Oracle Banking Digital Experience

Security Guide
Release 16.1.0.0.0

Part No. E71761-01

March 2016

ORACLE®

Security Guide

March 2016

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

This document provides a comprehensive overview of security for Oracle Banking Digital Experience. It includes conceptual information about security principles, descriptions of the product's security features, and procedural information that explains how to use those features to secure Oracle Banking Digital Experience.

This preface contains the following topics:

- Audience
- Documentation Accessibility
- Organization of the Guide
- Related Documents
- Conventions

1.1 Audience

The Oracle Security Guide is intended for Bank IT Staff responsible for application installation and security configuration.

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 your hearing is impaired.

1.4 Organization of the Guide

This document contains:

Chapter 1, "Overview"

This chapter presents an overview of Oracle Banking Digital Experience and explains the general principles of application security.

Chapter 1, "Secure Installation and Configuration"

This chapter provides an overview of secure installation process through recommended deployment topologies and describes the installation and configuration procedure for the infrastructure and product components of Oracle Banking Digital Experience.

Chapter 1, "Security Features"

This chapter outlines the specific security mechanisms offered by Oracle Banking Digital Experience.

Appendix A, "Appendix"

This appendix lists the Secure Deployment Checklist which includes guidelines that help secure Oracle Banking Digital Experience.

1.5 Related Documents

For more information, see the following documentation:

- Hardening Tips for Default Installation of Oracle Enterprise Linux 6 at https://docs.oracle.com/cd/E37670_01/E36387/E36387.pdf
- Oracle® Fusion Middleware Installation Guide for Oracle WebLogic Server at http://docs.oracle.com/cd/E17904_01/doc.1111/e14142/toc.htm
- Oracle® Fusion Middleware Application Security Guide - Configuring and Managing Auditing at

  http://docs.oracle.com/cd/E23943_01/core.1111/e10043/audpolicy.htm
- For installation and configuration information, see the Oracle Banking Digital Experience Installation Guide
- For the complete list of Oracle Banking licensed products and the Third Party licenses included with the license, see the Oracle Banking Licensing Guide

1.6 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.

2 Overview

This chapter presents an overview of Oracle Banking Digital Experience and explains the general principles of application security.

2.1 Product Overview

Oracle Banking Digital Experience delivers the capabilities that banks require to execute their unique digital strategies to enhance customer engagement and experience.

It provides more than 250 business services out of the box, including digital account and loan origination, digital wallets and mobile payments.

2.2 General Security Principles

The following principles are fundamental for using any application securely.

2.3 Restrict Network Access to Critical Services

Keep both the Oracle Banking Digital Experience middle-tier and the database behind a firewall. In addition, place a firewall between the middle-tier and the database. The firewalls provide assurance that access to these systems is restricted to a known network route, which can be monitored and restricted, if necessary. As an alternative, a firewall router substitutes for multiple, independent firewalls.

If firewalls cannot be used, be certain to configure the TNS Listener Valid Node Checking feature which restricts access based upon IP address. Restricting database access by IP address often causes application client or server programs to fail for DHCP clients. To resolve this, consider using static IP addresses, a software or a hardware VPN or Windows Terminal Services or its equivalent.

2.4 Follow the Principle of Least Privilege

The principle of least privilege states that users should be given the least amount of privilege to perform their jobs. User privileges should be reviewed periodically to determine relevance to current job responsibilities.

2.5 Monitor System Activity

System security stands on three legs:

- Good security protocols
- Proper system configuration
- System monitoring

System needs to be constantly monitored from Oracle Enterprise Manager.

2.6 Keep Up To Date on Latest Security Information

Oracle continually improves its software and documentation.

