

Oracle® Communications Session Delivery Manager Security Guide



Release 8.1
October 2018

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

ORACLE®

Copyright © 2014, 2018, 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

1	Session Delivery Manager Application Overview	
	Session Delivery Manager Product Plug-in Service	1-1
2	Secure Installation Guidelines	
	Secure the Server	2-1
	Check Firewall Settings	2-1
	System Support for Encryption and Random Number Generators	2-4
	Web Server Security	2-4
	Transport Layer Security Certificates	2-5
	Secure System Password Guidelines	2-6
	Resiliency and High Availability	2-6
3	Security Manager Feature Overview	
	Security Manager	3-1
	User Groups	3-1
	Users	3-1
	User Group Privileges	3-2
	User Inactivity Timer	3-2
	Audit Logs	3-2
	External User Authentication	3-3
4	Security Maintenance	
	Security Checklist	4-1
	Maintain Security Updates	4-2
	Security Considerations for Developers	4-2
	Database Redundancy	4-2

List of Tables

	Oracle Communications Session Delivery Manager Documentation Library	5
2-1	Communication Between OCSDM Cluster and Network Clients	2-2
2-2	Communication Between OCSDM Cluster and Network Devices	2-2
2-3	Communication Between OCSDM Servers in the Cluster	2-3

About This Guide

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

Oracle Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at <http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc>.

Related Documentation

Table 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 (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.

Revision History

Date	Description
July 2018	Initial release

1

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.

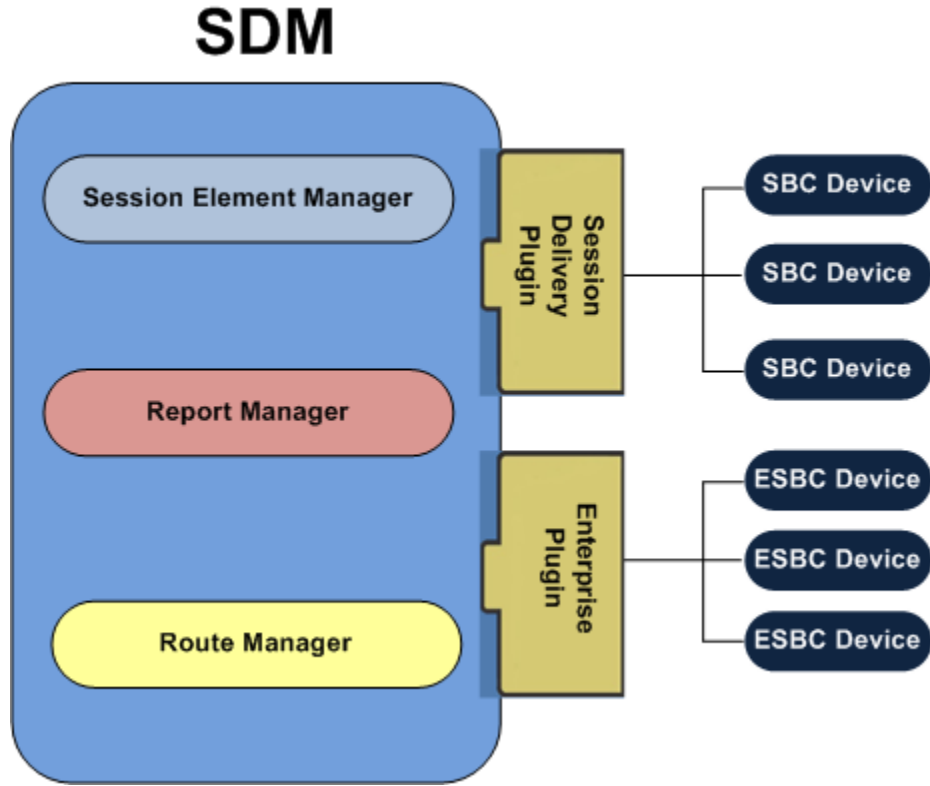
 **Note:**

Other sliders, such as the Device Manager, Configuration Manager, Performance Manager, and so on, are not displayed until you install a product plug-in.

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.

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 Prover and Enterprise product plugins provide their respective devices access to Session Element Manager, Report Manager and Route Manager.



2

Secure Installation Guidelines

This chapter outlines installation options for Oracle Communications Session Delivery Manager, and provides guidelines to install Oracle Communications Session Delivery Manager securely on your server. See your product installation guide for more information.

