

**Oracle® Unified Session Manager**  
Maintenance Release Guide  
Release SCZ725

December 2015

## Notices

Copyright ©2015 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

<b>1 SCZ7.2.5 M1</b> .....	<b>7</b>
Content Map.....	7
Determining Session Case and Served User for OOTB Calls Using the odi and orig Flags.....	8
Supported Sessioncase and Registration State.....	8
ACLI Instructions.....	9
S-CSCF Selection Based on Capabilities .....	10
Server-Capabilities AVP.....	11
Selection Process without SLRM.....	11
Selection Process with an SLRM.....	12
ACLI Instructions.....	13
Limiting AOR Contacts.....	14
ACLI Instructions.....	14
Maximum Number of Contacts.....	14
Matching Request URIs for Service Point Triggers.....	15
Issues Resolved.....	15
<b>2 SCZ7.2.5 M2</b> .....	<b>17</b>
Content Map.....	17
Configurable Response to Timed-Out OPTIONS Messages .....	18
Issues Resolved.....	18
<b>3 SCZ7.2.5 M3</b> .....	<b>19</b>
Content Map.....	19
Behavioral Changes.....	20
Handling Registration Termination Requests.....	20
Handling Barred PUIDs.....	21
Third Party Registration for an Implicit Registration Set.....	22
Registration Response with the Authentication-info Header.....	24
Issues Resolved.....	24
<b>4 SCZ7.2.5 M4</b> .....	<b>25</b>
Content Map.....	25
Limiting REGISTER CDR Generation.....	26
Issues Resolved.....	26
<b>A— Known Issues and Caveats (M1)</b> .....	<b>27</b>
Known Issues.....	27
Caveats (USM).....	28
<b>B— Known Issues and Caveats (M2)</b> .....	<b>31</b>
<b>C— Known Issues and Caveats (M3)</b> .....	<b>33</b>
Known Issues.....	33
Caveats.....	34

---

<b>D— Known Issues and Caveats (M4).....</b>	<b>37</b>
--	-----------

---

# About this Guide

This Oracle USM Maintenance Guide supports Release SCZ7.2.5 and its documentation set. It provides an overview of features and functions in Releases SCZ7.2.5M3 and SCZ7.2.5M4. This guide also documents issues fixed since between the M2 and M3 releases, as well as known issues and caveats associated with the M1, M2, M3 and M4 releases.

## Supported Platforms

Release Version S-CZ7.2.5 includes both the Oracle Core Session Manager (CSM) and Unified Session Manager (USM) products. The Oracle USM is supported on the Acme Packet 4500, 4600, 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 for updates specifying hardware support.

Platform support for the Oracle SLRM is the same as for the Oracle CSM.

Refer to the SCZ7.2.5 documentation set for more information about each platform.

## Audience

This Maintenance Guide is for service provider technicians who need to know about new features, fixed issues, known issues, and caveats associated with this release.

## Licensing

The SCZ7.2.5 release is an aggregation of software from various sources and organizations. These include Oracle software, third-party commercial software used under license, and publicly available software packages distributed under various open source licenses. For full details of the applicable licenses and how to obtain the corresponding source code for the open source components, click About on the Web GUI software Help menu or ask your Oracle representative.

## Revision History

Date	Revision Number	Description
May, 2015	1.00	Initial Release (M1)
July, 2015	2.00	Adds M2 Content
November, 2015	3.00	Adds M3 Content
December, 2015	4.00	Adds M4 Content



---

## SCZ7.2.5 M1

This section provides descriptions, explanations, and configuration information for the contents of Maintenance Release SCZ7.2.5M1. Maintenance Release content supercedes that distributed with the point release.

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

Current patch baseline: SCZ7.2.5 GA

### Content Map

The following table identifies the new content in this SCZ7.2.5 M1 Maintenance Release documentation.

Content Type	Description
Adaptation	Determining Session Case for Inbound OOTB Calls
Adaptation	S-CSCF Selection Based on Capabilities
Adaptation	Maximum Contacts per AOR (Contact Overwrite)
Adaptation	Matching Request URIs for Service Point Triggers

## 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.

When the ignore-psu-sesscase option is set, the Oracle USM determines Session Case for calls issued on behalf of a UE based on the presence of the **orig** or **odi** parameter in the top route header received by the Oracle USM, as follows:

- If the **odi** is present in the top route header, the Oracle USM continues to execute the original service logic (ORIG or TERM) and continues with additional iFC evaluation or subsequent routing.
- If the **orig** is present and there is no **odi** present in the top route header, the Oracle USM executes ORIGINATING OOTB procedures.
- If there is no **orig** or **odi** in the top route header, the Oracle USM executes TERMINATING OOTB procedures.

The Oracle USM identifies the Served User for OOTB calls based on Session Case, as follows:

- If the system is executing ORIGINATING procedures:
  1. The Served User is defined in the inbound PSU header .
  2. If the PSU is not present, the Served User is defined in the inbound P-Asserted-Identity header.
- If the system is executing TERMINATING procedures:
  1. The Served User is defined in the inbound P-Served-Used header .
  2. If the PSU is not present, the Served User is defined in the inbound Request-URI header.

## Supported Sessioncase and Registration State

The following cases are supported for IFC evaluation. Conditions for classifying the calls as such are listed below.

### Originating request - Registered User

When the Oracle USM receives an Initial request, it is validated as an originating request from or on behalf of a registered user when the following conditions are met:

- When the ignore-psu-sesscase option is not set:
  - The request is a dialog creating request or a standalone request.
  - There is no "odi" parameter in the top route of the request.
  - The regstate and sesscase parameters of the P-served-user indicate for this to be treated as originating request for a registered user.
- When the ignore-psu-sesscase option is set:
  - The request is a dialog creating request or a standalone request.
  - There is no "odi" parameter in the top route of the request.
  - There is an "orig" parameter in the top route of the request.
  - The served user is registered

### Originating request - Unregistered User

When the Oracle USM receives an Initial request, it is validated as an originating request from or on behalf of an unregistered user when the following conditions are met:

- When the ignore-psu-sesscase option is not set:
  - The request is a dialog creating request or a standalone request.
  - The served user is unregistered.



