Oracle® Communications Session Border Controller

Maintenance Release Guide
Release S-CZ7.2.0

December 2015

Notices

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 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 installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. 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 and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron 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.

Contents

Preface

About this Guide

The Maintenance Release Guide provides information about the contents of maintenance releases related to Oracle Communications Session Border Controller S-CZ7.2.0. This information can be related to defect fixes, to adaptations made to the system software, and to adaptations ported to this release from prior releases. When applicable, this guide contains explanations of defect fixes to the software and step-by-step instructions, if any, for how to enables these fixes on your system. This guide contains explanations of adaptations including conceptual information and configuration steps.

Purpose of this Document

Designed as a supplement to the main documentation set supporting Oracle Communications Session Border Controller release S-CZ7.2.0, this document informs you of changes made to the software in the maintenance releases of S-CZ7.2.0. Consult this document for content specific to maintenance releases. For information about general OCSBC features, configuration, and maintenance, consult the Related Documentation listed in the section below and then refer to the applicable document.

Organization

The Maintenance Release Guide is organized chronologically by maintenance release number, started with the oldest available maintenance release and ending with the most recently available maintenance release.

This document contains a Maintenance Release Availability Matrix, showing when and if given maintenance releases have been issued and the date of issue. Each available maintenance release constitutes one chapter of this guide.

In certain cases, a maintenance release will not have been made generally available. These cases are noted in the Maintenance Release Availability Matrix. When Oracle has not made a maintenance release available, there will be no corresponding chapter for that release. Therefore, you might encounter breaks in the chronological number of maintenance release.

Related Documentation

The following table lists the members that comprise the documentation set for this release:

Document Name	Document Description
Acme Packet 4500 Hardware Installation Guide	Contains information about the components and installation of the AP4500.

Document Name	Document Description
Acme Packet 3820 Hardware Installation Guide	Contains information about the components and installation of the AP 3800.
Acme Packet 6300 Hardware Installation Guide	Contains information about the components and installation of the AP 6300.
Acme Packet 6100 Hardware Installation Guide	Contains information about the components and installation of the AP 6100.
Release Notes	Contains information about the current documentation set release, including new features and management changes.
ACLI Configuration Guide	Contains information about the administration and software configuration of the Oracle Communications Session Border Controller.
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 Oracle Communications Session Border Controller logs, performance announcements, system management, inventory management, upgrades, working with configurations, and managing backups and archives.
MIB Reference Guide	Contains information about Management Information Base (MIBs), Acme Packet's enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management Protocol (SNMP) GET query information (including standard and enterprise SNMP GET query names, object identifier names and numbers, and descriptions), examples of scalar and table objects.
Accounting Guide	Contains information about the Oracle Communications Session Border Controller's accounting support, including details about RADIUS accounting.
HDR Resource Guide	Contains information about the Oracle Communications Session Border Controller's Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Administrative Security Essentials	Contains information about the Oracle Communications Session Border Controller'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 Oracle Communications Session Border Controller family of products.

Revision History

Date	Description
August 2014	Initial Release
October 2014	Corresponds to M2 release
November 2014	Adds Acme Packet 4600 information
March 2015	Corresponds to M3 release
May 2015	Corresponds to M4 release
June 2015	Adds Known Issues section to M4 chapter
July 2015	Corresponds to M5 release

Date	Description
December 2015	Corresponds to M6 release

1

S-CZ7.2.0M1

This chapter provides descriptions, explanations, and configuration information for the contents of Release S-CZ7.2.0M1.

Current SPL Engine versions supported:

- C2.0.0
- C2.0.1
- C2.0.2
- C2.0.9
- C2.1.0
- C2.2.0
- C3.0.0
- C3.0.1
- C3.0.2
- C3.0.3
- C3.0.4
- C3.0.6
- C3.1.0
- C3.1.1
- C3.1.2

Current patch baseline: S-CZ7.2.0 GA

Content Map for S-CZ7.2.0M1

The following content is newly available in release S-CZ7.2.0M1

Content Type	Description
Adaptation	DSCP Marking for MSRP and Media Over TCP
Feature	LI PCOM
Forward Merge	S-CZ7.1.2M3p1

Upgrading to S-CZ7.2.0M1

This note is only for users planning to load S-CZ7.2.0M1 on their Acme Packet 3820 and Acme Packet 4500 platforms.

- Upgrading from an S-CZ7.x.y release to S-CZ7.2.0M1 is supported.
- Upgrading from an S-CX6.4.0M4 or S-CX6.4.0M5 release requires a roll-through upgrade. You must first upgrade to S-CZ7.2.0GA. After you are running S-CZ7.2.0GA, you may proceed to upgrade to S-CZ7.2.0M1.

DSCP Marking for MSRP and Media Over TCP

The Oracle Communications Session Border Controller supports Differentiated Services Code Point (DSCP) marking of MSRP and Media over TCP traffic. This feature may be used for MSRP traffic in both B2BUA and non-B2BUA modes.

In order to configure the Oracle Communications Session Border Controller to mark MSRP or media over TCP packets with a value in the IP header's DSCP field, create a **media-manager** > **media-policy** > **tos-settings** configuration element and set the **media-type** parameter to **`message`**. This has the effect of marking all traffic described by prior SDP with m=message with this DSCP value.

Note that setting **media-type** to **`message`** can potentially mark a large range of traffic. For other common traffic to remain marked differently than marked MSRP, you need to create additional **tos-settings** configuration elements with valid **media-sub-type** configurations. The following values may be provisioned in the **media-sub-type** parameter to mark these other types of traffic differently (with an accompanying **tos-value**).

