Oracle® Banking Digital Experience Cloud Service

Getting Started with Oracle Banking Digital Experience Cloud Service

Release 25.1.2.0.0
G55570-01
April 2026

ORACLE

Oracle Banking Digital Experience Cloud Service Getting Started with Oracle Banking Digital Experience Cloud Service, Release 25.1.2.0.0

G55570-01

Copyright © 2025, 2026, 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

Copyright © 2025, 2026, Oracle and/or its affiliates.

Preface

Purpose

Getting Started with Oracle Banking Digital Experience Cloud Service introduces you to cloud concepts and describes how you can request a trial subscription or purchase a subscription for an Oracle Cloud service.

Audience

This Guide is primarily for users who are responsible for provisioning and activating Oracle Banking Digital Experience Cloud Services, for adding other users who would manage the services, or, who want to develop Oracle Banking Digital Experience Cloud Service.

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.

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.

Copyright © 2025, 2026, Oracle and/or its affiliates.

Related Resources

The related documents are as follows:

- Product User Guides

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.

Acronyms and Abbreviations

Table Acronyms and Abbreviations

Abbreviation	Abbreviation
OBDXCS	Oracle Banking Digital Experience Cloud Service
OBRH	Oracle Banking Routing Hub
SCIM	System for Cross-domain Identity Management
IDCS	Oracle Identity Cloud Service

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.

Copyright © 2025, 2026, Oracle and/or its affiliates.

1

Introduction

Oracle Banking Digital Experience Cloud Service (OBDXCS) is a modern digital banking platform that enables financial institutions to provide seamless, secure, and highly personalised digital banking services to our customers. The platform supports multiple banking segments including Retail, Corporate, and SMB banking, and offers a unified experience across digital channels such as Internet Banking and Mobile Banking.

OBDXCS is designed with a modular and scalable architecture that allows banks to rapidly deploy digital capabilities while maintaining high standards of security, compliance, and operational efficiency. Through its flexible configuration framework, banks can tailor the platform to meet their specific business requirements, product offerings, and regulatory guidelines.

This document serves as a step-by-step onboarding guide for setting up OBDXCS. It outlines the prerequisite information, configuration sequence, and administrative activities that must be completed before the platform can be used by bank administrators and end customers.

The guide covers the initial setup for the core components of the OBDX Cloud ecosystem:

- Oracle Banking Digital Experience Cloud Service (OBDXCS) – The primary digital banking platform used by bank administrators and customers for accessing banking services.
- Oracle Banking Routing Hub (OBRH) – A routing and integration layer responsible for connecting OBDX CS with Oracle Banking Cloud Services and other backend services.
  - App Shell – A platform administration layer used for application-level configuration and user management for certain components.
- Oracle Identity Cloud Service (IDCS) – The identity and access management system responsible for authentication, authorization, and user provisioning across the ecosystem.

This document is intended to help the bank's implementation, system administration, and technology teams understand the required configuration flow to successfully activate and operationalise OBDX CS. It includes guidance on:

- Prerequisites and access details required to begin configuration.
- Identity and access setup using IDCS.
- Initial administrator setup and system configuration in OBDXCS.
- Integration setup through OBRH.

By following the steps outlined in this guide, banks can ensure a structured, secure, and standardised setup of the OBDX CS environment, enabling them to quickly move forward with user onboarding, transaction enablement, and digital banking service rollout.

Copyright © 2025, 2026, Oracle and/or its affiliates.

2

Prerequisites

Before initiating the configuration of Oracle Banking Digital Experience Cloud Service (OBDX CS) in the cloud environment, certain access details, system URLs, and administrator credentials must be provisioned and shared with the bank's implementation team.

These prerequisites ensure that the bank administrators have the required access to all platform components that are part of the OBDX cloud ecosystem.

The following components must be accessible prior to beginning the configuration:

- Oracle Banking Digital Experience Cloud Service (OBDX CS)
- Oracle Banking Routing Hub (OBRH)
- Oracle Identity Cloud Service (IDCS)

Initial administrator credentials will be shared with the bank to allow access to the respective systems.

These credentials are used during the initial setup phase and may later be supplemented with additional administrative users created by the bank.

Table 2-1 Component

Component	Credentials Provided	Purpose
OBDXCS	**User ID**: SUPERADMIN (No password will be shared)	Used for initial OBDX CS login and system configuration
App Shell	App Shell Admin credentials	Used to create users required for OBRH
IDCS	IDCS Administrator credentials	Used to configure identity management and create users

> **Note**
>
> - The SUPERADMIN user must be created and activated in IDCS before logging into OBDXCS.
> - Login credentials should be configured during the activation process.

Copyright © 2025, 2026, Oracle and/or its affiliates.