- The request is from an AS or I-CSCF and the top route header contains the orig parameter OR The regstate and sesscase of the P-served-user header indicates that the request is an originating request for an unregistered user.
- When the ignore-psu-sesscase option is set:
  - The request is a dialog creating request or a standalone request.
  - There is no "odi" parameter in the top route of the request.
  - There is an "orig" parameter in the top route of the request.
  - The served user is unregistered

### Terminating Requests - Registered User

When the Oracle USM receives an Initial request, it is validated as a terminating request towards a registered user when the following conditions are met:

- When the ignore-psu-sesscase option is not set:
  - The request is a dialog creating request or a standalone request.
  - There is no "orig" parameter in the top route of the request.
  - There is no "odi" parameter in the top route of the request.
  - The regstate and sesscase parameters of the P-served-user indicate for this to be treated as terminating request for a registered user OR the request is finished with originating services if applicable and the request is destined to a user who is currently registered with the Oracle USM.
  - If the Request-URI changes when visiting an application server, the Oracle USM terminates the checking of filter criteria and routes the request based on the changed value of the Request-URI, per 3GPP Specification TS 23.218.
- When the ignore-psu-sesscase option is set:
  - The request is a dialog creating request or a standalone request.
  - There is no "odi" parameter in the top route of the request.
  - There is no "orig" parameter in the top route of the request.
  - The served user is registered

### Terminating Requests - Unregistered User

See the IFC Support for Unregistered Users section in the Configuration Guide for this case.

- When the ignore-psu-sesscase option is not set:
  - If the Request-URI changes when visiting an application server, the Oracle USM terminates the checking of filter criteria and routes the request based on the changed value of the Request-URI, per 3GPP Specification TS 23.218.
- When the ignore-psu-sesscase option is set:
  - The request is a dialog creating request or a standalone request.
  - There is no "odi" parameter in the top route of the request.
  - The served user is not registered.

The request is a dialog creating request or a standalone request.

- There is no "orig" parameter in the top route of the request.
- There is no "odi" parameter in the top route of the request.
- The regstate and sesscase parameters of the P-served-user indicate for this to be treated as terminating request for an unregistered user

## ACLI Instructions

To enable 3GPP-compliant served user and session case identification for OOTB calls:

1. In Superuser mode, type configure terminal and press Enter.

```
ORACLE# configure terminal
```

2. Type session-router and press Enter to access the session router path.

```
ORACLE (configure) # session-router  
ORACLE (session-router) #
```

3. Type sip-config and press Enter. The system prompt changes to let you know that you can begin configuring individual parameters.

```
ORACLE (session-router) # sip-config  
ORACLE (sip-config) #
```

4. Type select to continue.

```
ORACLE (sip-config) # select  
ORACLE (sip-config) #
```

5. options—Set the options parameter by typing options, a Space, ignore-psu-sescase with a plus sign in front of it, and then press Enter.

```
ORACLE (sip-config) # options +ignore-psu-sescase
```

If you type the option without the plus sign, you will overwrite any previously configured options. In order to append the new options to the realm configuration's options list, you must prepend the new option with a plus sign as shown in the previous example.

6. Type done and exit to complete configuration of this sip-config configuration element.
7. Save and activate.

---

## 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.

S-CSCF selection based on capabilities utilizes AVP information exchanged with the HSS to identify required and preferred capabilities on a per-user basis. Capabilities themselves vary widely. Examples include administrator routing preferences for divergent service types. Capabilities are manually defined at the HSS for endpoints or groups of endpoints. The Oracle CSM, Oracle USM and Oracle SLRM user configures tables on the I-CSCF that map the S-CSCF's with the capabilities they support. Further configuration enables the I-CSCF to make the best S-CSCF selection, then forward appropriately.

Diameter messaging that can generate capabilities parsing for S-CSCF selection includes UAR/UAA and LIR/LIA traffic. Inclusion of the capabilities AVPs in the message sequence triggers this enhanced S-CSCF selection by the I-CSCF.

Configuration on the HSS and the I-CSCF must be compatible in deployments that use this feature. Configuration required on the Oracle device performing the I-CSCF function includes:

- servers-capabilities-list—A sip-registrar parameter that allows you to configure the registrar with a servers-capabilities-table.
- servers-capabilities-table—A multi-instance element that names the table and includes multiple servers-capability.
  - servers-capability—A multi-instance element within the servers-capabilities-table that includes a capability (capability value associated with users and supported by servers in the list) and a server-name-list that identifies the servers that support this capability.

The Oracle USM verifies the servers-capabilities-list attribute with the servers-capabilities-table each time it loads the configuration. If the servers-capabilities-table with the name specified in the servers-capabilities-list does not exist , the system outputs the following message:

```
ERROR: sip-registrar [<object-name>] has invalid servers-capabilities-list entry [<entry-name>]
```

## Server-Capabilities AVP

The Server-Capabilities AVP is a group AVP including the Mandatory-Capability AVP and Optional-Capability AVP. The number of Mandatory-Capability and Optional-Capability AVPs is not limited in a Server-Capabilities AVP. The AVP symbol notation, format and reference follows:

3GPP 32.299 states the following symbols are used in the message format definitions:

- <AVP> indicates a mandatory AVP with a fixed position in the message.
- {AVP} indicates a mandatory AVP in the message.
- [AVP] indicates an optional AVP in the message.
- \*AVP indicates that multiple occurrences of an AVP is possible.

Format definitions include:

- Server-Capabilities ::= <AVP header: 603 10415>
- \*{Mandatory-Capability}
- \*[Optional-Capability]
- \*[Server-Name] (not supported in this release)
- \*[AVP] (not supported in this release)

AVP reference, including column definition and AVP table follows:

- AVP Name
- AVP Number
- Reference where the AVP was defined
- Type of data format used to express the AVP's data
- If a grouped AVP, the names of the AVPs in the group

AVP	Number	Reference	Type	Grouped
{ Server-Capabilities }	603	Base	Grouped	Mandatory-Capability Optional-Capability
{ Mandatory-Capability }	604	Base	Unsigned32	
[ Optional-Capability ]	605	Base	Unsigned32	

## Selection Process without SLRM

The capabilities-oriented S-CSCF selection algorithm on the Oracle CSM and Oracle USM S-CSCF include selections based on mandatory and optional capabilities information received from HSS and the configured S-CSCF Capabilities Database.

