

Set up your first SSH keys
Tutorials (<https://upcloud.com/community/tutorials/>).
authentication

How to use SSH keys for

Preparing your server

Using OpenSSH to generate a key pair

Using PuTTYTray to generate a key pair

Turn off password authentication

Conclusions

How to use SSH keys for authentication



Janne Ruostemaa

(<https://upcloud.com/blog/author/raiou/>)

Staff

Getting Started (<https://upcloud.com/tutorials-category/getting-started/>). Updated on 2020-11-06

27

Set up your first SSH keys

(<https://upcloud.com>)

Use **SSH keys** (<https://upcloud.com/community/tutorials/managing-ssh-keys/>) for authentication when you are connecting to your server, or even between your servers. They can greatly simplify and increase the security of your login process. When keys are implemented correctly they provide a secure, fast, and easy way of accessing your cloud server.

Set up your first SSH keys

Preparing your server

Follow our guide and learn how to set up your first SSH keys for authentication using OpenSSH or PuTTYTray.

Using OpenSSH to generate a key pair

[Test hosting on UpCloud! \(https://upcloud.com/signup/\)](https://upcloud.com/signup/)

Using PuTTYTray to generate a key pair

Preparing your server

Turn off password authentication

To add an SSH key pair, first, create a hidden folder to your user account home directory on your cloud server with the following command.

Conclusions

```
mkdir -p ~/.ssh
```

Then restrict the permissions to that directory to just yourself with the command below.

```
chmod 700 ~/.ssh
```

This creates a secure location for you to save your SSH keys for authentication. However, note that since the keys are stored in your user home directory, every user that wishes to connect using SSH keys for authentication has to repeat these steps on their own profile.

Using OpenSSH to generate a key pair

Set up your first SSH keys

Now continue on your own computer if you are using Linux or any other OS that has OpenSSH. PuTTY users should skip to the next section.

Preparing your server

1. Generate a new key pair in a terminal with the next command

Using OpenSSH to generate a key pair

Using PuTTYTray to generate a key pair

```
ssh-keygen -t rsa
```

Turn off password authentication

The key generator will ask for location and file name to which the key is saved to. Enter a new name or use the default by pressing enter.

Conclusions

2. (Optional) Create a passphrase for the key when prompted

This is a simple password that will protect your private key should someone be able to get their hands on it. Enter the password you wish or continue without a password. Press enter twice. Note that some automation tools might not be able to unlock passphrase-protected private keys.

3. Copy the public half of the key pair to your cloud server using the following command

Replace the user and server with your username and the server address you wish to use the key authentication on.

```
ssh-copy-id -i ~/.ssh/id_rsa.pub user@server
```

This also assumes you saved the key pair using the default file name and location. If not, just replace the key path `~/.ssh/id_rsa.pub` above with your own key name.

Enter your user account password for that SSH server when prompted.

Set up your first SSH keys

You can now authenticate to your server with the key pair, but at the moment you would need to enter the passphrase every time you connect.

Preparing your server

Using OpenSSH to generate a key pair

4. (Optional) Set up SSH Agent to store the keys to avoid having to re-enter passphrase at every login

Using PuTTYTray to generate a key pair

Turn off password authentication

Enter the following commands to start the agent and add the private SSH key.

Conclusions

```
ssh-agent $BASH
ssh-add ~/.ssh/id_rsa
```

Type in your key's current passphrase when asked. If you saved the private key somewhere other than the default location and name, you'll have to specify it when adding the key.

Afterwards, you can connect to your cloud server using the keys for authentication, and only having to unlock the key by repeating the last 2 steps once after every computer restart.

Using PuTTYTray to generate a key pair

If you are running Windows and **PuTTYTray**.

(<https://puttytray.goeswhere.com/>) for SSH, you can use the built-in key generator from PuTTY to create a new key pair.

(<https://upcloud.com>).

