle and/or its affiliates.

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 SBC 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

Copyright © 2024, 2026, Oracle and/or its affiliates.

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
31315823	When running IMS-AKA over UDP on virtual SBCs, 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 SBCs, 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

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
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
	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

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
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
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
32243204	STIR/SHAKEN entitlement is not available when the system is set up as a Peering Session Border Controller product.	2	S-Cz8.4.0p2	S-Cz8.4.0p4

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
32056356	While performing VoLTE Accounting on a 3G-to-4G MT call, the SBC incorrectly populates VSA ID 69 with the P-Asserted-Identity (PAI) retrieved from the response. This identifies the called side. Within the context of a mobile terminating call, the SBC should be identifying the caller, populating this VSA with the PAI retrieved from the INVITE. Workaround—You can correct this by setting the **unidirectional-p-asserted-id** option in the applicable **account-config** to **yes**.	2	S-Cz8.4.0	S-Cz8.4.0p4

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
31812964 31926021 31918592	The SBC incorrectly exhibits the following 3 incorrect behaviors with the PCRF during Register and Message call flows: 1. The SBC sends an STR to the PCRF in response to a de-register even though PCRF does not consider the session established, having sent an AAA with a 3xxx. 4xxx or 5xxx error in response to the corresponding Register. 2. The SBC keeps the hold timer active and holds an SMS message even though the PCRF has sent an ASR telling the SBC to abort the diameter session. 3. The SBC does not send an STR to the PCRF during Register flows that fail because of an error from the core, even though the Diameter session between the SBC and PCRF was established. Workaround—You can correct this by setting the **diam-rx-strict-**	3	S-Cz8.4.0	S-Cz8.4.0p4

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
	compliance option to the applicable **ext-policy-server** to **enabled**. When you set this option, you can correct the three issues above so that the SBC performs the following: 1. For Register flows that do not establish a diameter session with the PCRF due to a 3xxx. 4xxx or 5xxx error from the PCRF, the SBC does not send an STR to tear down the session when it receives a De-Register. 2. For Message flows, when the SBC receives an ASR from PCRF, it stops the hold timer, forwards the MESSAGE to the core, and sends an ASA with success. 3. For unsuccessful Register flows that include an established diameter session with the PCRF, the SBC sends an STR to tear down the session after the Register has failed due to, for example, responses from the core.			

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
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
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

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
30794993	The SBC 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

Copyright © 2024, 2026, Oracle and/or its affiliates.

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 SBC is under heavy load from SIP traffic, a mid-call intercept operation may not occur after the addition (causing the SBC to stop responding). If the SBC 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

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
30520108	Upon registering 100k or more IMS-AKA user registrations, and handling large numbers of VoLTE calls and registration refreshes, in excess of 8k for example, a vSBC may hang. At this point, you would find the vSBC unresponsive and inaccessible. An example of conditions when this may occur includes: • 100k IMS-AKA registrations with 100 registrations per second and an expiry timer of 18.0.0 seconds. • Forwarding cores at 60% or above utilization. • New calls at 50 registrations per second and 10 second hold timers. Reboot the system from the hypervisor to recover from this issue.	N/A	N/A	S-Cz8.3.0m1p5

Copyright © 2024, 2026, Oracle and/or its affiliates.

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

Copyright © 2024, 2026, Oracle and/or its affiliates.

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

Copyright © 2024, 2026, Oracle and/or its affiliates.

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
29913123	NMC causes the Acme Packet 6350 to switchover when NMC gets its first traffic match.	2	S-Cz8.1.0M1P9	S-Cz8.3.0m1p3
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

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
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
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 SBC 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 SBC 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

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
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
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

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
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

Copyright © 2024, 2026, Oracle and/or its affiliates.

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

Copyright © 2024, 2026, Oracle and/or its affiliates.

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

Copyright © 2024, 2026, Oracle and/or its affiliates.

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
29558827	IMS-AKA calls running over IPv6 networks which utilize VLANs on systems with Mellanox network interfaces may experience one-way audio.	3	S-Cz8.3.0p3	S-Cz8.3.0m1p2
29580506	SBCs running on virtual platforms or the Acme Packet 3900 could switch over when running IMS-AKA calls involving refresh registrations.	2	S-Cz8.3.0p3	S-Cz8.3.0m1p2

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
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
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

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
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
30453532	The Web GUI available in the S-Cz8.3.0M1 release cannot adequately be used to configure the Enterprise SBC. Workaround: For Web GUI support, use releases either prior to S-Cz8.3.0M1, or releases S-Cz8.3.M1p2 and later.	2	S-Cz8.3.0m1	S-Cz8.3.0m1p2
26258705	The **show sipd srvcc** command does not display the correct number of unsuccessful aSRVCC calls.	3	S-Cz8.0.0	S-Cz8.3.0

Copyright © 2024, 2026, Oracle and/or its affiliates.

