# Security Guide
# Oracle Banking Electronic Data Exchange for Corporates
# Release 14.5.3.0.0

Part No. F50162-01

November 2021

ORACLE

Security Guide

November 2021

Oracle Financial Services Software Limited

Oracle Park

Off Western Express Highway

Goregaon (East)

Mumbai, Maharashtra 400 063

India

Worldwide Inquiries:

Phone: +91 22 6718 3000

Fax:+91 22 6718 3001

www.oracle.com/financialservices/

# Table of Contents

# 1. Preface

## 1.1 Intended Audience

This document is intended for the following audience:

- Customers
- Partners

## 1.2 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.

## 1.3 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.

## 1.4 Structure

This manual is organized into the following categories:

Preface gives information on the intended audience. It also describes the overall structure of the User Manual.

The subsequent chapters describes following details:

- Introduction
- Preferences & Database
- Configuration / Installation.

## 1.5 Related Information Sources

For more information on Oracle Banking Electronic Data Exchange for Corporates Release 14.5.3.0.0, refer to the following documents:

- Oracle Banking Electronic Data Exchange for Corporates Installation Manuals

# 2. About This Manual

## 2.1 Introduction

**Purpose:**

This document provides security-related usage and configuration recommendations for Oracle Banking Electronic Data Exchange for Corporates. This guide may outline procedures required to implement or secure certain features, but it is also not a general-purpose configuration manual.

**Audience:**

This guide is primarily intended for IT department or administrators deploying Oracle Banking Electronic Data Exchange for Corporates and third party or vendor software's. Some information may be relevant to IT decision makers and users of the application are included. Readers are assumed to possess basic operating system, network, and system administration skills with awareness of vendor/third-party software's and knowledge of Oracle Banking Electronic Data Exchange for Corporates application.

## 2.2 Scope

### 2.2.1 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.

### 2.2.2 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.

### 2.2.3 Limitations

This 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.

### 2.2.4 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.

# 3. Prerequisite

## 3.1 Operating Environment Security

Please refer the vendor specific documentation for making the environment more safe and secured.

## 3.2 Network Security

Please refer the vendor specific documentation for making the environment more safe and secured.

## 3.3 Oracle Database Security

Please refer the Oracle Database Security specification document for making the environment more safe and secured.

### 3.3.1 Oracle Banking Electronic Data Exchange for Corporates Recommended configuration

This section contains security recommendations for the Database used for Oracle Banking Electronic Data Exchange for Corporates.

| | | |
|---|---|---|
| Init.ora | REMOTE_OS_AUTHENT=FALSE | Authentication |
| Init.ora | _TRACE_FILES_PUBLIC=FALSE | Authorization |
| Init.ora | REMOTE_OS_ROLES=FALSE | Authorization |
| Init.ora | O7_DICTIONARY_ACCESSIBILITY = FALSE | Authorization |
| Init.ora | AUDIT_TRAIL = OS | Audit |
| Init.ora | AUDIT_FILE_DEST = E:\logs\db\audit | Audit |
| To audit sessions | SQL> audit session; | Audit |
| To audit schema changes | SQL> audit user; | Audit |

| | | |
|---|---|---|
| To audit other events | SQL> AUDIT DATABASE LINK; -- Audit create or drop database links<br>SQL> AUDIT PUBLIC DATABASE LINK; -- Audit create or drop public database links<br>SQL> AUDIT SYSTEM AUDIT; -- Audit statements themselves<br>SQL> AUDIT ALTER ANY ROLE by ACCESS; -- Audit alter any role statements<br>SQL> AUDIT ALTER DATABASE by ACCESS; -- Audit alter database statements<br>SQL> AUDIT ALTER SYSTEM by ACCESS; -- Audit alter system statements<br>SQL> AUDIT CREATE ROLE by ACCESS; -- Audit create role statements<br>SQL> AUDIT DROP ANY ROLE by ACCESS; -- Audit drop any role statements<br>SQL> AUDIT PROFILE by ACCESS; -- Audit changes to profiles<br>SQL> AUDIT PUBLIC SYNONYM by ACCESS; -- Audit public synonyms statements<br>SQL> AUDIT SYSDBA by ACCESS; -- Audit SYSDBA privileges<br>SQL> AUDIT SYSOPER by ACCESS; -- Audit SYSOPER privileges<br>SQL> AUDIT SYSTEM GRANT by ACCESS; -- Audit System grant privileges | Audit |

To audit the events, login through sqlplus as SYSTEM and issue the commands.

