Viewing people in your enterprise

In this article

About the list of people in your enterprise
Viewing enterprise administrators
Viewing members
Viewing members' email addresses
Viewing outside collaborators
Viewing pending invitations
Viewing suspended members in an enterprise with managed users
Viewing dormant users
Filtering by member type in an enterprise with managed users
Viewing members without an email address from a verified domain
Viewing whether members in your enterprise have 2FA enabled
Further reading

To audit access to enterprise-owned resources or user license usage, enterprise owners can view every administrator and member of the enterprise.

> **Who can use this feature**
> Enterprise owners can view the people in an enterprise.

About the list of people in your enterprise

To audit access to your enterprise's resources and manage license usage, you can see a list of all the people who have access to your enterprise.

You can see all current enterprise members and enterprise administrators, as well as pending invitations to become members and administrators. To make it easier to consume this information, you can search and filter the lists. You can also view an overview of the number of members in your enterprise, grouped by role, type of license, or type of deployment.

If GitHub Connect is configured for your enterprise, when you filter a list of people in your enterprise, the following limitations apply.

- The filter for two-factor authentication (2FA) status does not show people who only have an account on a GitHub Enterprise Server instance.
- If you combine the filter for accounts on GitHub Enterprise Server instances with either the filter for organizations or 2FA status, you will not see any results.

For more information about GitHub Connect, see the following articles.

- "About GitHub Connect" in the GitHub Enterprise Server documentation
- "About GitHub Connect" in the GitHub AE documentation

You can also export membership information for your enterprise. For more information, see "Exporting membership information for your enterprise."

Viewing enterprise administrators

You can view all the current enterprise owners and billing managers for your enterprise. You can see useful information about each administrator and filter the list by role. You can find a specific person by searching for their username or display name.

You can also remove an administrator. For more information. see "Inviting people to manage your enterprise."

1. In the top-right corner of GitHub.com, click your profile photo, then click **Your enterprises**.
2. In the list of enterprises, click the enterprise you want to view.
3. In the enterprise account sidebar, click **People**.
4. Under "People", click **Administrators**.

Viewing members

You can see all the current members for your enterprise. You can see useful information about each account and filter the list in useful ways, such as by role. In addition to the list of members, you will see an overview of the number of members in your enterprise, grouped by role, type of license, and type of deployment.

You can find a specific person by searching for the person's username or display name. To view more information about the person's access to your enterprise, such as the organizations the person belongs to, you can click the person's name.

You can also remove any enterprise member from all organizations owned by the enterprise. For more information, see "Removing a member from your enterprise."

1. In the top-right corner of GitHub.com, click your profile photo, then click **Your enterprises**.
2. In the list of enterprises, click the enterprise you want to view.
3. In the enterprise account sidebar, click **People**.
4. Optionally, to export the list of members as a CSV report, click **CSV report**. For more information about the information included in the report, see "Exporting membership information for your enterprise."

About the membership overview

On the "Members" page, you will find an overview of the number of members in your enterprise, grouped by role, type of license consumed, and the type of deployment the member is on. The following sections explain how the numbers in this overview are calculated.

If your enterprise uses both GitHub Enterprise Cloud and GitHub Enterprise Server, to get accurate data about your members and licenses across your deployments, you will need to enable GitHub Connect and synchronize license usage. For more information, see "About GitHub Connect" in the GitHub Enterprise Server documentation.

Roles

The "Roles" column groups members by their role in the enterprise. For more information, see "Roles in an enterprise."

If a user has multiple roles in an enterprise, the user is counted once for each role. For example, if the same user is a member of three organizations and an owner of two organizations, the user counts once towards "Organization member" and once towards "Organization owner."

An "outside collaborator" is a user who has access to a repository in an organization, but is not a member of the organization. The user might be an outside collaborator in one organization in your enterprise and a member of another organization. In this case, the user counts towards each total. For more information, see "Adding outside collaborators to repositories in your organization."

If your enterprise uses managed user accounts, an "unaffiliated user" is someone who been provisioned with a user account, but is not a member of any of your organizations.

User licenses consumed

The "User licenses consumed" column shows you how licenses are consumed in your enterprise. For more information, see "About licenses for GitHub Enterprise."

If there are outside collaborators in your enterprise, the "total consumed" number of licenses may be larger than the number of people listed for your enterprise. An outside collaborator consumes a license, but is not counted in the total member count displayed next to "people in YOUR-ENTERPRISE". A pending invitation to an outside collaborator also consumes a license, but is not counted in the "By invitations" count in the overview.

