Oracle® Revenue Management and Billing Cloud Service

Release 8.1

Federated Identity Configuration Guide

Revision 3.1

F46275-01

October, 2021

ORACLE®

Oracle Revenue Management and Billing Cloud Service Federated Identity Configuration Guide

F46275-01

Copyright Notice

Copyright © 2014, 2021 Oracle and/or its affiliates. All rights reserved.

Trademark Notice

Oracle, Java, JD Edwards, PeopleSoft, and Siebel are registered trademarks of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon 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, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

License Restrictions Warranty/Consequential Damages Disclaimer

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 de-compilation of this software, unless required by law for interoperability, is prohibited.

Warranty Disclaimer

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.

Restricted Rights Notice

If this software or related documentation is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, the following notice is applicable:

> U.S. GOVERNMENT RIGHTS
>
> Oracle programs, including any operating system, integrated software, any programs installed on the hardware, documentation, and/or technical data delivered to U.S. Government end users are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, documentation, and/or technical data shall be subject to license terms and restrictions as mentioned in Oracle License Agreement, and to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). No other rights are granted to the U.S. Government.

Hazardous Applications Notice

This software 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 in dangerous applications, then you shall be responsible to take all appropriate fail-safe, backup, redundancy, and other measures to ensure the safe use of this software. Oracle Corporation and its affiliates disclaim any liability for any damages caused by use of this software in dangerous applications.

Third Party Content, Products, and Services Disclaimer

This software 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 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.

Preface

About This Document

This document provides an overview of federated SSO login. It explains how to configure federated SSO login with SAML for the ORMB Cloud Service.

Intended Audience

This document is intended for customers using Oracle Revenue Management and Billing Cloud Service. It assumes that you have administrative privileges on the host where you want to install the software.

Organization of the Document

The information in this document is organized into the following sections:

Section No.	Section Name	Description
Section 1	Federated Single Sign-On With SAML 2.0	Explains how to use the OpenID Connect and SAML 2.0, which provide secure mechanisms to transmit authentication credentials and related information between different web applications.

Conventions

The following conventions are used across the document:

Convention	Meaning
boldface	Boldface indicates graphical user interface elements associated with an action, or terms defined in the text.
italic	Italic indicates a document or book title.
monospace	Monospace indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or information that an end-user needs to enter in the application.

Acronyms

The following acronyms are used in this document:

Acronym	Meaning
ORMB	Oracle Revenue Management and Billing
SSO	Single Sign-On
IDCS	Oracle Identity Cloud Service
OIDC	OpenID Connect

Acronym	Meaning
JWT	JSON Web Tokens
IDP	External Identity Provider
WTSS	Web Tier Security Service
SAML	Security Assertion Markup Language

Related Documents

You can refer to the following documents for more information:

Document Name	Description
Oracle Revenue Management and Billing Cloud Service 8.1 Release Notes	Describes the feature enhancements and supported client platforms and browsers in this release. It highlights different roles and responsibilities of Oracle and Customer. It also highlights the known issues in this release.
Oracle Revenue Management and Billing Cloud Service REST Services Configuration Guide	Explains how to configure federated Web service login in order to access protected REST services on the ORMB Cloud environments.
Oracle Revenue Management and Billing Cloud Service End User Provisioning Guide	Explains how to setup the security administrator account for the ORMB Cloud Service. It also explains how to manage users and user groups for the ORMB Cloud Service. In addition, it explains how to import and export bulk users and user groups for the ORMB Cloud Service.
Oracle Revenue Management and Billing Cloud Service SaaS Reporting using OAS	Explains the ORMB SaaS reporting architecture and how you can use Oracle Analytics Server for ORMB SaaS reporting.
Oracle Revenue Management and Billing Cloud Service SFTP Authentication Guide	Explains how to configure SFTP authentication for the ORMB Cloud Service.

Change Log

Revision	Last Update	Updated Section	Comments
3.1	15-Feb-2022	Related Documents	Updated Information

Contents

1.   Federated Single Sign-On With SAML 2.0

Federated single sign-on (SSO) standards such as OpenID Connect (OIDC) provide secure mechanisms for passing credentials and related information between different web applications that have their own authorization and authentication systems. The OpenID Connect is a simple identity layer on top of the OAuth 2.0 protocol. It allows clients to verify the identity of the end-user based on the authentication performed by an Authorization Server, as well as to obtain basic profile information about the end-user in an interoperable and REST-like manner. OpenID Connect has become the leading standard for single sign-on and identity provision on the Internet. Its formula for success: simple JSON-based identity tokens (JWT), delivered via OAuth 2.0 flows designed for web, browser-based and native, mobile applications.

