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 or password at each visit.

When you set up SSH, you'll generate an SSH key and add it to the ssh-agent and then add the key to your GitHub account. Adding the SSH key to the ssh-agent ensures that your SSH key has an extra layer of security through the use of a passphrase. For more information, see "Working with SSH key passphrases."

We recommend that you regularly review your SSH keys list and revoke any that are invalid or have been compromised.

Note: Organizations that use SAML single sign-on (SSO) cannot be accessed with SSH. To access repositories in organizations that use SAML SSO, use an authorized personal access token with HTTPS.

Further reading

- "Checking for existing SSH keys"
- "Testing your SSH connection"
- "Working with SSH key passphrases"
- "Troubleshooting SSH"