3

SCIM Configuration in IDCS

OBDXCS supports SCIM-based provisioning to enable integration with IDCS for user identity management.

For the detailed step-by-step process for configuring SCIM and onboarding users through IDCS, refer to the SCIM configuration document provided below.

For more information, refer SCIM Configuration.

Copyright © 2025, 2026, Oracle and/or its affiliates.

4

OBDX Admin User setup in IDCS

User management in the OBDX CS is handled through Oracle Identity Cloud Service (IDCS). IDCS serves as the central identity and authentication provider for the OBDX CS platform. All users must be created and managed in IDCS.

Once a user is created in IDCS, the user can then be onboarded into OBDX CS through the OBDX CS Admin application.

As a result, users cannot be created directly within OBDX CS. The user lifecycle must always begin in IDCS, followed by onboarding into OBDX CS.

As part of the environment setup, a SUPERADMIN user ID is provisioned for the bank. Before the SUPERADMIN can log into OBDX CS, the user must be created and activated in IDCS and a password must be set. Once activated, the SUPERADMIN user can log into OBDX CS and perform the initial system configuration and administrative setup.

Copyright © 2025, 2026, Oracle and/or its affiliates.

5

OBRH Configuration within OBDX

Prerequisite

As the first step, log in to App Shell using the App Shell Admin credentials provided during environment setup.

For configuring Oracle Banking Routing Hub (OBRH) for OBDX CS, the required sub-namespace name for the foundation environment must first be obtained from the Oracle AMS team. This sub-namespace is required for completing the OBRH configuration related to OBDX CS integrations.

After obtaining the required details, the necessary OBRH configurations should be performed by referring to the OBRH configuration documentation, which provides the detailed step-by-step process for the required maintenances.

For initial configuration, please refer to this document.

For more information, refer Oracle Banking Routing Hub.

Copyright © 2025, 2026, Oracle and/or its affiliates.

6

OBRH Module Specific Maintenances

Module-level configurations in Oracle Banking Routing Hub (OBRH) are required to support operations, and the following outlines the module-specific configurations.

Module Specific Configuration

1. **Party, CASA, TD, and Loans**
   For enabling core banking operations across customer (party), account (CASA & TD), and loan modules, with required configurations in Oracle Banking Routing Hub (OBRH) to enable seamless transaction routing, integration, and end-to-end processing of related services.

   The detailed steps and configuration guidelines for OBRH setup are provided in the OBRH Party,CASA,TD,Loansconfiguration document. Refer to the document for the step-by-step instructions to complete the required configurations.

   For more information, refer OBRH_CASA, CA, SA, TD, & Loans
2. **Payments**
   For enabling Payments functionality, specific configurations need to be performed in Oracle Banking Routing Hub (OBRH) to support the required routing and integration with backend systems.

   The detailed steps and configuration guidelines for Payments-related OBRH setup are provided in the OBRH Payments configuration document. Refer to the document for the step-by-step instructions to complete the required configurations.

   For more information, refer Payments.
3. **Trade Finance**
   For enabling Trade Finance functionality, specific configurations need to be performed in Oracle Banking Routing Hub (OBRH) to support routing, processing, and integration with the respective backend trade systems.

   The detailed steps and configuration guidelines for Trade Finance-related OBRH setup are provided in the OBRH Trade Finance configuration document. Refer to the document for step-by-step instructions to complete the required configurations.

   For more information, refer Trade Finance.
4. **Originations**
   For enabling Originations functionality, required configurations need to be carried out to support integration with the onboarding/origination systems and ensure seamless processing of customer applications.

   The detailed steps and configuration guidelines for Originations setup are provided in the respective configuration document. Refer to the document for step-by-step instructions to complete the required configurations.

   For more information, refer Originations.

Copyright © 2025, 2026, Oracle and/or its affiliates.

7

Mobile Configuration

As part of the Mobile Banking channel setup, the required configuration must be completed in Oracle Identity Cloud Service (IDCS) to enable authentication and user access for the mobile application. This includes configuring the Mobile Banking / Onboarding channel in IDCS so that users can securely authenticate and access OBDX CS through the mobile application.

These configurations ensure proper integration between the mobile workspace and IDCS for authentication and user management.

For the detailed step-by-step procedure, refer to the Mobile Configuration setup documentation provided in the link below:

For more information, refer Mobile Application Builder Guide-iOS.

For more information, refer OBDXCS Mobile Configuration in IDCS.

Copyright © 2025, 2026, Oracle and/or its affiliates.

8

Basic OBDX Configurations

OBDXCS application using the OBDXCS URL provided during environment setup.

Upon the first successful login, the SUPERADMIN user will automatically be assigned the AUTHADMIN role, which grants the required privileges to perform the initial administrative configurations within the system.

After login, the administrator should complete the following configuration activities to prepare the platform for further administrative setup and user onboarding.

