

Oracle® Communications Session Delivery Manager Release Notes



Release 8.2
December 2019



Oracle Communications Session Delivery Manager Release Notes, Release 8.2

Copyright © 2014, 2019, Oracle and/or its affiliates. All rights reserved.

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

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

If this is software or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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

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

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

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

Contents

About This Guide

My Oracle Support vi

Revision History

1 Overview

Session Delivery Manager Application Overview 1-1
Session Delivery Manager Product Plug-in Service 1-1
Session Element Manager Plug-in Support Matrix 1-2
Session Element Manager Plug-in Device Software Support 1-4
External Interfaces 1-5
Documentation Distribution 1-5

2 Release 8.2.1

Release 8.2.1 Features 2-1
Session Delivery Manager Software Distribution Media for Release 8.2.1 GA 2-4
Session Element Manager Plug-in Support Matrix for 8.2.1 2-5
Session Element Manager Plug-in Device Software Support for 8.2.1 2-6
Documentation Changes 2-6

3 Session Delivery Manager Installation

Check System Requirements 3-1
Software Installation Prerequisites 3-2
 Check that Work Orders are in a Committed State 3-2
 Report Manager Installation 3-3
Session Delivery Manager Software Distribution Media 3-3
 Session Delivery Manager Software Distribution Media for Release 8.2 GA 3-3

4	Session Delivery Manager Features	
	Release 8.2 Features	4-1
5	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 3.0	5-1
6	Session Element Manager Features Delivered by the Enterprise Plug-in	
	Session Element Manager Features Delivered by the Enterprise Edge and Core Plug-in Release 2.0 and 2.1	6-1
7	Session Element Manager Features Delivered by the Enterprise Utilities Plug-in	
	Session Element Manager Features Delivered by the Enterprise Utilities Plug-in Release 2.0	7-1
8	Known Issues	
	Caveats and Limitations	8-6
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.
Installation Guide	<p>Provides the following installation information:</p> <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	<p>Contains information about the administration and software configuration of the OCSDM feature support new to this release.</p>

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

Document Name	Document Description
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.

Revision History

This section provides a revision history for this document.

Date	Revision
May 2019	<ul style="list-style-type: none"><li data-bbox="876 611 1377 653">• Initial Release.
December 2019	<ul style="list-style-type: none"><li data-bbox="876 653 1377 695">• Adds updates for OCSDM 8.2.1.<li data-bbox="876 695 1377 816">• Adds Oracle Communications Core Session Manager (OCCSM) to the list of products supported by the AcmeSD and SP Edge & Core.

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:

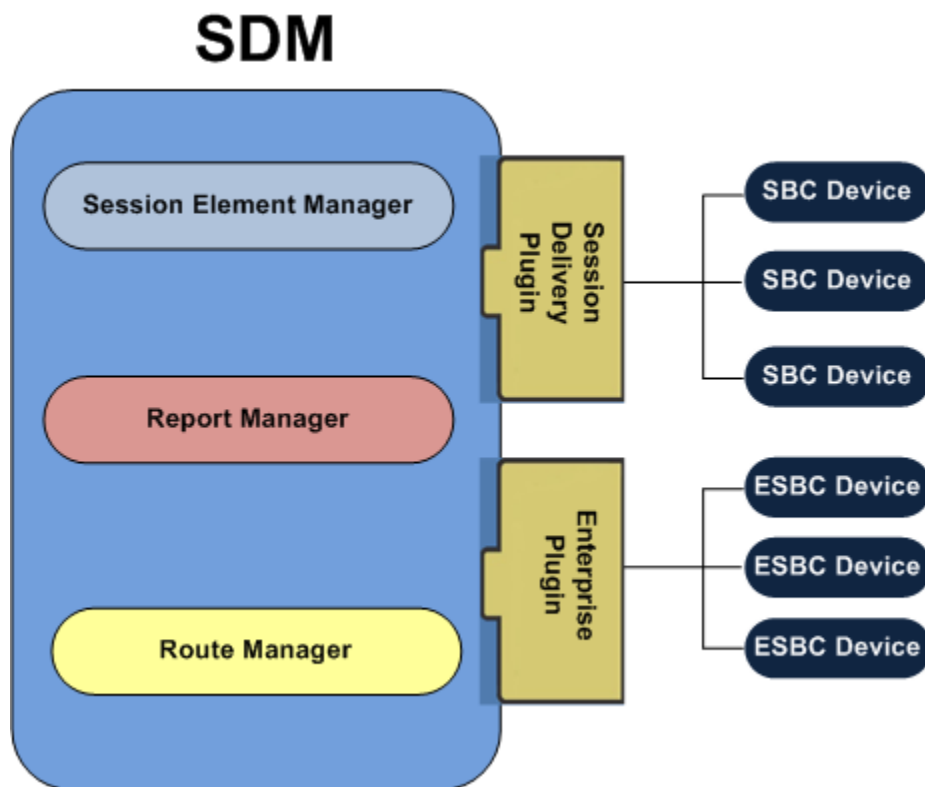
Upon installation of one of these plugins, the OCSDM displays only the applicable sliders and their relevant configuration elements to enable.

