# Table of Contents

1. Preface .......................................................................................................................... 4  
   1.1 Intended Audience ..................................................................................................... 4  
   1.2 Documentation Accessibility .................................................................................... 4  
   1.3 Access to OFSS Support ........................................................................................... 4  
   1.4 Structure ................................................................................................................... 4  
   1.5 Related Information Sources ..................................................................................... 4  
2. Pre-requisite .................................................................................................................... 5  
3. UI deployment .................................................................................................................. 6  
4. Configuration to run UI on Oracle HTTP Server ............................................................ 8  
   4.1 Authentication Configuration: .................................................................................... 10  
      4.1.1 Configuring the OAM Authentication .................................................................. 10  
      4.1.2 Configuring the Non OAM Authentication ....................................................... 10  
   4.2 Other Configurations ............................................................................................... 11  
5. Oracle HTTP Server Commands ..................................................................................... 13  
   5.1 Starting Oracle HTTP Server Instances from the Command Line ........................... 13  
   5.2 Stopping Oracle HTTP Server Instances from the Command Line ........................ 13
1. **Preface**

1.1 **Intended Audience**

This document is intended for the following audience:

- Customers
- Partners

1.2 **Documentation Accessibility**


1.3 **Access to OFSS Support**

Oracle customers have access to electronic support through My Oracle Support. For information, visit


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:

- Prerequisite
- UI Deployment
- Configuration / Installation

1.5 **Related Information Sources**

For more information on Oracle Banking APIs Release 19.1.0.0.0, refer to the following documents:

- Oracle Banking APIs Licensing Guide
- Oracle Banking APIs Security Guide
2. **Pre-requisite**

OHS software along with instance should be available for use.

For further detailed configuration of Oracle HTTP Server, please refer to https://docs.oracle.com/middleware/12213/webtier/administer-ohs/toc.htm.
3. **UI deployment**

Below steps needs to be performed for UI deployment on OHS server.

Copy the `obapi.conf` from `OBAPI_Installer/installables/ui/config` directory into the instance config directory (where `httpd.conf` is present). `httpd.conf` file is present at `{DOMAIN_HOME}/config/fmwconfig/components/OHS/instances/{componentName}`

- Create a directory where `obapi` UI files would be deployed on OHS server.
• Copy all files / directories from OBAPI_Installer/installables/ui/deploy into newly created directory.
4. **Configuration to run UI on Oracle HTTP Server**

Make sure following OHS modules must be loaded

- mod_rewrite.so
- mod_deflate.so
- mod_expires.so
- mod_mime.so
- mod_headers.so

Following are the changes needed to be done in the obapi.conf file and place this file in same folder where httpd.conf file exists.

1. Replace the `<CHANNEL_PATH>` (all occurrences) with the newly created directory (from previous UI deployment step).

2. Configuration for Content Security Policy, refer to the below document
   Oracle Banking APIs Security Guide

Include the obapi.conf into httpd.conf using below configuration

```conf
include "obapi.conf" (needs to be added in httpd.conf)
```

Read obapi.conf for inline documentation.
Following are the changes need to be done in mod_wl_ohs.conf which is present at
{DOMAIN_HOME}/config/fmwconfig/components/OHS/instances/{componentName}

Copy below configuration into mod_wl_ohs.conf

```xml
<IfModule weblogic_module>
  WebLogicHost HOSTNAME
  WebLogicPort MANAGE_SERVER_PORT
  Debug ON
  WLLogFile DIR/FILENAME
  MatchExpression /digx/*
  MatchExpression /digx-auth/*
  MatchExpression /digx-social/*
</IfModule>
```

Configure below properties

a. HOSTNAME – Weblogic server hostname (where OBAPI weblogic domain is configured)

b. MANAGE_SERVER_PORT – Weblogic manage server port (where OBAPI application is deployed)

c. DIR / FILENAME – Path where log file should be generated

Sample configuration (for reference purpose only)

```xml
<IfModule weblogic_module>
  WebLogicHost wls_server1
  WebLogicPort 7003
  Debug ON
  WLLogFile /tmp/weblogic_obp.log
  MatchExpression /digx/*
</IfModule>
```
4.1 Authentication Configuration:

OBAPI product ships with two type of authentication methods:

1. OAM Authentication
2. Non OAM Authentication

4.1.1 Configuring the OAM Authentication

By default OAM server URL is set as `http://mum00aon.in.oracle.com:14100/oam/server`.