1. Click the **Keygen** button at the bottom of the *PuTTY Configuration* window to get started.

Set up your first SSH keys

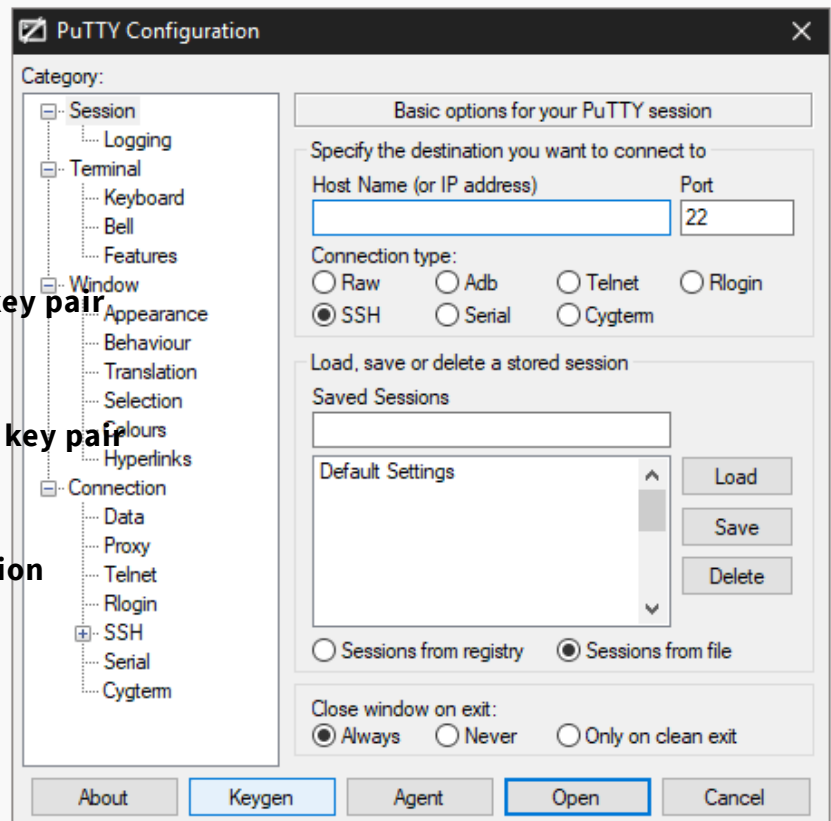
Preparing your server

Using OpenSSH to generate a key pair

Using PuTTYTray to generate a key pair

Turn off password authentication

Conclusions



Then in the *Key Generator* window, check that the *Type of key to generate* at the bottom is set to *SSH-2 RSA*. The older SSH-1 was the first version on the standard but is now generally considered obsolete. Most modern servers and clients support SSH-2.

2. Click the **Generate** button to begin.

Set up your first SSH keys

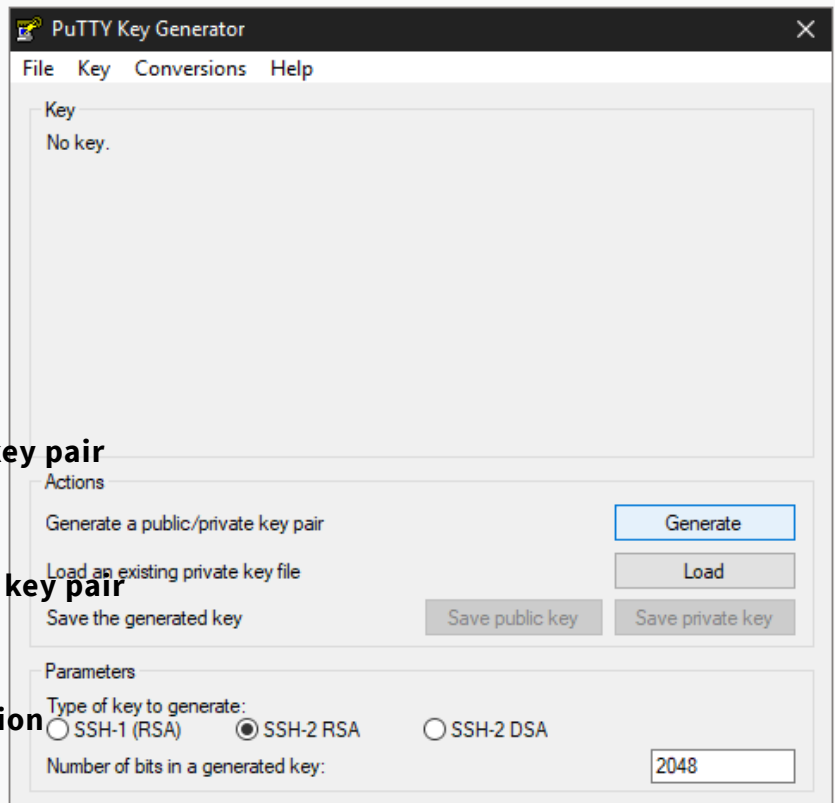
Preparing your server

Using OpenSSH to generate a key pair

Using PuTTYTray to generate a key pair

Turn off password authentication

Conclusions



3. Keep moving your mouse over the blank area in any manner to help generate randomness for a few moments until the progress is complete.

