

Oracle® Communications Session Delivery Manager Release Notes



Release 9.0

F52426-12

July 2024

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Copyright © 2022, 2024, Oracle and/or its affiliates.

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

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

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

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

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

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

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

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

Contents

About This Guide

My Oracle Support

vii

Revision History

1 Overview

Session Delivery Manager Application Overview	1-1
Session Delivery Manager Product Plug-in Service	1-1
External Interfaces	1-2
Documentation Distribution	1-3

2 Release 9.0.3

Release 9.0.3 Features	2-1
Session Delivery Manager Software Distribution Media for Release 9.0.3 GA	2-1
Session Element Manager Plug-in Support Matrix for 9.0.3	2-2
Session Element Manager Plug-in Device Software Support for 9.0.3	2-3
SDM Release 9.0.3.0.1	2-4
Session Delivery Manager Software Distribution Media for Release 9.0.3.0.1 GA	2-4
Session Element Manager Plug-in Support Matrix for 9.0.3.0.1	2-5

3 Release 9.0.2

Release 9.0.2 Features	3-1
Session Delivery Manager Software Distribution Media for Release 9.0.2 GA	3-1
Session Element Manager Plug-in Support Matrix for 9.0.2	3-2
Session Element Manager Plug-in Device Software Support for 9.0.2	3-3
SDM Release 9.0.2.0.1	3-4
Session Delivery Manager Software Distribution Media for Release 9.0.2.0.1 GA	3-4
Session Element Manager Plug-in Support Matrix for 9.0.2.0.1	3-5
SDM Release 9.0.2.0.2	3-6
Session Delivery Manager Software Distribution Media for Release 9.0.2.0.2 GA	3-6

4 Release 9.0.1

Release 9.0.1 Features	4-1
Session Delivery Manager Software Distribution Media for Release 9.0.1 GA	4-1
Session Element Manager Plug-in Support Matrix for 9.0.1	4-2
Session Element Manager Plug-in Device Software Support for 9.0.1	4-3

5 Release 9.0.0

Release 9.0.0 Features	5-1
Session Delivery Manager Software Distribution Media for Release 9.0.0 GA	5-1
Session Element Manager Plug-in Support Matrix for 9.0.0	5-2
Session Element Manager Plug-in Device Software Support for 9.0.0	5-3

6 OCSDM Releases 8.2.5 to 8.2.1

Features in SDM Releases 8.2.5 to 8.2.1	6-1
Plug-in Support Matrix for SDM 8.2.5 to 8.2.1 Releases	6-7
Plug-in Device Software Support for SDM 8.2.5 to 8.2.1 Releases	6-8

7 Session Delivery Manager Installation

Check System Requirements	7-1
Software Installation Prerequisites	7-3
Check that Work Orders are in a Committed State	7-3
Report Manager Installation	7-3

8 Session Element Manager Features Delivered by the Service Provider Plug-in

Session Element Manager Features Delivered by the Service Provider Edge and Core Plug-in Release	8-1
--	-----

9 Session Element Manager Features Delivered by the Enterprise Edge and Core Plug-in

Session Element Manager Features Delivered by the Enterprise Edge and Core Plug-in	9-1
--	-----

10	Session Element Manager Features Delivered by the Enterprise Utilities Plug-in	
	Session Element Manager Features Delivered by the Enterprise Utilities Plug-in Release	10-1
11	Interface Changes	
	Differences in REST Response - JSON Format	11-1
	Differences in REST Request - XML Format	11-1
	Differences in REST Response - XML Format	11-3
12	Resolved Known Issues and Known Issues in SDM 9.0	
13	Caveats and Limitations	
14	Known Issues and Resolved Known Issues	
A	Historical Session Element Manager Device Software Support	

About This Guide

This document and other product-related documents are described in the Related Documentation table.

Related Documentation

Table 1 Oracle Communications Session Delivery Manager Documentation Library

Document Name	Document Description
Administration Guide	<p>Provides the following administration information:</p> <ul style="list-style-type: none"> • Implement OCSDM on your network as a standalone server or high availability (HA) server. • Login to the OCSDM application, access GUI menus including help, customize the OCSDM application, and change your password. • Access the product plugin service through the GUI to manage product plugin tasks, including how product plugins are uploaded and installed. • Manage security, faults, and transport layer security certificates for east-west peer OCSDM server communication, and southbound communication with network function (NF) devices. • Configure northbound interface (destination) fault trap receivers and configure the heartbeat trap for northbound systems. • Monitor OCSDM server health to detect heartbeat messages and display the server status to prevent health problems, or view server disk utilization information and server directory statistics. • Maintain OCSDM server operations, which includes database backup and database restoration and performing server cluster operations. • Use available OCSDM server scripts, the contents of fault trap notifications, and a list of northbound notification traps generated by the OCSDM server.

Table 1 (Cont.) Oracle Communications Session Delivery Manager Documentation Library

Document Name	Document Description
Installation Guide	Provides the following installation information: <ul style="list-style-type: none"> Do pre-installation tasks, which include reviewing system requirements, adjusting linux and firewall settings, completing OCSDM server settings and configuring your NNCentral account for security reasons. Do the typical installation to perform the minimal configuration required to run the OCSDM server. Do the custom installation to perform more advanced configurations including the mail server, cluster management, Route Manager, transport layer security (TLS), and Oracle database configuration.
Release Notes	Contains information about the administration and software configuration of the OCSDM feature support new to this release.
Security Guide	Provides the following security guidelines: <ul style="list-style-type: none"> Use guidelines to perform a secure installation of OCSDM on your server, which includes methods for securing the server, firewall settings, system support for encryption and random number generators (RNG), using HTTPS, and password guidelines. Review Security Manager features that are used to configure groups, users, operations, privileges, and manage access to the system. Follow a checklist to securely deploy OCSDM on your network and maintain security updates.
REST API Guide	Provides information for the supported REST APIs and how to use the REST API interface. The REST API interface allows a northbound client application, such as a network service orchestrator (NSO), to interact with OCSDM and its supported product plugins.
SOAP API Guide	The SOAP API guide provides information for the SOAP and XML provisioning Application Programming Interface (API) client and server programming model that enables users to write client applications that automate the provisioning of devices. The web service consists of operations that can be performed on devices managed by the SDM server and data structures that are used as input and output parameters for these operations.

My Oracle Support

My Oracle Support (<https://support.oracle.com>) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request.
2. Select 3 for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
 - For technical issues such as creating a new Service Request (SR), select 1.
 - For non-technical issues such as registration or assistance with My Oracle Support, select 2.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at <http://www.oracle.com/us/support/contact/index.html>. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, <http://docs.oracle.com>. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at <http://www.adobe.com>.

1. Access the Oracle Help Center site at <http://docs.oracle.com>.
2. Click **Industries**.
3. Under the Oracle Communications sub-header, click the **Oracle Communications documentation** link.

The Communications Documentation page appears. Most products covered by these documentation sets appear under the headings "Network Session Delivery and Control Infrastructure" or "Platforms."

4. Click on your Product and then Release Number.
A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info> or visit <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs> if you are hearing impaired.

Revision History

This section provides a revision history for this document.

Date	Revision
April 2022	<ul style="list-style-type: none">Initial Release.
September 2022	<ul style="list-style-type: none">Adds Known Issue about local help files.
October 2022	<ul style="list-style-type: none">Adds updates for the SDM 9.0.1 Release
November 2022	<ul style="list-style-type: none">Adds updates for the SDM 9.0.1 Plug-in Device Software
April 2023	<ul style="list-style-type: none">SDM 9.0.2 updates.
July 2023	<ul style="list-style-type: none">Adds updates regarding ECB 4.1.0
October 2023	<ul style="list-style-type: none">Adds content updates, Resolved Known Issues list, and plug-in versions for SDM Release 9.0.2.0.1
January 2024	<ul style="list-style-type: none">Adds content updates, and plug-in versions for the Release SDM 9.0.2.0.2
April 2024	<ul style="list-style-type: none">SDM 9.0.3 Release
June 2024	<ul style="list-style-type: none">Content updates in the Caveats and Limitations section.
July 2024	<ul style="list-style-type: none">Content updates for the SDM 9.0.3.0.1 Release

1

Overview

Oracle Communications Session Delivery Manager is a network element management system that can be accessed through a graphical user interface (GUI), REST API interface, or SOAP interface.

Read and understand all sections in the Oracle Communications Session Delivery Manager Release Notes before installing, upgrading, or using this product.

Session Delivery Manager Application Overview

Once Oracle Communications Session Delivery Manager is installed, you can access the following features through their respective sliders:

- **Device Manager**—Use this slider to configure device groups. The functionality of this slider is dependant on the product plug-in(s) that you have installed.
- **Security Manager**—Use this slider to configure any security privileges that are specific to OCSDM and the product plugin.
- **Fault Manager**—View events, alarms, and trap summary data.

Note:

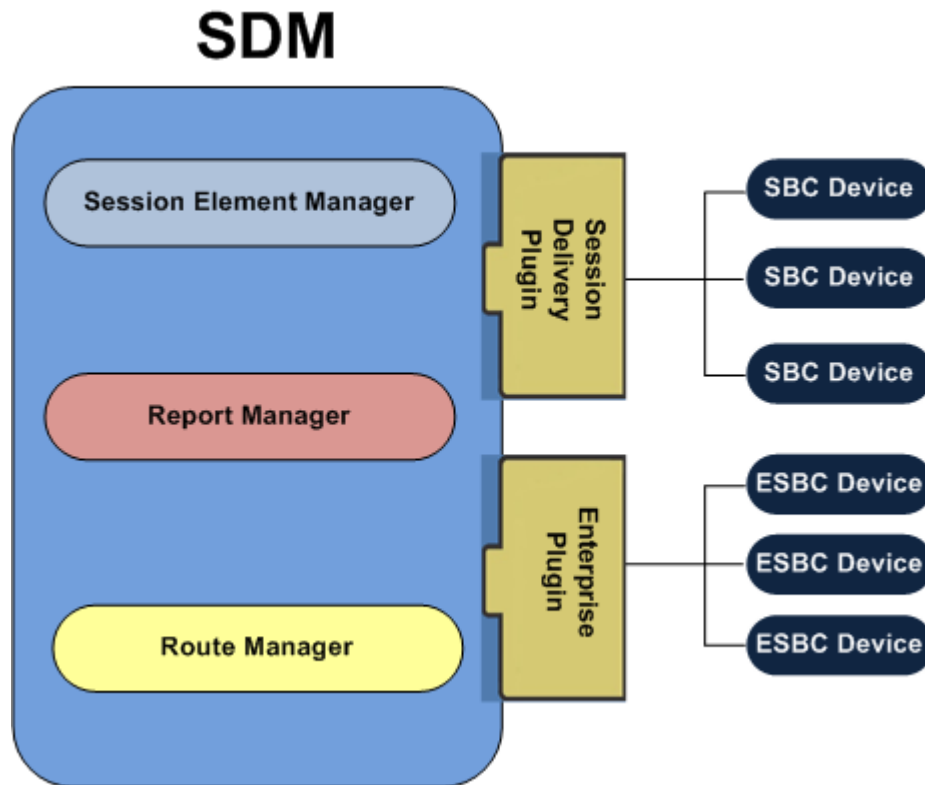
Upon installation of one of these plugins, the OCSDM displays only the applicable sliders and their relevant configuration elements to enable.

Session Delivery Manager Product Plug-in Service

A product plug-in is used to activate Oracle Communications Session Delivery Manager to provide fault, configuration, accounting, performance, and security (FCAPS) for devices, and control communications with network elements over secure protocols.

OCSDM has limited functionality until a plug-in is uploaded and installed in OCSDM. Product functionality activated by the plugin in the OCSDM GUI is specific to what the plugin supports. For example, if you see a drop-down menu, field or checkbox that cannot be accessed, the plugin does not support this functionality in the GUI.

Use the plugin service in Oracle Communications Session Delivery Manager to install the product plugin. More than one product plugin can be installed on OCSDM at the same time, and the functionality of the plugin(s) is propagated to other OCSDM nodes in a clustered environment. The following example shows how the Service Provider and Enterprise product plugins provide their respective devices access to Session Element Manager, Report Manager and Route Manager.



External Interfaces

This section describes the supported external API interfaces.

REST API

Oracle Communications Session Delivery Manager supports a REST API interface, allowing northbound client applications to interact with OCSDM and its supported product plugins. For information on supported REST APIs and how to use the REST API interface, see the *REST API for Session Delivery Manager* guide.

SOAP API

Post OCSDM Release 8.2, the SOAP API and SOAP API client will not introduce any new APIs. Oracle recommends using the REST API for OCSDM, if you require access to new OCSDM features via a programmatic API.

 **Note:**

Existing SOAP APIs will continue to provide configuration management support for new SBC releases that can be managed by a given SDM release.

Documentation Distribution

You can access the latest Oracle Communications Session Delivery Manager documents by selecting [Session Delivery Manager](#) from the [Oracle Help Center Communications Documentation](#) web page.

From the main Session Delivery Manager (NNC) Documentation page, you can access links to the following documentation pages for various releases:

- [Oracle Communications Session Delivery Manager page](#)—Access the installation, administration, security, release notes, and access a link to the REST API documentation.
- [Oracle Communications Session Element Manager page](#)—Access the Oracle Communications Session Element Manager user guides customized for each plug-in product, the SOAP API guide, and license documentation.
- [Oracle Communications Report Manager page](#)—Access the Oracle Communications Report Manager user guide, installation guide, and license documentation.
- [Oracle Communications Route Manager page](#)—Access the Oracle Communications Route Manager user guide and license documentation.

2

Release 9.0.3

The following topics provide descriptions, explanations, and configuration information for the contents of Release 9.0.3.

Unless otherwise stated, requirements and other release information is identical to 9.0 GA, noted in the other chapter of this document.

Release 9.0.3 Features

New Features in the SDM 9.0.3 Release.

The following table describes the Release 9.0.3 features for Oracle Communications Session Delivery Manager (OCSDM).

Table 2-1 This table lists and describes the 9.0.3 features

Feature	Description	Where Documented
Audit Log Description Enhancement	SDM 9.0.3 Audit logs store information on various operations in the database. This information is now displayed on the GUI. On clicking saveToFile , you can also download the data in a .CSV file to the your local storage.	SDM 9.0.3 Administration Guide
Support for Oracle Linux 8.8 and 8.9 versions	SDM 9.0.3 now supports Oracle Linux 8.8 and 8.9 versions	SDM 9.0.3 Release Notes
Support for Oracle Business Intelligence Publisher 12.2.1.4	SDM 9.0.3 now supports Oracle Business Intelligence Publisher 12.2.1.4	<ul style="list-style-type: none">• Session Report Manager Installation Guide for Oracle Fusion Middleware 19c• Session Report Manager Upgrade Guide for Oracle Fusion Middleware 19c
Support for TLS v1.3	<ul style="list-style-type: none">• TLS v1.3 is supported from SDM Release 9.0.3, and SDM is backward compatible with TLSv1.2• Open SSL version must be 3.0.12• TLS 1.1 and 1.0 support has been deprecated from SDM Release 9.0.3	SDM 9.3.0 Release Notes

Session Delivery Manager Software Distribution Media for Release 9.0.3 GA

The following files are available for Oracle Communications Session Delivery Manager, Release 9.0.3

Table 2-2 Software Distribution Media for Release 9.0.3

File	Description
NNC903_OracleLinux70_64bit.tar.gz	Oracle Linux operating system version 7.0 to 7.9, 64 bit installation file package.
NNC903_OracleLinux80_64bit.tar.gz	Oracle Linux operating system version 8.0 to 8.9, 64 bit installation file package.
NNC903_RESTClient.zip	NNC9.0.3 REST client zip file.
MIBS_NNC903.zip	NNC9.0.3 Release MIBs zip file, which contains the latest ap-nnc.mib and ap-ems.mib that provide SNMP support for Oracle Communications Session Delivery Manager. This distribution media supersedes previous versions that were released with your device software.
sp_edge_core17.0_Package.zip	The Session Element Manager application provided in this package supports the following components: <ul style="list-style-type: none"> • Session Border Controller (SBC) • Session Router (SR) • Session Load Balancer (SLB) • Core Session Manager (CSM) • Subscriber-aware Load Balancing and Route Management (SLRM) • Mobile Security Gateway (MSG)
ent_edge_core17.0_Package.zip	The Session Element Manager application provided in this package supports the following components: <ul style="list-style-type: none"> • Enterprise Session Border Controller (ESBC) • Enterprise Communications Broker (ECB)
ent_utilities17.0_Package.zip	The Session Element Manager application provided in this package supports the following components: <ul style="list-style-type: none"> • Enterprise Operations Monitor (EOM) • Interactive Session Recorder (ISR) • Fraud Monitor (FDP)

Session Element Manager Plug-in Support Matrix for 9.0.3

Use the following table to determine Oracle Communications Session Delivery Manager (SDM) release compatibility that was introduced in OCSDM release 9.0.3. Oracle Communications Session Delivery Manager and Oracle Communications Session Element Manager Plug-in Release Compatibility.

The following table describes plug-ins support for the OCSDM 9.0.3 Release.

OCSDM Release	OCSEM Plug-in Name	OCSEM Plug-in Release
9.0.3	<ul style="list-style-type: none"> • SP Edge and Core • Enterprise Edge and Core • Enterprise Utilities 	17.0



Note:

All plug-ins inherit the support of the previous release.

Device Platform Support For Oracle Communications Session Element Manager Plug-ins

The table describes each device platform and what OCSEM plug-ins support this platform.