Entity Maintenance

After logging into OBDX CS for the first time, the Entity Maintenance page is displayed as the default landing page.

Entity Maintenance allows the administrator to define and manage the bank entity within the system. This is a mandatory step required to ensure that the platform is correctly associated with the bank's operational entity.

The administrator should review the entity details and ensure that the required information is correctly configured before proceeding with other system configurations.

For the detailed step-by-step process for Entity Maintenace, refer to the configuration document provided in the link below.

For more information, refer **Entity Maintenance** in **Core User Manual**.

System Configuration

The next step involves configuring key system parameters through the System Configuration module. This section allows administrators to define important system settings required for the operation of the OBDX platform.

During this step, the administrator should:

- Provide values for the mandatory configuration fields
- Review the default values provided by the system
- Modify configuration parameters if required based on bank policies
- Configure the required parameters at the module level based on the bank's requirements.
- Perform any module-specific configurations required for enabled modules
- Configure the Email server settings required for sending system notifications and alerts
- Define the Bank Name, which will be used in system-generated communications and alerts sent to users

Most mandatory fields are pre-populated with default system values. These values can be retained or modified based on the bank's operational requirements.

For more information, refer **System Maintenance** in **Core User Manual**.

Copyright © 2025, 2026, Oracle and/or its affiliates.

Locale Maintenance

By default, all supported languages are enabled in the system. The SUPERADMIN can disable languages that are not required and set the preferred default language for the application. This allows the bank to control which languages are available to users based on their requirements.

For the detailed step-by-step procedure for Locale Maintenance, refer to the document provided in the link below.

For more information, refer **Locale Maintenance**.

Touch Point Maintenance

Touch Point Maintenance is used to configure and manage the digital channels through which users can access the OBDX platform. This configuration allows the bank to define the available touch points and control how different banking services are made accessible across these channels. The SUPERADMIN must ensure that the required touch points are appropriately configured before enabling user access to the platform.

The following internal touch points are defined and available as part of the OBDX system:

- Internet
- Mobile App
- Mobile Browser
- Snapshot

For the detailed step-by-step procedure for configuring Touch Point Maintenance, refer to the document provided in the link below. Specifically, refer to the following sections in the document:

- Touch Point Maintenance
- Touch Point Group Maintenance

For more information, refer **Touch Point Maintenance** in **Core User Manual**.

For more information, refer **Touch Point Group Maintenance** in **Core User Manual**.

Role Maintenance

Role Maintenance is used to define and manage application roles within the OBDX platform, which control the transactions, widgets, dashboards, and privileges available to different users. Roles are defined for various user types such as Retail & Business, Corporate, and Admin, and can be mapped to both internal and external touch points.

Application roles determine the level of access a user has within the system. Users are able to view and perform only those transactions, menu options, widgets, and dashboards that are mapped to the roles assigned to them. System administrators can map entitlements, transactions, and privileges such as Perform, Approve, View, Release, and Check to specific roles based on the bank’s access control policies.

Roles can also be associated with specific entities, although this is optional. If no entity is mapped, the role will be available globally across all entities. Additionally, roles can be mapped to internal touch points (such as Internet, Mobile App) used directly by OBDX, or to external touch points used by third-party systems through defined scopes in the Identity Management System.

Proper role configuration ensures that users and external systems can access only the functionalities permitted by the bank’s security and operational policies.

Copyright © 2025, 2026, Oracle and/or its affiliates.

For the detailed step-by-step procedure for Role Maintenance, refer to the document provided in the link below.

For more information, refer **Role Maintenance** in **Core User Manual**.

Limit Package Maintenance

Limit Package Maintenance is used to define and manage transaction limits within the OBDX platform. A limit package represents a group of transaction limits that can be applied to specific transactions or transaction groups. These limits are created through Limit Definition and can be mapped either to individual transactions or to transaction groups defined through Transaction Group Maintenance. Each limit package can also be associated with a specific channel or touch point, or with a group of touch points.

Limit packages allow the bank to control the maximum transaction values and usage thresholds across different users, parties, and channels. For Retail party transactions, the limit package assigned at the user level will be applied. For Business party transactions, the limit package configured at the party level through Party Preferences will be used.

Once created, limit packages can be mapped across various levels within the system, including Enterprise Roles (Retail, Corporate, or Administrator), User Segments, Parties, and Users. This enables the bank to apply different limit structures based on roles, customer segments, or specific users, ensuring compliance with internal policies and regulatory requirements.

For the detailed step-by-step procedure for Limit Package Maintenance, refer to the document provided in the link below. Specifically, refer to the following sections in the document:

- Limits Definition
- Limit Package Management

For more information, refer **Limit Package Maitenance** in **Core User Manual**.

