

Oracle® Unified Session Manager

Release Notes

Release S-CZ7.3.5

October 2017

Notices

Copyright© 2017, 2004, Oracle and/or its affiliates. All rights reserved.

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 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

About This Guide.....	5
1 Introduction to S-CZ7.3.5.....	9
Platform Support.....	9
Image and Bootloader File Conventions.....	9
Bootloader Requirements.....	10
NIU and Feature Group Requirement.....	10
Supported Upgrade Paths.....	11
Co-Product Support.....	11
QoS NIU Version Requirement for Acme Packet 4500.....	12
System Capacities.....	12
Neighbor Release Patch Equivalency.....	12
Access Control Endpoint Classification Capacity and DoS.....	12
Supported SPL Engines.....	12
2 New Features in Service Provider Release S-CZ7.3.5.....	15
IMS Features.....	15
3 Inherited Features.....	19
System Features.....	19
Inherited Sec Features.....	20
IMS Features.....	21
Signaling Application and Monitoring Features.....	21
TSCF Features.....	23
Inherited Transcoding Features.....	23
4 Interface Changes.....	25
ACLI Command Changes.....	25
ACLI Configuration Element Changes.....	25
SNMP/MIB Changes.....	29
5 Caveats, Known Issues, and Behavioral Changes.....	35
Issues Resolved and Known Issues in this Release.....	35
Caveats.....	37
Behavioral Changes.....	38



About This Guide

Overview

The Oracle USM Release Notes provides the following information when applicable:

- An overview of the new features available
- An overview of the interface enhancements
- A summary of known issues and caveats

If any of these sections does not appear in the document, then there were no changes to summarize in that category for this release.

Supported Platforms

Release Version S-CZ7.3.5 includes both the Oracle Core Session Manager (CSM) and Unified Session Manager (USM) products. The Oracle USM is supported on the Acme Packet 4600, 4500, 6100, and 6300 series platforms. The Oracle CSM is supplied as virtual machine software or as a software-only delivery suitable for operation on server hardware. Refer to sales documentation updates for information further specifying hardware support.

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.
Acme Packet 4600 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 4600.
Acme Packet 6100 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6100.
Acme Packet 6300 Hardware Installation Guide	Contains information about the components and installation of the Acme Packet 6300.
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 Service Provider Oracle USM.
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 USM 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), Oracle Communication's enterprise MIBs, general trap information, including specific details about standard traps and enterprise traps, Simple Network Management

About This Guide

Document Name	Document Description
	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 USM's accounting support, including details about RADIUS and Diameter accounting.
HDR Resource Guide	Contains information about the Oracle USM's Historical Data Recording (HDR) feature. This guide includes HDR configuration and system-wide statistical information.
Administrative Security Essentials	Contains information about the Oracle USM'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 USM family of products.
Installation and Platform Preparation Guide	Contains information about upgrading system images and any pre-boot system provisioning.
Call Traffic Monitoring Guide	Contains information about traffic monitoring and packet traces as collected on the system. This guide also includes WebGUI configuration used for the SIP Monitor and Trace application.

Hardware documentation listed above is relevant only to the Oracle USM. Refer to your hardware vendor's documentation for information required for Oracle CSM operation.

The version SCZ735 software documentation set relies on three version SCZ730 documents:

- The ACLI Reference Guide
- The Troubleshooting and Maintenance Guide
- The Administrative Security Essentials Guide

Revision History

Date	Description
March, 2016	<ul style="list-style-type: none">• Initial Release
April, 2016	<ul style="list-style-type: none">• Corrects 4500 encryption phy support
May, 2016	<ul style="list-style-type: none">• Adds known issue on addressing that must not be used for HA deployments that include transcoding cards
May, 2016	<ul style="list-style-type: none">• Adds SRS deprecation caveat
July, 2016	<ul style="list-style-type: none">• Updated for M1 release
September, 2016	<ul style="list-style-type: none">• Removes defect description unrelated to release

Date	Description
March 2017	<ul style="list-style-type: none">• Updates the supported FPGA version to 2.22 and removes the show qos command from the "QoS NIU Version Requirement for Acme Packet 3820 and Acme Packet 4500" section.
March 2017	<ul style="list-style-type: none">• Updates the supported FPGA version to 2.22 and removes the show qos command from the "QoS NIU Version Requirement for Acme Packet 3820 and Acme Packet 4500" section.
May 2017	<ul style="list-style-type: none">• Updated for M2 release
October 2017	Includes the following Caveats <ul style="list-style-type: none">• Interface Utilization Support

Introduction to S-CZ7.3.5

The Oracle USM S-CZ7.3.5 Release Notes provide the following information about this product:

- Supported platforms and hardware requirements
- An overview of the new features available in this release
- An overview of previously-available features that are new to the GA of this major release
- A summary of changes the Oracle USM interfaces including the ACLI, MIB Support, and accounting interfaces.
- A summary of known issues, caveats, and behavioral changes

Platform Support

The following platforms are supported by S-CZ7.3.5:

- AP4500
- AP4600
- AP6100
- AP6300

4500 CPU Support

- Only the 64-bit CPU 2 on the AP4500 is supported. The AP4500's CPU revision must be MOD-0026-xx. Systems containing MOD-0008-xx are unsupported. You may query this with the **show prom-info cpu** command.

Acme Packet 4000 Transcoding NIU Support

Acme Packet 4000 chassis with a transcoding NIU upgrading to S-CZ7.3.5 and above must have a high-speed fan module to ensure sufficient cooling.

Image and Bootloader File Conventions

The AP 4500, AP 4600, AP6100, and AP6300 should be provisioned with the 64-bit Oracle USM image file in the boot parameters. 64-bit image files are recognized by the "64" between the image revision and file extension. e.g., nnSCZ735.64.bz.

All platforms require that you install a stage 3 bootloader. The Stage 3 bootloader is identified by ending with a `.boot` extension. Stage 3 bootloaders and system image files have identical name portions of the

Introduction to S-CZ7.3.5

filename, and are distributed together. For this software the GA system image and Stage 3 bootloader are nnSCZ735.64.bz and nnSCZ735.boot respectively.

Bootloader Requirements

Acme Packet 4500 Bootloaders

The Acme Packet 4500 requires Stage 1, Stage 2, and Stage 3 bootloaders.

Stage 1 and Stage 2 bootloaders should be dated no earlier than July 3, 2013 (MOS patch # 18185632). Use the **show version boot** command to view current bootloader version on your system.

Stage 1 and Stage 2 bootloader updates are available on My Oracle Support listed under the respective hardware.

The Stage 3 bootloader accompanies the image file, as distributed. It should be installed according to the instructions found in the Maintenance and Troubleshooting Guide.

Acme Packet 4600, 6100 and 6300 Bootloaders

Acme Packet 4600, 6100 and 6300 require a Stage 3 bootloader that accompanies the image file, as distributed. It should be installed according to the instructions found in the Maintenance and Troubleshooting Guide.

NIU and Feature Group Requirement

This section includes tables that list the feature groups that require specific NIUs for all hardware platforms.

Table 1: Acme Packet 4500 NIU and Feature Group Support Matrix

S-CZ7.3.5 supports the NIUs listed in the left column on the Acme Packet 4500. The matrix indicates the feature sets that require the supported NIUs.

