Oracle® Fusion Middleware

Oracle Advanced Authentication and Oracle Adaptive Risk Management Readme

OAA and OARM 12.2.1.4.1

F43824-16

February 2025

Oracle Advanced Authentication and Oracle Adaptive Risk Management Readme

This is a readme document for Oracle Advanced Authentication (OAA) and Oracle Adaptive Risk Management (OARM) 12.2.1.4.1.

OAA, OARM, and OUA Installation Images

Oracle Advanced Authentication (OAA) and Oracle Adaptive Risk Management (OARM) can be deployed as standalone products or can be deployed together. The following deployment modes are supported:

- `OAA-OARM`

- `OAA` only
- `OARM` only

Oracle Universal Authenticator (OUA) must be deployed with OAA and OARM, hence the only deployment mode supported for OUA is: `OAA-OARM-OUA`

To download the installation images see document ID 2723908.1 on My Oracle Support.

For installation instructions, see Installing OAA, OARM, and OUA.

Updates in OAA, OARM, and OUA February 2025 Refresh

OAA, OARM, and OUA includes the following updates in this refresh:

- **Support for SSL to Oracle Database**:
  This refresh includes changes to configuring the OAA installation to communicate with the Oracle Database via SSL. See, Database Configuration.
- **Self-Service Portal Customization**:

  Additional customization features added for button, text, and menu colors for the Self-Service Portal. See, Customizing the OAA User Interface.
- **Oracle Universal Authenticator Client Application Customization**

  Support added to OAA to allow customization of the Oracle Universal Authenticator client application. See, Customizing Oracle Universal Authenticator.

  The documentation has been updated to reflect these changes. For previous releases of the documentation, contact Oracle Support.

Updates in OAA, OARM, and OUA December 2024 Refresh

OAA, OARM, and OUA includes the following updates in this refresh:

- **Installation Simplification:**
  This refresh includes changes to the installation procedure. Multiple prerequsite and post installation tasks have now been removed and occur as part of the installation.

  The documentation has been updated to reflect these changes. For previous releases of the documentation, contact Oracle Support.

Updates in OAA and OARM, October 2024 Refresh

OAA and OARM includes the following updates in this refresh:

- **Support for New Features in Oracle Universal Authenticator:**
  This refresh includes support for configurable challenges and enhancements to password management in OUA.

Updates in OAA and OARM, June 2024 Refresh

OAA and OARM includes the following updates in this refresh:

- **Support for JSON Web Token:**
  OAA now supports the use of a JSON Web Token (JWT) in the authentication header for invoking OAA REST APIs. See Configuring OAuth JWT For REST APIs.
- **SafeID Support for Time-based OTP**
  SafeID is a security device that generates time-based one-time passwords (TOTP). OAA now supports the SafeID/Classic device as a TOTP authenticator that generates a TOTP passcode. See Managing Factors in the Self-Service Portal.
- **Support for Google Firebase Cloud Messaging HTTPv1 API in Mobile Push Notification**
  Google is deprecating their legacy Firebase Cloud Messaging (FCM) APIs in June 2024 and migrating to HTTP v1 APIs. It is recommended that all new configurations use HTTP v1 APIs. See Configuring Oracle Mobile Authenticator Push Notification for Android.

  To use HTTPv1 APIs you must be using the OAA June 2024 refresh release or later.

  If you have configured push notifications for Android in releases prior to the OAA June 2024 refresh, you will be using legacy FCM APIs. Administrators should migrate to HTTP v1 APIs by upgrading to the OAA June 2024 refresh or later. The steps to upgrade and migrate to HTTP v1 APIs can be found in Upgrading OAA, OARM, and OUA. See Upgrading OAA, OARM, and OUA.

Updates in OAA and OARM, April 2024 Refresh

OAA and OARM includes the following updates in this refresh:

- **Support for Oracle Universal Authenticator:**
  Oracle Universal Authenticator (OUA) is a unified authentication solution that provides device authentication and cross-platform single sign-on (SSO) to web-based applications. OUA uses OAA to extend device authentication with multi-factor authentication (MFA). See About OUA.

Updates in OAA and OARM, January 2024 Refresh

OAA and OARM includes the following updates in this refresh:

- **Support for TOTP Registration URL:**
  OAA provides a Rest API to generate a Registration URL for mobile applications enrolling for Time-based One Time Password (TOTP) creation.

  See Configuration Properties for OAA for more information on the configuration properties provided for controlling REST API services.
- **Support to Configure Bypass Challenge Property**

Customers can now configure the bypass challenge property, which allows them to bypass challenges during subsequent logins for a configurable time period. See Configuration Properties for OAA .

- **Enhanced Error Handling for OAA and OAM Integration**
  Error handling is now improved significantly, when OAA and OAM are integrated for runtime user flows. This enhancement requires the corresponding OAM bundle patch, which is released in January 2024.

Updates in OAA and OARM, September 2023 Refresh

OAA and OARM includes the following updates in this refresh:

- **Support for XML-formatted payload for REST APIs:**
  XML payloads are now supported by the OAA/OARM Runtime and Risk Service APIs. See REST API for Risk Service in Oracle Advanced Risk Manager and OAA Runtime API.
- **Enhancements to the OAA/OARM User Runtime and Administration Screens:**
  The OAA/OARM Runtime UI now allows you to customize the colors of the buttons and header/footer. The Administrative UI now allows you to customize the colors of the header and footer. See Customizing the OAA User Interface.
- **Enhancements to the Geo-location Data Loader:**
  The geo-location data loader now uses the install properties file for database connection details. See Loading Geo-Location Data.
- **Configurable Number of Devices for Challenge Factor:**
  End-users can now register more number of devices for each challenge factor.