ORMB uses 'Authorization code' flow. This flow is the most commonly used flow, intended for traditional web apps. Involves an initial browser redirection to/from the OpenID Provider/Identity Provider for user authentication and consent, then a second back-channel request to retrieve the ID token. This flow offers optimal security, as tokens are not revealed to the browser and the client can be authenticated.

ORMB provides two types of configuration options:

- Customer can integrate IDCS (as SP) with their On Premise Identity Provider using SAML protocol
- Customer can leverage IDCS as their identity provider

1.1   OpenID Connect Terminology

The SAML 2.0 specification provides a Web Browser SSO Profile, which describes how web applications can achieve Single Sign-On. Following are the main players in OpenID Connect:

- **Client** - This is how the user is interacting with the Resource Server, like a web application being served through a web browser.

- **Identity Provider (Authorization Server)** – This server owns the user identities and credentials, and authenticates the user.

- **SAML Token** - The term SAML token refers to SAML Assertion, often compressed, encoded, possibly encrypted. SAML Assertion is just an XML node with certain elements.

- **Metadata***:* Metadata defines how SAML 2.0 shares configuration information between two communicating entities. You can access and share the Access Manager Metadata information with the federated application. You can also access and share the federated application metadata with Access Manager.

1.2   Federated SSO Login Overview

With federated login, an External Identity Provider (IDP), such as an on premise corporate login system, is used to authenticate the user Id and password and, if successful, a token (SAML assertion) is generated by the IDP and used to grant access to the target application.
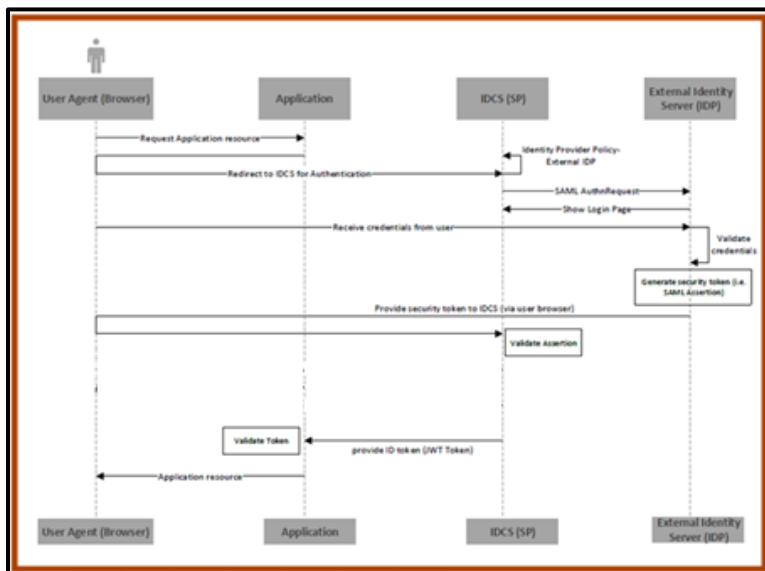
1.2.1   Option 1

The login process is as follows:

1. User accesses the ORMB application through the Web Tier Security Service (WTSS) URL.
2. WTSS intercepts the request and identifies the user is not authenticated.
3. WTSS redirects the user to the configured IDCS.
4. An external identity provider as configured in IDCS should do the authentication. It creates a SAML 2.0 request and responds to the browser with a redirect to the IDP.
5. The IDP is invoked with the SAML request and the IDP challenges the user with a login prompt.
6. The IDP authenticates the user and responds with a SAML 2.0 assertion and IDCS validates the assertion.
7. IDCS generates an access token and returns to WTSS through the callback URL.
8. WTSS redirects the user back to the originally requested resource.
9. WebLogic validates the JWT assertion token and then redirects to the ORMB application.