NIU	IPSec	IMS-AKA	SRTP	QoS	Transcoding	MSRP B2BUA
Clear (RJ45)	X	X	X	X	X	X
Clear (SFP)	X	X	X	X	X	X
ETCv1	✓	✓	✓	✓	X	✓
ETCv2	✓	✓	✓	✓	X	✓
Encryption	✓	X	✓	X	X	X
QoS	X	X	X	✓	X	X
Encryption & QoS	X	X	X	✓	X	X
Transcoding	X	X	X	✓	✓	X

Table 2: Acme Packet 4600 NIU and Feature Group Support Matrix

S-CZ7.3.5 supports the NIUs listed in the left column on the Acme Packet 4600. The matrix indicates the feature sets that require the supported NIUs.

NIU	IPSec	IMS-AKA	SRTP	QoS	Transcoding	MSRP B2BUA
2x10Gig NIU	✓	✓	✓	✓	✓	✓

Table 3: Acme Packet 6100 NIU and Feature Group Support Matrix

S-CZ7.3.5 supports the NIUs listed in the left column on the Acme Packet 6100. The matrix indicates the feature sets that require the supported NIUs.

NIU	IPSec	IMS-AKA	SRTP	QoS	Transcoding	MSRP B2BUA
2x10Gig NIU	✓	✓	✓	✓	✗	✓
Transcode NIU	N/A	N/A	N/A	N/A	N/A	N/A

Table 4: AP6300 NIU and Feature Group Support Matrix

S-CZ7.3.5 supports the NIUs listed in the left column on the Acme Packet 6300. The matrix indicates the feature sets that require the supported NIUs.

NIU	IPSec	IMS-AKA	SRTP	QoS	Transcoding	MSRP B2BUA
2x10Gig NIU	✓	✓	✓	✓	✓ (required)	✓
Transcode NIU	✗	✗	✗	✗	✓	✗

Unsupported Hardware

- ETCv1 Cards with 4GB RAM. These NIUs can be identified by a revision lower than 2.09 (use **show prom-info phy** to query this NIU attribute).

Supported Upgrade Paths

The following upgrade paths are supported:

- S-CZ7.2.5 -> S-CZ7.3.5

These upgrades are transparent, consisting of backing up configuration and booting on new S-CZ7.3.5 software.

Co-Product Support

The products/features listed in this section run in concert with the Oracle USM for their respective solutions.

Oracle Communications Session Load Balancer

With an Oracle Communications Session Load Balancer running L-CX1.5.0 software, Oracle USM cluster members may run S-CZ7.3.5 on the following hardware:

- Acme Packet 4500
- Acme Packet 4600
- Acme Packet 6100

Introduction to S-CZ7.3.5

- Acme Packet 6300

Pooled Transcoding

The pooled transcoding feature requires an access function Oracle USM (P-CSCF) using transcoding resources provided by Oracle USMs with transcoding hardware (T-SBC). When the P-CSCF function is based on S-CZ7.3.5 software, the following hardware/software combinations may be used as a T-SBC in a pooled transcoding scenario:

- AP4500, Transcoding NIU, S-CX6.3.7M2+, S-CZ7.2.0+ or S-CZ7.3.0+
- AP6300, Transcoding NIU, S-CZ7.1.2+, S-CZ7.2.0+ or S-CZ7.3.0+

Oracle Communications Session Element Manager

Oracle Communications Session Element Manager versions 7.4M1 and later support this GA release of the Oracle USM.

QoS NIU Version Requirement for Acme Packet 4500

A Network Interface Unit (NIU) that supports the Quality of Service (QoS) feature group on the Acme Packet 4500, except the two Enhanced Traffic Control (ETC) cards, requires QoS Field Programmable Gate Array (FPGA) revision 2.22 or higher for the S-CZ7.3.5M1 release. The *Acme Packet 4500/3820 V2.22 QoS FPGA Upgrade 24369382* image is available at My Oracle Support, <https://support.oracle.com/>, with a customer account.

System Capacities

To query the current system capacities for the platform you are using, execute the **show platform limit** command. System capacities vary across the full range of platforms which support the Oracle USM.

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-CZ7.3.0 GA:

- S-CZ7.3.0p1

Access Control Endpoint Classification Capacity and DoS

The following capacities are for both IPv4 and IPv6 endpoints.

Platform	Denied	Trusted	Media	Untrusted	Dynamic Trusted	ARP	VLAN
AP4500	32000	8000	32000	2000	250000	4000	4000

Supported SPL Engines

The following SPL engine versions are supported by this software:

- 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

New Features in Service Provider Release S-CZ7.3.5

IMS Features

The features listed in this section are related to the Oracle USM suite of IMS features functionality. These features are often used within VoLTE deployments. Feature descriptions of the following items may be found in the ACLI Configuration Guide, IMS Chapter unless noted otherwise.

Diameter Message Manipulation

This version of the Oracle USM includes Diameter Manipulation capability, allowing the user to specify changes to Diameter messages upon ingress and/or egress.

Oracle Communications Operations Monitor (OCOM) Probe

This version of the Oracle USM includes the OCOM probe, allowing it to send traffic trace information to an OCOM mediation engine. This capability is documented in the Oracle USM Call Monitoring Guide.

TEL URI Replacement with SIP URI in R-URI to AS

When the Oracle USM receives a request containing a TEL URI from the Media Gateway Control Function (MGCF), it sends the TEL URI as an R-URI to the Application Server (AS) to perform services. However, in some implementations, the AS does not accept TEL URI and requires the trigger to be based on SIP URI. This feature, when enabled, causes the Oracle USM to replace the TEL R-URI with a SIP URI based on the first SIP user in the implicit set.

Determining Session Case and Served User for OOTB Calls Using the `odi` and `orig` Flags

The Oracle USM provides an alternative, configurable option that allows the user to specify the use of route header information to determine Served User and Session Case for out-of-the-blue (OOTB) calls. This method is 3GPP-compliant. By default, the Oracle USM uses information from the P-Served-User (PSU) header. The user configures this behavior by enabling the `ignore-psu-sesscase` option in the `ifc-profile`.

S-CSCF Selection Based on Capabilities

Within IMS environments, the I-CSCF identifies target S-CSCF's in response to SIP traffic for which the assigned S-CSCF is not known. Enhanced selection environments can include the HSS offering mandatory and optional capabilities for a user, and the I-CSCF selecting the best S-CSCF based on capabilities the S-CSCF is best suited to support (in addition to standard criteria). The user can configure the I-CSCF resident within Oracle CSM, Oracle USM and Oracle SLRM to support this capabilities-based S-CSCF selection. Resultant operation is compliant with ETSI TS 129 228 and ETSI TS 129 229.

Limiting AOR Contacts

The Oracle USM allows you to limit the number of contacts that apply to AORs. It also provides a configurable behavior allowing the system to either reject a new contact or overwrite an existing contact with the new one. The user specifies the maximum number of contacts and the operation mode on a per-registrar basis. Alternatively, the user can disable the feature. This feature is applicable to Cx and local database deployments.

Matching Request URIs for Service Point Triggers

The Oracle USM matches REQUEST URIs for iFC triggers in compliance with 3GPP TS 29.228 version 11.6.0 Release 11 by using Regex to extract the string for comparison. The user can revert to the previous method, which directly compares the REQUEST URI and service point trigger strings, by setting an option in the iFC profile.

Configurable Response to Timed-Out OPTIONS Messages

The Oracle USM allows the user to configure a function by which they can cause the system to send a 408 as a response to an OPTIONS message sent to an un-responsive, registered called party. In addition, this function allows the user to specify when to send that 408.

