Using SAML for enterprise IAM

You can centrally manage accounts and access to your GitHub Enterprise Server instance with SAML single sign-on (SSO).

About SAML for enterprise IAM

You can use SAML single sign-on (SSO) to centrally manage access to your GitHub Enterprise Server instance.

SAML configuration reference

You can see SAML metadata for your GitHub Enterprise Server instance, and you can learn more about available SAML attributes and response requirements.

Configuring SAML single sign-on for your enterprise

You can control and secure access to your GitHub Enterprise Server instance by configuring SAML single sign-on (SSO) through your identity provider (IdP).

Configuring user provisioning with SCIM for your enterprise

You can configure System for Cross-domain Identity Management (SCIM) for your GitHub Enterprise Server instance, which automatically provisions user accounts when you assign the application for your instance to a user on your identity provider (IdP).

Configuring authentication and provisioning for your enterprise using Azure AD

You can use a tenant in Azure Active Directory (Azure AD) as an identity provider (IdP) to centrally manage authentication and user provisioning for your GitHub Enterprise Server instance.

Enabling encrypted assertions

You can improve your GitHub Enterprise Server instance's security with SAML single sign-on (SSO) by encrypting the messages that your SAML identity provider (IdP) sends.

Updating a user's SAML NameID

When an account's `NameID` changes on your identity provider (IdP) and the person can no longer sign into your GitHub Enterprise Server instance, you must update the `NameID` mapping on your GitHub Enterprise Server instance.

Troubleshooting SAML authentication

If you use SAML single sign-on (SSO) and people are unable to authenticate to access

your GitHub Enterprise Server instance, you can troubleshoot the problem.