## 3.4 Securing the Oracle Banking Electronic Data Exchange for Corporates Applications

The Oracle Banking Electronic Data Exchange for Corporates online web application uses JWT (JSON Web Tokens) to maintain the state for authenticated users.

JSON Web Tokens are an open, industry standard RFC 7519 method for representing claims securely between two parties. JSON Web Token (JWT) is a compact, URL-safe means of representing claims to be transferred between two parties. The claims in a JWT are encoded as a JSON object that is used as the payload of a JSON Web Signature (JWS) structure or as the plaintext of a JSON Web Encryption (JWE) structure, enabling the claims to be digitally signed.

- No Session to Manage (stateless): The JWT is a self-contained token which has authentication information, expire time information, and other user defined claims digitally signed.
- Portable: A single token can be used with multiple backend.
- No Cookies Required, So It's Very Mobile Friendly
- Good Performance: It reduces the network round trip time.
- Decoupled/Decentralized: The token can be generated anywhere. Authentication can happen on the resource server, or easily separated into its own server.

In addition, the following policies are followed for JWT,

- **Token Store:** To increase the security and better usability, every authentication/refresh request is secured by random unique key. The generated token and the secure key are persisted in the table, so that during the horizontal scaling of the servers, any API gateway instance can serve for the request.
- **Cipher strength:** Platform security module hashes the JWT footer with HS512 algorithm.
- **Refresh Token:** Users are allowed to get the new token any time before expiring the existing token.
- **Claims:** The JWT Claims Set represents a JSON object whose members are the claims conveyed by the JWT. Platform security module validates below claims during the process.

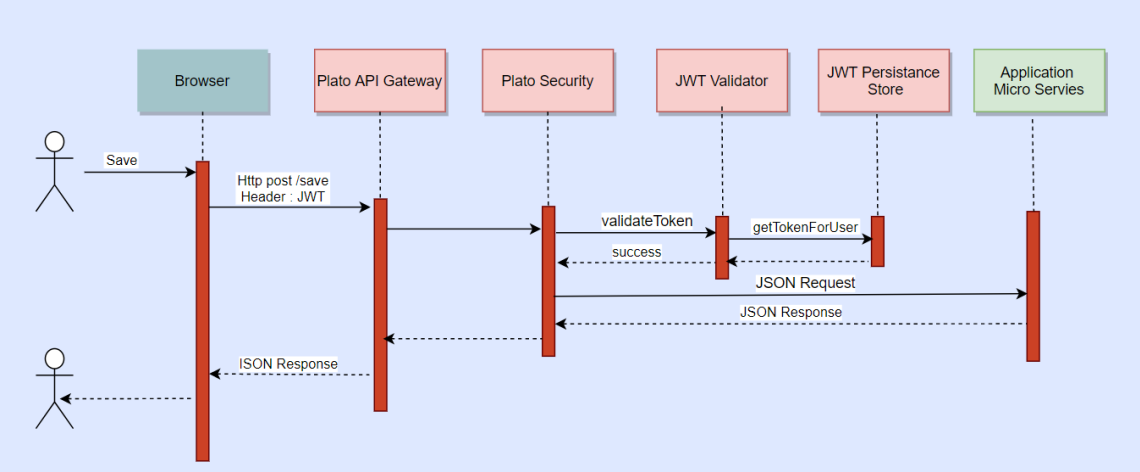
| Claim Name | Description | Mandatory | Type |
|---|---|---|---|
| iss | Issuer | Yes | Registered |
| sub | Subject | Yes | Registered |
| aud | Audience | No | Registered |
| exp | Expiration Time | Yes | Registered |
| nbf | Not Before | No | Registered |
| iat | Issued At | Yes | Registered |

| | | | |
|---|---|---|---|
| jti | JWT Id | Yes | Registered |
| tid | Tenant Id | Yes | Private |

- **Token Expiry:** Platform security module invalidates the token, if the client submits after the Expiration time. In addition, token becomes invalid, if the user password changed after the token issuance.
- **Logout:** While user calls the logout operation, platform security module clears the issued token and deletes the record from the table as well. The old token no longer will be used for any purpose.

The security flow for the online web application is depicted below

**JWT Authentication**




- The user is presented the standard login page for the OBEDXC application
- The user enters a user id and password. The credentials are validated against a JWT persistence store.
- If successful, the API Gateway generates a JWT token (Utilizing Oracle's Security Developer Toolkit part of Oracle's Platform Security Services), persists it in the Database and returns the same.
-

# 4. Securing Oracle Banking Electronic Data Exchange for Corporates

## 4.1 Oracle Banking Electronic Data Exchange for Corporates Controls

### 4.1.1 Overview

This chapter describes the various programs available within Oracle Banking Electronic Data Exchange for Corporates, 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 Security Officer, based on the Event Log and the Violation Log reports can review the activities of the users.

