Connecting to GitHub with SSH

You can connect to GitHub using the Secure Shell Protocol (SSH), which provides a secure channel over an unsecured network.

About SSH

Using the SSH protocol, you can connect and authenticate to remote servers and services. With SSH keys, you can connect to GitHub without supplying your username and personal access token at each visit. You can also use an SSH key to sign commits.

Using SSH agent forwarding

To simplify deploying to a server, you can set up SSH agent forwarding to securely use local SSH keys.

Managing deploy keys

Learn different ways to manage SSH keys on your servers when you automate deployment scripts and which way is best for you.

Checking for existing SSH keys

Before you generate an SSH key, you can check to see if you have any existing SSH keys.

Generating a new SSH key and adding it to the ssh-agent

After you've checked for existing SSH keys, you can generate a new SSH key to use for authentication, then add it to the ssh-agent.

Adding a new SSH key to your GitHub account

To configure your account on GitHub.com to use your new (or existing) SSH key, you'll also need to add the key to your account.

Testing your SSH connection

After you've set up your SSH key and added it to GitHub, you can test your connection.

Working with SSH key passphrases

You can secure your SSH keys and configure an authentication agent so that you won't have to reenter your passphrase every time you use your SSH keys.