For more information about how license usage is calculated across deployments, see "Troubleshooting license usage for GitHub Enterprise."

Deployment

The "Deployment" column groups users by the type of deployment they are using. For more information, see "About GitHub for enterprises."

"Cloud members" are a member or owner of any organization in your enterprise on GitHub.com. "Server members" have an account on a GitHub Enterprise Server instance owned by your enterprise. "Members on cloud and server" are users who match both these criteria.

Viewing members' email addresses

You may be able to view the email addresses for members of your enterprise on either GitHub.com or an external identity system. The visibility of the email addresses depends on your enterprise's authentication method, domains, and potentially the member's user profile configuration.

- If you use Enterprise Managed Users and the `NameID` for your SAML configuration is an email address, you can view the `NameID` for each of your enterprise members.
- If you verify a domain for your enterprise, you can view members' email addresses for the verified domain. For more information, see "Verifying or approving a domain for your enterprise."
- If you don't use Enterprise Managed Users, and you also don't configure SAML single sign-on (SSO), members access your enterprise's resources on GitHub.com solely using a personal account. The owner of a personal account can choose whether or not to publicly display an email address. If a user chooses not to display the email address, you cannot view the email address. Without SAML, GitHub cannot display external identity information, like the `NameID`, which is typically an email address.

If you use Enterprise Managed Users, verify a domain, or configure SAML SSO for your enterprise, you may be able to view the email addresses in one or more of the following ways.

1. On your SAML Identity Provider (IdP), review the email addresses of users with access to GitHub Enterprise Cloud. For more information, see "About SAML for enterprise IAM."
2. Export the membership report for your enterprise on GitHub. The report may contain the user's email address, stored as the following values.
   - `GitHub com saml name`: The `NameID` from the user's linked SAML identity, which is typically the user's email address (for more information, see "SAML configuration reference")
   - `GitHub com verified domain emails`: Email addresses for any verified domains (for more information, see "Verifying or approving a domain for your enterprise")

   For more information, see "Exporting membership information for your enterprise."
3. Use the GraphQL API to retrieve the `ExternalIdentity` for each member. For more information, see "About the GraphQL API" and "Objects" in the GraphQL API documentation.

Viewing outside collaborators

You can see all the current outside collaborators for your enterprise. You can see useful information about each collaborator and filter the list in useful ways, such as by organization. You can find a specific collaborator by searching for their username or display name.

You can view more information about the person's access to your enterprise, such as a list of all the repositories the collaborator has access to, by clicking on the person's name.

1. In the top-right corner of GitHub.com, click your profile photo, then click **Your enterprises**.
2. In the list of enterprises, click the enterprise you want to view.
3. In the enterprise account sidebar, click **People**.
4. Under "People", click **Outside collaborators**.

Viewing pending invitations

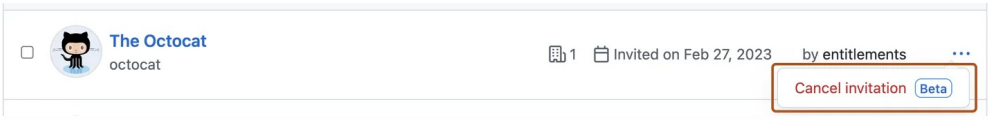
You can see all the pending invitations to become members, administrators, or outside collaborators in your enterprise. You can filter the list in useful ways, such as by license, by organization, or by source. You can find a specific person by searching for their username or display name.

In the list of pending members, for any individual account, you can cancel all invitations to join organizations owned by your enterprise. This does not cancel any invitations for that same person to become an enterprise administrator or outside collaborator.

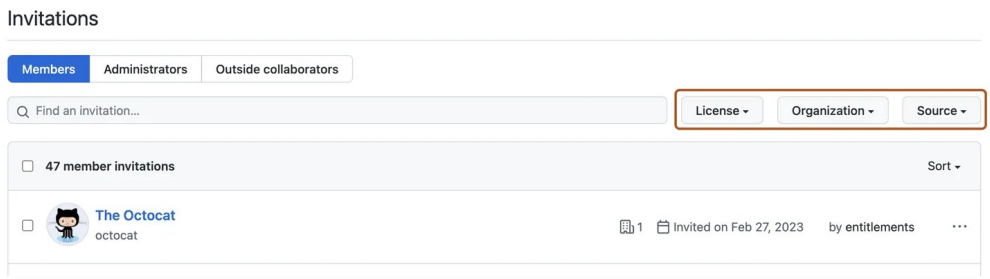
> **Note:** If an invitation was provisioned via SCIM, you must cancel the invitation via your identity provider (IdP) instead of on GitHub.