System Rules Configuration

System Rules are used to define platform-level parameters for different enterprise roles, such as Retail, Corporate, and Administrator. It is important to note that within System Rules, only Limits support configuration at the Entity level and Touchpoint level is available.

For the detailed step-by-step procedure for configuring System Rules, refer to the document provided in the link below.

For more information, refer **System Rules** in **Core User Manual**.

Approval Configuration

To enable administrative activities within the system, the SUPERADMIN must configure an approval rule.

As part of the initial setup, it is recommended to create an Auto Authorization (AutoAuth) approval rule with minimum permissions required for user creation. This enables the administrator to quickly create additional administrative users required for further platform configuration.

Once additional administrators are onboarded, more structured maker-checker approval workflows can be configured as per the bank’s governance policies.

For the detailed step-by-step procedure for Approval Configuration, refer to the document provided in the link below. Specifically, refer to the following sections in the document:

- User Group Management

Copyright © 2025, 2026, Oracle and/or its affiliates.

- Workflow Management
- Approval Rule Management

For more information, refer **Approval** in **Core User Manual**.

User Onboarding Process

After completing the initial system setup, the SUPERADMIN is responsible for onboarding additional users required to operate and manage the OBDX platform. This includes onboarding Bank Administrative users (such as BANKADMIN or other admin roles) as well as customer users who will access digital banking services.

All users who require access to OBDX must first be created in Oracle Identity Cloud Service (IDCS). Once the user is created in IDCS, the user can then be onboarded into OBDX through the OBDX Admin application. Users cannot be created directly within the OBDX application; the user lifecycle must always begin in IDCS, followed by onboarding in OBDX.

The SUPERADMIN should initially create bank administrative users to support operational activities. Subsequently, customer users can be onboarded and provided access to the relevant digital banking services based on the roles and entitlements assigned to them.

For the detailed step-by-step process for creating users in IDCS and onboarding them into OBDX, refer to the SCIM configuration and user onboarding documentation provided in the link below.

IDCS User Creation: **User Profile Maintenance**.

OBDX User Onboarding:

- Admin User Onboarding – Performed through User Management
- Retail/Business User Onboarding – Performed through User Management
- Corporate User Onboarding – Requires Party Preference Maintenance (one-time setup for each party) along with Group Corporate Onboarding

For more information, refer **User Onboarding** in **Core User Manual**.

Two-Factor Authentication (2FA) Configuration

Two-Factor Authentication (2FA) adds an additional layer of security to the OBDX platform by requiring users to verify their identity using two authentication factors before completing certain actions, such as login or transactions. This helps reduce the risk of unauthorized access and protects against identity theft and phishing attacks.

SUPERADMIN can configure 2FA for different user types (Retail and Corporate) and, where applicable, for user segments. In a multi-entity setup, authentication rules can be defined separately for each entity. If a user switches entities after login, the system may prompt for second-factor authentication again.

OBDX provides multiple authentication mechanisms, including OTP (delivered to the registered mobile number or email), security questions, and push notification–based authentication.

Two-factor authentication (2FA) is applicable to all transactions in OBDX, excluding login.

For the detailed step-by-step procedure for configuring Two-Factor Authentication, refer to the document provided in the link below. Specifically, refer to the following section in the document:

For more information, refer **Authentication** in **Core User Manual**.

Copyright © 2025, 2026, Oracle and/or its affiliates.

Brand Management

Brand Management allows the bank to customize the look and feel of the OBDX application to align with its branding guidelines. Through this configuration, the bank can manage elements such as logos, color schemes, and other visual components that define the user interface and overall digital banking experience. This helps ensure a consistent brand identity across the digital banking platform.

For the detailed step-by-step procedure for configuring Brand, refer to the document provided in the link below. Specifically, refer to the following section in the document:

For more information, refer **Experience Builder** in **Core User Manual**.

Template Maintenance

Template Maintenance allows the bank to customize the format of downloadable documents for transactions that support downloads. Using this feature, the Bank Administrator can download the existing XSL template, modify it as required (for example, formatting or layout changes), and upload the updated template back into the system. The *header.xsl* template needs to be updated to configure the bank's logo; this is mandatory.

This enables the bank to tailor transaction download formats according to its reporting or documentation requirements.

For the detailed step-by-step procedure, refer to the Template Maintenance documentation provided in the link below.

For more information, refer **Template Maintenance** in **Core User Manual**.

> **Note**
>
> For security reasons, it is recommended to revoke or disable the SUPERADMIN access once all initial setup and configurations are completed. Ongoing administration activities should be performed using designated Bank Admin users with appropriate roles and maker-checker controls.

Copyright © 2025, 2026, Oracle and/or its affiliates.

Index

Copyright © 2025, 2026, Oracle and/or its affiliates.