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."

To use your SSH key with a repository owned by an organization that uses SAML single sign-on, you'll need to authorize it first. For more information, see "Authorizing an SSH key for use with SAML single sign-on."

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

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."

If you're a member of an organization that provides SSH certificates, you can use your certificate to access that organization's repositories without adding the certificate to your GitHub account. For more information, see "About SSH certificate authorities."

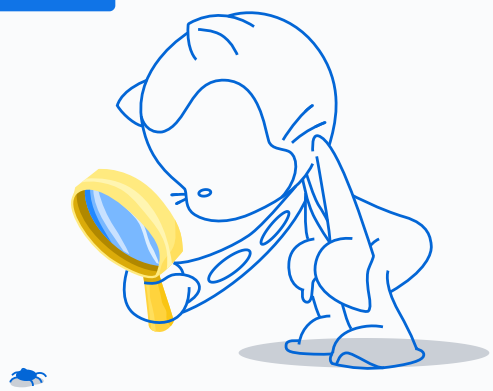
Further reading

- "Checking for existing SSH keys"
- "Testing your SSH connection"
- "Working with SSH key passphrases"
- "Troubleshooting SSH"
- "Authorizing an SSH key for use with SAML single sign-on"

Ask a human

Can't find what you're looking for?

Contact us



GitHub

Product	Platform	Support	Company
Features	Developer API	Help	About
Security	Partners	Community Forum	Blog
Enterprise	Atom	Training	Careers
Case Studies	Electron	Status	Press
Pricing	GitHub Desktop	Contact GitHub	Shop
Resources			