Testing your SSH connection

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

Mac Windows Linux

Before testing your SSH connection, you should have already:

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

You'll need to authenticate this action using your password, which is the SSH key passphrase you created earlier. See "Working with SSH key passphrases."

1. Open Terminal.
2. Enter the following:

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

You may see a warning like this:

```
> The authenticity of host 'github.com (IP ADDRESS)' can't be
established.
> ED25519 key fingerprint is SHA256:+DiY3wvvV6TuJJhbpZisF/
zLDA0zPMSvHdkr4UvCOqU.
> Are you sure you want to continue connecting (yes/no)?
```

3. Verify that the fingerprint in the message you see matches GitHub's public key fingerprint. If it does, then type `yes`:

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

You may see this error message:

```
...
Agent admitted failure to sign using the key.
debug1: No more authentication methods to try.
Permission denied (publickey).
```

This is a known problem with certain Linux distributions. For more information, see "Error: Agent admitted failure to sign."

> **Note:** The remote command should exit with code 1.

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

Legal