

**Oracle® Communications Application  
Orchestrator**  
Security Guide  
Release 1.1

April 2016

## Notices

Copyright© 2016, 2016, 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

<b>About This Guide.....</b>	<b>5</b>
Revision History.....	6
<b>1 Overview.....</b>	<b>7</b>
<b>2 Secure Installation Guidelines.....</b>	<b>9</b>
Secure the Server.....	9
About the Application Orchestrator Installation.....	9
Check Firewall Settings.....	10
System Support for Encryption and Random Number Generators.....	11
Device Security.....	12
Web Server Security.....	12
Secure System Password Guidelines.....	13
<b>3 Security Manager Feature Overview.....</b>	<b>15</b>
Security Manager.....	15
User Groups.....	16
Users.....	16
Operations Tree Structure.....	16
Change Privileges for User Groups.....	16
Set the User Inactivity Timer to Prevent Unauthorized Access.....	16
Audit Logs.....	17
Configure External User Authentication.....	17
<b>4 Security Maintenance.....</b>	<b>19</b>
Security Checklist.....	19
Maintain Security Updates.....	20
Security Considerations for Developers.....	20



---

# 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	<p>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:</p> <ul style="list-style-type: none"><li>• Use the Security Manager to create new users and new user groups, and set group-based authorization.</li><li>• Configure X.509 certificate authentication.</li><li>• Add a virtual infrastructure management (VIM) system to manage VNF life-cycles.</li><li>• Register an Element Manager (EM) with Oracle Communications Application Orchestrator in order to stage a CNF from its CNF descriptor (CNFD).</li><li>• 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.</li><li>• Automate the manual process of making a CNF operational by using the hierarchical service configuration (HSC) feature.</li><li>• Monitor Oracle Communications Application Orchestrator real-time KPI thresholds, device status and performance information for CNFs.</li><li>• Use the Fault Manager to view events, alarms and trap event settings.</li></ul>
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	<p>Provides the following security guidelines and topics:</p> <ul style="list-style-type: none"><li>• 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.</li><li>• An overview of the Security Manager features that are used to configure groups, users, operations, privileges, and manage access to the system.</li></ul>

## About This Guide

Document Name	Document Description
	<ul style="list-style-type: none"><li>• Security maintenance, which includes a checklist to securely deploy Oracle Communications Application Orchestrator on your network, maintaining security updates, and security considerations for developers.</li></ul>

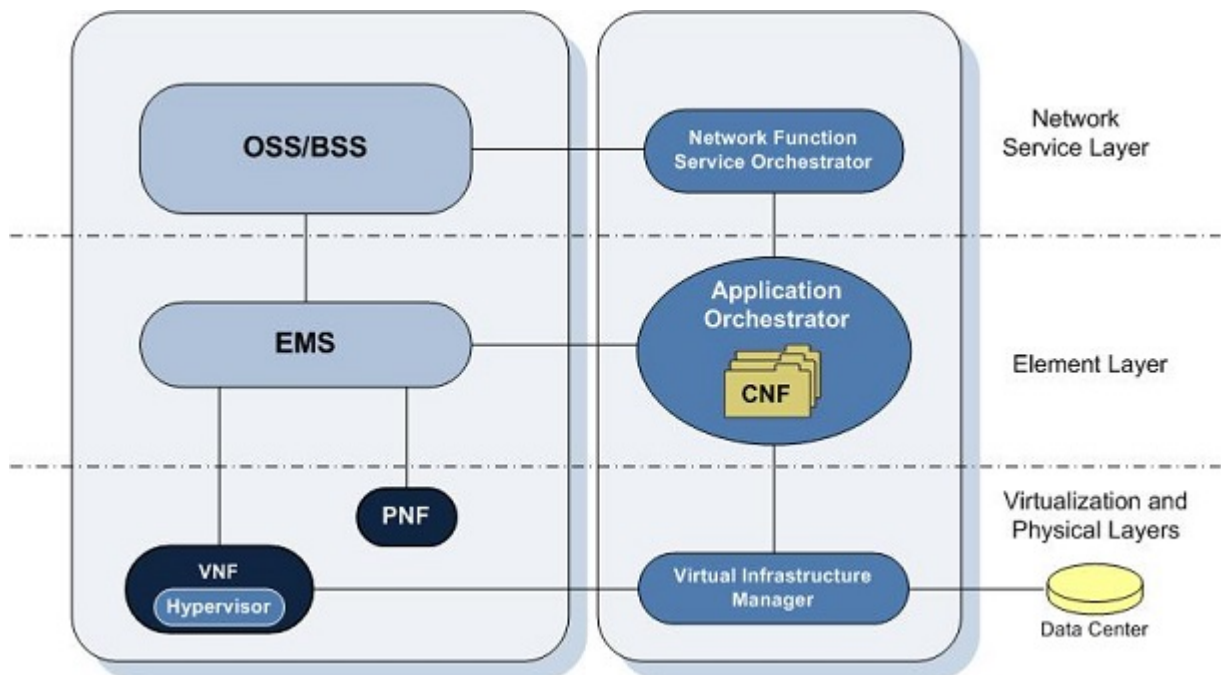
## Revision History

Date	Description
August 2015	<ul style="list-style-type: none"><li>• Initial release</li></ul>
April 2016	<p>The following information was added to the Web Server Security section:</p> <ul style="list-style-type: none"><li>• Maximum upload file size limitations</li><li>• HTTP certificate support</li><li>• HTTPS installation changes when installing your Web server.</li></ul>

