

Configuring Oracle Identity Cloud Service for Single Sign-On (SSO) with Oracle Aconex

Oracle Identity Cloud Service (IDCS)
configuration for accessing Oracle Aconex through
SSO via the Construction and Engineering Lobby

January, 2022, Version 0.1
Copyright © 2022, Oracle and/or its affiliates
Public

Oracle Identity Cloud Service (IDCS) configuration for accessing Oracle Aconex through SSO via the Construction and Engineering Lobby

Who this document is for

Configuring SSO requires a knowledge of SAML concepts and access to your company's Identity Provider (IdP) to add configurations. This will normally be a member of the IT or Identity team within your company.

Your IdP will typically be a system such as Microsoft Azure Active Directory or other product.

You will need an Oracle Identity Cloud Service (IDCS) company account

A Foundation license for IDCS is provided with our Cloud SaaS products such as Aconex. If your company already has an IDCS company account (often because they use other Oracle products), it's usually best to use the same account for access to Aconex.

If no account is currently available, your Oracle account team will arrange for this to be created.

Configuring your IDCS company account

How to configure IDCS to use your Identity Provider for SSO.

Step 1: Start configuration of SAML-based integration of your IdP

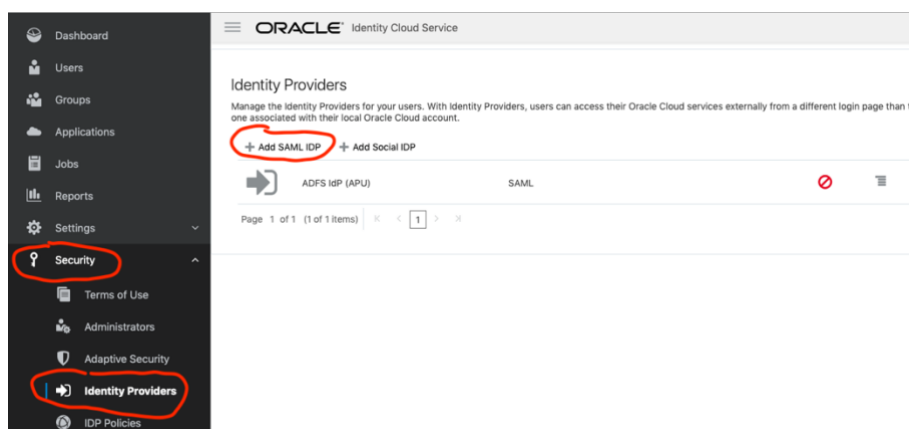
Details of this step are specific to your IdP application and provider (Microsoft Azure Active Directory, Microsoft ADFS, Okta etc.), but for all SAML-based IdP integrations the process is similar.

Follow your application's instructions to create a new SAML-based integration. This will involve downloading a Federation Metadata XML file that you will later import into IDCS. Once IDCS setup is complete you can return to your IdP SAML setup screen (it's good to have it open in the other window) and complete it the process.

Once you have the Federation Metadata XML file, the first stage of your IdP setup is now complete – you will return to complete this later. You can now continue to set up your IDCS configuration.

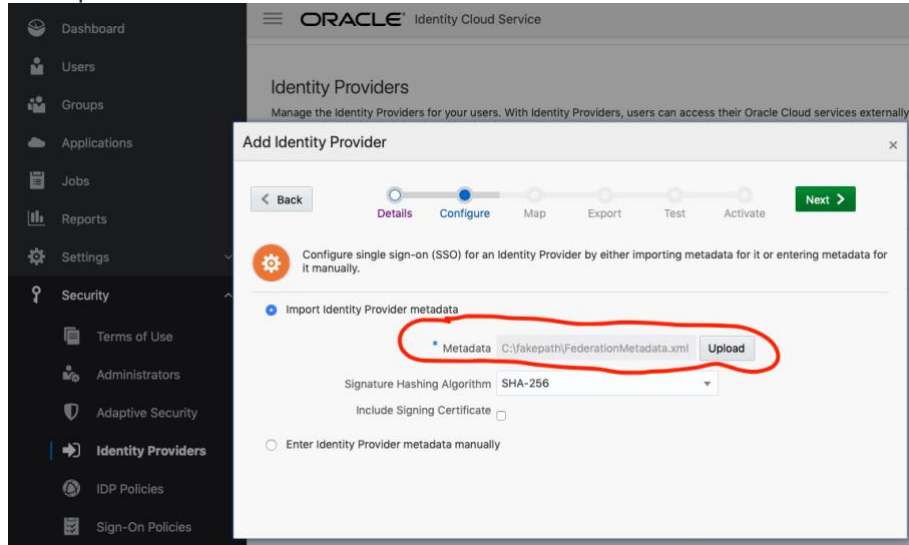
Step 2: IDCS Configuration

Once you have the Federated Metadata XML file from your IdP, switch to IDCS.