Set up your first SSH keys

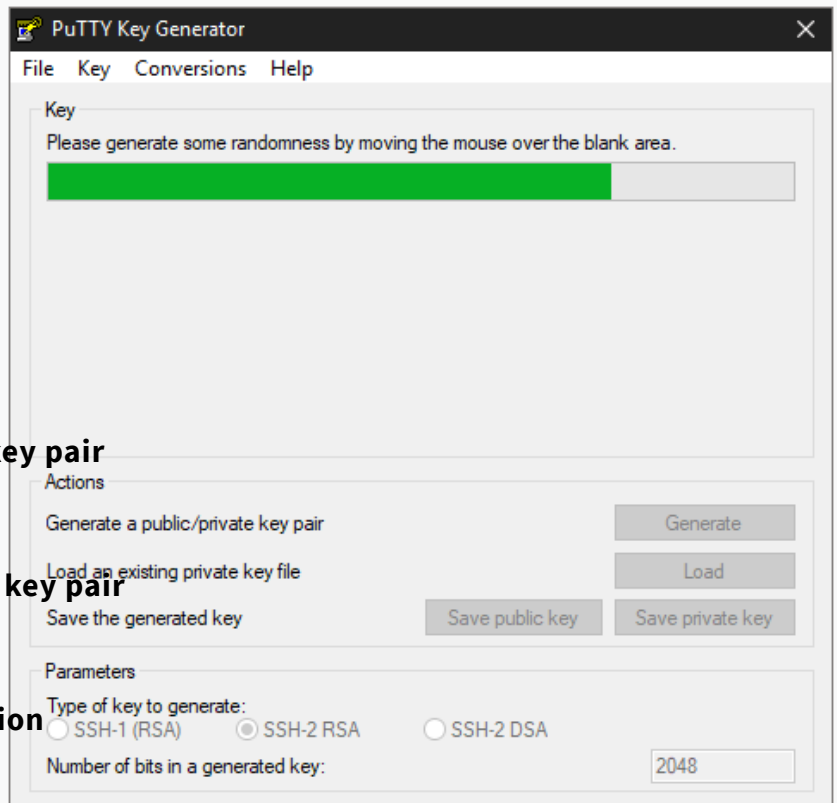
Preparing your server

Using OpenSSH to generate a key pair

Using PuTTYTray to generate a key pair

Turn off password authentication

Conclusions



With the keys finished, PuTTY will show the relative information about the pair along with the public key for easier copying.

4. (Optional) Enter a key passphrase in the 2 empty fields for the added security before continuing. The passphrase will protect your key from unauthorized use should someone be able to copy it. However, some automation tools might not be able to unlock passphrase-protected private keys.

5. Click the *Save private key* button and store it somewhere safe. Generally anywhere in your user directory is fine as long as your PC is password protected. Before closing the keygen, you may want to copy the public key to your clipboard, but you can always get it later as well.