Session Delivery Manager Product Plug-in Service

A product plugin 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 plugin 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.



Session Element Manager Plug-in Support Matrix

Use the following tables to determine Oracle Communications Session Delivery Manager (SDM) release compatibility, OCSEM plug-in platform support, plug-in product device compatibility, and the product device software plug-in support that was introduced in OCSDM release 8.x.

Oracle Communications Session Delivery Manager and Oracle Communications Session Element Manager Plug-in Release Compatibility

OCSDM Release	OCSEM Plug-in Name	OCSEM Plug-in Release
8.0	<ul style="list-style-type: none"> AcmeSD Enterprise EnterpriseExt 	1.0
8.1	<ul style="list-style-type: none"> SP Edge and Core Enterprise Edge and Core Enterprise Utilities 	2.0
8.1.1	<ul style="list-style-type: none"> SP Edge and Core Enterprise Edge and Core Enterprise Utilities 	2.1
8.2	<ul style="list-style-type: none"> SP Edge and Core Enterprise Edge and Core Enterprise Utilities 	3.0

 **Note:**

All plugins inherit the support of the previous release.

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

The following 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 3800	Yes	No	No
Acme Packet 3810	Yes	No	No
Acme Packet 3820	Yes	No	No
Acme Packet 3900	Yes	Yes	No
Acme Packet 4250	Yes	No	No
Acme Packet 4500	Yes	Yes	No
Acme Packet 4600	Yes	Yes	No
Acme Packet 6100	Yes	Yes	No
Acme Packet 6300	Yes	Yes	No
Acme Packet 6350	Yes	No	No
Acme Packet 9200	Yes	No	No
	The Acme Packet 9200 is not supported by Oracle Communications Report Manager.		
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

Oracle Communications Session Element Manager Plug-in Product Device Compatibility

The following table describes the products that each OCSEM plug-in supports.

OCSEM Plug-ins	Product Support
AcmeSD and SP Edge and Core	<ul style="list-style-type: none"> • Oracle Communications Session Border Controller (OCSBC) • Oracle Communications Subscriber-Aware Load Balancer (OCSLB) • Oracle Communications Mobile Security Gateway (MSG) • Oracle Communications Unified Session Manager (USM) • Subscriber-aware Load Balancing and Route Management (SLRM) • Oracle Communications Session Router (OCSR) • Oracle Communications Core Session Manager (OCCSM)
Enterprise Edge and Core and Enterprise	Oracle Enterprise Session Border Controller, Oracle Enterprise Communications Broker Release
EnterpriseExt and Enterprise Utilities	EOM and ISR

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.

Note:

Refer to the "Plug-in Support Matrix" section for more information about what plugin is used with the product device releases mentioned below. All plugins inherit the support of the previous release, including the device releases mentioned in the "Historical Session Element Manager Device Software Support" section.

OCSEM Plug-in Name	Release Introduced	Latest Releases Supported
SP Edge and Core	3.0	<ul style="list-style-type: none"> • S-Cz8.3.0 • S-Cz8.2.0 • S-Cz8.1.0M1P6 • S-Cz8.1.0M1 • S-Cz7.4.0M2
Enterprise Edge and Core	3.0	<ul style="list-style-type: none"> • S-CZ8.3.0 • S-Cz8.2.0 • E-Cz8.1.0M1 • PCZ3.1.0 • PCZ3.0.0
Enterprise Utilities	3.0	<ul style="list-style-type: none"> • ISR • EOM • Oracle Fraud Detection and Prevention (FDP)

For products/models supported in earlier OCSEM plug-ins, see the "Session Element Manager Plug-in Device Software Support" section in the "Historical Session Element Manager Device Software Support" appendix.