Refer to the below image for better understanding of Screen Login flow:

Figure 1: Option 1 – Screen Login Flow

1.2.2   Option 2

The login process is as follows:

1. User accesses the ORMB application through the Web Tier Security Service (WTSS) URL.
2. WTSS on ORMB app server intercepts the request and identifies the user is not authenticated.
3. WTSS redirects the user to the configured IDCS. IDCS challenges the user to enter the credentials.
4. IDCS authenticates the user and if successfully authenticated, generates an access token and returns to WTSS through the callback URL.
5. WTSS redirects the user back to the originally requested resource.
6. WebLogic validates the JWT assertion token and then redirects to the ORMB application.

Refer to the below image for better understanding of Login flow:
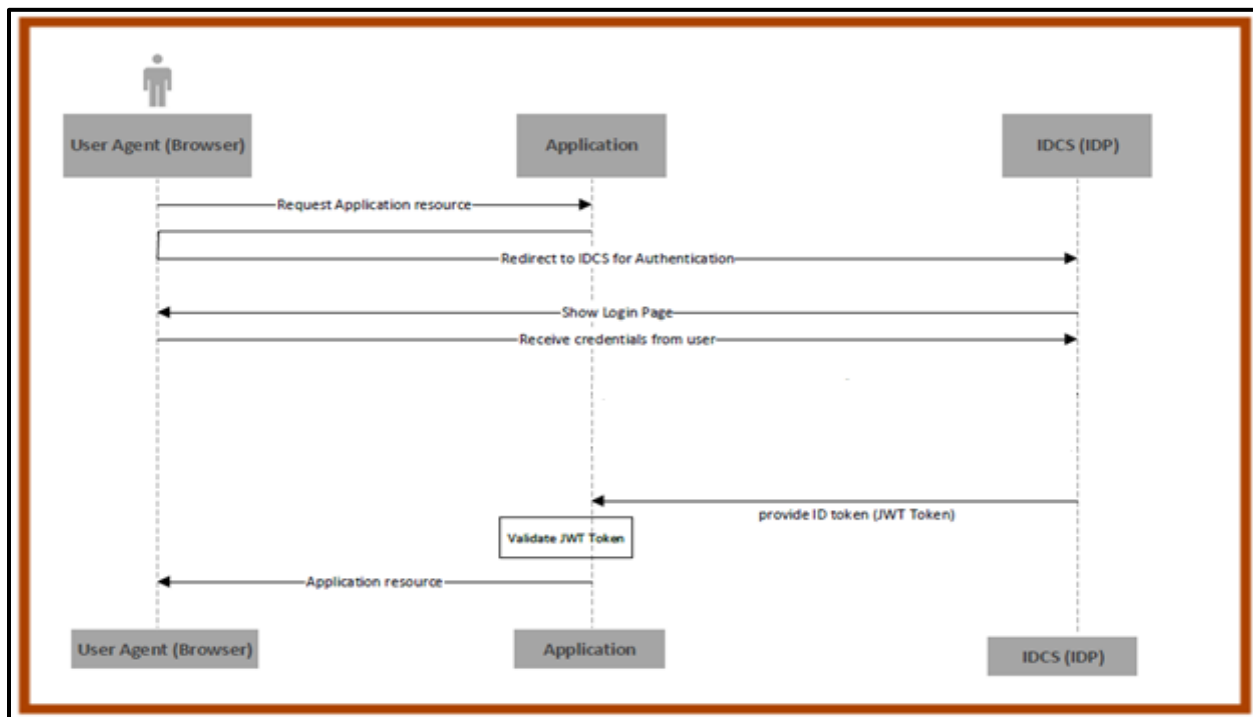
Figure 2: Option 2 - **Screen Login Flow**

1.3   OpenID Connect Implementation

IDCS OAuth key used for signing the JWT Access Token is imported in ORMB App Server (WebLogic) using chef automation script. These exchanges of signing keys will happen over SFTP or email. ORMB application server in order to validate JWT Access Token will use JWT Identity Assertor using JWT signing certificate.

1.4   SAML 2.0 Implementation (Only for Option1)

External Identity Provider (IDP) will handle the sign-in process and will eventually provide the authentication to ORMB application users. Users are authenticated through SAML Assertion at IDCS ends. Any changes you perform on premise accounts (namely first name, last name, and email) is synced back to the ORMB account through external REST services. The only user data necessary for ORMB is a user id for each user, the user's first name, last name and email. ORMB does not store passwords.

