Roles in an organization

In this article

Organization owners can assign roles to individuals and teams giving them different sets of permissions in the organization.

About roles

To perform any actions on GitHub, such as creating a pull request in a repository or changing an organization's billing settings, a person must have sufficient access to the relevant account or resource. This access is controlled by permissions. A permission is the ability to perform a specific action. For example, the ability to delete an issue is a permission. A role is a set of permissions you can assign to individuals or teams.

Repository-level roles give organization members, outside collaborators and teams of people varying levels of access to repositories. For more information, see "Repository roles for an organization."

Team-level roles are roles that give permissions to manage a team. You can give any individual member of a team the team maintainer role, which gives the member a number of administrative permissions over a team. For more information, see "Assigning the team maintainer role to a team member."

Organization-level roles are sets of permissions that can be assigned to individuals or teams to manage an organization and the organization's repositories, teams, and settings. For more information about all the roles available at the organization level, see "About organization roles."

About organization roles

You can assign people to a variety of organization-level roles to control your members' access to your organization and its resources. For more details about the individual permissions included in each role, see "Permissions for organization roles."

If your organization is owned by an enterprise account, enterprise owners can choose to join your organization with any role. For more information, see "Managing your role in an organization owned by your enterprise."

Organization owners

Organization owners have complete administrative access to your organization. This role should be limited, but to no less than two people, in your organization. For more information, see "Maintaining ownership continuity for your organization."

Organization members

The default, non-administrative role for people in an organization is the organization member. By default, organization members have a number of permissions, including the ability to create repositories and project boards.

Organization moderators

Moderators are organization members who, in addition to their permissions as members, are allowed to block and unblock non-member contributors, set interaction limits, and hide comments in public repositories owned by the organization. For more information, see "Managing moderators in your organization."

Billing managers

Billing managers are users who can manage the billing settings for your organization, such as payment information. This is a useful option if members of your organization don't usually have access to billing resources. For more information, see "Adding a billing manager to your organization."

Security managers

Note: The security manager role is in public beta and subject to change.

Security manager is an organization-level role that organization owners can assign to any team in an organization. When applied, it gives every member of the team permissions to manage security alerts and settings across your organization, as well as read permissions for all repositories in the organization.

If your organization has a security team, you can use the security manager role to give members of the team the least access they need to the organization. For more information, see "Managing security managers in your organization."

GitHub App managers

By default, only organization owners can manage the settings of GitHub App registrations owned by an organization. To allow additional users to manage GitHub App registrations owned by an organization, an owner can grant them GitHub App manager permissions.

When you designate a user as a GitHub App manager in your organization, you can grant them access to manage the settings of some or all GitHub App registrations owned by the organization. The GitHub App manager role does not grant users access to install and uninstall GitHub Apps on an organization. For more information, see "Adding and removing GitHub App managers in your organization."

Outside collaborators

To keep your organization's data secure while allowing access to repositories, you can add *outside collaborators*. An outside collaborator is a person who has access to one or more organization repositories but is not explicitly a member of the organization, such as a consultant or temporary employee. For more information, see:

- "Adding outside collaborators to repositories in your organization"
- "Converting an organization member to an outside collaborator"
- "Removing an outside collaborator from an organization repository"

Permissions for organization roles

Organization permission	Owners	Members	Moderators	Billing managers	Security managers
Create repositories (see "Restricting repository creation in your organization")	✓	✓	✓	✕	✓
View and edit billing information	✓	✕	✕	✓	✕
Invite people to join the organization	✓	✕	✕	✕	✕
Edit and cancel invitations to join the organization	✓	✕	✕	✕	✕
Remove members from the organization	✓	✕	✕	✕	✕
Reinstate former members to the organization	✓	✕	✕	✕	✕
Add and remove people from all teams	✓	✕	✕	✕	✕
Promote organization members to *team maintainer*	✓	✕	✕	✕	✕
Configure code review assignments (see "Managing code review settings for your team")	✓	✕	✕	✕	✕
Set scheduled reminders (see "Managing	✓	✕	✕	✕	✕

scheduled reminders for your team")					
Add collaborators to all repositories	✓	✗	✗	✗	✗
Access the organization audit log	✓	✗	✗	✗	✗
Edit the organization's profile page (see "About your organization's profile")	✓	✗	✗	✗	✗
Verify the organization's domains (see "Verifying or approving a domain for your organization")	✓	✗	✗	✗	✗
Restrict email notifications to verified or approved domains (see "Restricting email notifications for your organization")	✓	✗	✗	✗	✗
Delete all teams	✓	✗	✗	✗	✗
Delete the organization account, including all repositories	✓	✗	✗	✗	✗
Create teams (see "Setting team creation permissions in your organization")	✓	✓	✓	✗	✓
Move teams in an organization's hierarchy	✓	✗	✗	✗	✗
Create	✓	✓	✓	✗	✓