Handling Registration Termination Requests

In compliance with 3GPP specifications, the Oracle USM responds to a Registration Termination Request (RTR) by de-registering contacts associated with the IMPI presented in the RTR.

Handling Barred PUIDs

The Oracle USM supports PUID barring functionality per 3GPP specification TS 24.229. As such, the system does not service any request method other than REGISTERs for SIP or Tel-URI PUIDs designated as barred by the HSS. The Oracle USM also complies with the requirement that it allow Push Profile Requests (PPRs) to change a PUID from barred to non-barred (and vice versa) and issues a NOTIFY of the event to subscribers. No configuration is required.

Third Party Registration for an Implicit Registration Set

When using iFCs, the Oracle USM performs third party registrations based on the iFC downloaded for each PUID. By default, the Oracle USM performs third party registration for the service profiles of all PUID's in a user's implicit registration set. This is compliant with 3GPP specifications. The system includes any shared or default iFCs that apply to each PUID during this process. The system performs this function when it receives user-initiated de-registrations, but not when it receives RTRs. If desired, the user can configure the Oracle USM to perform third party registration for only the REGISTERED PUID in the registration using a **sip-registrar** option.

Registration Response with the Authentication-info Header

The Oracle USM can include the authentication-info header, as described in RFC 2617, in its 200 OK response to REGISTERs when using SIP digest. The user enables this functionality using a **sip-registrar** option.

Limiting REGISTER CDR Generation

The Oracle USM allows the user to generate RADIUS CDRs for REGISTER events via configuration. Large networks, however, can generate an inordinate volume of CDRs. So the Oracle USM also allows the user to reduce REGISTER CDR generation by filtering out some of the messages it sends.

Enhanced Orchestration

This version of the CSM adds additional KPIs that the AO can use for orchestration. These KPIs include signaling messages per second and per-thread CPU usage by SIP, Diameter, ENUM and ATCP processes. These KPIs are implemented using new SNMP MIBOIDS. Using these KPIs, AO is able to make better-informed decisions on the elasticity of CSM and SLRM instance deployments.

Inherited Features

Feature descriptions found in this chapter are inherited (forward merged) from Oracle USM and/or Oracle SBC releases:

- S-CZ7.3.0

These features were included in S-CZ7.3.0 GA docset.

System Features

The features listed in this section are related to the Oracle USM's internal systems functionality. These features are used for every day integration and maintenance within in your network. Locations of the features descriptions are noted.

IPv6 Trap Receiver Transport Support

This feature supports configuring trap receivers with IPv6 address notation, and allows traps to be sent to IPv6 targets.

This feature description is found in the ACLI Configuration Guide, System Configuration chapter.

Link Redundancy

Link redundancy enables the Oracle USM to run a pair of media interfaces redundantly so that in the event of a network or link failure, the Oracle USM automatically fails over to the redundant physical link. The Oracle USM polls link state on a one-second basis, so the maximum outage time is one second. And if gateway heartbeats are enabled, then gateway timeout alarms will also cause failovers.

This feature is only supported on the Acme Packet 3820 and 4500 on the following NIUs:

- 4-port 10/100/1000 copper
- 4-port 1Gig SFP
- 4-port 10/100/1000 copper

4-port 1Gig SFP phy card with QoS

This feature description is found in the ACLI Configuration Guide, Getting Started chapter.

Inherited Features

IPv6 NTP Server Support

The Oracle USM can be configured with IPv6 addresses of NTP servers. When multiple NTP servers are configured, they may be of mixed address family.

This feature description is found in the Maintenance and Troubleshooting Guide, System Management chapter.

Interface Description in MIB Enhancement

The *ifDescr* object in the *ifEntry* object in *ifTable* is a string of up to 255 characters. It currently contains the name of the interface only. This change adds to the *ifDescr* string, separated from the first part by a space, a keyword that represents the internal interface type. The values can be {ETH, FE, GE, OC, XE, null}.

This feature description is found in the MIB Guide.

TCP and SCTP State Connection Counters

Systemwide counts of TCP and SCTP states are available by using **show ip tcp** and **show ip sctp** commands respectively, from the ACLI.

SLB Client Support of IPsec traffic within L3 Tunnels

The Oracle USM, acting as a Subscriber-aware Load Balancer (SLB) client can exchange IPsec traffic within the L3 tunnels between itself and the SLB server.

This feature description is found in the Oracle Communications Session Load Balancer Essentials Guide.

Inherited Sec Features

The features listed in this section are related to the Oracle USM's suite of security features for both traffic transport and system hardening. Feature descriptions of the following items may be found in the Security chapter of the ACLI Configuration Guide, except where otherwise noted.

Remove All Default Passwords

The Oracle USM utilizes default or hard-coded passwords as shipped. These are predictable and pose a security risk if not changed promptly. Password setup must be completed through SSH or Console connections. Passwords need to be set when a particular privilege level is accessed and the system determines when the password is the default value.

This feature description is found in the ACLI Configuration Guide, Getting Started chapter.

TACACS+ Administrative Security

Oracle USMs use either the RADIUS (Remote Authentication Dial-In User Service) or the TACACS+ (Terminal Access Control Access Control System Plus) protocol for centralized access control administration; however, prior to this release, you could connect to the TACACS+ server only from the system's media interfaces. This feature implements TACACS+ authorization (user permissions management on a command basis), authentication (user management), and accounting on management interfaces.

This feature description is found in the ACLI Configuration Guide, Getting Started chapter.

TACACS+ Authorization Command and Arguments Boundary

Each TACACS+ authorization entry on an ACLI command line comprises the command and its arguments. Currently everything typed as a TACACS+ authorization command by an authenticated admin user, including the arguments, is sent to the TACACS+ server in the command field of the TACACS+ message; the argument field in the TACACS+ message contains no arguments and is set to "cmd-

arg=<CR>". This feature adds the new parameter **tacacs-authorization-arg-mode** to the **authentication** configuration element, which enables the TACACS+ authorization command and its arguments to be sent to the TACACS+ server separately.

This feature description is found in the ACLI Configuration Guide, Getting Started chapter.

SRTP Re-keying

Initialization of SRTP re-keying is supported by the Oracle USM.

This feature description is found in the ACLI Configuration Guide, Security chapter.

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).

This feature description is found in the ACLI Configuration Guide, Security chapter.

IMS Features

The features listed in this section are related to the Oracle USM suite of IMS features functionality. These features are often used within VoLTE deployments. Feature descriptions of the following items may be found in the ACLI Configuration Guide, IMS Chapter unless noted otherwise.

AAR Message Optimization

The Oracle USM, acting as a P-CSCF, already supports AAR message optimization (the suppression of unnecessary AARs). This feature reduces the number of AAR transactions to the minimum to assure that the end-to-end session set-up and dedicated bearer creation works seamlessly. For more information, see the ACLI Configuration Guide, External Policy Servers Chapter.

Signaling Application and Monitoring Features

The features listed in this section are related to the Oracle USM's VoIP application functions. New functionality listed in this section may include protocol features, application-oriented network entity features, and application monitoring features. Locations of the features descriptions within the Oracle USM documentation set are noted.

SIP Recursion Policy

Session Agents (and Session agent groups) can utilize a SIP Recursion policy to customize the Oracle USM behavior when recursing through a list of target SIP peers. These policies are useful for networks with large numbers of SIP peers that wish to customize recursive routing behavior for individual session agents or session agent groups, based on number of recursion attempts or the returned SIP response code.

