Oracle® Banking Microservices Architecture

Security Guide

Release 14.7.1.0.0
F87330-01
September 2023

ORACLE

Oracle Banking Microservices Architecture Security Guide, Release 14.7.1.0.0

F87330-01

Contents

Preface

Purpose

This guide provides security-related usage and configuration recommendations for Oracle Banking Microservices Architecture. It also describes the procedures required to implement or secure certain features, but it is not a general-purpose configuration manual.

Audience

This guide is primarily intended for IT department or administrators deploying Oracle Banking Microservices Architecture and Third-party or vendor software's. It includes the information related to IT decision makers and users of the application.

> **Note:**
>
> Readers are expected to have basic operating system, network, and system administration skills with an awareness of vendor/third-party software's and knowledge of Oracle Banking Microservices Architecture application.

Scope

Read Sections Completely

Each section should be read and understood completely. Instructions should never be blindly applied. Relevant discussion may occur immediately after instructions for an action, so be sure to read whole sections before beginning implementation.

Understand the Purpose of this Guidance

The purpose of the guidance is to provide security-relevant configuration recommendations. It does not imply the suitability or unsuitability of any product for any particular situation, which entails a risk decision.

Limitations

The guide is limited in its scope to security-related issues. This guide does not claim to offer comprehensive configuration guidance. For general configuration and implementation guidance refer to other sources such as Vendor specific sites.

Test in Non-Production Environment

To the extent possible, guidance should be tested in a non-production environment before deployment.

Ensure that any test environment simulates the configuration in which the application will be deployed as closely as possible.

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.

Related Resources

For more information on any related features, refer to the following documents:

- Oracle Banking Microservices Architecture Product User Guides
- Oracle Banking Microservices Architecture API Security Guide

Conventions

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Acronyms and Abbreviations

The list of acronyms and abbreviations used in this guide are as follows:

Table 1 Acronyms

Abbreviation	Description
JWE	JSON Web Encryption
JWS	JSON Web Signature
JWT	JSON Web Token
OAM	Oracle Access Manager
OSSA	Oracle Software Security Assurance
SAML	Security Assertion Mark-up Language
SSO	Single Sign-On
SSL	Secure Sockets Layer

1

Securing the Oracle Banking Microservices Architecture Application

This topic describes about securing the Oracle Banking Microservices Architecture Application.

This topic contains the following subtopics:

- Desktop Security
  This topic describes about desktop security.
- Oracle Banking Microservices Architecture Controls
  This topic describes about Oracle Banking Microservices Architecture controls.

1.1 Desktop Security

This topic describes about desktop security.

Refer to the vendor specific relevant sections for securing the Desktops Operating system. Also refer to the Browser specific security settings mentioned in the vendor specific documents.

Refer the client browser setting required for Oracle Banking Microservices Architecture.

1.2 Oracle Banking Microservices Architecture Controls

This topic describes about Oracle Banking Microservices Architecture controls.

This topic contains the following subtopics:

- Overview
  This topic describes describe the various programs available within Oracle Banking Microservices Architecture, to help in the maintenance of security.
- Sign-on Messages
  This topic lists the sign-on messages and its explanations.
- Authentication and Authorization
  This topic describes about the authentication and authorization to have the access to the system.
- Role Based Access Controls
  This topic describes about role based access controls.
- Access Controls - Branch Level
  This topic describes about access controls at branch levels.
- Maker - Checker
  This topic describes about maker and checker.
- Access Enforcement
  This topic describes about access enforcement.

- Password Management
  This topic describes about password management.

1.2.1 Overview

This topic describes describe the various programs available within Oracle Banking Microservices Architecture, to help in the maintenance of security.

Access to the system is possible only if the user logs in with a valid ID and the *correct* password. The activities of the users can be reviewed by the Security Officer in the Event Log and the Violation Log reports

1.2.2 Sign-on Messages

This topic lists the sign-on messages and its explanations.

Table 1-1 Sign on Messages

Message	Explanation
User Authentication Failed/ Invalid Login	An incorrect **user ID** or **password** was entered.
User Status is Locked. Please contact your System Administrator	The user profile has been disabled due to an excessive number of attempts to login, using an incorrect **User ID** or **Password**. The number of attempts could have matched either the successive or cumulative number of login failures (configured for the system).

1.2.3 Authentication and Authorization

This topic describes about the authentication and authorization to have the access to the system.

Only authenticated users can access the system.

A user must have access rights to execute a function. The user profile of a user contains the User ID and the functions to which the user has access. Oracle Banking Microservices Architecture operation such as new, copy, query, unlock, and so on are enabled based on function rights available for the user. The function rights are checked for each operation performed by the user in Security Management Service module of Oracle Banking Microservices Architecture.

1.2.4 Role Based Access Controls

This topic describes about role based access controls.

- Application level access has implemented via the Security Management System module.
- Security Management System supports ROLE BASED access of Screens and different types of operations.
- Oracle Banking Liquidity Management supports dual control methodology, in which another user must be authorized with the requisite rights for each operation performed.

- Security Management System provides an option to map multiple roles for a user in a given branch. Allowed operations are mapped to the roles and Security Management System authorizes the user based on it.

1.2.5 Access Controls - Branch Level

This topic describes about access controls at branch levels.

Security Management System provides the branch level access through the roles provided for the user at a particular branch.

1.2.6 Maker - Checker

This topic describes about maker and checker.

The application supports dual control methodology, in which another user must have the necessary rights for each operation performed.

1.2.7 Access Enforcement

This topic describes about access enforcement.

Access management in Oracle Banking Microservices Architecture can be done in two steps.

- **Branch level:** The user cannot view even the menu list of the Oracle Banking Microservices Architecture when the user tries to login into the restricted branch. Thus, no transactions could be performed.
- **Roles wise:** Based on the user-roles mapping, the user can access different functions of Oracle Banking Microservices Architecture. For example, a bank clerk has access to customer creation, account opening, term-deposits opening, and liquidation screens, but does not have access to User Creation function activity.

1.2.8 Password Management

This topic describes about password management.

The Oracle Banking Microservices Architecture application relies on external password management and does not store any credentials. The password management and policy rules can be set on OCI IAM.

Certain user password related parameters are defined at OCI level. These parameters will apply to all the users of the system. Examples of such parameters are the number of invalid login attempts after which a user ID should be disabled, the maximum and minimum length for a password, the number of previous passwords that should not be used, the interval at which the password should be changed by every user, etc.

Password Policies

Password validation criteria are configurable for your identity domain in the Identity Cloud Service console. The passport policies are also customized to meet the business and security requirements of the customer.

> **Note:**
>
> Refer **Managing Password Policies** topic in **Oracle Cloud Infrastructure** documentation for the detailed explanation.

2 General Information

Cryptography

Oracle Banking Microservices Architecture uses cryptography to protect the sensitive data. For encryption, AES is used which is considered the gold standard. It produces a key size of 256 bits when it comes to symmetric key encryption.

Oracle Software Security Assurance - Standards

Every acquired organization must complete the Mergers and Acquisitions (M&A) Security Integration process. The issues identified during this review must be addressed according to the agreed upon M&A remediation plan. The acquired organization must complete SPOC assignments and plan integration of OSSA methodologies and processes into its SDLC.

Index