Device Platform	SP Edge and Core	Enterprise Edge and Core	Enterprise Utilities
Acme Packet 1100	No	Yes	No
Acme Packet 3820	Yes	No	No
Acme Packet 3900	Yes	Yes	No
Acme Packet 4600	Yes	Yes	No
Acme Packet 6100	Yes	No	No
Acme Packet 6300	Yes	Yes	No
Acme Packet 6350	Yes	Yes	No
Acme Packet Session Director - Server Edition	Yes	No	No
Acme Packet Session Director - Virtual Machine Edition	Yes	No	No
Acme Packet Enterprise Session Director - Server Edition	No	Yes	No
Acme Packet Enterprise Session Director - Virtual Machine Edition	No	Yes	No
Oracle Enterprise Interactive Session Recorder (ISR)	No	No	Yes
Oracle Enterprise Operations Monitor (EOM)	No	No	Yes
Enterprise Communications Broker (ECB)	No	Yes. Not supported by Report Manager and Route Manager	No
Acme Packet 3950	Yes	Yes	No
Acme Packet 4900	Yes	Yes	No

Note:

The software and the platform versions listed above will not be supported by SDM if the Platforms have reached End of Life.

Session Element Manager Plug-in Device Software Support for 9.0.3

The following table describes device software support for the Oracle Communications Session Element Manager plug-in releases supporting OCSDM 9.0.3.

OCSEM Plug-in Name	Release Introduced	Latest Releases Supported
SP Edge and Core	17.0	<ul style="list-style-type: none"> • SCz 930 • SCz 920 p1 • SCz 920 p2 • SCz 920 p3 • SCz 920 p4 • SCz 920 p5 • SCz 910 p7 • SCz 910 p8 • SCz 910 p10 • SCz 900 p10
Enterprise Edge and Core	17.0	<ul style="list-style-type: none"> • SCz 930 • SCz 920 p1 • SCz 920 p2 • SCz 920 p3 • SCz 920 p4 • SCz 920 p5 • SCz 910 p7 • SCz 910 p8 • SCz 910 p10 • SCz 900 p10 • PCz 400 p5 • PCz 400 p6 • PCz 400 p7 • PCz 410 p1 • PCz 410 p2 • PCz 410 p3 • PCz 420 • PCz 330 p10
Enterprise Utilities	17.0	<ul style="list-style-type: none"> • ISR • EOM • Oracle Fraud Detection and Prevention (FDP)

SDM Release 9.0.3.0.1

The following topics provide descriptions, explanations, and configuration information for the contents of Release 9.0.3.0.1.

Session Delivery Manager Software Distribution Media for Release 9.0.3.0.1 GA

The following files are available for Oracle Communications Session Delivery Manager, Release 9.0.3.0.1

Table 2-3 Software Distribution Media for Release 9.0.3.0.1

File	Description
NNC903_01OracleLinux70_64bit.tar.gz	Oracle Linux operating system version 7.x 64 bit - latest version installation file package.

Table 2-3 (Cont.) Software Distribution Media for Release 9.0.3.0.1

File	Description
NNC903_01OracleLinux80_64bit.tar.gz	Oracle Linux operating system version 8.x 64 bit - latest version installation file package.
NNC903_01RESTClient.zip	NNC9.0.3.0.1 REST client zip file.
MIBS_NNC903_01.zip	NNC9.0.3.0.1 Release MIBs zip file, which contains the latest ap-nnc.mib and ap-ems.mib that provide SNMP support for Oracle Communications Session Delivery Manager. This distribution media supersedes previous versions that were released with your device software.
sp_edge_core18.0_Package.zip	The Session Element Manager application provided in this package supports the following components: <ul style="list-style-type: none"> • Session Border Controller (SBC) • Session Router (SR) • Session Load Balancer (SLB) • Core Session Manager (CSM) • Subscriber-aware Load Balancing and Route Management (SLRM) • Mobile Security Gateway (MSG)
ent_edge_core18.0_Package.zip	The Session Element Manager application provided in this package supports the following components: <ul style="list-style-type: none"> • Enterprise Session Border Controller (ESBC) • Enterprise Communications Broker (ECB)
ent_utilities18.0_Package.zip	The Session Element Manager application provided in this package supports the following components: <ul style="list-style-type: none"> • Enterprise Operations Monitor (EOM) • Interactive Session Recorder (ISR) • Fraud Monitor (FDP)

Session Element Manager Plug-in Support Matrix for 9.0.3.0.1

Use the following table to determine Oracle Communications Session Delivery Manager (SDM) release compatibility that was introduced in OCSDM release 9.0.3.0.1. Oracle Communications Session Delivery Manager and Oracle Communications Session Element Manager Plug-in Release Compatibility.

The following table describes plug-ins support for the OCSDM 9.0.3.0.1 Release.

OCSDM Release	OCSEM Plug-in Name	OCSEM Plug-in Release
9.0.3.0.1	<ul style="list-style-type: none"> • SP Edge and Core • Enterprise Edge and Core • Enterprise Utilities 	18.0



Note:

All plug-ins inherit the support of the previous release.

Device Platform Support For Oracle Communications Session Element Manager Plug-ins

For more information on device platforms and the supported OCSEM plug-ins, refer to [Session Element Manager Plug-in Support Matrix for 9.0.3](#)

3

Release 9.0.2

The following topics provide descriptions, explanations, and configuration information for the contents of Release 9.0.2.

Unless otherwise stated, requirements and other release information is identical to 9.0 GA, noted in the other chapter of this document.

Release 9.0.2 Features

New Features in the SDM 9.0.2 Release.

The following table describes the Release 9.0.2 features for Oracle Communications Session Delivery Manager (OCSDM).

Table 3-1 This table lists and describes the 9.0.2 features

Feature	Description	Where Documented
Support for Route Sets and Routes of the type Range.	SDM 9.0.2 allows you to perform addition of Route Sets and their corresponding routes of type Range. Additionally, SDM 9.0.2 allows you to retrieve LRT files of type Range and import Routes of the type Range from a CSV file by using both GUI and REST API	RTM 9.0 User Guide
Increase password reuse count range	In SDM 9.0.2, the password reuse count range has been set to 0-12. This is an increase from 10 to 12.	Release Notes
Oracle Linux Support	SDM 9.0.2 supports Oracle Linux version 8.7.	Release Notes
JDK Upgrade Description	With SDM 9.0.2, JDK has been upgraded from 1.8u341 to 1.8u361.	Release Notes

Session Delivery Manager Software Distribution Media for Release 9.0.2 GA

The following files are available for Oracle Communications Session Delivery Manager, Release 9.0.2

Table 3-2 Software Distribution Media for Release 9.0.2

File	Description
NNC90_2OracleLinux65_64bit.tar.gz	Oracle Linux operating system version 6.5 to 6.9, 64 bit installation file package.

Table 3-2 (Cont.) Software Distribution Media for Release 9.0.2

File	Description
NNC90_2OracleLinux70_64bit.tar.gz	Oracle Linux operating system version 7.0 to 7.9, 64 bit installation file package.
NNC90_2OracleLinux80_64bit.tar.gz	Oracle Linux operating system version 8.0 to 8.7, 64 bit installation file package.
NNC90_2RESTClient.zip	NNC9.0.2 REST client zip file.
MIBS_NNC90_2.zip	NNC9.0.2 release MIBs zip file, which contains the latest ap-nnc.mib and ap-ems.mib that provide SNMP support for Oracle Communications Session Delivery Manager. This distribution media supersedes previous versions that were released with your device software.
sp_edge_core14.0_Package.zip	The Session Element Manager application provided in this package supports the following components: <ul style="list-style-type: none"> • Session Border Controller (SBC) • Session Router (SR) • Session Load Balancer (SLB) • Core Session Manager (CSM) • Subscriber-aware Load Balancing and Route Management (SLRM) • Mobile Security Gateway (MSG)
ent_edge_core14.0_Package.zip	The Session Element Manager application provided in this package supports the following components: <ul style="list-style-type: none"> • Enterprise Session Border Controller (ESBC) • Enterprise Communications Broker (ECB)
ent_utilities14.0_Package.zip	The Session Element Manager application provided in this package supports the following components: <ul style="list-style-type: none"> • Enterprise Operations Monitor (EOM) • Interactive Session Recorder (ISR) • Fraud Monitor (FDP)

Session Element Manager Plug-in Support Matrix for 9.0.2

Use the following table to determine Oracle Communications Session Delivery Manager (SDM) release compatibility that was introduced in OCSDM release 9.0.2. Oracle Communications Session Delivery Manager and Oracle Communications Session Element Manager Plug-in Release Compatibility

The following table describes plug-ins support for the OCSDM 9.0.2 release.

OCSDM Release	OCSEM Plug-in Name	OCSEM Plug-in Release
9.0.2	<ul style="list-style-type: none"> • SP Edge and Core • Enterprise Edge and Core • Enterprise Utilities 	14.0



Note:

All plugins inherit the support of the previous release.

Device Platform Support For Oracle Communications Session Element Manager Plug-ins

The table describes each device platform and what OCSEM plug-ins support this platform.

Device Platform	SP Edge and Core	Enterprise Edge and Core	Enterprise Utilities
Acme Packet 1100	No	Yes	No
Acme Packet 3820	Yes	No	No
Acme Packet 3900	Yes	Yes	No
Acme Packet 4600	Yes	Yes	No
Acme Packet 6100	Yes	No	No
Acme Packet 6300	Yes	Yes	No
Acme Packet 6350	Yes	Yes	No
Acme Packet Session Director - Server Edition	Yes	No	No
Acme Packet Session Director - Virtual Machine Edition	Yes	No	No
Acme Packet Enterprise Session Director - Server Edition	No	Yes	No
Acme Packet Enterprise Session Director - Virtual Machine Edition	No	Yes	No
Oracle Enterprise Interactive Session Recorder (ISR)	No	No	Yes
Oracle Enterprise Operations Monitor (EOM)	No	No	Yes
Enterprise Communications Broker (ECB)	No	Yes. Not supported by Report Manager and Route Manager	No
Acme Packet 3950	Yes	Yes	No
Acme Packet 4900	Yes	Yes	No

Note:

The software and the platform versions listed above will not be supported by SDM if the Platforms have reached End of Life.

Session Element Manager Plug-in Device Software Support for 9.0.2

The following table describes device software support for the Oracle Communications Session Element Manager plug-in releases supporting OCSDM 9.0.2.

OCSEM Plug-in Name	Release Introduced	Latest Releases Supported
SP Edge and Core	14.0	<ul style="list-style-type: none"> • SCz 9.2.0 • SCz.9.0.0 p7 • SCz 9.1.0 p5 • SCz 9.0.0 p6* • SCz 9.1.0 p4* • SCz 8.4.0 p14* <p>Note: * Supports only List View of the Configuration Manager.</p>
Enterprise Edge and Core	14.0	<ul style="list-style-type: none"> • SCz 9.2.0 • SCz 9.0.0 p7 • SCz 9.1.0 p5 • PCz 4.1.0 • SCz 9.0.0 p6* • SCz 9.1.0 p4* • SCz 8.4.0 p14* • PCz 3.3.0 p8* • PCz 3.3.0 p9* • PCz 4.0.0 p2* • PCz 4.0.0 p3* <p>Note: * Supports only List View of the Configuration Manager.</p>
Enterprise Utilities	14.0	<ul style="list-style-type: none"> • ISR • EOM • Oracle Fraud Detection and Prevention (FDP)

SDM Release 9.0.2.0.1

The following topics provide descriptions, explanations, and configuration information for the contents of Release 9.0.2.0.1.

Session Delivery Manager Software Distribution Media for Release 9.0.2.0.1 GA

The following files are available for Oracle Communications Session Delivery Manager, Release 9.0.2.0.1

Table 3-3 Software Distribution Media for Release 9.0.2.0.1

File	Description
NNC902_01OracleLinux65_64bit.tar.gz	Oracle Linux operating system version 6.5 to 6.9, 64 bit installation file package.
NNC902_01OracleLinux70_64bit.tar.gz	Oracle Linux operating system version 7.0 to 7.9, 64 bit installation file package.
NNC902_01OracleLinux80_64bit.tar.gz	Oracle Linux operating system version 8.0 to 8.7, 64 bit installation file package.
NNC902_01RESTClient.zip	NNC9.0.2.1 REST client zip file.

Table 3-3 (Cont.) Software Distribution Media for Release 9.0.2.0.1

File	Description
MIBS_NNC902_01.zip	NNC9.0.2.1 Release MIBs zip file, which contains the latest ap-nnc.mib and ap-ems.mib that provide SNMP support for Oracle Communications Session Delivery Manager. This distribution media supersedes previous versions that were released with your device software.
sp_edge_core15.0_Package.zip	The Session Element Manager application provided in this package supports the following components: <ul style="list-style-type: none"> • Session Border Controller (SBC) • Session Router (SR) • Session Load Balancer (SLB) • Core Session Manager (CSM) • Subscriber-aware Load Balancing and Route Management (SLRM) • Mobile Security Gateway (MSG)
ent_edge_core15.0_Package.zip	The Session Element Manager application provided in this package supports the following components: <ul style="list-style-type: none"> • Enterprise Session Border Controller (ESBC) • Enterprise Communications Broker (ECB)
ent_utilities15.0_Package.zip	The Session Element Manager application provided in this package supports the following components: <ul style="list-style-type: none"> • Enterprise Operations Monitor (EOM) • Interactive Session Recorder (ISR) • Fraud Monitor (FDP)

Session Element Manager Plug-in Support Matrix for 9.0.2.0.1

Use the following table to determine Oracle Communications Session Delivery Manager (SDM) release compatibility that was introduced in OCSDM release 9.0.2.0.1. Oracle Communications Session Delivery Manager and Oracle Communications Session Element Manager Plug-in Release Compatibility.

The following table describes plug-ins support for the OCSDM 9.0.2.0.1 release.

OCSDM Release	OCSEM Plug-in Name	OCSEM Plug-in Release
9.0.2.0.1	<ul style="list-style-type: none"> • SP Edge and Core • Enterprise Edge and Core • Enterprise Utilities 	15.0

Note:

All plug-ins inherit the support of the previous release.

Device Platform Support For Oracle Communications Session Element Manager Plug-ins

For more information on device platforms and the supported OCSEM plug-ins, refer to [Session Element Manager Plug-in Support Matrix for 9.0.2](#).

SDM Release 9.0.2.0.2

The following topics provide descriptions, explanations, and configuration information for the contents of Release 9.0.2.0.2.

Session Delivery Manager Software Distribution Media for Release 9.0.2.0.2 GA

The following files are available for Oracle Communications Session Delivery Manager, Release 9.0.2.0.2

NOT_SUPPORTED:

Starting with the SDM 9.0.2.0.2 Release, support for Oracle Linux 6 has been removed. Hence, the related package - **NNC902_02OracleLinux65_64bit.tar.gz** has not been included in this SDM 9.0.2.0.2 Release.

SDM Release 9.0.2.0.2 supports only the following Operating systems:

1. Oracle Linux 7 (including its sub versions)
2. Oracle Linux 8 (including its sub versions)

Table 3-4 Software Distribution Media for Release 9.0.2.0.2

File	Description
NNC902_02OracleLinux70_64bit.tar.gz	Oracle Linux operating system version 7.0 to 7.9, 64 bit installation file package.
NNC902_02OracleLinux80_64bit.tar.gz	Oracle Linux operating system version 8.0 to 8.9, 64 bit installation file package.
NNC902_02RESTClient.zip	NNC9.0.2.0.2 REST client zip file.
MIBS_NNC902_02.zip	NNC9.0.2.0.2 Release MIBs zip file, which contains the latest ap-nnc.mib and ap-ems.mib that provide SNMP support for Oracle Communications Session Delivery Manager. This distribution media supersedes previous versions that were released with your device software.
sp_edge_core16.0_Package.zip	The Session Element Manager application provided in this package supports the following components: <ul style="list-style-type: none"> • Session Border Controller (SBC) • Session Router (SR) • Session Load Balancer (SLB) • Core Session Manager (CSM) • Subscriber-aware Load Balancing and Route Management (SLRM) • Mobile Security Gateway (MSG)
ent_edge_core16.0_Package.zip	The Session Element Manager application provided in this package supports the following components: <ul style="list-style-type: none"> • Enterprise Session Border Controller (ESBC) • Enterprise Communications Broker (ECB)

Table 3-4 (Cont.) Software Distribution Media for Release 9.0.2.0.2

File	Description
ent_utilities16.0_Package.zip	The Session Element Manager application provided in this package supports the following components: <ul style="list-style-type: none"> • Enterprise Operations Monitor (EOM) • Interactive Session Recorder (ISR) • Fraud Monitor (FDP)

Session Element Manager Plug-in Support Matrix for 9.0.2.0.2

Use the following table to determine Oracle Communications Session Delivery Manager (SDM) release compatibility that was introduced in OCSDM release 9.0.2.0.2. Oracle Communications Session Delivery Manager and Oracle Communications Session Element Manager Plug-in Release Compatibility.

The following table describes plug-ins support for the OCSDM 9.0.2.0.2 release.

OCSDM Release	OCSEM Plug-in Name	OCSEM Plug-in Release
9.0.2.0.2	<ul style="list-style-type: none"> • SP Edge and Core • Enterprise Edge and Core • Enterprise Utilities 	16.0



Note:

All plug-ins inherit the support of the previous release.

Device Platform Support For Oracle Communications Session Element Manager Plug-ins

For more information on device platforms and the supported OCSEM plug-ins, refer to [Session Element Manager Plug-in Support Matrix for 9.0.2.](#)

4

Release 9.0.1

The following topics provide descriptions, explanations, and configuration information for the contents of Release 9.0.1. Unless otherwise stated, requirements and other release information is identical to 9.0 GA, noted in the other chapter of this document.

Release 9.0.1 Features

New Features in the Oracle Communications Session Delivery Manager 9.0.1 Release.