Create project boards (see "Project (classic) permissions for an organization")	✓	✓	✓	✕	✓
See all organization members and teams	✓	✓	✓	✕	✓
@mention any visible team	✓	✓	✓	✕	✓
Can be made a *team maintainer*	✓	✓	✓	✕	✓
View organization insights (see "Viewing insights for your organization")	✓	✓	✓	✕	✓
Hide comments on writable commits, pull requests, and issues (see "Managing disruptive comments")	✓	✓	✓	✕	✓
Hide comments on *all* commits, pull requests, and issues (see "Managing disruptive comments")	✓	✕	✓	✕	✓
Block and unblock non-member contributors (see "Blocking a user from your organization")	✓	✕	✓	✕	✕
Limit interactions for certain	✓	✕	✓	✕	✕

for certain users in public repositories (see "Limiting interactions in your organization")					
Manage viewing of organization dependency insights (see "Changing the visibility of your organization's dependency insights")	✓	✕	✕	✕	✕
Set a team profile picture in all teams (see "Setting your team's profile picture")	✓	✕	✕	✕	✕
Sponsor accounts and manage the organization's sponsorships (see "Sponsoring open source contributors")	✓	✕	✕	✓	✓
Manage email updates from sponsored accounts (see "Managing updates from accounts your organization sponsors")	✓	✕	✕	✕	✕
Attribute your sponsorships to another organization (see "Attributing sponsorships to your organization" for details)	✓	✕	✕	✕	✕
Manage the publication of GitHub Pages sites from repositories	✓	✕	✕	✕	✕

repositories in the organization (see "Managing the publication of GitHub Pages sites for your organization")					
Manage security and analysis settings (see "Managing security and analysis settings for your organization")	✓	✕	✕	✕	✓
View security overview for the organization (see "About security overview")	✓	✕	✕	✕	✓
Enable and enforce SAML single sign-on	✓	✕	✕	✕	✕
Manage a user's SAML access to your organization	✓	✕	✕	✕	✕
Manage an organization's SSH certificate authorities (see "Managing your organization's SSH certificate authorities")	✓	✕	✕	✕	✕
Transfer repositories	✓	✕	✕	✕	✕
Purchase, install, manage billing for, and cancel GitHub Marketplace apps	✓	✕	✕	✕	✕

List apps in GitHub Marketplace	✓	✕	✕	✕	✕
Receive Dependabot alerts about insecure dependencies for all of an organization's repositories	✓	✕	✕	✕	✓
Manage Dependabot security updates (see "About Dependabot security updates")	✓	✕	✕	✕	✓
Manage the forking policy	✓	✕	✕	✕	✕
Limit activity in public repositories in an organization	✓	✕	✕	✕	✕
Pull (read) *all repositories* in the organization	✓	✕	✕	✕	✓
Push (write) and clone (copy) *all repositories* in the organization	✓	✕	✕	✕	✕
Convert organization members to outside collaborators	✓	✕	✕	✕	✕
View people with access to an organization repository	✓	✕	✕	✕	✕
Export a list of people with access to an organization repository	✓	✕	✕	✕	✕
Manage the default	✓	✕	✕	✕	✕

default branch name (see "Managing the default branch name for repositories in your organization")					
Manage default labels (see "Managing default labels for repositories in your organization")	✓	×	×	×	×
Enable team synchronization (see "Managing team synchronization for your organization")	✓	×	×	×	×
Manage pull request reviews in the organization (see "Managing pull request reviews in your organization")	✓	×	×	×	×
Manage organization-level rulesets (see "Managing rulesets for repositories in your organization")	✓	×	×	×	×

Further reading

- "Repository roles for an organization"
- "Project (classic) permissions for an organization"