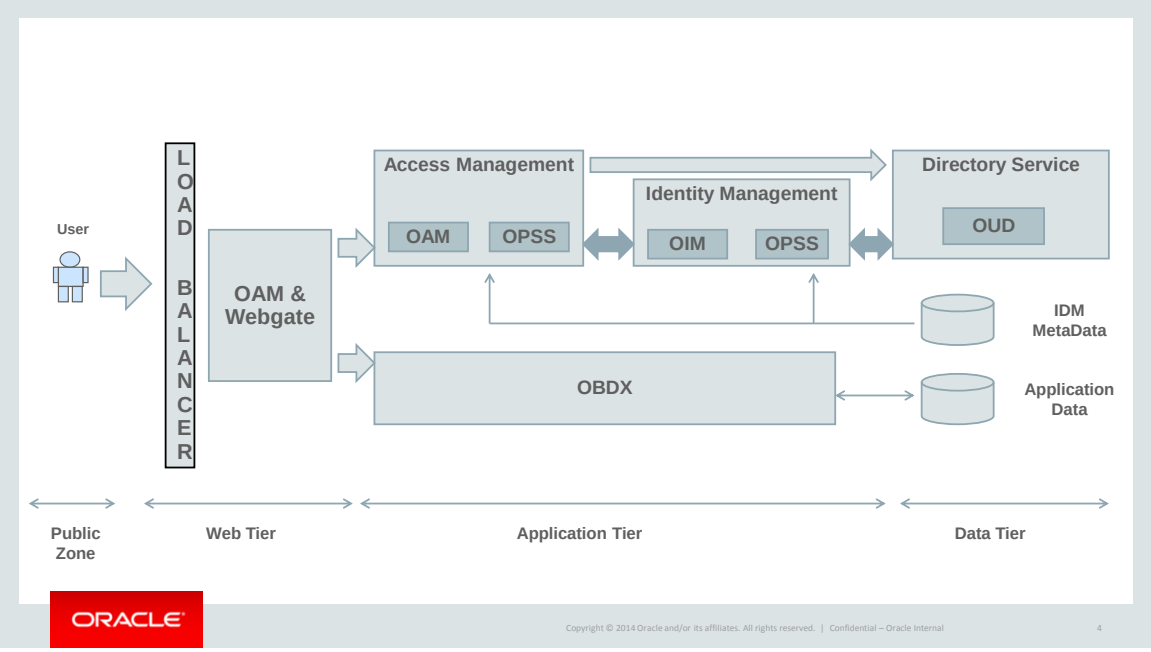
3 Secure Installation and Configuration

This chapter provides an overview of the architecture of the deployment and describes the installation and configuration procedure for the infrastructure and product components of Oracle Banking Digital Experience.

3.1 Architecture Diagram

This section describes the architecture with different components for Oracle Banking Digital Experience:

Figure 1–1Simplified Architecture View



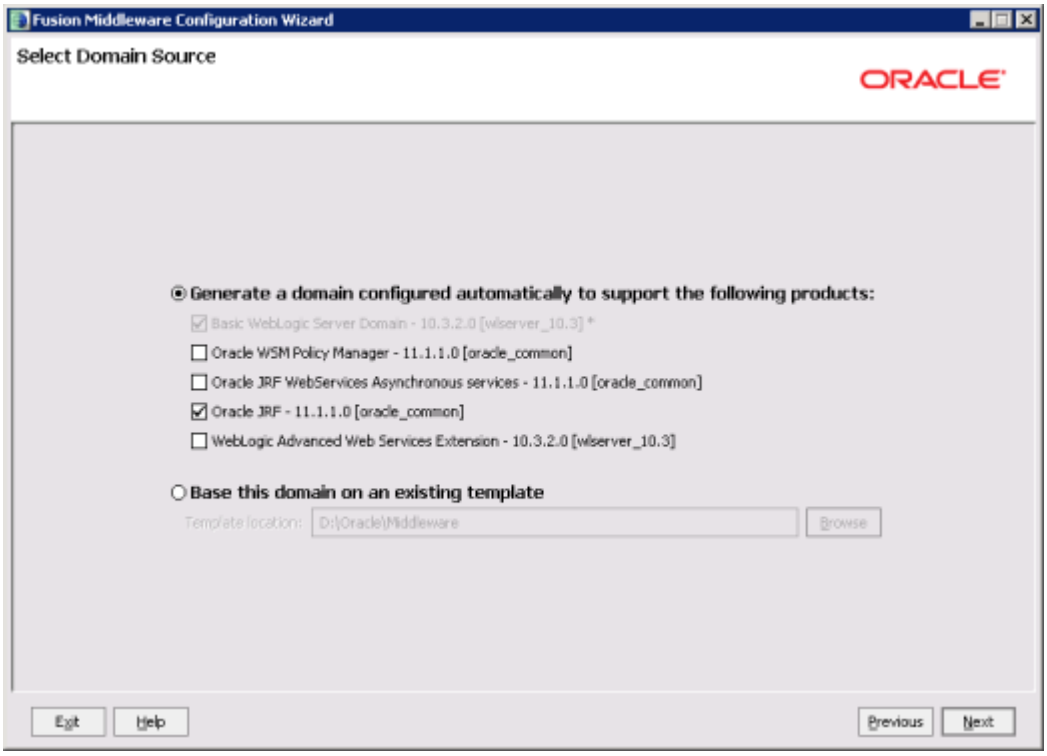
3.2 Installing WebLogic

Installation of WebLogic Server is done using the documentation as mentioned in the installation guide Oracle® Fusion Middleware Installation Guide for Oracle WebLogic Server at https://docs.oracle.com/cd/E24329_01/doc.1211/e24492/toc.htm.