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
29322490	The SBC intermittently does not process the registration (Event: reg) of a SUBSCRIBE with Expires header=0 that should be created after receiving a NOTIFY with a termination request from a UE.	2	S-Cz8.2.0	S-Cz8.3.0

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
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
28679339	When supporting SRVCC roaming calls, the OCSBC is handling SRVCC end-station de-registration events by properly including associated URIs in the 200 OK. It is not, however, saving those associated URIs in its registration cache. This causes the OCSBC to respond to calls to those URIs with 404 not found messages until the end-station re-registers.	2	S-Cz8.0.0	S-Cz8.3.0
26313330	In some early media call flows, the SBC may not present the correct address for RTP causing the call to terminate.	3	S-Cz8.0.0	S-Cz8.2.0

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
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
25144010	When an SBC operating on an Acme Packet 6300 switches over, the secondary can successfully add new ACL entries, but it also retains old ACL entries that it should have deleted.	3	S-Cz7.4.0p1	S-Cz8.2.0
26183767	When operating in HA mode and handling large traffic loads, the active SBC stops responding when you restore large configurations that are different from the configuration the active is currently running. The system subsequently goes out of service.	3	S-Cz8.0.0	S-Cz8.2.0

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
21975038	The Acme Packet 4600, 6100, 6300, and 6350 platforms do not support MSRP File Transfer.	3	S-Cz8.1.0	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
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
28071326	Calls that require LMSD interworking, as invoked by the lmsd-interworking option on a SIP interface, do not work in pooled transcoding architectures. During call establishment, when sending the 200 OK back to the original caller, the cached SDP is not included.	2	S-Cz7.4.0	S-Cz8.2.0

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
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
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 SBC a second time, after it initially starts.	3	SCz8.1.0m1	S-Cz8.2.0

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
	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
27811129	When upgrading an OCSBC from a version that uses License Keys to enable CODECs, you must reboot the system after setting any CODEC entitlements to override the License Keys.	3	S-Cz8.1.0	S-Cz8.3.0

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
30152019	Oracle has identified a Potential tSipd crash when configured for a VOLTE w/SRVCC scenario. When the issue is encountered, there is a sipd crash and, if configured, an HA switchover. This is a race condition that is relatively rare, but has been seen in internal testing. System Impact of HA Switchover: • The Registration cache and existing media sessions are replicated to the standby OCSBC. • During the switchover, transient calls/ registrations are lost. • After the switchover, TCP connections to and from the UE's must become re-established in order to make a new call out / refresh register / reregister. • The UEs is able to receive calls from the IMS-core because the setup message reestablishes the TCP connection towards the UE.	3	S-Cz8.3.0p7	S-Cz8.3.0m1

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description	Severity	Found In	Fixed In
28610095	In some circumstances, and with **add-sdp-invite** and **add-sdp-profile** configured, the SBC does not include the original SDP in a Re-INVITE that has no SDP. This does not comply with RFC 3264. Instead, the SBC inserts the negotiated media information from the last successful negotiation as the ReINVITE's SDP offer and sends this ReINVITE with inserted SDP to the next hop signaling entity. This issue is evident by the contents of the SDP o line.	3	S-Cz7.4.0	S-Cz8.3.0m1
29541242	*Installation and Platform Preparation* guide incorrectly includes information about setting up HA on Oracle Cloud platforms. These platforms do not support HA deployments at this time.	3	S-Cz8.3.0	S-Cz8.3.0m1

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

ID	Description
26316821	When you configure the 10 second QoS update mechanism for OCOM, the SBC 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.
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description
32709550	When operating over the Azure platform, the SBC displays an inordinate number of kernel messages during the bootup process. You can safely ignore these messages.
28617865	This version of the OCSBC is not supported as a VNF over VMware using Mellanox interface cards.
35575147	The *System Access Based on Server Availability* topic in the Authentication and Authorization section of the Admin Security Guide has been created to document this incorrectly labeled known issue as expected behavior.
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 SBC. Furthermore, the SBC 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.
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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

