Oracle Banking APIs
Web Service Username Token Configuration Guide
Release 19.1.0.0.0

Part No. F18559-01

May 2019
# 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. Anonymous User Configuration ........................................................................................................ 5

3. Logged-In User Configuration ........................................................................................................... 9
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 OFSS 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:
  - Prerequisite
  - UI Deployment
  - Configuration / Installation

1.5 Related Information Sources
For more information on Oracle Banking APIs Release 18.3.0.0.0, refer to the following documents:
- Oracle Banking APIs Licensing Guide
- Oracle Banking APIs Security Guide
2. **Anonymous User Configuration**

- Insert/Update security policy to be used in the field in *Anonymous Security Policy* at Day1 (defaulted to “oracle/wss_username_token_client_policy”)

- Insert/Update security policy key to be used in the field in *Anonymous Security Key* at Day1 (defaulted to “origination_owsm_key”)

- Name should match with credential key stored inside the credential store repository.

- Create a map named “oracle.wsm.security” in credential store provider.
- Create credential key and provide username & password which will be used for authentication and authorization at OBP.
3. Logged-In User Configuration

- Insert a credentials entry for the connector.

Insert into DIGX_FW_CONFIG_ALL_B (PROP_ID, CATEGORY_ID, PROP_VALUE, FACTORY_SHIPPED_FLAG, PROP_COMMENTS, SUMMARY_TEXT, CREATED_BY, CREATION_DATE, LAST_UPDATED_BY, LAST_UPDATED_DATE, OBJECT_STATUS, OBJECT_VERSION_NUMBER, EDITABLE, CATEGORY_DESCRIPTION) values ('OBP_RA_JNDIKEY', 'CredentialConnector', 'ra/DIGXConnectorOBP', 'N', 'RA Connector for OBP', 'RA Connector for OBP', 'ofssuser', sysdate, 'ofssuser', sysdate, 'Y', 1, 'N', '1');

- Update the connector name for the logged-in user.

update DIGX_FW_CONFIG_OUT_WS_CFG_B set HTTP_BASIC_AUTH_CONNECTOR='OBP' where SECURITY_POLICY='oracle/wss10_saml_token_client_policy';

- Update security policy of logged-in user from saml token to user token policy

update DIGX_FW_CONFIG_OUT_WS_CFG_B set SECURITY_POLICY='oracle/wss_username_token_client_policy' where SECURITY_POLICY='oracle/wss10_saml_token_client_policy';

- Create a new “Outbound Credentials Mapping” in the connector (com.ofss.digx.app.connector.ear) ear and create a default user (use user id and credentials as provided by OBP team) for the mapping in the security tab. Managed server restart is required after these changes.

- Login into Weblogic console.

- Click on Deployments.

- Expand by clicking ‘+’ icon present in front of com.ofss.digx.app.connector application as shown below.

- Click com.ofss.digx.connector.rar as shown below.

- Click On “configuration” tab as shown in figure.
• Click on “New” button and select connection factory. Refer Screenshot.

• Provide JINDI name as inserted in previous scripts. In this case name will be “ra/DIGXConnectorOBP”. After providing the name and Click on “Next”.
- Click on "Ok" to confirm.

- Click on Activate changes.
• Click on Security tab of connector, click on “Outbound credentials mapping”, click on “New” and select the newly created provider “ra/DIGXConnectorOBP” and click on “Next”.
- Select the default user and Click on “Next”.

- Provide the user details as provided by OBP Team and Click on Finish.
• Restart managed server to take effects.