

# Oracle Warehouse Management Cloud

---

## **SSO and Alternate Authentication Setup**

**Release 21D**



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 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" or commercial computer software documentation 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. Governments 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 and Java 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.

## Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website.

## Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit My Oracle Support or visit Accessible Oracle Support if you are hearing impaired.

# Contents

|                                                               |          |
|---------------------------------------------------------------|----------|
| <b>Preface</b>                                                | <b>i</b> |
| <hr/>                                                         |          |
| <b>1 Oracle WMS Cloud Alternate Authentication Mechanisms</b> | <b>1</b> |
| Identity Providers                                            | 1        |
| WMS Configuration for Alternate Authentication                | 1        |
| Built-in Authentication                                       | 1        |
| OAuth2 Authentication                                         | 2        |
| <b>2 SSO Authentication</b>                                   | <b>5</b> |
| Technical Configuration for SSO                               | 5        |
| IDCS SSO Information                                          | 6        |
| Azure AD SSO Authentication                                   | 6        |



# Preface

Oracle® Warehouse Management Cloud SSO and Alternate Authentication Setup, Release 21D

Part No. F46339-01

This guide describes in detail how to configure and use Oracle Warehouse Management (WMS) Cloud. All functionality unless specifically noted is available in Oracle Warehouse Management Enterprise Edition Cloud. Please direct any functionality questions to [My Oracle Support](#).

## Change History

| Date      | Document Revision | Summary of Changes |
|-----------|-------------------|--------------------|
| 5/26/2021 | -01               | Updates for 21C.   |

## Using Applications

### Additional Resources

- **Community:** Use [Oracle Cloud Customer Connect](#) to get information from experts at Oracle, the partner community, and other users.
- **Guides and Videos:** Go to the [Oracle Help Center](#) to find guides and videos.
- **Training:** Take courses on Oracle Cloud from [Oracle University](#).

### Conventions

The following table explains the text conventions used in this guide.

| Convention             | Meaning                                                                                           |
|------------------------|---------------------------------------------------------------------------------------------------|
| <b>boldface</b>        | Boldface type indicates user interface elements, navigation paths, or values you enter or select. |
| <code>monospace</code> | Monospace type indicates file, folder, and directory names, code examples, commands, and URLs.    |
| >                      | Greater than symbol separates elements in a navigation path.                                      |

# Contacting Oracle

## Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit [My Oracle Support](#) or visit [Accessible Oracle Support](#) if you are hearing impaired.

# 1 Oracle WMS Cloud Alternate Authentication Mechanisms

Oracle® Fusion Cloud Warehouse Management includes a built-in authentication mechanism using which users can be setup with their own user-id and passwords to access the Oracle Warehouse Management (WMS) Web UI, WMS Cloud Mobile App and Mobile RF applications. In addition, it also supports authenticating users against external identity providers (IDP). It supports multiple authentication mechanisms:

- SAML2 Single Sign On, or SSO in short
  - A web-based authentication standard that can be used only to login to the WMS Web UI
- OAuth2
  - Another authentication standard that can be used for the WMS Web UI, the WMS Cloud Mobile App and Mobile RF.

## Identity Providers

Oracle Identity Cloud Service (IDCS) and Azure AD/ADFS are Identity Providers that have been tested with Oracle WMS Cloud. Other providers that support these standards may also work. Customers can request their environments to be configured to use SSO and/or OAuth2 by raising a Service Request (SR). Oracle will provide a template via the SR for customers to fill out certain technical pieces of information which will be used by our Cloud operations team to configure the customers environment.

## WMS Configuration for Alternate Authentication

Once the WMS Cloud environment has been setup for SSO or OAuth2 authentication, usernames in WMS Cloud have to be associated with a corresponding username in the external Identity Provider. This is the “Alternate username” field in WMS Cloud and must be of the format:

<username>@<domain>

WMS Cloud users can be created/configured from the Users screen or by uploading a User Excel file from the Input Interface screen.

It is possible to have some WMS users be locally authenticated (add note about temp users) and others externally authenticated. It's possible to have both SSO and OAuth2 backends configured for one customer.

## Built-in Authentication

The user types in the username and password on the WMS Cloud login page, whether the Web, Mobile App, or Mobile RF device. The encrypted credentials are validated against the WMS Cloud Service.

## OAuth2 Authentication

The user types in the username and password on the WMS Cloud login page, whether the Web, Mobile App or Mobile RF device. The encrypted credentials are sent to the WMS Cloud Service. If the username has an associated “alternate username”, WMS Cloud will delegate the authentication to the external identity provider and validate against that service. If the authentication succeeds, the user is logged into the WMS.

OAuth2 backends that have been validated with WMS Cloud are Oracle IDCS and Azure AD.

## Technical Configuration for OAuth2

**Note:** Federation and MFA (Multi Factor Authentication) are not supported. The OAuth2 flow only supports the ROPC (Resource Owner Password Credentials) grant type, as defined here:

<https://tools.ietf.org/html/rfc6749#section-4.3>

When submitting an SR to [My Oracle Support](#) to setup OAuth2 authentication, you need to provide the data per the table below. The technical details are explained in the reference links below.