- sip
- li
- dns

2

S-CZ7.2.0M2

This chapter provides feature descriptions for the contents of Release S-CZ7.2.0M2.

Current SPL Engine versions supported:

- C2.0.0
- C2.0.1
- C2.0.2
- C2.0.9
- C2.1.0
- C2.2.0
- C3.0.0
- C3.0.1
- C3.0.2
- C3.0.3
- C3.0.4
- C3.0.6
- C3.1.0
- C3.1.1
- C3.1.2

Current patch baseline: S-CZ7.2.0M1

Content Map for S-CZ7.2.0M2

The following content is available in release S-CZ7.2.0M2
New content in S-CZ7.2.0M2

Content Type	Description
Feature interoperability support	Transcoding and SRTP may now be used together on the same call on the Acme Packet 6300 or Acme Packet 4600.
Adaptation	REFER call transfer UUI relay
Adaptation	IPSec for Session Load Balancer L3 tunnels

Content Type	Description
Forward Merge	S-CZ7.1.2M3p2
Platform Support	Acme Packet 4600 is released and supported with this software

Known Issues

The following are known issues new to S-CZ7.2.0M2. Please review the Caveats and Known Issues sections in the Release Notes document upon any upgrade or when deploying new features.

- When performing an online upgrade to S-CZ7.2.0M2 with LI enabled, no intercepted sessions may be active. Please re-route all traffic that could trigger intercepted sessions to an SBC other than the one you are upgrading.
- In deployments utilizing MSRP over TLS on the Acme Packet 6300 platform, calls may fail when using 4 media ports in certain network configurations. This occurs when reusing the same IP address for SIP interfaces and SIP steering pools on different realms, but no VLANs are used.

Upgrading to S-CZ7.2.0M2

This note is only for users planning to load S-CZ7.2.0M2 on their Acme Packet 3820 and Acme Packet 4500 platforms.

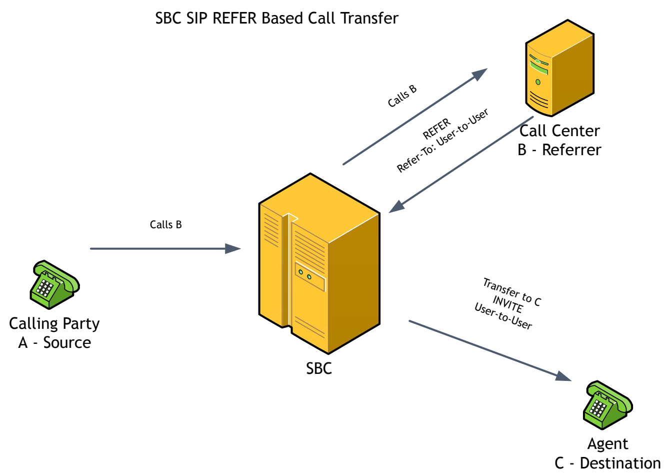
- Upgrading from an S-CZ7.x.y release to S-CZ7.2.0M2 is supported.
- Upgrading from an S-CX6.4.0M4 or S-CX6.4.0M5 release requires a roll-through upgrade. You must first upgrade to S-CZ7.2.0GA. After you are running S-CZ7.2.0GA, you may proceed to upgrade to S-CZ7.2.0M2.

SIP REFER Call Transfer UUI Relay

The SIP REFER Call Transfer *User to User Information (UUI)* Relay option assists in the transfer of caller details through using the information in the "Refer-To" header in a new "User to User" header in the INVITE to the Referred-to party. This feature only works when the **refer-call-transfer** option is enabled on the realm or session agent where the REFER is received. This behavior change is enabled by default. This option can be used by a Call Center application to transfer a call with user information to an agent.

A new INVITE is sent with the information about the calling user to the agent by way of the "Refer-To" header using the *User to User Information.* The product variable needs to relay this UUI as a separate header in the INVITE message while transferring the call to the destination. In this scenario, the product terminates the REFER message having captured the UUI and then sends an INVITE with the UUI to the agent. This feature works only when the **refer-call-transfer** option is enabled on the Realm or Session Agent where REFER is received. By default this option is enabled and thus needs to be specifically disabled in the configuration if not wanted.

The following illustration shows the path of the call from the source to the destination by way of the product utilizing the *User to User Information* relay



SIP REFER UUI Relay

Refer-To Header

The Oracle Communications Session Border Controller supports the format of *User-to-User* in the "Refer-To" header in the REFER message. The following example shows the new text after the IP address and port in the second to last line.

```
REFER sip:7325550000@192.168.28.10:5060 SIP/2.0
Via: SIP/2.0/UDP 192.168.29.1:5060;branch=z9hG4bK-10659-1-4
From: 7325550000 <sip:7325550000@192.168.29.1:5060>;tag=1
To: 7321110000 <sip:732111000@192.168.28.19:5060>;tag=1
Call-ID: 1-10679@192.168.28.1
...
Refer-To: <sip:9785550000@192.168.29.1:6062?User-to-
User=56a390f3d2b7310023a%3Bencoding%3Dhex%3Bpurpose%3Disdn-
interwork%3Bcontent%3Disdn-uui
Content-Length:0
```