The following table describes the Release 9.0.1 features for Oracle Communications Session Delivery Manager (OCSDM).

Table 4-1 This table lists and describes the 9.0.1 features

Feature	Description	Where Documented
JDK Upgrade	With SDM 9.0.1, JDK has been upgraded from 1.8u321 to 1.8u341.	Release Notes
Oracle Linux support	SDM 9.0.1 supports Oracle Linux version 8.6.	Release Notes, and Installation Guide.
RMI feature enhancement with SDM 9.0.1	This feature introduces a new option <code>RMI over SSL</code> under all OCSDM main set up options such as, Typical, Custom and Easy-Install. Starting with SDM.9.0.1, by default, RMI ports 1099 and 1098 are secured using SSL connections.	Installation Guide

Session Delivery Manager Software Distribution Media for Release 9.0.1 GA

The following files are available for Oracle Communications Session Delivery Manager, Release 9.0.1

Table 4-2 Software Distribution Media for Release 9.0.1

File	Description
NNC901OracleLinux65_64bit.tar.gz	Oracle Linux operating system version 6.5 to 6.9, 64 bit installation file package.
NNC901OracleLinux70_64bit.tar.gz	Oracle Linux operating system version 7.0 to 7.9, 64 bit installation file package.
NNC901OracleLinux80_64bit.tar.gz	Oracle Linux operating system version 8.0 to 8.6, 64 bit installation file package.

Table 4-2 (Cont.) Software Distribution Media for Release 9.0.1

File	Description
NNC901RESTClient.zip	NNC9.0.1 REST client zip file.
MIBS_NNC901.zip	NNC9.0.1 release MIBs zip file, which contains the latest ap-nnc.mib and ap-ems.mib that provide SNMP support for Oracle Communications Session Delivery Manager. This distribution media supersedes previous versions that were released with your device software.
sp_edge_core13.0_Package.zip	The Session Element Manager application provided in this package supports the following components: <ul style="list-style-type: none"> • Session Border Controller (SBC) • Session Router (SR) • Session Load Balancer (SLB) • Core Session Manager (CSM) • Subscriber-aware Load Balancing and Route Management (SLRM) • Mobile Security Gateway (MSG)
ent_edge_core13.0_Package.zip	The Session Element Manager application provided in this package supports the following components: <ul style="list-style-type: none"> • Enterprise Session Border Controller (ESBC) • Enterprise Communications Broker (ECB)
ent_utilities13.0_Package.zip	The Session Element Manager application provided in this package supports the following components: <ul style="list-style-type: none"> • Enterprise Operations Monitor (EOM) • Interactive Session Recorder (ISR) • Fraud Monitor (FDP)

Session Element Manager Plug-in Support Matrix for 9.0.1

Use the following table to determine Oracle Communications Session Delivery Manager (SDM) release compatibility that was introduced in OCSDM release 9.0.1. Oracle Communications Session Delivery Manager and Oracle Communications Session Element Manager Plug-in Release Compatibility

The following table describes plug-ins support for the OCSDM 9.0.1 release.

OCSDM Release	OCSEM Plug-in Name	OCSEM Plug-in Release
9.0.1	<ul style="list-style-type: none"> • SP Edge and Core • Enterprise Edge and Core • Enterprise Utilities 	13.0



Note:

All plugins inherit the support of the previous release.

Device Platform Support For Oracle Communications Session Element Manager Plug-ins

The table describes each device platform and what OCSEM plug-ins support this platform.

Device Platform	SP Edge and Core	Enterprise Edge and Core	Enterprise Utilities
Acme Packet 1100	No	Yes	No
Acme Packet 3820	Yes	No	No
Acme Packet 3900	Yes	Yes	No
Acme Packet 4600	Yes	Yes	No
Acme Packet 6100	Yes	No	No
Acme Packet 6300	Yes	Yes	No
Acme Packet 6350	Yes	Yes	No
Acme Packet Session Director - Server Edition	Yes	No	No
Acme Packet Session Director - Virtual Machine Edition	Yes	No	No
Acme Packet Enterprise Session Director - Server Edition	No	Yes	No
Acme Packet Enterprise Session Director - Virtual Machine Edition	No	Yes	No
Oracle Enterprise Interactive Session Recorder (ISR)	No	No	Yes
Oracle Enterprise Operations Monitor (EOM)	No	No	Yes
Enterprise Communications Broker (ECB)	No	Yes. Not supported by Report Manager and Route Manager	No
Acme Packet 3950	Yes	Yes	No
Acme Packet 4900	Yes	Yes	No

 **Note:**

The software and the platform versions listed above will not be supported by SDM if the Platforms have reached End of Life.

Session Element Manager Plug-in Device Software Support for 9.0.1

The following table describes device software support for the Oracle Communications Session Element Manager plug-in releases supporting OCSDM 9.0.1.

OCSEM Plug-in Name	Release Introduced	Latest Releases Supported
SP Edge and Core	13.0	<ul style="list-style-type: none"> • S-Cz 9.1.5 • S-Cz 8.4.0 p12 • S-Cz 9.0.0 p4 * • S-Cz 9.1.0 p1* • S-Cz 9.1.0 p2 • S-CZ 9.1.0 p3 * <p>Note: * Supports only List View of the Configuration Manager.</p>
Enterprise Edge and Core	13.0	<ul style="list-style-type: none"> • S-Cz 8.4.0 p12 • S-Cz 9.0.0 p4 * • S-Cz 9.1.0 p1* • S-Cz 9.1.0 p2 • S-CZ 9.1.0 p3 * • P-Cz 3.3.0 p6 • P-Cz 3.3.0 p7* • P-Cz 4.0.0 <p>Note: * Supports only List View of the Configuration Manager.</p>
Enterprise Utilities	13.0	<ul style="list-style-type: none"> • ISR • EOM • Oracle Fraud Detection and Prevention (FDP)

5

Release 9.0.0

The following topics provide descriptions, explanations, and configuration information for the contents of Release 9.0.0.

Release 9.0.0 Features

New Features in the Oracle Communications Session Delivery Manager 9.0 Release.

The following table describes the Release 9.0.0 features for Oracle Communications Session Delivery Manager (OCSDM).

Table 5-1 This table lists and describes the 9.0.0 features

Feature	Description	Where Documented
JDK Upgrade	With SDM 9.0.0, JDK has been upgraded from 1.8u311 to 1.8u321	Release Notes

Session Delivery Manager Software Distribution Media for Release 9.0.0 GA

The following files are available for Oracle Communications Session Delivery Manager, Release 9.0.0

Table 5-2 Software Distribution Media for Release 9.0.0

File	Description
NNC90OracleLinux65_64bit.tar.gz	Oracle Linux operating system version 6.5 to 6.9, 64 bit installation file package.
NNC90OracleLinux70_64bit.tar.gz	Oracle Linux operating system version 7.0 to 7.9, 64 bit installation file package.
NNC90OracleLinux80_64bit.tar.gz	Oracle Linux operating system version 8.0 to 8.5, 64 bit installation file package.
NNC90RESTClient.zip	NNC9.0.0 REST client zip file.
MIBS_NNC90.zip	NNC9.0.0 release MIBs zip file, which contains the latest ap-nnc.mib and ap-ems.mib that provide SNMP support for Oracle Communications Session Delivery Manager. This distribution media supersedes previous versions that were released with your device software.

Table 5-2 (Cont.) Software Distribution Media for Release 9.0.0

File	Description
sp_edge_core11.0_Package.zip	The Session Element Manager application provided in this package supports the following components: <ul style="list-style-type: none"> • Session Border Controller (SBC) • Session Router (SR) • Session Load Balancer (SLB) • Core Session Manager (CSM) • Subscriber-aware Load Balancing and Route Management (SLRM) • Mobile Security Gateway (MSG)
ent_edge_core11.0_Package.zip	The Session Element Manager application provided in this package supports the following components: <ul style="list-style-type: none"> • Enterprise Session Border Controller (ESBC) • Enterprise Communications Broker (ECB)
ent_utilities11.0_Package.zip	The Session Element Manager application provided in this package supports the following components: <ul style="list-style-type: none"> • Enterprise Operations Monitor (EOM) • Interactive Session Recorder (ISR) • Fraud Monitor (FDP)

Session Element Manager Plug-in Support Matrix for 9.0.0

Use the following table to determine Oracle Communications Session Delivery Manager (SDM) release compatibility that was introduced in OCSDM release 9.0.0. Oracle Communications Session Delivery Manager and Oracle Communications Session Element Manager Plug-in Release Compatibility

The following table describes plug-ins support for the OCSDM 9.0.0 release.

OCSDM Release	OCSEM Plug-in Name	OCSEM Plug-in Release
9.0.0	<ul style="list-style-type: none"> • SP Edge and Core • Enterprise Edge and Core • Enterprise Utilities 	11.0



Note:

All plugins inherit the support of the previous release.

Device Platform Support For Oracle Communications Session Element Manager Plug-ins

The table describes each device platform and what OCSEM plug-ins support this platform.

Device Platform	SP Edge and Core	Enterprise Edge and Core	Enterprise Utilities
Acme Packet 1100	No	Yes	No
Acme Packet 3820	Yes	No	No

Device Platform	SP Edge and Core	Enterprise Edge and Core	Enterprise Utilities
Acme Packet 3900	Yes	Yes	No
Acme Packet 4500	Yes	Yes	No
Acme Packet 4600	Yes	Yes	No
Acme Packet 6100	Yes	No	No
Acme Packet 6300	Yes	Yes	No
Acme Packet 6350	Yes	Yes	No
Acme Packet Session Director - Server Edition	Yes	No	No
Acme Packet Session Director - Virtual Machine Edition	Yes	No	No
Acme Packet Enterprise Session Director - Server Edition	No	Yes	No
Acme Packet Enterprise Session Director - Virtual Machine Edition	No	Yes	No
Oracle Enterprise Interactive Session Recorder (ISR)	No	No	Yes
Oracle Enterprise Operations Monitor (EOM)	No	No	Yes
Enterprise Communications Broker (ECB)	No	Yes. Not supported by Report Manager and Route Manager	No
Acme Packet 3950	Yes	Yes	No
Acme Packet 4900	Yes	Yes	No



Note:

Platforms Acmepacket 3800, 3810, 4250 and 9200 have been deprecated and are out of support.

Session Element Manager Plug-in Device Software Support for 9.0.0

The following table describes device software support for the Oracle Communications Session Element Manager plug-in releases supporting OCSDM 9.0.0.

OCSEM Plug-in Name	Release Introduced	Latest Releases Supported
SP Edge and Core	11.0	<ul style="list-style-type: none"> • SCZ900p2 • SCZ900p3 • SCz9.1.0 • SCZ840p8A

OCSEM Plug-in Name	Release Introduced	Latest Releases Supported
Enterprise Edge and Core	11.0	<ul style="list-style-type: none">• SCZ900p2• SCZ900p3• SCZ910• SCZ840p8A• PCZ320p9• PCZ330p4
Enterprise Utilities	11.0	<ul style="list-style-type: none">• ISR• EOM• Oracle Fraud Detection and Prevention (FDP)

6

OCSDM Releases 8.2.5 to 8.2.1

This section provides information on the features, plug-ins and device support introduced in the OCSDM releases.

The OCSDM Releases listed are:

- OCSDM 8.2.5
- OCSDM 8.2.4
- OCSDM 8.2.3
- OCSDM 8.2.2
- OCSDM 8.2.1

Features in SDM Releases 8.2.5 to 8.2.1

This section provides a summary of the features introduced in the Releases SDM 8.2.5 to 8.2.1.

Features listed from Releases SDM 8.2.5 to 8.2.1.

Feature	Description	Where Documented
SDM 8.2.5 Release		
Log4J upgrade to 2.16	SDM 8.2.5 addresses CVE-2021-44228 and CVE-2021-45046, a remote code execution vulnerability, where Apache Log4J2 2.16.0 version has been applied.	Release Notes
View and save an audit log function	The downloaded CSV file is limited to 500 entries.	Administration Guide
JDK Upgrade	With SDM 8.2.5, JDK has been upgraded from 1.8u291 to 1.8u311	Release Notes
Oracle Linux support	SDM 8.2.5 supports Oracle linux version 8.4	Installation Guide
Fraud Protection List Data Type Formats	Phone numbers with a leading '+' Plus symbol are allowed	<ul style="list-style-type: none">• User Guide for Enterprise Utilities Plug-in• User Guide for the Enterprise Edge and Core Plug-in
SDM 8.2.4 Release		

Feature	Description	Where Documented
SBC Software image and Bootloader file integrity Check	OCSDM performs a file integrity check on software image file and bootloader file. OCSDM continues with the workorder to upgrade a target SBC only if the image file integrity check is positive. If the image file integrity check fails, then the upgrade process is aborted on that specific SBC and continues with the workorder to upgrade the next target SBC.	<ul style="list-style-type: none"> SDM 8.2.4 Release Notes
Route Manager LRT Support	<p>SDM 8.2.4 has new fields format, priority and weight for each route entry.</p> <p>In the GUI, format is a check box which can be toggled based on the user input. If it is checked, then both priority and weight attributes must be mentioned for each route to be added using SDM.</p> <p>SDM 8.2.4 supports the import and export of the Priority and Weight fields from a CSV file or an existing LRT file.</p> <p>SDM 8.2.4 supports management of the fields Priority and Weight using the Route Manager northbound REST API interface.</p>	<ul style="list-style-type: none"> Session Route Manager User Guide
Restriction to Purge Audit Logs	SDM 8.2.4 restricts the number of days to retain audit logs by introducing a range of 2-90 days. This range is checked during manual purge and automatic purge.	<ul style="list-style-type: none"> Oracle Communications Session Delivery Manager Administration Guide.
JDK Upgrade	With SDM 8.2.4, JDK has been upgraded from from JDK 1.8u261 to JDK 1.8u291	<ul style="list-style-type: none"> SDM 8.2.4 Release Notes
SDM 8.2.3 Release		
Support for full FCAPS support for ECB.	The OCSDM 8.2.3 schema model provides the required Fault, Configuration, Auditing, Performance and Security FCAPS support for managing the Enterprise Communications Broker (ECB) devices. Configuration support, Performance support, and new Trap support have been introduced in addition to existing Traps support and Device manager support on release nnPCZ330.bz.	<ul style="list-style-type: none"> SDM 8.2.3 Release Notes

Feature	Description	Where Documented
Display of alphabets in device version and schema in OCSDM	SDM now allows the display of the complete patch version number to be incorporated with the device version. For example, Acme Packet 4600 SCZ8.3.0 MR-1 Patch 10 A (Build 542) which translates to SCZ830m1p10A, is displayed as device version on the GUI and retained as is for all the modules in SDM.	SDM 8.2.3 Release Notes
Bootloader Upgrade with R226 license enabled	Starting with SCz8.4, when the R226 license is enabled, users cannot modify or list files from the '/boot' directory using external applications. New commands have been introduced to modify files in the '/boot' directory, and to provide support for the automated software and bootloader upgrades on the network function using OCSDM.	SDM 8.2.3 Release Notes
Route Manager LRT comment support	With SDM 8.2.3 a new field has been introduced to include descriptions for the individual route entries in a route set. SDM provides full support for the route level description field from the Web GUI, CSV provisioning and through REST interface.	Session Route Manager User Guide
Removing Flash Player graph and chart	31 December 2020 was the end-of-life for the Flash Player. Charts and graphs using the Flash player have been removed and tabular data is now made available for the following: <ul style="list-style-type: none"> • Health Summary: Health Score in tabular format has been retained and Pie chart has been removed. • Alarms Summary: Bar graph has been removed and tabular format has been retained. 	<ul style="list-style-type: none"> • Service Provider Edge and Core Plug-in User Guide • Enterprise Edge and Core Plug-in User Guide
Deleting or adding a sub-element using the REST API	Using REST northbound API you can programmatically add, update, and delete the configuration sub-elements.	<ul style="list-style-type: none"> • REST API Guide • SDM 8.2.3 Release Notes

SDM 8.2.2 Release

Feature	Description	Where Documented
Golden Configuration Comparison and Report	Users of the Administrator and LI Administrator group can create and manage the Golden Configuration of a SDM-managed device to maintain the integrity of the network. SDM users can create, and manage a configuration comparison report. This report can be used to compare a device configuration with the master Golden Configuration. The deviations in the configuration are highlighted in the comparison report. Users can download the report as a PDF or GZIP file.	<ul style="list-style-type: none"> • Session Element Manager User Guide for Service Provider Edge & Core Plug-in • Session Element Manager User Guide for Enterprise Edge and Core Plug-in. <ul style="list-style-type: none"> – Updates the "Configuration Manager" and chapter.
OCSDM uses FQDN to launch the GUI	Configuring and accessing the GUI for ESBC, ECB, EOM, FDP, and ISR using an IP address (http/https) has been extended. OCSDM now allows managing SBC, ESBC, ECB, FDP, EOM, or ISR by using FQDN or IP address. You can configure OCSDM to use FQDN when connecting to the web GUI using http/https for ESBC, ECB, EOM, FDP and ISR. OCSDM can continue to manage SBC, ESBC, ECB, FDP, EOM, or ISR by preserving the current ability of managing the network function using the resolved IP address.	<ul style="list-style-type: none"> • Session Element Manager User Guide for Edge & Core Plug-in • Session Element Manager User Guide for Service Provider Edge & Core • Session Element Manager User Guide for the Enterprise Utilities Plug-in • Updates the "Device Manager" and chapter.
North Bound SNMPv3 support	In SDM, you can specify a Northbound interface for example, a network management system to receive the SNMP traps. With SDM 8.2.2, SNMPv3 is supported to forward traps to the Northbound interface. The SNMPv3 protocol provides authentication, privacy, access control, and address security vulnerabilities over SNMPv2.	<ul style="list-style-type: none"> • Session Delivery Manager Administration Guide <ul style="list-style-type: none"> – Updates the chapter "Configure Northbound Interface Traps".
Enable access control on the server-side	The Security Manager component of SDM controls access and authorization through permissions granted to user groups. Server-side access control introduces permission checks for all the APIs. If an SDM user attempts to perform an unauthorized request, the action is recorded in the application logs.	<ul style="list-style-type: none"> • Session Delivery Manager Administrators Guide <ul style="list-style-type: none"> – Updates the chapter "Security Manager".