Set up your first SSH keys

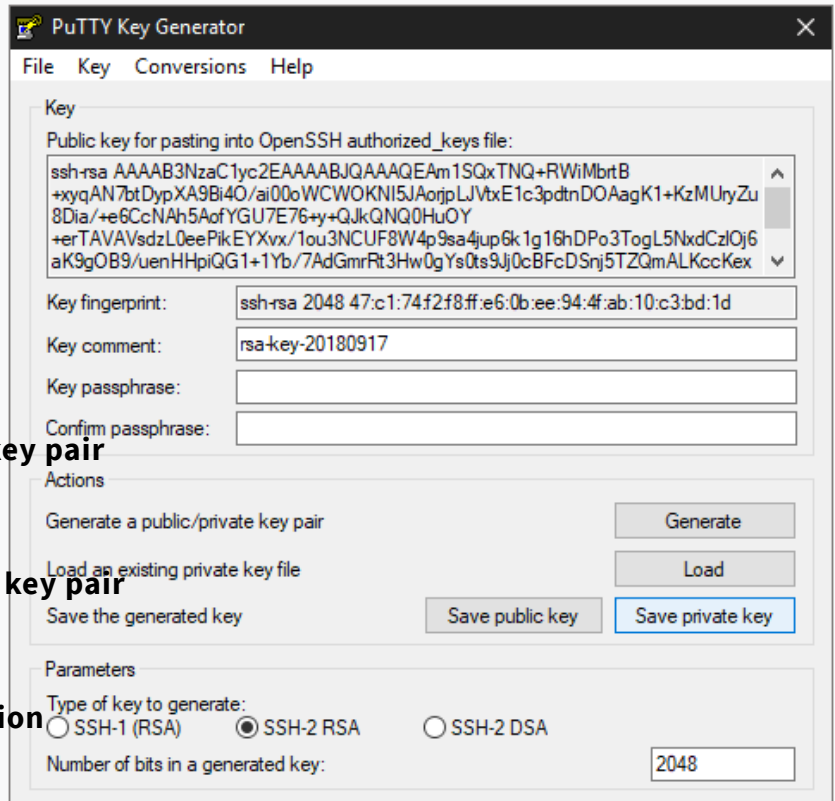
Preparing your server

Using OpenSSH to generate a key pair

Using PuTTYTray to generate a key pair

Turn off password authentication

Conclusions



Now that you have a new key saved on your computer, you'll need to import it into the PuTTY key agent.

6. Click the *Agent* button to open the key manager in the PuTTY Configuration window.

Set up your first SSH keys

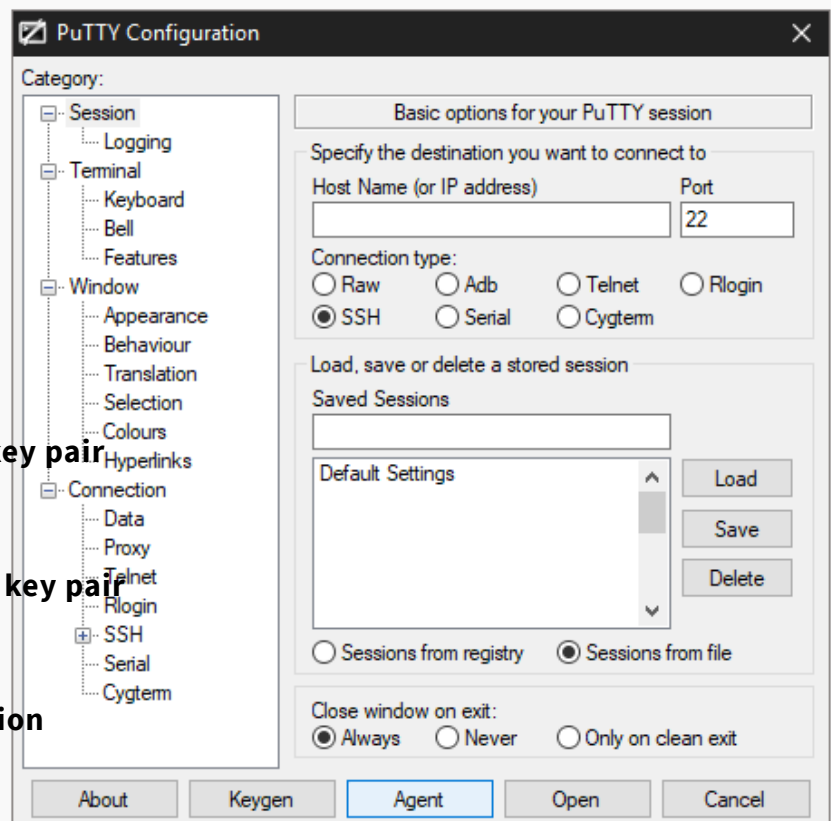
Preparing your server

Using OpenSSH to generate a key pair

Using PuTTYTray to generate a key pair

Turn off password authentication

Conclusions



7. Click *Add Key* button in the Key List, then browse to the location you saved the private key, select it and click *Open*.

