ORACLE

Oracle Guided Learning: Transitioning to SSO

This document covers the transition in the Oracle Guided Learning (OGL) sign-in process to Oracle SSO and provides instructions on how to associate your email address to an Oracle SSO profile.

June 2023, Version 1.2
Copyright © 2023, Oracle and/or its affiliates
Public

Table of contents

Overview of Single Sign-On (SSO) 3

Why is OGL transitioning to SSO? 3

New OGL Account Sign In Page 4

Copyright © 2023, Oracle and/or its affiliates / Public

Overview of Single Sign-On (SSO)

What is Single Sign-On?

Single Sign-On (SSO) is an authentication method that enables users to securely authenticate ("sign in") with multiple websites and online applications by using just one set of credentials.

How Does SSO Work?

SSO works based upon a trust relationship that is established between an application, called a "service provider", and an "identity provider". This trust relationship usually involves the exchange of a certificate between the identity provider and the service provider. This certificate can be used to sign identity information that is being sent from the identity provider to the service provider so that the service provider knows it is coming from a trusted source. With SSO, this identity data takes the form of tokens which contain identifying information about the user like a user's email address or a username.

A typical SSO login flow:

1. A user browses to the application or website they wish to access (the "Service Provider").
2. The Service Provider sends a token containing some information about the user, such as an email address, to the SSO system (the "Identity Provider"), as part of a request to authenticate the user.
3. The Identity Provider first checks to see whether the user has already been authenticated, in which case it will grant the user access to the Service Provider application and skip to step 5.
4. If the user hasn't logged in, they will be prompted to do so by providing the credentials required by the Identity Provider. This could simply be a username and password, or it might include some other form of authentication like a One-Time Password (OTP) or Multi-Factor Authentication (MFA).
5. Once the Identity Provider validates the credentials provided, it will send a token back to the Service Provider confirming a successful authentication.
6. This token is passed through the user's browser to the Service Provider.
7. The token that is received by the Service Provider is then validated according to the trust relationship that was set up between the Service Provider and the Identity Provider during the initial configuration.
8. The user is granted access to the Service Provider.

When the user tries to access a different website, the new website would need to have a similar trust relationship configured with the SSO solution and the authentication flow would follow the same steps above.

Why is OGL transitioning to SSO?

To meet Oracle security compliance requirements and to align with industry security best practices, Oracle Guided Learning (OGL) is transitioning to SSO to provide more enhanced security and data privacy for our customers and users.

Why should I switch to SSO?

Key benefits:

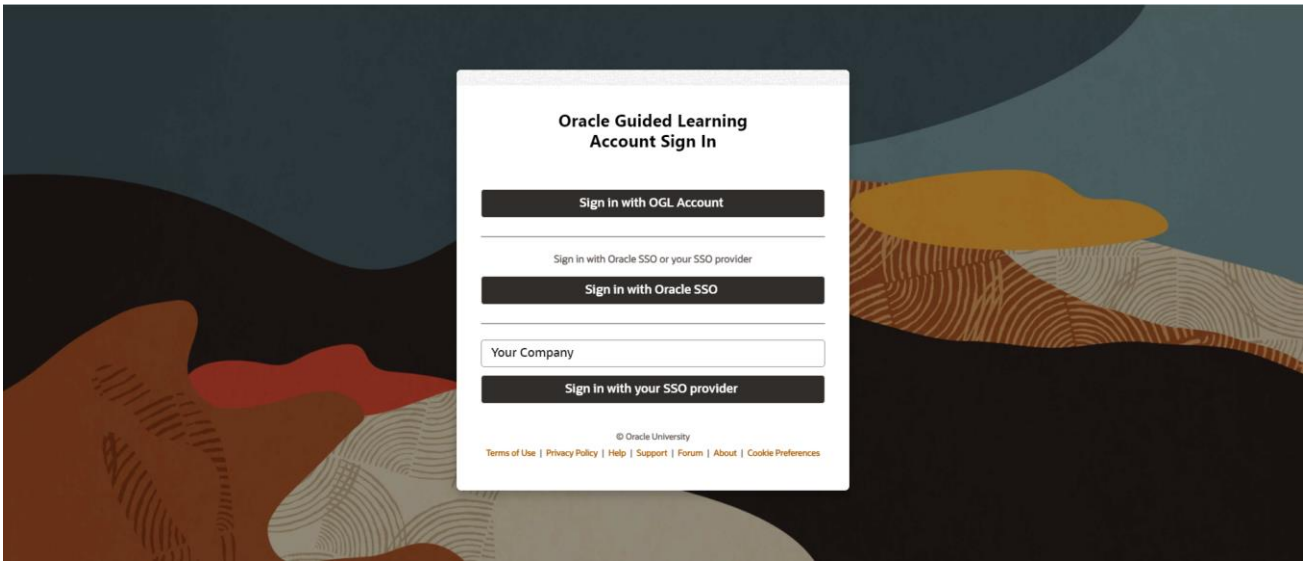
- Enhanced security and privacy of your data.
- More simplified authentication process. You only need to sign in once!
- Fewer passwords to manage.
- Unified sign in experience with other applications that use.
- More efficient password reset process if you forget your password.

