Identifying the best authentication method for your enterprise

In this article

You can determine whether your enterprise would benefit more from SAML SSO or Enterprise Managed Users by asking yourself some questions about your enterprise's needs and workflows.

About authentication methods for your enterprise

You can choose to allow members to create and manage user accounts, or your enterprise can create and manage accounts for members with Enterprise Managed Users. If you allow members to manage their own accounts, you can also configure SAML authentication to both increase security and centralize identity and access for the web applications that your team uses. For more information, see "About authentication for your enterprise."

Both SAML SSO and Enterprise Managed Users increase security for your enterprise's resources. Enterprise Managed Users additionally allows you to control the user accounts for your enterprise members and restricts what the accounts are able to do. However, those restrictions may be unacceptable for your enterprise if they obstruct your developers' workflows.

To determine whether your enterprise would benefit more from SAML SSO or Enterprise Managed Users, ask yourself the following questions.

Do you want to control the user accounts for your users?

Enterprise Managed Users may be right for your enterprise if you don't want enterprise members to use their own personal accounts on GitHub.com to access your enterprise's resources.

With SAML SSO, developers create and manage their own personal accounts, and each account is linked to a SAML identity in your IdP. Enterprise Managed Users functions more like other familiar SSO solutions, as you will provision the accounts for your users. You can also ensure user accounts conform with your company identity, by controlling usernames and the email addresses associated with the accounts.

If you currently require your users to create a new account on GitHub.com to use with your enterprise only, Enterprise Managed Users might be right for you. However, SAML SSO may be a better option if using your IdP as the source of truth for your user and access management would add too much complexity. For example, perhaps your enterprise does not have an established process for onboarding new users in your IdP.

Which identity provider does your enterprise use?

Enterprise Managed Users is supported for a limited number of IdPs and requires SCIM, while SAML SSO offers full support for a larger number of IdPs, plus limited support for all IdPs that implement the SAML 2.0 standard, and does not require SCIM. For the list of supported IdPs for each option, see "About Enterprise Managed Users" and "About SAML for enterprise IAM."

You can use Enterprise Managed Users with an unsupported IdP only if you federate the unsupported IdP to a supported IdP to use as an integration point. If you wish to avoid this extra complexity, SAML SSO may be a better solution for you.

Do your developers work in public repositories, gists, or GitHub Pages sites?

To prevent enterprise members from accidentally leaking corporate-owned content to the public on GitHub.com, Enterprise Managed Users imposes strong restrictions on what users can do. For example, managed user accounts cannot create public repositories, gists of any visibility, or GitHub Pages sites that are visible outside the enterprise. For a full list of restrictions, see "About Enterprise Managed Users."

These restrictions are unacceptable for some enterprises. To determine whether Enterprise Managed Users will work for you, review the restrictions with your developers, and confirm whether any of the restrictions will hinder your existing workflows. If so, SAML SSO may be a better choice for your enterprise.

Do your developers rely on collaboration outside of your enterprise?

Managed user accounts can only contribute to repositories within your enterprise. If your developers must contribute to both repositories within and outside of your enterprise, including private repositories, Enterprise Managed Users may not be right for your enterprise. SAML SSO may be a better solution.

Some companies maintain repositories within an existing enterprise using SAML SSO on GitHub.com, and also create an enterprise with managed users. Developers who contribute to repositories owned by both enterprises from a single workstation must switch between the accounts on GitHub.com within a single browser, or use a different browser for each account. The developer may also need to customize the workstation's Git configuration to accommodate the two accounts. The complexity of this workflow can increase the risk of mistakenly leaking internal code to the public.

If you decide to create an enterprise with managed users but require that developers contribute to resources outside of the enterprise from a single workstation, you can provide support for switching between the accounts in a developer's local Git configuration. For more information, see "About Enterprise Managed Users."

Does your enterprise rely on outside collaborators?

With SAML SSO, you can give access to specific repositories to people who are not members of your IdP's directory, by using the outside collaborator role. This can be especially useful for collaborators that are external to your business, such as contractors. For more information, see "Adding outside collaborators to repositories in your organization."

With Enterprise Managed Users, the outside collaborator role does not exist. Your enterprise's resources can only be accessed by managed user accounts, which are always provisioned by your IdP. To give external collaborators access to your enterprise, you would have to use guest accounts in your IdP. If you're interested in Enterprise Managed Users, confirm with your developers whether this will hinder any of their existing workflows. If so, SAML SSO may be a better solution.

Can your enterprise tolerate migration costs?

If your enterprise is new to GitHub.com, SAML SSO and Enterprise Managed Users are equally easy to adopt.

If you're already using GitHub.com with developers managing their own user accounts, adopting Enterprise Managed Users requires migrating to a new enterprise account. For more information, see "About Enterprise Managed Users."

Although Enterprise Managed Users is free, the migration process may require time or cost from your team. Confirm that this migration process is acceptable to your business and your developers. If not, SAML SSO may be the better choice for you.

Further reading

- "Deciding whether to configure SAML for your enterprise or your organizations"

Legal