Secure the Server

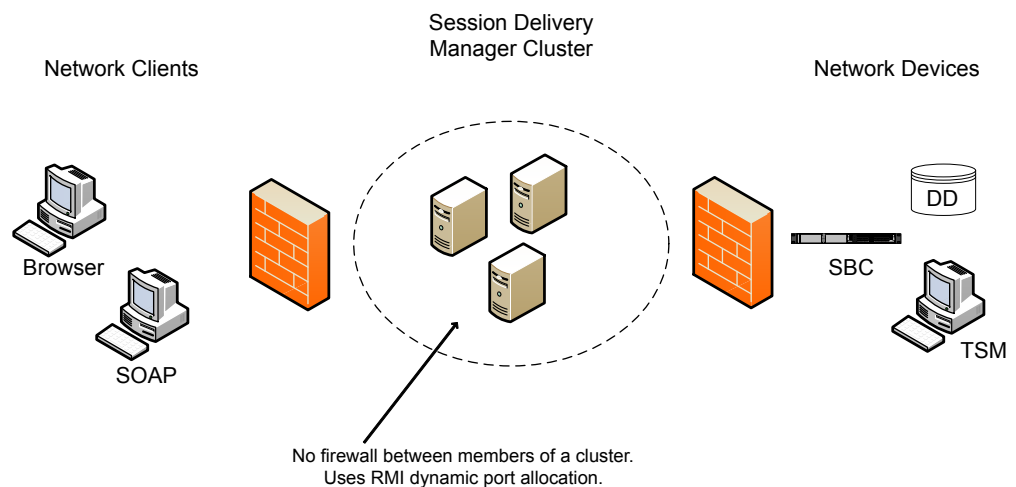
You must secure the server before you install Oracle Communications Session Delivery Manager .

Use the following documents to help secure the server on which Oracle Communications Session Delivery Manager is installed:

- [Guide to the Secure Configuration of Red Hat Enterprise Linux 6](#)
- [Hardening Tips for the Red Hat Enterprise Linux 6](#)
- [Oracle Linux Security Guide for Release 6](#)
- [Tips for Hardening an Oracle Linux Server](#)
- [CentOS Wiki: OS Protection](#)

Check Firewall Settings

When setting up Oracle Communications Session Delivery Manager (OCSDM) in your network, you may have a firewall between the clients (browsers, SOAP, etc.) and the OCSDM cluster, and a firewall between the OCSDM cluster and other devices.



**Note:**

You cannot have firewalls between the servers in a cluster.

If firewalls exist on either side of the OCSDM cluster, ensure the ports listed in the following table are open. If your operating system comes with a firewall, you need to apply the same criteria. You must switch off the firewall in your operating system or ensure these ports are available.

Table 2-1 Communication Between OCSDM Cluster and Network Clients

Port Number	Protocol	Service	Configurable	Affects Firewall?	Purpose
8443	TCP	HTTPS	N	Y	Apache port. HTTPS port for client/server communication.
8080	TCP	HTTP	N	Y	HTTP port for client/server communication.

Table 2-2 Communication Between OCSDM Cluster and Network Devices

Port Number	Protocol	Service	Configurable	Affects Firewall?	Purpose
161	UDP	SNMP	N	Y	SNMP traffic between the SDM server and the device.
162	UDP	SNMP	N	Y	SNMP trap reporting from the device to the OCSDM server.
21	TCP	FTP	N	Y	Used for file transfer.
22	TCP	SFTP/SSH	N	Y	Used for secure file transfer (such as Route Manager and LRT updates) and SSH sessions between OCSDM and southbound devices (For example, SBC).

Table 2-2 (Cont.) Communication Between OCSDM Cluster and Network Devices

Port Number	Protocol	Service	Configurable	Affects Firewall?	Purpose
3001/ 3000	TCP	ACP/ACLI	N	Y	Used by OCSDM to communicate with all versions of a device except for the Acme Packet 9200.

Table 2-3 Communication Between OCSDM Servers in the Cluster

Port Number	Protocol	Service	Configurable	Affects Firewall?	Purpose
22	TCP	SFTP	N	Y	Used to transfer files between OCSDM servers.
1098	TCP	RMI	N	Y	RMI Communication between host members in a cluster.
1099	TCP	RMI Lookup	N	Y	RMI registry port. Used for the RMI communication between host members in a cluster.
8005	TCP	HTTP	N	Y	Tomcat shutdown port used by the shutdown script. Can be blocked on a firewall because it is local to the OCSDM server.
8009	TCP	Apache	N	Y	Tomcat port.
8088	UDP	Coherence	N	Y	Used by the OCSDM Coherence REST application to handle HTTP requests on localhost and port 8088.
9000	TCP	Berkeley	N	Y	Berkeley database.
61616	TCP	Apache	N	Y	Message broker.