Copyright © 2023, Oracle and/or its affiliates / Public

New OGL Account Sign-In Page

Beginning in OGL 23C Release, users will experience a newly updated OGL Account Sign In screen and process (see screenshot below).

Screenshot of new OGL Sign In Page:



Users will have 3 options with which to sign-in to the OGL Console:

- **Option 1: Sign In with OGL Account** – Use your current OGL username and password. This is the current OGL sign-in process but will be removed in a future release.
- **Option 2: Sign In with Oracle SSO** – Use your Oracle account. This is the same sign-in you use for other Oracle applications, like Cloud Customer Connect. If you don't have an Oracle account, you can easily create one.
- **Option 3: Sign In with your SSO provider** – If your company uses an SSO provider, check with your network administrator to see if it has been integrated with OGL. If yes, you can sign-in to OGL using your company's SSO. If no, use Option 2 above.

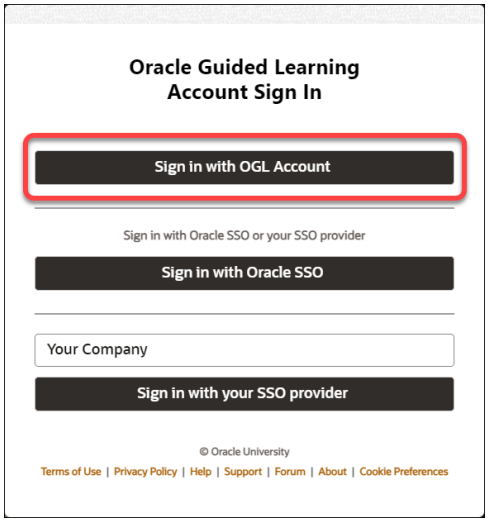
  Important: We strongly recommend all OGL users to transition to SSO soon (Options 2 or 3 above) as the current OGL sign-in option will be removed in a future release and will no longer be supported.

Copyright © 2023, Oracle and/or its affiliates / Public

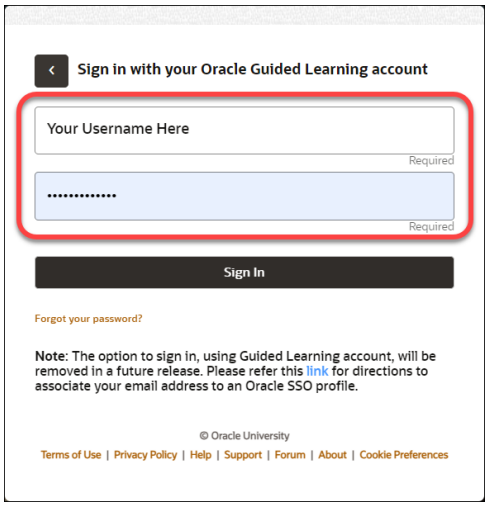
Option1: Sign In with OGL Account

Note: This sign-in option will be removed in an upcoming OGL release and no longer supported. We recommend that you transition to using your Oracle account to sign-in to OGL. See **Option 2** below.