Feature	Description	Where Documented
Query user before replacing network function certificates	SDM 8.2.2 prevents the replacement of security certificate and private key of the target SBC(s) with the certificate, and security key of the SBC used to create the Offline Configuration. The Offline Configuration is associated to the device cluster and bulk configuration.	<ul style="list-style-type: none"> • Session Element Manager User Guide for the Enterprise Edge and Core Plug-in. • Updates the chapter "Use an Offline Configuration for a Device Cluster"
Using li-admin credentials to push li-configuration	SDM can now use the li-admin credentials over ACP or ACP/TLS to push LI-configuration to the SBC device enabled with LI license.	<ul style="list-style-type: none"> • Session Element Manager User Guide for the Service Provider Edge and Core Plug-in <ul style="list-style-type: none"> – Updates the chapter "Device Manager".
Fix for Adobe Flash Player end-of-life	SDM 8.2.2 removes the dependency on Adobe Flash Player. Alarms Summary is now provided as a table along with a graphical representation.	<ul style="list-style-type: none"> • Session Element Manager User Guide for the Service Provider Edge and Core Plug-in • Session Element Manager User Guide for the Enterprise Edge and Core Plug-in <ul style="list-style-type: none"> – Updates the chapter "Dashboard Manager".
SDM 8.2.1 Release SBC Bootloader Upgrade	Adds the ability to remotely upgrade the SBC bootloader image in addition to the SBC software image during software updates.	<ul style="list-style-type: none"> • Session Element Manager User Guide for Edge & Core Plug-in <ul style="list-style-type: none"> – Updates the "Configure and Apply Global Parameters to Devices" and "Configure and Apply a Software Upgrade to Devices" chapters. • Session Element Manager User Guide for Service Provider Edge & Core <ul style="list-style-type: none"> – Updates the "Configure and Apply Global Parameters to Devices" and "Configure and Apply a Software Upgrade to Devices" chapters.

Feature	Description	Where Documented
R226 Compliance	Eliminates the ability to view and edit both Lawful intercept (LI) and SIPREC configuration elements when running in R226 mode. Note: When R226 compliance is enabled, devices added with a LI encryption password can be managed by changing the device permissions via the Security Manager.	<ul style="list-style-type: none"> • Session Delivery Manager Installation Guide • Session Delivery Manager Administrators Guide • Session Delivery Manager Security Guide • Session Element Manager User Guide for Edge & Core Plug-in • Session Element Manager User Guide for Service Provider Edge & Core • Report Manager User Guide
Lawful Intercept Config Options	Restricts the ability to view and edit LI configuration elements to the Lladmin user.	<ul style="list-style-type: none"> • Release Notes
LDAP Filters Support	In addition to the existing mandatory LDAP parameters, the OCSDM now supports the following additional LDAP attributes and parameters: <ul style="list-style-type: none"> • base-dn • bind-dn • user-principal-name (userprincipalname) • sam-account-name (samaccountname) • organizational-unit-name (ou) • is-member-of-dl (memberof) 	<ul style="list-style-type: none"> • Session Delivery Manager Administrators Guide <ul style="list-style-type: none"> – Updates "Configuring Domain Controller Advanced Settings".
Audit Log Policy Enhancement	The audit log purging policy has been enhanced to always retain the last 48 hours of audit logs and cannot be configured to a lesser value.	<ul style="list-style-type: none"> • Session Delivery Manager Administrators Guide <ul style="list-style-type: none"> – Updates "Schedule Audit Log Files to be Purged Automatically" and "Purge Audit Log Files Manually".

Feature	Description	Where Documented
Multiple Interface Support	<p>OCSDM supports multiple interfaces as follows:</p> <ul style="list-style-type: none"> • Northbound interfaces: These are used by clients (for example, SOAP clients, GUI, REST clients) communicating with the OCSDM hosts. This communication includes REST, SOAP, Apache, SFTP, Ping, SNMP, RMI, and Java socket protocols. • Southbound interfaces: These are used by OCSDM hosts communicating to devices. This communication includes SFTP, FTP, SSH, Telnet Ping, SNMP, ACP, SOAP, and Java socket protocols. • Eastbound and Westbound interfaces: These are used by OCSDM hosts communicating to each host in an OCSDM cluster. This communication includes SFTP, Ping, RMI, and Java socket protocols. 	<ul style="list-style-type: none"> • Release Notes
IPv6 Support	<p>OCSDM supports IPv4 and IPv6 addresses for the following different interfaces:</p> <ul style="list-style-type: none"> • For both Northbound and Southbound interfaces, the OCSDM can have an IPv4 or IPv6 address for the NIC. If both virtual and physical interfaces are present, then IPv4 and IPv6 are supported for these interfaces. • For Eastbound and Westbound interfaces, the OCSDM can have an IPv4 or IPv6 address for any physical or virtual interface. 	<ul style="list-style-type: none"> • Release Notes

Plug-in Support Matrix for SDM 8.2.5 to 8.2.1 Releases

This section describes the OCSEM plug-ins introduced for each plug-in release.

Table 6-1 Plug-ins

OCSDM Release	OCSEM Plug-in Name	OCSEM Plug-in Release
8.2.5	<ul style="list-style-type: none"> • SP Edge and Core • Enterprise Edge and Core • Enterprise Utilities 	10.0

Table 6-1 (Cont.) Plug-ins

OCSDM Release	OCSEM Plug-in Name	OCSEM Plug-in Release
8.2.4	<ul style="list-style-type: none"> • SP Edge and Core • Enterprise Edge and Core • Enterprise Utilities 	9.0
8.2.3	<ul style="list-style-type: none"> • SP Edge and Core • Enterprise Edge and Core • Enterprise Utilities 	8.0
8.2.2	<ul style="list-style-type: none"> • SP Edge and Core • Enterprise Edge and Core • Enterprise Utilities 	5.0
8.2.1	<ul style="list-style-type: none"> • SP Edge and Core • Enterprise Edge and Core • Enterprise Utilities 	4.0

Plug-in Device Software Support for SDM 8.2.5 to 8.2.1 Releases

The following table describes device software support for the Oracle Communications Session Element Manager plug-in releases supporting OCSDM 8.2.5 to 8.2.1.

OCSEM Plug-in Name	Release Introduced	Latest Releases Supported
SDM 8.2.5 Release		
SP Edge and Core	10.0	<ul style="list-style-type: none"> • SCz9.0.0 • S-Cz8.4.0P5 • S-Cz8.4.0P4 • S-Cz8.3.0M1P13 • SCZ810M1P25C • S-Cz8.4.5
Enterprise Edge and Core	10.0	<ul style="list-style-type: none"> • SCz9.0.0 • S-Cz8.4.0P5 • S-Cz8.4.0P4 • ECZ810m1p25C • SCZ830M1P13 • PCZ330P1
Enterprise Utilities	10.0	<ul style="list-style-type: none"> • ISR • EOM • Oracle Fraud Detection and Prevention (FDP)
SDM 8.2.4 Release		
SP Edge and Core	9.0	<ul style="list-style-type: none"> • SCz9.0.0 • S-Cz8.4.0P5 • S-Cz8.4.0P4 • S-Cz8.3.0M1P13 • SCZ810M1P25C • S-Cz8.4.5

OCSEM Plug-in Name	Release Introduced	Latest Releases Supported
Enterprise Edge and Core	9.0	<ul style="list-style-type: none"> • SCz9.0.0 • S-Cz8.4.0P5 • S-Cz8.4.0P4 • ECZ810m1p25C • SCZ830M1P13 • PCZ330P1
Enterprise Utilities	9.0	<ul style="list-style-type: none"> • ISR • EOM • Oracle Fraud Detection and Prevention (FDP)
SDM 8.2.3 Release		
SP Edge and Core	8.0	<ul style="list-style-type: none"> • SCz830m1p10 • SCz8.4p2 • SCz8.4p3
Enterprise Edge and Core	8.0	<ul style="list-style-type: none"> • SCz830m1p10 • SCz8.4p2 • PCZ3.3.0 • SCz8.4p3
Enterprise Utilities	8.0	<ul style="list-style-type: none"> • ISR • EOM • Oracle Fraud Detection and Prevention (FDP)
SDM 8.2.2 Release		
SP Edge and Core	5.0	<ul style="list-style-type: none"> • S-Cz8.3.0M1P2 • S-Cz8.3.0M1P1 • SCZ8.4.0 • SZ825M1 • SCZ825P3 • SCZ830M1P8 • SCZ810M1P23
Enterprise Edge and Core	5.0	<ul style="list-style-type: none"> • S-Cz8.3.0M1P2 • S-Cz8.3.0M1P1 • SCZ830M1P8 • SCZ840 • ECZ810M1p23
Enterprise Utilities	5.0	<ul style="list-style-type: none"> • ISR • EOM • Oracle Fraud Detection and Prevention (FDP)
SDM 8.2.1 Release		
SP Edge and Core	4.0	<ul style="list-style-type: none"> • S-Cz8.3.0M1P2 • S-Cz8.3.0M1P1 • S-Cz8.3.0M1 • S-Cz8.2.5
Enterprise Edge and Core	4.0	<ul style="list-style-type: none"> • S-Cz8.3.0M1P2 • S-Cz8.3.0M1P1 • S-Cz8.3.0M1 • S-Cz8.2.5

OCSEM Plug-in Name	Release Introduced	Latest Releases Supported
Enterprise Utilities	4.0	<ul style="list-style-type: none">• ISR• EOM• Oracle Fraud Detection and Prevention (FDP)

7

Session Delivery Manager Installation

Use this chapter to quickly review Oracle Communications Session Delivery Manager system requirements, high-level prerequisites, and the required software distribution media that you must download before you install OCSDM on your system(s).

Refer to the *Oracle Communications Session Delivery Manager Installation Guide* for the following installation information:

- Perform pre-requisite tasks, such as configuring firewall settings, checking Linux support and Linux version dependencies, and ensuring that the `SDM_localhost` entry is configured in the Hosts File.
- Configure your NNCentral account.
- Choose the type of OCSDM installation that you want to do (Typical, Custom, Easy Install, Headless Install).
- Perform a new OCSDM installation or upgrade.
- Perform specific setup instructions for each OCSDM installation type.

Note:

If you are running any release prior to 7.5M3, you must upgrade to 7.5M3 before you can upgrade to 8.2. You must be running OCSDM Release 7.5M3, 8.0, 8.1, or 8.1.1 to upgrade to 8.2 (with 11g Oracle DB). You can upgrade to OCSDM 9.0 from OCSDM 8.x or 8.x.x.

Check System Requirements

Oracle has certified the following hardware and software server platforms, as well as client requirements, for use with Oracle Communications Session Delivery Manager.

Note:

Other hardware configurations might work with Oracle Communications Session Delivery Manager, but Oracle has verified the configurations listed here.

Oracle Communications Session Delivery Manager Server Requirements

- CPU: 4-core 2.1 GHz processor or better
- 16 GB RAM minimum, 24 GB RAM recommended
- 300 GB hard drive minimum

Supported Operating Systems

Oracle supports the following installations of Oracle Communications Session Delivery Manager:

- Oracle Linux 6.x 64-bit - latest version¹
- Oracle Linux 7.x 64 bit - latest version²
- Oracle Linux 8.x 64 bit - latest version.

Note:

TLS v1.3 is supported by Oracle Linux 8.x only.

Use the default OpenSSL version provided by Oracle Linux on your Linux server. This needs to be done to use the HTTPS service on the Apache web server to support the options to run HTTPS with Transport Layer Security (TLS) 1.0, 1.1, and 1.2. SDM is backward compatible with TLSv1.2. To check the version of OpenSSL on your system, run the following command:

```
openssl version
```

Starting with the SDM 9.0.2.0.2 and later versions, support for Oracle Linux 6 has been removed. Hence, the related package - **NNC<release_number>OracleLinux65_64bit.tar.gz** has not been included in this SDM Release 9.0.2.0.2 and later versions.

Oracle Communications Report Manager

Oracle supports the following installations of Oracle Communications Session Delivery Manager with Oracle Communications Report Manager:

- Oracle Communications Report Manager for Oracle Fusion Middleware 12c is supported on Oracle Linux 7.x 64-bit - latest version.
- Oracle Communications Report Manager for Oracle Fusion Middleware 12c is supported on Oracle Linux 8.x 64-bit - latest version.

Client Requirements

- Oracle recommends:
 - Microsoft Edge version 122 from SDM 9.0.3
 - Mozilla Firefox versions 43.3.1 and later
 - Google Chrome version 56 and later.
 - Internet Explorer version 11.0³
- A Flash player compatible with your browser that is installed locally.
- If the server is not part of your DNS domain, the hosts file on each client must be edited to include the host name and IP address of the Oracle Communications Session Delivery Manager server.

¹ Starting with the SDM 9.0.2.0.2, support for Oracle Linux 6.x versions has been removed.

² Ensure that you update older versions of Oracle Linux specifically Oracle Linux 7.0 through 7.3 to a newer version.

³ Internet Explorer is not supported from SDM 9.0.3.

Language Requirements

On the Linux server, ensure that the US English language UTF-8 character encoding method is specified.

Software Installation Prerequisites

Before you start the installation of Oracle Communications Session Delivery Manager you must check the following prerequisites.

Check that Work Orders are in a Committed State

If you are upgrading from the previous version of Oracle Communications Session Delivery Manager, you must check the status of scheduled work orders before you upgrade to OCSDM Release 9.0.

All work orders must be in a **Committed** state before you upgrade to OCSDM Release 9.0, because the migration of existing work orders on a server running OCSDM Release 8.x is not provided when you upgrade to OCSDM, Release 9.0. See your product plugin documentation for more information about placing your work orders into a **Committed** state.

Report Manager Installation

The following table provides a migration matrix for the Report Manager.



Note:

Currently, Oracle Communications Report Manager supports Oracle Fusion Middleware 12c only, and 11g is not supported.

Table 7-1 Migration Matrix

SDM Release with Oracle DB	SDM 8.2/9.0 Core	Report Manager 11g Migration	Report Manager 12c Migration	Report Manager 19c Migration
8.2.5 with 12c	Yes	Not Supported	Yes	No
8.2.5 with 19c	Yes	Not supported	No	Yes
9.0.0 with 12c	Yes	Not supported	Yes	No
9.0.0 with 19c	Yes	Not supported	No	Yes
9.0.1 with 12c	Yes	Not supported	Yes	No
9.0.1 with 19c	Yes	Not supported	No	Yes
9.0.2 with 12c	Yes	Not Supported	Yes	No
9.0.2 with 19c	Yes	Not Supported	No	Yes
9.0.3 with 12c	Yes	Not Supported	Yes	No
9.0.3 with 19c	Yes	Not Supported	No	Yes

If you are installing the Oracle Communications Session Delivery Manager product software for the first time or upgrading from a previous version, complete the instructions in the *Oracle Communications Session Delivery Manager Installation Guide* before installing Oracle Communications Report Manager.

Support Matrix for Report Manager, Oracle Database, and Oracle Linux

Table 7-2 Software Compatibility

Oracle Linux	Oracle Database	Oracle BI Publisher/Oracle Analytics Publisher
OL 6.x ¹	12c	12.2.1.4
OL 7.x	12c	12.2.1.4
OL 8.x	19c	12.2.1.4

¹ 1 SDM 9.0.3 does not support Oracle Linux 6.x.

8

Session Element Manager Features Delivered by the Service Provider Plug-in

The Service Provider (SP) Edge and Core plug-in (formerly called the AcmeSD plug-in) contains the Oracle Communications Session Element Manager (OCSEM) application, which is used to manage and optimize network infrastructure elements and their functions for the following:

- Oracle Communications Session Border Controller (SBC)
- Oracle Communications Subscriber-Aware Load Balancer (SLB)
- Oracle Communications Mobile Security Gateway (MSG)
- Oracle Communications Unified Session Manager (USM)
- Oracle Communications Core Session Manager (CSM)
- Subscriber-aware Load Balancing and Route Management (SLRM)
- Oracle Communications Session Router (OCSR)
- Product devices with comprehensive tools and applications on the OCSDM.

The OCSEM can also provision fault, configuration, accounting, performance, and security (FCAPS) support for managed devices. Upon installation of the plug-in, OCSEM sliders and any Report Manager and Route Manager co-product sliders appear. For information on supported sliders and devices, see *Oracle Communications Session Element Manager User Guide for the Service Provider Edge and Core Product Plug-in*.



Note:

The AcmeSD plug-in name changes to SP Edge and Core in its second version.

Session Element Manager Features Delivered by the Service Provider Edge and Core Plug-in Release

No SP Edge and Core plug-in features were added for this release.

9

Session Element Manager Features Delivered by the Enterprise Edge and Core Plug-in

The Enterprise Edge and Core plug-in (formerly called the Enterprise plug-in) contains the Oracle Communications Session Element Manager application, which is used to manage and optimize network infrastructure elements and their functions for the Oracle Enterprise Session Border Controller (E-SBC) and Oracle Enterprise Communications Broker (ECB) product devices with comprehensive tools and applications on the Oracle Communications Session Delivery Manager Oracle Communications Session Delivery Manager to provision fault, configuration, accounting, performance, and security (FCAPS) support for managed devices.