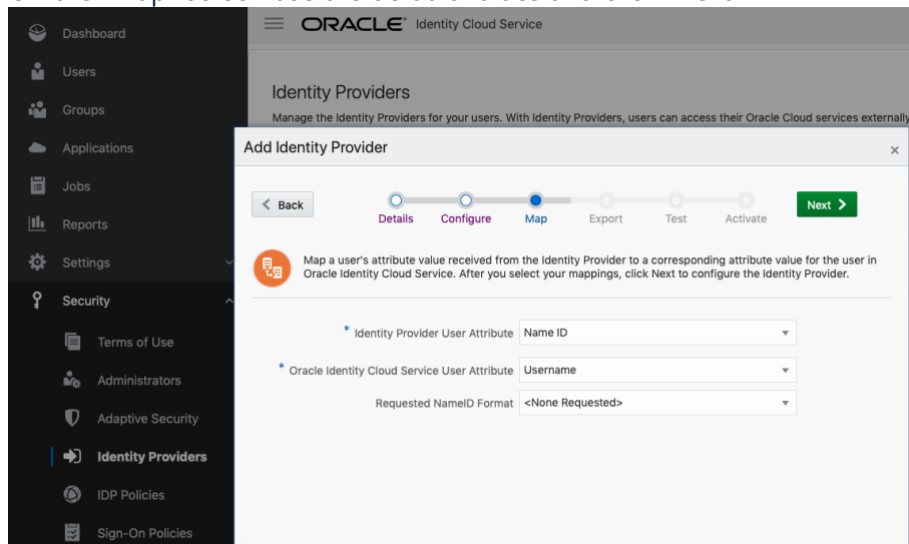


1. Sign in to the IDCS Admin Console :
<https://<idcs-tenant-id>.identity.oraclecloud.com/ui/v1/adminconsole>
2. Click on the menu in upper-left corner, select "Security" section and then the "Identity Providers" item.
3. Click on "+Add **SAML** IDP" - to create a new SAML-based link to an identity provider

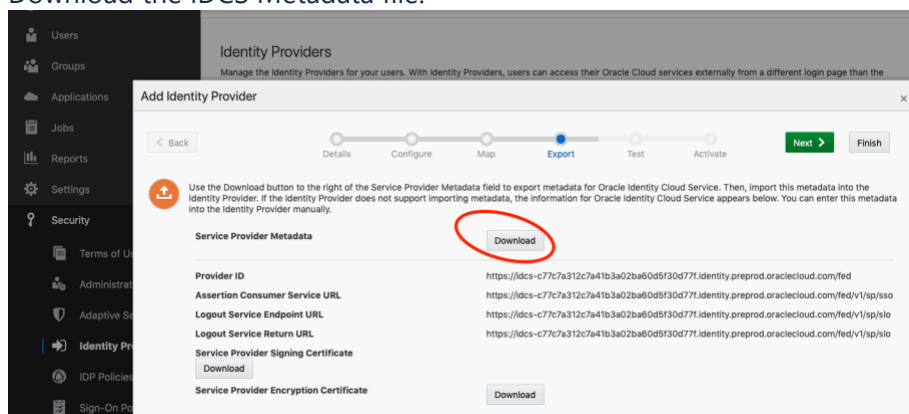
4. Upload the Federated Metadata XML file that you downloaded from your SAML IdP in Step 1.



5. On the "Map" screen use the default values and click "Next"



6. Download the IDCS Metadata file.



Now switch back to your SAML IdP to complete its setup.

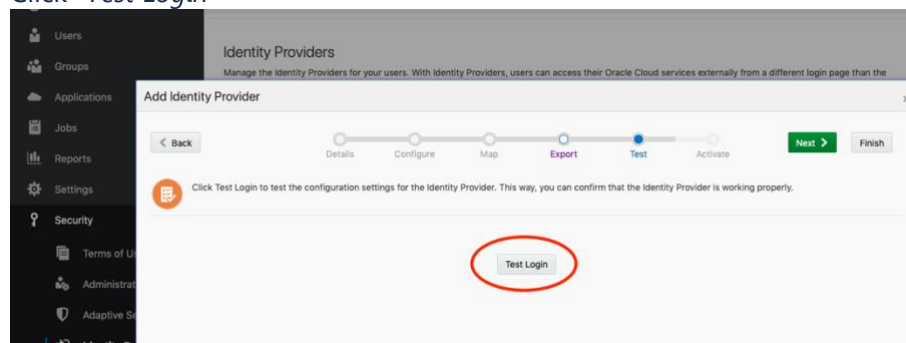
Step 3: Finish configuration in your IdP

You can now return to the configuration of your IdP service.