If you use Visual Studio subscriptions with GitHub Enterprise, the list of pending invitations includes all Visual Studio subscribers that haven't joined any of your organizations on GitHub, even if the subscriber does not have a pending invitation to join an organization. For more information about how to get Visual Studio subscribers access to GitHub Enterprise, see "Setting up Visual Studio subscriptions with GitHub Enterprise."

1. In the top-right corner of GitHub.com, click your profile photo, then click **Your enterprises**.
2. In the list of enterprises, click the enterprise you want to view.
3. In the enterprise account sidebar, click **People**.
4. Under "People", click **Invitations**.
5. Optionally, you can cancel all invitations for an account to join organizations owned by your enterprise. To the right of the account, click ···, then click **Cancel invitation**.



6. Optionally, you can view pending invitations for enterprise administrators or outside collaborators. Under "Invitations", click **Administrators** or **Outside collaborators**.
7. Optionally, to filter the list of pending invitations by license, by organization, or by source, use the dropdown menus at the top of the list.



Viewing suspended members in an enterprise with managed users

If your enterprise uses Enterprise Managed Users, you can view suspended users. Suspended users are members who have been deprovisioned after being unassigned from the GitHub Enterprise Managed User application or deleted from the identity provider. For more information, see "About Enterprise Managed Users."

1. In the top-right corner of GitHub.com, click your profile photo, then click **Your enterprises**.
2. In the list of enterprises, click the enterprise you want to view.
3. In the enterprise account sidebar, click **People**.
4. Under "People", click **Suspended**.

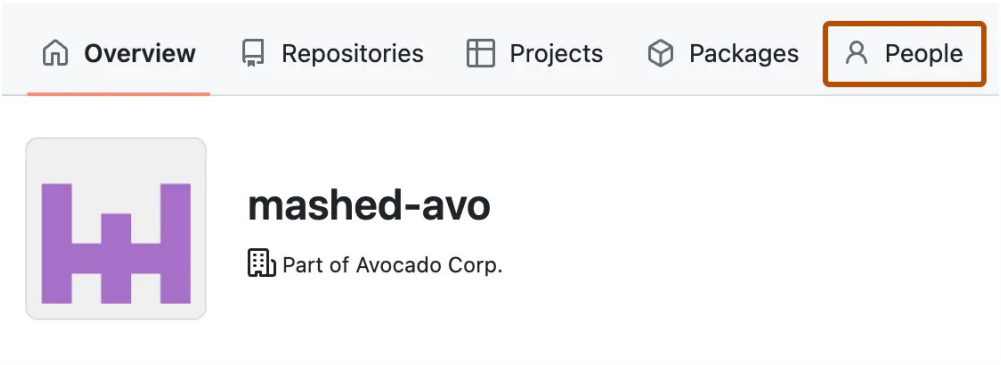
Viewing dormant users

You can view a list of all dormant users who are not site administrators. A user account is considered to be dormant if it has not been active for 90 days. For more information, see "Managing dormant users."

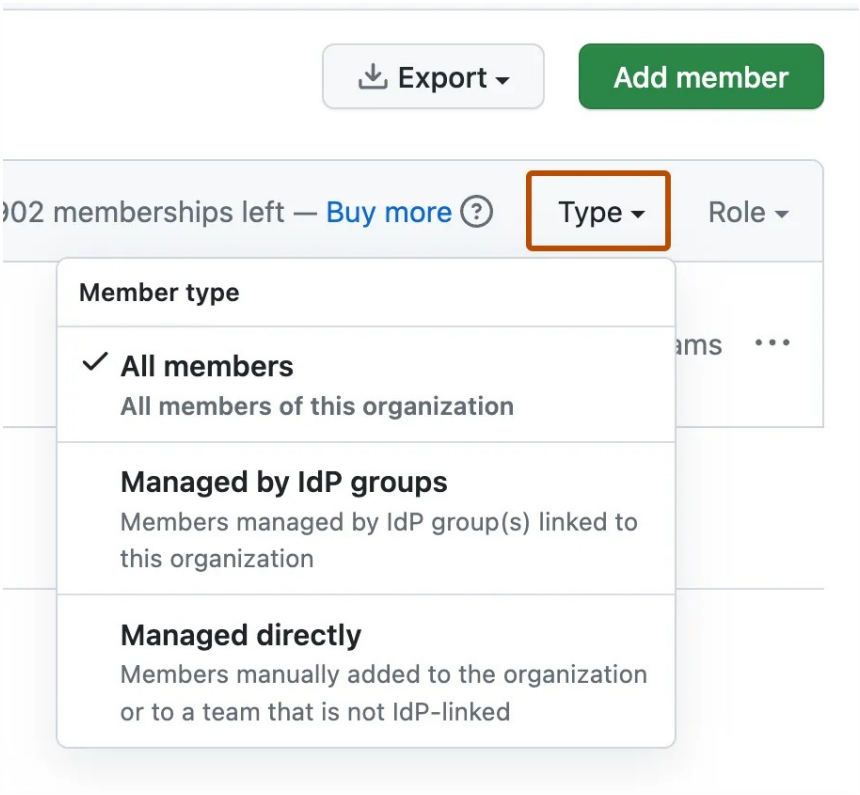
Filtering by member type in an enterprise with managed users