Following options need to be selected during the installation process:

1. Select the option **Generate a domain configured automatically to support the following products:**
2. Under the above option, select the check box against **Oracle JRF - 11.1.1.0 [oracle_common]**.

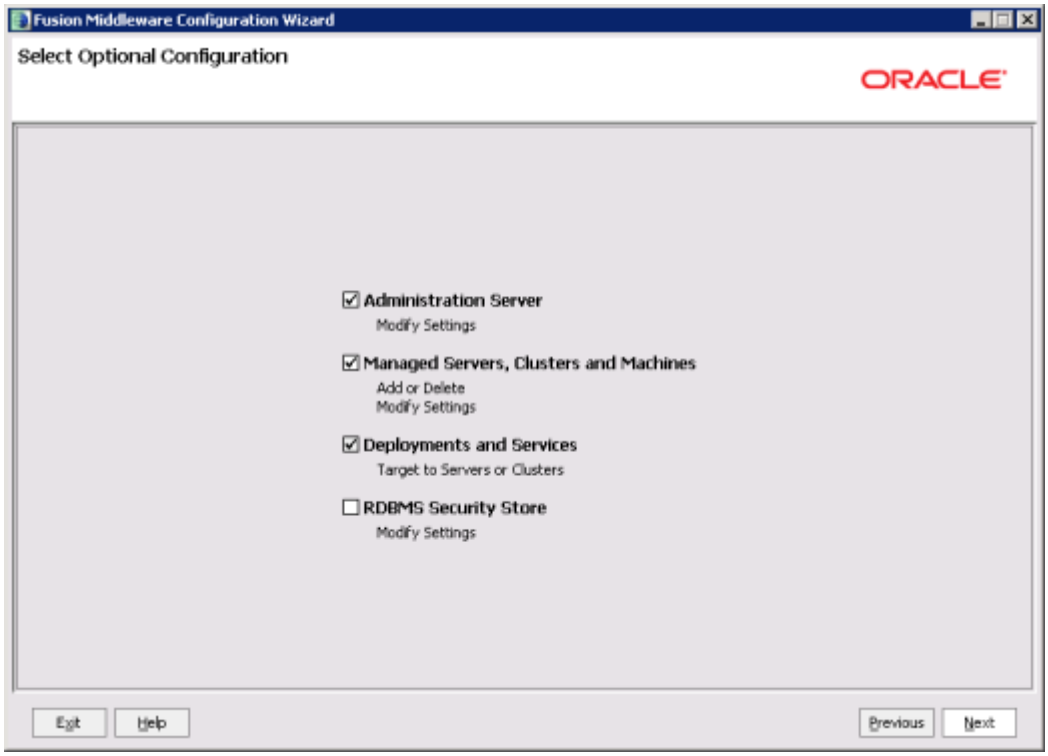
Figure 1–3 Select Domain Source



3. Click **Next**.
4. Select the check box against the following options:

- Administration Server
- Managed Servers, Clusters and Machines
- Deployments and Services

Figure 1–4 Select Optional Configuration



3.3 Installing Oracle Banking Digital Experience

The detailed installation steps are present in the Oracle Banking Digital Experience Installation Guide.

