

Oracle® Banking APIs

Connector Credential Store Guide



Patchset Release 22.2.5.0.0

G15748-01

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 Creating Credential Mapping

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
boldface	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

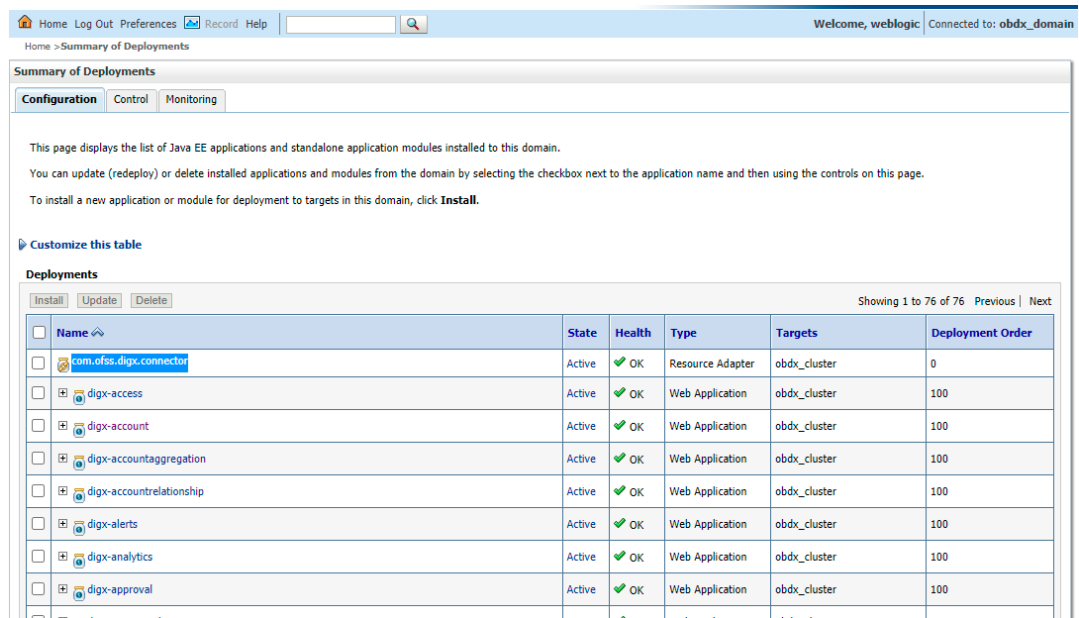
1

Creating Credential Mapping

Steps to create credential mapping are:

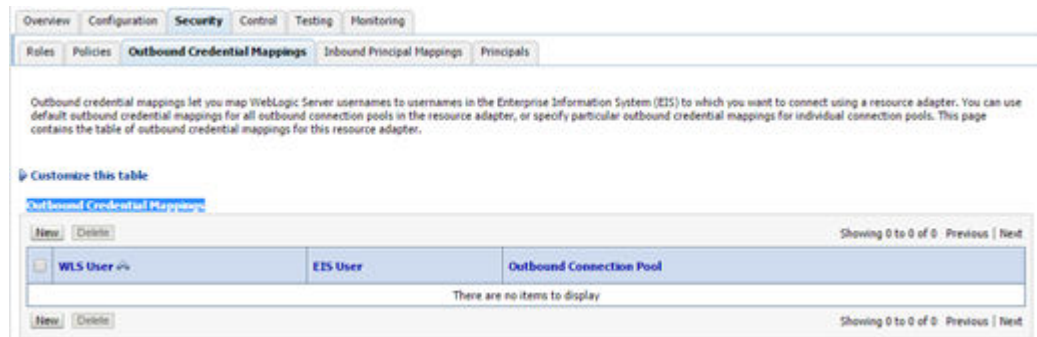
1. In WebLogic, go to **Deployments**, and click on **com.ofss.digx.connector**