ID	Description
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 SBC 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 SBC 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	When deployed as a vSBC, configured for IMS-AKA, and operating with registrations exceeding 60k, the OCSBC may exhibit performance degradation, exhibited by high CPU load or system crash. Workaround - Oracle has found that disabling the **security-policy sa-lookup-exception** parameter allows IMS-AKA to function correctly while supporting a high number of registrations. This parameter is enabled by default. Disable this parameter within all applicable security policies before running IMS-AKA. This parameter, when enabled on Acme Packet hardware, works as designed.
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 SBC retains some IMS-AKA subscriber TCP sockets. You can clear these sockets by rebooting the SBC.
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 SBC 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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

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.
N/A	Version S-Cz7.4.0 does not support the enhancement to SMP-Aware Task Load Limiting, which adds a second parameter to the sip-config load-limit option.

Caveats

The following information lists and describes the caveats 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.

Encryption and FAX Transcoding On the Same Call

The SBC does not support Encryption and FAX Transcoding on the same call. Using them together results in the call failing.

Azure HA Deployment

You should be aware that there are two change procedures that one might expect Azure to perform automatically but must be performed manually. These Public IP resource changes differed until a switchover/failover occurs. Applicable caveats include:

- The secondary Private IP configuration resources (VIPs) are not deleted on the active SBC media interface when VIPs are removed from SBC configuration objects, including:
  - **network-interface** parameters including:
    - **ip-address**
    - **hip-ip-list**
  - **sip-interface**

  You can delete them manually, however, using the Azure console.
- The Public IPs are not disassociated from the secondary Private IP config (VIPs) on the Azure active SBC media interface by removing the VIP-to-PIP mapping from the **redundancy-config** options parameter.
  You can disassociate the Public IP from the Secondary private IP manually, however, using the Azure console.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- In Azure HA environments, vSBC Switchovers are experiencing high Latency. This is due to Latency in the Azure Network's infrastructure during VIP movement between the vSBC HA pair. Typical Switchover times observed during internals test are in range of 14 to 40 Seconds. In production environment, these values could differ based on Network conditions and configurations.

  > **Note**
  >
  > During discussions, the Azure team has indicated that optimizing Switchover latency issues due to SDN is not in their current work plan/roadmap.

- With Public-IP configuration of the vSBC on Azure infrastructure, system instability is experienced during Switchovers. This Impacts the use case of End Points Connecting over Public IPs for VOIP calls. Based on analysis and discussions with Azure team, this is suspected to be SDN/Infrastructure issue in Azure Cloud.

NIC Detachment during Live Updates on Azure

Azure infrastructure has the ability to push live online updates to their Infrastructure components. During such Online updates, we have experienced sudden vNIC detachment from the vSBC instance, resulting in vNIC device access failures, manifesting as crashes in vSBC.

Workaround—Oracle recommends disabling AN mode while assigning vNIC interfaces to vSBC instance. This circumvents this NIC detachment issue with AN.

HDR Push Failures on Specific S-Cz9.3.0 Releases

The libssh, for SBC devices running on S-Cz9.3.0/S-Cz9.3.0p1/S-Cz9.3.0p2, sends only 'ssh-rsa' host key algorithm while exchanging keys. Because the SBC’s HDR push mechanism uses libssh, this older cipher can cause HDR push to fail on these systems because the HDR server rejects this cipher.

Version S-Cz9.3.0p3 of the SBC, however, uses rsa-sha2 as its first cipher option and, therefore, typically succeeds with establishing HDR push connections.

Oracle recommends you upgrade to SBC version S-Cz9.3.0p3 for deployments that must support HDR push. Alternatively, you could establish an S-Cz9.3.0/S-Cz9.3.0p1/S-Cz9.3.0p2 deployment that uses ssh-rsa for HDR push, but Oracle does not recommend this because ssh-rsa is less secure.”

Login Issues with Local Account User Created Using Web GUI After Upgrade or Restore Backup Config

The SBC is not allowing login, either through ACLI or Web GUI, with local-accounts users created (prior to 920p7) using Web GUI after upgrade to 920p7 or higher.

Workaround: Either reset the user accounts password or delete those users and recreate them again after an upgrade to 920p7 or higher.

Static Flows and Media Policing

The Acme Packet 1100, 3900, and 4600 as well as all software-only deployments do not support the **average-rate-limit** parameter in a **static-flow** configuration when the profile applies to static flows.

