Credential Store Setup Guide
Oracle Banking Digital Experience
Patchset Release 22.2.6.0.0

Part No. F72987-01

April 2025

Connector Credential Store Guide
April 2025
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/

This software or hardware is developed for general use in a variety of information management applications. It is not developed or intended for use in any inherently dangerous applications, including applications that may create a risk of personal injury. If you use this software or hardware in dangerous applications, then you shall be responsible to take all appropriate failsafe, backup, redundancy, and other measures to ensure its safe use. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software or hardware in dangerous applications.

The information contained herein is subject to change without notice and is not warranted to be error-free. If you find any errors, please report them to us in writing.

This software or hardware and documentation may provide access to or information on content, products and services from third parties. Oracle Corporation and its affiliates are not responsible for and expressly disclaim all warranties of any kind with respect to third-party content, products, and services. Oracle Corporation and its affiliates will not be responsible for any loss, costs, or damages incurred due to your access to or use of third-party content, products, or services.

Table of Contents

1. Preface

1.1 Purpose

Welcome to the User Guide for Oracle Banking Digital Experience. This guide explains the operations that the user will follow while using the application.

1.2 Audience

This manual is intended for Customers and Partners who setup and use Oracle Banking Digital Experience.

1.3 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.

Access to Oracle Support

Oracle customers that have purchased support 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 Critical Patches

Oracle advises customers to get all their security vulnerability information from the Oracle Critical Patch Update Advisory, which is available at Critical Patches, Security Alerts and Bulletins. All critical patches should be applied in a timely manner to ensure effective security, as strongly recommended by Oracle Software Security Assurance.

1.5 Diversity and Inclusion

Oracle is fully committed to diversity and inclusion. Oracle respects and values having a diverse workforce that increases thought leadership and innovation. As part of our initiative to build a more inclusive culture that positively impacts our employees, customers, and partners, we are working to remove insensitive terms from our products and documentation. We are also mindful of the necessity to maintain compatibility with our customers' existing technologies and the need to ensure continuity of service as Oracle's offerings and industry standards evolve. Because of these technical constraints, our effort to remove insensitive terms is ongoing and will take time and external cooperation.

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.

1.7 Screenshot Disclaimer

The images of screens used in this user manual are for illustrative purpose only, to provide improved understanding of the functionality; actual screens that appear in the application may vary based on selected browser, theme, and mobile devices.

1.8 Acronyms and Abbreviations

The list of the acronyms and abbreviations that you are likely to find in the manual are as follows:

Abbreviation	**Description**
OBDX	Oracle Banking Digital Experience

2. Steps to Create Credential Mapping

Credential Store Mapping

The OBDX system utilizes external integrations to facilitate seamless communication with various services. To establish these connections, credentials are required to authenticate and authorize access. These credentials are not hardcoded but rather initialized post-installation. They are subsequently encrypted and stored within the database, ensuring confidentiality and integrity. Upon application startup, the credentials undergo decryption, enabling secure loading into the system. This subsequent section outlines the procedures and guidelines for configuring and managing these credentials within the OBDX environment.

To utilize the credential mapping functionality, retrieve the com.ofss.digx.CredentialsStore.jar file from the designated location:

OBDX_Installer/installables/OBDX/BASE/22.2.6.0.0/utils/tools

Running the Credential Mapping Application

Execute the application using the following command:

```
java -jar com.ofss.digx.CredentialsStore.jar <csv_file> <DataBaseCredentials> <DataSeedFlag>
<AES_KEY>
```

Command Parameters:

1. <csv_file>

Provide the path to your CSV file containing user credentials by replacing <csv_file> with the actual file location.

CSV File Format Requirements

The CSV file must adhere to the following structure:

- Contain exactly three columns: type, username, and password
- Include a header row with column names: type,username,password
- Subsequent rows should contain individual credential entries, with each row representing a distinct set of credentials
- Ensure that the value in the type column is unique for each credential entry

Example CSV File

type	Username	password
MERCHANT	OBDX	PASSWORD111

2. <DataBaseCredentials>

Specify the <DataBaseCredentials> parameter as a comma-delimited string comprising the following components:

- Database username
- Password
- JDBC URL (in the format jdbc:oracle:thin:@host:port/service_id)

The expected format for <DataBaseCredentials> is: username,password,jdbc_url.

Example: User,Password123,jdbc:oracle:thin:@host:port/service_id

Ensure accurate input of these values to establish a successful connection to the database.

3. <DataSeedFlag>

To control the seeding of data into the digx_fw_credentials table, set the <DataSeedFlag> parameter to 'Y' to populate the table with the generated credentials. Alternatively, specify 'N' to simply display the credentials without persisting them to the database.

<AES_KEY>

The <AES_KEY> parameter is the AES encryption key used to secure sensitive data. If data is already encrypted with a previous key, use the same key here. This avoids decrypting and re-encrypting existing data. Enter the key in plaintext. Handle this key securely to prevent unauthorized access.

Example:

password

Example command to run this

```
java -jar com.ofss.digx.CredentialsStore.jar data.csv
DB_USER,DB_PASSWORD,jdbc:oracle:thin:@//HOST:PORT/SERVICE_ID Y password
```

Upon executing this utility, you will obtain an encrypted password, which can then be utilized in conjunction with other credentials. Subsequently, these credentials will be populated into the database.

Extensibility:

To leverage custom credentials inserted into the system, utilize the following code snippet:

```
ICredentialStore store =
CredentialStoreFactory.getCredentials(CredentialStoreKeys.CREDENTIAL_IPMLEMENTATION);
```

Credential credentials = store.getCredentials(<custom_type>);

Replace <custom_type> with the desired type associated with the custom credentials.

Import:

Import the jar implementation

"com.ofss.digx.infra:com.ofss.digx.infra.crypto.impl:$libs_digxVersion"

into your gradle project

To ensure proper configuration, verify that the entry in the digx_fw_config_all_b table has a prop_id of “credential_impl”, a category_id of “CredentialStore”, and a PROP_VALUE of “com.ofss.digx.infra.cred.DatabaseCredentialsStore”. Confirm that these values match exactly to guarantee correct functionality. If discrepancies are found, update the entry accordingly to reflect the specified values.

Note:

The AES key is no longer stored in the Credential Store but inside a keystore in DIGX_FW_KEYSTORE.

For any encryption operations that require the use of the AES key, utilize the SymmetricCryptographyProviderFactory class, which is available in the same JAR, instead of relying on the credential. This approach streamlines the encryption process and enhances overall security.

```
SymmetricCryptographyProviderFactory.getInstance().getLatestProvider().encrypt(data);

SymmetricCryptographyProviderFactory.getInstance().getLatestProvider().decrypt(data);
```