# Oracle® Application Integration Architecture

## Security Guide

Release 12.3.2
F92299-01
June 2024

ORACLE

Oracle Application Integration Architecture Security Guide, Release 12.3.2

F92299-01

# Contents

# Preface

This document describes Oracle Application Integration Architecture (Oracle AIA) security considerations and procedures.

## Audience

This document is intended for system administrators, system integrators, database administrators, and other individuals who are responsible for managing Oracle AIA and ensuring that the software is operating in a secure manner. This guide assumes that you have a working knowledge of Oracle AIA, the relevant operating system, Oracle Database, Oracle Fusion Middleware, and Oracle Service-Oriented Architecture.

## 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.

## Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

1

# Overview

This chapter provides an overview of Oracle Application Integration Architecture (Oracle AIA) 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, and how often, and monitor those components.
- **Install software securely.** For example, use firewalls, secure protocols (such as Transport Layer Security (TLS) and Secure Sockets Layer (SSL), and secure passwords. See "Performing a Secure Oracle AIA Installation " for more information.
- **Learn about and use the Oracle AIA security features.** See "Implementing Oracle AIA Security " for more information.
- **Use secure development practices.** For example, take advantage of existing database security functionality instead of creating your own application security. See "Security Considerations for Developers " 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 website:

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

## Overview of Oracle AIA Security

Oracle AIA security is designed to protect product, account, order, and asset data, logs, and interfaces.

Oracle AIA pre-built integrations are built on Oracle Service-Oriented Architecture (SOA) and an infrastructure stack that includes Oracle WebLogic Server and Oracle Database. This stack is secured by default by the WebLogic Server Security Infrastructure.

- **Application security:** Access to application modules and artifacts is authenticated using the WebLogic Server authentication framework.
- **Data security:** Solution data, including product, account, order, and asset data, is stored in Oracle Metadata Services and SOA schemas in the Oracle Database, which requires database credentials to access.

- **Interface security:** Oracle AIA composite service and references (interfaces) are secured by WebLogic Server security policies using Web Services Manager (WSM). Credentials for accessing external systems are configured and stored securely.
- **Application log security:** Application log content is configured by users of the WebLogic Server **Administrators** group. The application distribution, settings and properties, and logs are protected by the user authorization and authentication procedures of the host operating system. Only the user who starts WebLogic Server has access to the files, based on file permissions.
- **Database security:** The database credentials are stored securely in Oracle AIA configuration files in the WebLogic Server SOA domain.

## Understanding the Oracle AIA Environment

When planning your Oracle AIA implementation, consider the following:

- **Which resources need to be protected?**
  - You need to protect customer data, such as credit card numbers.
  - You need to protect internal data, such as confidential proprietary source code.
  - 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 subscribers' data from other subscribers, 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 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.