Copyright © 2024, 2026, Oracle and/or its affiliates.

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.

IKE/IPSEC Key Length over Wancom0

Connection setup to wancom0 interfaces using IKEv2/IPSEC using certificate authentication fail when using a key length of 1024. Workaround: Configure any IKEv2/IPSEC connections to wancom0 interfaces using certificate key lengths of 2048 or larger.

IKE/IPSEC Key Length over Wancom0 for KVM Platforms and TACACS Authentication

TACACS authentication via IKEv2/IPSec over a wancom0 based on certificate-based authentication is not applicable to KVM platform.

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).

Incorrect STI Server Statistics Updated

The Oracle Communications Session Border Controller (SBC) is displaying incorrect STI statistics when multiple servers are added.

Workaround: When using multiple servers, create a group to add them to and then assign them to the realm, interface, or session agent.

If you must use multiple servers, ensure the first server name is not configured as the sti-as or sti-vs on any realm, interface, or session agent.

Elin Table Entries Not Replicated on Standby SBC After Reboot

In an HA setup, when the standby SBC is rebooted, it loses the existing Elin table entries. However, any newly created entries post reboot are in sync between the Active and Standby SBCs.

Copyright © 2024, 2026, Oracle and/or its affiliates.

DTLS and SDES SRTP Transport

If a network deployment involves realms where endpoint (UAC) initiates a call that requires secure DTLS-SRTP transport to SBC and the call is being forwarded to a realm where the callee (UAS) requires SDES-SRTP, then the ingress realm must have media-sec-policy configured with SDES in addition to dtls-srtp-profile.

Uneven Load Distribution on Forwarding Core on GCP

There is an imbalance when there are an odd number of queues for packets.

Workaround: Configure an even number of forwarding cores.

Load Variation With the Same Number of Sessions in GCP

When a vSBC is rebooted from the console, the load on the F core is significantly different for the same number of calls previous to the reboot.

Unsupported GCP Migration

Do not migrate an existing vSBC from a small GCP machine type to a larger GCP machine type. This is not supported on GCP.

VM Migration Not Supported

The queue allocation cannot be changed once a VM is created.

Acquire Config and acp-tls-profile

The **acquire-config** process fails if your configuration includes an **acp-tls-profile**. The system does 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 and 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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

- 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.

Transcoding - general

Only SIP signaling is supported with transcoding.

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

The T.140 to Baudot Relay transcoding support is not available on vSBC or Acme Packet 3900 platforms.

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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

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.

Lawful Intercept

Lawful Intercept is supported for the X123 and PCOM protocols only. PCOM support for LI is not available on virtual platforms.

Fragmented Ping Support

The Oracle Communications 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.

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

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 SBC, 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.

Copyright © 2024, 2026, Oracle and/or its affiliates.

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 Communications Session Border Controller (SBC). 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 SBC, 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.

IPv6 On X1 Interface

IPv6 does not work on X1 interface.

Diameter Server Timeout during Save/Activate

When saving and activating a configuration, the SBC may disconnect from an external policy server. The cause of this disconnect is based on SCTP HEARTBEAT value configured on the Diameter policy server.

Solution: You can work around this issue by setting the policy server's SCTP HEARTBEAT to a value greater than 750ms, which exceeds the amount of time it takes to perform a save/activate on the SBC.

Simultaneous Use of Trace Tools

See "Trace Tools" caveat.

LI and Rx Interfaces using the same Address

Do not configure an X1, X2, or X3 TCP endpoint with the same address as an Rx interface. These configurations create conflicts between the Linux TCP stack and atcpd.

IKE

ECDSA and RSAPSS 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

Copyright © 2024, 2026, Oracle and/or its affiliates.

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 SBC does not include UUID in ACK or BYE messages post REFER processing.

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.

TLS Secure Negotiation

The SBC requires the use of TLS Secure Renegotiation as described in RFC 5746 in order to counter the prefix attack described in CVE-2009-3555. If the devices attempting a TLS connection to the SBC don't support TLS Secure Renegotiation, the TLS handshake fails. Oracle recommends updating such devices to support TLS Secure Renegotiation.

Limitations

The following information lists and describes the 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.

Transcoding Limitations on the Acme Packet 4900

The Acme Packet 4900 does not support 40 and 60 packetization times for the EVS codec.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Virtual Network Function (VNF) Limitations

SBC functions not available in VNF deployments of this release include:

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

Packet Trace Limitations

- 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.