Once the plug-in is installed, Oracle Communications Session Element Manager sliders appear along with the Report Manager and Route Manager co-product sliders. Refer to the *Oracle Communications Session Element Manager User Guide for the Enterprise Edge and Core Product Plug-in* for more information about supported sliders and device support information.



Note:

The Enterprise plug-in name changes to Enterprise Edge and Core in its second version.

Session Element Manager Features Delivered by the Enterprise Edge and Core Plug-in

No Enterprise Edge and Core plug-in features were added for this release.

10

Session Element Manager Features Delivered by the Enterprise Utilities Plug-in

The Enterprise Utilities plug-ins contain the Oracle Communications Session Element Manager, which manages the Oracle Enterprise Interactive Session Recorder (ISR), Oracle Enterprise Operations Monitor Users (EOM), and Fraud Detection and Prevention (FDP) devices.

Once the plug-in is installed, Oracle Communications Session Element Manager sliders appear along with the Report Manager and Route Manager co-product sliders. Refer to the *Oracle Communications Session Element Manager User Guide for the Enterprise Utilities Product Plug-in* for more information about supported sliders and device support information.

Session Element Manager Features Delivered by the Enterprise Utilities Plug-in Release

The Enterprise Utilities plug-in has limited Oracle Communication Session Element Manager (OCSEM) support for the Oracle Communications Interactive Session Recorder (ISR), and the Oracle Enterprise Operations Monitor (EOM).

See the Oracle Communications Session Element Manager User Guide for the Enterprise Utilities Plug-in Release documentation for more information about adding ISR devices to Oracle Communications Session Element Manager, and launching the EOM login page from OCSEM to perform operations on the EOM.

No Enterprise Utilities plug-in features were added for this release.

11

Interface Changes

This chapter identifies interface changes for the REST APIs.

Starting with the SDM 9.0.1 Release onwards, changes have been introduced in the REST API Response payload using JSON format, and the Request and Response Payload using XML format.

Differences in REST Response - JSON Format

This chapter identifies interface changes for the REST APIs and SOAP APIs.

Use the table below to check the differences in the REST API JSON responses between the SDM 9.0.0 and 9.0.1 and later Releases.

Table 11-1 Differences in REST Response - JSON Format

Serial Number	REST APIs	REST Endpoints	SDM 9.0.0	SDM 9.0.1 and Later Releases	Remarks
1	Assign a Device to Element Manager for FCAPS	/rest/v1.3/configuration/devices	NA	"type": "restManagedDevice",	9.0.0 does not have "type" tag
2	Get Device Configuration Management Summary	/rest/v1.3/configuration/devices/ID1	NA	type: "restManagedDevice"	9.0.0 does not have "type" tag
3	Load a Configuration for a Targeted Device	/rest/v1.3/configuration/devices/ID1/loadConfig	NA	type: "restManagedDevice"	9.0.0 does not have "type" tag

Differences in REST Request - XML Format

Use the table below to check the differences in the REST API XML Request between SDM 9.0.0 release and SDM 9.0.1 and later releases.

Here is the list of REST APIs from SDM 9.0.0 and SDM 9.0.1 and later releases as examples.

Table 11-2 Differences in REST Request - XML Format

Serial Number	REST APIs	URL Examples	SDM 9.0.0	SDM 9.0.1 and Later Releases	Remarks
1	Add a configuration element	/rest/v1.3/ configuration/ deviceConfigs/ D1/ configElements/ add	"<configElement> <attributes> <attribute> <childrenElements> <childrenElement> <attributes> <attribute>"	"<configElement> <attributes> <childrenElements> <attributes>"	"9.0.0 has <attribute> inside <attributes>. 9.0.1 and later releases have only <attributes>. Similarly for childrenElements tag as well."
2	Delete a Configuration Element	/rest/v1.3/ configuration/ deviceConfigs/ D1/ configElements/ delete	"<configElement> <attributes> <attribute> <childrenElements> <childrenElement> <attributes> <attribute>"	"<configElement> <attributes> <childrenElements> <attributes>"	"9.0.0 has <attribute> inside of <attributes>. 9.0.1 and later releases have only <attributes>. Similarly for childrenElements tag as well."
3	Get a Configuration Element Instance	/rest/v1.3/ configuration/ deviceConfigs/ D1/ configElements/ retrieve	"<configElement> <attributes> <attribute> <childrenElements> <childrenElement> <attributes> <attribute>"	"<configElement> <attributes> <childrenElements> <attributes>"	"9.0.0 has <attribute> inside of <attributes>. 9.0.1 and later releases have only <attributes>. Similarly for childrenElements tag as well."
4	Update a Configuration Element	/rest/v1.3/ configuration/ deviceConfigs/ D3/ configElements/ update	"<configElement> <attributes> <attribute> <childrenElements> <childrenElement> <attributes> <attribute>"	"<configElement> <attributes> <childrenElements> <attributes>"	"9.0.0 has <attribute> inside of <attributes>. 9.0.1 and later releases have only <attributes>. Similarly for childrenElements tag as well."
5	Add an NF	/rest/v1.1/ inventory/ nfMgmt/nfs	" </nfType> <parameters> <parameter>"	" </nfType> <parameters>"	9.0.0 has extra tag <parameters> while 9.0.1 and later releases do not.

Table 11-2 (Cont.) Differences in REST Request - XML Format

Serial Number	REST APIs	URL Examples	SDM 9.0.0	SDM 9.0.1 and Later Releases	Remarks
6	Update NF Information	/rest/v1.1/inventory/nfMgmt/nfs/ID7/groups/ID7	"<parameters><parameter>"	<parameters>	9.0.0 has <parameters> and <parameter>, 9.0.1 and later releases have <parameters>

Differences in REST Response - XML Format

Use the table below to check the differences in the REST API XML response between the SDM 9.0.0 release and 9.0.1 and later releases.

Here is the list of REST APIs from the SDM 9.0.0 and SDM 9.0.1 and later releases listed as examples.

Table 11-3 Differences in REST Response - XML Format

Serial Number	REST APIs	URL Examples	SDM 9.0.0	SDM 9.0.1 and Later Releases	Remarks
1	Login	/rest/v1.3/admin/login	NA	NA	No change
2	Logout	/rest/v1.3/admin/logout	NA	NA	No change
3	Get Information on SDM Servers	/rest/v1.3/admin/serverInfo	"<serverInfo><clusterMembers><clusterMember><downTime>NA</downTime>"	"<serverInfo><clusterMembers><downTime>NA</downTime>"	9.0.0 has "clusterMembers" inside of "clusterMembers" but 9.0.1 and later releases only have "clusterMembers"
4	Add a configuration element	/rest/v1.3/configuration/deviceConfigs/ID1/configElements/add	"<configElement><attributes><attribute><childrenElements><childrenElement><attributes><attribute>"	"<configElement><attributes><childrenElements><attributes>"	"9.0.0 has <attribute> inside of <attributes>. 9.0.1 and later releases have only <attributes>. Similarly for childrenElements tag as well."
5	Assign a Device to Element Manager for FCAPS	/rest/v1.1/configuration/devices	NA	NA	No changes

Table 11-3 (Cont.) Differences in REST Response - XML Format

Serial Number	REST APIs	URL Examples	SDM 9.0.0	SDM 9.0.1 and Later Releases	Remarks
6	Create a Configuration Element	/rest/v1.1/ configuration/ deviceConfigs/I D1/ configElements/ create	"<configElemen t> <attributes> <attribute>"	"<configElemen t> <attributes>"	9.0.0 has an <attribute> inside of <attributes>. 9.0.1 and later releases have only <attributes>.
7	Delete a Configuration Element	/rest/v1.3/ configuration/ deviceConfigs/I D1/ configElements/ delete	NA	NA	No changes
8	Delete Pending Configuration Modifications	/rest/v1.1/ configuration/ deviceConfigs/I D1/ configurationCh anges	NA	NA	No changes
9	Get a Configuration Element Instance	/rest/v1.3/ configuration/ deviceConfigs/I D1/ configElements/ retrieve	"<configElemen t> <attributes> <attribute> <childrenElemen ts> <childrenElemen t> <attributes> <attribute>"	"<configElemen t> <attributes> <childrenElemen ts> <attributes>"	"9.0.0 has <attribute> inside of <attributes>. 9.0.1 and later releases have only <attributes>. Similarly for childrenElemen ts tag as well."
10	Get a List of Configuration Element Instances	/rest/v1.1/ configuration/ deviceConfigs/I D2/ configElements	"<configElemen ts> <configElement > <attributes> <attribute>"	"<configElemen ts> <configElement s> <attributes>"	No remarks
11	Get a List of Devices associated with Element Manager	/rest/v1.3/ configuration/ devices	"<devices> <device>"	"<devices> <devices>"	No remarks
12	Get a List of Top-level Configuration Element Types	/rest/v1.3/ configuration/ deviceConfigs/I D1/ elementTypes	"<elementTypes > <elementType> "	"<elementTypes > <types>"	No remarks

Table 11-3 (Cont.) Differences in REST Response - XML Format

Serial Number	REST APIs	URL Examples	SDM 9.0.0	SDM 9.0.1 and Later Releases	Remarks
13	Get additional Element Metadata	/rest/v1.1/ configuration/ deviceConfigs/ ID1/ elementTypes/ elementMetadata	"<elementMetadata> <attributeMetadata> <attributeMetadata>"	"<elementMetadata> <attributeMetadata> <attributeMetadata>"	No remarks
14	Get additional attribute Metadata	/rest/v1.3/ configuration/ deviceConfigs/ ID2/ elementTypes/ attributeMetadata	"<enumeratedValues> <enumeratedValue>deny</enumeratedValue> <enumeratedValue> <enumeratedValue>permit</enumeratedValue> </enumeratedValues>"	"<enumeratedValues>deny</enumeratedValues> <enumeratedValues> <enumeratedValues>permit</enumeratedValues>"	No remarks
15	Get Device Configuration Management Summary	/rest/v1.3/ configuration/ devices/ ID1/ loadConfig	NA	NA	No changes
16	Get Pending Configuration Modification	"<configurationChanges> <configurationChange>"	"<configurationChanges> <changedConfigElements>"	"<configurationChanges> <changedConfigElements>"	9.0.0 has subtag <configurationChange>, 9.0.1 and later releases have subtag <changedConfigElements>
17	Load a Configuration for a Targeted Device	/rest/v1.3/ configuration/ devices/ ID1/ loadConfig	NA	NA	No changes
18	Unassign a Device from Element Manager to Stop FCAPS	/rest/v1.1/ configuration/ devices/ ID3	NA	NA	No changes
19	Update a Configuration Element	/rest/v1.3/ configuration/ deviceConfigs/ ID3/ configElements/ update	"<configElement> <attributes> <attribute> <childrenElements> <childrenElement> <attributes> <attribute>"	"<configElement> <attributes> <childrenElements> <attributes>"	"9.0.0 has <attribute> inside of <attributes>. 9.0.1 and later releases have only <attributes>. Similarly for childrenElements tag as well."

Table 11-3 (Cont.) Differences in REST Response - XML Format

Serial Number	REST APIs	URL Examples	SDM 9.0.0	SDM 9.0.1 and Later Releases	Remarks
20	Update a Configuration Password	/rest/v1.3/configuration/deviceConfigs/ID3/util/encryptPassword	NA	NA	No changes
21	Update the Configuration on a Device	/rest/v1.3/configuration/deviceConfigs/ID3/configElements/update	"<configElement> <attributes> <attribute> <childrenElements> <childrenElement> <attributes> <attribute>"	"<configElement> <attributes> <childrenElements> <attributes>"	"9.0.0 has <attribute> inside of <attributes>. 9.0.1 and later releases have only <attributes>. Similarly for childrenElements tag as well."
22	Get a List of Alarms	/rest/v1.1/fault/alarms	NA	NA	No changes
23	Get a List of Northbound Trap Receivers	/rest/v1.1/fault/trapReceivers	<trapReceivers> <trapReceiver>	"<trapReceivers> <trapReceivers>"	9.0.0 has subtag <trapReceiver>, but 9.0.1 and later releases have it as <trapReceivers>
24	Get Information of a Targeted Northbound Trap Receiver	/rest/v1.1/fault/trapReceivers/ID1021	NA	NA	No changes
25	Initiate a Request for Synchronization of Events or Alarms	/rest/v1.1/fault/trapReceivers/ID1021/action	NA	NA	No changes
26	Get Device Information	/rest/v1.2/inventory/deviceMgmt/devices/ID3	<groupParameters> <groupParameter>	<groupParameters>	9.0.0 has <groupParameter> subtag, 9.0.1 and later releases have <groupParameters>
27	Get Device License Information	/rest/v1.2/inventory/deviceMgmt/devices/capabilities/entitlements	NA	NA	No changes

Table 11-3 (Cont.) Differences in REST Response - XML Format

Serial Number	REST APIs	URL Examples	SDM 9.0.0	SDM 9.0.1 and Later Releases	Remarks
28	Get Device Management Summary Information	/rest/v1.3/inventory/deviceMgmt/devices	"<devices><device>"	"<devices><devices>"	9.0.0 has subtag <device>, but 9.0.1 and later releases have it as <devices>
29	Lock or Unlock a Device	/rest/v1.3/inventory/deviceMgmt/devices/ID4/action	NA	NA	No changes
30	Add a Device Group	/rest/v1.2/inventory/deviceMgmt/deviceGroups	NA	NA	No changes
31	Delete a Device Group	/rest/v1.1/inventory/deviceMgmt/deviceGroups/ID3	NA	NA	No changes
32	Get Device Group Information	/rest/v1.2/inventory/deviceMgmt/deviceGroups/ID1	NA	NA	No changes
33	Get Existing Device Groups	/rest/v1.3/inventory/deviceMgmt/deviceGroups	"<deviceGroups><deviceGroup>"	"<deviceGroups><deviceGroups>"	9.0.0 has subtag <deviceGroup>, but 9.0.1 and later releases have it as <deviceGroups>
34	Update a Device Group	/rest/v1.1/inventory/deviceMgmt/deviceGroups/ID7	NA	NA	No change
35	Add an NF	/rest/v1.1/inventory/nfMgmt/nfs	"<nf> <groups><group>"	"<nf><children>"	9.0.0 has <groups> and <group>, 9.0.1 and later releases have the <children> tag.
36	Delete an NF	/rest/v1.1/inventory/nfMgmt/nfs/ID3	NA	NA	No changes

Table 11-3 (Cont.) Differences in REST Response - XML Format

Serial Number	REST APIs	URL Examples	SDM 9.0.0	SDM 9.0.1 and Later Releases	Remarks
37	Get a Targeted NF	/rest/v1.1/ inventory/ nfMgmt/nfs/ID3	"<nf> <groups> <group>"	"<nf> <children>"	9.0.0 has <groups> and <group>, 9.0.1 and later releases have <children> tag.
38	Get Information on an NF Group	/rest/v1.1/ inventory/ nfMgmt/nfs/ID7/ groups/ID7	" <parameters> <parameter>"	<parameters>	9.0.0 has <parameters> and <parameter>, 9.0.1 and later releases have <parameters>.
39	Get List of NFs in Device Management	/rest/v1.1/ inventory/ nfMgmt/nfs	"<deviceGroups > <deviceGroup> <parameters> <parameter>"	"<nfs> <nflist>"	Different tags in both. 9.0.0 has parameters and paramter as well.
40	Submit a Request to Resynchronize an NF	/rest/v1.1/ inventory/ nfMgmt/nfs/ID7/ groups	" <parameters> <parameter>"	<parameters>	9.0.0 has <parameters> and <parameter>, 9.0.1 and later releases have <parameters>.
41	Lock or Unlock a Devices	/rest/v1.3/ inventory/ deviceMgmt/ devices/ID4/ action	NA	NA	No changes
42	Move an NF to Another Device Group Parent	/rest/v1.1/ inventory/ nfMgmt/nfs/ID5	NA	NA	No changes
43	Submit a Request to Resynchronize an NF	/rest/v1.1/ inventory/ nfMgmt/nfs/ID7/ action	NA	NA	No changes
44	Update NF Information	/rest/v1.1/ inventory/ nfMgmt/nfs/ID7/ groups/ID7	" <parameters> <parameter>"	<parameters>	9.0.0 has <parameters> and <parameter>, 9.0.1 and later releases have <parameters>.
45	Get a Targeted category	/rest/v1.3/ inventory/ nfMgmt/ nfCategories/ID 1	" <nfTypes> <nfType>"	<nfTypes>	9.0.0 has <nfTypes> and <nfType>, 9.0.1 and later releases have <nfTypes>.

