Oracle® Communications Offline Mediation Controller

Security Guide

Release 6.0

E28284-01

April 2012

ORACLE®

Oracle Communications Offline Mediation Controller Security Guide, Release 6.0

E28284-01

Contents

Preface

This guide provides guidelines and recommendations for managing security in Oracle Communications Offline Mediation Controller. It also describes how to install Offline Mediation Controller securely.

Audience

This guide is intended for system administrators, database administrators, and developers.

Downloading Oracle Documentation

Offline Mediation Controller documentation is available from the Oracle Software Delivery Cloud Web site:

http://edelivery.oracle.com

Additional Oracle documentation; for example, documentation for Oracle Database and WebLogic Server, is available from Oracle Technology Network:

http://docs.oracle.com

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 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

For information on managing users and passwords in the Administration Client, see *Administration Client Help*.

1

Offline Mediation Controller Security Overview

This chapter provides an overview of Oracle Communications Offline Mediation Controller 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 as much access as necessary to perform their work. User privileges should be reviewed regularly to determine relevance to current work requirements.
- **Monitor system activity.** Establish who should access which system components, and how often, and monitor those components.
- **Install software securely.** For example, use firewalls, secure protocols such as SSL, and secure passwords.

  See "Performing a Secure Offline Mediation Controller Installation" for more information.
- **Learn and use the Offline Mediation Controller security features.** See "Managing Offline Mediation Controller Security".
- **Use secure development practices.** For example, configure secure file transfers. See "Distributing Files Securely" 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" article on the Oracle Technology Web site:

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

About Offline Mediation Controller Security

Oracle Communications Offline Mediation Controller uses Oracle Unified Directory (OUD), an LDAP database, to store credentials for the users who should be authenticated to use the system. Offline Mediation Controller creates the default password policy for all the users. See the OUD documentation for more information.

Important: To enable user authentication, always install and configure OUD when you install Offline Mediation Controller.

An OUD Administrator role is created at installation. The Administrator role can perform all operations. Change the Administrator password immediately after installation. Assign the User role to most users.

Offline Mediation Controller uses Secure Sockets Layer (SSL) to enable secure communications between applications for inter-process communication. SSL enables authentication, data integrity, and data encryption. Secure Java keystore is used for storing the SSL certificates. Oracle recommends using CA certified certificates in a production environment.

Offline Mediation Controller allows deploying Node Managers on different physical hosts, which are administered through a single Administration Server. It is mandatory to run either SSL enabled or SSL disabled on all components.

Important: Oracle does not recommend running the Administration Server in unauthenticated mode.

About Protecting Data

When planning your Offline Mediation Controller implementation, consider the following:

- **Which resources need to be protected?**

  You need to protect internal data, such as network accounting records, which hold the usage information from the network for billing, reporting, and monitoring.

- **Who are you protecting data from?**

  For example, the network accounting records carry mediation data with identifiable information. This data should only be accessible to users that have a business need to see it.

- **What will happen if protections on 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 helps you protect it properly.

  If the security of network accounting records is compromised, data can be corrupted, which could lead to revenue leakage. Protecting the network accounting records provides revenue assurance.

Distributing Files Securely

Oracle Communication Offline Mediation Controller can use distribution cartridges to distribute the mediation data in the form of files to either a local directory in the file system or to a remote directory. To distribute files, Offline Mediation Controller can use FTP or SFTP. Make sure you select SFTP to make the file transfer secure.

If you are using the JDBC Distribution Cartridge, the credentials are stored in JDBC DC configuration file. This file must carry file permission of **600**.

2

Performing a Secure Offline Mediation Controller Installation

This chapter describes recommended installation steps for Oracle Communications Offline Mediation Controller.

For information about installing Offline Mediation Controller, see *Offline Mediation Controller Installation Guide*.

Pre-Installation Tasks

Perform the following pre-installation tasks:

- Before installing Offline Mediation Controller with the Complete installation option, you must have the empty OUD instance with the base DN configured as:

  ```
  dc=ocomcexample.com
  ```

- Configure Oracle Database advanced security encryption and integrity algorithms for a secure connection from the installer. See the Oracle Database documentation for advanced security configuration parameters. This is required for the Offline Mediation Controller installer to make a secured (encrypted) database connection over the network. For more details, see *Oracle Database Advanced Security Administrator's Guide* at:

  http://docs.oracle.com

- Verify that you have JDK 1.6.0_31 or later installed.

Installing Offline Mediation Controller Securely

When installing a deployment that includes the Administration Server, you must choose the **Complete** installation option to ensure that Oracle Unified Directory (LDAP) is configured. For deployments on a node host that do not need the Administration Server, you can choose the **Custom** installation and select only the required components. See *Offline Mediation Controller Installation Guide* for more information.

During the Offline Mediation Controller installation, the following log files are generated in the **oraInventory/logs** folder. See the Oracle Universal Installer documentation for more information.

- **installAction***TimeStamp***.log**
- **oraInstall***TimeStamp***.err**
- **oraInstall***TimeStamp***.out**

- **silentInstall***TimeStamp***.log** (for silent mode installation)

  where *TimeStamp* is the date and time the log file was created.

The **installAction***TimeStamp***.log** and **oraInstall***TimeStamp***.err** files include details in clear text form entered in the Offline Mediation Controller installation screens. Passwords entered in the screen are not logged in any of the Offline Mediation Controller installation logs. Delete these files if you do not need them for future reference, or protect them appropriately if you do require them. These log files are created with the file-level permission 640 (owner can read/write, group members can read, others cannot do anything).