3.4 Configuring SSL

One way SSL between the presentation and application WebLogic server is supported. The detailed configuration is explained below:

Note: Procure an external CA signed certificate before proceeding further. Follow the instructions below to install the certificate once the certificate is available

---

Step 1 Import the Certificate into a Java Trust Keystore

Execute the following command:

```
keytool -import -trustcacerts -alias sampletrustself -keystore SampleTrust.jks -file SampleSelfCA.cer.der -keyalg RSA
```

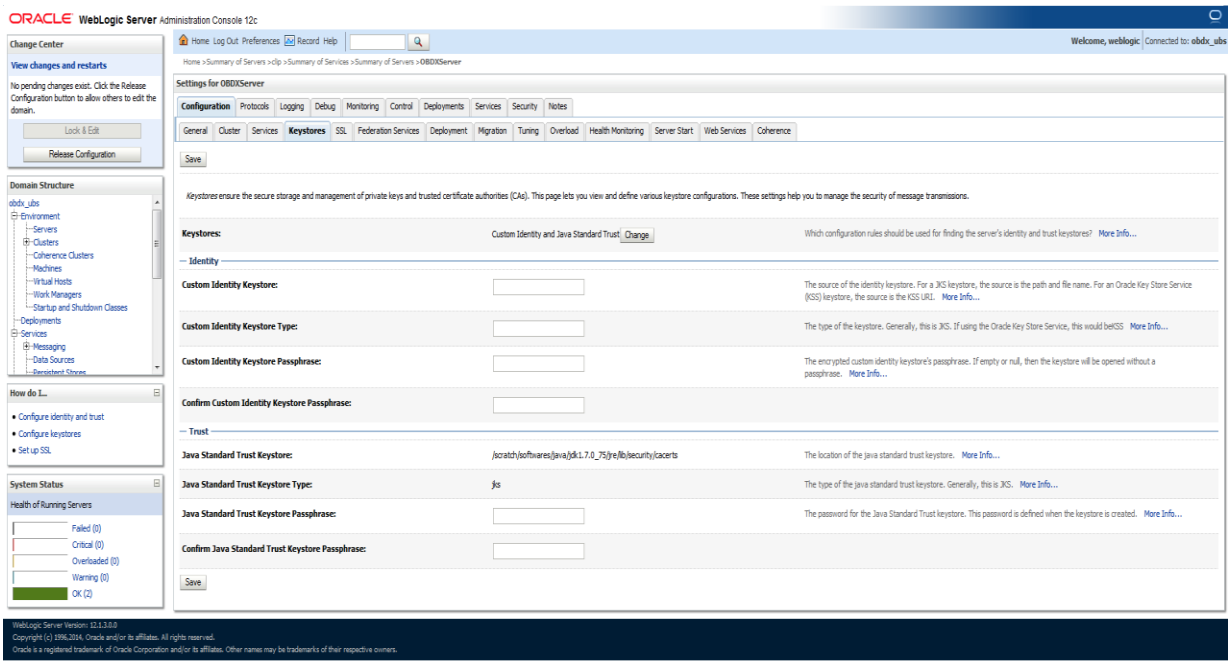
```
keytool -import -alias `hostname -f` -file `hostname -f`.cer -keystore <JAVA_HOME>/jre/lib/security/cacerts -storepass changeit -noprompt
```

Step 2 Configure Application Domain's WebLogic with Custom Identity and Trust Keystores

To configure the application domain's WebLogic:

1. Open WebLogic admin console and navigate to *Home --> Summary of Servers --> AdminServer*. Click the **Keystores** tab.

