

**Oracle® Communications Session Delivery
Manager**
Installation Guide
Release 7.5

November 2017

Notices

Copyright© 2017, 2012, Oracle and/or its affiliates. All rights reserved.

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

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

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

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

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

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

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

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

Contents

About This Guide	5
Revision History.....	6
1 Pre-Installation Tasks	9
Check System Requirements.....	10
Shut Down the System.....	11
Upgrade to a Supported Version of Linux.....	12
Upgrade Linux on Your Server.....	12
Check Firewall Settings.....	12
Edit the Hosts File.....	14
Disable the Default HTTP Daemon.....	15
Specify the System Locale.....	15
Resolve Any RPM Installation Dependencies.....	15
Configure the NNCentral Account.....	16
Add the NNCentral Group and NNCentral User Account.....	17
Specify NNCentral User Privileges.....	17
Unzip the Tar File to Create the Installation Directory.....	17
2 Typical Installation	19
Start the Installation.....	19
Upgrade Oracle Communications Session Delivery Manager.....	20
Transfer Application Data to the New Version.....	20
Select the Product Installation.....	23
Select the Typical Installation.....	23
Configure User Account Passwords.....	23
Specify the Global ID for Northbound Trap Receivers.....	24
Configure Web Server Security.....	24
Configure Fault Management.....	26
Start the Oracle Communications Session Delivery Manager Server.....	26
Check Server Processes.....	27
3 Custom Installation	29
Start the Installation.....	29
Select the Custom Installation.....	30
Configure the Mail Server.....	30
Configure Clusters.....	31
Add New Members to a Cluster.....	31
Managing Cluster Members.....	32
Delete a Cluster.....	32
Configure a Clustered Server to be a Standalone Server.....	32
Configure Route Management Central.....	32
Configure Southbound Interface Transport Layer Security.....	33
Configure Entity Certificates.....	33
Configure Trusted Certificates.....	33
About Creating a Report Manager Database Instance on the External Oracle Database.....	34
Exit the Custom Installation.....	34
Start the Oracle Communications Session Delivery Manager Server.....	34
Check Server Processes.....	35

4 Install Software Patches.....	37
Shut Down Your System.....	37
Shut Down the System.....	37
Shut Down the Cluster System.....	38
Install a Session Delivery Manager Patch.....	38
Check Your Setup Configuration After a Patch Installation.....	40

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
Release Notes	Contains information about the administration and software configuration of the Oracle Communications Session Delivery Manager feature support new to this release.
Installation Guide	The Installation guide describes the process to install the Session Delivery Manager including both the typical installation process as well as the custom installation options.
Administration Guide	Contains information about security administration, which lets you create new users and new user groups, and set group-based authorization.
Security Guide	Provides the following security guidelines and topics: <ul style="list-style-type: none">• Guidelines for performing a secure installation of Oracle Communications Session Delivery Manager 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.• An overview of the Security Manager features that are used to configure groups, users, operations, privileges, and manage access to the system.• Security maintenance, which includes a checklist to securely deploy Oracle Communications Session Delivery Manager on your network, maintaining security updates, and security considerations for developers.

Table 2: Oracle Communications Session Element Manager Documentation Library

Document Name	Document Description
User Guide	Contains detailed information pertaining to the Session Element Manager application and describes the dashboard summary view, audit log, fault, and performance views.

About This Guide

Document Name	Document Description
Web Services SOAP XML Provisioning API Guide	Contains a full description of the individual interface definitions that make up the Application Programming Interface (API).

Table 3: Oracle Communications Report Manager Documentation Library

Document Name	Description
User Guide	Contains information about configuring Report Manager to interoperate with Oracle BI Publisher as well as creating reports on network devices.
Installation Guide	Contains instructions for installing Oracle Communications Report Manager as an Add-on to the Session Delivery Manager including the database and BI Publisher components.

Table 4: Oracle Communications Session Route Manager Documentation Library

Document Name	Description
User Guide	Contains documentation and about using the Session Route Manager with Oracle Communications Session Delivery Products.


Revision History

Date	Description
August 2015	<ul style="list-style-type: none">Initial release
January 2016	<ul style="list-style-type: none">The organization of the content was improved, missing sections and information were added, incorrect information was fixed, and the content has been improved overall.
February 2016	<ul style="list-style-type: none">Changed the Set the Global Identifier section so that it provides more information for why the global identifier is set.
April 2016	<ul style="list-style-type: none">The <i>About This Guide</i> section was updated.The <i>Oracle Legal Notices</i> section was updated.Added a step to each of the <i>Transfer Application Data</i> sub-sections that prompts the user to continue and complete the installation in order to use the current product version on their system(s).The <i>Configure HTTP or HTTPs</i> section was changed to <i>Configure Web Server Security</i>. The following Web server security features were added:

Date	Description
	<ul style="list-style-type: none"> • HTTPS is now the default installation option for your Web server. • You can now specify maximum upload file size limitations.
July 2016	<ul style="list-style-type: none"> • A note was added to the <i>Upgrade Communications Session Delivery Manager</i> section in the <i>Typical Installation</i> chapter that says if you are upgrading Report Manager, the Oracle Database and Oracle BI Publisher must be running before you upgrade Oracle Communications Session Delivery Manager. • A note was added to the <i>Configure Web Server Security</i> section in the <i>Typical Installation</i> chapter that says the specified DNS server name must match the common name (CN) of the certificate.
January 2017	<ul style="list-style-type: none"> • The <i>Check System Requirements</i> section in the <i>Pre-installation Tasks</i> chapter was updated to indicate that the server on which Oracle Communications Session Delivery Manager is installed requires a 300 GB hard drive. • The syntax for specifying the NNCentral user privileges in the sudoer configuration (step 4) in the <i>Specify NNCentral User Privileges</i> section of the <i>Pre-installation Tasks</i> chapter was fixed. • The <i>Set the Global Identifier</i> section was renamed <i>Specify the Global ID for Northbound Trap Receivers</i> and the introductory paragraph was updated for clarity.
November 2017	<ul style="list-style-type: none"> • OpenSSL information was added to the <i>Check System Requirements</i> section.

Pre-Installation Tasks

Read and understand the summary of pre-installation tasks that need to be done before installing Oracle Communications Session Delivery Manager. Each of these pre-installation tasks are described in more detail in subsequent sections.

 **Note:** This installation assumes that the Linux installation directory is the /opt directory. If you decide to use a different installation directory, remember to modify any commands or strings so that they comply with your installation directory schema.

1. Read and understand this installation guide, and see the flow diagram below for more information about how to use the product documentation for installing or upgrading Oracle Communications Session Delivery Manager with the Oracle Communications Report Manager application.

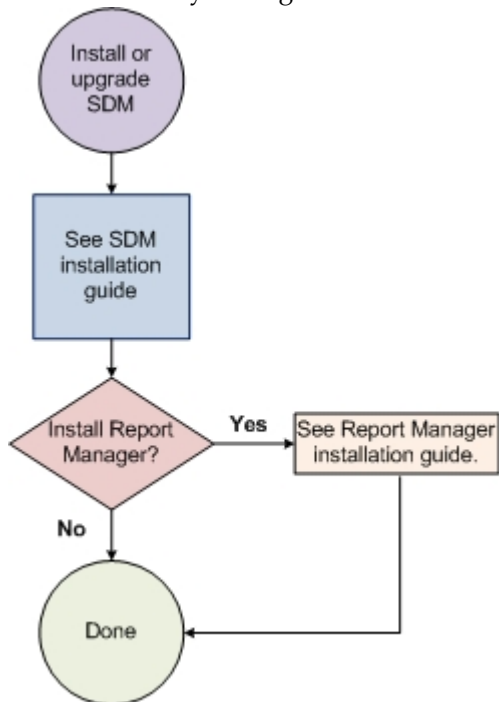



Figure 1: Installing or upgrading Oracle Communications Session Delivery Manager with Report Manager

2. Check to ensure your system meets the minimum requirements.
3. Shut down your Oracle Communications Session Delivery Manager server(s).