User to User Parameter in INVITE

If the UUI is received in the "Refer-To" header in the REFER message, the Oracle Communications Session Border Controller adds the new UUI header in the INVITE message to the destination party. The system encodes the INVITE message as shown in the following example. All the escape characters received in the UUI parameter converts to plain text and all the UUI header parameters are relayed. In the example below, note the new UUI content below *Content-Length* and in the *Supported* fields.

```
INVITE sip:9785550000@192.168.29.1:6062 SIP/2.0
Via: SIP/2.0/UDP 192.168.29.20:5060;branch=z9hG4bKgkm8110090jmlvcfk80.1
From: 7321110000 <sip:7321110000@192.168.28.1:5060>;tag=1
To: <sip:9785550000@192.168.29.1:6062>
Call-ID: 537e3302f02bbb0ddd8b8d7538f8b33030@192.168.28.1
```

```
CSeq: 2 INVITE
Contact:<sip:sipp@192.168.29.20:5060;transport=UDP>
Session-Expires: 3600;refresher=uac
Max-Forwards: 69
Subject: Performance Test
Content-Type: application/sdp
Content-Length: 135
User-to-User:56a390f3d2b7310023a;encoding=hex;purpose=isdn-
interwork;content=isdn-uui
Supported: timer,uui
Referred-By:<sip.7325550000@192.168.29.1:5060>
Route:<sip:9785550000@core2:6020,lr>

v=0
o=user153655765 2353687637 IN IP$ 192.168.28.1
s=-
c=IN IP4 192.168.28.1
t= 0 0
m=audio 8000 RTP/AVP 8
a=rtpmap 8 PCMA/8000
```

User to User Header in REFER

The product supports the REFER header that replaces the default header with the UUI header in an attended call transfer.

```
Aug 4 10:09:10.233 On [256:0]192.168.12.1:5060 received from
192.168.12.2:5060
REFER sip:1000@192.168.12.1:5060 SIP/2.0
Via: SIP/2.0/udp 192.168.12.2:5060;branch=z9hG4bK-bob2alice-9
Max-Forwards: 10
From: bob <sip:2000@acme.com>;tag=bob-0
To: alice <sip:1000@acme.com>;tag=alice-1
Call-ID: 1-192.168.11.2
CSeq: 3 REFER
Refer-To: <sip:3000@acme.com?Replaces=1-192.168.12.2%3Bto-tag
%3Dcarol2bob-0%3Bfrom-tag%3Dbob2carol-2&
User-to-User=56a390f3d2b7310023a%3Bencoding%3Dhex%3Bpurpose%3Disdn-interwork
%3Bcontent%3Disdn-uui>
```

INVITE Message Details

The Oracle Communications Session Border Controller adds the UUI parameter to the *Supported* header in the INVITE message to the *Referred-to* party. The Oracle Communications Session Border Controller encodes only one instance of the UUI header in the INVITE message to the *Referred-to* party. The Oracle Communications Session Border Controller will only process the first UUI parameter received in the "Refer-To" header. The Oracle Communications Session Border Controller supports a maximum of 128 octets hex content in the UUI header field, excluding parameters. The overall length of the header complies with RFC 3261. If the header length exceeds the maximum, the Oracle Communications Session Border Controller discards the UUI header and cannot relay the call.

SIP REFER Call Transfer UUI Relay Configuration

The SIP REFER Call Transfer *User to User Information* Relay is enabled by default. To disable UUI relaying on a configured realm:

1. Access the **realm-config** configuration element.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# media-manager
ACMEPACKET(media-manager)# realm-config
ACMEPACKET(realm-config)#
```

2. Select the **realm-config** object to edit.

```
ACMEPACKET(realm-config)# select
identifier:
1: realm01 left-left:0 0.0.0.0

selection: 1
ACMEPACKET(realm-config)#
```

3. **options**—Set the options parameter by typing options, a space, **disable-refer-to-uui=yes**. You may prepend the option name with a plus to add and not replace this option to the existing **realm-config** option list.