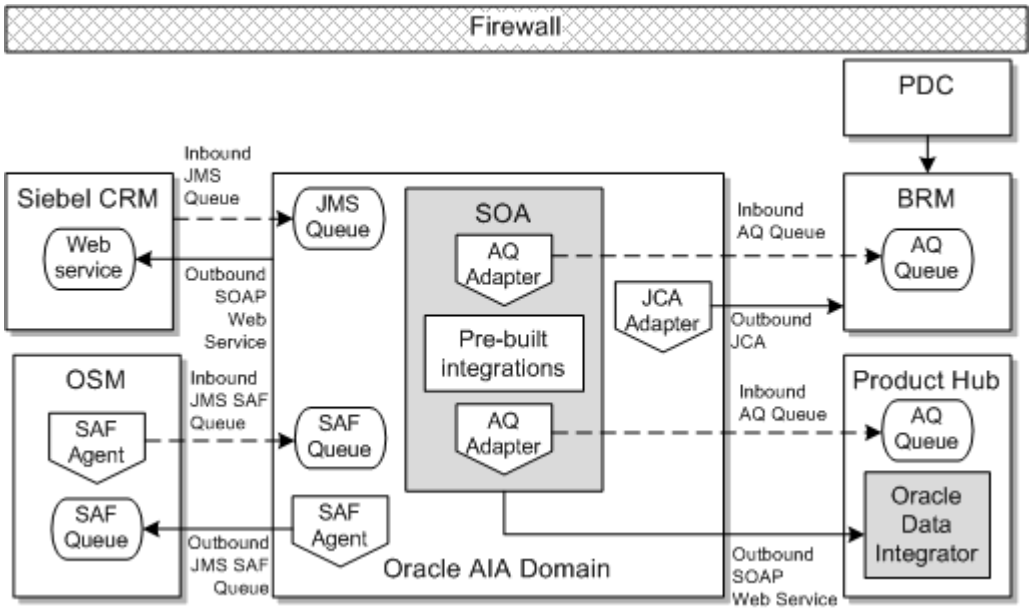
## Recommended Deployment Topology

In the recommended deployment for Oracle AIA all applications reside on your premises and are protected from attacks by a firewall, which can be configured to block known illegal traffic types. Communication occurs between queues, adapters and agents.

Figure 1-1 shows on an on-premises topology with the following integrated applications:

- Siebel CRM for customer relationship management and order capture
- Oracle Communications Order and Service Management (OSM) for order processing and fulfillment
- Oracle Communications Billing and Revenue Management (BRM) for billing
- Oracle Communications Pricing Design Center (PDC), Oracle Product Hub, and Oracle Data Integrator for Communications for product and pricing management

**Figure 1-1 On-Premises Oracle AIA Topology**




# Operating System Security

This section describes operating system security topics that are specific to Oracle AIA. Oracle AIA is configured and managed within WebLogic Server, the SOA container, and the SOA Core Extension.

See the documentation for your operating system and for these foundation applications for general information about security.

See the Certifications tab on My Oracle Support for information about required software versions and patches.

## Restricting Permissions for Oracle AIA Directories

Oracle recommends keeping the permissions as restrictive as possible for your business needs. When installing on UNIX or Linux, consider using **umask 066** to deny read and write permission to all users except the user that installed the software. Oracle AIA creates files in the directories listed in Table 1-1. Examine these directories to ensure they have the appropriate permissions.

**Table 1-1 Oracle AIA Directories**

| Name | Description |
|---|---|
| Fusion Middleware home | The directory in which Oracle Fusion Middleware components are installed. This directory contains the base directory for Oracle WebLogic Server, among other files and directories. |
| Oracle AIA home (COMMS_HOME environment variable) | The directory in which Oracle AIA is installed. This is the **comms_home** directory within the Oracle base directory. |

**Table 1-1 (Cont.) Oracle AIA Directories**

| Name | Description |
|---|---|
| Domain home | The directory that contains the configuration for the domain onto which Oracle AIA is deployed. The default is *MW_home*/**user_projects/domains/***domain_name* (where *MW_home* is the Fusion Middleware home and *domain_name* is the name of the Oracle AIA domain), but it is frequently set to some other directory at installation. |

## Port Security

Oracle AIA communicates over a limited number of ports. Depending on your solution requirements, additional ports may be required, especially if Oracle AIA is deployed to a WebLogic Server cluster.

The types of ports Oracle AIA uses are listed in Table 1-2.

**Table 1-2 Oracle AIA Ports**

| Port | Port Description |
|---|---|
| Administration server port | The default value is 7001, but a different value can be set during domain creation. |
| Administration server SSL port | The default value is 7002, but a different value can be set during domain creation. |
| Node Manager port | The default value is 5556, but a different value can be set during Node Manager configuration. |
| SOA managed server ports | The default value is 8001, but a different value can be set during domain creation.<br>In a clustered deployment, each managed server should have a different port. For example, 8002, 8003, and so on. |
| Oracle HTTP Server port | The default value is 7777, but a different value can be set during Oracle HTTP Server configuration. |
| SOA database port | The default is 1521, but a different value can be set during database creation. |

# Oracle Database Security

This section describes database security topics specific to Oracle AIA. For more information about securing Oracle Database, see *Oracle Database Security Guide* and *Oracle Database Advanced Security Guide*.