### 4.1.2 Disable Logging

It is recommended that the debug logging facility of the application be turned off, once the system is in production. This is achieved by updating the logback.xml file of the application.

### 4.1.3 Sign-on Messages

| Message | Explanation |
|---|---|
| User Authentication Failed | An incorrect user ID or password was entered. |

### 4.1.4 Authentication & Authorization

Only authorized users can access the system with the help of a unique User ID and a password. User should have access rights to execute a function. The user profile of a user contains the User ID, the password and the functions to which the user has access. Oracle Banking Electronic Data Exchange for Corporates operation such as new, copy, query, unlock etc. will be enabled based on function rights available for the user. The function rights will be checked for each operation performed by the user, in Security Management Service module of Oracle Banking Electronic Data Exchange for Corporates.

### 4.1.5 Role Based Access Controls

Application level access has implemented via the Security Management System (SMS) module.

SMS supports “ROLE BASED” access of Screens and different types of operations.

Oracle Banking Electronic Data Exchange for Corporates supports dual control methodology, wherein every operation performed has to be authorized by another user with the requisite rights.

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

### 4.1.6 Access controls - Branch level

SMS provides the branch level access through the roles provided for the user at a particular branch

### 4.1.7 Maker – Checker

Application supports dual control methodology, wherein every operation performed has to be authorized by another user with the requisite rights.

On these user- roles mapping the user will have access to different functions.

### 4.1.8 Access Enforcement

Access management in Oracle Banking Electronic Data Exchange for Corporates's Security Management Service, can be done in four steps.

1. Branch level— in such a case the user cannot view even the menu list of the Oracle Banking Electronic Data Exchange for Corporates when he tries to login into the restricted branch. Thus, no transactions could be performed
2. Roles wise—as described above basing on the user-roles mapping, the user can access different functions of Oracle Banking Electronic Data Exchange for Corporates. For an example, a credit officer will have access to initiating a Collateral or a Facility application, but he will not have access to User Creation function activity.

### 4.1.9 Password Management

The OBEDXC application stores credentials in Oracle database in encrypted format. For encrypting password, Bcrypt Hash Generator is used.

# 5. General Information

## 5.1 Oracle Database Security Suggestions

### Access Control

Database Vault (DV) Provides enterprises with protection from the insider threats and in advantage leakage of sensitive application data. Access to application data by users and administrators is controlled using DV realms, command rules and multi factor authorization. DV also address Access privilege by separating responsibilities.

### Data Protection

Advance Security provides the most advance encryption capabilities for protecting sensitive information without requiring any change to the application. TDE is native database solution that is completely transparent to the existing applications.

Advance Security also provides strong protection for data in transit by using network encryption capabilities. Features like Easy to deploy, Ensure secure by default to accept communication from client using encryption, Network encryption using SSL/TLS.

### Monitoring and Compliance

Audit Vault (AV) transparently collects and consolidate audit data from multiple databases across the enterprise, does provide valuable insight into who did what with which data & when including privilege users. The integrity of the audit data is ensured using controls including DV, Advance Security. Access to AV data is strictly controlled. It also does provide graphical summaries of activity causing alerts, in addition database audit setting are centrally managed and monitored.

## 5.2 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.

## 5.3 References

### 5.3.1 Datacenter Security considerations

Please refer to the following links to understand Datacenter Security considerations
http://docs.oracle.com/cd/B14099_19/core.1012/b13999/rectop.htm

### 5.3.2 Database Security considerations

Please refer the below links to understand more on Database Security considerations recommended to be followed
http://www.oracle.com/us/products/database/security/overview/index.html
http://www.oracle.com/technetwork/database/security/twp-security-checklist-database-1-132870.pdf

### 5.3.3 Security recommendations / practices followed for Database Environment

Please refer the below mentioned links to understand more on Security recommendations / practices followed for Database Environment
http://docs.oracle.com/cd/B28359_01/network.111/b28531/guidelines.htm

### 5.3.4 Common security considerations

Please refer below links to understand some of the common security considerations to be followed

http://docs.oracle.com/cd/B14099_19/core.1012/b28654.pdf

http://docs.oracle.com/cd/E14899_01/doc.9102/e14761/tuningforappserver.htm
http://docs.oracle.com/cd/E13222_01/wls/docs81b/lockdown/practices.html
http://docs.oracle.com/cd/E23943_01/web.1111/e14529/security.htm
http://www.oracle.com/us/solutions/oos/weblogic-server/overview/index.html

**Home**