Pre-Installation Tasks


4. Upgrade the version of Linux on your server(s) on which Oracle Communications Session Delivery Manager is running, if the version of Linux is not supported with the release of Oracle Communications Session Delivery Manager that you are installing.
5. Open the appropriate ports on the network and system firewall.
6. If your system does not rely on DNS, edit the `/etc/hosts` file to specify a host name for your system.
7. Disable the default `httpd` daemon.
8. Specify your system locale to the US English language UTF-8 character encoding method (`LANG=en_US.UTF-8`).
9. If any required redhat Package Manager (RPM) software libraries that are shared with Oracle Communications Session Delivery Manager are missing, you must install them using the `yum` program.

 **Note:** Your system may already have the required RPM software libraries.

10. Setup the `nncentral` group and user account to administer Oracle Communications Session Delivery Manager server operations on your Linux server.
11. Unzip the Oracle Communications Session Delivery Manager tar file on your server to create the installation directory (called `AcmePacket`) for Oracle Communications Session Delivery Manager.

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

OpenSSL

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 Feb 2016
```

Certified Operating Systems


- Oracle Linux 6.3, 6.4, 6.5, 6.6, 6.7 64-bit
- Red Hat Linux 6.3, 6.4, 6.5, 6.6, 6.7 64-bit
- CentOS 6.3, 6.4, 6.5, 6.6, 6.7 64-bit

Session Border Controller Hardware Requirements

The Oracle Communications Session Delivery Manager supports the following SBC hardware:

- Acme Packet 1100
- Acme Packet 2600
- Acme Packet 3800
- Acme Packet 3810
- Acme Packet 3820
- Acme Packet 4250

- Acme Packet 4500
- Acme Packet 4600
- Acme Packet 6100
- Acme Packet 6300
- Acme Packet 7000
- Acme Packet 7250
- Acme Packet 9200
- Acme Packet 17350
- Acme Packet Enterprise Session Director - Server Edition
- Acme Packet Enterprise Session Director - Virtual Machine Edition

 **Note:** For the Acme Packet 2600, the Oracle Communications Session Delivery Manager supports traps in Fault Management. For performance statistics and configuration management, the Session Delivery Manager will redirect the user to the Acme Packet 2600 onboard GUI.

Client Requirements

- We recommend Internet Explorer versions 11.0 and later, Mozilla Firefox versions 26.0 (10.0 Linux) and later, or Google Chrome version 44.0 or 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.

Shut Down the System


You can shut down the existing Oracle Communications Session Delivery Manager software version running on your system to install a new version of the software, restore a database or apply a software patch.

1. Log in as the nncentral user.
2. Change directory to the bin directory.

For example:

```
cd /opt/AcmePacket/NNC75/bin
```

3. Execute the **shutdownnnc.sh** script. By default, the shutdownnnc.sh script detects whether the existing installation is a standalone or clustered system and prompts you with the option to shut down the entire cluster if no flag options are provided.

 **Note:** However, You can script an option ahead of time by adding -local for single nodes and -cluster to shutdown an entire cluster.


```
./shutdownnnc.sh
Shutdown back-end server
Do you wish to shut down the entire cluster (Yes/No)? Yes
```

Upgrade to a Supported Version of Linux

This task is optional. Use this task if you have an old version of Linux that needs to be upgraded to a supported version of Linux in order to install the latest version of Oracle Communications Session Delivery Manager.

Upgrade Linux on Your Server

Use this task if you need to upgrade the Linux server operating system on your server in order to upgrade Oracle Communications Session Delivery Manager.


 **Note:** Ensure that the server is shut down before you do this task. See the *Shut Down Your System* section for more information on shutting down the Oracle Communications Session Delivery Manager server.

1. Log in to the server as the nncentral user.
2. Change to the bin directory. For example:

```
cd /opt/AcmePacket/NNC7x/bin
```

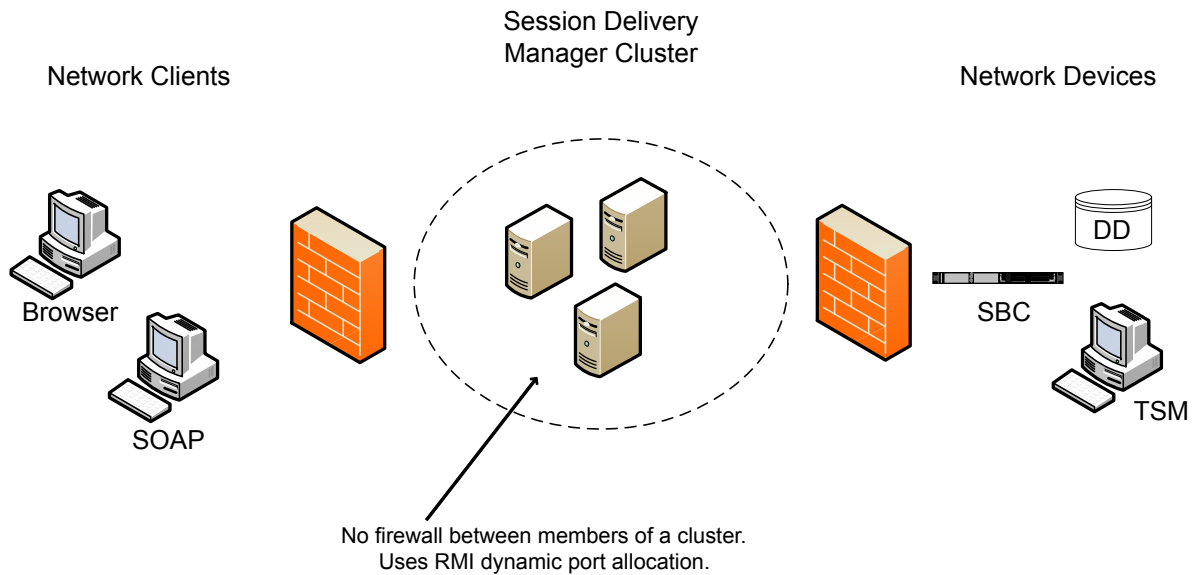
3. Perform a cold backup of the application database (that is, the Oracle Communications Session Delivery Manager server is shut down) to a local server or remote server directory path, enter the **backupdbcold.sh** script. For example:

```
backupdbcold.sh /<path>/ColdBackup_YYYY_MM_DD_<title>.tar.gz
```

-  **Note:** See the Database Tasks chapter in the *Oracle Communications Session Delivery Manager Administration Guide* for more information on restoring the application database.
4. Upgrade the server to a supported version of Linux. See *Check System Requirements* for more information.
 5. Repeat the steps above if you need to upgrade another Linux server on which Oracle Communications Session Delivery Manager needs to run.

Check Firewall Settings

When setting up Oracle Communications Session Delivery Manager in your network, you may have a firewall between the clients (browsers, SOAP, etc.) and the Oracle Communications Session Delivery Manager cluster, and a firewall between the Oracle Communications Session Delivery Manager cluster and other devices (SBCs, Data Domain (DD), Terminal Server Manager (TSM)).



Note: You cannot have firewalls between the servers in a cluster.


If firewalls exist on either side of the Oracle Communications Session Delivery Manager 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.

Port Number	Protocol	Service	Configurable	Affects Firewall?	Purpose
Between Oracle Communications Session Delivery Manager Cluster and Network Clients					
8443	TCP	HTTPS	N	Y	Apache port. HTTPS port for client/server communication.
8080	HTTP	HTTP	N	Y	HTTP port for client/server communication.
Between Oracle Communications Session Delivery Manager Cluster and Network Devices					
161	UDP	SNMP	N	Y	SNMP traffic between the SDM server and the SBC.
162	UDP	SNMP	N	Y	SNMP trap reporting from the SBC to the Oracle Communications Session Delivery Manager server.
22/21	SFTP/FTP				Used for file transfer (such as Route Manager and LRT updates).
8080	HTTP	AMI	N	Y	Used by Oracle Communications Session Delivery Manager to communicate with 9200 devices via AMI.
5060	TCP		N	Y	Used for Oracle Communications Session Delivery Manager Trunk Manager (SIPTX) to communicate with SP-SBC.

Pre-Installation Tasks

Port Number	Protocol	Service	Configurable	Affects Firewall?	Purpose
3001/ 3000		ACP/ ACLI			Used by Oracle Communications Session Delivery Manager to communicate with all versions of the SBC except for the Acme Packet 9200.
Between Oracle Communications Session Delivery Manager Servers in the Cluster					
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.
5701	TCP	Hazelcast	N		Used by Hazelcast communication for distributed data structures, peer-to-peer collective data distribution.
5000/ 5801	TCP	Hazelcast	N	Y	Used by the Hazelcast management console port for the Oracle Communications Session Delivery Manager distributed scheduler service.
54327	UDP	Hazelcast	N	Y	Used by Hazelcast for cluster member discovery.
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 Oracle Communications Session Delivery Manager server.
8009	TCP	Apache	N	Y	Tomcat port.
9000	TCP	Berkeley	N	Y	Berkeley database.
61616	TCP	Apache	N	Y	Message broker.
22	SFTP	ActiveMQ	N	Y	Used to transfer files between Oracle Communications Session Delivery Manager servers.

Either port 8080 (HTTP) or port 8443 (HTTPS) must be open on the firewall, depending on which port you choose between the network client and Oracle Communications Session Delivery Manager server. If installing on a Linux system, the Linux firewall must also have either 8080 (HTTP) or port 8443 (HTTPS) open.

 **Note:** Ports are assigned dynamically via Remote Method Invocation (RMI) dynamic port allocation. If you are enabling and configuring iptables/ipf, all traffic must be allowed between servers in the cluster. Communication between clustered Oracle Communications Session Delivery Manager servers must not be restricted.

Edit the Hosts File

If your system does not rely on DNS, add the system's hostname to the `/etc/hosts` file.

1. Log in as root.

- Determine your system's host name with the `hostname` command.
- Edit the `/etc/hosts` file to include the Linux system host name in the following format:

```
<IP address> <hostname> <hostname>.localdomain
```

For example:

```
[bash]$ cat /etc/hosts
127.0.0.1    localhost    localhost.localdomain
10.0.0.252  nncsvr      nncsvr.localdomain
```

Disable the Default HTTP Daemon

If your Oracle Communications Session Delivery Manager server is running a default HTTP daemon (HTTPD) process, disable that process from restarting.

- Log in as the root user.
- To discover if the HTTPD is installed or running:

```
service httpd status
```

The following message appears if the HTTPD is not installed. Continue to the next sections.

```
httpd: unrecognized service
```

The following message appears if the HTTPD is installed but not running. Continue to the next sections.

```
httpd is stopped
```

A message similar to the following appears if the HTTPD is installed and running:

```
httpd (pid 5644) is running...
```

- If the HTTPD is running, stop the HTTPD:

```
service httpd stop
```

- Disable the HTTPD from restarting when the system reboots:

```
chkconfig httpd off
```

- Verify that the HTTPD is not running:

```
service httpd status
```

Specify the System Locale

You must specify the system location to `LANG=en_US.UTF-8` (United States English language) in order for Oracle Communications Session Delivery Manager to install properly.

- Log in as the root user.
- Ensure that the US English language UTF-8 character encoding method (`LANG=en_US.UTF-8`) parameter is specified in the `i18n` (Internationalization) file in the `/etc/sysconfig/i18n` directory. This file specifies the current language settings.

Resolve Any RPM Installation Dependencies

The following table describes redhat Package Manager (RPM) software libraries that are shared with Oracle Communications Session Delivery Manager. These shared libraries need to be installed on your Linux system in order for Oracle Communications Session Delivery Manager to run properly:

Table 5: RPM software library packages shared with Oracle Communications Session Delivery Manager

Name	Description
apr	The Apache Portable Runtime (APR) supporting library is for the Apache web server that provides a set of application programming interfaces (APIs) that map to the underlying operating system (OS). The APR provides emulation where the OS does not support a particular function to make a program portable across different platforms.
apr-util	The Apache Portable Runtime Utility Library (APR-Util) provides a predictable and consistent interface for underlying client library interfaces. This API assures predictable if not identical behaviour regardless of which libraries are available on a given platform.
compat-expat1	Expat is a stream-orientated C language library XML parser used for parsing XML documents for Red Hat Fedora.
libxslt	The package contains extensible stylesheet language transformations (XSLT) libraries. These are useful for extending libxml2 libraries that are used to manipulate XML files to support XSLT files.
libaprutil	APR database binding library for the Apache web server.
libGL	OpenGL-based programs must link with the libGL library that implements the GLX interface as well as the main OpenGL API entry points.
libX11	The X.Org stack, which provides an open source implementation of the X Window System for the C language X interface. See the X.Org Foundation for more information.
libXxf86vm	X11 XFree86 video mode extension library provides an interface to the XFree86-VidModeExtension extension, which allows client applications to get and set video mode timings in extensive detail. It is used by the xvidtune program in particular.
alsa-lib	Advanced Linux Sound Architecture (ALSA) library package used by programs (including ALSA Utilities) requiring access to the ALSA sound interface.

If you are missing any RPM libraries in your Linux environment, run the "yum" program. Yum is the primary tool for getting, installing, deleting, querying, and managing Red Hat Enterprise Linux RPM software packages from official Red Hat software repositories, as well as other third-party repositories. Yum is used in Red Hat Enterprise Linux versions 5 and later. See the [redhat customer portal](#) for more information.

1. Log in to your Linux system on which Oracle Communications Session Delivery Manager is to be installed as the **root** user.
2. Install the RPM software on your linux system using the "yum" program. For example:

```
yum install -y libGL
```

Configure the NNCentral Account

For security reasons, you must create an NNCentral user account named `nncentral` and an NNCentral group named `nncentral` on the server to administer Oracle Communications Session Delivery Manager related server operations. You also must specify limited sudo privileges for the `nncentral` user and `nncentral` group. After the Oracle Communications Session Delivery Manager installation, all the installed files are owned by the `nncentral` account. The main Oracle Communications Session Delivery Manager process has to run as a sudo user in order to have access to port 162.

Add the NNCentral Group and NNCentral User Account

The nncentral group and user account must be added to administer Oracle Communications Session Delivery Manager server operations on your Linux server.

1. Log in as root.

2. Add the nncentral group

```
groupadd nncentral
```

3. Add the nncentral user account.

```
useradd -m -g nncentral -d /home/nncentral -s /bin/bash nncentral
```

4. Set the password for the nncentral user.

```
passwd nncentral
```

5. If you are prompted to enter a new password, reenter the password that you entered in step 4.


The following message displays:

```
passwd: all authentication tokens updated successfully.
```

Specify NNCentral User Privileges

You must specify limited privileges for an NNCentral user on the Linux server, so this user can administer Oracle Communications Session Delivery Manager operations on the server.

You must use visudo to make edits to the sudoer configuration file.

 **Note:** This file can only be edited using Linux visual text editor (vi editor) commands.

1. Log in as root.

2. Execute visudo.

```
# visudo
```


3. Press **i** to enter insert mode and begin adding text.

4. Add the following line to specify NNCentral user privileges in the the sudoer configuration to give the NNCentral user the limited authority to run Oracle Communications Session Delivery Manager later:

```
nncentral ALL=/opt/AcmePacket/NNC*/jre/bin/java * -Dlog4j.configuration=* -  
cp * com.acmepacket.ems.server.services.snmp.TrapRelay.TrapRelay *
```

5. Press Esc to return to command mode.

6. Press **:wq** to save your changes and exit visudo.

 **Note:** If you want to quit without saving your changes, press **:q!**.

7. Ensure that the sudoer configuration for the nncentral user is specified.

```
grep nncentral /etc/sudoers
```

Unzip the Tar File to Create the Installation Directory

Unzip the tar file to create the AcmePacket installation directory for the Oracle Communications Session Delivery Manager software.

1. Get the appropriate tar.gz file from the Oracle customer portal.

2. Copy the relevant tar.gz file to the installation directory (for example: /opt) on your server.

- If your server runs Oracle Linux, use the NNC<version_number>OracleLinux63_64bit.tar.gz file.
- If your server runs Red Hat or CentOS, use the NNC<version_number>RHEL63_64bit.tar.gz file.



Warning: This guide assumes the installation directory is /opt. Modify subsequent instructions accordingly if using a different installation directory.

Pre-Installation Tasks

3. Log in as root user.
4. Navigate to the /opt directory.

