Requiring two-factor authentication for an organization

In this article

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

When using LDAP or built-in authentication, two-factor authentication is supported on your GitHub Enterprise Server instance. Organization owners can require members to have two-factor authentication enabled.

When using SAML or CAS, two-factor authentication is not supported or managed on the GitHub Enterprise Server instance, but may be supported by the external authentication provider. Two-factor authentication enforcement on organizations is not available. For more information about enforcing two-factor authentication on organizations, see "Requiring two-factor authentication in your organization."

For more information, see "About two-factor authentication."

Requirements for enforcing two-factor authentication

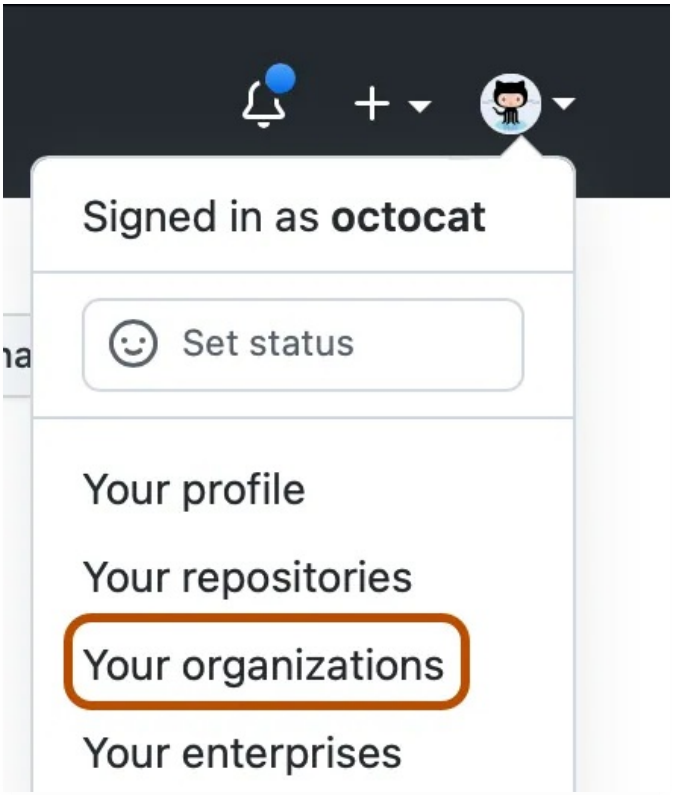
Before you can require organization members and outside collaborators to use 2FA, you must enable two-factor authentication for your own personal account.

Warnings:

- When your require two-factor authentication, members and outside collaborators (including bot accounts) who do not use 2FA will be removed from the organization and lose access to its repositories, including their forks of private repositories. If they enable 2FA for their personal account within three months of being removed from the organization, you can reinstate their access privileges and settings.
- When 2FA is required, organization members or outside collaborators who disable 2FA 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.

Before you require use of two-factor authentication, we recommend notifying organization members and outside collaborators and asking them to set up 2FA for their accounts. You can see if members and outside collaborators already use 2FA on an organization's People tab.

1. In the top right corner of GitHub Enterprise Server, click 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**.

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 the audit log using `reason:two_factor_requirement_non_compliance` in the search field.

1. In the upper-left corner of any page, click .
2. From an administrative account on GitHub Enterprise Server, in the upper-right corner of any page, click .
3. If you're not already on the "Site admin" page, in the upper-left corner, click **Site admin**.
4. In the "Archives" section of the sidebar, click **Security log**.
5. Enter your search query using `reason:two_factor_requirement_non_compliance`. To

narrow your search for:

- Organizations members removed, enter `action:org.remove_member AND reason:two_factor_requirement_non_compliance`
- Outside collaborators removed, enter `action:org.remove_outside_collaborator AND reason:two_factor_requirement_non_compliance`

You can also view people removed from a particular organization by using the organization name in your search:

- `org:octo-org AND reason:two_factor_requirement_non_compliance`

6. Click **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"