This feature description is found in the ACLI Configuration Guide, Routing with Local Policy chapter.

Timer to Tear Down Long Duration Calls

The Oracle USM currently provides the "flow-time-limit" timer to terminate long duration calls. However, this timer is reset whenever the Oracle USM receives a Re-INVITE or UPDATE message, even when it is provided for the session timer. This feature adds a non-resettable timer that, when enabled and upon expiration, tears down long duration calls.

This feature description is found in the ACLI Configuration Guide, System Configuration chapter.

Mapping of Diversion Information Between Diversion and History-Info Headers

History-Info and Diversion are the two headers in SIP signaling used to convey information related to call transfer and call diversion. Although both provide call diversion information, they have different syntaxes, the main difference being that the chronology of events is reversed between the two headers. To date, Oracle USMs have provided mapping and interworking of the History-Info and Diversion headers through the use of an SPL plug-in. This feature implements this interworking functionality within the software by adding a new parameter to the **sip-interface** configuration element.

This feature description is found in the ACLI Configuration Guide, SIP Signaling chapter.

DNS SRV Session Agent Recursion Error Handling

When a session request is sent from the Oracle USM to a session agent, and an error response is received (or a transport failure occurs), the Oracle USM attempts to reroute the message through the list of dynamically resolved IP addresses. The SBC can be configured to resend session requests through the list of IP addresses under more failure conditions.

This feature description is found in the ACLI Configuration Guide, Routing with Local Policy chapter.

Multipart Message Body Encoding Support

SIP messages and responses may arrive at the Oracle USM 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 USM 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 USM to accept, process and forward messages containing these encoded parts. This configuration causes the Oracle USM 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.

This feature description is found in the ACLI Configuration Guide, SIP Signaling chapter.

Configurable DNS Response Size

When a realm is used for DNS queries, the Oracle USM can accept UDP DNS responses configurable up to 65535 bytes.

This feature description is found in the ACLI Configuration Guide, Routing with Local Policy chapter.

LMSD Offerless INVITE Handling

To enhance LMSD interworking, the Oracle USM does not remove SDP from a 180 response sent back to the UAC when the initial request did not contain SDP. The Oracle USM also forwards UAS-side UPDATE requests to the UAC; it does not respond locally. These represent behavioral changes and require no configuration.

This feature description is found in the ACLI Configuration Guide, SIP Signaling chapter.

DSCP Marking for MSRP and Media over TCP

The Oracle USM 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.

This feature description is found in the ACLI Configuration Guide, Realms chapter.

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.

This feature description is found in the ACLI Configuration Guide, SIP Signaling chapter.

TSCF Features

The features in this section are related to Tunneled Services Control Function or TSCF support. Feature descriptions of the following items may be found in the Tunneled Services Control Function chapter in the ACLI Configuration Guide.

This release of the Oracle USM includes the Tunneled Services Control Function (TSCF) feature set, also called Tunnel Session Management (TSM). This technology improves firewall traversal for over-the-top (OTT) Voice-over-IP (VoIP) applications, and reduces the dependency on SIP/TLS and SRTP by encrypting access-side VoIP within standardized Virtual Private Network (VPN) tunnels. As calls or sessions traverse a TSM tunnel, the TSCF forwards all SIP and RTP traffic from within the TSM tunnel to appropriate servers or gateways within the secure network core. Operating in a TSM topology, the Oracle USM provides exceptional tunnel performance and capacity, as well as optional high availability (HA), DoS protection and tunnel redundancy that improves audio quality in lossy networks.

Refer to the ACLI Configuration Guide's Tunneled Service Control Function chapter for a detailed explanation of the licensing requirement for TSCF.

Prior to this release, the TSCF feature set was available as the Oracle Communications Tunneled Session Controller. That functionality is now available as an Oracle USM feature on the Acme Packet 4600 and Acme Packet 6000 series platforms.

Inherited Transcoding Features

The features listed in this section are related to the Oracle USM's suite of Transcoding and DTMF Interworking functions. Feature descriptions of the following items may be found in the Transcoding and DTMF Transfer sections of the ACLI Configuration Guide, except where otherwise noted.

Opus Codec Transcoding Support

Opus is an audio codec developed by the IETF that supports constant and variable bitrate encoding from 6 kbit/s to 510 kbit/s and sampling rates from 8 kHz (with 4 kHz bandwidth) to 48 kHz (with 20 kHz bandwidth, where the entire hearing range of the human auditory system can be reproduced). It incorporates technology from both Skype's speech-oriented SILK codec and Xiph.Org's low-latency CELT codec. This feature adds the Opus codec as well as support for transrating, transcoding, and pooled transcoding to the 4600 and 6300 platforms.

SILK Codec Transcoding Support

SILK is an audio codec developed by Skype Limited that supports bit rates from 6 kbit/s to 40 kbit/s and sampling rates of 8, 12, 16, or 24 kHz. It can also use a low algorithmic delay of 25 ms (20 ms frame size + 5 ms look-ahead). This feature adds the SILK codec as well as support for transrating, transcoding, and pooled transcoding to the 4600 and 6300 platforms.

T.140 to Baudot Relay

The T.140 to Baudot Relay feature uses the Oracle USM's transcoding resources to relay T.140 text messages to Baudot tones and vice versa. The T.140 Protocol is used for multimedia text conversation over IP and is designed as a replacement for TDD devices. Baudot tones are a common protocol in the US in Telecommunications Device for the Deaf (TDD). Details of the protocol implementation are available in TIA/EIA-825-A. The T.140-Baudot relay is a regulatory requirement, and is specified for both emergency

Inherited Features

and non-emergency traffic. This feature is only available on Acme Packet 4600 and 6300 with transcoding hardware.

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 USM 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. This feature is not available on the Acme Packet 3820 or Acme Packet 4500 platforms.

This feature description is found in the ACLI Configuration Guide, Transcoding and RCS Services chapter.

Interface Changes

This chapter summarizes ACLI, SNMP, and RADIUS changes (where applicable) for S-CZ7.3.5. Additions, removals, and changes appearing in this chapter are since the release of S-CZ7.2.5M4.

ACLI Command Changes

This section summarizes the ACLI command changes that first appear in release Version S-CZ7.3.5 of the Oracle USM.

Command	Description
<code>show sipd codecs</code>	Adds counts for newly supported SILK and opus codecs
<code>clear-cache registration sip</code>	Enhances command to restart the registration process for all address of record for surrogate agents to support the SIP Surrogate Agent Registration Re-initialization feature
<code>show ip tcp ; show ip sctp</code>	Adds options to display systemwide counts for TCP and SCTP State Connection Counters

ACLI Configuration Element Changes

This section summarizes the ACLI configuration element changes that first appear in release Version S-CZ7.3.5.

SIP Interface Features

New Parameter	Description
<code>session-router > sip-interface > redirect-action</code>	The default value for this parameter is changed to recurse-305-only.

Interface Changes

Session Router Features

New Parameters	Description
<code>session-router > server-capabilities-table</code>	Allows the user to name a servers-capability object, and configure it with servers and their capabilities.

SIP Registrar Features

New Parameters	Description
<code>sip-registrar > server-capabilities-list</code>	Allows you to configure the registrar with a servers-capabilities-table.
<code>sip-registrar > max-contacts-per-aor-mode</code>	Qualifies the operation of max-contacts-per-aor to overwrite or reject new contacts when the aor reaches its maximum.