The general approach to selection within this scenario include the following principles:

- Only S-CSCFs with all mandatory capabilities can be selected.
- The process gives priority to the S-CSCF with the most optional capabilities.
- The process gives priority to the local S-CSCF.
- The system attempts to spread assignments to remote S-CSCFs of the same priority.

The capabilities-oriented S-CSCF selection algorithm uses the following high-level steps within the I-CSCF function to arrive at a selection:

1. Determine that the capabilities algorithm is required:
  - a. No server-name in the LIA or UAA.
  - b. Capability list exists.
  - c. Assigned S-CSCF flag is not set.
  - d. Mandatory/Optional Capabilities received in UAA/LIA.

2. Identify potential S-CSCFs, which must support all mandatory capabilities:
  - a. Ensure the S-CSCF capabilities database is configured.
  - b. Build capable S-CSCF list. This list contains all S-CSCFs from the S-CSCF capabilities database that support the Mandatory capabilities.
  - c. Ensure that the capable S-CSCF list is not empty. If the capable S-CSCF list is empty, return an error to the UE.
3. Ensure that the I-CSCF is not SLRM.
4. Complete capabilities selection process using optional capabilities as criteria:
  - a. An S-CSCF has the most optional capabilities.  
(If so, forward.)
  - b. The local S-CSCF can take on more users, has all mandatory capabilities, and has most optional capabilities.  
(If so, forward locally.)
  - c. Use round robin to select the S-CSCF that has most optional capabilities.  
(If so, forward.)
5. Forward message:
  - a. Forward to selected S-CSCF.
  - b. Remove selected S-CSCF from capabilities list.
  - c. If there is an error, for example, the SIP response requires a re-assignment, check the assigned flag.
  - d. If the assigned flag is set, return to the top.  
  
If the assigned is not set, return to the step that checks whether the capable S-CSCF list is empty.
  - e. If the capable S-CSCF list is empty, return an error to the UE.  
  
If the capable S-CSCF list is not empty yet, perform capabilities selection process using optional capabilities as criteria again.

## Selection Process with an SLRM

The capabilities-oriented S-CSCF selection algorithm on the Oracle SLRM uses standard Oracle CSM selection criteria in addition to capabilities criteria. This criteria includes cluster configuration, S-CSCF resource utilization and SLRM synchronization.

The general approach to selection within this scenario include the following principles:

- Only Oracle CSMs with all mandatory capabilities can be selected.
- The process gives priority to the Oracle CSMs in the cluster with the most optional capabilities, and is best able to take on new users.

The capabilities-oriented S-CSCF selection algorithm uses the following high-level steps, including the SLRM's selection steps, within the I-CSCF function to arrive at a selection:

1. Determine that the capabilities algorithm is required:
  - a. No server-name in the LIA or UAA.
  - b. Capability list exists.
  - c. Assigned S-CSCF flag is not set.
  - d. Mandatory/Optional Capabilities received in UAA/LIA.
2. Execute capabilities selection:
  - a. Ensure the S-CSCF capabilities database is configured.
  - b. Build capable S-CSCF list. This list contains all S-CSCFs from the S-CSCF capability database that support the Mandatory capabilities.
  - c. Ensure that the capable S-CSCF list is not empty. If the capable S-CSCF list is empty, return an error to the UE.
3. Execute SLRM's selection procedure, cycle through all Oracle CSMs in the cluster:

- a. Identify applicable cluster. Begin to cycle through cluster.
  - b. Determine whether Oracle CSM is in capable list.
  - c. Determine whether Oracle CSM is at 100% utilization.
  - d. Determine whether the next Oracle CSM support more optional capabilities.
  - e. Determine whether the selected Oracle CSM is synchronized.
  - f. Determine whether the next Oracle CSM using fewer resources.
4. Complete capabilities selection process using optional capabilities as criteria:
    - a. An S-CSCF has the most optional capabilities.  
(If so, forward message.)
    - b. The local S-CSCF can take on more users and has all mandatory capabilities and most optional capabilities.  
(If so, forward message locally.)
    - c. Use round robin to select the S-CSCF that has most optional capabilities.  
(If so, forward message.)
  5. Forward message:
    - a. Forward to selected S-CSCF.
    - b. Remove selected S-CSCF from capabilities list.
    - c. If there is an error, for example, the SIP response requires a re-assignment, check the assigned flag.
    - d. If the assigned flag is set, return to the top.  
  
If the assigned is not set, return to the step that checks whether the capable S-CSCF list is empty.
    - e. If the capable S-CSCF list is empty, return an error to the UE.  
  
If the capable S-CSCF list is not empty yet, perform SLRM's selection procedure again.

## ACLI Instructions

### Configuring the server-capabilities-list

To assign a server capabilities list to a sip-registrar:

1. In Superuser mode, type configure terminal and press Enter.

```
ORACLE# configure terminal
```

2. Type session-router and press Enter to access the session router path.

```
ORACLE(configure)# session-router
```

3. Type sip-registrar and press Enter to access the session router path.

```
ORACLE(session-router)# sip-registrar
ORACLE(sip-registrar)#
```

4. Type server-capabilities-list and press Enter. Add a capability with associated servers.

```
ORACLE(sip-registrar)# server-capabilities-list my_capability_list1
ORACLE(sip-registrar)#
```

5. Type done and exit to complete configuration of this sip-registrar configuration element.

### Configuring the server-capabilities-table

A server-capabilities-table is a multi-instance element that allows the user to name a servers-capability object and apply it to a registrar. A servers-capability object is a server-capabilities-table sub-element that includes a capability and multiple server names, which support that capability.