## Dependent Schemas

Before creating the WebLogic Server domain, you must create certain database schemas using the Oracle Fusion Middleware Repository Creation Utility (RCU). For information about RCU, see *Oracle Fusion Middleware Creating Schemas with the Repository Creation Utility*.

# WebLogic Server Security

This section contains WebLogic Server security information relevant to Oracle AIA.

For additional information about WebLogic Server security, see *Oracle Fusion Middleware Securing a Production Environment for Oracle WebLogic Server* and *Oracle Fusion Middleware Administering Security for Oracle WebLogic Server*.

When planning your WebLogic Server domain installation, keep the following recommendations in mind:

- **Secure the WebLogic Server host:** WebLogic Server domain and server configuration files should be accessible only by the operating system users who configure or run WebLogic Server. The **AIAInstallProperties.xml** and **AIAConfigurationProperties.xml** files should be readable by the Oracle AIA user. No other operating system user (apart from the system administrators) should have read, write, or execute access to WebLogic Server product files or your domain files.
- **Do not run WebLogic Server in development mode in a production environment:** Production mode sets the server to run with settings that are more secure and appropriate for a production environment. For more information about development mode and production mode, see the information about domain modes in *Understanding Domain Configuration for Oracle WebLogic Server*.
- **Use appropriate encryption:** WebLogic Server includes a set of demonstration private keys, digital certificates, and trusted certificate authorities that are for development only; do not use the demonstration identity and trust in a production environment. See the topic on configuring keystores in the *Oracle WebLogic Server Administration Console Online Help* and the information about configuring SSL in *Administering Security for Oracle WebLogic Server* for more information about encryption.

2

# Performing a Secure Oracle AIA Installation

This chapter presents planning information for your Oracle Application Integration Architecture (Oracle AIA) installation.

For information about installing Oracle AIA, see *Oracle AIA Installation Guide*.

## Pre-Installation Configuration

Oracle AIA is installed on top of a database instance, an Oracle WebLogic Server domain, and SOA infrastructure deployments that have been properly configured. See "Operating System Security", "Oracle Database Security", and "WebLogic Server Security" for details on secure file system, database, and WebLogic Server domain configuration.

## Installing Oracle AIA Securely

This section describes ways of ensuring that Oracle AIA is installed securely and information that you can use to secure installed components after installation.

### Installation Type

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.

### Security-Relevant Installation Steps

Some steps in the installation process have security implications that you should keep in mind.

- Run the Oracle AIA Installer, Oracle AIA Configuration Wizard, and Oracle AIA deployment scripts from the same physical machine where the WebLogic administration server is running. This enhances security by avoiding communication over the network.

  > **Note:**
  >
  > The deployment scripts do not support communication by SSL for WebLogic Scripting Tool commands.

- When you run the Oracle AIA Installer and Oracle AIA Configuration Wizard, you can choose to save the information you entered to a response file, so that you can use it to perform a silent installation later. When you save the response, the Installer or Configuration Wizard saves passwords as **<SECURE>**. Immediately before running a silent installation or configuration, you must edit the file to enter the passwords and remove them when you are done.
- The Oracle AIA Installer and Oracle AIA Configuration Wizard automatically encrypt credentials collected when writing to the **AIAInstallProperties.xml** file. The deployment

scripts copies these credentials to the **AIAConfigurationProperties.xml** file in encrypted format for all required Oracle AIA composites. The composites use the credentials to communicated with integrated applications at run time.