```
ACMEPACKET#options +disable-refer-to-uui=yes
```

4. Type **done** to save your configuration.

SLB Client Support of IPsec traffic within L3 Tunnels

The Oracle Communications Session Border Controller, acting as a Subscriber-aware Load Balancer (SLB) client can exchange IPSec traffic within the L3 tunnels between itself and the SLB server. One application of this feature is using an SLB to balance and re-balance IMS-AKA traffic among an SLB cluster.

This version of the Oracle Communications Session Border Controller software requires an SLB running version L-CX1.5.0p3 or later for IPsec traffic support. In this scenario, the outer tunnel must be IPv4, while the inner IPsec tunnels can be IPv4 or IPv6.

Configuration Guidelines

There is no specific configuration required to create an IPsec bearing L3 tunnel between an SBC and SLB. The following table may be used as aid where identical values must be configured between the Oracle Communications Session Border Controller and SLB, or within each system. Each row in the table below lists the parameters on the SBC or SLB (as listed in the respective column) that must be configured with the same value.

SLB System	SBC System
Outer L3 Tunnel to SBC **network-interface** > **ip-address** **network-interface** > **tunnel-config** > **local-ip-address**	Outer L3 Tunnel to SLB **network-interface** > **tunnel-config** > **remote-ip-address**
	network-interface > **ip-address** **network-interface** > **tunnel-config** > **local-ip-address**
network-interface > **tunnel-config** > **port**	**network-interface** > **tunnel-config** > **port**
network-interface > **tunnel-config** > **protocol**	**network-interface** > **tunnel-config** > **protocol**
network-interface > **tunnel-config** > **name**	**sip-interface** > **tunnel-name**
Access-side SLB Network Interface, the network-interface between endpoints and the SLB. **network-interface** > **ip-address** **cluster-config** > **service-port** > **address**	Access-side SBC network interface. **sip-interface** > **sip-port** > **address**

Set the SLB's **cluster-config** > **service-port** > **port** to 0 in order to accept IMS-AKA traffic.

On the Oracle Communications Session Border Controller's **sip-interface**, the sec agree feature must be enabled by setting the **sec-agree-feature** parameter to **enabled** and the **sec-agree-pref** parameter to **ipsec3gpp**. All supporting security policies must also be configured.

SRTP and Transcoding

Secure Real Time Transport Protocol (SRTP) allows secure media transmission. Transcoding is the ability to convert between media streams that are based upon different codecs. The Oracle Enterprise Session Border Controller supports IP-to-IP transcoding for SIP sessions and can connect two voice streams that use different coding algorithms with one another. Both SRTP and transcoding are available in the same call.

As of this release of the software, SRTP and transcoding are available on the same call. This behavior is available by default and no configuration is required.

Acme Packet 4600

Oracle Communications introduces the Acme Packet 4600 hardware platform for S-CZ7.2.0.

The Acme Packet 4600 supports the Oracle Communications Session Border Controller and Session Router software. This platform is based on the Acme Packet 6300 architecture and features encryption and transcoding in a single system. Transcoding functionality can utilize up to 1 through 12 transcoding modules on the NIU. The encryption feature set relies on the SSM3 encryption module. The Acme Packet 4600 platform runs the 64-bit software image exclusively.

The NIU provides six media ports (i.e., 4 x GbE and 2 x 10GbE) on a single NIU card. Simultaneous operations of the GbE and 10GbE media ports is unsupported.

The Acme Packet 4600 has an internally mounted SSD memory drive (80GB or 400GB). The system employs the same file system as the Acme Packet 6300/6100 platform that runs the S-CZ7.2.0 Series software. The mounted partitions include the /boot partition (2GB), the /code partition (2GB) and the /opt partition. The /opt partition is intended for core dumps, log files, and CDRs.

The Acme Packet 4600 has 5 cooling fans mounted of the front on the chassis to maintain proper operating temperature. The chassis contains 1:1 fully redundant AC or DC power supplies and load share when both are powered on. The two power supplies also have integrated fans.

The Acme Packet 4600 FRU list consists of the following

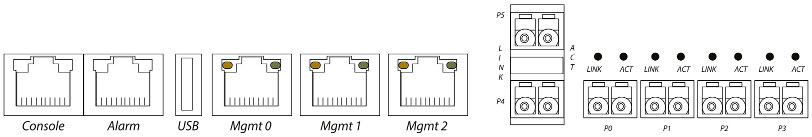
- Acme Packet 4600 Chassis w/Mainboard
- Acme Packet 4600 NIU
- Transcoding Module
- Signaling Security Module (aka Encryption SSM3)
- Solid State Drive (80GB SSD or 400GB SSD)
- AC-input 1100-watt Power Supply w/cabling
- DC-input 1100-watt Power Supply w/cabling
- Fan Pod
- System Air Filter
- SFP Module (1 GbE)
- SFP+ Module (10GbE)

Acme Packet 4600 Physical Interfaces

The Acme Packet 4600 has one network interface unit (NIU) that contains all external interfaces, including console, alarm, network management and media interfaces.

Warning: Customers must use either the 2 x 10GbE ports or the 4 x GbE ports. Using both P4-P5 and P0-P3 is not supported.

The following illustration shows the NIU labels and ports. These designations are an important point of reference when you set up the **phy-interface** configuration element.



The Acme Packet 4600 NIU contains the following ports (from left to right).

- Console—Provides serial access for administrative and maintenance purposes.
- Alarm—Dry contact alarm port.
- USB—The USB port is reserved for use by Oracle support employees, only.
- Mgmt 0–Mgmt 2—These 10/100/1000 Base-T Ethernet ports are used for EMS control, RADIUS accounting, CLI management, SNMP queries and traps, and other management functions.
- P4–P5—2 x 10GbE ports for signaling and media traffic.
- P0–P3—4 x GbE ports for signaling and media traffic.

The OID in ap-products.mib for the Acme Packet 4600 is 1.3.6.1.4.1.9148.1.1.3.

Acme Packet 4600 NIU Port Numbering Reference

Physical interfaces on the Acme Packet 4600 NIU are configured in the **phy-interface** configuration element. The **slot** parameter for this platform is always set to 0. The table below lists the mapping between the label on the NIU, **operation-type** parameter, and **port** parameter in the **phy-interface** configuration element.

NIU Label	operation-type	slot	port
Mgmt 0	maintenance	0	0
Mgmt 1	maintenance	0	1
Mgmt 2	maintenance	0	2
P0	media	0	0
P1	media	0	1

NIU Label	operation-type	slot	port
P2	media	0	2
P3	media	0	3
P4	media	0	4
P5	media	0	5

Acme Packet 4600 Physical Interface Configuration

To configure the **phy-interface** configuration element on an Acme Packet 4600:

1. Access the **phy-interface** configuration element.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# system
ACMEPACKET(system)#phy-interface
ACMEPACKET(phy-interface)#
```

2. **name**—Set a name for the interface using any combination of characters entered without spaces. For example: **`Internet`** (for a Fast Ethernet media and signaling interface) or **`maint0`** (for a maintenance interface).
3. **admin-state**—Leave the administrative state parameter set to **enabled** to receive and send media and signaling on an interface. Select **disabled** to prevent media and signaling from being received and sent. The default for this parameter is **enabled**. The valid values are:
   - enabled | disabled
4. **operation-type**—Select the type of physical interface connection to use. The default value is **control**. The valid values are:
   - **media**—Use this value for configuring either the four 1 GbE ports (P0-P3) or the two 10 GbE ports (P4-P5).

