Oracle® Application Management Pack for Oracle Communications

Security Guide

Release 12.1.0.2

E57647-01

December 2014

Oracle Application Management Pack for Oracle Communications Security Guide, Release 12.1.0.2

E57647-01

Contents

Preface

This guide provides guidelines and recommendations for setting up Oracle Application Management Pack for Oracle Communications and its components in a secure configuration.

Audience

This document is intended for system administrators, systems integrators, and other individuals who are responsible for installing, implementing, and administering the Application Management Pack for Oracle Communications software and ensuring that it operates in the manner required by your business.

Documentation Accessibility

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

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` or visit `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` if you are hearing impaired.

Related Documents

To implement security, Application Management Pack for Oracle Communications uses other Oracle products, such as Oracle Enterprise Manager Cloud Control, Oracle Database and WebLogic Server. See the following documents for information on related Oracle products:

- *Oracle Enterprise Manager Cloud Control Security Guide*
- *Oracle Database Security Guide*
- *Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server*

You must also secure Oracle Communications applications installed, configured and monitored by Application Management Pack for Oracle Communications. See the following documents for more information:

- *Oracle Communications ASAP Security Guide*

- *Oracle Communications Billing and Revenue Management Security Guide*
- *Oracle Communications BRM Pipeline Configuration Center Security Guide*
- *Oracle Communications Elastic Charging Engine Security Guide*
- *Oracle Communications Network Charging and Control Security Guide*
- *Oracle Communications Pricing Design Center Security Guide*
- *Oracle Communications Unified Inventory Management Security Guide*

Oracle documentation is available from Oracle Help Center:

http://docs.oracle.com

1

Application Management Pack for Oracle Communications Security Overview

This chapter provides an overview of Oracle Application Management Pack for Oracle Communications security.

Basic Security Considerations

The following principles are fundamental to using any application securely:

- **Keep software up to date.** This includes the latest product release and any patches that apply to it.
- **Limit privileges as much as possible.** Users should be given only the access necessary to perform their work. User privileges should be reviewed periodically to determine relevance to current work requirements.
- **Monitor system activity.** Establish who should access which system components, including how often, and monitor those components.
- **Install software securely.** For example, use firewalls, secure protocols such as SSL and secure passwords.
- **Learn about and use the Application Management Pack for Oracle Communications security features.** See "Implementing Application Management Pack for Oracle Communications Security" for more information.
- **Keep up to date on security information.** Oracle regularly issues security-related patch updates and security alerts. You must install all security patches as soon as possible. See the "Critical Patch Updates and Security Alerts" Web site at:

  `http://www.oracle.com/technetwork/topics/security/alerts-086861.html`

Overview of Application Management Pack for Oracle Communications Security

Application Management Pack for Oracle Communications consists of an Enterprise Manager Cloud Control plug-in providing management capabilities for Oracle Communications applications. The plug-in uses Enterprise Manager Cloud Control as a foundation and therefore relies on the security features implemented by Enterprise Manager Cloud Control. You must also secure the managed Oracle Communications applications.

- System architecture can be referred from *Oracle Enterprise Manager Cloud Control Introduction* document.

- Access to Application Management Pack for Oracle Communications features is controlled by means of Function points, Data based Security, and Workflow based security.
- Application Management Pack for Oracle Communications is dependent on Oracle Enterprise Manager Cloud Control, Oracle WebLogic Server and Oracle Database server. Consult the respective security guides regarding secured use of these tools.
- All Oracle Communications applications managed by the Application Management Pack for Oracle Communications plug-in in Enterprise Manager Cloud Control must also be secured. Consult the respective security guides regarding secured use of these applications.

Understanding the Application Management Pack Environment

When planning your implementation, consider the following:

- **Which resources need to be protected?**
  - You need to protect user data, such as host credentials.
  - You need to protect internal data, such as proprietary source code or application configurations.
  - You need to protect system components from being disabled by external attacks or intentional system overloads.
- **Who are you protecting data from?**

  For example, you need to protect your pricing configuration from competitors, but someone in your organization might need to access that data to manage it. You can analyze your workflows to determine who needs access to the data; for example, it is possible that a system administrator can manage your system components without needing to access the system data.
- **What will happen if protections on a strategic resources fail?**

  In some cases, a fault in your security scheme is nothing more than an inconvenience. In other cases, a fault might cause great damage to you or your customers. Understanding the security ramifications of each resource will help you protect it properly.

Operating System Security

Environments managed by the Application Management Pack for Oracle Communications plug-in in Enterprise Manager Cloud Control likely contain multiple different operating systems in addition to that used on the management server. Enterprise Manager Cloud Control supports many operating systems for both the management server and management agents.

See the following documents for more information on operating system security:

- *Oracle Enterprise Manager Cloud Control Basic Installation Guide*
- *Oracle Linux Security Guide*
- Additional security documentation for operating systems used in your environment.

Oracle Enterprise Manager Cloud Control Security

See *Oracle Enterprise Manager Cloud Control Security Guide*.

Oracle Database Security

See *Oracle Database Security Guide*.

WebLogic Server Security

See *Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server*.

2

Performing a Secure Application Management Pack for Oracle Communications Installation

This chapter presents planning information for your Oracle Application Management Pack for Oracle Communications installation.