```
cd /opt
```

5. Extract the tar.gz file.

For example:

```
tar -xzvf NNC75RHEL63_64bit.tar.gz
```

The installation directory is created. For example:

```
/opt/AcmePacket/
```

Typical Installation

The Typical installation performs the minimal configuration required to run the Oracle Communications Session Delivery Manager server. The Typical installation:

1. Configures passwords for the default user accounts
2. Configures the global identifier
3. Configures either HTTP or HTTPS on your server
4. Configures the SNMP Trap Relay port for Fault Manager

Verify you have the correct sudo password before continuing.

Start the Installation

1. Log in as root user.
2. Navigate to the bin directory.

For example:

```
cd /opt/AcmePacket/NNC75/bin
```

3. Run setup.sh.

```
./setup.sh
```



Warning: This process may take several minutes to complete. Interrupting the setup.sh process risks corrupting the system.



Note: A warning message appears if you have less than the recommended minimum physical memory. Proceeding without the recommended minimum physical memory may result in performance degradation.



Note: Install missing packages with the command `yum install -y <package name>`. Then run setup.sh again.

Upgrade Considerations

If you are upgrading from a previous version of Oracle Communications Session Delivery Manager, the migration tool detects any previous versions and prompts you depending on whether the existing installation is on a standalone or clustered system.

You can complete the Oracle Communications Session Delivery Manager installation in standalone or cluster mode.

Typical Installation


If you try to migrate data without running setup first, the following message appears.

```
Starting Migration Application 2011-05-25 14:11:27,086
Please run OCSDM setup first. 2011-05-25 14:11:52,377
```

The following sections provide more information about transferring existing Oracle Communications Session Delivery Manager application data to the new version of Oracle Communications Session Delivery Manager. If you are installing Oracle Communications Session Delivery Manager for the first time, proceed to the *Select how Session Delivery Manager is Installed* section.

Upgrade Oracle Communications Session Delivery Manager

If you are upgrading Oracle Communications Session Delivery Manager from a previous version, you must transfer the existing application data to the new version. This includes Oracle Communications Route Manager, if you are updating this application too.

 **Note:** If you are upgrading Report Manager, the Oracle Database and Oracle BI Publisher must be running before you upgrade Oracle Communications Session Delivery Manager so that Report Manager database data is migrated.

Transfer Application Data to the New Version

You can transfer application data from the existing version of Oracle Communications Session Delivery Manager to the new version Oracle Communications Session Delivery Manager when you install the new version of Oracle Communications Session Delivery Manager. The data migration tool automatically detects older versions of Oracle Communications Session Delivery Manager during the setup and prompts you with the option of migrating data from the previous version of Oracle Communications Session Delivery Manager.

Transfer Data on a Standalone System

Transfer the application data on the master node (member) of the cluster system.

1. Enter 1 to proceed with database migration.

```
Setup has detected that database migration needs to be performed.
The migration process involves backing up the existing database and then
performing various operations to migrate the database to the current
version.
Depending on size of the existing database and the operations to be
performed,
this process may take up to an hour to complete, however you can cancel and
rollback the process at any time by pressing the <a> key followed by
<enter>.
Note that database migration MUST be performed before setup can continue.
[X] 1 - Proceed with database migration [Default]
[ ] 2 - Cancel and exit setup
Please select an option [1] 1
```

2. Enter Yes to migrate data from the previous Oracle Communications Session Delivery Manager installation.

```
[X] 1 - Proceed with database migration [Default]
[ ] 2 - Cancel and exit setup
Do you want to continue Yes/No? Yes
```

Pressing the a key anytime during the process aborts the current migration. You cannot be able to launch the target version of Oracle Communications Session Delivery Manager until setup is re-run and database migration is performed.

```
Database migration beginning.
To abort and rollback database migration, press <a> then <enter> at any time
```

The database migration starts and progress information displays on the screen.

```
backing up existing database....done
migrating database...done
creating migrated master database archive...done
Database migration is now complete.
Press <enter> to continue with setup
```

3. Press Enter to continue the Typical Installation and the Custom Installation of Oracle Communications Session Delivery Manager (depending on your installation requirements of Oracle Communications Session Delivery Manager). These installation(s) must be completed to use the current Oracle Communications Session Delivery Manager software version on this standalone system.

Transfer Data on the Master Node of the Cluster

Transfer the application data on the master node (member) of the cluster system.

1. Enter 1 to transfer application data from the previous Oracle Communications Session Delivery Manager installation.

```
Setup has detected that database migration needs to be performed.
The migration process involves backing up the existing database and then
performing various operations to migrate the database to the current
version.
Depending on size of the existing database and the operations to be
performed,
this process may take up to an hour to complete, however you can cancel and
rollback the process at any time by pressing the <a> key followed by
<enter>.
Note that database migration MUST be performed before setup can continue.
[X] 1 - Proceed with database migration [Default]
[ ] 2 - Cancel and exit setup
Please select an option [1] 1
```

2. When prompted, enter Yes to transfer application data from the previous Oracle Communications Session Delivery Manager installation.

```
[X] 1 - Proceed with database migration [Default]
[ ] 2 - Cancel and exit setup
Do you want to continue Yes/No? Yes
Database migration beginning.
To abort and rollback database migration, press <a> then <enter> at any time
backing up existing database....done
migrating database...done
creating migrated master database archive...done
```

3. Enter 1 to copy the transferred database to other cluster nodes.

```
Your existing setup is configured for a clustered environment. Setup on all
other nodes in your cluster will require the migrated database archive just
created. Setup can now attempt to copy this archive via SFTP to other
cluster
nodes.
Note that if you skip this step, you must manually copy the migrated
database
archive to all other nodes in the cluster, as this archive will be required
during setup on the other cluster nodes
[X] 1 - Copy the migrated database archive to other cluster nodes
[Default]
[ ] 2 - Do not copy the migrated database archive
Please select an option [1] 1
```

4. When prompted, enter Yes to continue.
5. Enter the username, password, and folder path for the SFTP credentials for each cluster node when prompted.

```
Provide SFTP credentials for cluster node 2.2.2.2:
username: [ ] myuser
password: [ ] xxxxx
```

Typical Installation

```
remote folder path: [          ] /home/myuser
remote folder path: [/home/myuser]
```

For example, a successful application data transfer shows information similar to the following:

```
cluster node: 2.2.2.2
destination file: /home/myuser/ColdBackup_2012_02_13_112911_db.tar.gz
result: SUCCEEDED
cluster node: 3.3.3.3
destination file: /home/otheruser/ColdBackup_2012_02_13_112911_db.tar.gz
result: SUCCEEDED
Press <enter> to continue
Database migration is now complete.
Press <enter> to continue with setup
```

6. Press Enter to continue the Typical Installation and the Custom Installation of Oracle Communications Session Delivery Manager (depending on your installation requirements of Oracle Communications Session Delivery Manager). These installation(s) must be completed to use the current Oracle Communications Session Delivery Manager software version on this master node system.

Transfer Data on Each Replica Node of the Cluster

Transfer the application data on each replica node (member) of the cluster system.

1. Enter 1 to continue importing the database backup.

```
Setup has detected that database migration needs to be performed.
The migration process involves backing up the existing database and then
performing various operations to migrate the database to the current
version.
Depending on size of the existing database and the operations to be
performed,
this process may take up to an hour to complete, however you can cancel and
rollback the process at any time by pressing the <a> key followed by
<enter>.
Note that database migration MUST be performed before setup can continue.
[X] 1 - Proceed with database migration [Default]
[ ] 2 - Cancel and exit setup
Please select an option [1] 1
```

2. Enter Yes to continue.

```
[X] 1 - Proceed with database migration [Default]
[ ] 2 - Cancel and exit setup
Do you want to continue Yes/No? Yes
```

3. Enter 1 to continue.