     ⚠ **Warning:** Use either the two 10 GbE ports or the four 1 GbE ports. Mixing these two is not supported.
   - **maintenance**—Use this value for configuring the management ports (Mgmt0-Mgmt2).
   - **control**—Use this value for configuring control traffic on the management ports (Mgmt0-Mgmt2), such as the HA control plane data.
5. **slot**—The only valid value on the Acme Packet 4600 is 0.
6. **port**—Set the port. Valid values are:
   - If operation-type is set to **media**, P0-P5
   - If operation-type is set to **maintenance**, P0-P2
   - If operation-type is set to **control**, P0-P2
7. Type **done** to save your configuration.

3

S-CZ7.2.0M3

This chapter provides feature descriptions for the contents of Release S-CZ7.2.0M3.

Current SPL Engine versions supported:

- C2.0.0
- C2.0.1
- C2.0.2
- C2.0.9
- C2.1.0
- C2.2.0
- C3.0.0
- C3.0.1
- C3.0.2
- C3.0.3
- C3.0.4
- C3.0.6
- C3.1.0
- C3.1.1
- C3.1.2

Current patch baseline: S-CZ7.2.0M2p3

Content Map for S-CZ7.2.0M3

The following content is available in release S-CZ7.2.0M3

Content Type	Description
Adaptation	SRTP Re-keying on reINVITE
Behavioral Change - Security	The user-level account now has read-only access on the filesystem. In order to SFTP files onto an Oracle Communications Session Border Controller's filesystem, you must log in with a superuser-level account.

SRTP Re-keying

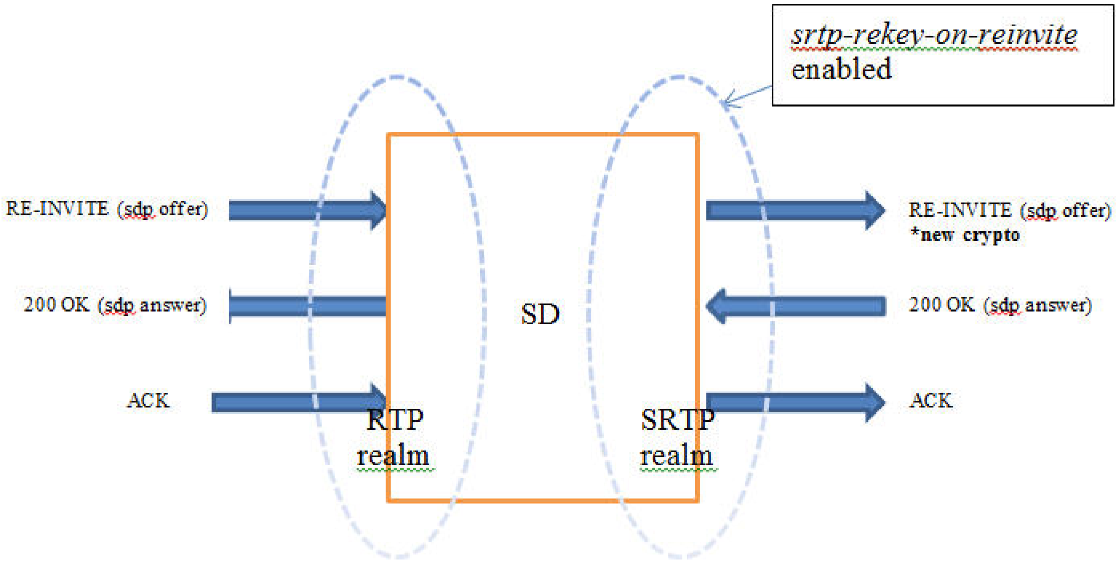
Initialization of SRTP re-keying is supported by the Oracle Communications Session Border Controller.

The Oracle Communications Session Border Controller can generate a new outbound crypto attribute in the SDP offer in a SIP re-INVITE when the **srtp-rekey-on-reinvite** parameter is set to **enabled**. The system generates the attribute regardless of the state of the flow, active or not.

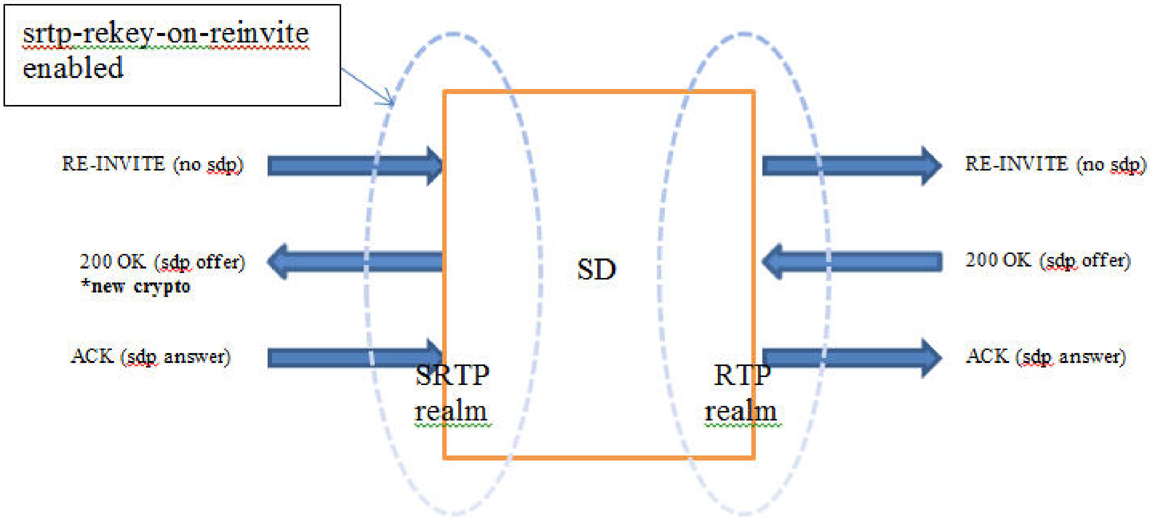
This capability is important for some clients that reside on the SRTP side in a single SRTP termination mode configuration. Any media changes that happen in the RTP side are hidden by the Oracle Communications Session Border Controller. This concealment may cause issues in some configurations, where media servers are involved. When the media changes from media server to called phone, the SRTP endpoint is not aware the media source changed because the SDP offer from the Oracle Communications Session Border Controller is the same as original invite. The result is that some devices drop packets because of Synchronization Source Identifier (SSRC) values mismatch, unexpected jumps in sequence number, sequence number reversions back to 1 triggering replay attack defense, and so forth. In certain environment is has been found that re-keying on every re-invite eliminates all these issues especially in customer setups that use Microsoft Lync products.