Fragmented SIP Message Limitations

Fragmented SIP messages are intercepted but not forwarded to the X2 server if IKEv1/IPsec or IKEv2/IPsec tunnels are configured as transport mode.

Workaround: Configure IKEv1/IPsec or IKEv2/IPsec tunnels as "tunnel mode".

Header Mapping Limitations

This version of the includes the following limitations to the header mapping feature:

- Indexing is not supported for HTTP headers.
  Per the Section 4.2 of RFC 2616, Multiple message-header fields with the same field-name may be present in a message if and only if the entire field-value for that header field is defined as a comma-separated list. But, because indexing is not supported, the following configuration is not supported:
  - When the direction is outbound, the target-header field (HTTP header) does not support indexing and subscript.
  - When the direction is inbound, source-header (HTTP header) field does not support indexing and subscript.

  If you configure either of the above, the SBC displays an error at the ACLI when you run the **done** command on the applicable **mapping-rules** instance.
- If you are using 3GPP mode and the SBC receives two responses, SHAKEN and DIV signing responses, on which it performs header mapping, the SBC saves the first response. When it receives the second, the SBC processes this second response but does not save it. This is also true for any ensuing responses. Finally, the SBC processes the saved response, which can result in the system replacing the last mapping with the saved mapping.
  Consider the following mapping ruleset and the steps below to understand what to expect in an INVITE after the mapping processing is completed:

```
sti-header-mapping-ruleset
          name                                    ruleset1
          mapping-rules
```


Copyright © 2024, 2026, Oracle and/or its affiliates.

```
id                                HttpToSip
source-header                     X-Test-Id
target-header                     Test-Id
direction                         inbound
role                              STI-AS
```

This processing causes the SBC to behave and generate the final message, in this case an INVITE. as follows:

1. The SBC receives a SHAKEN Signing Response received with an X-Test-Id header and a value of 123.
2. The system saves this response and waits.
3. The SBC receives a DIV Signing Response with an X-Test-Id and a value of 345.
4. The system processes the DIV response first, because it was received last, and applies the mapping. The system adds a new header to the egress INVITE called **Test-Id: 345**.
5. The system processes the SHAKEN response next, and applies the mapping. This time, the system replaces the existing header with a header called **Test-Id: 123** in the INVITE.
6. The system forwards the completed INVITE.

- For authentication scenarios, after receiving a response from the STI-AS, the SBC removes any previous signaling before sending the INVITE out. It does so by removing the following four headers, if present in the ingress INVITE:
  - Attestation-Info
  - P-Attestation-Info
  - Origination-Id
  - P-Origination-Id

  But the SBC only deletes the first occurrence of these headers. This results in an issue during AS inbound (HTTP to SIP) mapping. Specifically, when you configure digits greater than 0 in the subscript operator, the system may process the wrong header if one of these headers is removed before applying the mapping rules.

DTLS-SRTP Limitations

This version of the SBC has some feature limitations within its DTLS-SRTP implementation. For DTLS-SRTP, the SBC does not support:

- The SBC operating as a DTLS client.

  > **Note**
  >
  > You can only configure the system for passive setup

- Complete security of media streams using integrity protection, as defined in section 3 of RFC 5764.
- Conference specific functions, such as RTP mixing
- Re-keying
- DTLS-SRTP in SBC ICE Lite mode

Copyright © 2024, 2026, Oracle and/or its affiliates.

- Hairpin call scenarios
- The “use_srtp” extension with non-zero MKI value
- Multiple media lines of the same media type, with one of them being DTLS

> **Note**
>
> Calls that establish multiple media sessions for different media types, audio and video for example, are supported.

- Detection of the “two-time pad” SRTP error (per section 3 of RFC 5764)
- Attended transfer
- The SBC does not support the AEAD_AES_256_GCM cipher on hardware datapath platforms.
- DTLS-SRTP calls with RTP/RTCP flows that are not multiplexed. This limitation generates a requirement and several behaviors:
  - Requirement - You must enable the **rtcp-mux** parameter on each realm that has a valid **dtls-srtp-profile**.
  - Behavior - The SBC replies with a "488 Not Acceptable Here" response if it receives an initial INVITE that includes DTLS-SRTP attributes, but does not include the rtcp-mux attribute.
  - Behavior - If the SBC receives a 200 OK, a 180 ringing, or a 183 session progress from a callee that includes DTLS-SRTP attributes, but does not include the rtcp-mux attribute., the system sends a BYE to the callee and a “503 service unavailable” message to the caller.
  - Behavior - If the SBC receives an ACK from a caller that is in response to a delayed offer SDP from a callee, and that ACK does not include the rtcp-mux attribute., the system:
    1. Sends an ACK to the callee to acknowledge the 200 OK with the delayed offer.
    2. Sends a BYE to both the caller and callee to terminate the call.

