Enforcing policies for security settings in your enterprise

In this article

You can enforce policies to manage security settings in your enterprise's organizations, or allow policies to be set in each organization.

> **Who can use this feature**
> Enterprise owners can enforce policies for security settings in an enterprise.

About policies for security settings in your enterprise

You can enforce policies to control the security settings for organizations owned by your enterprise on GitHub Enterprise Cloud. By default, organization owners can manage security settings.

Requiring two-factor authentication for organizations in your enterprise

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.

Enterprise owners can require that organization members, billing managers, and outside collaborators in all organizations owned by an enterprise use two-factor authentication to secure their user accounts.

Before you can require 2FA for all organizations owned by your enterprise, you must enable two-factor authentication for your own account. For more information, see "Securing your account with two-factor authentication (2FA)."

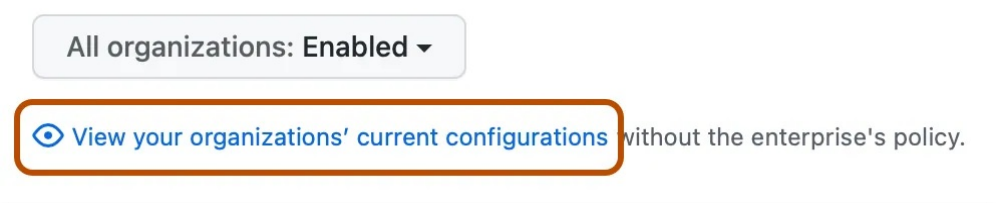
Warnings:

- When you require two-factor authentication for your enterprise, members, outside collaborators, and billing managers (including bot accounts) in all organizations owned by your enterprise who do not use 2FA will be removed from the organization and lose access to its repositories. They will also lose access to their forks of the organization's private repositories. You can reinstate their access privileges and settings if they enable two-factor authentication for their account within three months of their removal from your organization. For more information, see "Reinstating a former member of your organization."
- Any organization owner, member, billing manager, or outside collaborator in any of the organizations owned by your enterprise who disables 2FA for their account after you've enabled required two-factor authentication will automatically be removed from the organization.
- If you're the sole owner of an enterprise that requires two-factor authentication, you won't be able to disable 2FA for your user account without disabling required two-factor authentication for the enterprise.

Before you require use of two-factor authentication, we recommend notifying organization members, outside collaborators, and billing managers and asking them to set up 2FA for their accounts. Organization owners can see if members and outside collaborators already use 2FA on each organization's People page. For more information, see "Viewing whether users in your organization have 2FA enabled."

Note: Some of the users in your organizations may have been selected for mandatory two-factor authentication enrollment by GitHub.com, but it has no impact on how you enable the 2FA requirement for the organizations in your enterprise. If you enable the 2FA requirement for organizations in your enterprise, all users without 2FA currently enabled will be removed from the organizations, including those that are required to enable it by 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 **Authentication security**.
5. Under "Two-factor authentication", review the information about changing the setting. Optionally, to view the current configuration for all organizations in the enterprise account before you change the setting, click **View your organizations' current configurations**.



6. Under "Two-factor authentication", select **Require two-factor authentication for all organizations in your business**, then click **Save**.
7. If prompted, read the information about members and outside collaborators who will be removed from the organizations owned by your enterprise. To confirm the change, type your enterprise's name, then click **Remove members & require two-factor authentication**.
8. Optionally, if any members or outside collaborators are removed from the organizations owned by your enterprise, we recommend sending them an invitation to reinstate their former privileges and access to your organization. Each person must enable two-factor authentication before they can accept your invitation.

Managing SSH certificate authorities for your enterprise

You can use a SSH certificate authorities (CA) to allow members of any organization owned by your enterprise to access that organization's repositories using SSH certificates you provide. You can require that members use SSH certificates to access organization resources, unless SSH is disabled in your repository. For more information, see "About SSH certificate authorities."

When you issue each client certificate, you must include an extension that specifies which GitHub Enterprise Cloud user the certificate is for. For more information, see "About SSH certificate authorities."

Adding an SSH certificate authority

If you require SSH certificates for your enterprise, enterprise members should use a special URL for Git operations over SSH. For more information, see "About SSH certificate authorities."

Each certificate authority can only be uploaded to one account on GitHub.com. If an SSH certificate authority has been added to an organization or enterprise account, you cannot add the same certificate authority to another organization or enterprise 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 **Authentication security**.
5. To the right of "SSH Certificate Authorities", click **New CA**.
6. Under "Key," paste your public SSH key.
7. Click **Add CA**.
8. Optionally, to require members to use SSH certificates, select **Require SSH Certificates**, then click **Save**.

> **Note:** When you require SSH certificates, the requirement does not apply to authorized OAuth apps and GitHub Apps (including user-to-server tokens) or to GitHub features such as GitHub Actions and Codespaces, which are trusted environments within the GitHub ecosystem.

Deleting an SSH certificate authority

Deleting a CA cannot be undone. If you want to use the same CA in the future, you'll need to upload the CA again.

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 **Authentication security**.
5. Under "SSH Certificate Authorities", to the right of the CA you want to delete, click **Delete**.
6. Read the warning, then click **I understand, please delete this CA**.

Managing SSO for unauthenticated users

> **Note:** Automatically redirecting users to sign in is currently in beta for Enterprise Managed Users and subject to change.

If your enterprise uses Enterprise Managed Users, you can choose what unauthenticated users see when they attempt to access your enterprise's resources. For more information about Enterprise Managed Users, see "About Enterprise Managed Users."

By default, to hide the existence of private resources, when an unauthenticated user attempts to access your enterprise, GitHub displays a 404 error.

To prevent confusion from your developers, you can change this behavior so that users are automatically redirected to single sign-on (SSO) through your identity provider (IdP). When you enable automatic redirects, anyone who visits the URL for any of your enterprise's resources will be able to see that the resource exists. However, they'll only be able to see the resource if they have appropriate access after authenticating with your IdP.

> **Note:** If a user is signed in to their personal account when they attempt to access any of your enterprise's resources, they'll be automatically signed out and redirected to SSO to sign in to their managed user account. For more information, see "Managing multiple accounts."

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 **Authentication security**.
5. Under "Single sign-on settings", select or deselect **Automatically redirect users to sign in**.

Further reading

- "About SAML for enterprise IAM"
- "Accessing compliance reports for your enterprise"
- "Restricting network traffic to your enterprise with an IP allow list"