1.4.1   Configure SAML 2.0 Compliant Identity Provider

This section contains guidelines on how to configure SAML 2.0 Identity Provider to federate with ORMB application server to enable Single Sign-On access to one or more ORMB cloud service using the OpenID Connect protocol. The SAML 2.0 relying party for ORMB cloud service used in this scenario is External IDP and service provider is IDCS.
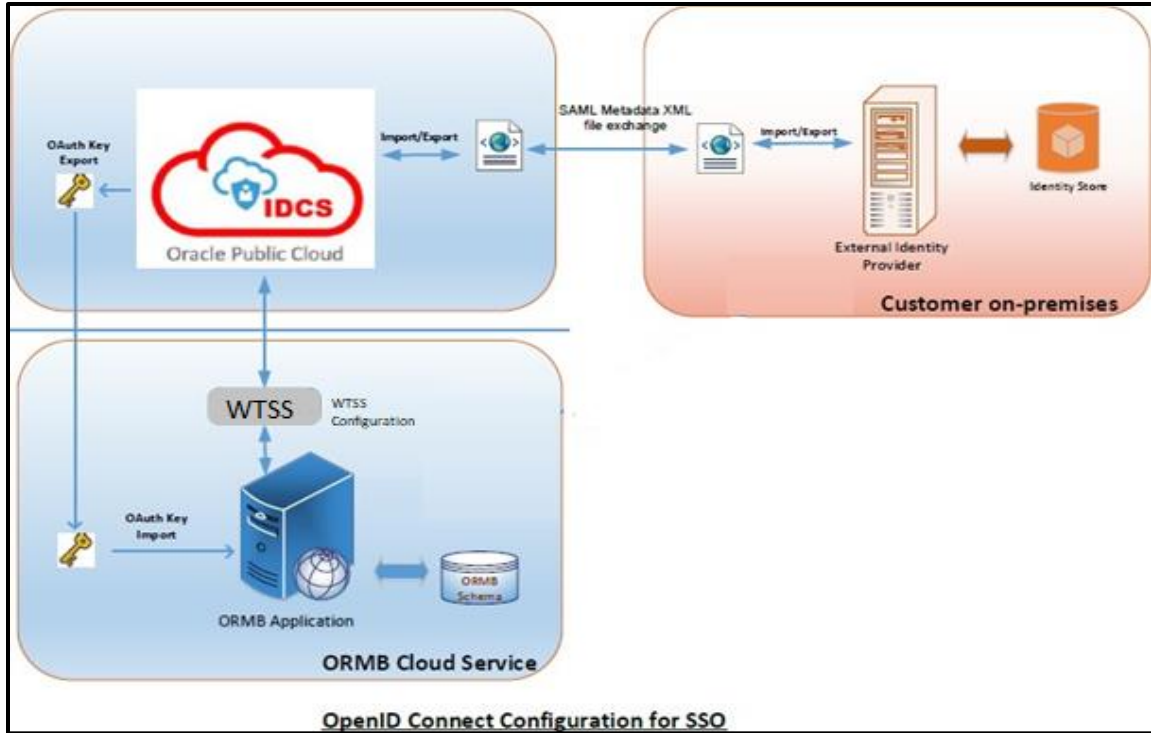
Figure 3: SAML Configuration

1.4.2   SAML Metadata

IDP imports IDCS's SAML metadata and thereby exchange public keys, IP addresses and communication information. Thus, ORMB IDCS provides you with the SAML metadata XML file, including the correct X509 certificates. It is recommended that you always import the latest ORMB metadata when configuring SAML 2.0 identity provider.

The following image shows a sample SAML 2.0 metadata XML:

Figure 4: Sample SAML Metadata XML

Note: The metadata XML varies from server to server.

1.4.3   User Provisioning

For user provisioning, external identity server must compatible with JWT. Customer needs to create users into ORMB application through REST services. For detailed instructions, refer to *Oracle Revenue Management and Billing Cloud Service REST Services Configuration Guide*. User must be present in ORMB application.

1.5   Why SAML?

The benefits of SAML include:

- **Platform neutrality -** SAML abstracts the security framework away from platform architectures and particular vendor implementations. Making security more independent of application logic is an important principle of Service-Oriented Architecture.

- **Loose coupling of directories** - SAML does not require user information to be maintained and synchronized between directories.

- **Improved online experience for end users** - SAML enables Single Sign-On by allowing users to authenticate at an Identity Provider and then access service providers without additional authentication. Additionally, identity federation (linking of multiple identities) with SAML allows for a better-customized user experience at each service while promoting privacy.