Oracle® Revenue Management and Billing Cloud Service

Federated Identity Configuration Using IAM

Revision 1.0

F83797-01

July 2023

Oracle Revenue Management and Billing Cloud Service Federated Identity Configuration Using IAM

F83797-01

Copyright Notice

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 the following audience:

- System Administrators
- Consulting Team
- Implementation Team

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 using 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
IAM	Oracle Identity and Access Management
ID	Identity Domains

Acronym	Meaning
IDP	External Identity Provider
JWT	JSON Web Tokens
OCI	Oracle Cloud Infrastructure
OIDC	OpenID Connect
ORMB	Oracle Revenue Management and Billing
ORMBCS	Oracle Revenue Management and Billing Cloud Service
SAML	Security Assertion Markup Language
SP	Service Provider
SSO	Single Sign-On
WTSS	Web Tier Security Service

Related Documents

You can refer to the following documents for more information:

Document Name	Description
Oracle Revenue Management and Billing Cloud Service Release 8.1.1 Release Notes	Lists the feature enhancements and client platforms and browsers that are supported in this release. It highlights different roles and responsibilities of Oracle and Customer in deploying, configuring, and maintaining the Oracle Revenue Management and Billing Cloud Service. It also highlights the known issues in this release.
Oracle Revenue Management and Billing Cloud Service Licensing Guide	Lists different features which are offered when you acquire a license for the following cloud services: • Oracle Financial Services Revenue Management and Billing • Oracle Insurance Revenue Management and Billing It also provides the licensing information of Oracle software and third-party JARs and components which are included in the above-mentioned cloud services.
Oracle Revenue Management and Billing Cloud Service REST Services Configuration Guide	Explains how to configure federated Web service login to access protected REST services on the ORMB Cloud environments.

Document Name	Description
Oracle Revenue Management and Billing Cloud Service SFTP Authentication and Access Permissions Guide	Explains how to configure SFTP authentication for the ORMB Cloud Service. It also explains how to access the SFTP server using WinSCP, how to create the directories and files on the SFTP server, and how to set the read, write, and execute permissions for a file or folder on the SFTP server.
Oracle Revenue Management and Billing Cloud Service SaaS Reporting using OAS	Provides an overview of the ORMB SaaS reporting architecture. It also explains how to use Oracle Analytics Server for ORMB SaaS reporting.
Oracle Revenue Management and Billing Cloud Service End-User Onboarding Using IAM	Explains how to setup the security administrator account for the ORMB Cloud Service. It explains how to manage users and groups for the ORMB Cloud Service. In addition, it explains how to import and export bulk users and groups for the ORMB Cloud Service and how to use SAML on the Cloud environment for single sign-on.

Contents

1. Federated Single Sign-On using 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 and 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 is simple JSON-based identity tokens (JWT), delivered via OAuth 2.0 flows designed for web, browser-based and native or mobile applications.

ORMB Cloud Service uses ‘Authorization Code Flow’. This flow is the commonly used flow, intended for traditional web applications. It involves an initial browser redirection to and from the OpenID Provider or Identity Provider for user authentication and consent, then a second back-channel request is sent to retrieve the ID token. This flow offers optimal security, as tokens are not revealed to the browser and still the client can be authenticated.

Oracle Identity and Access Management (IAM) with Identity Domains is provided to the customer as part of the service subscriptions. Oracle Identity and Access Management (IAM) with Identity Domains is a built-in part of the Oracle Cloud Infrastructure, and it governs the access to Oracle Cloud Infrastructure’s resources along with Oracle Cloud Services.

ORMB Cloud Service provides two types of configuration options:

- Customer can integrate IAM with Identity Domains (as SP) with their On Premise Identity Provider using the SAML protocol
- Customer can leverage IAM with Identity Domains 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. The 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 Login Method 1

In the Login Method 1, the login process is as follows:

1. User accesses the ORMB Cloud Service 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 IAM.
4. An external identity provider as configured in IAM 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 IAM validates the assertion.
7. IAM 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 Cloud Service.

The following figure graphically illustrates the flow of Login Method 1:

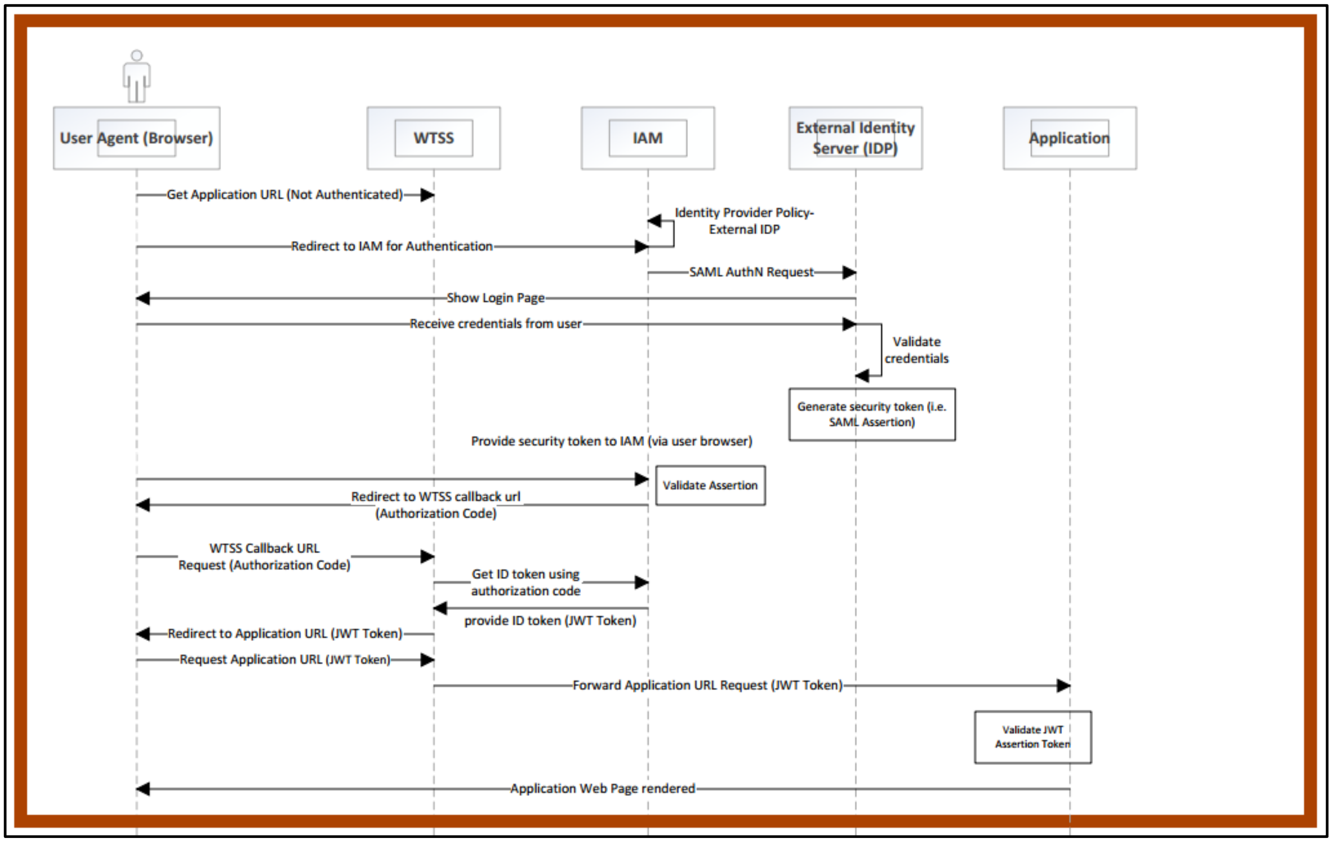

User Agent (Browser)
WTSS
IAM
External Identity Server (IDP)
Application
Get Application URL (Not Authenticated)
Identity Provider Policy- External IDP
Redirect to IAM for Authentication
SAML AuthN Request
Show Login Page
Receive credentials from user
Validate credentials
Generate security token (i.e. SAML Assertion)
Provide security token to IAM (via user browser)
Validate Assertion
Redirect to WTSS callback url (Authorization Code)
WTSS Callback URL Request (Authorization Code)
Get ID token using authorization code
provide ID token (JWT Token)
Redirect to Application URL (JWT Token)
Request Application URL (JWT Token)
Forward Application URL Request (JWT Token)
Validate JWT Assertion Token
Application Web Page rendered

Figure 1: Method 1 – Screen Login Flow

1.2.2 Login Method 2

In the Login Method 2, the login process is as follows:

1. User accesses the ORMB Cloud Service through the Web Tier Security Service (WTSS) URL.
2. WTSS on the ORMB application server intercepts the request and identifies the user is not authenticated.
3. WTSS redirects the user to the configured IAM. IAM challenges the user to enter the credentials.
4. IAM 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 Cloud Service.

The following figure graphically illustrates the flow of Login Method 2:

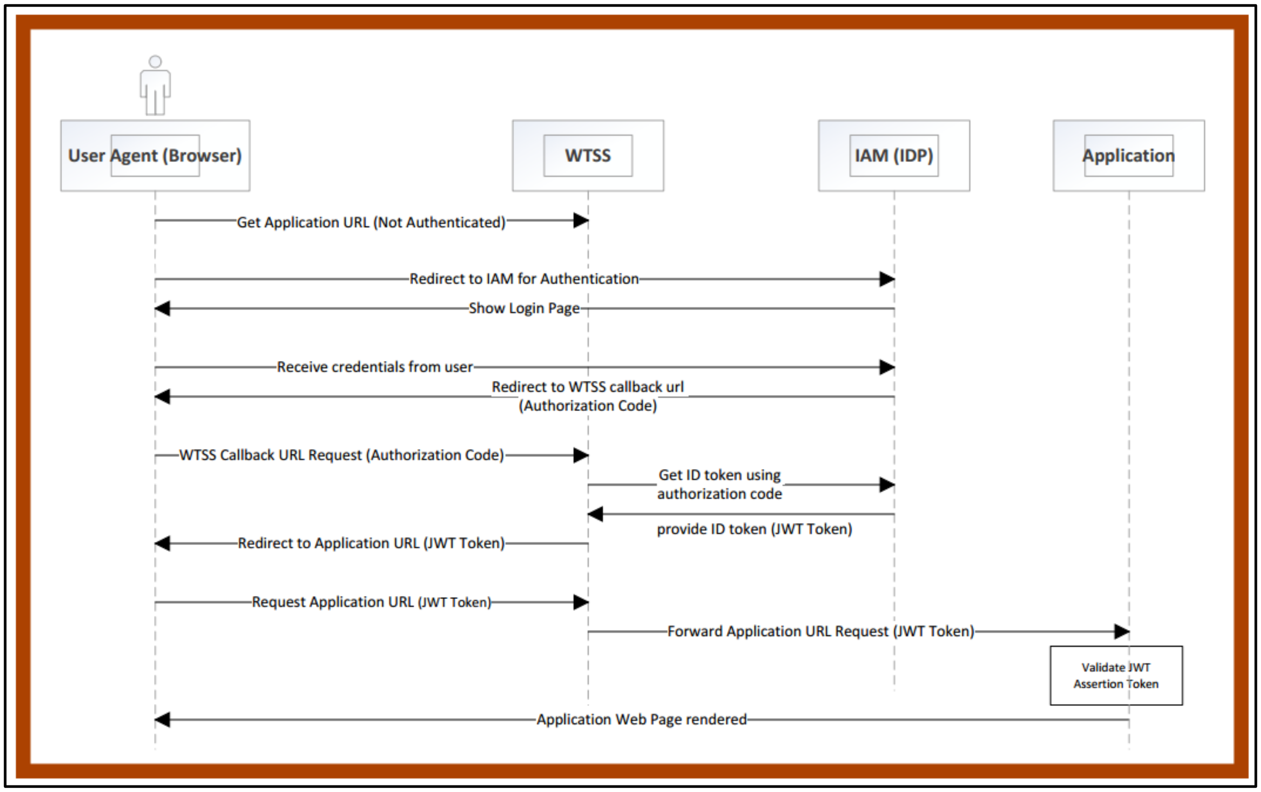

User Agent (Browser)
WTSS
IAM (IDP)
Application
Get Application URL (Not Authenticated)
Redirect to IAM for Authentication
Show Login Page
Receive credentials from user
Redirect to WTSS callback url (Authorization Code)
WTSS Callback URL Request (Authorization Code)
Get ID token using authorization code
provide ID token (JWT Token)
Redirect to Application URL (JWT Token)
Request Application URL (JWT Token)
Forward Application URL Request (JWT Token)
Validate JWT Assertion Token
Application Web Page rendered

Figure 2: Method 2 - Screen Login Flow

1.3 OpenID Connect Implementation

IAM OAuth key used for signing the JWT Access Token is imported in the ORMB application server (WebLogic) using chef automation script. These exchanges of signing keys will happen over SFTP or email. ORMB application server validates JWT Access Token through JWT Identity Assertor using JWT signing certificate.

1.4 SAML 2.0 Implementation (Only for Method 1)

External Identity Provider (IDP) will handle the sign-in process and will eventually provide the authentication to the ORMB Cloud Service users. Users are authenticated through SAML Assertion in IAM. 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 user data that is 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 graphically explains 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 IAM.

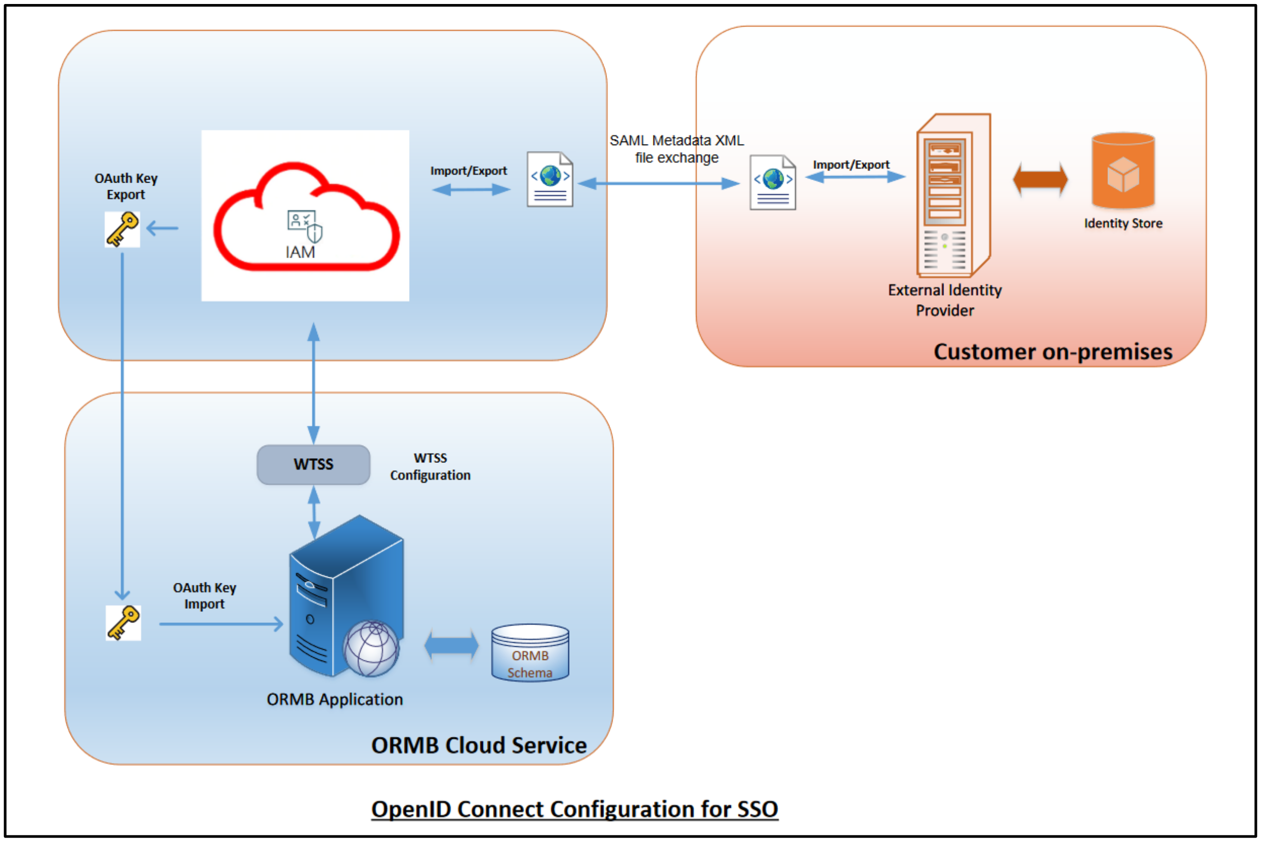
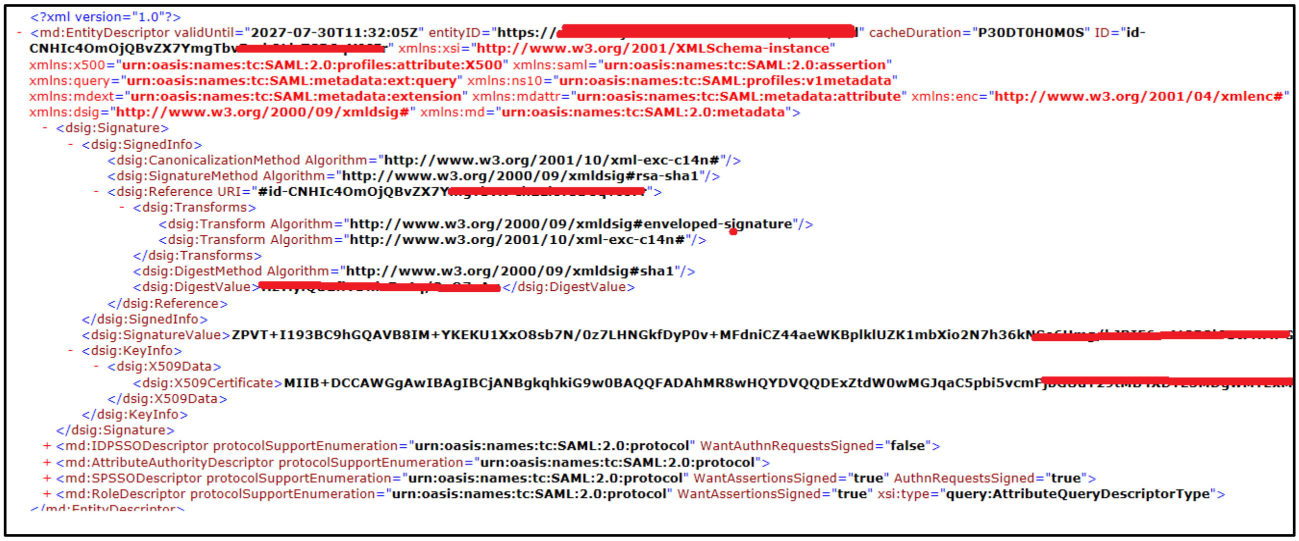


Figure 3: SAML Configuration

1.4.2 SAML Metadata

IDP imports IAM’s SAML metadata and thereby exchange public keys, IP addresses and communication information. Thus, Oracle IAM 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 figure illustrates a sample SAML 2.0 metadata XML:



```
  <?xml version="1.0"?>
- <md:EntityDescriptor validUntil="2027-07-30T11:32:05Z" entityID="https://[redacted]" cacheDuration="P30DT0H0M0S" ID="id-
  CNHIc4OmOjQBvZX7YmgTbv[redacted]" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500" xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
  xmlns:query="urn:oasis:names:tc:SAML:metadata:ext:query" xmlns:ns10="urn:oasis:names:tc:SAML:profiles:v1metadata"
  xmlns:mdext="urn:oasis:names:tc:SAML:metadata:extension" xmlns:mdattr="urn:oasis:names:tc:SAML:metadata:attribute" xmlns:enc="http://www.w3.org/2001/04/xmlenc#"
  xmlns:dsig="http://www.w3.org/2000/09/xmldsig#" xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata">
  - <dsig:Signature>
    - <dsig:SignedInfo>
        <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      - <dsig:Reference URI="#id-CNHIc4OmOjQBvZX7Y[redacted]">
        - <dsig:Transforms>
            <dsig:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
          </dsig:Transforms>
          <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <dsig:DigestValue>[redacted]</dsig:DigestValue>
        </dsig:Reference>
      </dsig:SignedInfo>
      <dsig:SignatureValue>ZPVT+I193BC9hGQAVB8IM+YKEKU1XxO8sb7N/0z7LHNGkfDyP0v+MFdniCZ44aeWKBplklUZK1mbXio2N7h36kN[redacted]
    - <dsig:KeyInfo>
      - <dsig:X509Data>
          <dsig:X509Certificate>MIIB+DCCAWGgAwIBAgIBCjANBgkqhkiG9w0BAQQFADAhMR8wHQYDVQQDExZtdW0wMGJqaC5pbi5vcmF[redacted]
        </dsig:X509Data>
      </dsig:KeyInfo>
    </dsig:Signature>
  + <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAuthnRequestsSigned="false">
  + <md:AttributeAuthorityDescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
  + <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" AuthnRequestsSigned="true">
  + <md:RoleDescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" xsi:type="query:AttributeQueryDescriptorType">
  </md:EntityDescriptor>
```

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

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 in an Identity Provider and then access service providers without additional authentication. Additionally, identity federation (linking of multiple identities) with SAML provides better customized user experience for each service while ensuring privacy.