The processing of standard RE-INVITES (those containing an SDP offer) and offerless RE-INVITES is shown below.

With SDP:



No SDP:



If the re-invite message is a refresh and **srtp-rekey-on-reinvite** is enabled, the outbound crypto will change but the SDP version will not be incremented on the outgoing invite. If this scenario causes incompatibility issues with customer equipment then add the unique-sdp-id option to media-manager->option configuration so the Oracle Communications Session Border Controller increments the SDP version in the outgoing invite.

SRTP Re-keying Configuration

Configure **srtp-rekey-on-reinvite** to enable the negotiation and generation of new SRTP keys upon the receipt of a SIP RE-INVITE message that contains SDP.

Confirm that an **sdes-profile** exists.

In the following procedure, change the default state to enabled.

1. Access the **sdes-profile** configuration element.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# security
ACMEPACKET(security)# media-security
ACMEPACKET(media-security)# sdes-profile
ACMEPACKET(sdes-profile)#
```

2. Type **select** to choose and configure an existing object.

```
ACMEPACKET(sdes-profile)# select
<name>:
1:  name=sdesprofile01

selection: 1
ACMEPACKET(sdes-profile)#
```

3. **srtp-rekey-on-reinvite**—Set this parameter to **enabled** for re-keying upon the receipt of an SIP reINVITE that contains SDP.
4. Type **done** to save your configuration.

4

S-CZ7.2.0M4

This chapter provides feature descriptions for the contents of Release S-CZ7.2.0M4.

Current SPL Engine versions supported:

- C2.0.0
- C2.0.1
- C2.0.2
- C2.0.9
- C2.1.0
- C2.2.0
- C2.2.1
- C3.0.0
- C3.0.1
- C3.0.2
- C3.0.3
- C3.0.4
- C3.0.6
- C3.1.0
- C3.1.1
- C3.1.2
- C3.1.3

Current patch baseline: S-CZ7.2.0M3p1

Content Map for S-CZ7.2.0M4

The following content is available in release S-CZ7.2.0M4

Content Type	Description
Adaptation	Minimum Advertised SSL/TLS Version
Forward Merge	S-CZ7.1.2M4

S-CZ7.2.0M4 Known Issues

- Media and management (wancom) interfaces may not be configured with the same subnet, regardless of VLAN.

Minimum Advertised SSL/TLS Version

The sslmin option is available to set a minimum advertised security level to mitigate using older, more vulnerable versions of SSL. One such problem is the poodle attack(CVE-2014-3566).

Oracle Communications Session Border Controller uses OpenSSL in its SSL/TLS connections. Due to at least one vulnerability, the Poodle attack (CVE-2014-3566), SSLv3 is deemed insecure. Oracle Global Product Security (GPS) suggests that SSLv3 be disabled by default. Setting the option **sslmin** advertises the minimum version the server supports. Should you have SSLv3 set as the **tls-version** in any **tls-profile**, you will need to set **sslmin** to that version, if configured. It would be a configuration error if **sslmin** is greater than the **tls-version** value in any **tls-profile**.

Note: Note: The next SSL/TLS version after SSLv3 is TLS1.0.

In **security-config**, the **sslmin** option values can be: sslv3, tls1.0, tls1.1 or tls1.2. This change is platform-independent and applies to all Oracle Communications Session Border Controller.

Minimum Advertised SSL/TLS Version Configuration

Configuring the option **sslmin** to at least tls1.0 for security purposes, provided no **tls-version** in a **tls-profile** requires SSLv3.

1. Access the **security-config** configuration element.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# security
ACMEPACKET(security)# security-config
ACMEPACKET(security-config)#
```

2. Select the **security-config** object to edit.

```
ACMEPACKET(security-config)#

ACMEPACKET(security-config)#
```

3. **options**— Set the options parameter by typing **options**, a space, a plus sign, the option name **sslmin=** and then one of the valid values. Valid values are:

   - sslv3
   - tls1.0
   - tls1.1
   - tls1.2

```
ACMEPACKET(security-config)#options +sslmin=sslv3
```

4. Type **done** to save your configuration.

5

S-CZ7.2.0M5

This chapter provides feature descriptions for the contents of Release S-CZ7.2.0M5.

Current SPL Engine versions supported:

- C2.0.0
- C2.0.1
- C2.0.2
- C2.0.9
- C2.1.0
- C2.2.0
- C2.2.1
- C3.0.0
- C3.0.1
- C3.0.2
- C3.0.3
- C3.0.4
- C3.0.6
- C3.1.0
- C3.1.1
- C3.1.2
- C3.1.3

Current patch baseline: S-CZ7.2.0M4

Content Map for SCZ720M5

The following content is available in release S-CZ7.2.0M5

Content Type	Description
Forward Merge	S-CZ7.1.2M5

6

S-CZ7.2.0M6

This chapter provides feature descriptions for the contents of Release S-CZ7.2.0M6.

