Configuring user provisioning with SCIM for your enterprise

In this article

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).

> **Who can use this feature**
> Site administrators can configure user provisioning for a GitHub Enterprise Server instance.

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."

About user provisioning for GitHub Enterprise Server

If you use SAML single sign-on (SSO) for your GitHub Enterprise Server instance, you can configure SCIM to automatically create or suspend user accounts and grant access to your instance when you assign or unassign the application on your IdP. For more information about SCIM, see System for Cross-domain Identity Management: Protocol (RFC 7644) on the IETF website.

If you do not configure user provisioning with SCIM, your IdP will not communicate with GitHub Enterprise Server automatically when you assign or unassign the application to a user. Without SCIM, 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.

Configuring provisioning allows your IdP to communicate with your GitHub Enterprise Server instance when you assign or unassign the application for GitHub Enterprise Server to a user on your IdP. When you assign the application, your IdP will prompt your GitHub Enterprise Server instance to create an account and send an onboarding email to the

user. When you unassign the application, your IdP will communicate with GitHub Enterprise Server to invalidate any SAML sessions and disable the member's account.

To configure provisioning for your enterprise, you must enable provisioning on GitHub Enterprise Server, then install and configure a provisioning application on your IdP.

The provisioning application on your IdP communicates with GitHub Enterprise Server using the SCIM API. For more information, see "SCIM" in the REST API documentation.

About identities and claims

After an IdP administrator grants a person access to your GitHub Enterprise Server instance, the user can authenticate through the IdP to access GitHub Enterprise Server using SAML SSO.

During authentication, the instance attempts to associate the user with a SAML identity. By default, the instance compares the `NameID` claim from the IdP to the account's username. GitHub Enterprise Server normalizes the value of `NameID` for the comparison. For more information about username normalization, see "Username considerations for external authentication."

If there is no existing account with a matching username on the instance, the user will fail to sign in. To make this match, GitHub Enterprise Server compares the SAML `NameId` claim from the IdP to the `username` claim for each user account provisioned by SCIM on the instance.

During SAML authentication, some environments may use a value other than `NameID` as the unique identifying claim. If your environment does not use `NameID` to identify users, a site administrator can configure custom user attributes for the instance. GitHub Enterprise Server will respect this mapping when SCIM is configured. For more information about mapping user attributes, see "Configuring SAML single sign-on for your enterprise."

If GitHub Enterprise Server successfully identifies a user from the IdP, but account details such as email address, first name, or last name don't match, the instance overwrites the details with values from the IdP. Any email addresses other than the primary email provisioned by SCIM will also be deleted from the user account.

Supported identity providers

During the private beta, your account team will provide documentation for the configuration of SCIM for GitHub Enterprise Server on a supported IdP.

Prerequisites

- 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 allow built-in authentication for users who don't have an account on your IdP. For more information, see "Allowing built-in authentication for users outside your provider."
- Your IdP must support making SCIM calls to a Service Provider (SP).
- You must have administrative access on your IdP to configure the application for user provisioning for GitHub Enterprise Server.

Enabling user provisioning for your enterprise

To perform provisioning actions on your instance, you will create a built-in user account and promote the account to an enterprise owner.

After you enable SCIM on a GitHub Enterprise Server instance, all user accounts are suspended. The built-in user account will continue to perform provisioning actions. After you grant a user access to your instance from your IdP, the IdP will communicate with the instance using SCIM to unsuspend the user's account.

1. Create a built-in user account to perform provisioning actions on your instance. For more information, see "Allowing built-in authentication for users outside your provider."
2. Promote the dedicated user account to an enterprise owner. For more information, see "Inviting people to manage your enterprise."
3. Sign into your instance as the new enterprise owner.
4. Create a personal access token (classic) with **admin:enterprise** scope. Do not specify an expiration date for the personal access token (classic). For more information, see "Managing your personal access tokens."

   Warning: Ensure that you don't specify an expiration date for the personal access token (classic). If you specify an expiration date, SCIM will no longer function after the expiration date passes.

   Note: You'll need this personal access token to test the SCIM configuration, and to configure the application for SCIM on your IdP. Store the token securely in a password manager until you need the token again later in these instructions.

5. SSH into your GitHub Enterprise Server instance. If your instance comprises multiple nodes, for example if high availability or geo-replication are configured, SSH into the primary node. If you use a cluster, you can SSH into any node. For more information about SSH access, see "Accessing the administrative shell (SSH)."

   ```
   ssh -p 122 admin@HOSTNAME
   ```

6. To enable SCIM, run the commands provided to you by your account manager on GitHub's Sales team.
7. Wait for the configuration run to complete.
8. To validate that SCIM is operational, run the following commands. Replace *PAT FROM STEP 3* and *YOUR INSTANCE'S HOSTNAME* with actual values.

   ```
   $ GHES_PAT="PAT FROM STEP 3"
   $ GHES_HOSTNAME="YOUR INSTANCE'S HOSTNAME"
   $ curl --location --request GET
   'https://$GHES_HOSTNAME/api/v3/scim/v2/Users' \
       --header 'Content-Type: application/scim' \
       --header 'Authorization: Bearer $GHES_PAT'
   ```

   The command should return an empty array.

9. Configure user provisioning in the application for GitHub Enterprise Server on your IdP. To request documentation for a supported IdP, contact your account manager on GitHub's Sales team. If your IdP is unsupported, you must create the application and configure SCIM manually.