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.

You can access and write data in repositories on GitHub.com using SSH (Secure Shell Protocol). When you connect via SSH, you authenticate using a private key file on your local machine. For more information about SSH, see Secure Shell on Wikipedia.

When you set up SSH, you will need to generate a new private SSH key and add it to the SSH agent. You must also add the public SSH key to your account on GitHub before you use the key to authenticate or sign commits. For more information, see "Generating a new SSH key and adding it to the ssh-agent", "Adding a new SSH key to your GitHub account" and "About commit signature verification."

You can further secure your SSH key by using a hardware security key, which requires the physical hardware security key to be attached to your computer when the key pair is used to authenticate with SSH. You can also secure your SSH key by adding your key to the ssh-agent and using a passphrase. For more information, see "Working with SSH key passphrases."

To use your SSH key with a repository owned by an organization that uses SAML single sign-on, you must authorize the key. For more information, see "Authorizing an SSH key for use with SAML single sign-on" in the GitHub Enterprise Cloud documentation.

To maintain account security, you can regularly review your SSH keys list and revoke any keys that are invalid or have been compromised. For more information, see "Reviewing your SSH keys."

If you haven't used your SSH key for a year, then GitHub will automatically delete your inactive SSH key as a security precaution. For more information, see "Deleted or missing SSH keys."

Organizations that use GitHub Enterprise Cloud can provide SSH certificates, which members can use to access that organization's repositories without adding the certificate to their account on GitHub. If you're using an SSH certificate, you cannot use the certificate to access forks of the organization's repositories, if the fork is owned by your personal account. For more information, see "About SSH certificate authorities" in the GitHub Enterprise Cloud documentation.

Further reading

- "Troubleshooting SSH"