1. In Superuser mode, type configure terminal and press Enter.

```
ORACLE# configure terminal
```

2. Type session-router and press Enter to access the session router path.

```
ORACLE(configure)# session-router
```

3. Type `server-capabilities-table` and press Enter to access the path.

```
ORACLE(session-router)# server-capabilities-table
ORACLE(server-capabilities-table)#
```

4. Enter a contiguous string to the name field. This name is the reference used in the registrar configuration to specify the use of this server capabilities table.
5. Type `servers-capability` and press Enter to access the path.

```
ORACLE(server-capabilities-table)# servers-capability
ORACLE(servers-capability)#
```

6. Enter a number to specify the capability capability. Valid entries range from 0 to 999999999.
7. Enter the names of the servers that belong to this server-name-list. Name format is the same as that used within the registrar's home-server-route field. The format is the URI (containing FQDN or IP address) used to identify a server to the HSS. Each entry in the list is enclosed with quotes and separated by comma.
8. Type done and exit twice to complete configuration of this server-capabilities-table configuration element.

---

## 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.

The value for `max-contacts-per-aor` ranges from 0-256. A value of 0 disables the function. When `max-contacts-per-aor` is greater than zero, the Oracle USM tracks the number of contacts registered per AOR. Settings for `max-contacts-mode` include REJECT and OVERWRITE.

If you change the configured maximum while the system is operational, your setting only applies to new registrations. If there are more contacts than your newly configured maximum, the system removes older contacts. This ensures that the contacts are always within the configured maximum.

Both `max-contacts-per-aor` and `max-contacts-mode` are RTC supported.

### Maximum Contacts REJECT Mode

If the Oracle USM receives a registration request that exceeds the maximum that you configured, it responds with a local response, a 403 Forbidden by default, and does not register the additional contact. The system only rejects registration requests that exceed the maximum. Existing contacts persist normally.

### Maximum Contacts OVERWRITE Mode

If the number of contacts in the initial registration exceeds the maximum, the Oracle USM selects only the highest priority contact based on q-values. If there are no q values, the Oracle USM adds contacts in the order they appear in the REGISTER message until it reaches the maximum. The system then identifies the oldest contacts for overwriting using the last registered time stamp.

In all cases, the Oracle USM follows this procedure to remove old contacts:

1. If `reg-id/instance-id` is present in the contact, the system simply updates the contact.
2. The system sends NOTIFY messages to the subscriber for whom the contact has been removed with a status of "terminated" and "de-activated" as the reason.
3. The system removes the contact from the registration cache.

## ACLI Instructions

### Maximum Number of Contacts

To configure a sip-registrar with a maximum of 10 contacts per AOR and a mode of overwrite:

1. From superuser mode, use the following command sequence to access sip-registrar element.

```
ORACLE# configure terminal
ORACLE(configure)# session-router
ORACLE(session-router)# sip-registrar
ORACLE(sip-registrar)# select
```

Select the registrar you want to configure.

2. Specify the number of contacts.

```
ORACLE(sip-registrar)# max-contacts-per-aor 10
ORACLE
```

3. Specify the contact mode to overwrite.

```
ORACLE(sip-registrar)# max-contacts-mode overwrite
ORACLE
```

4. Type done and exit to complete configuration of this sip-registrar configuration element.

## Matching Request URIs for Service Point Triggers

Version SCZ7.2.5 M1 of 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.

The Oracle USM uses Regex to match a REQUEST URI to a service point trigger to initiate service evaluation, as follows.

- SIP URI—The regular expression is matched against the hostport of the SIP-URI.
- Tel URI—The regular expression is matched against the telephone-subscriber of the telephone-URI.

The above is the default behavior for version 7.2.5 M1. If desired, however, the user can configure the system to revert to the previous behavior by setting an ifc-config option, as follows:

```
ORACLE(ifc-profile)#options +match-exact-requri
```

## Issues Resolved

Documented issues resolved between Release SCZ7.2.5 GA and Release SCZ7.2.5 M1 for the Oracle USM are listed below.

- 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.
- In versions SCZ7.1.5 and SCZ7.2.5, the Oracle USM removes ODIs from its database as soon as it has finished evaluating the service profile and the session is started. In some cases, however, an AS may request a follow up service referencing the call with the same ODI. Because the ODI is removed from the database, versions SCZ7.1.5 and SCZ7.2.5 reply to these follow-up service requests for a call with a 500 - Internal Service Error message.

Some deployments, however, may require that the Oracle USM either:

- Continue the IFC evaluation, if applicable
- Restart services

This is now the default behavior for version 7.2.5 M1. (This is also the default behavior for version 6.3.15.)

If desired, the user can configure the system to revert to the SCZ7.1.5 and SCZ7.2.5 behavior using a sip-config option, as follows:

```
ORACLE(sip-config)#options +error-on-invalid-odi
```

This resolution is to a previously undocumented issue.





---

## SCZ7.2.5 M2

This section provides descriptions, explanations, and configuration information for the contents of Maintenance Release SCZ7.2.5M2. Maintenance Release content supercedes that distributed with the point release.

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

Current patch baseline: SCZ7.2.5 M1

## Content Map

The following table identifies the new content in this SCZ7.2.5 M2 Maintenance Release documentation.

Content Type	Description
Adaptation	S-CSCF Provides 408 Response to Options Timeout

## 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.

By default, the Oracle USM does not send messages to an originating node when OPTIONS transactions time out. This complies with RFC 4321.

When registered users do not respond to OPTIONS requests, the network never informs the calling party of the called party's status. Instead, the calling party waits for the standard 32-second retry timeout to expire. If the called party was previously reachable, the calling party treats it as reachable for the entire 32-second window.

The Oracle USM includes a configuration option that:

- Starts a timer when the system forwards an applicable OPTIONS message and,
- Upon expiry of that timer, causes the system to send a 408 message to the calling party.

This option allows the network administrator to provide the calling party with this 408 response, and specify a shorter interval between request and response.

This feature works for:

- A called party that is registered via its P-CSCF, but not currently reachable.
- A called party that is reachable via an IBCF or BGCF.