Either port 8080 (HTTP) or port 8443 (HTTPS) must be open on the firewall, depending on which port you select between the network client and OCSDM server.



Note:

Ports are assigned dynamically through Remote Method Invocation (RMI) dynamic port allocation. If you are enabling and configuring iptables, all traffic must be allowed between servers in the cluster. Communication between clustered OCSDM servers must not be restricted.

System Support for Encryption and Random Number Generators

The following table describes HTTPS web encryption, password encryption, and safe file transfer system support.

Algorithm(s)	Type	Bit Length	Description
MD5 and SHA-1	Asymmetric	128	Provides the following HTTPS encryption support: <ul style="list-style-type: none"> • Weak cipher secure socket layer (SSL) Version 2.0 • Strong cipher SSL 3.0 • Strong Transport Layer Security (TLS) 1.0, 1.1, 1.2
Password-based Encryption (PBE)	Symmetric	16	Encrypts stored passwords. During the system run time, all the passwords obtained, generated, stored, or transmitted are encrypted using password-based encryption (PBE).
3des-cbc, aes128-cbc, aes192-cbc, aes256-cbc, aes256-Gcm@openssh.com, aes128-Gcm@openssh.com, aes128-ctr, aes192-ctr, aes256-ctr, 3des-ctr, arcfour, arcfour128, arcfour256	Asymmetric	128	Provides secure shell version 2 (SSH2), and secure file transfer protocol (SFTP) communications support for file transfer between servers, and between servers to devices.

Web Server Security

During the installation, when you are in the Typical Installation mode, HTTPS is selected for you (by default) as the running mode of your system. We recommend that you maintain the default (HTTPS) to create secure connections over the network. If you have a specific reason for not using the default, you can alternately select HTTP (unsecured). See the *Configure Web*

Server Security section of your Oracle Communications Session Delivery Manager Installation Guide for more information.

 **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 to support the options of running HTTPS with Transport Layer Security (TLS) 1.0, 1.1, and 1.2.

HTTPS Certificate Support

Oracle Communications Session Delivery Manager fully supports X.509 certificates and the following certificate extensions are supported through HTTPS:

- .csr—Certificate signing request certificate used in public key infrastructure (PKI) systems.
- .cer—Internet security certificate (CER) in sockets layer (SSL) format that is used by web servers to help verify the identity and security of a site in question. SSL certificates are provided by a third-party security certificate authority such as VeriSign, GlobalSign or Thawte.
- .crt—Certificate is used with a web browser to verify the authenticity of a secure website, and is distributed by certificate authority (CA) companies such as GlobalSign, VeriSign and Thawte. CRT files allow a web browser to connect securely using SSL, and can be viewed by clicking the lock icon within your web browser.
- .der—Distinguished encoding rules certificate provides a method for encoding a data object, such as an X.509 certificate, to be digitally signed or to have its signature verified.

Set the Maximum Upload File Size Limit

You can optionally configure the upload file-size limit, from 2 to 100 gigabytes (GB) for files being uploaded to the web server for its secure operation. The default upload file-size limit is 2 gigabytes. See the *Configure Web Server Security* section of your Oracle Communications Session Delivery Manager Installation Guide for more information.

Transport Layer Security Certificates

Transport Layer Security (TLS) provides a single secure sockets layer (SSL) keystore of entity or trusted certificates that provide support for all applications, product plugins, and their respective devices that run on Oracle Communications Session Delivery Manager.

See the *Oracle Communications Session Delivery Manager Installation Guide* for more information about configuring transport layer security certificates.

 **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 to support the options of running HTTPS with TLS 1.0, 1.1, and 1.2.

Secure System Password Guidelines

No default passwords are used in the system, and the system ensures that permissions for generated files (such as temp files, configuration files, and log files) are as restrictive as possible so that they cannot be read or edited. During the system run time, all the passwords obtained, generated, stored, or transmitted are encrypted using password-based encryption (PBE).

