Deciding whether to configure SAML for your enterprise or your organizations

You can configure SAML for your enterprise account, with the same configuration applying to all of its organizations, or you can create separate configurations for individual organizations.

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."

If you decide to use SAML instead of Enterprise Managed Users, you must choose whether to configure SAML at the enterprise level or the organization level.

If some groups within your enterprise must use different SAML authentication providers to grant access to your resources on GitHub.com, configure SAML for individual organizations. You can implement SAML for your organizations over time by allowing users to gradually authenticate using SAML, or you can require SAML authentication by a certain date. Organization members who do not authenticate using SAML by this date will be removed. For more information about organization-level SAML, see "About identity and access management with SAML single sign-on."

If you configure SAML at the organization level, members are not required to authenticate via SAML to access internal repositories. For more information about internal repositories, see "About repositories."

If you need to protect internal repositories or enforce a consistent authentication experience for every organization in your enterprise, you can configure SAML authentication for your enterprise account instead. The SAML configuration for your enterprise overrides any SAML configuration for individual organizations, and organizations cannot override the enterprise configuration. After you configure SAML for your enterprise, organization members must authenticate with SAML before accessing organization resources, including internal repositories.

SCIM is not available for enterprise accounts, and team synchronization is only available for SAML at the enterprise level if you use Azure AD as an IdP. For more information, see "Managing team synchronization for organizations in your enterprise."

Regardless of the SAML implementation you choose, you cannot add external collaborators to organizations or teams. You can only add external collaborators to individual repositories.