Enter your key passphrase if asked.

Set up your first SSH keys

Preparing your server

Using OpenSSH to generate a key pair

Using PuTTYTray to generate a key pair



Turn off password authentication

Conclusions

This will import the key to your PuTTY client, but you still need to copy the public key over to your server.

8. Open an SSH connection to your cloud server and go to the SSH key directory.

```
cd ~/.ssh/
```

9. Open or create the default file OpenSSH looks for public keys called `authorized_keys`.

```
sudo nano authorized_keys
```

10. Paste the public key into the file by simply right-clicking the SSH client window. Make sure the key goes on a single line for OpenSSH to be able to read it. Note that the key type needs to also be included, `ssh-rsa` as shown in the example below.

(<https://upcloud.com>)

```
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQgQDEeV/UKOVqNUwmEL
```

Set up your first SSH keys

Preparing your server

Using OpenSSH to generate a key pair

Using PuTTYTray to generate a key pair

Turn off password authentication

Conclusions

When you've copied the public key over to the authorized keys list, save the file and exit the editor. You can now test the public key authentication by logging in to your server again. You should not get asked for your password, but instead logged straight in with the key. If it's not working, check that your private key is unlocked at your SSH Agent and try again.

Turn off password authentication

With SSH key authentication configured and tested, you can disable password authentication for SSH all together to prevent brute-forcing. When logged in to your cloud server.

1. Open the SSH configuration file with the following command.

```
sudo nano /etc/ssh/sshd_config
```

2. Set the password authentication to *no* to disable clear text passwords.

```
PasswordAuthentication no
```

3. Check that public key authentication is enabled, just to be safe and not get locked out from your server. If you do find yourself unable to log in with SSH, you can always use the Web terminal at your UpCloud control panel.

(<https://upcloud.com>).

```
PubkeyAuthentication yes
```

Then save and exit the editor.

Set up your first SSH keys

4. Restart the SSH service to apply the changes by using the command below.

Preparing your server

```
sudo systemctl restart sshd
```

Using OpenSSH to generate a key pair

Using PuTTYTray to generate a key pair

With that done your cloud server is now another step along towards security. Malicious attempts to connect to your server will result in authentication rejection, as plain passwords are not allowed, and brute-forcing an RSA key is practically impossible.

Turn off password authentication

Conclusions

Conclusions

Remember to always keep your private keys safe. You can use the same key from multiple computers if you wish, or generate new ones on each client connecting to your cloud server for added security. Each user should generate their own key pair and passphrase for secure access control. With proper management, even in case one of the private keys gets compromised you won't have to replace them all.




Janne Ruostemaa

(<https://upcloud.com/blog/author/raiou/>)

Editor-in-chief and Technical writer at UpCloud since 2015. Cloud enthusiast writing about server technology and software.

(<https://upcloud.com>)

Share this tutorial

 **Twitter** ([https://twitter.com/share?url=https://upcloud.com/community/tutorials/use-ssh-keys-authentication/&text=How to use SSH keys for authentication &hashtags=upcloud](https://twitter.com/share?url=https://upcloud.com/community/tutorials/use-ssh-keys-authentication/&text=How%20to%20use%20SSH%20keys%20for%20authentication&hashtags=upcloud))

 **Facebook** (<https://www.facebook.com/sharer.php?u=https://upcloud.com/community/tutorials/use-ssh-keys-authentication/>)

Set up your first SSH keys

Preparing your server

Using OpenSSH to generate a key pair

Using PuTTYTray to generate a key pair

27 thoughts on “How to use SSH keys for authentication”

Turn off password authentication



Walt says:

Conclusions

2019-02-13 at 11:23

(<https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-1868>)

Already setup ssh keys on server and running well. But now my local computer is dead and maybe motherboard is dead and cannot connect to server as private keys were saved in computer. Now lost private keys with computer and cannot connect to server. How to fix this problem?

Pls send detailed answers how to connect again to server.