Current SPL Engine versions supported:

- C2.0.0
- C2.0.1
- C2.0.2
- C2.0.9
- C2.1.0
- C2.2.0
- C2.2.1
- C3.0.0
- C3.0.1
- C3.0.2
- C3.0.3
- C3.0.4
- C3.0.6
- C3.1.0
- C3.1.1
- C3.1.2
- C3.1.3
- C3.1.4
- C3.1.5

Current patch baseline: S-CZ7.2.0M5p4

Neighbor Release Patch Equivalency

Patch equivalency indicates which patch content in neighbor releases is included in this release. This can assure you in upgrading that defect fixes in neighbor stream releases are included in this release.

Neighbor Release Patch Equivalency for S-CZ7.2.0M6:

- S-CZ7.2.0M5p3

Content Map for SCZ720M6

The following content is available in release S-CZ7.2.0M6.

Content Type	Description
Platform Support	The OC-SR is now supported on HP DL 360 Gen9 platforms running SPP2015.06 firmware
Coproduct Support	Compatibility with L-CX1.5.0M1 Balance on IP/Port Feature
Entitlement Change	Requirement for entitlement configuration when using IMS-AKA or IPSec Trunking
Adaptation	Asynchronous SIP-Diameter Communication
Adaptation	SIP Pre-emptive Symmetric Media Latching
Adaptation	Rx Support in the Context of Media Release

Known Issues

The following are known issues new to S-CZ7.2.0M6. Please review the Caveats and Known Issues sections in the Release Notes document upon any upgrade or when deploying new features.

- The High Availability (HA) function can fail to synchronize registrations when operating over an Acme Packet 4500 that includes a HiFN-QOS physical interface card and configured with a large number (1000) of VLANs.

Platform Support

The OC-SR is now supported on HP DL 360 Gen9 platforms running SPP2015.06 firmware. See the *Software Installation on HP Platforms*, available on Oracle's Communications Documentation website under Session Router > Release S-CZ7.3.0 for instructions on installing the OC-SC on the HP DL 360.

Coproduct Support

The products/features listed in this section run in concert with the Oracle Communications Session Border Controller for their respective solutions.

Oracle Communications Subscriber-Aware Load Balancer

With an Oracle Communications Subscriber-Aware Load Balancer running L-CX1.5.0M1, all SBC cluster members must run S-CZ7.2.0M6 to use the Address/Port balancing feature released with L-CX1.5.0M1.

Please refer to the *Oracle Communications Subscriber-Aware Load Balancer Essentials Guide* for additional information.

IMS-AKA Endpoint and IPSec Trunking Session Allocations

Users with IMS-AKA or IPSec Trunking (IPSec with IKEv1) deployments must set the maximum number of endpoints/sessions they require using the **setup entitlements** command. These two capacities are listed in the **setup entitlements** command as follows:

- IMS-AKA Endpoints
- IPSec Trunking Sessions

Maximum configurable values per platform are listed as follows.

Platform	Maximum Capacity:	
	IMS-AKA Endpoints	IPSec Trunking Sessions
Acme Packet 3820	-	1024
Acme Packet 4500	100,000	1024
Acme Packet 4600	500,000	1024
Acme Packet 6100	500,000	1024
Acme Packet 6300	500,000	1024

Note: Despite these numbers, other capacity limitations my apply first, e.g., maximum IMS-AKA TCP subscribers could be less than the maximum configurable IMS-AKA Endpoints entitlement, on a platform basis.

After you change these values, a reboot is required.

Upgrade Considerations

When upgrading to this release, you must invoke the **setup entitlements** command before performing the actual upgrade for changes to take effect. This action must be performed on both the active and standby systems in an HA configuration.

Asynchronous SIP-Diameter Communication

The Oracle Communications Session Border Controller's Diameter-based external policy server support now offers an asynchronous mode in which the SBC does not wait for a Diameter Authorization-Authentication Answer (AAA) response to an Authorization-Authentication Request (AAR) before allowing the SIP 200 OK to proceed through the SBC.

One of the fundamental behaviors in the Oracle Communications Session Border Controller's Diameter model relies on the external policy server making an authorization decision which is then communicated to the SBC. Part of the call authorization sequence of events involves the SBC waiting for an external policy server's response before the SBC can completely set up, modify, or update the call. The long pause that the endpoints experience, while the SBC holds up SIP flows waiting for the external policy server's response, can lead to unnecessary call failure situations.

In some Diameter-based external policy server deployments, the media traverses a Cable Modem Termination System (CMTS) at the edge of the network; the CMTS gates may be established by a Policy Server to dynamically enable QoS from a UE toward another UE. If no gate is established then the media traverses the CMTS and is admitted to the network with a "best-effort" network path.

As QoS sessions might not be the most important priority to a network, Oracle now allows network operators the ability to decouple the call set up (signaling) from the request for bandwidth. The SBC's default external policy server model is the synchronous model, in which the SBC sends a policy server request based on a SIP or SDP trigger point, and the SIP signaling is held until a response is returned from the Policy Sever. In the asynchronous model the request that the SBC sends to the Policy Server flows in an asynchronous state with respect to SIP messaging; that is, the SBC allows the SIP session to proceed naturally, and does not pause for outstanding Policy Server answers to be received. The establishment of a SIP session is not affected by Policy Server answers, or answer timeouts, related to the SIP session. To enable the asynchronous model, the new parameter **asynchronous-mode** has been added to the **ext-policy-server** configuration element, with a default of **disabled** so as not to affect current default behavior.

