Oracle® Communications Application Orchestrator

Installation Guide
Release 1.1

January 2017

ORACLE

Notices

Contents

About This Guide

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

Related Documentation

Table 1: Oracle Communications Application Orchestrator Library

Document Name	Document Description
Release Notes	Contains feature support information, and known issues pertaining to this release.
Installation Guide	Contains instructions for installing Oracle Communications Application Orchestrator as a standalone application or installing Oracle Communications Application Orchestrator together with Oracle Communications Session Delivery Manager.
Plug-in Guide for Session Delivery Network Elements	Describes how to use Oracle session delivery product plug-ins with Oracle Communications Application Orchestrator.
User Guide	Describes how to centrally manage and automate your virtual and physical network environment of composite network functions (CNFs). The Oracle Communications Application Orchestrator application is implemented by doing the following: • Use the Security Manager to create new users and new user groups, and set group-based authorization. • Configure X.509 certificate authentication. • Add a virtual infrastructure management (VIM) system to manage VNF life-cycles. • Register an Element Manager (EM) with Oracle Communications Application Orchestrator in order to stage a CNF from its CNF descriptor (CNFD). • Manually use the CNF onboarding workflow to choose, stage, and promote a pre-existing CNF plug-in, and configure the CNF to deploy and make this CNF operational. • Automate the manual process of making a CNF operational by using the hierarchical service configuration (HSC) feature. • Monitor Oracle Communications Application Orchestrator real-time KPI thresholds, device status and performance information for CNFs. • Use the Fault Manager to view events, alarms and trap event settings.
REST API Guide	The Oracle Communications Application Orchestrator REST API interface interacts with the Northbound Interface (NBI) to get the available fault alarms.
Security Guide	Provides the following security guidelines and topics: • Guidelines for performing a secure installation of Oracle Communications Application Orchestrator 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.

Document Name	Document Description
	• Security maintenance, which includes a checklist to securely deploy Oracle Communications Application Orchestrator on your network, maintaining security updates, and security considerations for developers.

Revision History

Date	Description
August 2015	• Initial release
January 2016	• 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	• Changed the Set the Global Identifier section so that it provides more information for why the global identifier is set.

April 2016	• Added a step to the *Transfer Application Data on a Standalone* section that prompts the user to continue and complete the installation in order to use the current product version on their system.
	• The *Configure HTTP or HTTPs* section was changed to *Configure Web Server Security*. The following Web server security features were added:
	  • HTTPS is now the default installation option for your Web server.
	  • You can now specify maximum upload file size limitations.

July 2016	• A note was added to the *Configure Web Server Security* section in the *Typical Installation* chapter that says the specified DNS server name must match the common name (CN) of the certificate.
January 2017	• The *Check System Requirements* section in the *Pre-installation Tasks* chapter was updated to indicate that the server on which Oracle Communications Application Orchestrator is installed requires a 300 GB hard drive. • The syntax for specifying the NNCentral user privileges in the sudoer configuration (step 4) in the *Specify NNCentral User Privileges* section of the *Pre-installation Tasks* chapter was fixed. • The *Set the Global Identifier* section was renamed *Specify the Global ID for Northbound Trap Receivers* and the introductory paragraph was updated for clarity.

1

Pre-Installation Tasks

Read and understand the summary of pre-installation tasks that need to be done before installing Oracle Communications Application Orchestrator. 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. Check to ensure your system meets the minimum requirements.
2. Shut down your Oracle Communications Application Orchestrator server(s).
3. Upgrade the version of Linux on your server(s) on which Oracle Communications Application Orchestrator is running, if the version of Linux is not supported with the release of Oracle Communications Application Orchestrator that you are installing.
4. Open the appropriate ports on the network and system firewall.
5. If your system does not rely on DNS, edit the /etc/hosts file to specify a host name for your system.
6. Disable the default httpd daemon.
7. Specify your system locale to the US English language UTF-8 character encoding method (LANG=en_US.UTF-8).
8. If any required redhat Package Manager (RPM) software libraries that are shared with Oracle Communications Application Orchestrator are missing, you must install them using the yum program.

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

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

Undeploy and Delete CNFs

If you are upgrading from Oracle Communications Application Orchestrator, Release 1.1 to a newer version, you must undeploy all CNFs that were operationalized manually and then delete them.

Note: Manual mode must be enabled in Oracle Communications Application Orchestrator to deploy or undeploy DUs.

1. Expand the **Application Orchestrator** slider and select **Deployed** > **CNF**.
2. In the deployed **Composite Network Functions** table, select the CNF and click **Expand** to go to the **CNF details** table.
3. Click the CNF folder and select **Manage** drop-down list and select **Undeploy** to begin the CNF undeployment process.
4. Repeat the steps above for any other operational CNFs that you want to undeploy.
5. In the **Composite Network Functions**, select the undeployed CNF and click **Delete**.
6. In the **Delete** confirmation dialog box, click **Yes**.
7. Repeat the steps above for any other undeployed CNFs that you want to delete.

Check System Requirements

Oracle has certified the following hardware and software server platforms as well as client requirements for use with Oracle Communications Application Orchestrator.

Note: Other hardware configurations might work with Oracle Communications Application Orchestrator, but Oracle has verified the configurations listed here.

Oracle Communications Application Orchestrator Server Requirements

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

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

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 Application Orchestrator 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 Application Orchestrator 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.

```
./shutdownnnc.sh
```

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 Application Orchestrator.

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 Application Orchestrator.