Thanks

Walt

[Reply](#)



Janne Ruostemaa says:

2019-02-13 at 12:13

(<https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-1869>)

Hi Walt, sorry to hear about your computer. If you can't recover the private key from your hard drive, you can always reset the root password following

(<https://upcloud.com>)

these steps: [https://upcloud.com/community/](https://upcloud.com/community/(https://upcloud.com/community/)./tutorials/reset-root-password-cloud-server/)
[\(https://upcloud.com/community/\)](https://upcloud.com/community/(https://upcloud.com/community/)./tutorials/reset-root-password-cloud-server/)
[/tutorials/reset-root-password-cloud-server/](https://upcloud.com/community/(https://upcloud.com/community/)./tutorials/reset-root-password-cloud-server/)

[Reply](#)

Set up your first SSH keys

Preparing your server



Sarun says:

2019-06-28 at 17:05

Using OpenSSH to generate a key pair [.\(https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-12592\)](https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-12592)

Awesome! thanks for the information. I was trying to

Using PuTTYTray to generate a key pair the private key for the appuser to use it in Azure ADO service connection and this really helped.

Turn off password authentication

[Reply](#)

Conclusions



Daniel says:

2019-10-01 at 09:07

[.\(https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-28827\)](https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-28827)

Hey there bud,

So im trying to follow your guide because I have an assignment that requires me to get access to the ubuntu server from ssh, without the need for passwords on the admins.

Yet at almost the very beginning of the guide im stuck, on my win10 laptop I tried to copy ssh, and it doesnt recognize the command. So what am I supposed to do here?

[Reply](#)



Janne Ruostemaa says:

2019-10-02 at 10:34

[.\(https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-29073\)](https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-29073)

[.\(https://upcloud.com\)](https://upcloud.com)

Hi Daniel, thanks for the question. The terminal commands are intended for Linux systems but you can find instructions on how to do the same on Windows in the section about PuTTYTray.

Alternatively, you could **install the Windows Subsystem for Linux (WSL)**.

([https://docs.microsoft.com/en-](https://docs.microsoft.com/en-us/windows/wsl/install-win10)

us/windows/wsl/install-win10), allowing you to run Linux terminal commands on your Windows laptop.

Set up your first SSH keys

Preparing your server

Using OpenSSH to generate a key pair

Reply

Using PuTTYTray to generate a key pair



Daniel says:

2019-10-04 at 10:29

Turn off password authentication

(<https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-29513>)

Conclusions

I used another program called WinSCP 5.15, since it was alot easier to actually pair the two pc's together. Putty as shown in your guide isnt the same version I tried and got confused by other guides because they didnt seem to have the same guide either.

But got it sorted, thanks for the guide friend!

Reply



Janne Ruostemaa says:

2019-10-07 at 20:37

(<https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-30065>)

Indeed, PuTTY is slightly different to PuTTYtray that is linked in this guide. WinSCP then again is more akin to an FTP client and doesn't include SSH option. Each server different purposes but glad to hear you managed to complete the task.

Reply

(<https://upcloud.com>)



ardan (<http://ardan7779.web.id>) says:

2019-10-14 at 03:44

(<https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-31451>)

Set up your first SSH keys

I have try the instructions with Putty, but i have an issue I Cannot login with error “Access Denied”, even though I have double check my username is correct, and it ask to use password, so i use the passphrase from the private key.

Preparing your server

Using OpenSSH to generate a key pair How to fix it..?

Reply

Using PuTTYTray to generate a key pair



Janne Ruostemaa says:

Turn off password authentication

2019-10-14 at 07:07

(<https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-31472>)

Conclusions

Hi Ardan, thanks for the question. By the sound of it, you haven’t yet copied the public half of your SSH key onto your server. Use PuTTY to SSH into your server and log in with the server password. The private key passphrase is just to unlock the key when you wish to use it, the server has its own password.

Reply



Bobby Zopfan (<https://Bathinda.xyz>) says:

2019-10-18 at 07:15

(<https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-32095>)

I’ve deleted all my private key files from my own windows pc (c:\users\bob.ssh\idrsa) and still I’m able to connect to my DO droplet. How come?

And on Win10 Bash, I’ve deleted the keys from

“C:\Users\Bob\AppData\Local\Packages\CanonicalGroupLimited and still I’m able to connect. How come?

