

This version of GitHub Enterprise was discontinued on 2023-03-15. No patch releases will be made, even for critical security issues. For better performance, improved security, and new features, [upgrade to the latest version of GitHub Enterprise](#). For help with the upgrade, [contact GitHub Enterprise support](#).

Accessing GitHub using two-factor authentication

In this article

Performing 2FA when signing in to the website

Using two-factor authentication with the command line

Using two-factor authentication to access a repository using Subversion

Troubleshooting

Further reading

With 2FA enabled, you'll be asked to provide your 2FA authentication code, as well as your password, when you sign in to GitHub Enterprise Server.

With two-factor authentication enabled, you'll need to provide an authentication code or use a security key when accessing GitHub Enterprise Server through your browser. If you access GitHub Enterprise Server using other methods, such as the API or the command line, you'll need to use an alternative form of authentication. For more information, see "[About authentication to GitHub](#)."

Performing 2FA when signing in to the website

After you sign in to GitHub Enterprise Server using your password, you'll need to provide an authentication code or use a security key to perform 2FA.

GitHub Enterprise Server will only ask you to provide your 2FA authentication code again if you've logged out, are using a new device, are performing a sensitive action, or your session expires. For more information on 2FA for sensitive actions, see "[Sudo mode](#)."

Generating a code through a TOTP application

If you chose to set up two-factor authentication using a TOTP application on your smartphone, you can generate an authentication code for GitHub Enterprise Server at any time. In most cases, just launching the application will generate a new code. You should refer to your application's documentation for specific instructions.

If you delete your authenticator application after configuring two-factor authentication, you'll need to provide your recovery code to get access to your account. Many TOTP apps support the secure backup of your authentication codes in the cloud and can be restored if you lose access to your device. For more information, see "[Recovering your account if you lose your 2FA credentials](#)."

Using a security key

If you've set up a security key on your account, and your browser supports security keys, you can use it to complete your sign in.

- 1 Using your username and password, sign in to GitHub Enterprise Server through your browser.
- 2 If you use a physical security key, ensure it's connected to your device.
- 3 To trigger the security key prompt from your operating system, select "Use security key".
- 4 Select the appropriate option in the prompt. Depending on your security key configuration, you may type a PIN, complete a biometric prompt, or use a physical security key.

Using two-factor authentication with the command line

After you've enabled 2FA, you will no longer use your password to access GitHub Enterprise Server on the command line. Instead, use Git Credential Manager, a personal access token, or an SSH key.

Authenticating on the command line using Git Credential Manager

[Git Credential Manager](#) is a secure Git credential helper that runs on Windows, macOS, and Linux. For more information about Git credential helpers, see [Avoiding repetition](#) in the Pro Git book.

Setup instructions vary based on your computer's operating system. For more information, see [Download and install](#) in the GitCredentialManager/git-credential-manager repository.

Authenticating on the command line using HTTPS

You must create a personal access token to use as a password when authenticating to GitHub Enterprise Server on the command line using HTTPS URLs.

When prompted for a username and password on the command line, use your GitHub Enterprise Server username and personal access token. The command line prompt won't specify that you should enter your personal access token when it asks for your password.

For more information, see "[Managing your personal access tokens](#)."

Authenticating on the command line using SSH

Enabling 2FA doesn't change how you authenticate to GitHub Enterprise Server on the command line using SSH URLs. For more information about setting up and using an SSH key, see "[Connecting to GitHub with SSH](#)."

Using two-factor authentication to access a repository using Subversion

Note: Subversion support will be removed from GitHub on January 8, 2024. A future release of GitHub Enterprise Server after January 8, 2024 will also remove Subversion support. To read more about this, see [the GitHub blog](#).

When you access a repository via Subversion, you must provide a personal access token instead of entering your password. For more information, see "[Managing your personal access tokens](#)."

Troubleshooting

If you lose access to your two-factor authentication credentials, you can use your recovery codes or another recovery method (if you've set one up) to regain access to your account. For more information, see "[Recovering your account if you lose your 2FA credentials](#)."

If your authentication fails several times, you may wish to synchronize your phone's clock with your mobile provider. Often, this involves checking the "Set automatically" option on your phone's clock, rather than providing your own time zone.

Further reading

- "[About two-factor authentication](#)"
- "[Configuring two-factor authentication](#)"
- "[Configuring two-factor authentication recovery methods](#)"
- "[Recovering your account if you lose your 2FA credentials](#)"

Legal

© 2023 GitHub, Inc. [Terms](#) [Privacy](#) [Status](#) [Pricing](#) [Expert services](#) [Blog](#)