```
Your existing setup is configured for a clustered environment. For your
existing environment, setup must be run on cluster node 1.1.1.1 prior
to running setup on any other cluster node (including this one). When setup
is run on cluster node 1.1.1.1, a migrated master database archive
file will be produced.
If you have already run setup on 1.1.1.1 and either allowed setup to
automatically copy the database archive file to this node, or have copied
this
file manually, please select option [1] below. Otherwise, please select
option [2] below to cancel setup. Then run setup on 1.1.1.1 before
running setup again on this node.
[X] 1 - Specify location of migrated master database archive file
[Default]
[ ] 2 - Cancel and exit setup
Please select an option [1] 1
```

4. Enter Yes to continue.

```
[X] 1 - Proceed with database migration [Default]
[ ] 2 - Cancel and exit setup
Do you want to continue Yes/No? Yes
```

5. Enter the full path to the database backup and enter yes to continue the import process.

```
Enter migrated master database archive file path:
[      ] /home/myuser/ColdBackup_2012_02_13_112911_db.tar.gz
[/home/myuser/ColdBackup_2012_02_13_112911_db.tar.gz]
backing up existing database....done
restoring the migrated master database...done
Restore migrated master database archive succeeded
Press <enter> to continue with setup
```

6. Press Enter to continue the Typical Installation and later the Custom Installation of Oracle Communications Session Delivery Manager (depending on your installation requirements of Oracle Communications Session Delivery Manager). These installation(s) must be completed to use the current Oracle Communications Session Delivery Manager software version on this replica node system.
7. Repeat the previous steps if you need to transfer application data on another replica node (member) of the cluster system.

Select the Product Installation

The following describes the available installation modes after you start the installation:

- ALL—Installs both Oracle Communications Application Orchestrator (standalone only) and Oracle Communications Session Delivery Manager products.
- OCSDM mode—Installs only the Oracle Communications Session Delivery Manager (including Oracle Communications Session Element Manager) product.
- OCAO mode—Installs Oracle Communications Application Orchestrator product only (standalone).

1. Select the installation mode.

```
Select a product:
[X] 1 - ALL                OCAO+OCSDM   [Default]
[ ] 2 - OCSDM mode        Session Delivery Manager
[ ] 3 - OCAO mode         Application Orchestrator

Please select an option [1]
```



Note: After this point, the installation procedure for each mode is identical.

2. You can run setup repeatedly to change existing configuration values, but this option is only available the first time setup runs.

Select the Typical Installation

Select option 1, **Typical**. Press Enter to continue.

```
[X] 1 - Typical
[ ] 2 - Custom
[ ] 3 - Quit
```

Configure User Account Passwords

You need to configure passwords for the admin and Lladmin user groups before starting the Oracle Communications Session Delivery Manager application. Identical credentials must be configured during installation on all nodes of a clustered deployment.

1. Select option 1, **Enter Passwords for default user accounts that will be created**. Press Enter to continue.

```
[X] 1 - Enter Passwords for default user accounts that will be created
[Default]
[ ] 2 - OC SDM global identifier configuration
```


Typical Installation

```
[ ] 3 - HTTP/HTTPS configuration
[ ] 4 - Fault Management configuration
[ ] 5 - Quit setup
```

2. Enter the admin password and confirm by re-entering it.
3. Enter the Lladmin password and confirm by re-entering it.

Specify the Global ID for Northbound Trap Receivers

The OC SDM **global identifier configuration** installation option must be configured on an Oracle Communications Session Delivery Manager server to create a unique global identifier (ID). When a device that is managed by Oracle Communications Session Delivery Manager forwards SNMP trap fault notifications, the global ID that you configure is used in this notification. When an administrator receives the SNMP trap fault notification on their northbound system, the originating device can be determined by viewing the global ID contained in the SNMP trap fault notification.

 **Note:** The global identifier must be the same for all nodes in a clustered system.

1. Select option 2, **OC SDM global identifier configuration**. Press Enter to continue.


```
[ ] 1 - Enter Passwords for default user accounts that will be created
[Default]
[X] 2 - Global identifier configuration
[ ] 3 - Web Server configuration
[ ] 4 - Fault Management configuration
[ ] 5 - Quit setup
```

2. Enter a global unique identifier for the system and press Enter. For example:

```
Enter global identifier: [ ] OCSDM
```

Configure Web Server Security

This task is used to configure the server to run in either HTTPS or HTTP mode, configure web server parameters, and optionally configure the size of files being uploaded to the web server for the secure functioning of the web server and Oracle Communications Session Delivery Manager.

 **Note:** You cannot use the value `root` for either the Apache user or Apache group name.

1. Select option 3, **Web Server configuration**. Press the Enter key to continue.

```
[ ] 1 - Enter Passwords for default user accounts that will be created
[Default]
[ ] 2 - Global identifier configuration
[X] 3 - Web Server configuration
[ ] 4 - Fault Management configuration
[ ] 5 - Quit setup
```

2. Option 1 (**HTTP/HTTPS configuration**) is selected by default to configure the your web server parameters. Press Enter to continue.

```
[X] 1 - HTTP/HTTPS configuration - Setup HTTP or HTTPS configuration
[Default]
[ ] 2 - Security configuration - Options below can be used to modify the
Web server security configurations of OCSDM
```

- a) We highly recommend that you keep HTTPS (default) as the system running mode for your system to create secure connections over the network. If you need HTTP (unsecured) select option 2. Press Enter to continue.


```
[X] 1 - HTTPS mode [Default]
[ ] 2 - HTTP mode
```

- b) Accept the default nncentral user as the Apache user.

```
Apache User [nncentral]
```

- c) Accept the default nncentral group as the Apache group.

```
Apache Group [nncentral]
```


- d) Enter an Apache port number or accept the default port of 8443 (secure HTTPS).

 **Note:** Port 8080 is the port number for unsecured HTTP.

```
Apache Port Number (1024-65535) [8443]
```

- e) Enter the DNS name of the server.

```
Server name [ ] myserver1
```

 **Note:** The specified DNS server name must match the common name (CN) of the certificate.

- f) (For HTTPS configuration only) If your certificate is signed by a certificate authority, select option 2, **No**, when prompted about creating a self-signed certificate. Press Enter to continue. If your certificate is not signed, continue to sub-step g.

1. Enter the absolute path to the private key file.

```
Private key file [ ]
```

2. Enter the absolute path to the certificate file.

```
Certificate file [ ]
```

3. If there are intermediate certificates, select option 1. Press Enter to continue. Then enter the absolute path to the certificate chain file. Otherwise, select the default option 2.

```
Are there intermediate certificates?
```

```
[ ] 1 - Yes
```

```
[X] 2 - No [Default]
```

- g) If you want to create a self signed certificate, select option 1, **Yes**. Press Enter to continue.

- h) Accent nncentral as the certificate alias name.

```
Certificate alias name [nncentral]
```

- i) Enter the truststore password.

```
Truststore password [ ]
```

The upper-level the security configuration is complete and the main web server menu returns. If you do not need to adjust the default maximum file size for files that are uploaded to the web server, your web server configuration is complete.

3. (Optional) Select option 2, **Security configuration** to update the Apache HTTP Daemon (HTTPD) server configuration files, if you need to change the default value set by Oracle Communications Session Delivery Manager for files that can be uploaded to the web server. Press the Enter key to continue.

```
[X] 1 - HTTP/HTTPS configuration - Setup HTTP or HTTPS configuration
[Default]
[ ] 2 - Security configuration - Options below can be used to modify the
Web server security configurations of OCSDM
```

- a) Press Enter to continue.

```
[X] 1 - Modify web server file directive size limit [Default]
```

```
[ ] 2 - Cancel out and do not apply changes
```

- b) Press Enter to continue.

```
[X] 1 - Modify web server file directive size limit [Default]
```

```
[ ] 2 - Cancel out and do not apply changes
```

Typical Installation

- c) You are next prompted to enter the upload file size limit in gigabytes (GB).

```
Web server File Size Limit in GB (2-100) [2]
```

If the entered value exceeds the file-size limit, an error message displays and prompts you to re-enter the value.

Configure Fault Management


1. Select option 4, **Fault Management configuration**. Press Enter to continue.