Figure 1–5 Keystores



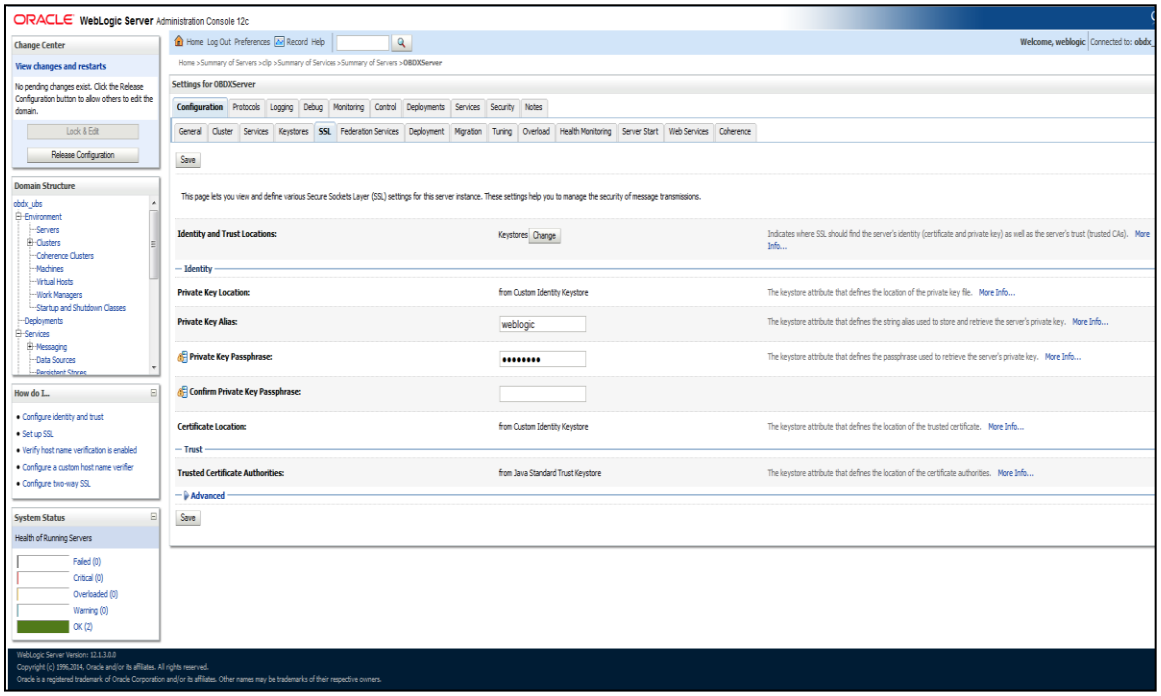
2. Click the **Change** button.
3. Select **Custom Identity and Java Standard Trust** option from the list.
4. Click the **Save** button.
5. Enter the following details in the **Identity** and **Trust** sections:

Table 1–1 Keystore Configuration

Field	Value
Identity	
Custom Identity Keystore	Absolute path of `hostname -f`_identity.jck file
Custom Identity Keystore Type	JCKES
Custom Identity Keystore Passphrase	***
Confirm Custom Identity Keystore Passphrase	***

6. Enter the passphrases that were used while creating Identity Keystore and certificate.
7. Click the **Save** button.
8. Click the **SSL** Tab.

Figure 1–9SSL



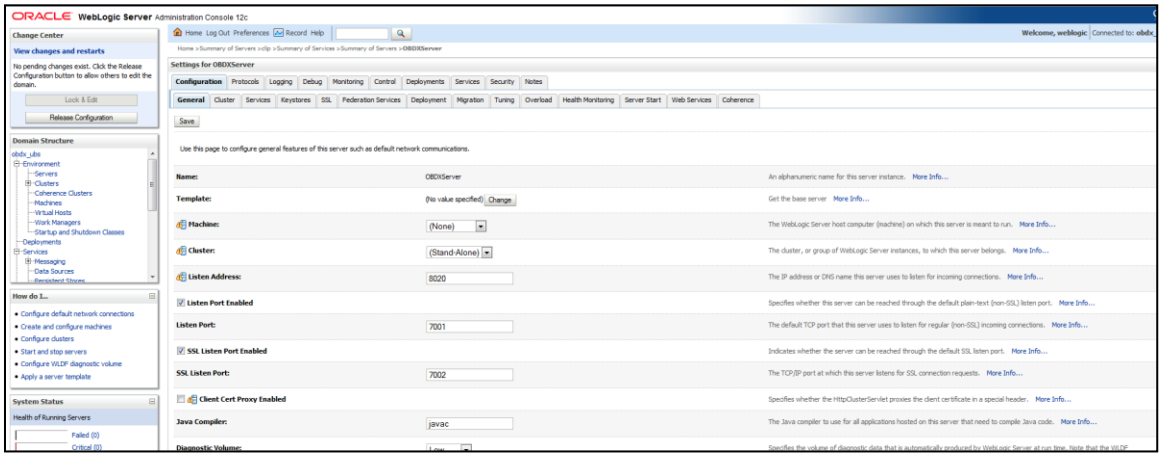
9. Enter the following details in the **Identity** section:

Table 1–2SSL Configuration

Field	Value
Private Key Alias	`hostname -f`
Private Key Passphrase	***
Confirm Private Key Passphrase	***

10. Enter the passphrases that were used while creating the certificate.
11. Click the **Save** button.
12. Click the **Advanced** link. Ensure that **Two Way Client Cert Behavior** is set to **Client Certs Not Requested**.
13. Click the **General** tab.
    Select the **SSL Listen Port Enabled** check box.

Figure 1–12 General



14. Click the **Save** button.

By default, SSLv3 should be disabled.