# 3
# Implementing Oracle AIA Security

This chapter provides a synopsis of the Oracle Application Integration Architecture security features.

## Foundation Software Security

Oracle AIA runs within an Oracle WebLogic Server Service-Oriented Architecture (SOA) container. You can leverage all WebLogic Server security infrastructure functionality, such as authentication, authorization, and secure auditing.

## Secure Inbound Communication Points

The following inbound communication points must be managed securely:

- Siebel customer relationship management (Siebel CRM) to Oracle AIA:
  - Siebel CRM communicates asynchronously with Oracle AIA.
  - Oracle AIA exposes Java Message Service (JMS) queues to Siebel CRM.
  - Siebel CRM adds messages to Oracle AIA JMS queues.
  - The Oracle AIA consumer services subscribed to the queues pick up the messages for processing.
  - Oracle AIA JMS queues are protected with user credentials created and maintained in WebLogic Server security infrastructure.
  - You configure and maintain Oracle AIA queue details and credentials in Siebel CRM. See *Siebel CRM Security Guide* for more information about managing security in Siebel CRM.
- Oracle Communications Order and Service Management (OSM) to Oracle AIA:
  - OSM communicates asynchronously with Oracle AIA.
  - Oracle AIA exposes JMS Store and Forward (SAF) queues to OSM.
  - OSM adds messages to Oracle AIA JMS SAF queues.
  - The Oracle AIA consumer services subscribed to the queues pick up the messages for processing.
  - Oracle AIA JMS SAF queues are protected with user credentials created and maintained in WebLogic Server security infrastructure.
  - You configure and maintain Oracle AIA JMS SAF queue details and credentials in OSM. See *OSM Security Guide* for more information about managing security in OSM.
- Oracle Communications Billing and Revenue Management (BRM) to Oracle AIA:
  - BRM communicates asynchronously with Oracle AIA.
  - BRM exposes Advanced Queueing (AQ) database queues to Oracle AIA.
  - BRM adds messages to the AQ database queues.

  - The Oracle AIA AQ adapter polls the AQ database queues and picks up the messages for processing.
  - You configure and maintain the BRM AQ database queue details and credentials in Oracle AIA.
- Oracle Product Hub to Oracle AIA:
  - Product Hub communicates asynchronously with Oracle AIA.
  - Product Hub exposes Advanced Queueing (AQ) database queues to Oracle AIA.
  - Product Hub adds messages to the AQ database queues.
  - The Oracle AIA AQ adapter polls the AQ database queues and picks up the messages for processing.
  - You configure and maintain the Product Hub database queue details and credentials in Oracle AIA.

# Secure Outbound Communication Points

The following outbound communication points must be managed securely:

- Oracle AIA to Siebel CRM:
  - Oracle AIA communicates synchronously with Siebel CRM in a request-response pattern.
  - Siebel CRM exposes SOAP web services to Oracle AIA.
  - Oracle AIA invokes the SOAP web services and receives a response from Siebel CRM.
  - Siebel CRM web services are protected with user credentials.
  - You configure encrypted Siebel CRM web service credentials in Oracle AIA configuration files.
  - Oracle AIA uses Session Pool Manager to get a session token that is associated with the SOAP request.
  - Oracle AIA releases the session token when it receives a response from Siebel CRM.
- Oracle AIA to OSM:
  - Oracle AIA communicates asynchronously with OSM.
  - Oracle AIA adds messages to the OSM JMS SAF queues.
  - The OSM JMS consumers subscribed to the queues pick up the messages for processing.
  - OSM JMS SAF queues are protected with user credentials created and maintained in WebLogic Server security infrastructure.
  - Oracle AIA stores the encrypted OSM JMS SAF queue credentials in configuration files.
- Oracle AIA to BRM:
  - Oracle AIA communicates synchronously with BRM in a request-response pattern.
  - BRM exposes the JCA Resource Adapter to Oracle AIA.
  - Oracle AIA invokes the JCA Resource Adapter and it invokes BRM opcodes.
  - The JCA Resource Adapter is protected with user credentials.