Replace it to your OAM server URL in the following files:

1. `<CHANNEL_PATH>/components/login/login-form-web.js`
2. `<CHANNEL_PATH>/framework/js/constants/constants.js`
   a. Set the `authenticator` property as “OUD”.

4.1.2 Configuring the Non OAM Authentication

Configuring Non OAM Authentication implementer needs to change following files:

1. `<CHANNEL_PATH>/framework/js/constants/constants.js`
   a. Set the `authenticator` property as “OBAPIAuthenticator”.

---

**Note:** This is a read-only file; do not modify this file unless changes are made at the base virtual root level.
i. In \{DOMAIN_HOME\}/config/fmwconfig/components/OHS/instances/{componentName}/httpd.conf remove webgate.conf entry

4.2 Other Configurations

Google Map Configuration:
By default Google map SDK URL is set as
https://maps.googleapis.com/maps/api/js?key=AIzaSyCYFGuo6wj7CTEaBILF3qaRcJWuYI53f8&libraries=geometry,places
Replace it with your Google map SDK URL in the following files:
- <CHANNEL_PATH>/components/inputs/map.js
- <CHANNEL_PATH>/components/location-maintenance/location-add.js
- <CHANNEL_PATH>/components/location-maintenance/location-update.js
- <CHANNEL_PATH>/components/atm-branch-locator/locator.js

Social Media Configurations:
By default Linkedin and Facebook API key is set as
Linkedin Key: 86hg2yshsq76yd
Facebook Key: 233137313819556
Replace it to your social media API keys in the following files:
- <CHANNEL_PATH>/components/social-media/facebook.js
Wallet Configurations:
By default OBAPI Base server URL is set as http://mum00apu.in.oracle.com:7777/digx/v1/

Replace it to your OBAPI Base server URL in the following files:
- <CHANNEL_PATH>/components/wallet-external/addfund.js
- <CHANNEL_PATH>/components/wallet/add_paymentMode.js

Since OBAPI UI support subresource integrity and changing files mentioned above will impact it and files which are changed won’t work. SHA hash for all files are maintained in <CHANNEL_PATH>/framework/js/pages/security.js. There are two ways for solving this problem:
  - Remove the SHA hash of the changed files along with the file name in security.js
  - Generate SHA hash of modified files and update it in the security.js

Once all above steps are completed, restart the OHS server.
For the restarting of the OHS Server first go to the bin directory of the OHS instance.

Mandate SSL Configurations:
Configuring SSL as mandatory option, Implementer have to set the value ssl.status in <CHANNEL_PATH>/framework/js/constants/constants.js. If its value set as disabled application can work in both secure and unsecure connection but if its value is enabled application works only in secure connection.
5. **Oracle HTTP Server Commands**

5.1 **Starting Oracle HTTP Server Instances from the Command Line**

You can start up Oracle HTTP Server instances from the command line via a script.

1. Ensure that Node Manager is running.
2. Enter the following command:

   **Linux or UNIX:** $DOMAIN_HOME/bin/startComponent.sh componentName

   **Windows:** %DOMAIN_HOME%\bin\startComponent.cmd componentName

   For example:

   $DOMAIN_HOME/bin/startComponent.sh ohs1

   The startComponent script contacts the Node Manager and runs the nmStart() command.

   When prompted, enter your Node Manager password. The system responds with these messages:

   Successfully started server componentName...

   Successfully disconnected from Node Manager...

   Exiting WebLogic Scripting Tool.

5.2 **Stopping Oracle HTTP Server Instances from the Command Line**

You can stop Oracle HTTP Server instances from the command line via a script.

Enter the following command:

   **Linux or UNIX:** $DOMAIN_HOME/bin/stopComponent.sh componentName

   **Windows:** %DOMAIN_HOME%\bin\stopComponent.cmd componentName

   For example:

   $DOMAIN_HOME/bin/stopComponent.sh ohs1

   This command invokes WLST and executes the nmKill() command.

   The stopComponent command will not function if the Node Manager is not running.

   For more commands refer the following URL:

   https://docs.oracle.com/middleware/1221/webtier/administer-ohs/getstart.htm