Steps to disable SSLv3 protocol on Weblogic:

1. The weblogic.security.SSL.protocolVersion command-line argument lets you specify which protocol is used for SSL connections.

2. After enabling/configuring the SSL for weblogic server, append the following option to the JAVA_OPTIONS variable

Dweblogic.security.SSL.protocolVersion=TLS1

Note: If you don't specify the above property, by default it takes SSLv3.

3.5 Post Installation Configuration

The security practices that should always be followed are listed below:

- Set the proper permissions for users accessing databases. You could also implement roles to manage privileges. Check whether permissions are correctly set in operating system. If these are not correctly set, there may be a security loophole.

3.6 HTTP Security

Add the following line to the httpd.conf file of your web server.

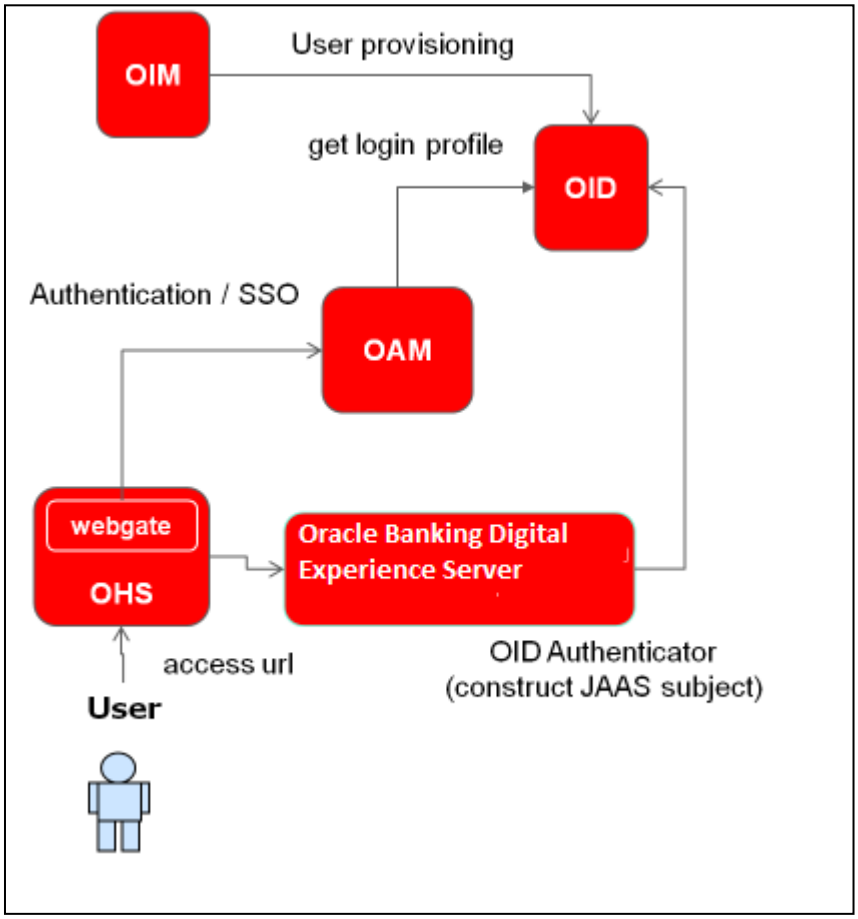
```
Header always append X-Frame-Options SAMEORIGIN
```

4 Security Configurations

4.1 Configuring and Using Authentication

Oracle Banking Digital Experience uses OAM to authenticate users.

