This article is also available in French.   ✕

GitHub Docs   **Version:** Free, Pro, & Team ⌄   Search GitHub Docs 🔍   🌐 | Sign up

☰ Organizations / Organization security / Manage 2FA / Require 2FA

Requiring two-factor authentication in your organization

Organization owners can require organization members, outside collaborators, and billing managers to enable two-factor authentication for their personal accounts, making it harder for malicious actors to access an organization's repositories and settings.

> **Who can use this feature?**
>
> 💼 Requiring two-factor authentication is available to organizations on a GitHub Free or GitHub Team plan, as well as organizations on GitHub Enterprise Cloud or GitHub Enterprise Server. With GitHub Enterprise Cloud, this feature is unavailable for organizations in an enterprise with managed users.

> **Note:** As of March 2023, GitHub required all users who contribute code on GitHub.com to enable one or more forms of two-factor authentication (2FA). If you were in an eligible group, you would have received a notification email when that group was selected for enrollment, marking the beginning of a 45-day 2FA enrollment period, and you would have seen banners asking you to enroll in 2FA on GitHub.com. If you didn't receive a notification, then you were 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](#).

About two-factor authentication for organizations 🔗

Two-factor authentication (2FA) is an extra layer of security used when logging into websites or apps. You can require all members, outside collaborators, and billing managers in your organization to enable two-factor authentication on GitHub. For more information about two-factor authentication, see "[Securing your account with two-factor authentication (2FA)](#)."

You can also require two-factor authentication for organizations in an enterprise. For more information, see "[Enforcing policies for security settings in your enterprise](#)."

> **Note**: Some of the users in your organization may have been selected for mandatory two-factor authentication enrollment by GitHub, but it has no impact on how you enable the 2FA requirement for your organization. If you enable the 2FA requirement in your organization, all users without 2FA currently enabled will be removed from your organization, including those that are required to enable it by GitHub.

> **Warnings:**
>
> - When you require use of two-factor authentication for your organization, members, outside collaborators, and billing managers who do not use 2FA will be removed from the organization and lose access to its repositories. They will also lose access to their

In this article

- About two-factor authentication for organizations
- Prerequisites
- Requiring two-factor authentication in your organization
- Viewing people who were removed from your organization
- Helping removed members and outside collaborators rejoin your organization
- Further reading

forks of the organization's private repositories. You can reinstate their access privileges and settings if they enable two-factor authentication for their personal account within three months of their removal from your organization. For more information, see "Reinstating a former member of your organization."

- You will also need to enable 2FA for unattended or shared access accounts, such as bots and service accounts. If you do not configure 2FA for these unattended accounts after you've enabled required two-factor authentication, the accounts will be removed from the organization and lose access to their repositories. For more information, see "Managing bots and service accounts with two-factor authentication."

- If an organization owner, member, billing manager, or outside collaborator disables 2FA for their personal account after you've enabled required two-factor authentication, they will automatically be removed from the organization.

- If you're the sole owner of an organization that requires two-factor authentication, you won't be able to disable 2FA for your personal account without disabling required two-factor authentication for the organization.

Prerequisites 🔗

Before you can require organization members, outside collaborators, and billing managers to use two-factor authentication, you must enable two-factor authentication for your account on GitHub. For more information, see "Securing your account with two-factor authentication (2FA)."

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. You can see if members and outside collaborators already use 2FA. For more information, see "Viewing whether users in your organization have 2FA enabled."

Requiring two-factor authentication in your organization 🔗

1. In the upper-right corner of GitHub, select your profile photo, then click 🏢 **Your organizations**.

2. Next to the organization, click **Settings**.

3. In the "Security" section of the sidebar, click 🛡 **Authentication security**.

4. Under "Two-factor authentication", select **Require two-factor authentication for everyone in your organization**, then click **Save**.

5. If prompted, read the information about members and outside collaborators who will be removed from the organization.

6. In the text field, type your organization's name to confirm the change, then click **Remove members & require two-factor authentication**.

7. If any members or outside collaborators are removed from the organization, we recommend sending them an invitation that can reinstate their former privileges and access to your organization. They must enable two-factor authentication before they can accept your invitation.

Viewing people who were removed from your organization 🔗

To view people who were automatically removed from your organization for non-compliance when you required two-factor authentication, you can search your organization's audit log for people removed from your organization. The audit log event will show if a person was removed for 2FA non-compliance. For more information, see "Reviewing the audit log for your organization."

1. In the upper-right corner of GitHub, select your profile photo, then click 🏢 **Your organizations**.

2 Next to the organization, click **Settings**.

3 In the "Archive" section of the sidebar, click ⧉ **Logs**, then click **Audit log**.

4 Enter your search query. To search for:

- Organization members removed, use `action:org.remove_member` in your search query
- Outside collaborators removed, use `action:org.remove_outside_collaborator` in your search query
- Billing managers removed, use `action:org.remove_billing_manager` in your search query

You can also view people who were removed from your organization by using a [time frame](#) in your search.

Helping removed members and outside collaborators rejoin your organization 🔗

If any members or outside collaborators are removed from the organization when you enable required use of two-factor authentication, they'll receive an email notifying them that they've been removed. They should then enable 2FA for their personal account, and contact an organization owner to request access to your organization.

Further reading 🔗

- "[Viewing whether users in your organization have 2FA enabled](#)"
- "[Securing your account with two-factor authentication (2FA)](#)"
- "[Reinstating a former member of your organization](#)"
- "[Reinstating a former outside collaborator's access to your organization](#)"

Help and support

Did you find what you needed?

👍 Yes   👎 No

[Privacy policy](#)

Help us make these docs great!

All GitHub docs are open source. See something that's wrong or unclear? Submit a pull request.

⤵ Make a contribution

[Learn how to contribute](#)

Still need help?

👥 [Ask the GitHub community](#)

💬 [Contact support](#)