DTLS-SRTP Platform Support

The SBC supports DTLS-SRTP on the following platforms:

- AP1100
- AP3900
- AP3950
- AP4900
- AP6350—Platform support as of S-Cz9.2.0p1
- vSBC deployment over:
  - KVM
  - VMware
  - OCI
  - AWS
  - Azure

Copyright © 2024, 2026, Oracle and/or its affiliates.

Parallel Forking Limitations

This version of the SBC includes the following limitations to its parallel forking support:

- If you configure two MS Teams destinations for parallel-forking, and one of them supports MS Teams LMO feature while other destination doesn't supports MS Teams LMO feature, then parallel forking call flows will not be supported.
- SRVCC handover calls are not supported within parallel forking call flows
- SIP to SIP-I interworking is not supported within parallel forking call flows
- SIPREC calls are not supported within parallel forking call flows
- All merge-early-dialogs limitations apply to parallel forking call flows, including:
  - Offerless call
  - Preconditions interworking
  - SRVCC
  - multiple audio or video m-line
  - p-early-media-header with 'add' and 'modify' options
- If the SBC receives an INVITE with its req-uri in the format "username@FQDN:port" and the applicable routes include:
  - Route1 (IP1) – cost 5 – parallel-forking enabled
  - Route2 (IP2) – cost 5 – parallel-forking enabled

  SBC behavior when Route1 or Route2 return 302 messages with multiple contacts:
  - If Route1 /Route2 replies with a 302 with 2 contacts, then the SBC attempts to reach those contacts serially.
  - If both contacts timeout, the SBC does NOT try the next policy-attributes.
- Note the SBC behavior when the routes are configured as below:
  - Route1 (IP1) – cost 5 – parallel-forking enabled
  - Route2 (FQDN) – cost 5 – parallel-forking enabled
  - Route3 (IP3) – cost 5 – parallel-forking enabled
  - DNS resolution of FQDN for Route2 returns 3 IPs (IPx, IPy, IPz)

  SBC behavior includes:
  - If the UAC sends an INVITE with req-uri as username@IP:port, the SBC forks the INVITE to Route1 and Route2 in parallel. If Route 2 replies to the INVITE with a 302 that includes 2 contacts, the SBC tries to reach those 2 contacts serially.
    If these 2 contacts timeout/18x timeout/error response, the SBC tries the next policy-attributes.
  - If the UAC sends an INVITE with number@FQDN, and IPx replies to the subsequent INVITE from the SBC with a 302 with 2 contacts, the SBC tries to reach those 2 contacts serially.
    If these 2 contacts timeout, the SBC does not attempt to reach any further DNS resolutions or next policy-attributes.
  - If the UAC sends an INVITE with number@IP:port, and IPx responds to the INVITE with a 302 with 2 contacts, the SBC tries to reach those 2 contacts serially.
    If these 2 contacts timeout, the SBC does not try to reach any further DNS resolutions, but does try to reach next policy-attributes.

Copyright © 2024, 2026, Oracle and/or its affiliates.

Playback Headers and Hairpin Calls

Playback headers are not supported for hairpin calls.

High Memory Use on Acme Packet 3950/4900

The Acme Packet 3950/4900 platform uses a software data path that reserves approximately 36% of total memory for the data path, even if there is no traffic. Consequently, memory statistics are higher on the Acme Packet 3950/4900 than on other platforms. This does not impact performance.

Limitations Removed

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

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.

RTCP on Virtual Platforms

Virtual Platforms support RTCP detection of incoming RTCP packets, which is used in our QoS feature and in RTCP round-trip delay calculations. Virtual Platforms perform RTCP round-trip delay calculations on incoming RTCP packets, and these calculations are realized in the outgoing RTCP packets that are generated.

RTCP detection for QoS does not require that you configure transcoding media cores.

RTCP generation requires that you configure transcoding media cores because all calls with RTCP generation are transcoded calls.

Copyright © 2024, 2026, Oracle and/or its affiliates.