Configuring authentication and provisioning for your enterprise using Azure AD

In this article

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.

> **Who can use this feature**
> Enterprise owners can configure authentication and provisioning for an enterprise on GitHub Enterprise Server.

About authentication and user provisioning with Azure AD

Azure Active Directory (Azure AD) is a service from Microsoft that allows you to centrally manage user accounts and access to web applications. For more information, see What is Azure Active Directory? in the Microsoft Docs.

When you use an IdP for IAM on GitHub Enterprise Server, SAML SSO controls and secures access to enterprise resources like repositories, issues, and pull requests. SCIM automatically creates user accounts and manages access to your GitHub Enterprise Server instance when you make changes on the IdP. You can also synchronize teams on GitHub Enterprise Server with groups on your IdP. For more information, see the following articles.

- "About SAML for enterprise IAM"
- "Configuring user provisioning with SCIM for your enterprise"
- "Synchronizing a team with an identity provider group"

Note: SCIM for GitHub Enterprise Server is currently in private beta and is subject to change. For access to the beta, contact your account manager on GitHub's Sales team. Please provide feedback in the GitHub Community discussion.

Warning: The beta is exclusively for testing and feedback, and no support is available. GitHub recommends testing with a staging instance. For more information, see "Setting up a staging instance."

After you enable SAML SSO and SCIM for GitHub Enterprise Server using Azure AD, you can accomplish the following from your Azure AD tenant.

- Assign the GitHub Enterprise Server application on Azure AD to a user account to automatically create and grant access to a corresponding user account on GitHub Enterprise Server.
- Unassign the GitHub Enterprise Server application to a user account on Azure AD to deactivate the corresponding user account on GitHub Enterprise Server.
- Assign the GitHub Enterprise Server application to an IdP group on Azure AD to automatically create and grant access to user accounts on GitHub Enterprise Server for all members of the IdP group. In addition, the IdP group is available on GitHub Enterprise Server for connection to a team and its parent organization.
- Unassign the GitHub Enterprise Server application from an IdP group to deactivate the GitHub Enterprise Server user accounts of all IdP users who had access only through that IdP group and remove the users from the parent organization. The IdP group will be disconnected from any teams on GitHub Enterprise Server.

For more information about managing identity and access for your enterprise on your GitHub Enterprise Server instance, see "Using SAML for enterprise IAM."

Prerequisites

- To configure authentication and user provisioning for GitHub Enterprise Server using Azure AD, you must have an Azure AD account and tenant. For more information, see the Azure AD website and Quickstart: Create an Azure Active Directory tenant in the Microsoft Docs.
- You must configure SAML SSO for your GitHub Enterprise Server instance. For more information, see "Configuring SAML single sign-on for your enterprise."
- You must create and use a dedicated machine user account on your IdP to associate with an enterprise owner account on GitHub Enterprise Server. Store the credentials for the user account securely in a password manager. For more information, see "Configuring user provisioning with SCIM for your enterprise."

Configuring authentication and user provisioning with Azure AD

1. Configure SAML SSO for your GitHub Enterprise Server instance. For more information, see "Configuring SAML single sign-on for your enterprise."
2. Configure user provisioning with SCIM for your instance. For more information, see "Configuring user provisioning with SCIM for your enterprise."

Managing enterprise owners

The steps to make a person an enterprise owner depend on whether you only use SAML or also use SCIM. For more information about enterprise owners, see "Roles in an enterprise."

If you configured provisioning, to grant the user enterprise ownership in GitHub Enterprise Server, assign the enterprise owner role to the user in Azure AD.

If you did not configure provisioning, to grant the user enterprise ownership in GitHub Enterprise Server, include the `administrator` attribute in the SAML assertion for the user account on the IdP, with the value of `true`. For more information about including the `administrator` attribute in the SAML claim from Azure AD, see How to: customize claims issued in the SAML token for enterprise applications in the Microsoft Docs.