System Features

New Parameter	Description
<code>ntp-sync > add-server</code>	Accepts IPv6 addresses for configured NTP time servers for IPv6 NTP Server Support feature.
<code>system > trap-receiver > ip-address</code>	Accepts IPv6 addresses for configured trap receiver for IPv6 Trap Receiver Transport Support feature.
<code>session-router > sip-config > retry-after-upon-offline</code>	Adds parameter to support load balancing restart for when Oracle USM is configured as a cluster member in conjunction with the Oracle Communications Session-aware Load Balancer.

Signaling Features

New Parameters	Description
<code>media-manager > realm-config > session-max-life-limit</code>	Adds parameter to set maximum interval before the system terminates long-duration calls for the Timer to Tear Down Long Duration Calls feature.
<code>session-router > sip-interface > diversion-info-mapping-mode</code>	Adds mode to enable the Mapping of Diversion Information Between Diversion and History-Info Headers

New Configuration Elements	New Parameters and Description
<code>session-router > sip-recursion-policy</code>	Adds the following parameters to terminate recursion on received responses to support the SIP Recursion Policy: <ul style="list-style-type: none">• name• description• global-count• mode• sip-response-code

New Configuration Elements	New Parameters and Description
<code>session-router > sip-recursion-policy > sip-response-code</code>	<p>Adds the following parameters for refined SIP Recursion Policy configuration:</p> <ul style="list-style-type: none"> • response-code • attempts

Security Features

New Parameters	Description
<code>security > authentication > tacacs-authorization-arg-mode</code>	Adds tacacs-authorization-arg-mode parameter for enabling TACACS+ Authorization Command and Arguments Boundary feature.
<code>media-manager > realm-config > dns-max-response-size</code>	Adds parameter to set maximum size of DNS response to queries for Configurable DNS Response Size
<code>security > media-security > sdes-profile > srtp-rekey-on-reinvite</code>	Adds parameter to enable re-key upon the receipt of a SIP reINVITE that contains SDP for the SRTP Re-keying.

Transcoding Features

New Parameters	Description
<code>media-manager > codec-policy > allow-codecs</code>	Parameter now allows text:no value which strips "m=text" occurrence in the outbound INVITE and enables T.140 to Baudot transcoding.
<code>session router > media profile > name</code>	Adds SILK and OPUS values

TSCF Features

TSCF Functionality includes a new top level menu, **tscf**, that appears within the security path.

New Configuration Elements	New Parameters and Description
<code>security > tscf > tscf-address-pool</code>	<p>This configuration element defines local address pools for the TSCF application. Supported parameters are:</p> <ul style="list-style-type: none"> • name • address-range • dns-realm-id • data-flow • protocol-policy
<code>security > tscf > tscf-address-pool > address-range</code>	<p>This configuration element defines the address ranges for the TSCF application. The following parameters are supported:</p> <ul style="list-style-type: none"> • network-address • subnet-mask

Interface Changes

New Configuration Elements	New Parameters and Description
security > tscf > tscf-config	Global parameters for tunneled services control function. Supported parameters are: <ul style="list-style-type: none"> • keepalive-timer • keepalive-timer-datagram • tunnel-persistence-time • red-port • red-max-trans • red-sync-start-time • red-sync-comp-time • element-id
security > tscf > tscf-data-flow	Configures the data flow name for managing data traffic within an address pool. The following parameters are supported: <ul style="list-style-type: none"> • name • realm-id • group-size • upstream-rate • downstream-rate
security > tscf > tscf-interface	Used to configure interfaces for the TSCF application. The following parameters are supported: <ul style="list-style-type: none"> • state • realm-id • max-tunnels • local-address-pools • nagle-state • assigned-services • tscf-ports
security > tscf > tscf-interface > tscf-port	Used to configure TSCF ports on TSCF interfaces. Supported parameters are: <ul style="list-style-type: none"> • address • port • transport-protocol • tls-profile
security > tscf > tscf-protocol-policy	Configures the protocol policy to enable policy-based forwarding. The following parameters are supported: <ul style="list-style-type: none"> • name • ip-address • port • transport-type • realm-id • remote-ip-address

Media Features

New Parameters	Description
media-manager > realm-config > dns-max-response-size	Adds parameter to set maximum size of DNS response to queries for Configurable DNS Response Size

SNMP/MIB Changes

This section summarizes the Application SNMP/MIB changes that appear in the Oracle USM version S-CZ7.3.5.

ap-codec.mib

Object Name/OID	Description
apCodecRealmCountOpus 1.3.6.1.4.1.9148.3.7.1.1.1.25	The count of SDP media streams received in the realm which negotiated to the Opus codec.
apCodecRealmCountSILK 1.3.6.1.4.1.9148.3.7.1.1.1.26	The count of SDP media streams received in the realm which negotiated to the SILK codec.
apCodecRealmCountT140 1.3.6.1.4.1.9148.3.7.1.1.1.27	The count of SDP media streams received in the realm which negotiated to the T140 codec.
apCodecRealmCountBAUDOT 1.3.6.1.4.1.9148.3.7.1.1.1.28	The count of SDP media streams received in the realm which negotiated to the BAUDOT codec.
apCodecRealmCountH264 1.3.6.1.4.1.9148.3.7.1.1.1.29	The count of SDP media streams received in the realm which negotiated to the H264 codec .
apCodecRealmStatsObjectsGroup5 1.3.6.1.4.1.9148.3.7.5.2.7	A collection of objects providing additional realm codec statistics, including Opus and SILK.
apCodecRealmStatsObjectsGroup6 1.3.6.1.4.1.9148.3.7.5.2.8	A collection of objects providing additional realm codec statistics, including T.140.
apCodecRealmStatsObjectsGroup7 1.3.6.1.4.1.9148.3.7.5.2.9	A collection of objects providing additional realm codec statistics, including BAUDOT.
apCodecRealmStatsObjectsGroup8 1.3.6.1.4.1.9148.3.7.5.2.10	A collection of objects providing additional realm codec statistics, including H.264.

Interface Changes

ap-smgmt.mib

Table 5: New MIB Objects

Object Name/OID	Description
apSysCPULoadAvgOneMinute 1.3.6.1.4.1.9148.3.2.1.1.43	The percentage of CPU Load across all cores measured over 1 minute.
apSysCPULoadAvgFiveMinute 1.3.6.1.4.1.9148.3.2.1.1.44	The percentage of CPU Load across all cores measured over 5 minutes.
apSysCPULoadAvgFiftnMinute 1.3.6.1.4.1.9148.3.2.1.1.45	The percentage of CPU Load across all cores measured over 15 minutes.
apSysXCodeOpusCapacity 1.3.6.1.4.1.9148.3.2.1.1.46	The percentage of licensed Opus transcoding utilization (non pollable).
apSysXCodeSILKCapacity 1.3.6.1.4.1.9148.3.2.1.1.47	The percentage of licensed SILK transcoding utilization (non pollable).
apSysMgmtCPULoadAvgGroup 1.3.6.1.4.1.9148.3.2.4.2.31	Object to monitor CPU Load Average across all CPU cores for 1, 5, and 15 minutes.
apSysMgmtXCodeOpusUtilGroup 1.3.6.1.4.1.9148.3.2.4.2.32	Object to monitor licensed Opus transcoding utilization .
apSysMgmtXCodeSILKUtilGroup 1.3.6.1.4.1.9148.3.2.4.2.33	Object to monitor licensed SILK transcoding utilization.

