ssh-copy-id -i ~/.ssh/mykey user@host

[**https://www.digitalocean.com/community/tutorials/how-to-configure-apache-using-ansible-on-ubuntu-14-04**](https://www.digitalocean.com/community/tutorials/how-to-configure-apache-using-ansible-on-ubuntu-14-04)

### TEST THE NEW KEY

Once the key has been copied, it is best to test it:

ssh -i ~/.ssh/mykey user@host

nano ~/.ssh/authorized\_keys.

**Creating SSH keys**

* 1. Check for existing SSH keys
* 2. Back up old SSH keys
* 3. Generate a new SSH key
* Creating an SSH key on Linux & Mac OS X
* 1. Check for existing SSH keys
* 2. Back up old SSH keys
* 3. Generate a new key

**Related content**

* SSH user keys for personal use
* SSH access keys for system use
* Getting started with Git and Bitbucket Server
* Clone your repository and manage files locally
* Bitbucket Data Center in AWS
* Importing code from an existing project

This page describes how to create SSH keys.

SSH keys can be used to establish a secure connection with Bitbucket Server for:

* when you are performing Git operations from your local machine
* when another system or process needs access to repositories in Bitbucket Server (for example your build server)

Creating an SSH key on Windows

**1. Check for existing SSH keys**

You should check for existing SSH keys on your local computer.*You can use an existing SSH key with Bitbucket Server if you want, in which case you can go straight to either SSH user keys for personal use or SSH access keys for system use.*

Open a command prompt, and run:

cd %userprofile%/.ssh

* If you see "No such file or directory", then there aren't any existing keys: ***go to step 3****.*
* Check to see if you have a key already:

dir id\_\*

If there are existing keys, you may want to use those: go to either SSH user keys for personal use or SSH access keys for system use.

**2. Back up old SSH keys**

If you have existing SSH keys, but you don't want to use them when connecting to Bitbucket Server, you should back those up.

In a command prompt on your local computer, run:

mkdir key\_backup

copy id\_rsa\* key\_backup

**3. Generate a new SSH key**

If you don't have an existing SSH key that you wish to use, generate one as follows:

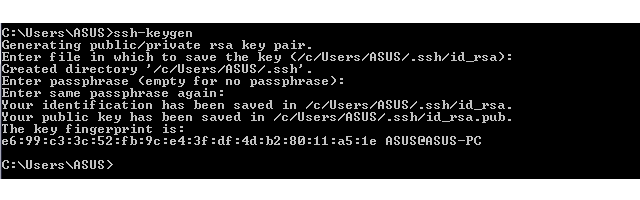
1. Log in to your local computer as an administrator.
2. In a command prompt, run:

ssh-keygen -t rsa -C "your\_email@example.com"

Associating the key with your email address helps you to identify the key later on.

Note that the ssh-keygen command is only available if you have already installed Git (with Git Bash).  
You'll see a response similar to this:

https://confluence.atlassian.com/bitbucketserver/files/776639788/776639789/1/1386202193726/STASH_11_win_keygen_1.png

1. Just press <Enter> to accept the default location and file name. If the .ssh directory doesn't exist, the system creates one for you.
2. Enter, and re-enter, a passphrase when prompted. The whole interaction will look similar to this:  
   
3. .

Creating an SSH key on Linux & Mac OS X

**1. Check for existing SSH keys**

You should check for existing SSH keys on your local computer.*You can use an existing SSH key with Bitbucket Server if you want, in which case you can go straight to either SSH user keys for personal use or SSH access keys for system use.*

Open a terminal and run the following:

cd ~/.ssh

* If you see "No such file or directory, then there aren't any existing keys: ***go to step 3****.*
* Check to see if you have a key already:

ls id\_\*

* If there are existing keys, you may want to use them; go to either SSH user keys for personal use or SSH access keys for system use.

**2. Back up old SSH keys**

If you have existing SSH keys, but you don't want to use them when connecting to Bitbucket Server, you should back those up.

Do this in a terminal on your local computer, by running:

mkdir key\_backup

cp id\_rsa\* key\_backup

**3. Generate a new key**

If you don't have an existing SSH key that you wish to use, generate one as follows:

1. Open a terminal on your local computer and enter the following:

ssh-keygen -t rsa -C "your\_email@example.com"

Associating the key with your email address helps you to identify the key later on.

You'll see a response similar to this:

https://confluence.atlassian.com/bitbucketserver/files/776639788/776639791/1/1386202192799/STASH_11_keygen1.png

1. Just press <Enter> to accept the default location and file name. If the .ssh directory doesn't exist, the system creates one for you.
2. Enter, and re-enter, a passphrase when prompted.  
   The whole interaction will look similar to this:

