Oracle® Revenue Management and Billing Cloud Services

Release 7

Authentication SAML Configuration Guide

Revision 1.0

F24199-01

November, 2019

ORACLE

Oracle Revenue Management and Billing Cloud Services Authentication SAML Configuration Guide

F24199-01

ORACLE

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 details of ORMB cloud federated identity to configure SSO (Single Sign On) with SAML2.0 token. This document will help you to understand how to configure federated identity with SAML2.0 for Oracle Revenue Management and Billing (ORMB) cloud service.

Intended Audience

This document is intended for customers using Oracle Revenue Management and Billing (ORMB) cloud service and assumes that you have administrative privileges on the host where you want to install the software.

Contents

1. Federated Single Sign On With SAML 2.0 6

1.1 SAML2.0 Terminology 6

1.2 Federated SSO Login Overview 6

1.3 SAML 2.0 Implementation 7

1.3.1. Configure SAML 2.0 Compliant Identity Provider 7

1.3.2. SAML Metadata 8

1.3.3. User Provisioning 9

1.4 Why SAML? 9

1. Federated Single Sign On With SAML 2.0

Federated single sign-on (SSO) standards such as SAML 2.0 provide secure mechanisms for passing credentials and related information between different web applications that have their own authorization and authentication systems. SAML 2.0 is an open standard developed by the OASIS Security Services Technical Committee. The SAML 2.0 protocol has seen significant success, gaining momentum in financial services, higher education, government, and other industry segments. All major web-access management vendors have implemented SAML 2.0 support.

SAML 2.0-compliant web applications exchange user credential information using SAML assertions. SAML assertion is an XML document that contains trusted statements about a subject including, for example, a username and privileges. SAML assertions are digitally signed to ensure their authenticity.

1.1 SAML2.0 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 SAML:

- **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's Id and password and, if successful, a token (SAML assertion) is generated by the IDP and used to grant access to the target application.

The login process is as follows:

1. User accesses the ORMB application through the OHS URL. OHS redirects the flow to the application server.
2. The application server determines that the user has not been authenticated and creates a SAML 2.0 request, and responds back with a redirect (302) to the configured Identity provider (IDP) through the browser.
3. The IDP is invoked with the SAML request and if the user is not authenticated, it challenges the user with a login prompt.
4. The IDP authenticates the user and responds with a SAML 2.0 assertion, which includes the authenticated user data.

5. The browser sends the SAML response to the application server.
6. The Application server validates the assertion, create an SSO session and login to the ORMB application.