Table 6: New Traps

Trap Name (clear trap)	Description
apSysMgmtCPULoadAvgTrap (apSysMgmtCPULoadAvgClearTrap)	The trap will be generated when CPU Load Average Alarm exceeds its minor alarm threshold. The clear trap will be sent when the CPU load average recedes to the minor alarm level.

capability MIBs


Table 7: New Capability MIBs

Object Name/OID	MIB file
apSmgmtCPULoadAvgCap 1.3.6.1.4.1.9148.2.1.8.55	ap-smgmt.mib
apSmgmtXCodeOpusUtilCap 1.3.6.1.4.1.9148.2.1.8.56	ap-smgmt.mib
apSmgmtXCodeSILKUtilCap	ap-smgmt.mib

Object Name/OID	MIB file
1.3.6.1.4.1.9148.2.1.8.57	
apCodecRealmCodecCap5 1.3.6.1.4.1.9148.2.1.13.7	ap-codec.mib
apCodecRealmCodecCap6 1.3.6.1.4.1.9148.2.1.13.8	ap-codec.mib
apCodecRealmCodecCap7 1.3.6.1.4.1.9148.2.1.13.9	ap-codec.mib
apCodecRealmCodecCap8 1.3.6.1.4.1.9148.2.1.13.10	ap-codec.mib

MIB Changes

apSipRecNotificationGroup (1.3.6.1.4.1.9148.3.15.3.2.4) has changed to apSipRecNotificationsGroup (1.3.6.1.4.1.9148.3.15.3.2.4).

 **Note:** An "s" has been added to the end of "Notifications" in the MIB Object name.

Other Traps

When either Opus or SILK session utilization exceeds 90%, an apSysMgmtGroupTrap is sent that includes the non-pollable apSysXCodeOPUSCapacity or apSysXCodeSILKWBCapacity OIDs, respectively. When utilization falls below 85%, the apSysMgmtGroupClearTrap is sent.

Unsupported MIBs

The following MIB objects are new this release, but are not supported for this product.

- apSecurityDhcpInterfaceCap 1.3.6.1.4.1.9148.2.1.14.14
- apUsbcSysDPDKMibCapabilities 1.3.6.1.4.1.9148.2.1.25
- apUsbcSysDPDKCap 1.3.6.1.4.1.9148.2.1.25.1
- apUsbcSysScalingMibCapabilities 1.3.6.1.4.1.9148.2.1.26
- apUsbcSysScalingCap 1.3.6.1.4.1.9148.2.1.26.1
- apNNCTrapRelayNotAliveNotification 1.3.6.1.4.1.9148.3.8.5.3.1.0.3
- apNNCTrapRelayAliveNotification 1.3.6.1.4.1.9148.3.8.5.3.1.0.4
- apSecurityDhcpInterfaceStatsTable 1.3.6.1.4.1.9148.3.9.1.11
- apSecurityDhcpInterfaceStatsEntry 1.3.6.1.4.1.9148.3.9.1.11.1
- apSecurityDhcpInterfaceType 1.3.6.1.4.1.9148.3.9.1.11.1.1
- apSecurityDhcpInterfaceAddress 1.3.6.1.4.1.9148.3.9.1.11.1.2
- apSecurityDhcpInterfaceDisRcvd 1.3.6.1.4.1.9148.3.9.1.11.1.3
- apSecurityDhcpInterfaceOfferSent 1.3.6.1.4.1.9148.3.9.1.11.1.4
- apSecurityDhcpInterfaceReqRcvd 1.3.6.1.4.1.9148.3.9.1.11.1.5
- apSecurityDhcpInterfaceAckSent 1.3.6.1.4.1.9148.3.9.1.11.1.6
- apSecurityDhcpInterfaceNAckSent 1.3.6.1.4.1.9148.3.9.1.11.1.7
- apSecurityDhcpInterfaceFailures 1.3.6.1.4.1.9148.3.9.1.11.1.8
- apSecurityDhcpInterfaceRelRcvd 1.3.6.1.4.1.9148.3.9.1.11.1.9
- apSecurityDhcpInterfaceOfferTimeouts 1.3.6.1.4.1.9148.3.9.1.11.1.10
- apSecurityDhcpInterfaceLeaseTimeouts 1.3.6.1.4.1.9148.3.9.1.11.1.11

Interface Changes

- apSecurityDhcpInterfaceCurrentSessions 1.3.6.1.4.1.9148.3.9.1.11.1.12
- apSecurityDhcpInterfaceMaxSessions 1.3.6.1.4.1.9148.3.9.1.11.1.13
- apSecurityDhcpInterfaceTotalSessions 1.3.6.1.4.1.9148.3.9.1.11.1.14
- apUsbcSysScalingObjects 1.3.6.1.4.1.9148.3.17.1.1.12
- apUsbcSysEstSessions 1.3.6.1.4.1.9148.3.17.1.1.12.1
- apUsbcSysEstG711G729Trans 1.3.6.1.4.1.9148.3.17.1.1.12.2
- apUsbcSysEstSigTPS 1.3.6.1.4.1.9148.3.17.1.1.12.3
- apUsbcSysEstACLs 1.3.6.1.4.1.9148.3.17.1.1.12.4
- apUsbcSysEstTCP 1.3.6.1.4.1.9148.3.17.1.1.12.5
- apUsbcSysEstTL 1.3.6.1.4.1.9148.3.17.1.1.12.6
- apUsbcSysEstVLANs 1.3.6.1.4.1.9148.3.17.1.1.12.7
- apUsbcSysDPDKObjects 1.3.6.1.4.1.9148.3.17.1.1.13
- apUsbcSysDPDKFwdPurpose 1.3.6.1.4.1.9148.3.17.1.1.13.1
- apUsbcSysDPDKDOSPurpose 1.3.6.1.4.1.9148.3.17.1.1.13.2
- apUsbcSysDPDKSigPurpose 1.3.6.1.4.1.9148.3.17.1.1.13.3
- apUsbcSysDPDKTransPurpose 1.3.6.1.4.1.9148.3.17.1.1.13.4
- apUsbcSysDPDKCmdLine 1.3.6.1.4.1.9148.3.17.1.1.13.5
- apUsbcSysDPDKFileMem 1.3.6.1.4.1.9148.3.17.1.1.13.6
- apUsbcSysDPDKSysMem 1.3.6.1.4.1.9148.3.17.1.1.13.7
- apUsbcSysDPDKNum1G 1.3.6.1.4.1.9148.3.17.1.1.13.8
- apUsbcSysDPDKNum2MB 1.3.6.1.4.1.9148.3.17.1.1.13.9
- apUsbcSysDPDKHypervisorType 1.3.6.1.4.1.9148.3.17.1.1.13.10
- apUsbcSysDPDKAddFwdCores 1.3.6.1.4.1.9148.3.17.1.1.13.11
- apUsbcSysDPDKAddSigCores 1.3.6.1.4.1.9148.3.17.1.1.13.12
- apUsbcSysDPDKAddTransCores 1.3.6.1.4.1.9148.3.17.1.1.13.13
- apUsbcSysScalingGroup 1.3.6.1.4.1.9148.3.17.3.1.3
- apUsbcSysDPDKGroup 1.3.6.1.4.1.9148.3.17.3.1.4
- apUsbcSysThreadObjects 1.3.6.1.4.1.9148.3.17.1.2
- apUsbcThreadUsageTableObject 1.3.6.1.4.1.9148.3.17.1.2.1
- apUsbcThreadUsageTable 1.3.6.1.4.1.9148.3.17.1.2.1.1
- apThreadUsageEntry 1.3.6.1.4.1.9148.3.17.1.2.1.1.1
- apThreadId 1.3.6.1.4.1.9148.3.17.1.2.1.1.1.1
- apThreadName 1.3.6.1.4.1.9148.3.17.1.2.1.1.1.2
- apThreadCurrentUsage 1.3.6.1.4.1.9148.3.17.1.2.1.1.1.3
- apThreadOverloaded 1.3.6.1.4.1.9148.3.17.1.2.1.1.1.4
- apUsbcThreadEventTableObject 1.3.6.1.4.1.9148.3.17.1.2.2
- apUsbcThreadEventTable 1.3.6.1.4.1.9148.3.17.1.2.2.1
- apThreadEventEntry 1.3.6.1.4.1.9148.3.17.1.2.2.1.1
- apThreadEventPendingCurrent 1.3.6.1.4.1.9148.3.17.1.2.2.1.1.1
- apThreadEventPendingCurhigh 1.3.6.1.4.1.9148.3.17.1.2.2.1.1.2
- apThreadEventPendingWindow 1.3.6.1.4.1.9148.3.17.1.2.2.1.1.3
- apThreadEventPendingTotal 1.3.6.1.4.1.9148.3.17.1.2.2.1.1.4
- apThreadEventPendingMaximum 1.3.6.1.4.1.9148.3.17.1.2.2.1.1.5
- apThreadEventPendingHigh 1.3.6.1.4.1.9148.3.17.1.2.2.1.1.6
- apThreadEventDroppedCurrent 1.3.6.1.4.1.9148.3.17.1.2.2.1.1.7
- apThreadEventDroppedCurhigh 1.3.6.1.4.1.9148.3.17.1.2.2.1.1.8
- apThreadEventDroppedWindow 1.3.6.1.4.1.9148.3.17.1.2.2.1.1.9
- apThreadEventDroppedTotal 1.3.6.1.4.1.9148.3.17.1.2.2.1.1.10
- apThreadEventDroppedMaximum 1.3.6.1.4.1.9148.3.17.1.2.2.1.1.11
- apThreadEventDroppedHigh 1.3.6.1.4.1.9148.3.17.1.2.2.1.1.12