Figure 1-1 Deployed rar com.ofss.digx.app.connector



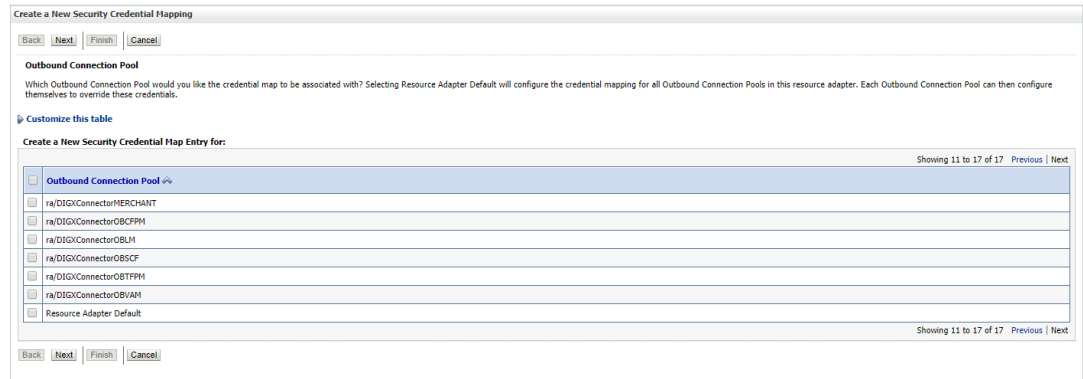
2. Click **Security** → **Outbound Credential Mapping**. This will display **Outbound Credential Mappings** table.

Figure 1-2 Shows setting for com.ofss.digx.connector.rar



3. Click **New** to add new credentials. This will display screen to create new security credential map entry. Also it shows **Outbound Connection** pool table. This table has **Outbound Connection pool** entry for each connection instance in weblogic-ra.xml in **Resource Adapter** along with default connection pool.

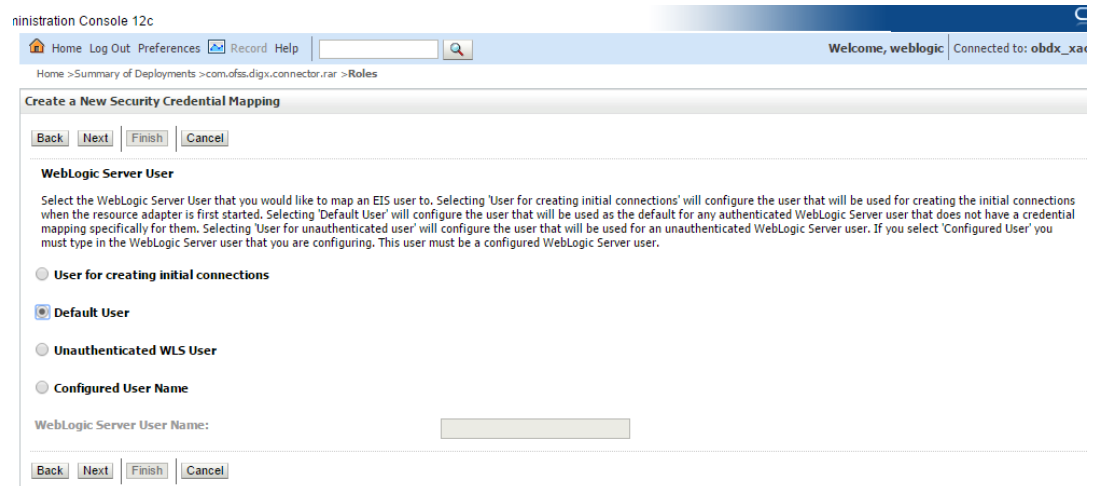
Figure 1-3 Shows Outbound Connection pool table



It shows corresponding weblogic-ra.xml file

4. Select Outbound connection pool to associate the credential map. And click **Next**. This will show screen to select weblogic server user.

Figure 1-4 Weblogic server user screen



5. Select Default User. Selecting 'Default User' as WebLogic Server user will configure the user that will be used as the default for any authenticated WebLogic Server user that does not have a credential mapping specifically for them.
6. And click Next. Screen to configure username and password will appear. Enter username and password.