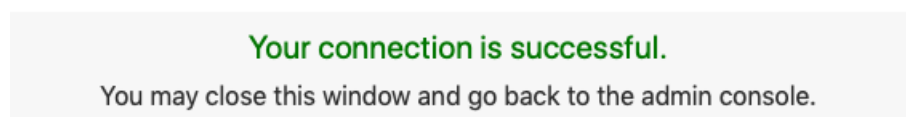
1. Follow your IdP application's process to **upload a metadata file** and upload the Federated Metadata XML file that you downloaded from IDCS.
2. After the upload you should see a screen indicating URLs and other info, taken from metadata file.
3. Confirm that the user identity is based on the user's email address.
4. Typically IdPs have policies or groups that indicate if a user is eligible to use a configured SAML provider. Confirm that users are added to those groups or policies in your IdP if required.
5. At this point both your IdP and IDCS are fully configured and ready for testing. Switch back to IDCS window and use its test capabilities.

Step 4: Test and finish configuration in IDCS

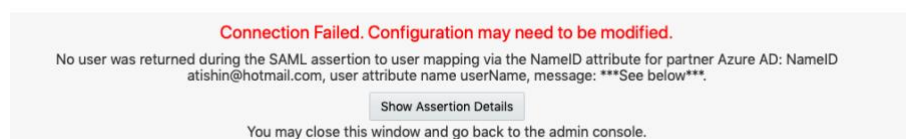
1. Click "Test Login"



2. You will be presented with your IdP's sign-in screen. Enter valid credentials for a user that exists in your IdP that is configured to use the SAML Federation App. A user account with same email must also exist in IDCS. You will need to ensure a user is created for testing and this user will be a member of the Lobby organization and able to access projects through the Lobby after setup is successfully completed.
3. If the test sign-in was successful you will see following message.



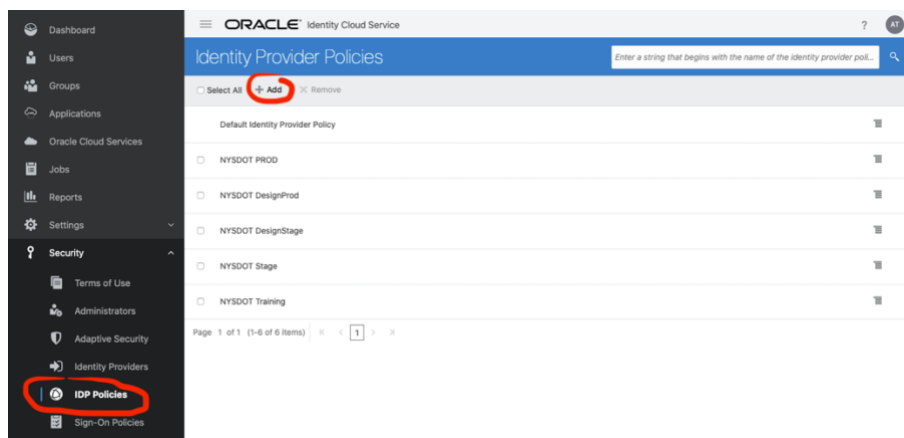
If the test login failed you will see a screen similar to one below. Please read the error description to amend the setup or creating missing data:



Step 5: Create an IdP Policy in IDCS

By default, IDCS offers its native login screen with an optional list of external IdPs at the side. By setting up an IdP policy for an IdP and Application pair we can avoid that step and present the user your IdP's login screen right away.

Click “Add” to create a new Identity Provider Policy.



Questions?


If you have questions about these changes, either contact your Oracle account team or [Aconex Support](#).

Connect with us

Call +1.800.ORACLE1 or visit oracle.com. Outside North America, find your local office at: oracle.com/contact.

 blogs.oracle.com

 facebook.com/oracle

 twitter.com/oracle

Copyright © 2022, Oracle and/or its affiliates. All rights reserved. This document is provided for information purposes only, and the contents hereof are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document, and no contractual obligations are formed either directly or indirectly by this document. This document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior written permission.

This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased, until authorization is obtained.

Oracle and Java are registered trademarks of Oracle 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. 0120

Disclaimer: If you are unsure whether your data sheet needs a disclaimer, read the revenue recognition policy. If you have further questions about your content and the disclaimer requirements, e-mail REVREC_US@oracle.com.

5 Data Sheet

Configuring Oracle Identity Cloud Service for Single Sign-On (SSO) with Oracle Aconex / Version 1.0

Copyright © 2022, Oracle and/or its affiliates / Public

ORACLE