- apThreadLatencyPendingAverage 1.3.6.1.4.1.9148.3.17.1.2.2.1.1.13
- apThreadLatencyPendingMax 1.3.6.1.4.1.9148.3.17.1.2.2.1.1.14
- apThreadLatencyProcessingAverage 1.3.6.1.4.1.9148.3.17.1.2.2.1.1.15
- apThreadLatencyProcessingMax 1.3.6.1.4.1.9148.3.17.1.2.2.1.1.16
- apUsbcSipObjects 1.3.6.1.4.1.9148.3.17.1.2.3
- apSipNumberOfThreads 1.3.6.1.4.1.9148.3.17.1.2.3.1
- apSipAverageCpuUtil 1.3.6.1.4.1.9148.3.17.1.2.3.2
- apSipPendingAverageLatency 1.3.6.1.4.1.9148.3.17.1.2.3.3
- apSipPendingMaxLatency 1.3.6.1.4.1.9148.3.17.1.2.3.4
- apSipProcessingAverageLatency 1.3.6.1.4.1.9148.3.17.1.2.3.5
- apSipProcessingMaxLatency 1.3.6.1.4.1.9148.3.17.1.2.3.6
- apUsbcAtcpObjects 1.3.6.1.4.1.9148.3.17.1.2.4
- apAtcpNumberOfThreads 1.3.6.1.4.1.9148.3.17.1.2.4.1
- apAtcpAverageCpuUtil 1.3.6.1.4.1.9148.3.17.1.2.4.2
- apAtcpPendingAverageLatency 1.3.6.1.4.1.9148.3.17.1.2.4.3
- apAtcpPendingMaxLatency 1.3.6.1.4.1.9148.3.17.1.2.4.4
- apAtcpProcessingAverageLatency 1.3.6.1.4.1.9148.3.17.1.2.4.5
- apAtcpProcessingMaxLatency 1.3.6.1.4.1.9148.3.17.1.2.4.6
- apUsbcMbcdObjects 1.3.6.1.4.1.9148.3.17.1.2.5
- apMbcdNumberOfThreads 1.3.6.1.4.1.9148.3.17.1.2.5.1
- apMbcdAverageCpuUtil 1.3.6.1.4.1.9148.3.17.1.2.5.2
- apUsbcEbmdObjects 1.3.6.1.4.1.9148.3.17.1.2.6
- apEbmdNumberOfThreads 1.3.6.1.4.1.9148.3.17.1.2.6.1
- apEbmdAverageCpuUtil 1.3.6.1.4.1.9148.3.17.1.2.6.2
- apUsbcDnsObjects 1.3.6.1.4.1.9148.3.17.1.2.7
- apDnsNumberOfThreads 1.3.6.1.4.1.9148.3.17.1.2.7.1
- apDnsAverageCpuUtil 1.3.6.1.4.1.9148.3.17.1.2.7.2

Caveats, Known Issues, and Behavioral Changes

Issues Resolved and Known Issues in this Release

Known Issues in this Release

This section lists known issues in version S-Cz7.3.5 of the Oracle USM.

- Oracle has observed occasional reboots during automated regression testing of the S-Cz7.3.5m1 version of the Oracle USM when the **save-config** and **activate-config** commands are issued. Configuration changes are stored on the system, allowing the user to simply re-issue **save-config** and **activate-config** after the reboot. Oracle has not observed this behavior when issuing **save-config** and **activate-config** manually.
- Configuring support for SNMPv3 is not supported as a real-time configuration change. Reboot the system after establishing an SNMPv3 configuration on the Oracle USM.
- The ISC interface does not work when dialog transparency is enabled on the Oracle USM.
 - Resolution - Do not enable dialog transparency if your Oracle USM must support ISC.
- The Oracle USM does not work with an iFC when its default handling is set to "SESSION CONTINUED".



Note: This issue was resolved in SCZ-7.3.5M2.

- The Oracle USM accepts only the first message received from an application server in response to messages from the Oracle USM that included an ODI. The Oracle USM drops any subsequent messages with the same ODI.
 - Resolution - Do not configure an AS to fork responses to the Oracle USM that include an ODI originally provided by the Oracle USM.
- Instead of routing a message via local policy, the Oracle USM incorrectly issues an LIR when the following two conditions exist simultaneously:
 - The Oracle USM is not configured with the e164-primary-config and e164-secondary-config options, and
 - The Oracle USM receives a request with a tel-URI or a sip-URI with the user=phone parameter.

Caveats, Known Issues, and Behavioral Changes

Note that the Oracle USM sends the request via local-policy if the LIA for a tel-URI or sip-URI with user=phone returns 5001 DIAMETER_ERROR_USER_UNKNOWN. For all other errors in the LIA, the Oracle USM returns an error.

- With this release, the **sip-registrar** element's **home-server-route** parameter is not supported for real time configuration. The user must reboot the Oracle USM to have a changed **home-server-route** setting take effect.

IPSec

When the security-association configuration element is configured as an IPv6 SA, it is not RTC enabled.