Use the following guidelines to create the applicable user accounts:

1. Create the **nncentral** group and **nncentral** user account on the Oracle Communications Session Delivery Manager server to set permissions and lock file systems.
2. Specify limited privileges for an NNCentral user on the Linux server, so this user can administer OCSDM operations on the server by using visudo to make edits to the sudoer configuration file.
3. In the OCSDM setup installation program, configure the sudo password on the system in the Fault Management configuration. This password is required to enable a trap listener to listen on port 162 and forward device traps from OCSDM to its main northbound trap receiver(s).

 **Note:**

The main OCSDM process has to run as a sudo user to access port 162.

4. Also in the OCSDM setup installation program, configure the default user account passwords for the **admin** and **LJadmin** user groups before starting OCSDM.
5. Use the default Oracle database accounts for the Report Manager installation.

Resiliency and High Availability

Oracle Communications Session Delivery Manager offers high availability and resiliency through clustering to create a reliable deployment. When the product is deployed in a cluster, it protects the service of multiple individual members if one or more members fail. See your product installation guide for more information.

3

Security Manager Feature Overview

You can use the Oracle Communications Session Delivery Manager Security Manager slider to manage user accounts and maintain the authentication and authorization policies for each user.

This chapter provides an overview of the Security Manager features. See the *Oracle® Communications Session Delivery Manager Administration Guide* Security Manager chapter for more information about these features and how they are configured.

Security Manager

With administrator privileges, Security Manager allows you to do the following:

- Create and manage users.
- Create and manage groups.
- Configure security authorization levels, policies and privileges for user groups.
- Provide specific access controls for individual user groups, views, and operations.
- Limit access to specific features and functionality for specific users.
- Configure audit log parameters.

User Groups

A user group is a logical collection of users grouped together to access common information or perform similar tasks in OCSDM. The default **LIAdministrators**, **administrators**, **provisioners**, and **monitor** user groups are provided in OCSDM for you, or you can add new user groups so that you have the flexibility to define specific privileges for them based on the unique needs of your users. You can also map a local default user group or a local user group that you add in OCSDM to an external domain user group provided by RADIUS or LDAP authentication so that the external group can inherit the authorization privileges of the local user group.

Users

A user is a person who logs into the system to perform application-related operations. Before this user can access any operations, they must be added to a user group. Each user group has a defined set of privileges. The operations that a user can do depends on the privileges of the user group to which the user belongs.

The following guidelines are used for user names:

- Use a minimum of 3 characters and maximum of 50 characters.
- The name must start with an alphabetical character.
- The use of alphanumeric characters, hyphens, and underscores are allowed.
- The name is case insensitive.

- The name cannot be the same as an existing group name.

The following guidelines are used for user passwords:

- The password must be at least 8 characters long.
- Use at least one numeric character from 0 to 9 in the password.
- Use at least one alphabetic character from the English language alphabet in the password.
- Special characters include {, |, }, ~, [, \,], ^, _, ' , ; , < , = , > , ? , ! , " , # , \$, % , & , ` , (,) , * , + , , , - , . , and /
- You can configure when passwords expire or if they expire.

User Group Privileges

In Oracle Communications Session Delivery Manager, user group privileges can be applied to user groups that you add to allow or deny all users within this user group the ability to perform certain operations. This includes items intended for use with separate application products. For the default **LIAdministrators**, **administrators**, **provisioners**, and **monitor** user groups, only device group privileges can be changed.

User group privileges that are assigned to either the **administrators** or **LIAdministrators** user groups inherit most of the same access privileges. However, users assigned to the **LIAdministrators** user group have full configuration privileges to manage the **Configure LI** element (Lawful Intercept) in the **Device configuration** subfolder within the **Configuration** folder in the **Configuration** tab. Users assigned to **administrators**, **provisioners** and **monitors** default user groups do not have privileges to configure the **Configure LI** element.

Note:

If Lawful Intercept (LI) is enabled on a device that OCSDM manages, LI configuration values become encrypted on this device and OCSDM.

User Inactivity Timer

We recommend configuring the inactivity timer to prevent unauthorized access to the system.

The inactivity timer logs off the user from the Oracle Communications Session Delivery Manager session when its value is exceeded. The user must re-enter their password to continue. You can set different values for a user with administrative permissions and users who do not have administrative permissions.

Audit Logs

You can use the audit log (containing audit trails) generated by OCSDM to view performed operations information, which includes the time these operations were performed, whether they were successful, and who performed them when they were logged into the system.

Note:

Audit logs contain different information depending on its implementation.