This function has no impact on requests that result in a response, such as SIP 480, for un-registered subscribers.

For registered users with multiple contacts, the Oracle USM uses a response from any contact as a trigger to stop the timer and not send a 408. The Oracle USM cancels all remaining OPTIONS transactions when it receives a response from a contact. In addition, if the system used parallel forking to reach multiple contacts, it waits for the timer expiry before it sends the 200OK to the caller.

The option is available via S-CSCF processing and, as such, is available on both the Oracle USM and Oracle CSM products. There is, however, one operational difference between the Oracle USM and Oracle CSM. If the called party finally responds after this timer expires and the S-CSCF logic has sent the 408, the Oracle USM drops the response, whereas the Oracle CSM forwards it to the originating node.

The user sets the option globally in sip-config or on a sip-interface, with the sip-interface taking precedence. Values range from 1 to 32 seconds. Invalid ranges cause the system to use the maximum value of 32. The example below sets a sip-interface's timer to 4 seconds.

```
ORACLE (session-router) #sip-interface
ORACLE (sip-interface) #options +options-408-timeout=4
```

Option syntax on the sip-config and sip-interface configuration elements is the same.

The user must consider the infrastructure carefully. Setting the value too low can cause an inordinate number of invalid 408 responses.

## Issues Resolved

---

There are no previously documented issues to report as fixed between Release SCZ7.2.5 M1 and Release SCZ7.2.5 M2 for the Oracle USM.

---

## SCZ7.2.5 M3

This section provides descriptions, explanations, and configuration information for the contents of Maintenance Release SCZ7.2.5M3. Maintenance Release content supercedes that distributed with the point release.

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

Current patch baseline: SCZ7.2.5 M2

## Content Map

The following table identifies the new content in this SCZ7.2.5 M3 Maintenance Release documentation.

Content Type	Description
Adaptation	Explicit De-registration of a Contact Based on IMPI
Adaptation	Handling barred PUIDs
Adaptation	3rd Party Registration Enhancement
Adaptation	Authentication-Info header in the 200OK response
Defect Tracking	Issues Resolved

## Behavioral Changes

---

Please review the following sections prior to using this software release.

### 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\_UNKNOWN (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.

## 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.

The Oracle USM's behaviors when it receives RTRs are compliant with the following specifications:

- 3GPP TS 24.229 V13.1.0 (2015-03)
- 3GPP TS 29.228 V11.0.0 (2011-06)

The Oracle USM refers to specific AVPs within the RTR to determine its behavior. Applicable AVPs and Oracle USM behavior include:

- **User-Name**—This is a mandatory AVP, carrying the Private User Identity (IMPI). If this is the only AVP in the RTR, the Oracle USM de-registers all contacts of all the users that registered with this IMPI. Contacts registered with a different IMPI are not removed.
- **Associated-Identities**—This is an optional AVP. The HSS may send one or more of these AVPs when it intends to remove multiple associated private identities. If any of these AVPs are in the RTR, the Oracle USM de-registers all contacts or all users that registered with the IMPIs presented in the User-Name AVP and the Associated-Identities AVP.
- **Public-Identity**—This is an optional AVP, used to limit the effect of the RTR. The RTR may include more than one of these AVPs, which carry Public User Identities (IMPU/PUID). If these AVPs are in the RTR, the Oracle USM de-registers contacts of the IMPUs identified in the Public-Identity AVP that also registered using the IMPI in the User-Name AVP.

An RTR requesting de-registration of any of the identities included in an implicitly registered Public User Identity set triggers de-registration of the entire set. This is also true of wildcarded PUIDs and PSIs. If multiple IMPIs are associated with an unregistered user, then on receiving an RTR with one of the IMPIs, the Oracle USM removes the unregistered user entry, which, because it was never registered, has no contacts.

The Oracle USM does not terminate active calls during this RTR evaluation in compliance with TS 24.229.

After de-registering, the Oracle USM issues a NOTIFY to all applicable subscribed users detailing the event. This NOTIFY includes, for each applicable contact, a status of 'terminated' and an event of 'deactivated'. In addition, the Oracle USM de-registers all applicable users from third party registration ASs. Finally, the Oracle USM sends an RTA to the HSS after de-registration is complete.

The user can configure the Oracle USM to de-register all contacts associated with the user, regardless of the IMPI used during registration. Setting the sip-registrar option, disable-impi-specific-RTR establishes this behavior. The ACLI syntax for this option follows.

```
ORACLE (sip-registrar) #options +disable-impi-specific-RTR
```



**Note:** Prior to this version, the Oracle USM's default behavior was the same as if the disable-impi-specific-RTR option was set. Users upgrading to this version of the Oracle USM must set the disable-impi-specific-RTR option if they need to retain the previous behavior.

## 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.


A common use case for barring information is a cell phone registering with a temporary PUID (that is barred), along with a set of non-barred PUIDs in the P-Associated User (PAU) header. After registration, the cell phone should use only the non-barred PUIDs for all ensuing methods and its contacts.

An HSS should be configured with barring information for all PUIDs. During registration procedures, the HSS provides this information to the S-CSCF. PUID information in the User Data AVP of the Diameter SAA includes a tag indicating whether the PUID is barred. The Oracle USM retains this information in the registration cache. To complete the registration, the Oracle USM replies to the UE with a list of all non-barred PUIDs in the 200OK. For all the further procedures, the UE should use a PUID from the non-barred P-Associated-URI list. If the HSS does not identify a PUID's barring status, the Oracle USM assumes it is not barred.

Typical Oracle USM behaviors related to barring include:

- Responds to ensuing requests from barred PUIDs with (403) Forbidden.
- Responds to requests that have no PSU, but include barred PUIDs in their PAI header list with 403 (Forbidden).
- Responds to requests to or from wildcarded PUIDs that match barred PUIDs with 403 (Forbidden).
- Responds to registration attempts that have all barred implicit identities with 403 (Forbidden).
- Responds to requests for termination services wherein the served user (PSU/RURI) is barred with (404) Not Found.
- Recognizes barring status during third party registration procedures and does not attempt to register a barred PUID to an AS.
- Handles related subscription scenarios as follows:
  - When receiving a subscription from a barred subscriber, responds with 403 (Forbidden).
  - When receiving a subscription for a barred user, allows the SUBSCRIBE to proceed.
  - Does not include a barred identity in any NOTIFY.
    - When receiving a subscription for a user that has barred identities in its implicit set, issues NOTIFYs that only include non-barred identities.

