Oracle® Communications Session Border Controller

Maintenance Release Guide
Release S-CZ7.1.2

June 2015

ORACLE

Notices

Contents

About this guide

The Maintenance Release Guide provides information about the contents of maintenance releases related to Oracle Communications Session Border Controller S-CZ7.1.2. 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-CZ7.1.2, this document informs you of changes made to the software in the maintenance releases of S-CZ7.1.2. Consult this document for content specific to maintenance releases. For information about general Oracle Communications Session Border Controller 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.

Maintenance Release Availability Matrix

The table below lists the availability for version S-CZ7.1.2 maintenance releases.

Maintenance release number	Availability Notes
S-CZ7.1.2M1	September 13, 2013
S-CZ7.1.2M2	November 26, 2013
S-CZ7.1.2M3	May 23, 2014
S-CZ7.1.2M4	March 27, 2015
S-CZ7.1.2M5	May 21, 2015

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 Acme Packet 4500 system.
Acme Packet 3820 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 3800 system.

Document Name	Document Description
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 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 accounting support, including details about RADIUS accounting.
HDR Resource Guide	Contains information about the Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Administrative Security Essentials	Contains information about support for the Administrative Security license.

Revision History

Date	Description
September 13, 2013	Initial Release
November 26, 2013	This release corresponds with the S-CZ7.1.2M2 maintenance release.
February 3, 2014	Updates S-CZ7.1.2M2 Chapter to indicate new platform support.
May 23, 2014	This release corresponds with the S-CZ7.1.2M3 maintenance release.
March 27, 2015	This release corresponds with the S-CZ7.1.2M4 maintenance release.
May 21, 2015	This release corresponds with the S-CZ7.1.2M5 maintenance release.
June 5, 2015	Adds Known Issue section to S-CZ7.1.2M5 chapter.

1

S-CZ7.1.2M1

This chapter provides descriptions, explanations, and configuration information for the contents of Release S-CZ7.1.2M1.

Current SPL Engine Version: C3.0.0

Current patch baseline: S-CZ7.1.2p1

Content Map for S-CZ7.1.2M1

This section provides a table listing all content in Release S-CZ7.1.2M1.

Content Type	Description
Adaptation	Transcoding Support for Asymmetric Dynamic Payload Types

Transcoding Support for Asymmetric Dynamic Payload Types

Transcoding Support for Asymmetric Dynamic Payload Types supports the case when asymmetric payload types such that the RTP offered with one payload type and answered with another payload type will be acceptable to the Oracle Communications Session Border Controller when performing transcoding.

In certain network environments, MSC (Mobile Switching Center) equipment may require that originally offered (PT) payload type mappings be retained for the session duration, even if they are have been subsequently re-mapped as a result, for instance, of a RE-INVITE, PRACK or local codec policies.

For example:

1. The originating MSC issues an INVITE with an SDP offer of EVRCO (96).
2. The Oracle Communications Session Border Controller responds with EVRCO (96) in the SDP answer.
3. The far end puts the established call on hold, and subsequently resumes the call with a RE-INVITE.
4. The originating network policy adds EVCRO (97), incrementing the PT.
5. The originating MSC accepts the offered payload, EVRCO (97),but still answers with the originally negotiated PT, EVCRO (96).
6. Since the Oracle Communications Session Border Controller does not support asymmetric payloads, it accepts EVRCO (96) for both RTP flows, and sets up digital signal processors (DSPs) with these parameters.
7. However since the originating MSC received the EVCRO (97) and responded with EVCRO (96), it expects to receive RTP with PT=96, and send RTP with PT=97.

8. Consequently, the origination-side RTP is broken because the Oracle Communications Session Border Controller drops the RTP it receives with an unexpected PT=97.

To address this problem, this version supports asymmetric payload types such that RTP offered with one payload type and answered with another payload type is acceptable to the Oracle Communications Session Border Controller when providing transcoding.

Configure Transcoding for Asymmetric Dynamic Payload Types

Transcoding support for asymmetric dynamic payload types enables the Oracle Communications Session Border Controller to perform transcoding when the Real-time Transport Protocol (RTP) is offered with one payload type and is answered with another payload type. Enable transcoding for asymmetric dynamic payload types from the command line.

Before You Begin

- Confirm that you are in Superuser mode.

Procedure

1. Access the **media-manager-config** configuration element.

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

2. Type select to begin editing.

```
ACMEPACKET(media-manager-config)# select

ACMEPACKET(media-manager-config)#
```

3. Use the **options +audio-allow-asymmetric-pt** command to enable support for asymmetric payload types.

```
ACMEPACKET#(media-manager) options +audio-allow-asymmetric-pt
ACMEPACKET#(media-manager)
```

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

2

S-CZ7.1.2M2

This chapter provides descriptions, explanations, and configuration information for the contents of Release S-CZ7.1.2M2.

Current SPL Engine Version: C3.0.1

Current patch baseline: S-CZ7.1.2M1p1

Content Map for S-CZ7.1.2M2

This section provides a table listing all content in Release S-CZ7.1.2M2.

Content Type	Description
Adaptation	IMS-AKA Port Change on Client
Defect fix	Show prom-info command updated
Platform Support	Acme Packet 6100 added to supported platforms as of S-CZ7.1.2M2

S-CZ7.1.2M2 Caveats and Known Issues

IMS-AKA Caveats

- Security Association (SA) entries are not cleared after Deregistration when an IMS-AKA protected port pool is enabled.

  This behavior has been observed on both Acme Packet 4500 and 6300 Session Border Controllers (SBC).
- After failover, the newly designated Active SBC always uses port 5060, the assigned SIP port when it sends an initial SIP message to an endpoint even when the IMS-AKA protected port pool is enabled.

  With the port pool enabled, the active SBC should use a port number from the protected pool. After the initial message, subsequent SIP transactions correctly use a port number from the protected pool.

  This behavior has been observed on both Acme Packet 4500 and 6300 SBCs.
- Inbound and outbound SA counts can lose synchronization when an IMS-AKA protected port pool is enabled.

  This behavior has been observed on both Acme Packet 4500 and 6300 SBCs.

- After failover, Security Parameter Index (SPI) value are not properly synchronized when the IMS-AKA protected port pool is enabled.

  This behavior has been observed on both Acme Packet 4500 and 6300 SBCs.

Web GUI Caveats

- Release S-CZ7.1.2M2 has temporarily disabled the Web Server. Disabling the Web Server impacts services such as SIP Monitoring and Tracing and System Tab. The Web Server will be upgraded and re-enabled in a future software release.

IMS-AKA Change Client Port

The Oracle Communications Session Border Controller is now in compliance with 3GPP TS 33.203, *Access Security for IP-Based Services*. Previous releases did not comply with requirements specified in Section 7.4, Authenticated re-registration, which reads in part:

Every registration that includes a user authentication attempt produces new security associations. If the authentication is successful, then these new security associations shall replace the previous ones. This clause describes how the UE and P CSCF handle this replacement and which SAs to apply to which message.

When security associations are changed in an authenticated re-registration then the protected server ports at the UE (port_us) and the P-CSCF (port_ps) shall remain unchanged, while the protected client ports at the UE (port_uc) and the P-CSCF (port_pc) shall change.

If the UE has an already active pair of security associations, then it shall use this to protect the REGISTER message. If the S-CSCF is notified by the P-CSCF that the REGISTER message from the UE was integrity-protected it may decide not to authenticate the user by means of the AKA protocol. However, the UE may send unprotected REGISTER messages at any time. In this case, the S-CSCF shall authenticate the user by means of the AKA protocol. In particular, if the UE considers the SAs no longer active at the P-CSCF, e.g., after receiving no response to several protected messages, then the UE should send an unprotected REGISTER message."

Prior releases failed to change the protected client ports after a successful re-registration.

Protected Ports

Within IMS networks, the P-CSCF provides the network access point and serves as the outbound proxy server for user equipment -- smart phones, tablets, and similar devices. The UE must connect to the P-CSCF prior to registration and initiation of SIP sessions. Connection to the P-CSCF, which can be in the user's home network, or in a visited network if the UE is roaming, is accomplished using Dynamic Host Control Protocol (DHCP) P-CSCF discovery procedures.