Table 11-3 (Cont.) Differences in REST Response - XML Format

Serial Number	REST APIs	URL Examples	SDM 9.0.0	SDM 9.0.1 and Later Releases	Remarks
46	Get Additional Category Metadata	/rest/v1.1/inventory/nfMgmt/nfCategories/ID1/nfTypes/Device%20Cluster	"<nfCategory><parameters><parameter>"	"<category><parameters>"	"9.0.0 has <nfCategory>, 9.0.1 and later releases have <category>. 9.0.0 has <parameters> and <parameter>, 9.0.1 and later releases have <parameters>."
47	Get Additional NF Metadata	/rest/v1.1/inventory/nfMgmt/nfCategories/ID1/nfTypes	"<nfTypes><nfType>"	"<nfTypes><nfTypes>"	9.0.0 has <nfTypes> and <nfType>, 9.0.1 and later releases have 2 <nfTypes>.
48	Get NF Supported product Categories	/rest/v1.1/inventory/nfMgmt/nfCategories	"<nfCategories>><nfCategory>"	"<nfCategories>><nfCategories>"	9.0.0 has <nfCategories> and <nfCategory>, 9.0.1 and later releases have 2 <nfCategories> tags.
49	Get All Plug-ins	/rest/v1.3/admin/plugins/	"<pluginInfo><pluginClusterMembers><pluginClusterMember>"	"<pluginInfos><clusterMembers>"	"9.0.0 has <pluginInfos> and <pluginInfo>, 9.0.1 and later releases have 2 <pluginInfos> tags. Also subtags in 9.0.0 are 2 <pluginClusterMembers> and <pluginClusterMember>, 9.0.1 and later releases have only <clusterMembers>"

Table 11-3 (Cont.) Differences in REST Response - XML Format

Serial Number	REST APIs	URL Examples	SDM 9.0.0	SDM 9.0.1 and Later Releases	Remarks
50	Get Plug-in Information	/rest/v1.1/admin/plugins/ID1	"<pluginInfo><pluginClusterMembers><pluginClusterMember>"	"<pluginInfo><clusterMembers>"	"Subtags in 9.0.0 are 2 <pluginClusterMembers> and <pluginClusterMember>, 9.0.1 and later releases have only <clusterMembers>"
51	Perform a Plug-in Action	/rest/v1.3/admin/plugins/ID2/action	NA	NA	No changes
52	Remove a Plug-in	/rest/v1.1/admin/plugins/ID1	NA	NA	No changes
53	Update Plug-in Information	/rest/v1.1/admin/plugins/ID1	"<pluginInfo><pluginClusterMembers><pluginClusterMember>"	"<pluginInfo><clusterMembers>"	"Subtags in 9.0.0 are 2 <pluginClusterMembers> and <pluginClusterMember>, 9.0.1 and later releases have only <clusterMembers>"
54	Upload a Plug-in	/rest/v1.1/admin/plugins/?file=	"<pluginInfo><pluginClusterMembers><pluginClusterMember>"	"<pluginInfo><clusterMembers>"	"Subtags in 9.0.0 are 2 <pluginClusterMembers> and <pluginClusterMember>, 9.0.1 and later releases have only <clusterMembers>"
55	Add a route to routeSet	/rest/v1.3/routeSets/1/entries	NA	NA	No changes
56	Add an associated device to a route set	/rest/v1.3/routeSets/1/devices	NA	NA	No changes
57	Commit/Rollback/Cancel a route set update	/rest/v1.3/routeSets/routeUpdates/ID3/action	NA	NA	No changes

Table 11-3 (Cont.) Differences in REST Response - XML Format

Serial Number	REST APIs	URL Examples	SDM 9.0.0	SDM 9.0.1 and Later Releases	Remarks
58	Create a new route set	/rest/v1.3/ routeSets	NA	NA	No changes
59	Delete a particular Route Set by Id	/rest/v1.3/ routeSets/2	NA	NA	No changes
60	Delete associated device from specified route set	/rest/v1.3/ routeSets/1/ devices/ID7	NA	NA	No changes
61	Delete Route Entry by ID	/rest/v1.3/ routeSets/1/ entries/ID1	NA	NA	No changes
62	Execute some action on CSV file import	/rest/v1.3/ routeSets/2/ importFile	NA	NA	No changes
63	Execute user action on Add route set task	/rest/v1.3/ routeSets/ tasks/30/action	NA	NA	No changes
64	GET all associated device from a particular route set	/rest/v1.3/ routeSets/1/ devices	"<associatedDevices> <associatedDevice>"	"<associatedDevices> <assocDevices>"	9.0.0 has <associatedDevice> subtag, while 9.0.1 and later releases have <assocDevices> subtag.
65	Get All Existing Route sets	/rest/v1.3/ routeSets	<routeSet>	<routeSets>	9.0.0 has <routeSet> subtag, while 9.0.1 and later releases have <routeSets> subtag.
66	Get ALL or subset of route entries from a particular route set	/rest/v1.3/ routeSets/1/ entries	NA	NA	No changes
67	Get all route updates on devices	/rest/v1.3/ routeSets/ routeUpdates	"<routeUpdateTasks> <routeUpdateTask>"	"<routeUpdateTaskList> <routeUpdateTaskList>"	9.0.0 has <routeUpdateTask> subtag, while 9.0.1 and later releases have <routeUpdateTaskList> subtag.
68	Get Route Entry by ID	/rest/v1.3/ routeSets/1/ entries/ID1	NA	NA	No changes

Table 11-3 (Cont.) Differences in REST Response - XML Format

Serial Number	REST APIs	URL Examples	SDM 9.0.0	SDM 9.0.1 and Later Releases	Remarks
69	Get Route Sets by specifying a Route Set Id	/rest/v1.3/routeSets/1	NA	NA	No changes
70	Get status of add route set task by restoring LRT from device	/rest/v1.3/routeSets/tasks/6?addMode=upload	NA	NA	No changes
71	Get status of update task by task id	/rest/v1.3/routeSets/routeUpdates/ID5	"<routeUpdateTaskDetails> <updateDeviceStatusList> <updateDeviceStatus>"	"<routeUpdateTaskDetails> <deviceStatusList>"	"9.0.0 has <updateDeviceStatusList> and subtag <updateDeviceStatus>, while 9.0.1 and later releases have only <deviceStatusList> subtag."
72	Get the list of templates on SDM Server	/rest/v1.3/routeSets/importTemplates	"<importTemplates> <importTemplates>"	"<importTemplates> <importTemplates>"	9.0.0 has <importTemplate> subtag, while 9.0.1 and later releases have <importTemplates> subtag.
73	Get the status of the file import task	/rest/v1.3/routeSets/2/importFile/85	<errorList/>	NA	Extra line <errorList/> coming in 9.0.0 response.
74	Import a CSV File in to route Set	/rest/v1.3/routeSets/2/importFile	NA	NA	No changes
75	Modify a particular route set	/rest/v1.3/routeSets/1	NA	NA	No changes
76	Modify Route Entry by Id	/rest/v1.3/routeSets/1/entries/ID1	NA	NA	No changes
77	POST to Lock/Unlock/OverrideLock a RouteSet	/rest/v1.3/routeSets/1/action	NA	NA	No changes
78	Update all associated SBC devices with specified route sets	/rest/v1.3/routeSets/devices/action	NA	NA	No changes

Table 11-3 (Cont.) Differences in REST Response - XML Format

Serial Number	REST APIs	URL Examples	SDM 9.0.0	SDM 9.0.1 and Later Releases	Remarks
79	Update specified SBC devices with specified route set	/rest/v1.3/routeSets/1/devices/action	NA	NA	No changes
80	Get User Account Information	/rest/v1.1/security/accountMgmt	NA	NA	No changes
81	Get User Information	/rest/v1.1/security/users/ID11	NA	NA	No changes
82	Get Users	/rest/v1.1/security/users	<user>	<users>	9.0.0 has main tag as <users> and subtag as <user>, 9.0.1 and later releases have both tags as <users>.
83	Deregister key performance indicators (KPIs) for devices	/rest/v1.1/performance/devices/kpis?devices=ID2	NA	NA	No changes
84	Display a list of device information that supports performance	/rest/v1.2/performance/devices	"<devices><device>"	"<devices><devices>"	9.0.0 has subtag <device>, but 9.0.1 and later releases have it as <devices>
85	Display the supported KPIs	/rest/v1.1/performance/devices/kpis?pluginKey=Oracle-SessionDelivery-AcmeSD&componentType=DUMMY_SAMPLE&platform=4500&softwareVersion=SCZ900	NA	NA	No changes
86	Register KPIs for devices	/rest/v1.3/performance/devices/kpis	NA	NA	No changes
87	Retrieve KPI statistics for devices	/rest/v1.3/performance/devices/kpis/stats	NA	NA	No changes

Table 11-3 (Cont.) Differences in REST Response - XML Format

Serial Number	REST APIs	URL Examples	SDM 9.0.0	SDM 9.0.1 and Later Releases	Remarks
88	Update registered KPIs for devices	/rest/v1.1/performance/devices/kpis	NA	NA	No changes

12

Resolved Known Issues and Known Issues in SDM 9.0

This chapter describes the known issues and caveats and limitations found in Oracle Communications Session Delivery Manager.

The following table provides the defect number, a description of the defect problem and any applicable workaround for a defect problem and what release the defect was found or fixed, and if the defect was closed because it was non-reproducible, or some other state. Refer to the Oracle external database (Bug DB) defect tool for more information about defect states.

Table 12-1 Known Issues

Defect Number	Description	Severity	Found In
35810068	<p>For Oracle Linux 7 you may encounter, libraries were missing error while running setup script as mentioned below.</p> <ul style="list-style-type: none"> • System Package Diagnostics • Error: Missing required shared library libicuuc.so.50 • Error: Missing required shared library libicudata.so.50 • Error: Missing required shared library libicui18n.so.50 • Setup encountered an error and cannot continue <p>Workaround:</p> <ol style="list-style-type: none"> 1. Install the rpm package libicu-50.2-4.e17_7.x86_64.rpm at the OS level, and start the servers. 2. Download the package libicu-50.2-4.e17_7.x86_64.rpm from the Internet 3. Execute the command: sudo rpm -libicu-50.2-4.e17_7.x86_64.rpm 	4	SDM 9.0.3

Table 12-1 (Cont.) Known Issues

Defect Number	Description	Severity	Found In
36376438	For an ECB device, a new dialing-context config element cannot be added directly under Geographic or Corporate through SDM. Workaround: Add the first-level elements under Geographic or Corporate through device ACLI or ECB GUI. The added element is shown in the SDM GUI and can be used to add further child elements for that parent through the SDM GUI.	4	SDM 9.0.3
36394319	For an ECB device, address of record and lookup queries are not available to configure in LDAP configuration, as multi-instance parameters are not supported under single instance sub-element in SDM. Workaround: Access or configure these elements through the ECB GUI.	4	SDM 9.0.3

Table 12-2 Resolved Known Issues

Defect Number	Description	Severity	Found In	Fixed In
36514777	Offline Configuration push from SDM to SBC fails when LI config is included	3	SDM 9.0.0	SDM 9.0.3.0.1
36710272	Monitors User group can modify elements	3	SDM 9.0.2.0.2	SDM 9.0.3.0.1
36568238	SBC upgrade to Cz920p5 fails	2	SDM 9.0.3	SDM 9.0.3.0.1
36518471	SDM API is using HTTP GET method with a request body		SDM 9.0.0	SDM 9.0.3.0.1
19735005	Import .CSV file having duplicate route entries with format or description is successful	4	SDM 9.0.0	SDM 9.0.3

Table 12-2 (Cont.) Resolved Known Issues

Defect Number	Description	Severity	Found In	Fixed In
36109899	SDM cannot be used to provision aethalgo in the SA object. "none" is sent, when "null" is expected.	3	SDM 9.0.0	SDM 9.0.3
32488346	SDM: RestAPI Configuration changes can be made through the Rest API if the device is associated to Sync OC in the GUI	3	SDM 8.2.0	SDM 9.0.3
35690707	SDM shows incorrect 10GE SFP speed	3	SDM 9.0.1	SDM 9.0.3
35679870	SDM : While changing the state of policy attribute via SDM, the sequences changes.	3	SDM 9.0.2	SDM 9.0.3
35191007	Issue in SNMP NB trap Forwarding for OCSDM format trap.	2	SDM 8.2.5	SDM 9.0.2.0.1
35351903	No dialog box is displayed to enter the number of seconds for auto refresh.	3	SDM 9.0.2	SDM 9.0.2.0.1
35669761	SDM 9.0.1 dashboard 'auto refresh' button generates java exception	3	SDM 9.0.1	SDM 9.0.2.0.1
35391955	Upgrade from 823 to 901 failed database migration. Manual migration successful	3	SDM 9.0.1	SDM 9.0.2.0.1
35430147	SDM displayed:"ConfigMgrImpl encountered a general error. Reason: java.lang.NullPointerException	4	SDM 9.0.1	SDM 9.0.2.0.1
35518243	Java Error When Trying to log in to SDM GUI	2	SDM 9.0.1	SDM 9.0.2.0.1

Table 12-2 (Cont.) Resolved Known Issues

Defect Number	Description	Severity	Found In	Fixed In
35519789	SDM is unable to update the subnet mask	3	SDM 9.0.1	SDM 9.0.2.0.1
35561648	Fraud protection issue in SDM 9.0.2 when file has xml.gz extension	2	SDM 9.0.2	SDM 9.0.2.0.1
35733216	SDM 9.0.2 Error Under Managed Devices JavaScript Exception	3	SDM 9.0.2	SDM 9.0.2.0.1
35733216	Not able to update local policy using REST/SDM	3	SDM 9.0.2	SDM 9.0.2.0.1
35708703	SBC upgrade using SDM failing when network function name has / character in it	2	SDM 9.0.0	SDM 9.0.2.0.1
35668410	Cluster SDM Fault Manager: No alarm showing for one SBC which is in HA after Factory reset.	2	SDM 9.0.0	SDM 9.0.2.0.1
34172758	Error seen when columns heading are clicked in SDM	3	SDM 9.0.0	SDM 9.0.2
34194867	SDM performance issues when displaying routes	2	SDM 8.2.1	SDM 9.0.2
34746577	SDM: SBC Platform 1100: Software Upgrade Fails in "failed to retrieve source images	3	SDM 9.0.0	SDM 9.0.2
35066307	nsep-stats-profile flag is not visible on CLI-View of SDM but visible on List-View	2	SDM 9.0.1	SDM 9.0.2
34701721	For a headless installation, the AOService is enabled to True and SDM fails to start.	3	SDM 8.2.5	SDM 9.0.1
33967236	SDM displays apSysMgmtAdmin AuditLog as unknown.	3	SDM 8.2.5	SDM 9.0.1

Table 12-2 (Cont.) Resolved Known Issues

Defect Number	Description	Severity	Found In	Fixed In
34478644	Unable to create collection group in Report Manager 9.0.	3	SDM 9.0.0	SDM 9.0.1
34047970	SDM security Audit - Missing Security-Relevant HTTP Headers (X-XSS-Protection).	3	SDM 8.2.5	SDM 9.0.1
34335076	JSON Structure on the REST API call modified.	2	SDM 8.2.5	SDM 9.0.1
34536222	local-subscriber-table and sip-authentication to take multiple entries	3	SDM 9.0.1	SDM 9.0.1
33911152	Could not convert date 1644814800000. ErrorCode:20003 when delete event by date criteria.	3	SDM 8.2.3	SDM 9.0.1
33967236	SDM displays apSysMgmtAdmin AuditLog as unknown.	3	SDM 8.2.5	SDM 9.0.1
33850239	SDM crashes with the reason 'too many Open files'. This issue has been observed in SDM 8.2.5, and it may also lead to Java Crash. It has been found that there was a leakage in resources.	2	SDM 8.2.5	SDM 9.0.0
33584427	SDM REST or SOAP allows invalid value to be set in SBC configuration.	3	SDM 8.2.4	SDM 8.2.5
33974166	Incremental updates from FDP device is not successful on SDM.	2	SDM 8.2.5	SDM 9.0.0

Table 12-2 (Cont.) Resolved Known Issues

Defect Number	Description	Severity	Found In	Fixed In
33557691	Acknowledged or Cleared alarms reappear as Acknowledged when an event reoccurs.	2	SDM 8.2.0	SDM 9.0.0
32917038	Unable to perform the config change using NNC when the configuration data size exceeded 16KB.	3	SDM 8.2.2	SDM 9.0.0
33799233	Software upgrade from SDM GUI fails when R226 is enabled and if Source or target version has Alphabet at the end of version	3	SDM 8.2.4	SDM 9.0.0
33768487	SDM allows to retrieve device LRT file with user type as Range.	3	SDM 9.0.0	SDM 9.0.0

Caveats and Limitations

The following sections lists known or reported issues that are either expected behavior or will not be fixed in future releases:

Caveats for Oracle Communications Session Delivery Manager

- **Caveats for SDM 9.0.3**

ID: 36775286 While creating a work order in SDM, the date and time for scheduling the work order represented by 'Start date and time' corresponds to the client browser time. But when we apply the work order, this time is converted to SDM server time in the background. The SDM user interface work order table displays the server time.

ID: 36419110

When a new attribute or element supported only by that version is set, for example, restricted-latching is set to "sdp-ip-port" which is supported by SCz 9.3.0, after a downgrade or upgrade the updated values are not seen on config backup or dataDoc xml files. This causes loading of the device on SDM to fail.

Workaround: The attribute or element needs to be explicitly set to the value it supports on the current version using ACLI, save-activate. After this, load the device using SDM GUI.

- **Caveats for ECB 4.1.0**

1. The nsep-media-policy attribute located under 'media-manager->realm-config->nsep-media-policy' must be hidden.
2. The following attribute and sub-element must be hidden:
 - system->phy-interface->auto-negotiation' attribute
 - system->phy-interface->network-alarm-threshold sub-element

- **Caveats for SDM 9.0.2**

- Software upgrade from the SDM GUI fails for HA pair devices from versions **SCz910p6**, **SCz900p8** and **SCz900p9** only. For more information, see find Knowledge Document # [2952935.1](#).
- The validations for the ntp-sync/ntp-config configuration are specifically done at the device end and deliberately bypassed in SDM.
- **Caveats for Model SCz 9.2.0:**
The **log-tls-key** attribute under system-config is visible for configuration on the GUI even though the FIPS or R226 entitlement is enabled on device.
- **Limitations for the LRT Feature:**
 1. The start and end values of a range must be valid E164 numbers. (Either Numerical or Numeric starting with +). For example:
Example 1: +123667 to +123980, 12345 to 12490 are valid values.
Example 2: +9876 to 9887, 5890 to +6889 are not valid values.
 2. To import the file functionality, only .csv or .txt format files are supported.
- **Caveats for SDM SCz 9.0.0 p7:**

- * SDM can configure **online-certificate-status-protocol** regardless of whether the entitlement '**Admin Security**' is enabled or disabled.
- * **ocsp-access-method-list** is not seen in SDM regardless of whether the entitlement Admin Security is enabled or disabled.
- * **online-certificate-status-protocol** cannot be configured using the Configuration Manager - Reusable Configuration Modules.

