Portal Single Sign-On

You can enable Single Sign-On (SSO) with the Portal as an extra layer of security for your organization.

When enabled, your users will have the same login experience on the Portal as they have in your internal systems. Typically this is done via Microsoft Azure AD, in which we use the same Identity Provider for our Portal that you use for your email.

How this benefits you

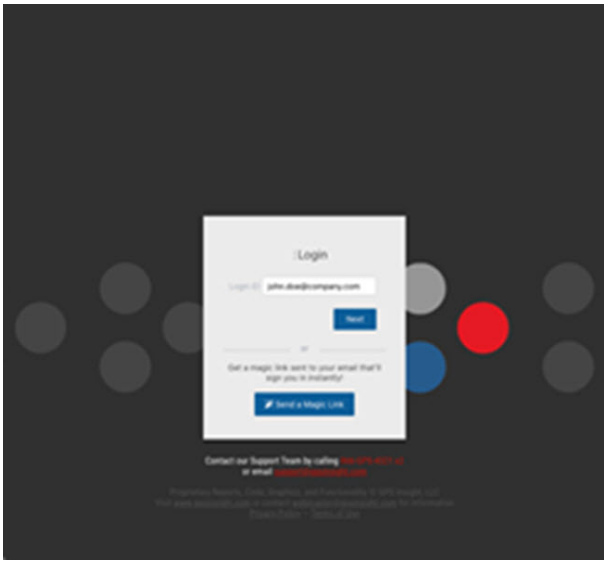
This Single Sign-On model increases security on multiple levels:

- **Fewer passwords** – Once SSO is enabled, a copy of your login password is no longer stored, meaning your passwords are stored in fewer places. This also means your users will have fewer passwords to remember.
- **World-Class Security** – Eliminate concerns regarding Portal login security. With SSO, authentication is delegated to industry leaders (e.g., Microsoft, etc.) with proven security models.
- **Revoke Access Instantly** – When you need to revoke access for a departing employee, that also means revoking access to various external systems. With SSO, cutting off their email account also cuts off their Portal access instantly.

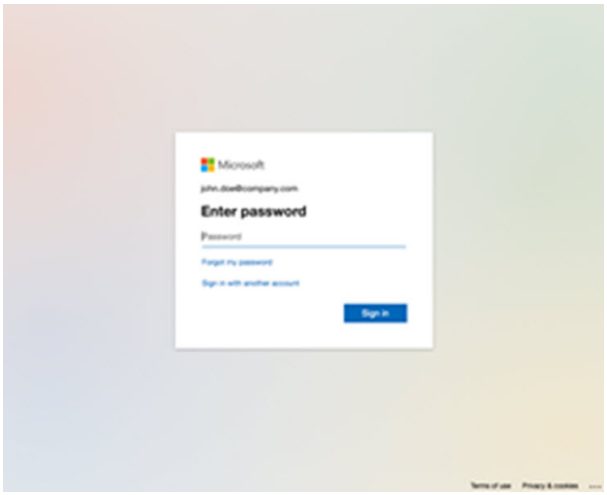
Portal SSO Example

The below is an example of how this works for your users.

1. When a user navigates to the login page, they enter their email address on your company's domain (i.e. john.doe@company.com), and click **Next**.
2. The user will be redirected to Azure AD to authenticate their password on a Microsoft.com website. There they can also fulfill any other security requirements for your organization, such as Multi-Factor Authentication.
3. Azure AD issues an authorization token that we then use to log the user into the Portal.



Copyright ©2026 GPS Insight



Note. In cases where Azure AD has already authenticated the user, step 2 above is bypassed. If Azure AD already knows the user, even from a different website, they'll issue the authorization token without prompting the user for a password again.

Frequently Asked Questions

Question	Answer
Do all of my users need to use SSO?	SSO will be bound to your company's email domain(s); however, logins with usernames or emails off that domain can be supported by storing a password like other users not using SSO. **Note.** A user with an email bound to SSO cannot alternately log in with their username to bypass SSO. All SSO users will need to use their email to log in.
Do you support automatic provisioning with SCIM?	We have not implemented SCIM endpoints, so all management or user accounts need to be done through the Portal or APIs. Users who are terminated in your IDP will have access cut off instantly in the Portal because they won't be able to log in, but their Portal user record will still be marked as active until you update it.
How often do users have to log in?	We have adopted Microsoft's refresh token expiration policy, which is common in most modern websites. A refresh token will be stored as a cookie in the browser allowing the user to refresh their login without a password. If the user doesn't log in for 90 days, this token will expire. Otherwise, it will continue to be valid as long as the user logs in regularly. It will also expire if the user changes their password, deletes their cookie, or access is revoked at their Identity Provider.

Copyright ©2026 GPS Insight

Question	Answer
What exactly do you mean by “Revoke Access Instantly”?	Modern authentication uses a short-lived token called an Access Token to allow for access. When a user is disabled in your Identity Provider, they will no longer be able to retrieve a new access token, so even if they are currently using a valid access token it will be valid for, at most, one hour after access is revoked.

Copyright ©2026 GPS Insight