### Oracle IDCS Reference

<https://docs.oracle.com/en/cloud/get-started/subscriptions-cloud/csimg/obtaining-access-token-using-user-credentials-client-assertion.html>

### Azure AD Reference

<https://docs.microsoft.com/en-us/azure/active-directory/develop/v2-oauth-ropc>

| Item                        | Description                                  |
|-----------------------------|----------------------------------------------|
| Identity Provider Name      | Name of IDP such as Azure AD or Oracle IDCS. |
| Endpoint URL                | Used by the WMS to authenticate              |
| Client ID                   | Needed for Oracle IDCS and Azure AD          |
| Client Secret               | Needed for Oracle IDCS and Azure AD          |
| Resource/Scope              | Needed for Oracle IDCS and Azure AD          |
| X-USER-IDENTITY-DOMAIN-NAME | Needed for Oracle IDCS                       |

| Item        | Description                                                                                                                                                                                                                                                                                                                                                 |
|-------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Domain name | <p>Used to link WMS username with the OAuth2 username, using "Alternate username"</p> <p>For example if the username is "jdoe"@somedomain.com, then the domain name is somedomain.com.</p> <p><b>NOTE:</b> Customers need to provide ALL domains that they need for WMS. We don't support generic consumer domains (for example: @yahoo.com @gmail.com)</p> |



## 2 SSO Authentication

SAML2 SSO works a bit differently. The username and password are not entered in the WMS Cloud login page. The user instead clicks the “Login using SSO” button (which will be available after the SSO configuration has been setup by following SR process mentioned earlier). The page gets redirected to the Identity Provider’s login page where the user will login using their username linked to the IDP (this is stored in the “Alternate username” field in WMS Cloud). If the authentication succeeds, a token is returned back to the WMS Cloud and the user is logged in to the application.

**Note:** SAML2 being a web-based standard, this mechanism can be used only to login to the WMS Cloud web UI. RF or App login will have to use either local authentication or OAuth2 authentication. It is possible for the same user to be linked to both SAML2 SSO and OAuth2 backends (the IDP has to be the same in this case), so the same user can login via SSO to the Web UI and via OAuth2 on the RF. SAML2 SSO backends that have been validated against WMS Cloud are Oracle IDCS and Azure AD.

## Technical Configuration for SSO

For SAML2 SSO setup, the customer and Oracle exchange certain technical information needed to configure both systems.

| Customer Provides                                                                                                                                                                                  | Oracle provides                                                                                                                                                                           |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>SAML2.0 Metadata including signing certificate.</li> <li>For some IDPs customer may also need to provide additional information (details below).</li> </ul> | <ul style="list-style-type: none"> <li>Application Service Provide ID</li> <li>The public key for request signing</li> <li>SAML assertion URL</li> <li>Other IDP configuration</li> </ul> |

### Customer provided information:

The customer configures their IDP for Cloud WMS authentication, generates the SAML2 Metadata file, and sends it to Oracle. IDPs that support SAML2 SSO will have a mechanism to generate this file, including Oracle IDCS and Azure AD.

**SAML2.0 MetaData** - Customer must provide IDP metadata for SAML2.0, it can be provided in a metadata.xml file or a URL allowing Oracle to download the IDP metadata from customer site.

The specific fields that are used by Oracle are explained below. In addition, for IDCS, the MyApp URL is also needed (details below) and has to be sent separately as its not part of the metadata file.

## IDCS SSO Information

| Item                                                              | Description                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Issuer ID                                                         | Unique identifier of the IDP                                                                                                                                                                                                                                                                                                                      |
| MyApp URL                                                         | The binding that is used to send the response to the Identity provider.<br><br><b>NOTE:</b> IDCS also has an SSO_URL which is different. The Metadata does not include the MyApp URL                                                                                                                                                              |
| Response signature certificate<br>(X509 Certificate) – PEM format | Will verify tokens signed by IDCS                                                                                                                                                                                                                                                                                                                 |
| Domain name                                                       | Used to link WMS username with the SSO username, using "Alternate username"<br><br>For example if the username is "jdoe"@somedomain.com, then the domain name is somedomain.com.<br><br><b>NOTE:</b> Customers need to provide ALL domains that they need for WMS. We don't support generic consumer domains (for example: @yahoo.com @gmail.com) |

**Note:** An app has to be created in IDCS using the ROPC grant type. This is required for WMS to authenticate using IDCS.

## Azure AD SSO Authentication

| Item                                                              | Description                                                             |
|-------------------------------------------------------------------|-------------------------------------------------------------------------|
| Issuer ID                                                         | Unique identifier of the IDP                                            |
| Single Sign-On URL                                                | The binding that is used to send the response to the Identity provider. |
| Response signature certificate<br>(X509 Certificate) – PEM format | Will verify tokens signed by the IDP                                    |

| Item        | Description                                                                                                                                                                                                                                                                                                                                              |
|-------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Domain name | <p>Used to link WMS username with the SSO username, using "Alternate username"</p> <p>For example: if the username is jdoe @somedomain.com, then the domain name is somedomain.com.</p> <p><b>NOTE:</b> Customers need to provide ALL domains that they need for WMS. We don't support generic consumer domains (for example: @yahoo.com @gmail.com)</p> |

**Note:** The SSO assertion returned by the IDP must contain NameID tag with the alternate username configured in our application as the value. We will use that to look up a user and create a session. Example assertion with NameID:

```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ...>
...
<saml:Subject>
<saml:NameID>username@domain</saml:NameID> ...
</saml:Subject>
...
</saml:Assertion>
```