(<https://upcloud.com>)

Reply



Janne Ruostemaa says:

2019-10-18 at 07:38

(<https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-32098>)

Set up your first SSH keys

Preparing your server

Using OpenSSH to generate a key pair

Hi Bobby, thanks for the question. Your private key is still likely cached in memory by your SSH agent or similar if you are able to connect using it even after deleting the private key file itself. Restarting your computer should clear that.

Reply

Using PuTTYTray to generate a key pair



Moamen says:

Turn off password authentication

2019-12-09 at 15:36

(<https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-41251>)

Conclusions

Hi Janne,

Is there a way to create ssh account for specific directory and it's content ?

Reply



Janne Ruostemaa says:

2019-12-10 at 11:59

(<https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-41300>)

Hi there, thanks for the question. There are a couple of ways to go about restricting SSH user permissions, one relatively simple solution would be **using rbash** (<https://www.tecmint.com/rbash-a-restricted-bash-shell-explained-with-practical-examples/>).

Reply



Mike (<http://m.com>) says:

(<https://upcloud.com>)

2020-07-15 at 23:29

(<https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-87992>)

Have you considered ftp?

Reply

Set up your first SSH keys



Janne Ruostemaa says:

Preparing your server

2020-07-16 at 11:55

(<https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-88092>)

Using OpenSSH to generate a key pair

Using PuTTYTray to generate a key pair

Turn off password authentication

Hi Mike, thanks for the comment. You are right that FTP can be used to restrict access to only specific directory and files, but in contrast to SSH, it lacks the possibility to run programs.

Reply

Conclusions



Jason Dinh (<http://tapbutdao.com>) says:

2020-04-07 at 18:55

(<https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-63171>)

hello Janne,

I have tried your method 1 (open ssh)
after turned PasswordAuthentication no
and restart the server then connect to server back I cannot
login back to my server cause this problem
“root@94.237.65.61: Permission denied (publickey)”
– can you help?

Reply



Janne Ruostemaa says:

2020-04-07 at 22:20

(<https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-63171>)

(<https://upcloud.com>)

[ssh-keys-authentication/#comment-63214](#))

Hi Jason, thanks for the question. It's possible that your public SSH key is missing on the server or has too broad permissions for the SSH service to accept using it. On our cloud servers, you can always use the web console at your control panel to access the server terminal directly allowing password login.

Set up your first SSH keys

Preparing your server

[Reply](#)

Using OpenSSH to generate a key pair



valerio says:

Using PuTTYTray to generate a key pair

2020-05-17 at 14:25

[\(https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-73584\)](#)

Turn off password authentication

Hello janne.

Conclusions

Can i access to a ssh server from another ssh server (or client) with the private key of the first ssh server without insert the password? I'm on a machine that wants to connect with this ssh server. I have his id_rsa (private key) and i tried to typing the following command: ssh -i id_rsa server@ip but still he keeps asking me for the password.

Thanks in advance for your time

[Reply](#)



Janne Ruostemaa says:

2020-05-18 at 10:50

[\(https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-73772\)](#)

Hi Valerio, thanks for the question. Yes, you can. What you are referring to is called SSH agent forwarding. You need to enable it on your local SSH client by setting ForwardAgent yes e.g. in the /etc/ssh/ssh_config. It also needs to be enabled on all SSH servers you wish to use to connect through to another server by setting AllowAgentForwarding yes in the /etc/ssh/sshd_config file, this might be enabled

[\(https://upcloud.com\)](#)

by default. Once these are set, just reconnect using SSH with the private keys you have configured on your servers.

[Reply](#)

Set up your first SSH keys

Preparing your server



Taufique says:

2020-06-17 at 02:34

Using OpenSSH to generate a key pair

(<https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-81152>)

Hello Janne!

Using PuTTYTray to generate a key pair

Thank you for the good post! I have a question actually, I want to format my Laptop, and I don't want to lose my ssh keys

Turn off password authentication

because I used them to authenticate me on the server! can I copy the whole .ssh folder on USB driver and paste it in

c/Users again after format laptop?? or there is another way to do that?

Conclusions

thanks for your answer!!

[Reply](#)



Janne Ruostemaa says:

2020-06-17 at 11:55

(<https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-81211>)

Hi there, thanks for the question. You can backup your private SSH keys any way you want. Simply copying them onto a USB drive will work just fine.