Post-Installation Tasks

Perform the following tasks after installing Offline Mediation Controller:

- Configuring Certificates
- Encoding Keystore Passwords
- Setting File Permissions

Configuring Certificates

To configure certificates:

1. Create the Node Manager certificate and import it to the Administrator Server truststore. See the discussion of post-installation tasks in *Offline Mediation Controller Installation Guide*.
2. Create the Administration Server certificate and import it to the Administration Client truststore. See the discussion of post-installation tasks in *Offline Mediation Controller Installation Guide*.
3. If you need to connect to a different Node Manager or Node Host by using a single Administration Server in secure mode, import the Node Manager certificate, *OMC_home***/config/nodemgr/nodeManager.cer**, to the respective remote **adminServerTruststore.jks**. The physical file of node manager certificate (**.cer**) must be securely copied to the respective Administration Server's machine. You can use the following command on the machine where the Administration Server is installed:

   ```
   $OMC_HOME/jre/bin/keytool -import -v -trustcacerts -alias <alias name> -file
   <nodeManager.cer file path> -keystore $OMC_
   HOME/config/adminserver/adminServerTruststore.jks
   ```

   This command asks you for the truststore password. Make sure you give different alias for different node manager while executing this import command.
4. After completing these steps, stop and restart Offline Mediation Controller.

Encoding Keystore Passwords

When secure communication is enabled, you must run the **encode** script to encode keystore passwords for the Administration Server and the Node Manager. You then add the encoded password to the following configuration files:

- Administration Server: *OMC_home***/config/adminserver/ASkeystore.cfg**
- Node Manager: *OMC_home***/config/nodemgr/NMkeystore.cfg**

See *Offline Mediation Controller Installation Guide* for more information.

Setting File Permissions

Oracle recommends keeping file permissions as restrictive as possible.

After installing Offline Mediation Controller, if you are configuring a JDBC Distribution cartridge, make sure that the file permission for its configuration file is set to **600**.

The default permissions set for the installed files are as follows:

- For non-executable files: **600**
- For executable files: **700**

Uninstalling Offline Mediation Controller

The following files remain in the system after uninstalling Offline Mediation Controller:

- Install logs in **oraInventory/logs**.
- *OMC_home***/oui/data.properties**: This file is used to auto-populate the data during re-installs.

Delete these files if you do not need them or protect them appropriately if they are required for further installations.

3

Managing Offline Mediation Controller Security

This chapter describes how to manage security in Oracle Communications Offline Mediation Controller.

Starting Offline Mediation Controller

When starting Offline Mediation Controller processes, make sure that the Oracle Unified Directory (LDAP) process starts with the Administration Server. This ensures that only authorized users can log in to mediation processes.

You can start the Oracle Unified Directory process in the following ways:

- Go to directory where OUD instance is created (*instance-dir***/OUD/bin**) and enter **start-ds**.
- You can start the Administration Server process manually (**adminsvr**), but do not use the **-x** option, because that does not start the Oracle Unified Directory process. Using the **-x** option runs the Administration Server in unauthenticated mode, which is not recommended.

Configuring Secure Communications Between Applications

Offline Mediation Controller uses Remote Method Invocation (RMI) over Secure Sockets Layer (SSL) to enable secure communications between applications. SSL enables authentication, data integrity, and data encryption.

The Administration Client communicates with the Administration Server by using SSL. During authentication, the Administration Server provides the information using a certificate. It also provides data integrity through an integrity check value. See the discussion on creating certificates in *Offline Mediation Controller Installation Guide*.

Offline Mediation Controller supports the session expiration between the Administration Client and the Administration Server based on the value configured in the **AdminServerImpl.properties** file in *OMC_home***/web/htdocs**. Oracle recommends using the default value.

Enabling and Disabling SSL Mode

It is assumed that if SSL is enabled for one of the Offline Mediation Controller components, SSL is enabled for the other components.By default, the Offline Mediation Controller system runs in secure mode with SSL enabled. See *Offline Mediation Controller System Administrator's Guide* for more information.

Configuring Password Policy Attributes

Offline Mediation Controller uses a predefined password policy. This can be updated to suit your business policies.

Attribute values can be modified in *OMC_home***/bin/createPasswordPolicy** script. To update the system with new attributes, edit and run the script, and restart the Administration Server. See *Offline Mediation Controller System Administrator's Guide* for more information.

A

Secure Deployment Checklist

Follow this checklist to deploy your Oracle Communications Offline Mediation Controller securely.

1. Pre-installation steps:
   a. Install Oracle Unified Directory (LDAP).
   b. Configure Oracle Database advanced security encryption and integrity algorithms for a secure connection from the installer.
2. Installation steps:
   a. Install Offline Mediation Controller with the default **Complete** mode.
3. Post-installation steps:
   a. Create, exchange, and import certificates. See "Configuring Certificates" for more information.
   b. Verify that file permissions for the installed files are **600** for all non-executable files and **700** for all executable files.
   c. Delete the log files in **oraInventory/logs** folder if you do not need them or protect them appropriately if they are required for further installations.
   d. When you are starting mediation processes, keep in mind to start Oracle Unified Directory (LDAP) along with the processes. This ensures that only authorized users can log in to the mediation processes. See "Starting Offline Mediation Controller" for more information.
   e. While configuring JDBC cartridges, make sure that the file permissions for the configuration file of the cartridge is set to **600**.