Figure 1-5 User name and password configuration

Administration Console 12c

Home Log Out Preferences Record Help Welcome, weblogic Connected to: obdx_xac

Home > Summary of Deployments > com.ofss.digx.connector.rar > Roles

Create a New Security Credential Mapping

Back Next Finish Cancel

WebLogic Server User

Select the WebLogic Server User that you would like to map an EIS user to. Selecting 'User for creating initial connections' will configure the user that will be used for creating the initial connections when the resource adapter is first started. Selecting 'Default User' will configure the user that will be used as the default for any authenticated WebLogic Server user that does not have a credential mapping specifically for them. Selecting 'User for unauthenticated user' will configure the user that will be used for an unauthenticated WebLogic Server user. If you select 'Configured User' you must type in the WebLogic Server user that you are configuring. This user must be a configured WebLogic Server user.

User for creating initial connections
 Default User
 Unauthenticated WLS User
 Configured User Name

WebLogic Server User Name:

Back Next Finish Cancel

- Click **Finish**. The new security credential map entry will be created.

Figure 1-6 Credential map entry

Administration Console 12c

Home Log Out Preferences Record Help Welcome, weblogic Connected to: obdx_xac

Home > Summary of Deployments > com.ofss.digx.connector.rar > Roles

Messages

✓ The new security credential map entry for this resource adapter was successfully created.

Settings for com.ofss.digx.connector.rar

Overview Configuration **Security** Control Testing Monitoring

Roles Policies **Outbound Credential Mappings** Inbound Principal Mappings Principals

Outbound credential mappings let you map WebLogic Server usernames to usernames in the Enterprise Information System (EIS) to which you want to connect using a resource adapter. You can use default outbound credential mappings for all outbound connection pools in the resource adapter, or specify particular outbound credential mappings for individual connection pools. This page contains the table of outbound credential mappings for this resource adapter.

Customize this table

Outbound Credential Mappings

New Delete Showing 1 to 1 of 1 Previous Next

	EIS User	Outbound Connection Pool
<input type="checkbox"/> WLS User ↕		
<input type="checkbox"/> Default	MERCHANT	ra/DIGXConnectorMERCHANT

New Delete Showing 1 to 1 of 1 Previous Next

It displays the Credential map entry with username as MERCHANT associated with ra/DIGXConnectorMERCHANT connection pool.

Below credential entries must be configured in connector. Managed server restart is required after this configuration

- DIGXConnectorAES is mandatory entry, The password value for this must be a 16 digit AES key that must be set
- Remaining entries are optional and depend on the module used.

Figure 1-7 Credential entries configured in connector

Outbound Credential Mappings

[New](#) [Delete](#) Showing 1 to 12 of 12 [Previous](#) | [Next](#)

<input type="checkbox"/>	WLS User ↕	EIS User	Outbound Connection Pool
<input type="checkbox"/>	Default	MERCHANT	ra/DIGXConnectorMERCHANT
<input type="checkbox"/>	Default	AES_KEY	ra/DIGXConnectorAES
<input type="checkbox"/>	Default	1*	ra/DIGXConnectorLIVEEXP
<input type="checkbox"/>	Default	1....J0d-d886-4l	ra/DIGXConnectorNETVERIFY
<input type="checkbox"/>	Default	OBDX01	ra/DIGXConnectorOBVAM
<input type="checkbox"/>	Default	OBDX	ra/DIGXConnectorOBSCF
<input type="checkbox"/>	Default	OBDX02	ra/DIGXConnectorOBLM
<input type="checkbox"/>	Default	SADHASIVAM1	ra/DIGXConnectorOBFCFM
<input type="checkbox"/>	Default	OBDX	ra/DIGXConnectorOBCM
<input type="checkbox"/>	Default	OBDX	ra/DIGXConnectorASP
<input type="checkbox"/>	Default	OBDX	ra/DIGXConnectorINV
<input type="checkbox"/>	Default	SADHASIVAM1	ra/DIGXConnectorMO_IPM

[New](#) [Delete](#) Showing 1 to 12 of 12 [Previous](#) | [Next](#)

2

List of Topics

This user manual is organized as follows:

Table 2-1 List of Topics

Topics	Description
Preface	This topic provides information on the introduction, intended audience, list of topics, and acronyms covered in this guide.
Steps to Create Credential Mapping	This topic provides explains the steps to create credential mapping.

Index

C

Creating Credential Mapping, [1-1](#)