- Includes only non-barred PUIDs in NOTIFY messages generated by network-initiated re-registration and authorization requests.


 **Note:** The Oracle USM does not support any PUID barring within the context of GRUU.

The user can verify PUID barring status using the `show reg sipd by-user <user> detailed` command. Example output is shown below.

```
ORACLE# show reg sipd by-user user detailed
Registration Cache (Detailed View)      Thu Jul 09 2015  15:16:08
User: sip:user_1@acme-ims.com
Registered at: 2015-07-09-15:16:04      Surrogate User: false
Emergency Registration? No
ContactsPerAor Rejects 0
ContactsPerAor OverWrites 0


Contact Information:
Contact:
  Name: sip:user_1@acme-ims.com
  Valid: true
...

Associated URI(s):
  URI: sip:user_1@acme-ims.com
  Status: Barred
...
```

 **Note:** The Oracle USM replicates barred status for PUIDs to standby systems.

## 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.

 **Note:** The Oracle USM does not attempt third party registration for any barred, tel or wildcard PUIDs.

The user can verify all third party registrations using the `show registration sipd by-user [user] detailed` command. Example output is shown below.

```
ORACLE# show registration sipd by-user 234 detailed
Registration Cache (Detailed View)      Wed Sep 16 2015  10:57:44
User: sip:234@acme-ims.com
Registered at: 2015-09-16-10:57:40      Surrogate User: false
Emergency Registration? No
ContactsPerAor Rejects 0
ContactsPerAor OverWrites 0

Contact Information:
Contact:
  Name: sip:234@acme-ims.com
  Valid: true
  Challenged: false
```

```
Registered at: 2015-09-16-10:57:40
Last Registered at: 2015-09-16-10:57:40
Expire: 3596
Local expire: 296
Half: 1796

Registrar IP: 0.0.0.0
Transport: UDP
Secure: false
Local IP: 192.168.53.99:5060

User Agent Info:
  Contact: sip:234@192.168.53.181:5060
  Realm: core
  IP: 192.168.53.181:5060

SD Info:
  Contact: sip:234-tbcktcgo177fc@192.168.53.99:5060
Call-ID: 1-5853@192.168.53.181
  Path: <sip:234@192.168.53.181:5060;lr;p-acme-serving>

Associated URI(s):
  URI: sip:234@acme-ims.com
  Status: Non-Barred
  Filter Criteria:
    Priority: 0
    Filter: ((method == REGISTER)) or
            ((method == INVITE))
    Application Server: sip:172.16.17.10:5060

  URI: sip:1@acme-ims.com
  Status: Non-Barred
  Filter Criteria:
    Priority: 0
    Filter: ((method == REGISTER)) or
            ((method == INVITE))
    Application Server: sip:172.16.17.10:5060
  Priority: 1
  Filter: ((method == INVITE)) or
          ((method == REGISTER))
  Application Server: sip:172.16.53.181:5065

  URI: tel:135
  Status: Barred
  Filter Criteria:
    Priority: 0
    Filter: ((method == INVITE)) or
            ((method == REGISTER))
    Application Server: sip:172.16.53.181:5065
  Priority: 1
  Filter: ((method == INVITE)) or
          ((method == REGISTER))
  Application Server: sip:172.16.53.181:5095

Third Party Registration(s):
  Third Party Registration Host: 172.16.17.10
  Registration State: REGISTERED
  Last Registered at: Never
  Third Party Registration Host: 172.16.53.181
  Registration State: REGISTERED
  Last Registered at: Never
```

The user can check for third party registrations errors using the show sipd third-party-reg all command. Example output is shown below.

```
ORACLE# show sipd third-party-reg all
3rd Party Registrar      SA State   Requests   200OK   Timeouts
Errors
(D) 111.11.17.10         INSV      1          1       0       0
(D) 111.11.53.181       INSV      1          1       0       0
```

The user can disable the default behavior and perform third party registration only for the PUID in the REGISTER by configuration. Disabling this behavior can improve system performance by preventing the system from having to walk through large PUID sets for large numbers of ASs. The ACLI syntax for disabling this functionality using the disable-thirdPartyReg-for-implicit-puid setting follows.

```
ORACLE (sip-registrar) #options +disable-thirdPartyReg-for-implicit-puid
```



**Note:** Prior to this version, the Oracle USM's default behavior was the same as if the disable-thirdPartyReg-for-implicit-puid option was set in the SIP registrar. Users upgrading to this version of the Oracle USM must set the disable-thirdPartyReg-for-implicit-puid option to retain the previous behavior.

## 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.

By default, the Oracle USM supports registration with SIP digest authentication without using the authentication-info header. This is not compliant with TS 24.229. Enabling the add-auth-info option causes the Oracle USM to calculate and insert the required authentication-info header fields in the 200 OK.

The Oracle USM also presents this authentication header during third party registrations. The system includes the entire 200OK message in the third party registration request.

This authentication state is not shared across high availability nodes. The user can expect the Oracle USM to request re-authentication by registering UEs after failover to a backup Oracle USM.

Authentication-Info header field parameters sent by the Oracle USM include:

- qop—Matches the qop sent by the UE
- rspauth—A response-digest calculated as described in RFC 2617
- cnonce—Matches the cnonce sent by the UE
- nonce-count—Matches the nonce-count sent by the UE

The nextnonce authentication-info header field parameter, which can request a new nonce for subsequent authentication responses from the UE, is not implemented on the Oracle USM.

The ACLI syntax for enabling the add-auth-info option follows.

```
ORACLE (sip-registrar) #+options=add-auth-info enabled
```

The Oracle USM provides NOTICE level log entries in log.sipd to indicate this option's status.