```
[ ] 1 - Enter Passwords for default user accounts that will be created
[Default]
[ ] 2 - OC SDM global identifier configuration
[ ] 3 - HTTP/HTTPS configuration
[X] 4 - Fault Management configuration
[ ] 5 - Quit setup
```

2. Select option 1, **Configure SNMP trap settings**. Press Enter to continue.


```
[X] 1 - Configure SNMP trap settings [Default]
[ ] 2 - Quit out of fault management configuration
```

3. Either enter the port number that your server will listen on for SNMP traps or press Enter to accept the default port of 162.

 **Note:** You cannot use a port number reserved for Oracle Communications Session Delivery Manager components.

```
Enter the port number that Trap Relay should listen on: (1-65535) [162]
```

4. If prompted (you entered a port below 1024), enter the sudo password. Then re-enter the sudo password to confirm.

 **Note:** The sudo password is the NNCentral password to provide root permissions for setting SNMP trap settings.

5. Select option 5, **Quit setup**. Press Enter to continue.

Next Step

Start the Oracle Communications Session Delivery Manager server.

Start the Oracle Communications Session Delivery Manager Server

1. Log in to the server as the nncentral user.
2. Change to the bin directory.

For example:

```
cd /opt/AcmePacket/NNC7x/bin
```

3. Execute the startnnc.sh script.

```
./startnnc.sh
```

The console displays the number of services started. After all services have started, the system is ready for use. Do not attempt to log in until the console has indicated that the web servers are up.

Next Steps

- Check Oracle Communications Session Delivery Manager server processes.
- Begin using Oracle Communications Session Delivery Manager. Use your web browser to navigate to the server login page by entering the host name or IP address, and port number in the web browser navigation bar. For example:

```
http://example.com:8080
```

In the login page, enter the administrator login name and password that you configured in the *Configure User Account Passwords* section.

Check Server Processes

After the `startnnc.sh` script has completed, you can verify that Oracle Communications Session Delivery Manager is up and running by entering the report process status command on the system. Depending on your hardware specifications it may take a few minutes for Oracle Communications Session Delivery Manager to start.

1. Execute the report process status command on the server.

```
ps -eaf | grep Acme
```


When Oracle Communications Session Delivery Manager is successfully running, you should see:

- Several `httpd` processes
 - Three or more Java processes
2. If the above processes are running and you still cannot connect to your server, check the firewall settings of your server and network. See *Firewall Settings* in chapter 1.

Custom Installation

The custom installation options are for more advanced users. The following custom options are displayed :

- Mail server configuration
- OC SDM cluster management
- Route Manager configuration
- SAML Single Sign-On configuration (This feature is not enabled in this release.)
- SBI TLS configuration
- Oracle Database configuration

 **Note:** The first four steps of the custom installation are identical to the steps of the typical installation.

Start the Installation

1. Log in as root user.
2. Navigate to the bin directory.

For example:

```
cd /opt/AcmePacket/NNC75/bin
```

3. Run setup.sh.

```
./setup.sh
```



Warning: This process may take several minutes to complete. Interrupting the setup.sh process risks corrupting the system.



Note: A warning message appears if you have less than the recommended minimum physical memory. Proceeding without the recommended minimum physical memory may result in performance degradation.



Note: Install missing packages with the command `yum install -y <package name>`. Then run setup.sh again.

Upgrade Considerations

If you are upgrading from a previous version of Oracle Communications Session Delivery Manager, the migration tool detects any previous versions and prompts you depending on whether the existing installation is on a standalone or clustered system.

Custom Installation

You can complete the Oracle Communications Session Delivery Manager installation in standalone or cluster mode.

If you try to migrate data without running setup first, the following message appears.

```
Starting Migration Application 2011-05-25 14:11:27,086
Please run OCSDM setup first. 2011-05-25 14:11:52,377
```


The following sections provide more information about transferring existing Oracle Communications Session Delivery Manager application data to the new version of Oracle Communications Session Delivery Manager. If you are installing Oracle Communications Session Delivery Manager for the first time, proceed to the *Select how Session Delivery Manager is Installed* section.

Select the Custom Installation

Select option 2, **Custom**. Press Enter to continue.

```
[ ] 1 - Typical
[X] 2 - Custom
[ ] 3 - Quit
```

Configure the Mail Server

 **Note:** If you want Session Delivery Manager products to send out emails, you can setup the mail server credentials to enable the sending of emails to a targeted Microsoft Exchange and Gmail server.

1. Select option 5, **Mail Server configuration**. Press Enter to continue.

```
[X] 5 - Mail Server configuration
```

2. Select option 1, **Configure mail server**. Press Enter to continue.

```
[X] 1 - Configure mail server [Default]
```

3. Select option 1, **Configure mail server host**. Press Enter to continue.

```
[X] 1 - Configure mail server host
```

4. Enter the DNS name of your mail server.

```
Provide the DNS name.
Host name [ ] mail.example.com
```

5. Select option 1, **Mail server secure protocol**. Press Enter to continue.

```
[X] 1 - Mail server secure protocol
```

6. Select your mail server's secure protocol.

Valid secure protocols are:

- starttls
- ssl

 **Note:** Customers may select none, but Oracle recommends all customers select starttls or ssl.

7. Select option 1, **Mail server port**. Press Enter to continue.

```
[X] 1 - Mail server port
```

8. Choose a port number or press Enter to select the default port 465.

9. Select option 1, **Configure mail from**. Press Enter to continue.

```
[X] 1 - Configure mail from
```

10. Enter the address you want used for the From address.

For example, if sending to Microsoft Exchange account, mailadmin@acmepacket.com. If sending to a Gmail account, mailadmin@gmail.com.

```
Provide the mail from.
Mail from [ ] mailadmin@example.com
```

11. Select option 1, **Configure mail user**. Press Enter to continue.

12. Enter the mail user id.

```
Provide the mail user id.
Mail user [ ] user@example.com
```

13. Select option 1, **Configure mail logon required**. Press Enter to continue.

14. Select either true or false.

```
Mail logon required true/false [false]
```

a) If you set the mail logon required to true, select option 1, **Configure mail logon user password**. Press Enter to continue.

```
[X] 1 - Configure mail logon user password
```

b) Enter the mail logon user password.

```
Mail logon user password [ ]
```

15. Select option 1, **Extra mail properties**. Press Enter to continue.

```
[X] 1 - Extra mail server properties [Default]
```

16. Enter the extra mail server properties you want to configure.

The format for entering multiple mail server properties is:


```
property1:value1;property2:value2;property3:value3
```

17. Select option 2, **Apply new mail server configuration**. Press Enter to continue.

18. Select option 2, **Quit out of mail server configuration**. Press Enter to continue.

Configure Clusters

When setting up the Oracle Communications Session Delivery Manager cluster, add all other nodes each time you run setup.sh. For example, say you are setting up a cluster with nodes A, B, and C. When running setup.sh on node A, add nodes B and C; when running setup.sh on node B, add nodes A and C; and when running setup.sh on node C, add nodes A and B.

 **Note:** When configuring or modifying a cluster, all cluster members must be shut down.

1. Select option 6, **OC DSM cluster management**. Press Enter to continue.

2. Select option 1, **Configure and manage members in cluster**. Press Enter to continue.

Add New Members to a Cluster

1. Select option 1, **Add a new member**. Press Enter to continue.

2. Enter the IP address of the member you are adding to the cluster.

```
Member host name [ ]
```

3. Repeat steps to add additional hosts to the cluster.

4. When done adding hosts, select option 3, **Apply new cluster configuration**. Press Enter to continue.

5. Select option 3, **Quit out of cluster configuration**. Press Enter to continue.

6. If this machine is not part of the cluster, select option 2, **No**. Otherwise, select option 1, **Yes**. Press Enter to continue.

7. If you selected **Yes**, enter the user name and password which other members of the cluster can use to SFTP files from this machine.

Managing Cluster Members

If one or more members need to be removed from a cluster, all members need to be removed from this cluster if the cluster is being retained. Members that need to stay in this cluster must be added again to the cluster.

1. After entering the **Configure and manage members in the cluster** menu, select option 2, **Remove all remote clusters**. Press Enter to continue.
2. Select option 1, **Proceed with removing all remote members**. Press Enter to continue.
3. Select option 3, **Apply new cluster configuration**. Press Enter to continue.
Applying the changes immediately removes all members of the cluster.
4. Select option 1, **Add a new member**. Press Enter to continue.
5. Enter the IP address of the member you are adding to the cluster.