External Interfaces

This section describes the supported external API interfaces.

REST API

As of Release 8.0, the 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

With the introduction of OCSDM, Release 8.0, the SOAP API client is provided for backwards compatibility only. The SOAP API will not support any new APIs for new OCSDM enhancements. Oracle recommends using the REST API for OCSDM if you require access to new OCSDM features via a programmatic API.

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 8.2.1


The following topics provide descriptions, explanations, and configuration information for the contents of Release 8.2.1. Unless otherwise stated, requirements and other release information is identical to 8.2 GA, noted in the other chapters of this document.

Release 8.2.1 Features

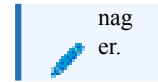
The following table describes the Release 8.2.1 features for Oracle Communications Session Delivery Manager (OCSDM).

Feature	Description	Where Documented
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.	<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

 **No**
te:
 When R226 compliance is enabled, devices added with a LI encryption password can be managed by changing the device permissions via the Security Ma

Feature	Description	Where Documented
Lawful Intercept Config Options	Restricts the ability to view and edit LI configuration elements to the LIadmin 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

Session Delivery Manager Software Distribution Media for Release 8.2.1 GA

The following files are available for Oracle Communications Session Delivery Manager, Release 8.2.1:

File Name	Description
NNC82_1OracleLinux65_64bit.tar.gz	Oracle Linux operating system version 6.5, 64 bit installation file package.
NNC82_1OracleLinux70_64bit.tar.gz	Oracle Linux operating system version 7.0, 64 bit installation file package.
CXFClientNNC82_1.zip	NNC8.2.1 Apache CXF client containing northbound SOAP client libraries and examples for JDK 1.8. See the Oracle Communications Session Element Manager SOAP API Guide for more information.
NNC82_1RESTClient.zip	NNC8.2.1 REST client zip file.
MIBs_NNC82_1.zip	NNC8.2.1 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_core4.0_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_core4.0_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_utilities4.0_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)

Session Element Manager Plug-in Support Matrix for 8.2.1

Use the following table to determine Oracle Communications Session Delivery Manager (SDM) release compatibility that was introduced in OCSDM release 8.2.1.

Oracle Communications Session Delivery Manager and Oracle Communications Session Element Manager Plug-in Release Compatibility

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



Note:

All plugins inherit the support of the previous release.

Session Element Manager Plug-in Device Software Support for 8.2.1

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



Note:

Refer to the "Plug-in Support Matrix" section for more information about what plugin is used with the product device releases mentioned below. All plugins inherit the support of the previous release, including the device releases mentioned in the "Historical Session Element Manager Device Software Support" section.

OCSEM Plug-in Name	Release Introduced	Latest Releases Supported
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 • PCZ3.2.0
Enterprise Utilities	4.0	<ul style="list-style-type: none"> • ISR • EOM • Oracle Fraud Detection and Prevention (FDP)

For products/models supported in earlier OCSEM plug-ins, see the "Session Element Manager Plug-in Device Software Support" section in the "Historical Session Element Manager Device Software Support" appendix.

Documentation Changes

The following information lists and describes the changes made to the Oracle Communications Session Delivery Manager documentation set for 8.2.1.

My Oracle Support

Each book in the OCSDM documentation set now contains the "My Oracle Support" topic. This topic contains information on contacting product support, accessing emergency help in the case of a critical emergency, and locating product documentation.

3

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:

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). If you are running any release prior to 7.5M3, you must upgrade to 7.5M3 before you can upgrade to 8.2.

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 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 6.9, 6.10, 7.2, 7.3, 7.4, 7.5, 7.6 64-bit.

Note:

OpenSSL 1.0.1e-fips or later must be installed on your Linux server in order to use the HTTPS service on the Apache web server. Most Linux distributions include OpenSSL as part of the OS installation. You can check the version on your system by using the following command:

```
openssl version  
OpenSSL 1.0.1e-fips 11 Jun 2017
```

- CentOS 6.8, 6.9, 7.3

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 (64-bit) 7.0, 7.1, 7.2, or 7.3
- Oracle Communications Report Manager for Oracle Fusion Middleware 11g is supported on Oracle Linux 6.5, 6.6, 6.7, 6.8 only.

