Preparing to require two-factor authentication in your organization

Before requiring two-factor authentication (2FA), you can notify users about the upcoming change and verify who already uses 2FA.

We recommend that you notify organization members and outside collaborators at least one week before you require 2FA in your organization.

When you require use of two-factor authentication for your organization, members, outside collaborators, and billing managers (including bot accounts) 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.

Before requiring 2FA in your organization, we recommend that you:

- Enable 2FA on your personal account. For more information, see "Securing your account with two-factor authentication (2FA)."
- Ask the people in your organization to set up 2FA for their accounts
- See whether users in your organization have 2FA enabled. For more information, see "Viewing whether users in your organization have 2FA enabled."
- Enable 2FA for unattended or shared access accounts, such as bots and service accounts. For more information, see "Managing bots and service accounts with two-factor authentication."
- Warn users that once 2FA is enabled, those without 2FA are automatically removed from the organization.