Figure 1–3 Authentication and Single Sign On



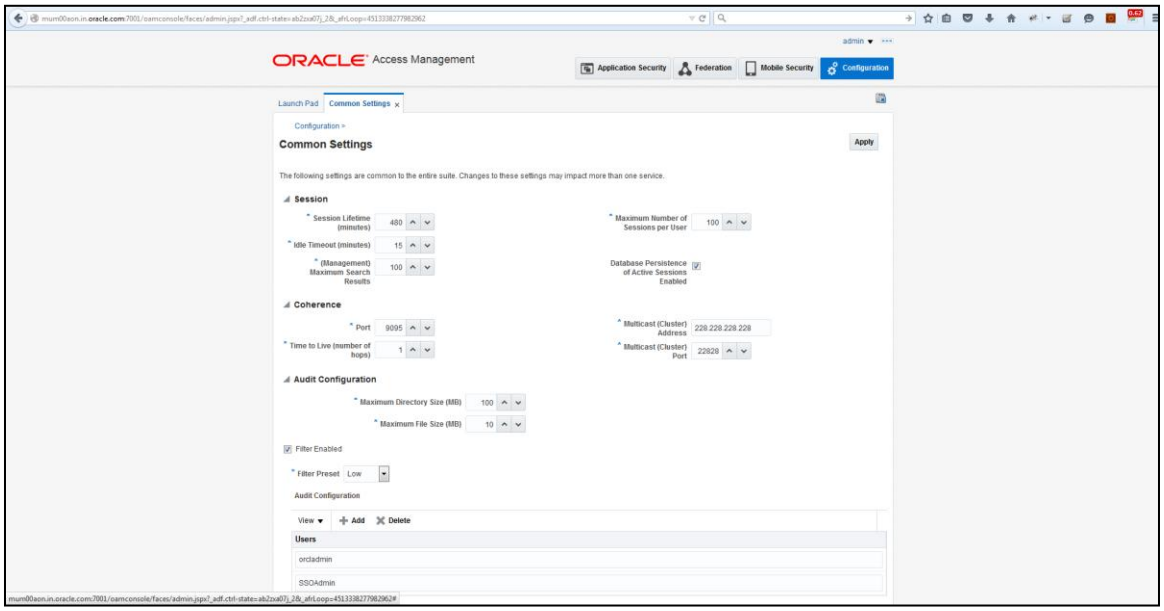
Data flow is as follows:

- OAM gets login profile from OID.
- OAM intercepts access call to Oracle Banking Digital Experience and authenticates user.
- OAM ensures single sign-on across participating applications (configurable).
- SSO across various enterprise applications for internal users.

1.1.2 SessionTimeouts

You can set the idle session timeout and the active session timeout from the OAM Console

Figure 1–4 OAM Console



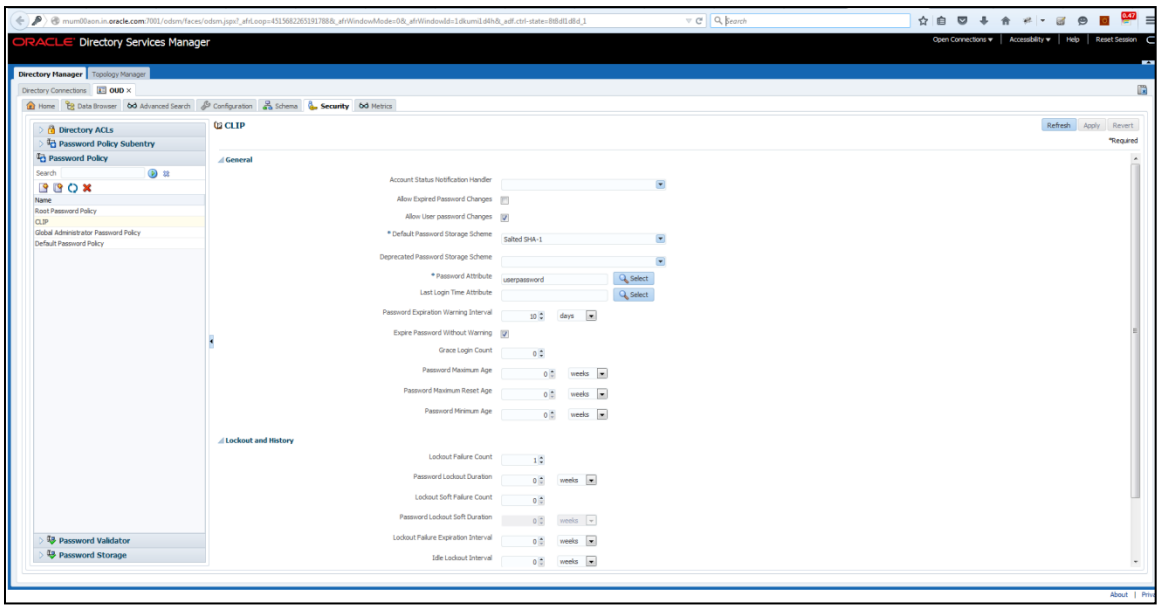
1. Log into http://<OAM_HOST>:<OAM_PORT>/oamconsole
2. Go to Settings >> View >> Common Settings.
3. You will reach the screen shown in Figure 1-4.
4. ***Session Lifetime*** is the active session timeout in minutes.
   We recommend that this value should not be more than 15 minutes.