Client Requirements

- Oracle recommends Internet Explorer versions 11.0 and later, Mozilla Firefox versions 43.3.1 and later, or Google Chrome version 56 and later.
- 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.

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 8.x.

All work orders must be in a **Committed** state before you upgrade to OCSDM, Release 8.x because the migration of existing work orders on a server running OCSDM, Release 7.5m3 is not provided when you upgrade to OCSDM, Release 8.x. 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 for Oracle Fusion Middleware 11g is not supported.

	SDM 8.2 Core	Report Manager 11g Migration	Report Manager 12c Migration
7.5M3 with 11g	Yes	Yes	No
8.0 with 11g	Yes	Yes	No
8.0 with 12c	Yes	No	Yes
8.1/8.1.1 with 11g	Yes	Yes	No
8.1/8.1.1 with 12c	Yes	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.

Session Delivery Manager Software Distribution Media

Session Delivery Manager Software Distribution Media for Release 8.2 GA

The following files are available for Oracle Communications Session Delivery Manager, Release 8.2:

File Name	Description
NNC82OracleLinux65_64bit.tar.gz	Oracle Linux operating system version 6.5, 64 bit installation file package.
NNC82OracleLinux70_64bit.tar.gz	Oracle Linux operating system version 7.0, 64 bit installation file package.

File Name	Description
CXFClientNNC82.zip	NNC8.2 Apache CXF client containing northbound SOAP client libraries and examples for JDK 1.8. See the Oracle Communications Session Element Manager SOAP API Guide for more information.
NNC82RESTClient.zip	NNC8.2 REST client zip file.
MIBs_NNC82.zip	NNC8.2 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_core3.0_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_core3.0_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_utilities3.0_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)

4

Session Delivery Manager Features

The following sections describe new Oracle Communications Session Delivery Manager features and the Oracle Communications Session Element Manager co-product features for Release 8.2.

Release 8.2 Features

The following table describes the Release 8.2 features for Oracle Communications Session Delivery Manager.

Feature	Description	Where Documented
Configure a Device Cluster Using a Bulk Spreadsheet	The OCSDM can provision a bulk device deployment using existing offline configurations and spreadsheets that contain required device details for the cluster.	The <i>User Guide for the Service Provider Edge and Core Plug-in</i> and <i>User Guide for the Enterprise Edge and Core Plug-in's</i> "Use an Offline Configuration for a Device Cluster" chapter includes a new section, "Configure a Device Cluster Using a Bulk Spreadsheet".
Manage Route Sets Using REST	A REST user can create and modify route sets, add or remove routes to a route set, and update all or some SBC devices with a specific route set.	The REST API documentation is located at https://docs.oracle.com/cd/F18700_01/REST/ . The REST API documentation for managing route sets is located at https://docs.oracle.com/cd/F18700_01/REST/api-route-sets-management.html .
Acme Packet 3900 Service Provider Edge and Core Plug-in Support	The Service Provider Edge and Core Plug-in now supports the Acme Packet 3900 platform.	The "Device Platform Support For Oracle Communications Session Element Manager Plug-ins" table in the Release Notes has been updated with this information.

5

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)
- Subscriber-aware Load Balancing and Route Management (SLRM)
- Oracle Communications Session Router (OCSR)
- product devices with comprehensive tools and applications on the OCSDM (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 3.0

The Service Provider (SP) Edge and Core plug-in for Release 3.0 provides the following features:

 **Note:**

As of Oracle Communications Session Delivery Manager Release 8.0, the previous device nodes (used in OCSDM 7.x) that maintained the standalone or HA pair devices were replaced with the concept of a Network Function (NF). NFs are a network architecture concept used to describe entire classes of network node functions into building blocks that may connect, or chain together, to create communication services as defined by the *GS NFV-MAN 001 - ETSI*. In this context, a NF can be composed of one-to-many Edge devices. For example, a SBC-based NF can be composed of two SBC instances running as a HA pair.

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

6

Session Element Manager Features Delivered by the Enterprise Plug-in

The Enterprise Edge and Core Release 3.0 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 (OCSDM) 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 Release 2.0 and 2.1

The following features are described for the Enterprise Edge and Core plug-in for Release 3.0. No Enterprise Edge and Core plug-in features were added in this release.

