Testing your SSH connection

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

Before testing your SSH connection, you should have:

- Checked for existing SSH keys
- Generated a new SSH key
- Added a new SSH key to your GitHub account

When you test your connection, you'll need to authenticate this action using your password, which is the SSH key passphrase you created earlier. For more information on working with SSH key passphrases, see "Working with SSH key passphrases".

1. Open Git Bash.
2. Enter the following:

```
$ ssh -T git@github.com
# Attempts to ssh to GitHub
```

You may see one of these warnings:

```
The authenticity of host 'github.com (192.30.252.1)' can't be established.
RSA key fingerprint is 16:27:ac:a5:76:28:2d:36:63:1b:56:4d:eb:df:a6:48.
Are you sure you want to continue connecting (yes/no)?
```

```
The authenticity of host 'github.com (192.30.252.1)' can't be established.
RSA key fingerprint is SHA256:nThbg6kXUpJWGl7E1IGOCspRomTxdCARLviKw6E5SY8.
Are you sure you want to continue connecting (yes/no)?
```

Note: The example above lists the GitHub IP address as 192.30.252.1. When pinging GitHub, you may see a range of IP addresses. For more information, see "What IP addresses does GitHub use that I should whitelist?"

3. Verify that the fingerprint in the message you see matches one of the messages in step 2, then type `yes`:

```
Hi username! You've successfully authenticated, but GitHub does not
provide shell access.
```

4. Verify that the resulting message contains your username. If you receive a "permission denied" message, see "Error: Permission denied (publickey)".

Contact a human

Article versions

GitHub.com
GitHub Enterprise 2.10
GitHub Enterprise 2.9
GitHub Enterprise 2.8

© 2017 GitHub Inc. All rights reserved.