Updates in OAA and OARM, June 2023 Refresh

OAA and OARM includes the following updates in this refresh:

- **Configurable Number of Questions for Challenge Flow:**
  OAA/OARM KBA REST API can now handle multiple questions that a user must answer in the challenge flow. See OAA Runtime API and Configuration Properties for OAA.
- **Process Rules and User Preferences REST API:**
  OAA/OARM REST API changes in Process Rules, and Get User Preferences, to only allow sensitive information to be passed in the request body. See Process rules and Get User Preferences.
- **Geolocation Performance Enhancement**
  Geolocation data load time for incremental loads is now reduced.
- **Administration Console improvements for handling expired Administration user session:**
  Expired administration user sessions now redirect the user to the login page and/or the OAuth consent page.

Updates in OAA and OARM, May 2023 Refresh

OAA and OARM includes the following updates in this refresh:

- **New API to Generate TOTP Secret Key with Expiry Time:**
  OAA/OARM APIs are enhanced to support generation of TOTP secret keys that automatically expire unless validated in the specified time window. See OAA Runtime API.
- **TOTP Registration Support with QR Code:**
  OAA/OARM now supports the ability for users to register a Mobile Authenticator using a QR code, as well as manual key entry. See Managing Factors in the User Preferences UI.
- **Screen Rendering Enhancements:**
  Screen rendering has been enhanced in runtime challenge factor screens to optimally render on small screens.
- **Email and SMS Message Content Enhancements:**
  Time of access and the accessed resource URL in the messages, are now based on information provided in the OAM integration flow.

Updates in OAA and OARM, March 2023 Refresh

OAA and OARM includes the following updates in this refresh:

- **Enhancements to the Geo Data Load:**
  OAA/OARM now provides support for Neustar Version 7 Geo Data format. Data files supplied in this format can now be imported using the Location Loader utility included with the Management Container.
- **Support for Knowledge-Based Authentication API:**
  OAA/OARM now supports Knowledge-Based Authentication question API for user challenge capabilities. See OAA Runtime API.
- **Support for Personal Image and Phrase for User Preferences API**
  OAA/OARM now supports managing personal image and phrase using the User Preferences API. See OAA Runtime API.

Updates in OAA and OARM, October 2022 Refresh

OAA and OARM includes the following updates in this refresh:

- **Enhancements to the OAA/OARM Administration Console**
  - OAA/OARM supports Knowledge-Based Authentication through Security Questions. Knowledge-based authentication is an authentication method which is used to challenge the user to prove identity based on the user's answers substantiated by a real-time interactive question and answer process. OAA/OARM Administration Console provides capabilities to manage Questions, Registration Logic, and Answer Logic. See Configuring Security Questions for Knowledge-Based Authentication.
  - OARM provides export and import capabilities for questions, validations, groups, and profiles.
- **Factor Verification**

Factor verification allows users to verify a factor in the User Preferences UI after the factor has been added. This allows a user to check the factor is working, before it is used in a user challenge. See Configuring Factor Verification.

In previous releases, when a factor was added, it was not possible to verify the factor until an end user accessed a resource that required second factor authentication.

- **Partitioned Schema**
  The introduction of partitioned schema allows for maintenance of transaction data. Scheduled jobs make sure that partitions are created for new data with correct details. Administrators can also purge and archive data to release data that is no longer required. See Understanding Partition Schemas.

Updates in OAA and OARM, April 2022 Refresh

OAA and OARM includes the following updates in this refresh:

- **OAA-OIM Integration**
  You can implement the password management feature for OAA-protected applications by integrating OAA with Oracle Identity Manager (OIM). For details, see Integrating OAA with OIM.
- **Runtime Support for CRI-O Environment**
  CRI-O is a lightweight container runtime for Kubernetes. When you deploy Kubernetes worker nodes, CRI-O can also be deployed. CRI-O allows Kubernetes to use any OCI-compliant (Open Container Initiative) runtime as the container runtime for running pods. It is an alternative to using Docker as the runtime for Kubernetes.

Updates in OAA and OARM, January 2022 Refresh

OAA and OARM includes the following updates in this refresh:

- **Oracle Adaptive Risk Management**
  Oracle Adaptive Risk Management (OARM) is a comprehensive system that provides a way to monitor and control any user activity in your IT infrastructure (Single sign-on, Business Transactions). For details, see Introducing Oracle Adaptive Risk Management
- **Customization of OAA User Interface**

  You can customize certain features of the OAA user interface (UI), such as the Administration Console UI, User Preferences Console UI, and the Runtime UI using the configuration properties. For details, see Customizing the OAA User Interface
- **Push Notification for Oracle Mobile Authenticator**

  OAA allows you to configure push notification for the OMA app. For details, see Configuring Push Notification for Oracle Mobile Authenticator
- **Knowledge Based Authentication (Challenge Question)**

  OAA supports Knowledge Based Authentication factor through challenge questions and answers.

Updates in OAA, July 2021 Refresh

Oracle Advanced Authentication includes the following updates in this refresh:

- **Support for Self Signed Certificates in OAA for OIDC Flow**

  Self signed certificates can be added into the JRE truststore. This enables the OAA installation in test environments to use self signed certificates.

- **Support for Distributed Cache for High Availability (HA) Scenarios**

  For HA scenarios, multiple replicas of pods can work together using a distributed cache.

Oracle Fusion Middleware Oracle Advanced Authentication and Oracle Adaptive Risk Management Readme, OAA and OARM 12.2.1.4.1
F43824-16