## Issues Resolved

Documented issues resolved between Release SCZ7.2.5 M2 and Release SCZ7.2.5 M3 for the Oracle USM are listed below.

- The Oracle USM now sends third party registration for the entire implicit registration set. The new behavior is documented herein as a 3rd party registration enhancement.



---

## SCZ7.2.5 M4

This section provides descriptions, explanations, and configuration information for the contents of Maintenance Release SCZ7.2.5M4. Maintenance Release content supercedes that distributed with the point release.

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

Current patch baseline: SCZ7.2.5 M3

## Content Map

The following table identifies the new content in this SCZ7.2.5 M4 Maintenance Release documentation.

Content Type	Description
Adaptation	Limiting REGISTER CDR Generation
Defect Tracking	Issues Resolved

## 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.

When the user enables accounting with the generate-events parameter, the Oracle USM can generate CDRs for the following register and/or local register events:

- Initial REGISTER
- REGISTER refresh
- REGISTER update
- de-REGISTER

Depending on the event, the system generates per-contact start, interim and/or stop CDRs. With no other configuration, the system generates the appropriate CDRs for all of these events.

The user can prevent the system from issuing some CDR via an account-config option that filters, as described below, and sets a timer that restarts the CDR suppression window. Use the syntax below to set this register-cdr-interval option with an expiry timer value of 43200 in minutes (30 days), and limit the number of generated CDRs as described below.

```
(account-config) #options +register-cdr-interval=43200
```

When configured with this option, the Oracle USM limits the generation of CDRs for each user as follows:

1. Send a START CDR for first Register message (for first contact).
2. Don't send CDRs until the user specified time period expires. After it expires, when a Registration message causes a 'START' or 'INTERIM' CDR event to occur, send it. Then, re-set the time value. Applicable 'START' CDR events include:
  - Add new contact
  - Replace contact
  - Overwrite contact

The applicable 'INTERIM' CDR event is a Refresh Contact.

The generate-event parameter must also be set to register.

## Issues Resolved

---

There are no previously documented issues to report as fixed between Release SCZ7.2.5 M3 and Release SCZ7.2.5 M4 for the Oracle USM.

---

## Known Issues and Caveats (M1)

### Known Issues

---

This section lists items that the customer needs to be aware of when deploying the Oracle USM. Oracle is working to fix these issues within the context of this major release version.

This section lists known issues related to Version S-Cz7.2.5M2 of the Oracle USM.

- Media and management (wancom) interfaces may not be configured with the same subnet, regardless of VLAN.
- 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.
- 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”.
- Multi-stage routing does not work for S-CSCF routing functions, such as ENUM lookups to resolve Tel URIs. For S-CSCF routing functions that require ENUM lookup, refer to the configuration option section.
- During ISC orchestration, if the Oracle USM receives the same ODI in subsequent messages from the AS (for e.g., forking), it is possible that the Oracle USM will either
  - Continue the IFC evaluation, if applicable
  - Reject the subsequent message request
  - Restart services

This behavior depends on when the subsequent messages in the call flow with the same ODI arrive at the CSM.

- Resolution - Do not configure an AS to fork responses to the Oracle USM that include an ODI originally provided by the Oracle USM, and if the calls flows rely on a specific behavior listed above and the call flow pattern can change.
- The Oracle USM does not send third party registration for the entire implicit registration set. It only sends this for the specific public user identity that is registering, de-registering or re-registering.
- Instead of routing a message via local policy after performing any originating services, the Oracle USM incorrectly issues an LIR when the following two conditions exist simultaneously:

## Known Issues and Caveats (M1)

---

- 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.

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. This would be true for OOTB calls. 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.

### Supported Hardware

AP4500 hardware with BoardRev: 3.00 will not load the licenses that are expected to appear. As a workaround, reinstall licenses manually after reboot with the original key. Use the **show version boot** command and look to the Mainboard Info section, BoardRev: attribute.

### 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.

### File Systems

For users with the AP4500 system with a hard-disk, an upgrade from pre-S-CZ7.1.5 software to this version will not change the hard drive's filesystem from FAT-32 to ext3 to preserve any existing data. This results in the SFTP application not providing the expected filesystem user security. To rectify this, reformat the system's hard-disk.



**Note:** By reformatting the hard-disk, you will lose the contents of /opt and any other user-created partitions located under /mnt.

### Encryption Hardware Support

On the AP4500, IPSec and SRTP are supported with ETCv1 and ETCv2 NIUs only.

### 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.

In an HA deployment, the primary Oracle USM synchronizes contacts for IMS AKA-based registrations to the standby very slowly. Under extreme load conditions, the standby may not receive all registrations.

### USM Running as an SLB Cluster Member

Rebalancing is unavailable on the Oracle Communications Session Load Balancer when running an AP6300 as a cluster member. Set the SLB's **cluster-config > auto-rebalance** parameter to **disabled** to use an AP6300 as a cluster member from that SLB.

### SIP over TCP

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

## Caveats (USM)

---

This section lists items that the customer needs to be aware of when deploying the Oracle USM.

**Release Caveats**

This section advises the user on important considerations for this release.

**Transcoding - general**

Only SIP signaling is supported with transcoding.

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

Transcoding is not available in conjunction with SRTP.

QoS is not supported for transcoded calls.

SIPREC may not be performed on a transcoded call.

**T.38 Fax Transcoding**

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

Fax codec policy based on D7.0 fax transcoding policy.

Pooled Transcoding for Fax is unsupported.

**High Availability**

When the AP6300 experiences call rates over 650 CPS, SIP and/or MBCD may fail to synchronize.

**Archive Logs**

Archiving log files is unsupported on the AP4500 platform without a HDD installed.

**HMR action on Call-ID**

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

**Lawful Intercept**

Lawful Intercept is supported for the X123 protocol only.

**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.

**SRTP Caveats**

MIKEY key negotiation is not supported.

The ARIA cipher is not supported.

Linksys SRTP is not supported.