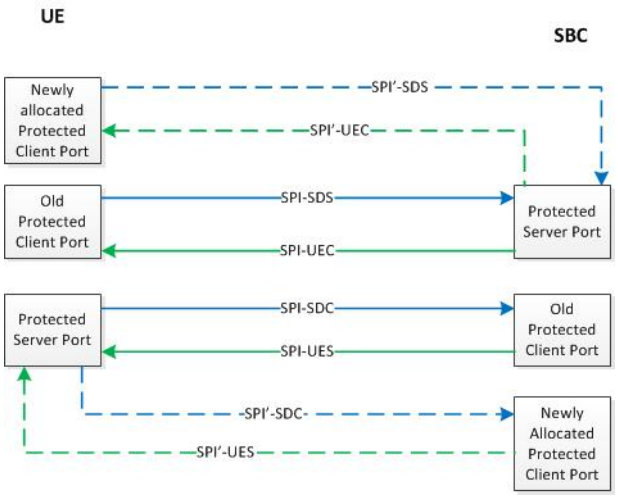
After successful discovery, the P-CSCF and UE negotiate IPSec security associations (SAs) which are used to establish four protected (authenticated and encrypted using Encapsulating Security Payload protocol) ports between the UE and the P-CSCF.

The four protected ports are shown in the following illustration:

As required by Section 7.4 of 3GPP TS 33.203, the protected client ports, one on the UE and the other on the SBC, must be changed after each successful re-registration.

To fulfill this requirement, this release adds a new attribute to the existing ims-aka-profile configuration object. This attribute (**end-protected-client-port**) works in conjunction with **start-protected-client-port** (**protected-client-port** in previous releases) to enable the identification of a pool of protected client ports, which will be used for re-registration scenarios where the SBC/P-CSCF is required to change the client port.

The SBC creates new protected client ports, one on the UE and the other on the SBC, after every re-registration. Old protected client ports, along with their associated SAs, are maintained for 30 seconds after re-registration to ensure correct handling or any pending responses to previously transmitted messages.



After successful re-registration, the SBC updates the registration cache with updated port information and checkpoint with the HA peer, if present.

IMS-AKA Change Client Port Configuration

An IMS-AKA profile establishes the client and server ports to be protected, and it defines lists of encryption and authentication algorithms the profile supports. You can configure multiple IMS-AKA profiles, which are uniquely identified by their names.

You apply an IMS-AKA profile to a SIP port configuration using the name.

To configure an IMS-AKA profile:

1. From Superuser mode, use the following command sequence to navigate to ims-aka-profile configuration mode.

```
ACMEPACKET# configure terminal
ACMEPACKET(configure)# security
ACMEPACKET(security)# ims-aka-profile
ACMEPACKET(ims-aka-profile)#
```

2. **name**—Enter the name you want to give this IMS-AKA profile. This is the value you will use to apply the profile to a SIP port configuration. This parameter is required, and it has no default value.
3. **protected-server-port**—Enter the port number of the protected server port, which is the port on which the Oracle Communications Session Border Controller receives protected messages. The protected server port should not overlap with the port range defined in the steering ports configuration using the same IP address and the SIP interface. If there is overlap, the NAT table entry for the steering port used in a call will prevent SIP messages from reaching the system's host processor.

   This parameter defaults to 0, which disables the function associated with the parameter. The valid range for values is 1025 to 65535.
4. **start-protected-client-port (protected-client-port in Release S-CX6.3.3M2 and earlier releases)**—Enter the start value for the pool of port numbers available following a successful re-authentication. Like the protected server port, the protected client port pool should not overlap with the port range defined in the steering ports configuration using the same IP address and the SIP interface. If there

is overlap, the NAT table entry for the steering port used in a call will prevent SIP messages from reaching the system's host processor.

Any existing configuration for **protected-client-port** will be mapped to both **start-protected-client-port** and **end-protected-client-port** parameter values.

This parameter defaults to 0, which disables the function associated with the parameter. The valid range for values is 1025 to 65535.