1. To sign-in with your current OGL username and password, select the **Sign In with OGL Account** button in the Oracle Guided Learning Account Sign In screen:



2. This opens the **Sign in with your Oracle Guided Learning account** screen



3. Enter your current OGL username and password.

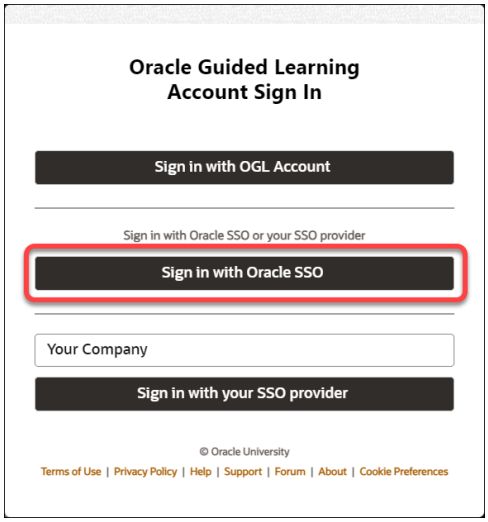
4. Select the **Sign In** button to continue to the OGL console.

Copyright © 2023, Oracle and/or its affiliates / Public

Option 2: Sign In with Oracle SSO (Recommended)

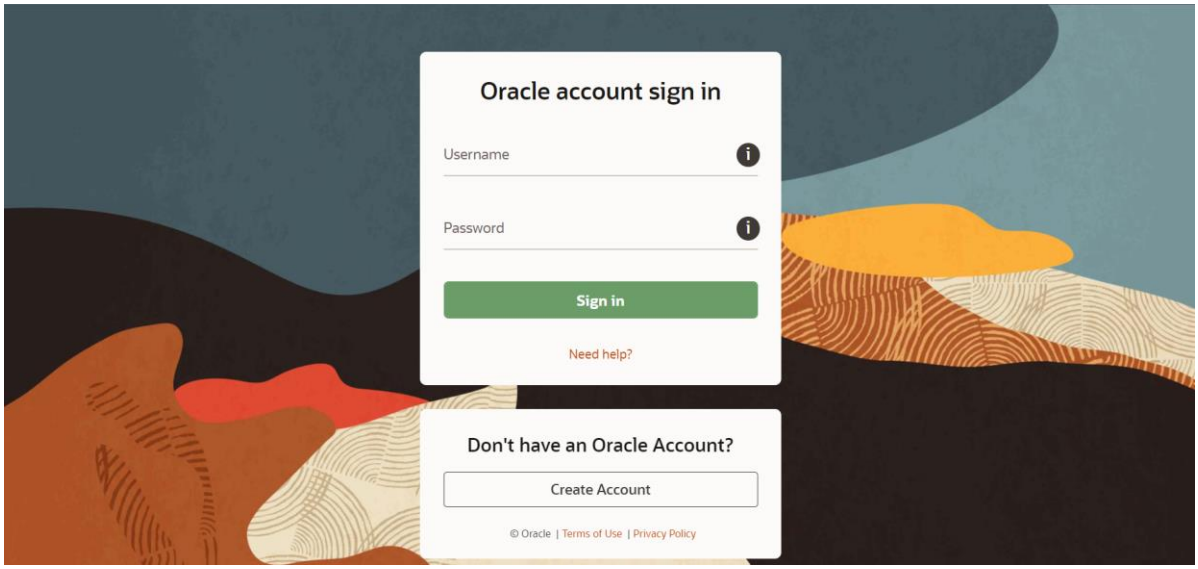
If you already have an Oracle account for other Oracle applications, such as Cloud Customer Connect or Oracle My Learn, you're already setup! Just sign in using your existing Oracle account. If you don't have an Oracle account, you can easily create one.