The **transport-protocols** parameter in **security-policy** configuration element is set to the default of all, regardless of configuration.

IMS AKA

Inbound and outbound SA counts can lose synchronization when an IMS-AKA protected port pool is enabled.

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

SIP over TCP

No more than 500 SIP Interfaces with SIP over TCP are supported.

Redundancy Configuration

Do not use the 169.254.16.x or 169.254.21.x networks in the redundancy-config of the Oracle SBC (including the network-interface configuration for the wancom1 and wancom2 interfaces) when installed on an Acme Packet platform that includes a transcoding card. The system uses these networks to provide software to transcoding DSPs. When the user configures the redundancy configuration with these networks, the system fails to route this software properly.

Workaround: Choose any available network for redundancy other than 169.254.16.x or 169.254.21.x. Note that user documentation describes redundancy configuration using the 169.254.1.x/16 network, which works properly with transcoding cards.

MSC Support

In the case of a hand-over INVITE from a mobile switching center (MSC) while in the alerting phase (180 ringing), the OCUSM may respond incorrectly with a 480 temporarily unavailable message.

Accounting

The OCUSM may incorrectly include the AF-Charging ID in AAR messages when it has an accounting-config enabled, and that config has the prevent-duplicate-attrs and cdr-output-inclusive enabled. Under these conditions, the USM may change the charging ID in the subsequent AVP. This would result in the PCRF rejecting the AAR.

Workaround: To work around this issue, create and apply the following diameter manipulation rule to the applicable outbound interface.

```
Oracle#(diameter-manipulation) # show
diameter-manipulation
  name          workaround
  description
  diameter-manip-rule
    name        delChargingAvp
    avp-code    505
```

descr-avp-code	AF-charging-id
avp-type	octet-string
action	delete
msg-type	request
msg-cmd-code	265
comparison-type	case-sensitive
match-value	
new-value	

Caveats

This section list caveats related to Version S-Cz7.3.5 of the Oracle USM.

- Do not load configurations from sibling products, the Oracle SBC for example, on the Oracle USM. Those configurations are incompatible with the Oracle USM, causing incorrect operation. Users should configure the Oracle USM from scratch or use another valid Oracle USM configuration.
- Multi-stage routing does not work for S-CSCF routing functions.

Interface Utilization Support

The Interface Utilization: Graceful Call Control, Monitoring, and Fault Management feature is unsupported for this release.

HMR action on Call-ID

HMR operations on the Call-ID: header are deprecated.

FTP Support

The Oracle USM's FTP Server is deprecated. Only SFTP server services are supported.

FTP Client access for features such as HDR/CDR push remains.

Fragmented Ping Support

The Oracle USM does not respond to inbound fragmented ping packets.

Physical Interface RTC Support

After changing any Physical Interface configuration, a system reboot is required.

Packet Trace

Output from the packet trace local feature on hardware platforms running this software version may display invalid MAC addresses for signaling packets.

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.

SRTP Caveats

For hold and resume SRTP calls, if the rollover counter increments, upon a subsequent hold and resume action without an SRTP rekey or SSRC change an SRTP rekey, the media portion of the call will be lost. This Caveat only applies to systems running Encryption or QoS & Encryption NIUs.

Source-based Routing

The source routing feature as configured by system-config --> source-routing is deprecated. Please review the HIP information in the Network Interface section in the System Configuration chapter of the ACLI Configuration guide for background of accessing SBC Administrative Applications over media Interfaces.

Session Replication for Recording

Session Replication for Recording is not supported in this release.

Although the CRS Session Replication for Recording (SRS) functionality is removed from the Oracle USM, the configuration element and parameters are still configurable from the ACLI. The user must not configure CRS in this version of the Oracle USM.

Note that, if SRS is set up in configurations from version 6 software, importing those configurations sets SRS. The user must remove the SRS portion of these configurations prior to upgrade.

Symptoms of SRS configuration in this software includes failed ACL creation.

Behavioral Changes

The following behavioral changes from the previous GA release appear in this release. These changes reflect new behaviors that occur without any user intervention.

SFTP Security Behavior

The user-level account now has read-only access on the filesystem for all platforms. In order to SFTP files onto an Oracle Communications Session Border Controller's filesystem, you must log in with a superuser-level (admin) account. This behavior only existed on certain platforms in the S-CZ7.2.0 GA release.

Default Password Removal

Upon starting the system, if default passwords exist, the user will be required to change them.

Minimum Advertised SSL/TLS Version

The default acceptable SSL/TLS version for clients connecting to the Oracle USM is TLS1.0. Prior to this release, SSLv3 was accepted. The legacy behavior may be enabled by configuration. More information is found in the ACLI Configuration Guide's Security chapter, Transport Layer Security section.

TLS1.2 Preferred Cyphers

When using TLS1.2, the advertised cypher suites order has changed to prioritize AES_GCM ciphers. The new order is:

```
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
TLS_DHE_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_AES_256_GCM_SHA384
TLS_RSA_WITH_AES_256_CBC_SHA256
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
TLS_DHE_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_128_GCM_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA256
TLS_RSA_WITH_AES_128_CBC_SHA
```

TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
TLS_DHE_RSA_WITH_DES_CBC_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_RSA_WITH_DES_CBC_SHA
TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA
TLS_RSA_WITH_NULL_SHA256
TLS_RSA_WITH_NULL_SHA
TLS_RSA_WITH_NULL_MD5

media-profile subtype Configuration Restrictions

media-profiles are subject to stringent configuration restrictions. You must avoid creating a **media-profile** with configured **subtype** parameter that does not substantively differ (in all additional parameters) from the default (unconfigured) media profile. An example of an invalid configuration is **media-profile > name** of g729, and a **media-profile > subtype** of g729, with no additional parameter configurations other than the default values. Such configuration can cause unexpected behaviors and must be avoided.

Deregistration of a Contact Based on IMPI

Here are the behavior changes introduced to the RTR functionality in 7.2.5m3:

- The default behavior of the Oracle USM has been changed to restrict the contacts de-registered via the RTR to those associated with the IMPIs presented in the AVPs of the RTR request. In previous versions, the Oracle USM removes all the contacts of the IMPUs. The user can revert to the previous behavior by enabling a configuration option in the sip-registrar, as described in detail in the "Handling of Registration Termination Request" in this document.
- The default behavior of the Oracle USM has been changed to do two validations on the AVPs of the RTR request before processing it. Note that there is no configuration option to revert to previous behavior:
 - If the IMPI presented in the User-Name AVP of the RTR is not present in its local cache, the Oracle USM returns Diameter error USER UNKNOW (5001) in the RTA. However, in the previous versions, even if the IMPI presented in the User-Name AVP of the RTR is not present in its local cache, the Oracle USM processes the RTR request to remove contacts associated with any IMPUs present in the AVPs if those IMPUs are present in the local cache.
 - If any of the IMPUs presented in the RTR request are not associated with the IMPI presented in RTR, the Oracle USM does NOT remove the contacts associated with that IMPU. However in previous versions, the Oracle USM removes contacts associated with those IMPUs.

Third Party Registration

The default behavior of the Oracle USM has been changed to perform third party registration for all PUIDs in the implicit set of a user that is registering at the Oracle USM.

Previously, the Oracle USM performed third party registration only for the PUID presented in a REGISTER.

The user can revert to the previous Oracle USM behavior using a sip-registrar option, as described in this document.