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 Application Orchestrator 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 Application Orchestrator server is shut down) to a local server or remote server directory path, enter the **backupdbcold.sh** script. For example:

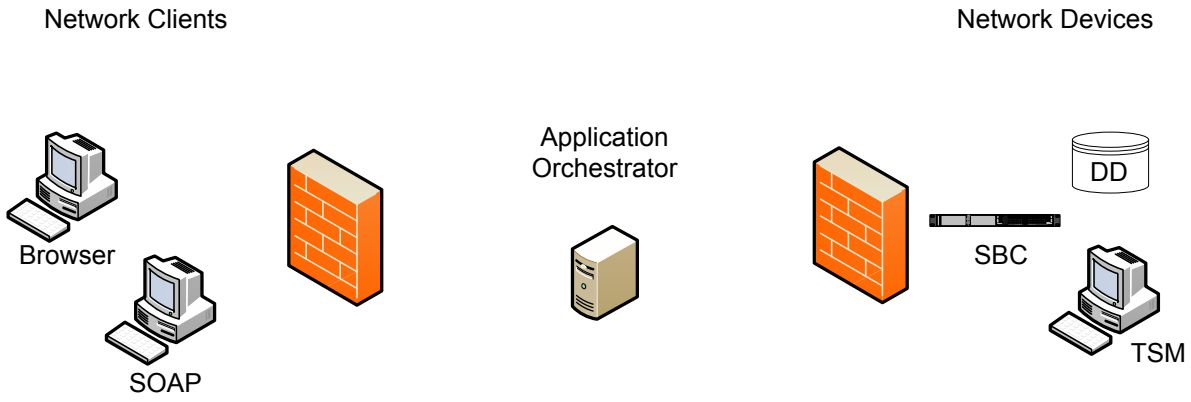
   ```
   backupdbcold.sh /<path>/ColdBackup_yyyy_mm_dd_<title>.tar.gz
   ```

   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.

Check Firewall Settings

When setting up Oracle Communications Application Orchestrator in your network, you may have a firewall between the clients (browsers, SOAP, etc.) and the Oracle Communications Application Orchestrator, and a firewall between the Oracle Communications Application Orchestrator and other devices.



If firewalls exist on either side of the Oracle Communications Application Orchestrator, 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 Application Orchestrator 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 Application Orchestrator 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 Application Orchestrator 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 Application Orchestrator to communicate with 9200 devices via AMI.
5060	TCP		N	Y	Used for Oracle Communications Application Orchestrator Trunk Manager (SIPTX) to communicate with SP-SBC.
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 Application Orchestrator distributed scheduler service.
54327	UDP	Hazelcast	N	Y	Used by Hazelcast for cluster member discovery.

Note: For additional ports that may need to be opened, see the Oracle Communications Application Orchestrator Plug-in Guide for Session Delivery Network Elements.

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 Application Orchestrator server. If installing on a Linux system, the Linux firewall must also have either 8080 (HTTP) or port 8443 (HTTPS) open.

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.
2. Determine your system's host name with the hostname command.
3. 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 Application Orchestrator server is running a default HTTP daemon (HTTPD) process, disable that process from restarting.

1. Log in as the root user.
2. 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...
   ```
3. If the HTTPD is running, stop the HTTPD:

   ```
   service httpd stop
   ```
4. Disable the HTTPD from restarting when the system reboots:

   ```
   chkconfig httpd off
   ```
5. 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 Application Orchestrator to install properly.

1. Log in as the root user.
2. 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 Application Orchestrator. These shared libraries need to be installed on your Linux system in order for Oracle Communications Application Orchestrator to run properly:

Table 2: RPM software library packages shared with Oracle Communications Application Orchestrator

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

Name	Description
	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 Application Orchestrator 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 Application Orchestrator related server operations. You also must specify limited sudo privileges for the nncentral user and nncentral group. After the Oracle Communications Application Orchestrator installation, all the installed files are owned by the nncentral account. The main Oracle Communications Application Orchestrator 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 Application Orchestrator 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 Application Orchestrator 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 sudoer configuration to give the NNCentral user the limited authority to run Oracle Communications Application Orchestrator:

```
nncentral ALL=/opt/AcmePacket/NNC*/jre/bin/java * -
Dlog4j.configurationFile=* -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 Application Orchestrator 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.

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/
```

2

Typical Installation

The Typical installation performs the minimal configuration required to run the Oracle Communications Application Orchestrator 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 Application Orchestrator, 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 Application Orchestrator 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 Application Orchestrator application data to the new version of Oracle Communications Application Orchestrator. If you are installing Oracle Communications Application Orchestrator for the first time, proceed to the *Select how Session Delivery Manager is Installed* section.

Upgrade Oracle Communications Application Orchestrator

If you are upgrading Oracle Communications Application Orchestrator from a previous version, you must transfer the existing application data to the new version.

Transfer Application Data to the New Version

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

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 Application Orchestrator 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 Application Orchestrator 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 Application Orchestrator (depending on your installation requirements of Oracle Communications Application

Orchestrator). These installation(s) must be completed to use the current Oracle Communications Application Orchestrator software version on this standalone 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: Application Orchestrator can only run as a standalone server; clustering is not yet supported.

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 LIadmin user groups before starting the Oracle Communications Application Orchestrator application.

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
[ ]  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 LIadmin 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 Application Orchestrator server to create a unique global identifier (ID). When a device that is managed by Oracle Communications Application Orchestrator 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.

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 - OC SDM global identifier configuration
[ ]  3 - HTTP/HTTPS configuration
[ ]  4 - Fault Management configuration
[ ]  5 - Quit setup
```

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

```
Enter global identifier: [OCAO+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 Application Orchestrator.

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 Application Orchestrator 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
```

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 Application Orchestrator 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 Application Orchestrator server.

Start the Oracle Communications Application Orchestrator 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 Application Orchestrator server processes.
- Begin using Oracle Communications Application Orchestrator. 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 Application Orchestrator 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 Application Orchestrator to start.

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

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

When Oracle Communications Application Orchestrator 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.