Oracle Banking Digital Experience
Web Service Username Token Configuration Guide

Release 18.1.0.0.0

Part No. E92727-01

January 2018
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
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**


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 Digital Experience Release 18.1.0.0.0, refer to the following documents:

- Oracle Banking Digital Experience Licensing Guide
- Oracle Banking Digital Experience 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.
• JAXWSFactory reads the anonymous security policy and key name from `digx-fw_config_out_ws_cfg_b` table. It then matches this key name with credential store provider. If match is successful, username & password is read and anonymous user is replaced with this username and used further for authentication & authorization at OBP.