- **Caveats for SDM**

During the course of SDM upgrades, any certificates uploaded to the Java keystore in a previous SDM version (for example – certificates for LDAP SSL connectivity) need to be imported again to the Java keystore of the new SDM version. This is needed for LDAP over SSL to work

- The REST and SOAP API response omits the reason phrase in SDM 8.2.3 and later versions, because Tomcat v9 and later versions have deprecated the reason phrase. The Tomcat server returns the status code as the reason phrase, hence the status code appears twice in the response. For example:

```
HTTP/1.1 200 200
```

instead of

```
HTTP/1.1 200 OK
```

- **Software and bootloader file integrity check**

- If the source device version is earlier than SCZ8.0.0 or ECZ8.0.0, file integrity check is not performed as the command to check file integrity is only available from SCZ8.0.0 and ECZ8.0.0 version.
- If the target software and bootloader file versions are earlier than SCZ8.0.0 or ECZ8.0.0, file integrity check is not performed as for most of the ECZ7*.bz, ECZ7*.boot images signature is not present.

- **Modelling**

- Offline Configuration or Global Parameters created using Software version for ECB - PCZ330 or above cannot be used to push dialing context entries.
- **Workaround:** Create Offline Configurations or Global Parameters from the managed device or make dialing-context modifications using the ECB user interface.
- It is not possible to perform software and bootloader upgrades from SDM for devices running SZ830m1. Devices running SCZ830m1pX work fine. As a workaround, upgrade devices running SZ830m1 using the device ACLI.
- The Offline Configurations functionality in the Configuration Manager is not supported for ECB HA pair devices.
- SDM will not be able to perform software upgrades (software image and/or bootloader) if the current software version on the device is SCz840 till SCz840p3 and R226 is enabled on the device. The reason is that on these versions the `/boot` is not accessible using SFTP. You will need to perform any upgrade from these versions using SBC ACLI.
- The current running software image must be present in the `/code/images/` directory of the network device, so that OCSDM can archive the image. This archived image can be used later during a rollback to recover from upgrade failures. If the existing image is not available, then you cannot use OCSDM for software upgrades.

- The LDAP configuration sub-element routing attribute 'address-of-record' which can be accessed using **LDAP-config routing address-of-record** will not be visible in the SDM user interface for ECB version PCZ330. Hence it cannot be configured from the SDM User Interface. **Workaround** You can configure the same attribute from the ECB PCZ330 device CLI or device GUI.
- When you add or edit the **snmp-user-entry** element through the OCSDM GUI for a device, applying a none or empty password for the **Auth protocol** and **Priv protocol** parameters are not supported.
Workaround: If a none or empty password is required for **Auth protocol** and **Priv protocol** parameters, you must apply these parameters through the device CLI.
- Do not add spaces to the "To Address" of the local routing policy.
- SNMPv3 parameters are not supported when adding a Network Function (NF) through the OCSDM REST API.
Workaround: You can enter SNMPv3 parameters for an NF that you want to add through the OCSDM GUI.
- OCSDM does not support devices with IPv6 management addresses. Refer to defect number 24361366 for more information.
- New R226 security features were introduced in the SCz8.1 and ECz 8.1 releases. If you need to manage devices with these releases (and later) with OCSDM, you must perform the following tasks:
 1. Upgrade to OCSDM 8.1 or later to manage releases which have the R226 security features.
 2. You must enable ACP over TLS on the devices.

Refer to the *Configure Transport Layer Security Certificates* section in the *Oracle Communications Session Delivery Manager Installation Guide* for more information regarding OCSDM support.

- For CSM/SLRM images 825p3 and later, you must mandatorily enable ACP over TLS.
- We recommend that the target name of your SBC device does not have an underscore character (_). This character may cause information to not appear correctly for an SBC device in OCSDM product applications. Also, the historical data record (HDR) data detection feature does not work on an SBC device if its name has an underscore.
- If the plug-in is replaced or upgraded, any previously uploaded XSD work spaces are removed.
Workaround: If required, reapply the XSD work spaces once the plug-in is installed.
- When a user installs a plug-in on a cluster node that supports new functionality, other users that are logged in may not see this new functionality.
Workaround: The user can use click Refresh in Device manager or log out of their SDM GUI session and then log back in to see the change.
- When you use the OCSDM setup process to create a self-signed certificate for OCSDM northbound WebServer HTTPS communication, a single DNS name can be used only because OCSDM supports one northbound HTTPS interface.
- When you use the OCSDM setup process to create an entity certificate to facilitate mutual authentication for OCSDM southbound (ACP), a single DNS name can be used only because the OCSDM supports one southbound ACP over TLS interface.
- In the **Element Manager Plugins** table **Tools Plugin Management**, you cannot sort the **Status**, **Server**, and **Date Modified** columns in ascending or descending order.
- If you implement an OCSDM cluster, one server only must be started successfully and operational before other servers in the cluster can be started.

- When connecting an SDM to an SBC with the Admin Security ACP feature enabled, you must have the **security, admin-security, enable-login-banner** configuration parameter set to **disabled**.
- When the Fraud Detection and Prevention feature is enabled, you must run the OCSDM as a standalone server only.
- When any changes are made to existing entitlements, OCSDM does not automatically refresh and the new entitlements changes are not enabled.
Workaround: Remove and re-add the device to OCSDM.
- In custom OCSDM installations, SAML Single sign on configuration for importing self-signed certificates into the Route Manager certificates file (cacerts), is not currently supported.
- No left-side Index/search in the browser for local help files.

Oracle Communications Session Element Manager

- Many components of the Oracle Communications session delivery product device software are licensed by Oracle and some product devices require a license key. Product devices that have applied a license key appear in Device Manager, however device license entitlements do not currently appear in Device Manager.
Workaround: Use the show entitlements command in the device CLI to gather license entitlement information.
- In the event of an unexpected server shutdown, the incremental save operation may be incorrectly reported as being successful if it is associated with a offline configuration update.
- When entering a single quote in an attribute value, use the backslash symbol "\" to escape.
- OCSDM does not support the CXF (SOAP) client.

Oracle Communications Report Manager

- If you are upgrading Oracle Communications Session Report Manager from a previous version, BI Publisher and Oracle database (Listener and Listener 2) need to be running and properly connected when you use the Oracle Communications Session Delivery Manager setup installation process, during which these databases are migrated. See the *Prepare for a Report Manager Upgrade* section in the *Pre-Installation Tasks* chapter of the *Oracle Communications Session Report Manager Installation Guide* for more information.
- By default, the password for the **nncentral** user, OCSREMDW database user, and BI Publisher (for example, DEV_MDS and DEV_BIPLATFORM) database users for the Oracle reporting database expires in 6 months. Once the password expires, the nightly backup and restore capability for reporting fails. You must go to the Oracle database to change each user password. Ask your Oracle support for more specific information about performing this task.

Note:

This limitation applies to Report Manager users who have installed an Oracle database on the same server as OCSDM only.

- With the introduction of OCSDM, Release 8.0, there is a single secure sockets layer (SSL) keystore that includes BI Publisher certificates. Any BI Publisher certificates that were previously imported into the keystore before Release 8.0 are lost.

- Ensure that the BI Publisher certificate is in the desired directory on the OCSDM server. If the BI Publisher certificate is not on the server you must transfer it to server. See the *Save and Transfer the BI Publisher Certificate to Session Delivery Manager* section in the *Register Oracle BI Publisher* chapter of the *Oracle Communications Report Manager Installation Guide* for more information.
- Ensure that the BI Publisher Certificate is added to the keystore either through the OCSDM server setup program (setup.sh) or upload it through the OCSDM GUI.

 **Note:**

If you are using the OCSDM server setup program to upload a BI Publisher certificate, you must run the setup program on each OCSDM server cluster node to upload the BI Publisher certificate on each node. If you perform this task through the OCSDM GUI, the BI Publisher certificate is replicated to all OCSDM server cluster nodes.

- * See the *Configure Southbound Interface Transport Layer Security* section in the *Custom Installation* chapter of the *Oracle Communications Session Delivery Manager Installation Guide* for more information about loading the BI Publisher certificate through the OCSDM server setup program.
- * See the *Manage Certificates for Southbound Authentication* chapter in the *Oracle Communications Session Delivery Manager Administration Guide* for more information about loading the BI Publisher certificate through the OCSDM GUI.
-
- Starting with SDM Release 9.0.3, Report Manager is supported on:
 - Oracle Database 12c and Oracle Business Publisher 12.2.1.4
 - Oracle Database 19c and Oracle Business Publisher 12.2.1.4
- In OCSDM, Release 8.0 or earlier, Report Manager is supported on Oracle Linux 6.5, 6.6, 6.7, 6.8 only. Also, Oracle Database 11g Standard Edition One, and Oracle Business Intelligence (BI) Publisher 11g are supported only.
- In OCSDM, Release 8.x, Report Manager does not support device clustering.
- In OCSDM 8.2.1, Report Manager works with Oracle Database 12c and Oracle BI Publisher 12.2.1.2.0 and not Oracle Database 11g. Therefore, during migration from a previous OCSDM 8.x release (running 11g) to OCSDM 8.2.1, only the Element Manager is migrated and the Report Manager is not.
- From OCSDM, Release 8.2.2 onwards, Report Manager works with:
 - Oracle Database 12c and Oracle BI Publisher 12.2.1.2.0
and
 - Oracle Database 19c and Oracle BI Publisher 12.2.1.2.0

The Report Manager does not work with Oracle Database 11g. Therefore, during migration from a previous OCSDM 8.x release (running 11g) to OCSDM 8.2.2, only Element Manager is migrated and Report Manager is not. Also, there is no migration path from Oracle Database 12c to Oracle Database 19c.

Known Issues and Resolved Known Issues

This chapter describes the known issues and caveats and limitations found in Oracle Communications Session Delivery Manager.

The following table provides the defect number, a description of the defect problem and any applicable workaround for a defect problem and what release the defect was found or fixed, and if the defect was closed because it was non-reproducible, or some other state. Refer to the Oracle external database (Bug DB) defect tool for more information about defect states.

Table 14-1 OCSDM Known Issues

Defect Number	Description	Severity	Found
33119585	Null message alert is displayed on selection of dialing-context for a OC and GP which is created by software version method for PCZ330 and above version.	3	8.2.3
33122661	ECB PCZ330 and above version added to a device cluster which is associated with OC created by software version method removes the existing DC data on device and data to dialing-context cannot be pushed using OC workorder. Workaround Offline Configuration created using software version for ECB - PCZ330 or above cannot be used to push dialing context entries. As a workaround, you can create Offline Configurations and GP from the managed device or make dialing-context modifications using ECB user interface.	3	8.2.3
32927603	Retrieve LRT file from the device on which a file does not exist	4	8.2.3

Table 14-1 (Cont.) OCSDM Known Issues

Defect Number	Description	Severity	Found
32927567	Route Manager - Preprocessing Table display during Import file is not visible with failure entries	4	8.2.3
31205343	<p>Device always shows green in the Device Manager after adding to cluster with error in Offline Configuration. Adding the device to a cluster shows green in the Device Manager but the device does not get added to the configuration Manager</p> <p>Workaround</p> <ul style="list-style-type: none"> • When the OC template is correct, add the device manually again and load the device to configuration manager. • When the OC template is erroneous with SNMPV3 related configuration, correct the OC template with SNMPV3 configuration and add the device again to the cluster using new OC template. 	4	8.2.2
31589522	<p>Unable to save and activate lawful-intercept configuration. OCSDM cannot provision li-config for SCZ840 even with li-admin credentials:</p> <p>Workaround: LI configuration must be performed through the ACLI.</p>	3	8.2.2

Table 14-1 (Cont.) OCSDM Known Issues

Defect Number	Description	Severity	Found
31660694	<p>OCSDM does not support bulk device deployment (with LI admin) for devices that have li config in templates.</p> <p>Workaround: You can add devices in Bulk Device Deployment as per the existing functionality. There is no provision to add an LI user password in the OC spreadsheet. Hence, the user cannot push LI-configuration related changes for device software version equal to or greater than 830m1p2 or any releases after this, during bulk device deployment via Lladmin login. However, once bulk device deployment is completed, the user can edit the li-admin password using SDM GUI. After this the LI configuration can be changed in SDM using the li-admin credentials.</p>	4	8.2.2
31661030	<p>SDM 8.2.2: Device cluster and bulk device deployment does not support addition of devices using FQDN</p> <p>OCSDM - bulk device deployment and adding device to a cluster does not support adding devices with FQDN.</p> <p>Workaround: There is no provision to add devices with FQDN to a cluster either manually or using bulk device deployment. You can add these devices using IP address or can be added manually to device groups with FQDN.</p>	4	8.2.2

Table 14-1 (Cont.) OCSDM Known Issues

Defect Number	Description	Severity	Found
ACMEESBC-102733167 3420	In local, self contained online help, the arrows and contract/expand, used for help navigation do not display as expected. Workaround: Click the box-like character.	4	8.2.2
29776859	Customers upgrading from Oracle DB 11g, BI Publisher 11.1.1.7.0 to DB 11g 11.1.1.9.0, will be able to view reports as an administrator only. As 11g is supported for only a short time longer, Oracle recommends customers perform greenfield installation to DB 12c, BI Publisher 12.2.1.1.0.	3	8.2.0
29557185	Bulk Device Deployment should be triggered from the same node from where the corresponding Offline configuration was created. It may fail when executed from a different cluster node.	2	8.2.0
29551254	A user is incorrectly able to modify the configuration from the Configuration Manager when Synchronized mode is set to TRUE for a device using the Offline Config spreadsheet. The Synchronized mode value set at the device cluster level overrides the value set at the device level.	3	8.2.0
29626456	Attributes under the ext-policy-server configuration element accepts IP addresses using an invalid format. A correction is also required on the SBC.	3	8.2.0
29669000	Configuration Manager input text boxes are not hardened.	4	8.2.0

Table 14-1 (Cont.) OCSDM Known Issues

Defect Number	Description	Severity	Found
29669522	When resetting a user password in User Management, the OCSDM does not perform validation against password rules.	3	8.2.0
28136135	In OCSDM Release 8.1, the xcode-session-gen-info HDR group is not supported.	4	8.1
26627620	In OCSDM Release 8.1, the subjects HDR group is not supported.	4	8.0
25388326	<p>The OCSDM setup application process may fail or the OCSDM server may fail to start if you enter a password for the Report Manager user (OCSREMDW) with \$, #, and & special character(s) in the Custom installation in the OCSDM setup application. Refer to the <i>Create a Report Manager Database Instance on the External Oracle Database</i> section in the <i>Oracle Communications Report Manager Installation Guide</i> for more information.</p> <p>Workaround: The password must be eight characters or more, contain at least one uppercase character, one lowercase character and a number (1-9). You cannot use the \$, #, and & special character(s) in the password. Use only the supported %, period (.), and ! special characters in your password at this time.</p>	3	8.1

Table 14-1 (Cont.) OCSDM Known Issues

Defect Number	Description	Severity	Found
28180392	Historical Data Recording (HDR) data that is pushed to Oracle Communications Report Manager from devices using SFTP does not work for SCz8.1 and ECx8.1 releases. Refer to the SCz and ECx defect 28163745 for more information.	4	8.1
27946885	Currently, both OCSDM and an SBC does not prevent a user from downgrading a device with a login password that is already encrypted by SHA-512 to an SBC version that does not support SHA-512 password encryption. If user takes this action, the device becomes unusable because they are not able to login again. Workaround: Change the password for the following user types if they are encrypted with SHA-512: admin , li-admin , and user	4	8.1

Table 14-1 (Cont.) OCSDM Known Issues

Defect Number	Description	Severity	Found
27631241	<p>The IPsec element can be configured from the OCSDM GUI even when the entitlement on the SBC is not enabled. However, the result is that a save and activate action (performed in the OCSDM GUI) fails on the device.</p> <p>Workaround: Remove the IPsec element and resubmit it by using the Save & activate configuration parameter in Configuration Manager (refer to the <i>Update a Network Function Device Configuration</i> section in the <i>Oracle Communication Session Element Manager User Guide</i> for more information) or enable the IPsec entitlement on the device if the IPsec entitlement is required.</p>	4	8.1

Table 14-1 (Cont.) OCSDM Known Issues

Defect Number	Description	Severity	Found
27069201	<p>For a device that is running SCz or ECz Release 8.1 (and later), the ACME Control Protocol (ACP) over Transport Layer Security (TLS) feature must be enabled on OCSDM Release 8.1 so that this device can be managed by OCSDM. If you disable the ACP over TLS feature on a device to run ACP only for releases prior to SCz or ECz Release 8.1, OCSDM management operations for this device are compromised.</p> <p>Workaround: Use the following steps to prompt OCSDM to start managing the device again:</p> <ol style="list-style-type: none"> 1. Reconfigure ACP/TLS through SSH. 2. Reboot the device through SSH to modify its configuration. 3. In the OCSDM GUI, remove the Network Function (NF) device from Configuration Manager. 4. Remove the NF device from Device Manager. 5. Add the NF device in Device Manager. 6. Assign the NF device in Configuration Manager. 	3	8.1

