PORTAL

PORTAL

SSO Instructions

gdportal.gdg.travel

18 September 2024

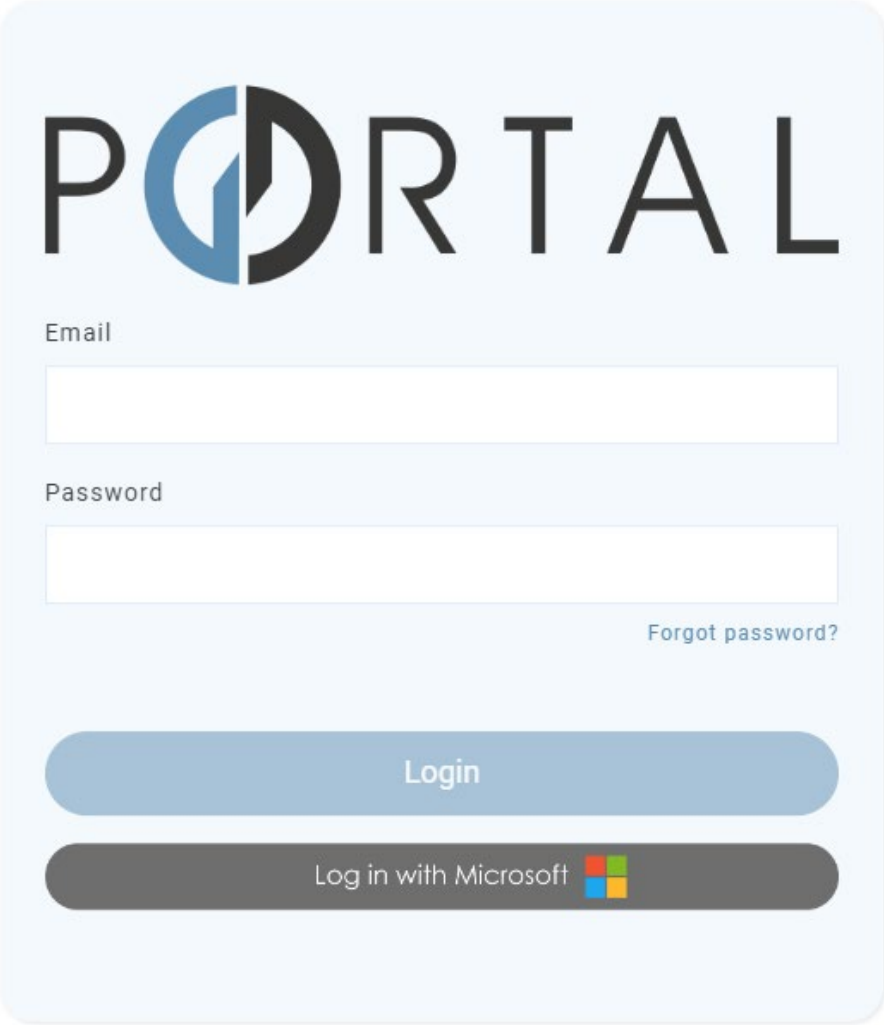
GRAY DAWES TRAVEL

GDPortal.gdg.travel supports SSO and MFA via Microsoft Azure Active Directory (now called Entra).

Your company will need to using Azure AD (Entra) as its identity and access manager. (Note, you will already be using this if you are using any of the Office365/Exchange online platforms). To ensure seamless integration with Azure Entra Single Sign-On (SSO), we require each user's Microsoft login ID. Please confirm if the Microsoft login ID differs from the primary email address provided.

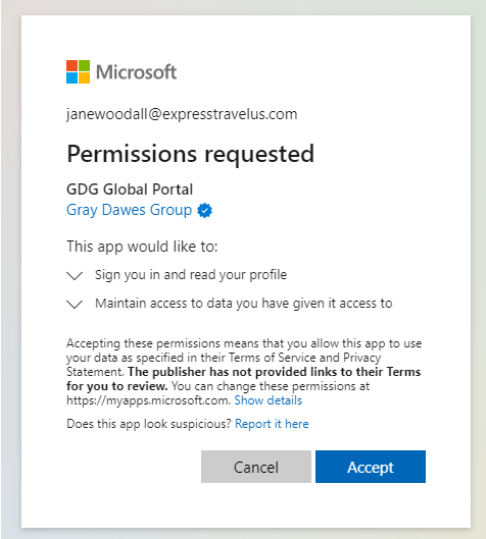
The URL of the application is https://gdportal.gdg.travel

When logging onto the platform the user will be presented with the following log in screen:



The user can select the "Log in with Microsoft" icon.

When a user logs in for the very first time they will be presented with a "Permissions Request" from Microsoft which looks like this:



If your company limits which enterprise applications are available to your users, then you will need a Global Admin to log in first and accept the application. Once accepted an enterprise application will automatically be created within your tenant with the following

Application details:

Name	GDPortal SSO App Current
Application (Client ID)	34cef1e4-9a5f-42f5-bfbe-cf07f0752a70

Further Information

This type of SSO makes use of the Microsoft identity platform and the protocols of OAuth 2.0 and OpenID Connect (OIDC).

You can read about this here (Microsoft Identity Platform)

Please note that this is NOT a SAML configuration.
No data is shared between your tenant and our application.
We do not require the setup of any secret keys or any access to your tenant.

When logging into our application using the "log in with Microsoft" option, the authentication is between your tenant and Microsoft.

Visit www.gdg.travel/portal for more information about PORTAL.