7

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) and Oracle Enterprise Operations Monitor Users (EOM) 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.

The following features are described for the Enterprise Utilities plug-in for Release 3.0.

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

Session Element Manager Features Delivered by the Enterprise Utilities Plug-in Release 2.0

The Enterprise Utilities plug-in for Release 2.0 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 2.0 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.

Note:

Fraud Detection and Prevention (FDP) device support is not available for the Enterprise Utilities plug-in. When the plug-in is installed and you try to add a Network Function (NF) for an FDP device, the NF type of **FDP** appears, but is not supported at this time.

8

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 8-1 OCSDM Known Issues

Defect Number	Description	Severity	Found
3064352 2	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
2977685 9	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
2962074 6	When running the 3.1.0 version of ECB, the clear trap is missing for apSysMgmtCSVCfgSaveFailTrap. Clear trap needs to be provided by the ECB product. The ECB product is tracking this issue in defect 29620746.	3	8.2.0
2955718 5	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
2955125 4	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
2962645 6	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
2966900 0	Configuration Manager input text boxes are not hardened.	4	8.2.0
2966952 2	When resetting a user password in User Management, the OCSDM does not perform validation against password rules.	3	8.2.0
2813613 5	In OCSDM Release 8.1, the xcode-session-gen-info HDR group is not supported.	4	8.1
2662762 0	In OCSDM Release 8.1, the subjects HDR group is not supported.	4	8.0

Table 8-1 (Cont.) OCSDM Known Issues

Defect Number	Description	Severity	Found
2538832 6	<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
2818039 2	<p>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.</p>	4	8.1
2794688 5	<p>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.</p> <p>Workaround: Change the password for the following user types if they are encrypted with SHA-512: admin, li-admin, and user</p>	4	8.1
2763124 1	<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 8-1 (Cont.) OCSDM Known Issues

Defect Number	Description	Severity	Found
2706920 1	<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
2591891 8	<p>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.</p>	4	8.0
2760127 0	<p>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.</p> <p>Workaround: Use a different web browser or to enable 3-D mode on the line graph through the Layout Editor.</p>	4	8.1
2769984 8	<p>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.</p> <p>Workaround: In OCSDM, delete the old LI configuration, and enter the current LI configuration that you want to use.</p>	3	8.1
2535389 1	<p>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.</p>	4	7.5M3
2812925 5	<p>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.</p> <p>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.</p>	3	8.1

Table 8-1 (Cont.) OCSDM Known Issues

Defect Number	Description	Severity	Found
2538219 8	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
2641711 1	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
2871525 0	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
2870757 0	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
2874203 2	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
2881796 2	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
282014 85	In OCSDM Release 8.1, the sip-codec-per-realm HDR group is not supported.	4	8.1	8.2.0
281943 22	In OCSDM Release 8.1, the sa-srtp HDR group is not supported.	4	8.1	8.2.0
283960 76	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

ID	Description	Severity	Found In	Fixed In
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
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
245881 16	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

Caveats and Limitations

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

Oracle Communications Session Delivery Manager

- Migration from OCSDM 7.5M3 to OCSDM 8.2.1 is not supported. Customers running OCSDM 7.5M3 must first migrate to any previous release of OCSDM 8.x and then upgrade to 8.2.1.
- 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 ACLI.
- 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.

- 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**, and then **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**.
- The ability to use an offline configuration to provision network function (NF) device clusters is not available for the Acme Packet 9200 platform.
- 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.

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 ACLI 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.
- A CXF (SOAP) client may have its connection closed by the server for long duration transactions.

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.

- Report Manager does not support data gathering or the TscfStats group for SBC devices with ScZ7.4.0 and ScZ7.4.0p1 releases. This problem will be fixed in the ScZ7.4.0p2 release.
- 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.
- 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 DB 12c/BIP 12.2.1.1.0 and not DB 11g. Therefore, during migration from a previous OCSDM 8.x release (running 11g) to OCSDM 8.2.1, only Element Manager is migrated and Report Manager is not.

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 8.1.

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

Table A-3 (Cont.) SCZ Software Support

Base Software Release	Follow-on Releases
S-Cz7.2.0	M1, M2, M3, M4, M5, M6
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	-

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	-

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	-

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

OCSEM Plug-in Name	Plug-in Version	Devices
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
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)

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