If your enterprise uses Enterprise Managed Users, you can filter the member list of an organization by type to determine if memberships are managed through an IdP or managed directly. Memberships managed through an IdP were added through an IdP group, and the IdP group was connected to a team within the organization. Memberships managed directly were added to the organization manually. The way a membership is mananaged in an organization determines how it must be removed. You can use this filter to determine how members were added to an organization, so you know how to remove them. For more information, see "About Enterprise Managed Users."

1. In the top-right corner of GitHub.com, click your profile photo, then click **Your enterprises**.
2. In the list of enterprises, click the enterprise you want to view.
3. Under "Organizations", in the search bar, begin typing the organization's name until it appears in the search results.
4. Click the name of the organization.
5. Above the organization name, click **People**.



6. Above the list of members, click **Type**, then select the type of members you want to view.



Viewing members without an email address from a verified domain

You can view a list of members in your enterprise who don't have an email address from a verified domain associated with their user account on GitHub.com.

1. In the top-right corner of GitHub.com, click your profile photo, then click **Your enterprises**.
2. In the list of enterprises, click the enterprise you want to view.
3. In the enterprise account sidebar, click **Settings**.
4. Under "Settings", click **Verified & approved domains**.
5. Under "Notification preferences", click the **View enterprise members without an approved or verified domain email** link.

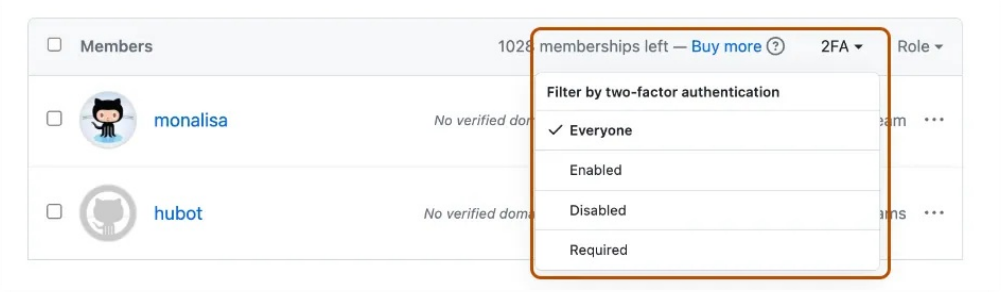
Viewing whether members in your enterprise have 2FA enabled

You can see which people in your enterprise have enabled two-factor authentication or are required to do so.

Note: Starting in March 2023 and through the end of 2023, GitHub will gradually begin to require all users who contribute code on GitHub.com to enable one or more forms of two-factor authentication (2FA). If you are in an eligible group, you will receive a notification email when that group is selected for enrollment, marking the beginning of a 45-day 2FA enrollment period, and you will see banners asking you to enroll in 2FA on GitHub.com. If you don't receive a notification, then you are not part of a group required to enable 2FA, though we strongly recommend it.

For more information about the 2FA enrollment rollout, see this blog post.

1. In the top-right corner of GitHub.com, click your profile photo, then click **Your enterprises**.
2. In the list of enterprises, click the enterprise you want to view.
3. In the enterprise account sidebar, click **People**.
4. To view enterprise members who have enabled or disabled two-factor authentication, on the right, select **2FA**, then click **Enabled** or **Disabled**. Additionally, you can view which members are required to enable two-factor authentication by clicking **Required**.



Further reading

- "Roles in an enterprise"