```
Member host name [ ]
```
6. Repeat steps four and five to add additional hosts to the cluster.
7. When done adding hosts, select option 3, **Apply new cluster configuration**. Press Enter to continue.
8. Select option 3, **Quit out of cluster configuration**. Press Enter to continue.
9. If this machine is not part of the cluster, select option 2, **No**. Otherwise, select option 1, **Yes**. Press Enter to continue.
10. If you selected **Yes**, enter the user name and password which other members of the cluster can use to SFTP files from this machine.

Delete a Cluster

All members of a cluster must be removed from a cluster in order to delete the cluster.

1. After entering the **Configure and manage members in the cluster** menu, select option 2, **Remove all remote clusters**. Press Enter to continue.
2. Select option 1, **Proceed with removing all remote members**. Press Enter to continue.
3. Select option 3, **Apply new cluster configuration**. Press Enter to continue.
Applying the changes immediately removes all members of the cluster.
4. Select option 2, **Remove all remote clusters**. Press Enter to continue.
5. Select option 3, **Apply new cluster configuration**. Press Enter to continue.
Applying the changes immediately removes the cluster.

Configure a Clustered Server to be a Standalone Server

You can configure a clustered server to be a standalone server by removing its cluster configuration.

1. From the cluster management menu, select option 2, **Run current host as a standalone**. Press Enter to continue.
2. Select option 1, **Configure application server to a standalone server**. Press Enter to continue.
3. Select option 3, **Quit out of cluster configuration**.
4. Select option 2, **No**.

Configure Route Management Central

1. Select option 7, **Route Manager Central configuration**. Press Enter to continue.
2. Set the maximum number of route set backups.

```
Please enter the maximum number of route set backups per route set/backup  
type combination  
# of backups (1-500) [10]
```

Configure Southbound Interface Transport Layer Security

The southbound interface (SBI) transport layer security (TLS) feature is provided for session delivery network functions (NFs) like multiservice security gateway (MSG) that supports Acme Control Protocol (ACP) over TLS. An SBI is the lower-level interface layer of a component that is directly connected to the northbound interface (NBI) of this lower layer. Refer to the specifications of your NF to determine if this NF supports the SBI TLS feature.

1. Select option 9, **SBI TLS configuration**. Press Enter to continue.
2. Select option 1, **Keystore Selection**. Press Enter to continue.
3. Select a keystore to explore. Press Enter to continue.

Valid options are:

- ACP TLS Keystore
- Elasticity Manager Keystore
- Report Manager Keystore

4. Select the certificate to create, view, or modify.

Valid options are:

- Entity Certificate
- Trusted Certificate

Configure Entity Certificates

1. Select option 1, **Entity Certificate**. Press Enter to continue.
2. Select option 1, **Create Entity Certificate**. Press Enter to continue.
3. Enter the certificate details.

- Common name
- Organization unit
- Organization
- City or locality
- State or province
- Country code
- Key size
- The number of days during which this certificate is valid

After creating an Entity Certificate, new options appear.

4. Select the action you wish to perform.
 - View Entity Certificates
 - Export Entity Certificate
 - Generate Certificate Signing Request (CSR)
 - Import Signed Entity Certificate
 - Delete Entity Certificates
 - Return to Main Menu
5. If you select the option to export the certificate, import a certificate, or generate a CSR, provide the absolute path to the file.
6. When finished configuring the entity certificate, select option 6, **Quit and back to Main Menu**. Press Enter to continue.

Configure Trusted Certificates

1. Select option 2, **Trusted Certificate**. Press Enter to continue.

Custom Installation

2. Select option 1, **Import Trusted Certificate**. Press Enter to continue.

3. Enter the alias name for the certificate.

4. Enter the full path to the certificate

For example:

```
Enter full path of the certificate to be imported: [ ] /etc/ssl/certs/  
server.crt
```

5. Select the action you wish to perform.

- Import Trusted Certificate
- List all Certificates
- View Certificate detail
- Delete Trusted Certificate
- Return to Main Menu

6. If you select the option to view or delete a certificate, provide the alias of the certificate.

7. When finished configuring trusted certificates, selection option 5, **Quit and back to Main Menu**. Press Enter to continue.

About Creating a Report Manager Database Instance on the External Oracle Database

If you are using Oracle Communications Report Manager with Oracle Communications Session Delivery Manager, option 10 (Oracle DB OCSDMDW configuration) in the Custom Installation is used to specify the Oracle home path (ORACLE_HOME) and the credentials of the Oracle database user instance (OCSREMDW).

For more information about creating the OCSDMDW database instance, see the *Create a Report Manager Database Instance* chapter in the *Oracle Communication Report Manager Installation Guide*.

Exit the Custom Installation

Select option 11, **Quit setup**. Press Enter to continue.

Start the Oracle Communications Session Delivery Manager Server

1. Log in to the server as the nncentral user.

2. Change to the bin directory.

For example:

```
cd /opt/AcmePacket/NNC7x/bin
```

3. Execute the startnnc.sh script.

```
./startnnc.sh
```

The console displays the number of services started. After all services have started, the system is ready for use. Do not attempt to log in until the console has indicated that the web servers are up.

Next Steps

- Check Oracle Communications Session Delivery Manager server processes.
- Begin using Oracle Communications Session Delivery Manager. Use your web browser to navigate to the server login page by entering the host name or IP address, and port number in the web browser navigation bar. For example:

```
http://example.com:8080
```

In the login page, enter the administrator login name and password that you configured in the *Configure User Account Passwords* section.

Check Server Processes

After the `startnnc.sh` script has completed, you can verify that Oracle Communications Session Delivery Manager is up and running by entering the report process status command on the system. Depending on your hardware specifications it may take a few minutes for Oracle Communications Session Delivery Manager to start.

1. Execute the report process status command on the server.

```
ps -eaf | grep Acme
```

When Oracle Communications Session Delivery Manager is successfully running, you should see:

- Several `httpd` processes
 - Three or more Java processes
2. If the above processes are running and you still cannot connect to your server, check the firewall settings of your server and network. See *Firewall Settings* in chapter 1.

Install Software Patches

Software patches can be installed to the release version of Oracle Communications Session Delivery Manager.

Oracle Communications Session Delivery Manager comes with the patch management tool that allows you to perform the following operations:

- List imported patches.
- Import patches.
- Apply a patch.

You must download the Oracle Communications Session Delivery Manager patch software (<filename>.tar.gz) to a directory on your system. Note the directory path. It is needed later when the patch management tool prompts you for the patch software file location. When directed, the patch management tool unzips and extracts the necessary files, and places them in the original Oracle Communications Session Delivery Manager installation directory, appending the directory where the patch files are located. Patches are cumulative. For example, patch 5 contains all the previous patches (that is, patches 1-4).

Once you have successfully applied a new patch with the patch management tool and the Oracle Communications Session Delivery Manager is running in your browser, select **Help** > **About** to verify the new Oracle Communications Session Delivery Manager patch software version.

Shut Down Your System

You can shut down the existing Oracle Communications Session Delivery Manager software version running on your system to install a new version of the software, restore a database or apply a software patch.

Shut Down the System

You can shut down the existing Oracle Communications Session Delivery Manager software version running on your system to install a new version of the software, restore a database or apply a software patch.


1. Log in as the nncentral user.
2. Change directory to the bin directory.

For example:

```
cd /opt/AcmePacket/NNC75/bin
```

Install Software Patches

- Execute the **shutdownnnc.sh** script. By default, the shutdownnnc.sh script detects whether the existing installation is a standalone or clustered system and prompts you with the option to shut down the entire cluster if no flag options are provided.

 **Note:** However, You can script an option ahead of time by adding `-local` for single nodes and `-cluster` to shutdown an entire cluster.