Table 14-1 (Cont.) OCSDM Known Issues

Defect Number	Description	Severity	Found
25918918	When you edit SNMP parameters for a Network Function (NF) with a device(s) in Device Manager to go from SNMPv1 or SNMPv2 to SNMPv3, the NF (with its associated devices) needs to be removed and added again.	4	8.0
27601270	The BI Publisher defect 27758948 states that anytime a line graph tries to display a constant value (horizontally across the x-axis) for a report, the report is not rendered in some web browsers. Workaround: Use a different web browser or to enable 3-D mode on the line graph through the Layout Editor.	4	8.1
27699848	When Lawful Intercept (LI) is configured on a device using its ACLI, the configuration is stored in on the device. If the device is ever restored using a backup of the device, the LI configuration cannot be accessed through its ACLI. However, when this device is loaded in OCSDM in Configuration Manager, the backed up device configuration appears, including the LI configuration. Workaround: In OCSDM, delete the old LI configuration, and enter the current LI configuration that you want to use.	3	8.1

Table 14-1 (Cont.) OCSDM Known Issues

Defect Number	Description	Severity	Found
25353891	When adding collection groups in Report Manager, you must collect HDR data for all HDR groups by clicking the Yes checkbox in the Add a Collection Group - Step 2 dialog box because of SBC defect 25576484. Refer to the <i>Add a Collection Group</i> section in the <i>Configure Report Manager to Run Reports</i> chapter of the <i>Oracle Communications Report Manager User Guide</i> for more information about setting this parameter.	4	7.5M3
28129255	When you are editing a Fraud Protection List (FPL) entry and enter the realm name into the field for the Realm parameter, this entry is not recorded in the database. Workaround: You must first click the Realm drop down-list arrow first to select the name of the SIP realm that is configured on the device. The SIP realm is associated with the match value. If the realm for which you are looking does not appear in the drop-down list, you can then type the name of this realm in the field.	3	8.1
25382198	Report Manager does not support data gathering or the TscfStats group for SBC devices with ScZ7.40 and ScZ7.4.0p1 releases. This problem was fixed in the ScZ7.4.0p2 release (refer to SBC defect 25341897).	2	7.5M3

Table 14-1 (Cont.) OCSDM Known Issues

Defect Number	Description	Severity	Found
26417111	HDR failed to load because there was a duplicated column of GPRS Tunneling Protocol (GTP) statistics.	4	8.0
N/A	For the Oracle Communications Mobile Security Gateway M-Cz4.1.0 Software Release, a duplicate entry is created in the CSV header (defect 26424107) for the gtp-stats HDR group. Report Manager does not process this HDR group.	N/A	8.0
N/A	If you are using the Internet Explorer web browser for your OCSDM session and you press the Backspace key on your key board while configuring fields or doing other operations in the application, you may be logged out of your OCSDM session and be forced to log back into OCSDM. Workaround: We suggest that you use another supported vendor web browser, such as Firefox.	N/A	8.0
N/A	Due to SBC defect 24361366, OCSDM does not support an SBC device with an IPv6 management address.	N/A	8.0

Table 14-1 (Cont.) OCSDM Known Issues

Defect Number	Description	Severity	Found
28715250	When the OCSDM is processing an update from the FTP server and you attempt to view the FPL, you may receive the error message, "Failed to load page table contents. Error: An attempt was made to reference a node that no longer exists; the node may be a bound variable or part of a query context". Workaround: Wait a short time and try displaying the list again.	4	8.1.1
28707570	While the OCSDM is processing an update from the FTP server, if a user tries to manually add an entry that is part of the update, the entry may be added twice.	4	8.1.1
28742032	Once you have successfully assigned and then unassigned an FPL to an FDP, you cannot assign that same FPL again. Workaround: Copy the current FPL and assign the copied FPL to FDP.	4	8.1.1
28817962	To properly configure an FDP registration name, the name cannot contain any blank spaces. If you attempt to register an FDP name that contains spaces, you get the following error: " FDP registration name contains invalid characters. Valid characters are a-z,A-Z,_,0-9,-."	4	8.1.1

Resolved Known Issues

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

ID	Description	Severity	Found In	Fixed In
	SDM service is getting shutdown.	2	8.2.5	8.2.5.0.1 and 9.0.0.0
	REST API issue on the SDM.	3	8.2.5	8.2.5.0.1
33004475	Fraud entries with '+' characters are rejected	3	8.2.0	8.2.5
33124034	Unable to add any FPL entry having hostname with Alphanumeric FQDN value	3	8.2.3	8.2.5
33387607	Issue with Rest API and the NetworkInterface Object.	2	8.2.2	8.2.5
33322677	Audit log csv export not working properly	3	8.2.2 and 8.2.3	8.2.5
33429098	Adding Performance Manager APIs to Rest APIs Documents	3	8.2.4	8.2.5
33217295	Error occurs while downloading alarms dump with date search criteria	3	8.2.0	8.2.5
33399900	SDM cannot add entries starting with DS:E and DS:F under local-policy	3	8.2.3	8.2.5
32840543	The unit of TCU load stats reading is one of 10000 th . For example, on the SBC CLI if the xcode load stats value is 0.16% then on the SDM user interface for TCU load stats value is 16.	3	8.2.4	8.2.4
32371360	Possible threat of CSV injections which occurs when data is not properly sanitized before exporting it to the CSV format. Once imported into Excel, functions can be executed, including opening malicious URLs.	3	8.2.0	8.2.4
32416031	SDM discloses the Apache Tomcat version	3	8.2.2	8.2.4
32470642	Missing Security-Relevant HTTP Headers	3	8.2.2	8.2.4
32548889	Route Set scheduled backups tab paging missing	3	8.2.2.2	8.2.4
32548889	SDM not sending unique SNMPv3 EngineID for the same managed device.	3	8.2.2.1	8.2.4
32777796	Unknown alarm in SDM	3	8.2.2.1	8.2.4
32606816	Config element 'dialing-context' provisioning performance needs to be improved for ECB device.	2	8.2.4	8.2.4
31819268	RPM gets purge error in oracle DB when purging hitting huge records to delete Report Manager Purging fails when there are very huge records in the database.	3		8.2.3

ID	Description	Severity	Found In	Fixed In
31408846	Sorting columns in the Performance Manager screen fails to sort across all the pages.	4		8.2.3
31979765	Deleting parent-config element leads to the deletion of the other config-elements which are dependent on the parent-config element. This should not be allowed ,instead the dependent elements should be deleted manually.	2		8.2.3
32224472	Device Manager does not display the complete patch version of the device and excludes any alphabet in the patch version.	3		8.2.3
32213411	Software Upgrade work order is stuck in case of multiple devices being updated. Only the first device upgrade is processed while the remaining devices are stuck in the 'Ready' state.	2	8.2.2	8.2.3
31864495, 31524420	REST API for import CSV file without headers does not support ';' as delimiter. <ul style="list-style-type: none"> • Verified import csv via REST API with ';' as delimiter. • Verified delimiter check in front of the rows in the CSV file during file Import. • Error Validations for the csv file Headers and Import file templates is not fixed in this release. 	3	8.2.3	8.2.3
32295283	Unable to delete local-policy config element through RCM delete template	4	8.2.2	8.2.3
32386828	Dashboard Manager does not display CPU usage for devices running on NNOSVM platform.	3	8.2.2	8.2.3
32377039	It is not possible to add more than one device to a device cluster (Manually or using Bulk Device Deployment) which is powered by OC.	2	8.2.3	8.2.3
32310148	Software update work order gets stuck intermittently in the 'Preload Pause' state if it is run in combination where both Preload Pause and Pause (after preload pause step) are selected.	3	8.2.3	8.2.3
32468109	In SDM it is possible to query external authentication details using chrome or postman if the user does not have the required privilege.	3	8.2.2	8.2.3

ID	Description	Severity	Found In	Fixed In
32468008	Work Order with more than one device and with concurrent run enabled upgrades same bootloader on all devices during rollback	3	8.2.3	8.2.3
32375557	Unable to add email id's with characters dot, hyphen and underscore in Fault Email Notification.	2	8.2.1	8.2.3
32412472	Starting with SDM version 8.2.2 till 8.2.3, if IPv6 is not enabled on the system that has OCSDM running, SDM server fails to start	3	8.2.3	8.2.3
30643522	OCSDM 8.2.1 cannot modify LI configuration for SBC S-Cz8.3.0m1p2 and later. Workaround: Perform all LI configuration through the ACLI.	4	8.2.1	8.2.2
28201485	In OCSDM Release 8.1, the sip-codec-per-realm HDR group is not supported.	4	8.1	8.2.0
28194322	In OCSDM Release 8.1, the sa-srtp HDR group is not supported.	4	8.1	8.2.0
28396076	The session-agent, local-response-map configuration parameter has the wrong default value, generating warnings when running verify-config .	3	8.1	8.1.1
28605180	OCSDM is sending trap information to trap receivers with the wrong sysUpTime OID type of gauge32 instead of TimeTick.	2	8.1	8.1.1
28151272	Fraud Detection and Prevention (FDP) device support is not available.	4	8.1	8.1.1
26620683	The Acme Control Protocol (ACP) Transport Layer Security (TLS) feature on a device must be disabled before this device can be added to a device cluster in Device Manager.	4	8.0	8.1
26268556	In OCSDM release 8.0 and later, the Berkley database and OCSDM plug-in management system encounters problems if any IP address changes are made for each cluster member node after a successful OCSDM cluster deployment. This happens if you shut down the OCSDM cluster and re-run the setup program to change any of the cluster member IP addresses.	3	8.0	8.1

ID	Description	Severity	Found In	Fixed In
28035170	If an SBC is upgraded from SCz7.2.0M4 to SCz7.4.0M1p6, OCSDM takes a long time to load and show the new configuration during its first attempt.	3	7.5	8.1
27970655	OCSDM cannot load a USM 6300 device configuration after OCSDM is upgraded to Release 8.0.	3	8.0	8.1
27770070	The configuration for a device could not be loaded in OCSDM because there are attribute issues introduced in OCSDM Release 8.0 that affected the operation of some models.	3	8.0	8.1
27450645	Orphaned commons-collections JAR files need to be removed from production directories.	4	8.0	8.1
27240846	When two different users associate the same route set to the same device, the device cannot be added to the route set.	2	7.5	8.1
27235892	If one user logs into OCSDM and is using Route Manager route sets and locks a route set, a different user logged into OCSDM at the same time can add this locked route set to another device in the Device Route Sets tab. Resolution: A confirmation message dialog box appears that asks the user if they want to continue with the operation.	4	7.5	8.1
27137117	After importing a file for a Route Set, if the user selected all the available columns for display, the browser client would crash and the browser cache would have to be cleared to regain GUI control.	2	7.5	8.1
26989900	A high-availability (HA) device pair cannot be added to OCSDM if the cli-more element is enabled in the device system-config.	3	8.0	8.1
26933744	Only the server where the schema upload was initiated has the new updated XSD schema in its local cache. The other nodes still retain the previous XSD schema in memory. For example, in a three-node cluster setup, if a schema file was uploaded on Member A, SBC provisioning fails on Member B and Member C.	2	7.5M3	8.1

ID	Description	Severity	Found In	Fixed In
24588116	The apEnvMonTrapCurrentState trap does not display the card name in SDM fault alarm description field due to SBC defect 25348541, which was fixed in SCZ7.3.0M3 and SCZ7.4.0M1. Workaround: The correct card name displays in SDM if the SBC is using either SCZ7.3.0M3 or SCZ7.4.0M1 versions or later.	4	7.5M1	8.1

A

Historical Session Element Manager Device Software Support

The following tables show the historical device software support for Oracle Communications Session Element Manager for Service Provider and Enterprise device releases prior to Release 9.0.

Oracle Communications Session Border Controller Releases

Table A-1 C/CX Software Support

Base Software Release	Follow-on Releases
C/CX6.0.0	M5, M6, M7, M8

Table A-2 SCX Software Support

Base Software Release	Follow-on Releases
S-C/S-Cx6.1.0	M2, M3, M4, M5, M6, M7, M8, M9, M10, M11
S-C/S-Cx6.2.0M1	M2, M3, M4, M5, M6, M7, M8, M9, M10, M11, M12
S-C/S-Cx6.2.1F1	F2, M1, M2
S-Cx6.2.3	-
S-Cx6.2.5F1	-
S-Cx6.3.0	F1, F2, M1, M2, M3, M4, M5
S-Cx6.3.15M1	M2, M3
S-Cx6.3.3	F1, F2, F3, F4, M1, M2, M3
S-Cx6.3.5	F1, M1, p3
S-Cx6.3.6F1	-
S-Cx6.3.7	F1, F2, F3, F4, M1, M2, M3
S-Cx6.3.9	F1, M1, M2, M3, M4, M5
S-Cx6.4.0	F1, M1, M2, M3, M4, M5, M6, M7
S-Cx6.4.6F1	F2, F3, F4, F5

Table A-3 SCZ Software Support

Base Software Release	Follow-on Releases
S-Cz6.3.15	M1, M2, M3
S-Cz6.3.9	M1, M2, M3, M4, M5
S-Cz7.0.2	F1, F2
S-Cz7.0.9	F1
S-Cz7.1.2	M2, M3, M4, M5
S-Cz7.1.5	M1
S-Cz7.2.0	M1, M2, M3, M4, M5, M6

Table A-3 (Cont.) SCZ Software Support

Base Software Release	Follow-on Releases
S-Cz7.2.10	-
S-Cz7.2.5	M1, M2, M3, M4
S-Cz7.2.9	-
S-Cz7.3.0	M1, M2, M3, M4
S-Cz7.3.5	M1, M2
S-Cz7.3.9	-
S-Cz7.3.10	-
S-Cz7.4.0	M1
S-Cz7.4.1	-
S-Cz8.0.0	-
S-Cz8.1.0	-
S-Cz820	
S-Cz830	
S-Cz840	
S-Cz900	

Table A-4 SD Software Support

Base Software Release	Follow-on Releases
SD7.0.0	M1, M2, M3, M4, M5, M6, M7, M8, M9, M10, M11, M12
SD7.1.0	M1, M2, M3, M4, M5, M6
SD7.2.0	F1, M1, M2, M3
SD7.2.3	F2, F3

Oracle Communications Subscriber-Aware Load Balancer Releases**Table A-5 LCX Software Support**

Base Software Release	Follow-on Releases
L-Cx1.0	-
L-Cx1.1.3	F1, F2, F3, M1, M2, M3
L-Cx1.5.0	M1

Oracle Communications Mobile Security Gateway Releases**Table A-6 MCX Software Support**

Base Software Release	Follow-on Releases
M-Cx1.2.0	F2, F3
M-Cx2.0.0	M1
M-Cx3.0.0	F1, M1, M2, p2, M3

Table A-7 MCZ Software Support

Base Software Release	Follow-on Releases
M-Cz4.0.0M1	M2
M-Cz4.1.0	-

Oracle Enterprise Session Border Controller Releases**Table A-8 ECX/Z Software Support**

Base Software Release	Follow-on Releases
E-Cx6.3.7	M1, M2, M3
E-Cx6.4.0	F1, M1, M2, M3, M4, M5
E-Cx6.4.1	M1
E-Cz7.1.0	-
E-Cz7.2.0	-
E-Cz7.3.0	M1, p2, M2 p1, M3
E-Cz7.4.0	p1
E-Cz7.5.0	-
E-Cz8.0.0	-
E-Cz8.1.0	-
S-Cz820	-
S-Cz830	-
S-Cz840	-
S-Cz900	-

Oracle Enterprise Communications Broker Release**Table A-9 PCX Software Support**

Base Software Release	Follow-on Releases
P-Cx100F1	-
P-Cz2.0.0	M4
P-Cz2.1.0	-
P-Cz2.2.0	-
P-Cz3.3.0	-

Session Element Manager Plug-in Device Software Support

The following table describes device software support for the Oracle Communications Session Element Manager plug-in releases which have occurred since the introduction of OCSDM 8.0.

OCSEM Plug-in Name	Plug-in Version	Devices
AcmeSD	1.0	<ul style="list-style-type: none"> • M-Cz4.1.0 • S-Cz7.3.0M3 • S-Cz7.3.0M4 • S-Cz7.3.5M2 • S-Cz7.4.0M1 • S-Cz7.4.1 • S-Cz8.0.0
Enterprise	1.0	<ul style="list-style-type: none"> • E-Cz7.3.0M3 • E-Cz7.5 • P-Cz2.2.0
EnterpriseExt	1.0	<ul style="list-style-type: none"> • Oracle Communications Interactive Session Recorder (ISR) • Oracle Enterprise Operations Monitor (EOM)
SP Edge and Core	2.0	<ul style="list-style-type: none"> • SCz7.4.1M1 • SCz8.1 • S-Cz8.2.0¹
Enterprise Edge and Core	2.0	<ul style="list-style-type: none"> • ECz8.0 • ECz 8.1
Enterprise Utilities	2.0	<ul style="list-style-type: none"> • ISR • EOM
SP Edge and Core	2.1	No new models added.
Enterprise Edge and Core	2.1	<ul style="list-style-type: none"> • ECz 8.1M1
Enterprise Utilities	2.1	<ul style="list-style-type: none"> • ISR • EOM • Oracle Fraud Detection and Prevention (FDP)
SP Edge and Core	3.0	<ul style="list-style-type: none"> • SCz7.4.0M2 • SCz8.2.0 • SCz8.3.0 • SCz8.2.0²
Enterprise Edge and Core	3.0	<ul style="list-style-type: none"> • ECz8.1.0M1 • SCz8.3.0 • SCz8.2.0³
Enterprise Utilities	3.0	<ul style="list-style-type: none"> • ISR • EOM • Oracle Fraud Detection and Prevention (FDP)

¹ S-Cz8.2.0 is used for both Service Provider and Enterprise SBCs with this plugin running on SDM 8.1.1 onwards.

² S-Cz8.2.0 is used for both Service Provider and Enterprise SBCs with this plugin running on SDM 8.1.1 onwards.

³ S-Cz8.2.0 is used for both Service Provider and Enterprise SBCs with this plugin running on SDM 8.1.1 onwards.