Idle Timeout is the idle session timeout in minutes.
We recommend that this value should not be more than 5 minutes.

1.1.3 Password Policy

You can set the password policy from the OUD management tool called the Oracle Directory Services Manager (ODSM).

Figure 1–5 Password Policy in ODSM



1. Login into ODSM >> Security Tab >> Password Policy
2. You can add a password policy here, or edit an existing one.
3. As is visible from Figure 1-5, you can set the hashing algorithm, password expiry and user lockout configurations.
4. We recommend that you set the password storage scheme as `Salted SHA-512`

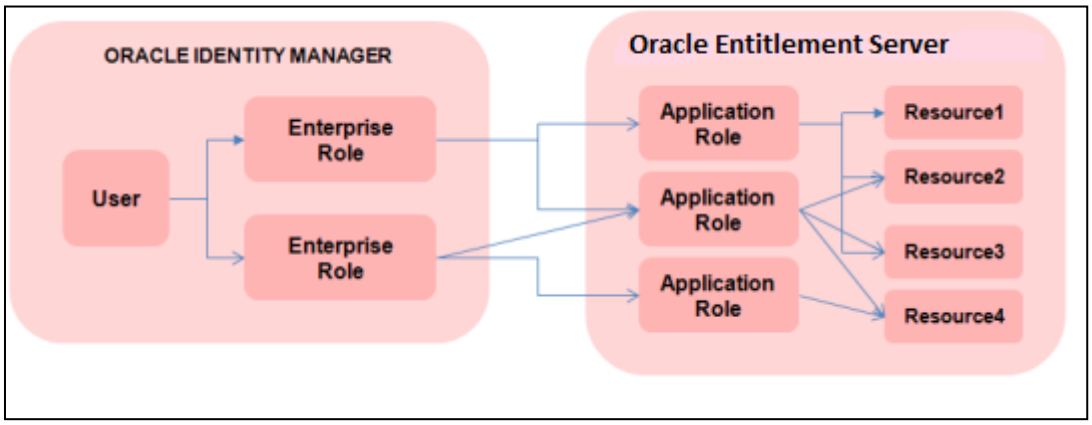
4.2 Configuring and Using Access Control

Authorization includes primarily two processes:

- Permitting only certain users to access, process, or alter transactions
- Applying varying limitations on user access or actions. The limitations placed on (or removed from) users can apply to transactions

Oracle Banking Digital Experience uses Oracle Entitlement Server for authorization.

Figure 1–6 Oracle Entitlement Server - Users / Roles / Services



The features are:

- User belongs to the enterprise.
- Users mapped to enterprise roles (used organization-wide)
- Enterprise roles mapped to application roles (application roles used within the application)
- Access policies defined for services defined on application roles.

4.3 Configuring and Using Security Audit

Oracle Banking Digital Experience relies on the Oracle Fusion Middleware Audit Framework for security audits.

The configuration and usage is explained in detail in the document Oracle® Fusion Middleware Application Security Guide - Configuring and Managing Auditing at http://docs.oracle.com/cd/E23943_01/core.1111/e10043/audpolicy.htm.

4.4 Configuring and Using TDE

Oracle Banking Digital Experience relies on Oracle® Database Advanced Security for encrypting sensitive data.

The configuration is explained in detail in Oracle® Database Advanced Security Administrator's Guide.

OBDX supports both TDE Tablespace Encryption as well as TDE Column Encryption.

5 Appendix

This appendix lists the Secure Deployment Checklist which includes guidelines that help secure Oracle Banking Digital Experience.

Secure Deployment Checklist

The following security checklist includes guidelines that help secure your installation:

1. Install only what is required.
2. Lock and expire default user accounts.
3. Enforce password management.
4. Practice the principle of least privilege.
5. Grant necessary privileges only.
    a. Revoke unnecessary privileges from the PUBLIC user group.
    b. Restrict permissions on run-time facilities.
6. Enforce access controls effectively and authenticate clients stringently.
7. Restrict network access.
    a. Use a firewall.
    b. Never poke a hole through a firewall.
    c. Monitor who accesses your systems.
    d. Check network IP addresses.
    e. Encrypt network traffic.
    f. Harden the operating system.
8. Apply all security patches and workarounds.
9. Contact Oracle Security Products if you come across vulnerability in Oracle Database.