For information about installing the Application Management Pack for Oracle Communications plug-in, see *Oracle Application Management Pack for Oracle Communications System Administrator's Guide*.

Application Management Pack for Oracle Communications uses an Oracle Enterprise Manager Cloud Control foundation. For information about installing Enterprise Manager Cloud Control, see *Oracle Enterprise Manager Cloud Control Basic Installation Guide* and *Oracle Enterprise Manager Cloud Control Advance Installation and Configuration Guide*.

Pre-Installation Configuration

You import the Application Management Pack for Oracle Communications plug-in into a running Enterprise Manager Cloud Control instance.

- Pre-installation configuration includes performing all of the required Enterprise Manager Cloud Control installation steps.
- Install the plug-in using the Enterprise Manager Command Line Interface (emcli). The emcli requires a configured client configuration connection to the management server. See the discussion on setting up the emcli connection in *Oracle Application Management Pack for Oracle Communications System Administrator's Guide*.

Installing Application Management Pack for Oracle Communications Securely

This section refers to installing the Enterprise Manager Cloud Control system on which you import the Application Management Pack for Oracle Communications plug-in.

You can perform a custom installation or a typical installation. Perform a custom installation to avoid installing options and products you do not need. If you perform a typical installation, remove or disable features that you do not need after the installation.

Post-Installation Configuration

This section explains security configuration to complete after installing Application Management Pack for Oracle Communications.

- Perform the necessary actions listed in the chapter on keeping Enterprise Manager secure in *Oracle Enterprise Manager Cloud Control Security Guide*.
- Access to log, XSD, XSL, and property files should be with restrictive permissions.
- Access to Oracle Communications application installers should be with restrictive permissions.
- Use secure credentials practices when creating additional Application Management Pack for Oracle Communications plug-in functionality users.

For more information, see *Oracle Application Management Pack for Oracle Communications System Administrator's Guide*.

3

Implementing Application Management Pack for Oracle Communications Security

This chapter provides an overview of the security mechanisms offered by Oracle Application Management Pack for Oracle Communications when used with Oracle Enterprise Manager Cloud Control. For complete instructions, see *Oracle Enterprise Manager Cloud Control System Administrator's Guide*.

About Access Control Points

Enterprise Manager Cloud Control provides many access control options. The following list describes some of the methods and settings you can configure for controlling access and security:

- Authentication Schemes

  Enterprise Manager Cloud Control supports multiple authentication schemes including:

  - Repository-Based Authentication
  - Oracle Access Manager (OAM) SSO
  - Oracle SSO Based Authentication
  - Enterprise User Security Based Authentication
  - LDAP Authentication

  Secure and limit access to Application Management Pack for Oracle Communications plug-in features using an authentication scheme. For more information about authentication schemes, see the chapter on security features in *Oracle Enterprise Manager Cloud Control Security Guide*.

- User Roles

  When you add a user to Enterprise Manager Cloud Control, you can assign that user to roles. For example, users with a system administrator role can access different parts of the administration console than users with a viewer role.

  For more information about user roles, see the chapter on creating roles and administrators in *Oracle Enterprise Manager Cloud Control Getting Started Guide*.

- Rules and Rulesets

  You can control Enterprise Manager Cloud Control behavior when triggering incidents using rules and rulesets ensuring that notifications are sent only to required users.

For more information about rules and rulesets, see the chapter on using Incident Management in *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

- Preferred Credentials

  You setup preferred credentials for connecting to host targets in your environment from the administration console. Enterprise Manager Cloud Control supports configuring preferred credentials by specific host or target type.

  For more information about preferred credentials, see the discussion on preferred credentials in *Oracle Enterprise Manager Cloud Control Security Guide*.

About Managing Enterprise Manager Cloud Control Security

Enterprise Manager Cloud Control offers these security mechanisms:

- Authentication: Validating user logins.
- Authorization: Validating access rights based on roles attached to the user.
  - You can use function points to control user access.
  - You can apply data security to control what data the user can see and the user privileges that operate on the data.
  - You can use Workflow to define user privileges for roles according to the Workflow definition.
  - A user can have multiple roles.
- Enterprise Manager Cloud Control supports audit-ability to track user login session details, areas accessed by user by means of function points and data audits to track data modifications.

Enterprise Manager Cloud Control provides password policy through which secured passwords can be set for users.

A

Secure Deployment Checklist

This appendix provides a checklist for securing Oracle Application Management Pack for Oracle Communications with Oracle Enterprise Manager Cloud Control.

Security Guideline Checklist

Use the following security guideline checklist to help you secure Application Management Pack for Oracle Communications, Enterprise Manager Cloud Control, and its components:

- Make sure the operating system is secured according to the security recommendations of the operating system security guide.
- Follow the guidelines in the *Oracle Enterprise Manager Cloud Control Security Guide*.
- Follow the Oracle Database Security checklist for Oracle Database installation.
- Follow the Oracle WebLogic Server Security checklist for WebLogic Server installation.
- Set the Enterprise Manager Cloud Control administrator password according to a secure password policy.
- Review and change log file permissions after installing Enterprise Manager Cloud Control and importing the Application Management Pack for Oracle Communications plug-in.
- Review roles and users along with the access privileges of each role.
- Use a secure preferred credentials policy for Oracle Communications host targets.