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

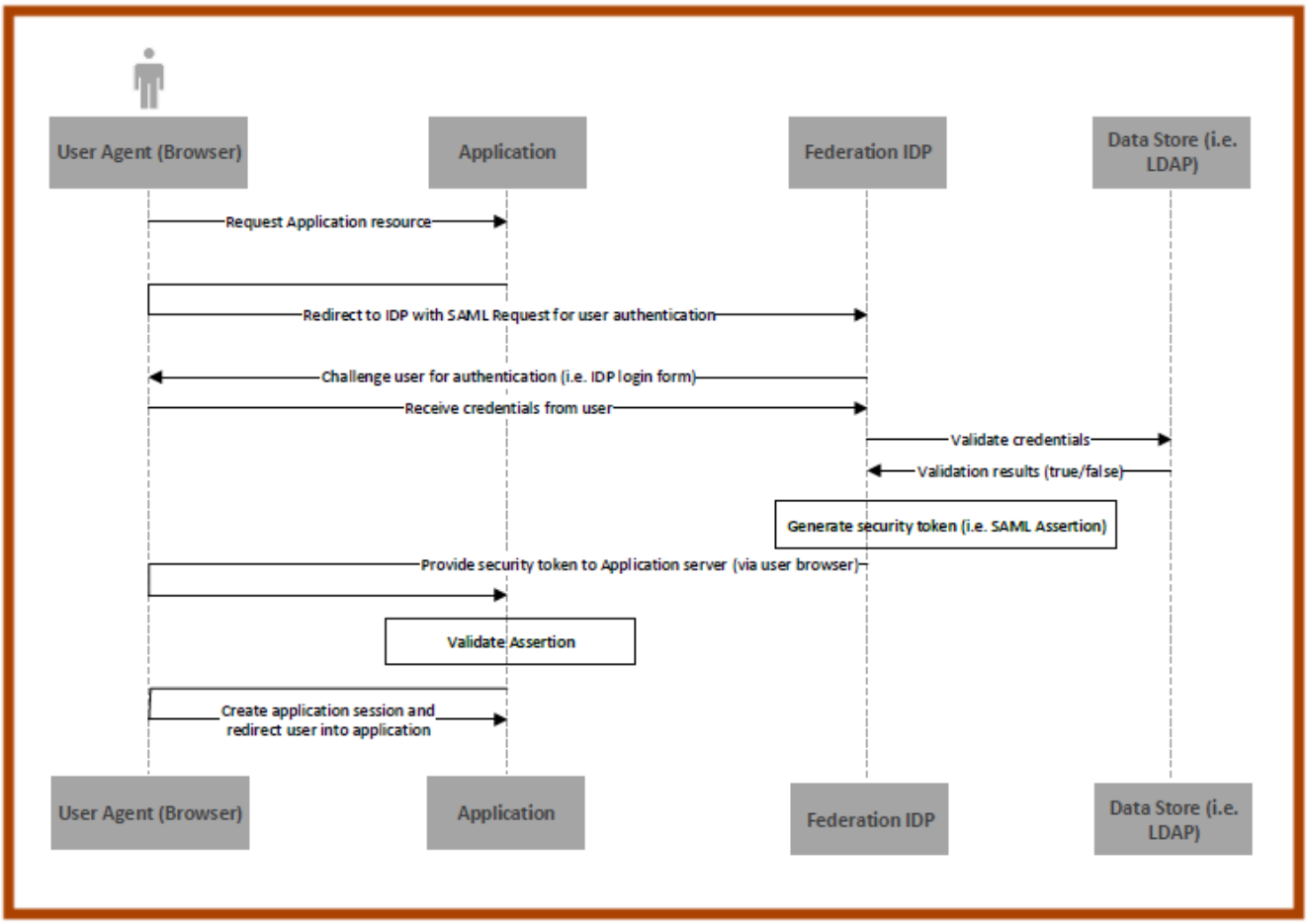

Fig 1: Screen Login Flow

1.3 SAML 2.0 Implementation

External Identity Provider (IP) handles the sign-in process and eventually provide the authentication to ORMB application users. Users are authenticated through SAML Assertion. 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.

1.3.1. 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 services using the SAML 2.0 protocol. The SAML 2.0 relying party for ORMB cloud service used in this scenario is IDCS.

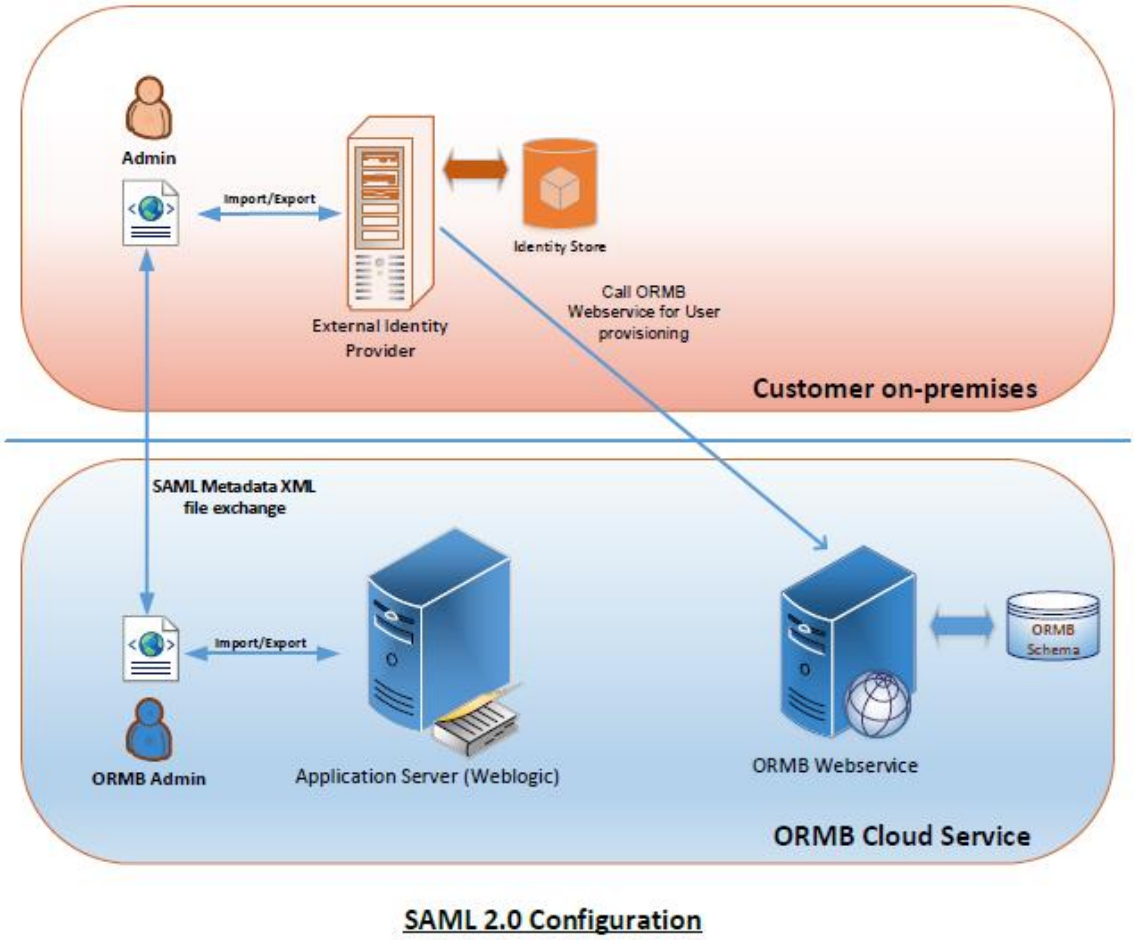

Fig2: SAML Configuration

1.3.2. SAML Metadata

SAML 2.0 Identity Provider adheres to information about the ORMB relying party. Application server publishes metadata. IDP imports ORMB's SAML metadata and thereby exchange public keys, IP addresses and communication information. Thus, ORMB application server 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 SAML2.0 metadata XML:

Fig 3: Sample SAML Metadata XML

Please note that the metadata XML varies from server to server.

1.3.3. 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 on how to do this, refer to the document: R7_REST_Services_Federated_Identity_Configuration.doc. User must be present in ORMB application.

1.4 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.