5. **end-protected-client-port**—Enter the end value for the pool of port numbers available following a successful re-authentication. Ensure that this value is greater than the value assigned to **start-protected-client-port**. Note that the maximum supported pool contains 5 entries. Like the protected server port, the protected client port pool should not overlap with the port range defined in the steering ports configuration using the same IP address and the SIP interface. If there is overlap, the NAT table entry for the steering port used in a call will prevent SIP messages from reaching the system's host processor.

   This parameter defaults to 0, which disables the function associated with the parameter. The valid range for values is 1025 to 65535.

6. **encr-alg-list**—Enter the list of encryption algorithms. You enter more than one value by separating the algorithms by <Spaces> and enclosing all values in quotations marks:

   This parameter defaults to the following three values: **aes-cbc**, **des-ede3-cbc**, and **null**.

7. **auth-alg-list**—Enter the list of authentication algorithms. You enter more than one value by separating the algorithms by <Spaces> and enclosing all values in quotations marks:

   This parameter defaults to hmac-sha-1-96.

Sample IMS-AKA Configuration

The following formatted extract from **show running-config** ACLI output shows a sample IMS-AKA profile configuration.

```
ims-aka-profile
name    TS33.203
start-protected-client-port    4060
end-protected-client-port    4064
protected-server-port    4070
encr-alg-list    aes-cbc des-ede3-cbc null
auth-alg-list    hmac-sha-1-96 hmac-md5-96
last-modified-by    admin@172.30.11.18
last-modified-date    2013-06-15 14:58:08
```

ACLI Command Changes and Updates

show prom-info

Syntax

```
show prom-info <devices>
```

The show prom-info command displays hard-coded information about Oracle Communications Session Border Controller PROM information. The valid arguments which you enter in the show prom-info command depend on the current platform.

The show prom-info command is most immediately used to obtain device part numbers and revisions.

Arguments

<devices> The following is a list of available prom-info devices to query:

Acme Packet 3820 (where supported) and Acme Packet 4500

- CPU— CPU PROM information
- MGMT—management interface card PROM information
- PHY0—NIU card PROM information
- POWER— power supply PROM information
- SEC0—security module PROM information
- TCU1-DIMM—lists the populated DSP DIMMs on a TCU card and their PROM information
- all—Show all available PROM information
- mainboard—Display mainboard PROM information

Acme Packet 6300

- CPU— CPU PROM information
- FLEX1—riser card between mainboard and NIU in slot 1 PROM information
- FLEX2—riser card between mainboard and NIU in slot 2 PROM information
- MGMT— management interface card PROM information
- PHY0—NIU card 0 (bottom) PROM information
- PHY1—NIU card 1 (middle) PROM information
- PHY2— NIU card 2 (top) PROM information
- POWER— power supply PROM information
- SEC1—security module 1 PROM information
- SEC2—security module 2 PROM information
- TCU1-DIMM— lists the populated DSP DIMMs on the TCU 1 card and the modules' PROM information
- TCU2-DIMM— lists the populated DSP DIMMs on the TCU 2 card and the modules' PROM information
- all—Show all available PROM information
- mainboard—Display mainboard PROM information

Acme Packet 6100

- CPU— CPU PROM information
- MGMT—management interface card PROM information
- PHY0— NIU card PROM information
- POWER—power supply PROM information
- SEC0—security module PROM information
- TCU1-DIMM— lists the populated DSP DIMMs on a TCU card and their PROM information
- all—Show all available PROM information
- mainboard—Display mainboard PROM information

Example

```
ACMEPACKET# show prom-info mainboard
```

3

S-CZ7.1.2M3

This chapter provides descriptions, explanations, and configuration information for the contents of Release S-CZ7.1.2M3.