1. Select the **Sign In with Oracle SSO** button in the OGL Account Sign In screen:



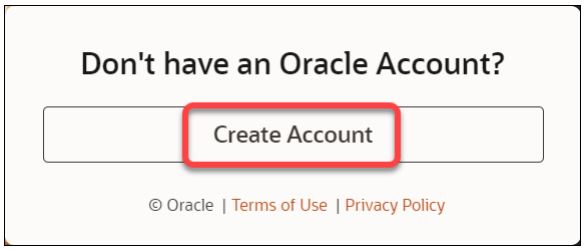
2. If prompted, enter your Oracle account username and password into the appropriate fields, then select **Sign In**.

   (**Note**: If you are already signed into your Oracle account through another application within the same browser, the sign in process will bypass the following screen and take you directly into the OGL console.)

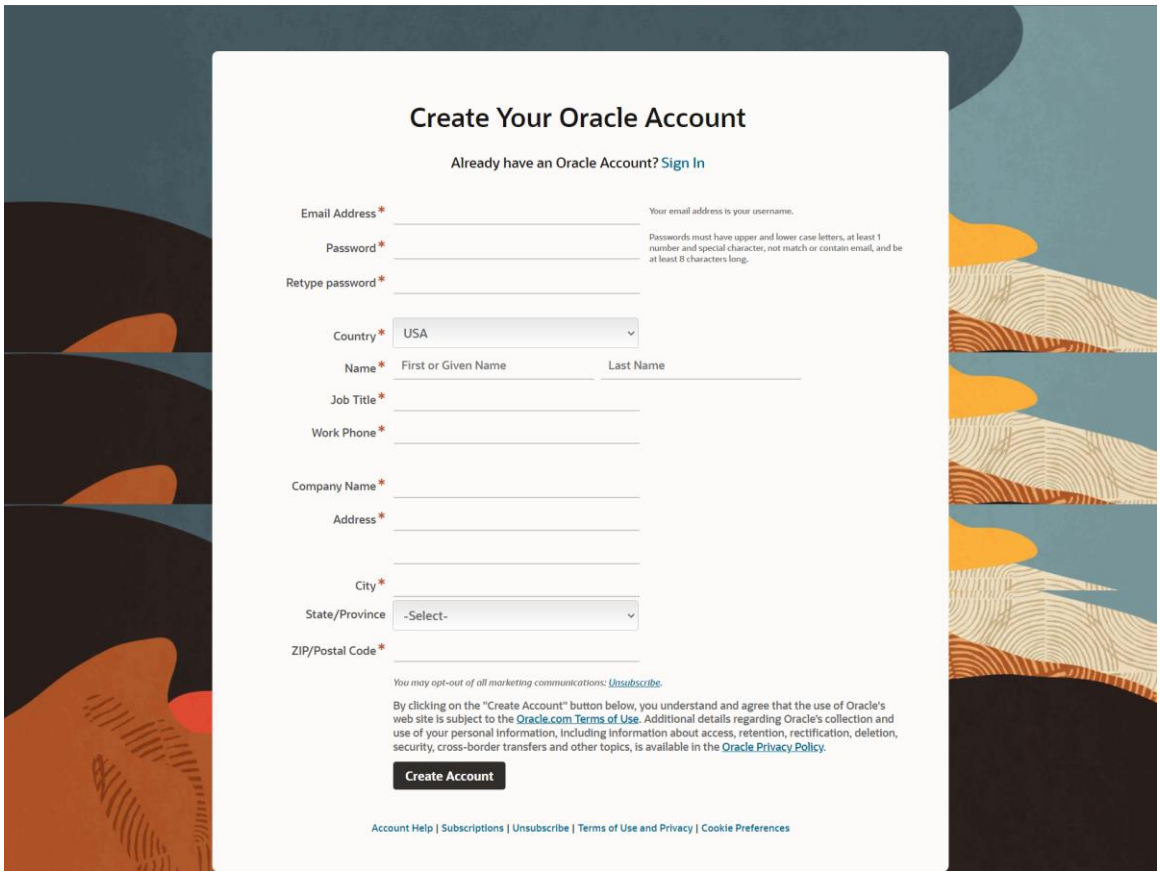


Copyright © 2023, Oracle and/or its affiliates / Public

3. If you do **not** currently have an Oracle account and wish to create one, select the **Create Account** link.



4. In the **Create Your Oracle Account** page, fill in all the required fields on the webform and be sure to use the same email address that you use for your OGL account.