## Overview

Oracle Communications Application Orchestrator provides a core management platform for communications service providers (CSPs). This platform supports a composite network function (CNF) that can be any combination of a virtualized network function (VNF) and physical network function (PNF) that runs as part of a network to provide one or more public, private, or hybrid cloud computing solutions.

When Oracle Communications Application Orchestrator starts a CNF, it constructs the CNF topology and deploys the CNF automatically. The following figure shows a simplified diagram for how Oracle Communications Application Orchestrator fits into the infrastructure of a network management environment.



**Figure 1: Oracle Communications Application Orchestrator in the network**

CSPs use Oracle Communications Application Orchestrator to deploy CNFs on their networks for the following reasons:

- Portability—Pre-existing CNFs can be imported or exported to a virtual network platform.

## Overview

---

- **Dynamic**—Cloud resources can be dynamically and automatically scaled to maintain network capacity requirements. This is accomplished by enabling elasticity mode, which calculates device thresholds on key performance indicator (KPI) metrics.
- **Centralized Provisioning**—Network functions (NFs) can be provisioned automatically or manually to meet virtual and physical device demands.
- **Cost-effective**—Supports both virtual and physical network functions through a single CNF. CNFs can be deployed automatically within minutes across a network topology that spans dispersed geographical areas, avoiding the costly manual deployment of Network Functions (NFs).
- **Reporting**—Performance information can be collected from actively deployed VM instances.



---

## Secure Installation Guidelines

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

---

### Secure the Server

You must secure the server before you install Oracle Communications Application Orchestrator .

Use the following documents to help secure the server on which Oracle Communications Application Orchestrator is installed:

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

---

### About the Application Orchestrator Installation

This section briefly describes the Oracle Communications Application Orchestrator installation scenarios.

