

**This version of GitHub Enterprise was discontinued on 2023-03-15.** No patch releases will be made, even for critical security issues. For better performance, improved security, and new features, [upgrade to the latest version of GitHub Enterprise](#). For help with the upgrade, [contact GitHub Enterprise support](#).

# About SAML for enterprise IAM

## In this article

About SAML SSO for your GitHub Enterprise Server instance

Supported IdPs

Further reading

---

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

## About SAML SSO for your GitHub Enterprise Server instance [↗](#)

SAML SSO allows people to authenticate and access your GitHub Enterprise Server instance through an external system for identity management.

SAML is an XML-based standard for authentication and authorization. When you configure SAML for your GitHub Enterprise Server instance, the external system for authentication is called an identity provider (IdP). Your instance acts as a SAML service provider (SP). For more information about the SAML standard, see [Security Assertion Markup Language](#) on Wikipedia.

**Note:** You can use either SAML or LDAP, but not both.

Your IdP does not communicate with GitHub Enterprise Server automatically when you assign or unassign the application. GitHub Enterprise Server creates a user account using SAML Just-in-Time (JIT) provisioning the first time someone navigates to GitHub Enterprise Server and signs in by authenticating through your IdP. You may need to manually notify users when you grant access to GitHub Enterprise Server.

When using SAML or CAS, two-factor authentication is not supported or managed on the GitHub Enterprise Server instance, but may be supported by the external authentication provider. Two-factor authentication enforcement on organizations is not available. For more information about enforcing two-factor authentication on organizations, see "[Requiring two-factor authentication in your organization](#)."

After you configure SAML, people who use your GitHub Enterprise Server instance must use a personal access token to authenticate API requests. For more information, see "[Managing your personal access tokens](#)."

If you want to allow authentication for some people who don't have an account on your external authentication provider, you can allow fallback authentication to local accounts on your GitHub Enterprise Server instance. For more information, see "[Allowing built-in authentication for users outside your provider](#)."

For more information about the configuration of SAML SSO on GitHub Enterprise Server, see "[Configuring SAML single sign-on for your enterprise](#)."

## Supported IdPs

---

GitHub Enterprise Server supports SAML SSO with IdPs that implement the SAML 2.0 standard. For more information, see the [SAML Wiki](#) on the OASIS website.

GitHub officially supports and internally tests the following IdPs.

- Active Directory Federation Services (AD FS)
- Azure Active Directory (Azure AD)
- Okta
- OneLogin
- PingOne
- Shibboleth

If your IdP supports encrypted assertions, you can configure encrypted assertions on GitHub Enterprise Server for increased security during the authentication process.

GitHub Enterprise Server does not support SAML Single Logout. To terminate an active SAML session, users should log out directly on your SAML IdP.

## Further reading

---

- [SAML Wiki](#) on the OASIS website

### Legal

© 2023 GitHub, Inc. [Terms](#) [Privacy](#) [Status](#) [Pricing](#) [Expert services](#) [Blog](#)