- You configure and maintain encrypted JCA Resource Adapter credentials in Oracle AIA configuration files.

# Web Service Security

By default, Oracle AIA services are secured by SOA and Oracle WebLogic Server security infrastructure. Oracle AIA composites are protected by authentication through Oracle Web Services Manager security policies. When you deploy pre-built integrations, the default policies are automatically applied as follows:

- Global security policies are automatically attached to all composites that match the Oracle AIA naming conventions.
- Local security policies are automatically attached to composites whose security requirements differ from the global policy or whose name does not match the Oracle AIA naming conventions.

Oracle recommends the following:

- Harden the services with message protection in your production environment. Before modifying the default security policies, you must understand Oracle Web Services Management security policy configuration and the global and local deployment strategies. Changes to the default policies without proper understanding could impact the integration's expected behavior.
- Do not completely disable default security policies.
- Validate that the default security policies are correctly deployed before running your production system.

For more information about security policies, see the discussion of working with security in *Oracle Fusion Middleware Developer's Guide for Oracle Application Integration Architecture Foundation Pack*.

4

# Security Considerations for Developers

This chapter provides information for developers about how to create secure applications for Oracle Application Integration Architecture (Oracle AIA), and how to extend Oracle AIA without compromising security.

## Secure Extensions and Customizations

For information about extending and customizing Oracle AIA, see:

- *Oracle Communications Order to Cash Integration Pack Implementation Guide*
- *Oracle Communications Agent Assisted Billing Care Integration Pack Implementation Guide*
- *Oracle Communications Product Master Data Management Integration Pack Implementation Guide*
- *Oracle Fusion Middleware Developer's Guide for Oracle AIA Foundation Pack*
- *Oracle AIA Installation Guide*

5

# Securing Your AIA Cloud Native Deployment

This chapter describes security considerations for your AIA cloud native deployment.

Based on the variety of customizations and plugins you have for your Kubernetes platform, you need to consider all possible security risks and have a mitigation plan in place.

## General Security Considerations

Consider the following general security guidelines:

- While the **values.yaml** file of the Helm charts can be stored in versioning systems, it is recommended that you do not use it to save sensitive information such as application credentials. Instead, use Kubernetes secrets.
- Use the sample scripts provided with the cloud native toolkit for creating secrets to maintain credentials for various applications such as OSM, Siebel, BRM, SOA, AIA, and RCU.
- Use the sample scripts for secrets and store them in a vault that has strong encryption.
- Secure your Kubernetes secrets by using strong encryption, instead of a default base64 encryption.
- Use Kubernetes RBAC on minimum privileges policy and restrict kubectl get, list, and watch privileges for secrets, pods, logs, and services.
- Use Kubernetes RBAC on minimum privileges policy and restrict resource access to pods such as secrets and network.
- Consider Kubernetes general security guidelines. For details, see Kubernetes documentation available at: https://kubernetes.io/docs/setup/best-practices/enforcing-pod-security-standards/.

# A

# Secure Deployment Checklist

The following security checklist lists guidelines to help you secure Oracle Application Integration Architecture (Oracle AIA) and its components.

- Configure and deploy only the pre-built integration options you need.
- Enforce strong password management.
- Restrict and control user privileges.
- Restrict network access by doing the following:
  - Use firewalls.
  - Never leave an unnecessary opening in a firewall.
  - Monitor who accesses your systems.
  - Because network traffic is not encrypted, you must physically secure the JDBC network connection between the application server to the database by using a subnet dedicated to this communication and ensure that the network is not accessible to ordinary users.
  - Install the operating system in a secure location that is difficult for a hacker to access.
- Apply all security patches and workarounds.
- Encrypt sensitive information.
- Contact Oracle support if you discover a vulnerability in any Oracle product.