When you install the software package that includes Oracle Communications Application Orchestrator, the following setup application appears:

```
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]

Each installation option that you can select for your system is described below:

- **ALL**—Installs both Application Orchestrator (standalone only) and Session Delivery Manager. Oracle Communications Application Orchestrator (standalone only) and *Oracle Communications Session Delivery Manager* (default).



**Note:** Oracle Communications Application Orchestrator can only run as a standalone server; clustering is not yet supported.


## Secure Installation Guidelines

Once the installation is complete, the **Application Orchestrator** slider appears with the *Oracle Communications Session Delivery Manager* navigation sliders as shown in the figure below:



**Figure 2: Session Delivery Manager with Application Orchestrator**

- **OCSDM mode**—Installs the Oracle Communications Session Delivery Manager (including Oracle Communications Session Element Manager) only.
- **OCAO mode**—Installs Oracle Communications Application Orchestrator only (standalone). In this configuration scenario, the **Security manager**, **Fault manager** and **Application Orchestrator** sliders are provided only. All other sliders are not available.

 **Note:** See the Oracle Communications Application Orchestrator Installation Guide, Release v1.1 for more detailed installation 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.

## System Support for Encryption and Random Number Generators

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

## Secure Installation Guidelines

Algorithm(s)	Type	Bit Length	Description
MD5 and SHA-1	Asymmetric	128	Provides the following HTTPS encryption support: <ul style="list-style-type: none"><li>• Weak cipher secure socket layer (SSL) Version 2.0</li><li>• Strong cipher SSL 3.0</li><li>• Strong Transport Layer Security (TLS) 1.0</li></ul>
OpenBSD-style Blowfish password hashing, described in "A Future-Adaptable Password Scheme" by Niels Provos and David Mazieres.	Symmetric	64	Encrypts stored passwords.
3des-cbc, aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr, 3des-ctr, arcfour, arcfour128, arcfour256	Asymmetric	128	Provides secure shell version 2 (SSH2) and secure file transfer protocol (SFTP) communications support for file transfer between servers, and between servers to devices.

## Device Security

The Oracle Communications Application Orchestrator server can use trusted X.509 certificates (certificates validated by a CA or self-signed certificate) in its trust store to authenticate Transport Layer Security (TLS) connections to a virtual infrastructure manager (VIM), element manager system (EMS), or to other devices through a plug-in when Transport Layer Security (TLS) communication is required. See the *Application Orchestrator X.509 Certificate Authentication* chapter in the Oracle Communications Application Orchestrator User Guide for more information about managing these certificates.

## Web Server Security

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

### HTTPS Certificate Support

Oracle Communications Application Orchestrator fully supports X.509 certificates and the following certificate extensions are supported through HTTPS:

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

### Set the Maximum Upload File Size Limit


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

## Secure System Password Guidelines

---

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

Use the following guidelines to create user accounts during the Oracle Communications Application Orchestrator installation:

1. Use default database accounts that are restricted for access to the local (Oracle) server only. This includes creating an **nncentral** group and **nncentral** user account to set permissions and lock file systems.
2. Create a sudo user account with limited privileges for running the SNMP Trap Relay port (**162**) for Fault Manager.  
 **Note:** The main Oracle Communications Application Orchestrator process has to run as a sudo user to access port 162.
3. Configure passwords for the **admin** and **Lladmin** user groups before starting Oracle Communications Application Orchestrator.



---

## Security Manager Feature Overview

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

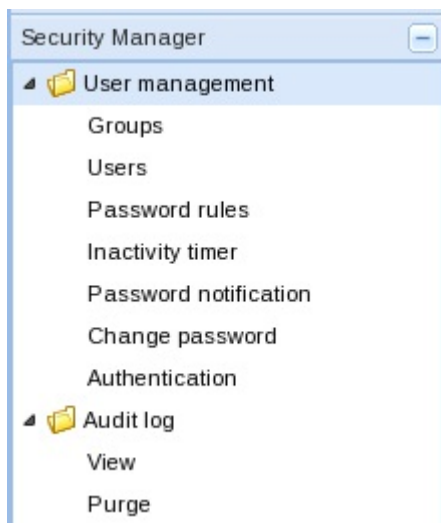
This chapter provides an overview of the Security Manager features. See the Security Manager chapter for more information about these features and how they are configured.

---

### Security Manager

The Security Manager product allows a user with administrator privileges to do the following:

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



**Figure 3: Security Manager Slider Parameters**

### User Groups

A user group is a logical collection of users grouped together to access common information or perform similar tasks. You assign specific permissions to a group and then assign users to it. Those users in turn, inherit the group-based permissions.

The following groups are created by default during the installation:

- **None**—Manually configure permissions for this user group.
- **administrators**—This super user group is privileged to perform all operations.
- **LIAdministrators**—This user group is privileged to perform most operations including Lawful Intercept (LI) configuration changes. These privileges do not include changing the default administrator user credentials. For example, users assigned to the default LI administration group cannot enable or disable accounts, change passwords, or expiration dates for other users in the default LI administration and administration groups.
- **provisioners**—This group is privileged to configure Oracle Communications Application Orchestrator and save and apply the configuration with the exception of a LI configuration.
- **monitors**—This group is privileged to view configuration data and other types of data only. This group cannot configure Oracle Communications Application Orchestrator, and has the fewest privileges.

### Users

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

### Operations Tree Structure

The operations tree structure contains all the security configuration and administrative tasks you can perform in Oracle Communications Application Orchestrator. It is logically arranged with parent and child operations that can be accessed once user group and user accounts are created. Individual access to a specific operation within the tree structure can be provided or denied by assigning a privilege to it. Although Oracle Communications Application Orchestrator displays all the operations it supports, some apply only to users who are licensed for a specific application operation.

The top of the operations tree is the root. There can be one or more operation categories below the root that serve as parents for individual operations (children). The child privilege type of higher-level (or parent) operation is equal or less than the privilege type of its parent. When you change the privilege type of a parent, the child privilege type can change based on this rule. However, if the parent privilege type is returned to its previous privilege type, the child remains at the privilege type to which it was bumped and needs to be promoted manually.

### Change Privileges for User Groups

By default, privileges are assigned to each category of a user group that allow or deny all users within this user group the ability to perform certain operations. You have the option to change the default privilege type for items in each category item of a pre-existing user group or a user group that you create allow or deny all users within this group the ability to perform certain operations. This includes items intended for use with separate application products that you are licensed to use.

### Set the User Inactivity Timer to Prevent Unauthorized Access

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

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



## Audit Logs

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



**Note:** Audit logs contain different information depending on its implementation.

Audit trails include the following information:

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

## Configure External User Authentication

Users belonging to the external domain user group are authenticated outside of Oracle Communications Application Orchestrator by an external domain server. You can select either a RADIUS domain server or Active Directory (AD) domain controller:

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

An external domain user group must be mapped to an internal (local) user group in Oracle Communications Application Orchestrator so that this external domain user group and its users inherit the authorization privileges that are specific to the local user group. See the *Add and Map a Local User Group to an External Domain User Group* section of this chapter for more information.



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



---

## Security Maintenance

Use the security maintenance practices in this chapter to keep Oracle Communications Application Orchestrator secure.

---

### Security Checklist

Use the following checklist to secure Oracle Communications Application Orchestrator before, during and after its installation.

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

### Maintain Security Updates

---

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

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

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

### Security Considerations for Developers

---

Fault resources for alarms can be configured through the Oracle Communications Application Orchestrator REST API. See the Oracle Communications Application Orchestrator REST API Guide, Release 1.1 for more information.