Current SPL Engine versions supported:

- 2.0.0
- 2.0.1
- 2.0.2
- 2.0.9
- 2.1.0
- 2.2.0
- 3.0.0
- 3.0.1
- 3.0.2
- 3.0.3
- 3.1.0

Current patch baseline: S-CZ7.1.2M2p4

Content Map for S-CZ7.1.2M3

This section provides a table listing all content in Release S-CZ7.1.2M3

Content Type	Description
Adaptation	Support for Encoded Multipart Message Bodies

Support for Encoded Multipart Message Bodies

SIP messages and responses may arrive at the Oracle Communications Session Border Controller with encoded multipart message bodies, such that the content of the body is unreadable. This information may be encoded for the purpose of compressing the data. Normally, the Oracle Communications Session Border Controller would consider the body invalid and reject the entire message, replying to the sender with a 400 Invalid Body error response. The user, however, can configure the **sip-config** option, **proxy-content-type-encodings**, allowing the Oracle Communications Session Border Controller to accept, process and forward messages containing these encoded parts. This configuration causes the Oracle Communications Session Border Controller to ignore the encoding, identify the

end of the message via content length, and pass the message towards its intended recipient with the multipart body fully encoded.

The condition that triggers this functionality is the Oracle Communications Session Border Controller recognizing the presence of a multipart message body and the definition of the encoding type within the message.

```
NOTIFY sip:user@example.com SIP/2.0
Via: SIP/2.0/TCP
...
Content-Type: multipart/mixed;boundary="imdn-boundary"
Content-Encoding: gzip

... Encoded multipart content ...
```

When configured, the **proxy-content-type-encodings** is simply a list of strings. The Oracle Communications Session Border Controller looks to match the string defining the content encoding with a string in the list to proceed with the functionality.

The Oracle Communications Session Border Controller only performs this procedure on messages encoded with types for which it is configured and that are properly formed. Examples of when the Oracle Communications Session Border Controller does not perform this procedure include:

- The Oracle Communications Session Border Controller receives a message with an encoded multipart message block, but **proxy-content-type-encodings** list is empty. In this case, the Oracle Communications Session Border Controller responds with a 415 Unsupported Media Type.
- The message arrives with a multipart message body with encoding for which the **proxy-content-type-encodings** is configured, but there is no terminating boundary. In this case, the Oracle Communications Session Border Controller replies with a 400 Invalid Body error.
- The Oracle Communications Session Border Controller receives a response with an encoded multipart message block, but **proxy-content-type-encodings** list is empty. In this case, the Oracle Communications Session Border Controller simple drops the response.

Multipart Message Encoding Support Configuration

The procedure below provides the steps needed to configure the Oracle Communications Session Border Controller for multipart message encoding support.

To have your Oracle Communications Session Border Controller proxy messages despite the presence of the specified multipart message encoding:

1. In Superuser mode, use the following command sequence to access the **sip-config** element.

   ```
   ACMEPACKET# configure terminal
   ACMEPACKET(configure)# session-router
   ACMEPACKET(session-router)# sip-config
   ACMEPACKET(sip-config)#
   ```

   From this point, you can configure encoding support.

2. Configure the desired encoding types using the option followed by comma-separated coding types.

   The example below configures support for gzip and compressed encoding.

   ```
   ACMEPACKET(sip-config)# options +proxy-content-type-encodings=gzip,compress
   ```

3. Type **done** and exit configuration mode. Save and activate your configuration.

4

S-CZ7.1.2M4

This chapter provides feature descriptions for the contents of Release S-CZ7.1.2M4.

Current SPL Engine versions supported:

- 2.0.0
- 2.0.1
- 2.0.2
- 2.0.9
- 2.1.0
- 2.2.0
- 3.0.0
- 3.0.1
- 3.0.2
- 3.0.3
- 3.0.6
- 3.1.0

Current patch baseline: S-CZ7.1.2M3p6

Content Map for S-CZ7.1.2M4

The following table classifies and lists the new content in this release.

Content Type	Description
Adaptation	Minimum Advertised SSL/TLS Version

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-CZ7.1.2M5

This chapter provides feature descriptions for the contents of Release S-CZ7.1.2M5.

Current SPL Engine versions supported:

- 2.0.0
- 2.0.1
- 2.0.2
- 2.0.9
- 2.1.0
- 2.2.0
- 3.0.0
- 3.0.1
- 3.0.2
- 3.0.3
- 3.0.6
- 3.1.0

Current patch baseline: S-CZ7.1.2M4p1

Content Map for S-CZ7.1.2M5

The following table classifies and lists the new content in this release.

Content Type	Description
Security Update	SSL Library Update

S-CZ7.1.2M5 Known Issues

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

Glossary