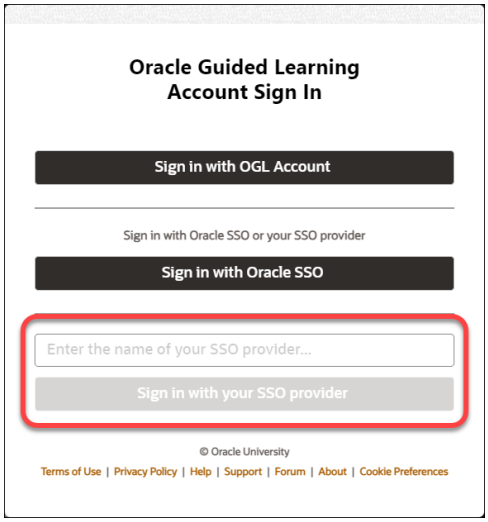
5. Once you've completed the webform, select the **Create Account** button. Then proceed back to Step 1 above to sign in using Oracle SSO.

Copyright © 2023, Oracle and/or its affiliates / Public

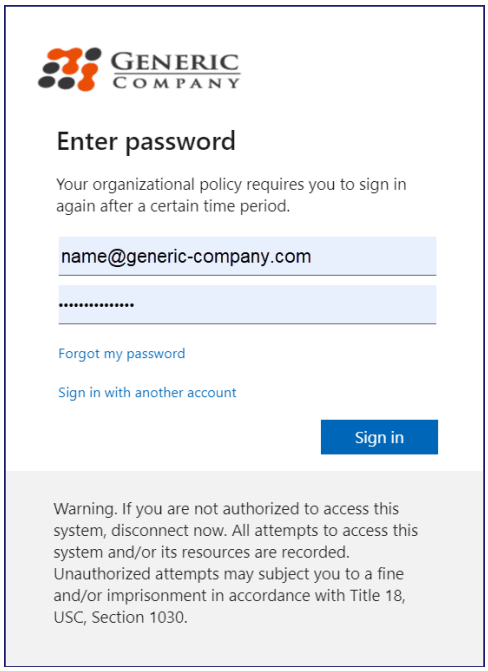
Option 3: Sign In with your SSO provider

Use this option if your company already uses an SSO provider and has integrated it with OGL. If you are unsure whether your company SSO is approved for use with OGL, please contact your network administrator for further instructions.

1. To sign in with your SSO provider, enter the name of your SSO provider (this is commonly your company name), then select the **Sign In with your SSO provider** button in the OGL Account Sign In screen:



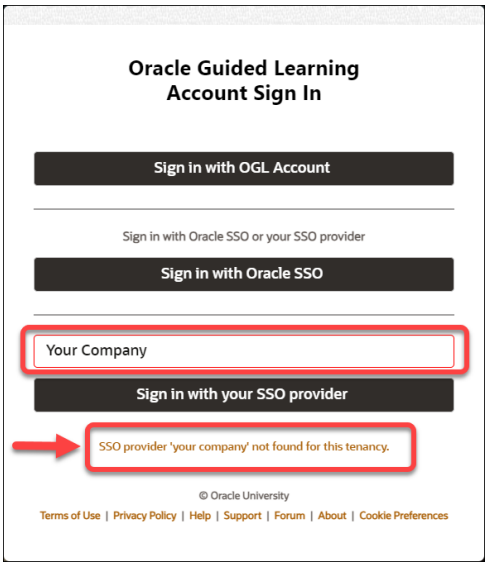
2. This will open your SSO provider's sign in screen. (Below screenshot is just an example) Enter your SSO username and password and sign in, as directed by your SSO provider.



If successful, you will be signed in to the OGL console.

Copyright © 2023, Oracle and/or its affiliates / Public

Note: If you see the error message below, this means that your SSO provider has not yet been integrated with OGL. Please contact your network administrator for further instructions.



In the meantime, you can still sign in to OGL using your existing OGL Account or Oracle SSO (See **Options 1 & 2** above.)

Copyright © 2023, Oracle and/or its affiliates / Public

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 © 2023, 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.