

# Oracle® Banking APIs

## User Password Printing Configuration Guide



Patchset Release 22.2.5.0.0

G15773-01

October 2024

The Oracle logo, consisting of a solid red square with the word "ORACLE" in white, uppercase, sans-serif font centered within it.

ORACLE®

Copyright © 2006, 2024, Oracle and/or its affiliates.

This software and related documentation are provided under a license agreement containing restrictions on use and disclosure and are protected by intellectual property laws. Except as expressly permitted in your license agreement or allowed by law, you may not use, copy, reproduce, translate, broadcast, modify, license, transmit, distribute, exhibit, perform, publish, or display any part, in any form, or by any means. Reverse engineering, disassembly, or decompilation of this software, unless required by law for interoperability, is prohibited.

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.

If this is software, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. No other rights are granted to the U.S. Government.

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 fail-safe, 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.

Oracle®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Epyc, and the AMD logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

This software or hardware and documentation may provide access to or information about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

# Contents

## Preface

---

Purpose	iv
Audience	iv
Documentation Accessibility	iv
Critical Patches	iv
Diversity and Inclusion	v
Conventions	v
Related Resources	v
Screenshot Disclaimer	v
Acronyms and Abbreviations	v

## 1 OBAPI User Password Print Configuration

---

1.1 Configure Password Encryption/Decryption Provider	1-1
1.2 Configure Password Printing Adapter	1-2

## 2 List of Topics

---

## Index

---

# Preface

- [Purpose](#)
- [Audience](#)
- [Documentation Accessibility](#)
- [Critical Patches](#)
- [Diversity and Inclusion](#)
- [Conventions](#)
- [Related Resources](#)
- [Screenshot Disclaimer](#)
- [Acronyms and Abbreviations](#)

## Purpose

This guide is designed to help acquaint you with the Oracle Banking APIs application. This guide provides answers to specific features and procedures that the user need to be aware of the module to function successfully.

## Audience

This document is intended for the following audience:

- Customers
- Partners

## 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 customer access to and use of Oracle support services will be pursuant to the terms and conditions specified in their Oracle order for the applicable services.

## 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](#).

## 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.

## Conventions

The following text conventions are used in this document:

Convention	Meaning
<b>boldface</b>	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	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.

## Related Resources

For more information on any related features, refer to the following documents:

- [Oracle Banking APIs Installation Manuals](#)

## Screenshot Disclaimer

Personal information used in the interface or documents is dummy and does not exist in the real world. It is only for reference purposes.

## Acronyms and Abbreviations

The list of the acronyms and abbreviations used in this guide are as follows:

**Table 1 Acronyms and Abbreviations**

Abbreviation	Description
OBAPI	Oracle Banking APIs

# 1

## OBAPI User Password Print Configuration

- [Configure Password Encryption/Decryption Provider](#)
- [Configure Password Printing Adapter](#)

### 1.1 Configure Password Encryption/Decryption Provider

1. When you create any new user or reset password for any existing user, user credential gets stored in system using two way cryptography so that same to be available for password printing
2. To override existing cryptography implementation, you need to perform following steps:
  - Add provider that implements `com.ofss.digx.app.sms.crypto.IUserCryptographyProvider`. Here you can add encryption and decryption implementation for Password.  
**Example:**

```
package com.ofss.digx.app.sms.crypto; publicclass
CustomUserCryptographyProvider implements
IUserCryptographyProvider
{
    @Override
    public String decrypt(String value)
    {
        // TODO Auto-generated method stub
        returnnull;
    }
    @Override
    public String encrypt(String value)
    {
        // TODO Auto-generated method stub
        returnnull;
    }
}
```

- Add one entry in Preferences.xml if not present for name '`UserConfig`'  
**Example:**

```
<Preference name="UserConfig' "  
PreferencesProvider="com.ofss.digx.infra.config.impl.DBBased  
PropertyProvider" parent="jdbcpreference"  
propertyFileName="select prop_id,  
prop_value from digx_fw_config_all_b where category_id = 'UserConfig'  
" syncTimeInterval="36000000" />
```

- Add one entry in database table `digx_fw_config_all_b` for `category_id = 'UserConfig'` and `prop_id = 'USER_CRYPTO_PROVIDER'`

```
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)values
('USER_CRYPTO_PROVIDER','UserConfig',
'com.ofss.digx.app.sms.crypto.CustomUserCryptographyProvider ','N',null,
'Custom provider for Password Encryption and
decryption','ofssuser',sysdate,'ofssuser',sysdate,'A',1);
```

### Note:

If above configuration is done, it will use `CustomUserCryptographyProvider` for password encryption and decryption and same encrypted password will be stored in `DIGX_UM_PWD_PRINTINFO` table. Currently by default `com.ofss.digx.app.sms.crypto.UserCryptographyProvider` provider will used if no configuration is done.

## 1.2 Configure Password Printing Adapter

1. After successfully storing password in System, same will be available for printing to administrator.
2. Currently when admin performs password printing for user, password printing data stored in system in blob using adapter.
3. To override existing password printing implementation, you need to perform following steps:
  - Add adapter that implements `com.ofss.digx.app.sms.user.printinformation.provider.IUserInformationPrintAdapter`. Here you can add implementation for printing document for a user. `PasswordPrintInformationDTO` object will contain username, password and other documents(Password Letter/Welcome Letter).

### Example:

```
package com.ofss.digx.app.sms.user.printinformation.provider;
import
com.ofss.digx.app.sms.dto.user.printInformation.PasswordPrintInformation
DTO;
import com.ofss.digx.infra.exceptions.Exception;
publicclass CustomUserInformationPrintAdapter implements
IUserInformationPrintAdapter
{
@Override publicvoid print
(
PasswordPrintInformationDTO userprintDTO
)
throws Exception
{
// TODO Auto-generated method stub
```



```
    }
}
```

- Add one entry in Preferences.xml if not present for name 'UserPrintConfig'.  
**Example:**

```
<Preference name="UserPrintConfig"

PreferencesProvider="com.ofss.digx.infra.config.impl.DBBasedPropertyProvider"
parent="jdbcpreference" propertyFileName="select prop_id,
prop_value from digx_fw_config_all_b where category_id =
'UserPrintConfig' '
"syncTimeInterval="3600000" />
```

- Add one entry in database table digx\_fw\_config\_all\_b for **category\_id** = 'UserPrintConfig' and **prop\_id** = 'USER\_INFORMATION\_PRINT\_PROVIDER' .

```
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)values
('USER_INFORMATION_PRINT_PROVIDER','UserPrintConfig',
'com.ofss.digx.app.sms.user.printinformation.provider.CustomUserInformationPrintAdapter','N',
null,'Custom adapter for User Password Information
Printing','ofssuser',sysdate,'ofssuser',sysdate,'A',1);
```



#### Note:

If above configuration is done, it will use `CustomUserInformationPrintAdapter` for user Password Information printing. Currently by default `com.ofss.digx.app.sms.user.printinformation.provider.UserInformationPrintAdapter` adapter will be used if it does not find any configuration.

# 2

## List of Topics

This user manual is organized as follows:

**Table 2-1 List of Topics**

<b>Topics</b>	<b>Description</b>
<b>Preface</b>	This topic provides information on the introduction, intended audience, list of topics, and acronyms covered in this guide.
<b><a href="#">OBAPI User Password Print Configuration</a></b>	This topic provides information about the configuration of the Password Encryption/Decryption Provider, and Password Printing adapter.

# Index

## C

---

Configure Password Encryption/Decryption  
Provider, [1-1](#)

Configure Password Printing Adapter, [1-2](#)