## Known Issues and Caveats (M1)

---

### **Packet Trace**

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

### **Phy Link Redundancy**

Phy link redundancy is not supported in this release.

### **Session Replication for Recording**

Session Replication for Recording is not supported in this release.

### **RTCP Generation**

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

### **SCTP**

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

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

---

## **Known Issues and Caveats (M2)**

There are no changes to the Known Issues and Caveat lists between Release SCZ7.2.5 M1 and Release SCZ7.2.5 M2 for the Oracle USM. Refer to Appendix A, Known Issues and Caveats (M1) for this information.





---

## Known Issues and Caveats (M3)

### Known Issues

---

This section lists items that the customer needs to be aware of when deploying the Oracle USM. Oracle is working to fix these issues within the context of this major release version.

This section lists known issues related to Version S-Cz7.2.5M3 of the Oracle USM.

- Media and management (wancom) interfaces may not be configured with the same subnet, regardless of VLAN.
- 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.
- 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”.
- Multi-stage routing does not work for S-CSCF routing functions, such as ENUM lookups to resolve Tel URIs. For S-CSCF routing functions that require ENUM lookup, refer to the configuration option section.
- During ISC orchestration, if the Oracle USM receives the same ODI in subsequent messages from the AS (for e.g., forking), it is possible that the Oracle USM will either
  - Continue the IFC evaluation, if applicable
  - Reject the subsequent message request
  - Restart services

This behavior depends on when the subsequent messages in the call flow with the same ODI arrive at the CSM.

- Resolution - Do not configure an AS to fork responses to the Oracle USM that include an ODI originally provided by the Oracle USM, and if the calls flows rely on a specific behavior listed above and the call flow pattern can change.
- Instead of routing a message via local policy after performing any originating services, 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.

## Known Issues and Caveats (M3)

---

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. This would be true for OOTB calls. 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.

### File Systems

For users with the AP4500 system with a hard-disk, an upgrade from pre-S-CZ7.1.5 software to this version will not change the hard drive's filesystem from FAT-32 to ext3 to preserve any existing data. This results in the SFTP application not providing the expected filesystem user security. To rectify this, reformat the system's hard-disk.

 **Note:** By reformatting the hard-disk, you will lose the contents of /opt and any other user-created partitions located under /mnt.

### Encryption Hardware Support

On the AP4500, IPSec and SRTP are supported with ETCv1 and ETCv2 NIUs only.

### 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.

In an HA deployment, the primary Oracle USM synchronizes contacts for IMS AKA-based registrations to the standby very slowly. Under extreme load conditions, the standby may not receive all registrations.

### USM Running as an SLB Cluster Member

Rebalancing is unavailable on the Oracle Communications Session Load Balancer when running an AP6300 as a cluster member. Set the SLB's **cluster-config > auto-rebalance** parameter to **disabled** to use an AP6300 as a cluster member from that SLB.

### SIP over TCP

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

## Caveats

---

This section lists items that the customer needs to be aware of when deploying the Oracle USM.

### Release Caveats

This section advises the user on important considerations for this release.

- Starting with Oracle USM version 7.2.5M3, RTR is processed only if the Private-Id that is present in the User-Name AVP is present in the Oracle USM local cache. Prior to 7.2.5M3, even if the Private-id in the User-Name AVP is not present in the local cache, the Oracle USM removes all the contacts associated with PUIDs sent in all the Public -Identities AVP.

- Starting with Oracle USM version 7.2.5M3, only those Public that are associated with the Private-Id sent in the User-Name AVP are processed. For details on how it is processed refer section for the RTR feature. However prior to 7.2.5M3, even if the PUIDs present in the Public-Identities AVP are not associated with Private-Identity sent in the User-Name AVP, they are removed from the Oracle USM.

### Third Party Registration for Implicit PUID

If third party registration for implicit PUID is configured, and if multiple service profiles for implicit users share the same application server, the Oracle USM sends only one 3rd Party registration for the AS. The system behaves this way because the key to a third party registration is the SIP user's AOR, which is the same for all implicit users.

### Barred Registration Management

- The Oracle USM does not support barred PUID handling with GRUU.
- The Oracle USM does not support barring for emergency registration.
- The Oracle USM, as S-CSCF, does not check whether the WAF is not barred, as specified in 3GPP TS 33.203 [9] annex X, and send a 403 (Forbidden) response to the REGISTER request when:
  - The REGISTER request contains an Authorization header field with the "authorization-entity" or "web server-entity" header field parameter, as defined in draft-holmberg-sipcore-auth-id [229], and
  - The S-CSCF supports WebRTC, and has received authorization information about WAF entities from the HSS, or per configuration.

### Transcoding - general

Only SIP signaling is supported with transcoding.

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

QoS is not supported for transcoded calls.

SIPREC may not be performed on a transcoded call.

### T.38 Fax Transcoding

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

Fax codec policy based on D7.0 fax transcoding policy.

Pooled Transcoding for Fax is unsupported.

### High Availability

When the AP6300 experiences call rates over 650 CPS, SIP and/or MBCD may fail to synchronize.

### Archive Logs

Archiving log files is unsupported on the AP4500 platform without a HDD installed.

### HMR action on Call-ID

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

### Lawful Intercept

Lawful Intercept is supported for the X123 protocol only.

### FTP Support

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

## Known Issues and Caveats (M3)

---

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.

### **SRTP Caveats**

MIKEY key negotiation is not supported.

The ARIA cipher is not supported.

Linksys SRTP is not supported.

### **Packet Trace**

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

### **Session Replication for Recording**

Session Replication for Recording is not supported in this release.

### **RTCP Generation**

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

### **SCTP**

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

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

---

## **Known Issues and Caveats (M4)**

Refer to Appendix C, Known Issues and Caveats (M3) for the Known Issues and Caveat lists documentation for Release SCZ7.2.5 M4.

There is one additional Known Issue in Release SCZ7.2.5 M4:

- When the register-cdr-interval is set, as described in this document's M4 feature description titled Limiting REGISTER CDR Generation, the Oracle USM does not issue RADIUS STOP CDRs for Registration events.