Note: Oracle Communications recommends that, for each SBC, the same model be used for all external policy server configuration instances. Failure to follow this guideline could result in complex interactions from a timing perspective which might lead to dropped or degraded calls.

Serialized Diameter Messaging

After the Oracle Communications Session Border Controller sends a Diameter request, it will not send another Diameter request, such as a Session Termination Request (STR), with the same Session-ID Attribute Value Pair (AVP) until the original request receives a response or times out.

Access networks with complex policy server structures can allow non-sequential delivery of Diameter requests into a Cable Modem Termination System (CMTS), even if Diameter message delivery was correctly ordered on the TCP connection between the SBC and a lower-tiered external policy server.

The SBC now prevents the external policy server from receiving out-of-order messages at the application layer by serializing them. The SBC serializes Diameter messages to ensure that a Diameter request for one session-ID is not sent until an answer is received from the previous request for the same session-ID. The SBC applies this constraint while waiting for a Diameter response or when considering a Diameter request timeout (15 seconds). Serialized Diameter messaging is always enforced for Diameter-based external policy server communication.

SIP-Diameter Communication Configuration

1. Access the **ext-policy-server** configuration element.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# media-manager
ACMEPACKET(media-manager)# ext-policy-server
ACMEPACKET(ext-policy-server)#
```

2. Select the **ext-policy-server** object to edit.

```
ACMEPACKET(ext-policy-server)# select
<name>:1:  name=extpol1

selection: 1
ACMEPACKET(ext-policy-server)#
```

3. **asynchronous-mode** — identifies whether to use the asynchronous mode of signaling on the external policy server interface rather than the default synchronous mode. Allowable values are **enabled** and **disabled**. The default is **disabled.**
4. Type **done** to save your configuration.

SIP Pre-emptive Symmetric Media Latching

The Oracle Communications Session Border Controller (SBC) supports symmetric media latching within a realm. However, when two SBCs are in different realms and both realms are configured for symmetric latching, then both will wait for received media packets from the other before transmitting, which results in dropped calls. This feature lets the user configure the SBC to transmit its RTP packets pre-emptively to the peer SDP connection address and then to re-latch the peer RTP source address after receiving the first RTP packet from that peer.

In a call forwarding scenario where a media server (MS) behind Network Address Translation (NAT) is between two SBCs, both SBCs will detect NAT, so both will wait to receive RTP packets before latching to the RTP source address. This feature prevents this by adding the new value **pre-emptive** to the configuration option parameter **symmetric-latching** in the configuration element **realm-config**. When the value is set to **pre-emptive**, the SBC sends the RTP packets to the received SDP connection address without waiting on the latch. Once the RTP packets are received from the peer endpoint, the SBC detects the NAT address mapping; if there is a change in the RTP source address, the SBC re-latches to the new RTP source address. Subsequent RTP packets are then sent to the peer RTP source address. This is also the behavior when there is an UPDATE or reINVITE with the SDP message.

Pre-emptive Symmetric Media Latching Configuration

1. Access the **realm-config** configuration element.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# media-manager
ACMEPACKET(media-manager)# realm-config
ACMEPACKET(realm-config)#
```

2. Select the **realm-config** object to edit.

```
ACMEPACKET(realm-config)# select
identifier:
1: realm01 left-left:0 0.0.0.0

selection: 1
ACMEPACKET(realm-config)#
```

3. **symmetric-latching** — identifies whether and how to enable symmetric latching in the realm. The default value is **disabled**.
   - **disabled**
   - **enabled**
   - **pre-emptive** — symmetric latching is enabled but the SBC sends RTP packets to the received SDP connection address without waiting on the latch
4. Type **done** to save your configuration.

Flow-Description AVP Change for Media Release

The current implementation of the Rx interface between the Oracle Communications Session Border Controller (SBC) and the Policy Server (PS) assumes that the media is always managed by the SBC and that the IP address and port number of one end of a service flow will always correspond to one present on the SBC. However, there are times when the media is released by the SBC, but a policy server request is still required. In these cases the flow descriptions should accurately represent the IP addresses of the two endpoints instead of that of the SBC. This feature lets the user configure the SBC to change the payload of the Flow-Description Attribute Value Pair (AVP) in the Diameter AAR messaging from the SBC to the PS, depending on whether the media is managed or released by the SBC.

In the case where the media is released, only incomplete flow information may be provided to the Policy Server because not all IP addresses and port numbers are known from the SDP offer. Media release is enabled on a per realm basis with the following settings in the **`realm-config`** configuration element:

```
        mm-in-realm                     disabled
        mm-in-network                   disabled
        mm-in-system                    disabled
        mm-same-ip                      disabled
        msm-release                     enabled
```

When the realm is configured for external bandwidth management, the media layer checks if any of the configuration parameters for media release have been invoked. If none of the media release parameters are invoked (meaning that the SBC is managing the media), then the signaling application constructs the bandwidth request to the PS as it currently does. If the media layer detects that the realm is configured to possibly release media, then a few more operations are performed to correctly populate the bandwidth request to the PS. If the media has been released for the session, the signaling application inserts the IP port of the called endpoint into the bandwidth request instead of the IP port for the SBC. If the media has not yet been released, the media layer determines if the initial signal is an OFFER or an ANSWER. If it is an ANSWER the IP port in the bandwidth request will be that of the SBC because the SBC is managing the media for the session. If it is an OFFER, the signaling application inserts an empty IP port into the bandwidth request and sets a flag in the bandwidth request indicating unqualified flow information at this time. This occurs regardless of the value of the parameter **reserve-incomplete** in the **ext-policy-server** configuration element.

To enable this behavior on the Rx interface, the new parameter **media-release** has been added to the **ext-policy-server** configuration element.