Audit trails include the following information:

- The user who performed the operation.
- What operation was performed by the user.
- When the operation was performed by the user.
- Whether the operation performed by the user was successful or failed.

External User Authentication

Users who belong to the external domain user group are authenticated outside of OCSDM by an external domain server. You can select either a RADIUS domain server or Active Directory (AD) domain controller:

- A RADIUS server provides centralized Authentication, Authorization, and Auditing/Accounting (AAA) security protocol management for users who connect and use a network service.
- An AD domain controller provides a directory service in a Windows domain type network using Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Microsoft's version of Kerberos, and DNS.

An external domain user group must be mapped to an internal (local) user group in OCSDM so that this external domain user group and its users inherit the authorization privileges that are specific to the local user group.

 **Note:**

Internal and external users are both supported simultaneously. However, external users do not have corresponding stored user records or username and password information.

4

Security Maintenance

Use the security maintenance practices in this chapter to keep Oracle Communications Session Delivery Manager secure.

Security Checklist

Use the following checklist to secure Oracle Communications Session Delivery Manager before, during and after its installation.

1. Do **NOT** connect your system to any untrusted networks, especially the Internet, until all protections have been configured. Customers have reported systems under configuration compromised within minutes due to incomplete configurations.
2. If you use identity management or single sign-on (SS) technologies, ensure that they are supported by security assertion markup language (SAML).
3. Harden the management environment.
 - a. Make sure all equipment is in locked cabinets or at least in a secure room.
 - b. Set strong passwords for all accounts and system users (nncentral user and nncentral group, sudo user, e-mail user, the admin user, L1admin user etc.) during the installation.
 - c. During the system installation, use **HTTPS** (default) as the system running mode.
 - d. Use secure protocols, such as SFTP, HTTPS, LDAP and SSH, to communicate with Oracle Communications Session Delivery Manager.
4. Once Oracle Communications Session Delivery Manager is started, use the Security Manager to limit user privileges:
 - a. Carefully consider who has access to the **administrators** password.
 - b. Authenticate local groups and users that access the system. The system comes with the following default user groups: **monitor**, **provisioner**, **administrators**, and **L1administrators**. Administrators have a complete set of permissions only, and the system provides role-based security policies for access control with dedicated user accounts that have pre-assigned privilege levels.
 - c. Authenticate and authorize external users through an existing RADIUS server or Active Directory (AD) server.
5. Configure the inactivity timer in Security Manager to stop the abuse of system services.
6. Use HP Fortify, HP WebInspect, and Tenable Nessus scans to perform static and dynamic security testing on Oracle Communications Session Delivery Manager periodically, or after each release.
7. Continue to monitor system activity to determine if someone is attempting to abuse system services and to detect if there is performance or availability problems. Useful monitoring information can be acquired through audit logs, system logs and SNMP.

Maintain Security Updates

You must install all security patch releases for Oracle Communications Session Delivery Manager software when they appear or as soon as possible to keep your system secure.

Oracle constantly reviews the latest security vulnerabilities, applies any required critical security patch (including any third-party components) to the Oracle Communications Session Delivery Manager software, and issues a security patch release with release notes that describe these updates. See the [Critical Patch Updates and Security Alerts](#) web page for these updates and other current security information. You can also use the instructions on this web page to receive email notifications for the following announcements:

- Critical Patch Updates
- Security Alerts
- Third Party Bulletins
- Fixed Public Vulnerabilities
- Policies
- Security Vulnerability Reports

Security Considerations for Developers

We highly recommend that application developers fully secure the link between the Web services application (Web service client) and follow secured coding standards.

Oracle Communications Session Delivery Manager offers a REST Application Programming Interface (API) and a SOAP/XML API to allow users to write applications that automate the provisioning of network elements. See the *REST API for Oracle® Communications Session Delivery Manager Release 8.1* for more information.

 **Note:**

The *Oracle® Communications Session Element Manager SOAP API Guide Release 8.1* is deprecated, but supported for backwards compatibility, however for new OCSDM features, the *REST API for Oracle® Communications Session Delivery Manager Release 8.1* is recommended.

You can use these APIs to perform operations against network elements managed by an OCSDM server, and data structures used as input and output parameters for those operations. These operations are invoked by a client application to provision network elements.

Database Redundancy

Use backup and restore scripts to implement the database geographic (GEO) redundancy. See the *Oracle® Communications Session Delivery Manager Administration Guide* for more information.