```
./shutdownnnc.sh
Shutdown back-end server
Do you wish to shut down the entire cluster (Yes/No)? Yes
```


Shut Down the Cluster System

Shut down the Oracle Communications Session Delivery Manager running on each server cluster (node) system.

- Change to the bin installation directory. For example:

```
cd /opt/AcmePacket/NNC75/bin
```

- Execute the shutdownnnc.sh script. By default, the shutdownnnc.sh script detects whether the existing installation is a standalone or clustered system and prompts you with the option to shut down the entire cluster if no flag options are provided.

 **Note:** However, You can script an option ahead of time by adding `-local` for single nodes and `-cluster` to shutdown an entire cluster.

```
Shutdown back-end server
Do you wish to shut down the entire cluster (Yes/No)? Yes
Shutting down cluster.....
```

- Enter Yes to continue and shut down the cluster.

Install a Session Delivery Manager Patch

Use the patch tool to install an Oracle Communications Session Delivery Manager patch on a standalone system or on each cluster system (node).

- Log in to the Oracle Communications Session Delivery Manager server as root.
- Navigate to the bin directory. For example:

```
cd /opt/AcmePacket/NNC75/bin
```

- Run the patchManagement.sh script.

```
./patchManagement.sh
```

A Welcome message appears and initialization processes occur. The patch management tool checks to ensure that minimal system requirements are met and the system is running.

```
cd /opt/AcmePacket/NNC75/bin
[root@nncentral bin]# ./patchManagement.sh
=====
Welcome to Oracle Communications Session Delivery Manager Patch Management
application
Current Oracle Communications Session Delivery Manager Version: NNC75P1
OS : Linux : amd64 : 2.6.18-194.el5
=====
Please wait while application loads
Checking environment for patch management application.
Please wait ....
100%[=====]
Patch Management Menu
Please select from the following options:
[X] 1 - List Imported patches
[ ] 2 - Import patch
```

```
[ ] 3 - Apply patch
[ ] 4 - Remove all applied patches
[ ] 5 - Quit
Please select an option [1]
```

- If you want to see what patches are installed on your Oracle Communications Session Delivery Manager system, select option 1 in the prompt. The patch management tool checks the system for available patches. If the current-running software version is a patch, that version has an asterisk [*] next to it.

```
=====
LIST_IMPORTED_PATCH
This option will list all imported patches
(*) Current Patch Level
NNC75P1*
=====
```

- Enter 2 to import the new patch. When prompted, enter the patch file name and its full directory path and press Enter. For example:

```
/opt/NNC75P1Linux64bit.tar.gz
```

The patch management tool performs the following actions sequentially:

- Checks that the import directory and patch file specified by the user exists.
- Checks that the parent destination directory exists. If not, the parent directory, /patches, is created.
- Checks whether a patch directory with the same name already exists. If so, the tool displays a message indicating that this patch has already been imported. The tool backs out from this option, and the user can select another option.
- Extracts the patch version information from the tar.gz file.
- Checks that the patch version matches the current Oracle Communications Session Delivery Manager GA version. If a mismatch is detected, an error message is displayed indicating that the patch version is not applicable to the current GA version. The extracted file is removed and the import process is halted.
- If the version check is successful, the tool extracts the remaining contents of the patch.
- Checks each file's MD5 hash to ensure the files are valid. If a discrepancy is detected during this process, the patch is considered corrupted and is removed from the patches directory. An error message is displayed.

Below is the output for a successful patch import:

```
=====
IMPORT_PATCH
This option will import a user specified patch
Please specify the patch file to import with full path
Patch file name [      ] /opt/NNC75P2Linux64bit.tar.gz
Patch file name [/opt/NNC75P2Linux64bit.tar.gz]
100%[=====]
```

- Enter 3 to apply the new patch. The patch tool displays a list of available patches on the system and prompts you to select a patch.
- Enter the patch option.
The system prompts you to confirm your selection.
- Enter Yes.
The patch management tool performs the following actions sequentially:
 - If the selected patch version is the same as the current-running patch version, the tool stops. The tool will prompt you to select one of two options: go back to the main menu, or select another patch to apply.
 - If the current-running software version is a patch, the system is rolled back to the GA software version first, and then proceed to the next step. If the current-running version is not a patch, it proceeds to the last step.

Install Software Patches

- Backs up the GA software version and files that the target patch replaces.
- Applies the targeted patch.

A success message is displayed once a patch is successfully applied.

```
(*) Current Patch Level
[ ] 1. NNC75P1 (*)
[ ] 2. NNC75P2
[ ] 3. NNC75P5
[X] 4. Quit
Please select an option [4] 2
[ ] 1. NNC75P1 (*)
[X] 2. NNC75P2
[ ] 3. NNC75P5
[ ] 4. Quit
Do you want to continue Yes/No?
Patch applied successfully!
```

9. Enter 5 to quit the patch management tool.

10. Navigate to the bin directory.

For example:

```
cd /opt/AcmePacket/NNC7x/bin
```

11. Run setup.sh.

```
./setup.sh
```



Warning: This process may take several minutes to complete. Interrupting the setup.sh process risks corrupting the system.


12. (Optional) If you are updating a cluster, apply the patch to each Oracle Communications Session Delivery Manager host in the cluster.

Check Your Setup Configuration After a Patch Installation

When you apply a new patch to Oracle Communications Session Delivery Manager, it is possible that some setup options that you previously specified are modified by the patch installation. If any setup files are affected, the setup process attempts to reapply the last setup configurations by doing the following verifications:

- Pre-condition—Checks for any version changes during the current session. If the version changes, checks are performed to discover if the current version modified any of the setup configuration files.
- User-required Inputs—Prompts you to enter any information for external dependencies, such as the license file location.
- Post-process—Reapplies the original setup configuration (if required). The screen output for this process is shown below:

When you are prompted to do the auto-setup, enter Yes.

 **Note:** If you select No and do not run the auto-setup, you receive a warning message and the setup may not run properly.

```
Auto Setup pre-checking starts...
Current installed version: NNC75P1 Initial installed version: NNC75
Detect setup configuration file change!
Done pre-checking for Auto Setup
Auto Setup is needed
Do you want to continue Yes/No?
=====
Welcome to Auto Setup Application
Version : NNC75
OS : Linux : amd64 : 2.6.18-194.26.1.el5
=====
```



```
Please wait while application loads
WARNING!!!! This process will automatically apply the previous setup
Do you want to continue Yes/No?
Checking environment and setting permissions.
Please wait ....
100%[=====]
=====
System Physical Memory Diagnostics
Total System Physical Memory = 24098 MB
Total System Free Physical Memory = 1637 MB
=====
System Disk Space Diagnostics
Total System Disk Space = 144 GB
Free System Disk Space = 93 GB
WARNING: Disk space is insufficient for running this application.
The recommended total disk space that should be available is = 300 GB
=====
System Port Availability Diagnostics : Oracle Communications Session Delivery
Manager Required Ports
The following port is available [ 5000 ]
The following port is available [ 8080 ]
The following port is available [ 61616 ]
The following port is available [ 9000 ]
The following port is available [ 8443 ]
The following port is available [ 1099 ]
The following port is available [ 8009 ]
The following port is available [ 1098 ]
The following port is available [ 8005 ]
=====
Auto setup completed for CHECK_APPLY_LICENSE
=====
HTTP/HTTPS configuration
No previous setup information found for HTTP
Auto setup completed for HTTPS
=====
Fault Management configuration
Auto setup completed for TRANSITION_HIDE
=====
Oracle Communications Session Delivery Manager cluster management.
No previous setup information found for CLUSTER_MEMBERSHIP
No previous setup information found for ROUTE_MGMT_SFTP
=====
Route Manager Central configuration
No previous setup information found for ROUTE_MGMT
=====
SAML Single sign on configuration
SANE does not support AutoSetup! Manual setup is required for this
configuration
=====
Mail Server configuration
No previous setup information found for CONFIG_MAIL_SERVER
Exit Auto Setup Application
```