Alternatively, if you use any cloud storage services such as Google Drive or Dropbox, you could also save your SSH keys there granted you take care of your account security.

[Reply](#)

(<https://upcloud.com>)



Dangelo says:

2020-07-15 at 07:30

(<https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-87793>)

Very nice guide Janne, thank you so much!!!

Set up your first SSH keys

I think its works great...

Preparing your server

but, I do not have access to the root user right now lol. I can only get access with the newer user I created with sudo privileges. Is it ok?

Reply

Using OpenSSH to generate a key pair



Janne Ruostemaa says:

Using PuTTYTray to generate a key pair

2020-07-15 at 12:08

Turn off password authentication

(<https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-87851>)

Conclusions

Hi Dangelo, thanks for the question. Now that you have sudo privileges, you can always switch to the root user for example with `sudo -i` command. Afterwards, return to your own user account simply with `exit`

Reply



Hans Zimmer says:

2020-09-04 at 15:54

(<https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-100687>)

Please make sure, that the public key you copied over to `authorized_keys` has to start with `ssh-rsa`.

I ran into problems because I saved the public key into a file and not directly to clipboard.

Maybe you can add this advice to your otherwise flawless tutorial.

Reply

(<https://upcloud.com>)



Janne Ruostemaa says:

2020-09-07 at 13:18

(<https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-100984>)

Hi Hans, thanks for the suggestion. Indeed the key type is important to include in the authorized_keys file for SSH to know how to read it. We've added a note of this in the tutorial.

Set up your first SSH keys

Preparing your server

Reply

Using OpenSSH to generate a key pair



Patrick says:

Using PuTTYTray to generate a key pair

2020-09-23 at 01:41

(<https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-104238>)

Turn off password authentication

Permission denied (publickey). Any help on this is greatly appreciated

Conclusions

Reply



Janne Ruostemaa says:

2020-09-25 at 12:25

(<https://upcloud.com/community/tutorials/use-ssh-keys-authentication/#comment-104783>)

Hi Patrick, thanks for the comment. If you've placed your public SSH key in the auhtorized_keys file but are still unable to log in without a password, it's possible SSH doesn't have access to the key or the permissions are too open. You should check that only your user account has access to the ~/.ssh/authorized_keys directory and file.

```
chmod 700 ~/.ssh
chmod 600 ~/.ssh/authorized_keys
```

Also check that public SSH key authentication is enabled in your /etc/ssh/sshd_config file by setting PubkeyAuthentication yes

(<https://upcloud.com>)

Reply

Leave a Reply

Set up your first SSH keys

Preparing your server

Using OpenSSH to generate a key pair

Using PuTTYTray to generate a key pair

Turn off password authentication

Conclusions

Your email address will not be published. Required fields are marked *

Comment

[Click here to leave a comment](#)

Name*

Email*

Website

Post Comment

Helsinki (HQ)

London

Singapore

Seattle

Helsinki (HQ)

Email

In the capital city of
(<https://upcloud.com>).
Finland, you will find

General
hello@upcloud.com

our headquarters, and [**\(mailto:hello@upcloud.com\)**](mailto:hello@upcloud.com).

our first data centre.

Sales

This is where we handle

[**sales@upcloud.com**](mailto:sales@upcloud.com)

most of our

[**\(mailto:sales@upcloud.com\)**](mailto:sales@upcloud.com).

development and

Support

innovation.

[**support@upcloud.com**](mailto:support@upcloud.com)

[**\(mailto:support@upcloud.com\)**](mailto:support@upcloud.com).

Preparing your server

Using OpenSSH to generate a key pair

Products

[**Using PuTTYTray to generate a key pair**](https://upcloud.com/products/)

[Cloud Servers](https://upcloud.com/products/cloud-servers/)

[\(https://upcloud.com/products/cloud-servers/\)](https://upcloud.com/products/cloud-servers/)

[MaxIOPS storage](https://upcloud.com/products/maxiops-storage/)

[\(https://upcloud.com/products/maxiops-storage/\)](https://upcloud.com/products/maxiops-storage/)

[Object Storage](https://upcloud.com/products/object-storage/)

[\(https://upcloud.com/products/object-storage/\)](https://upcloud.com/products/object-storage/)

[Simple Backup](https://upcloud.com/products/backup/)

[\(https://upcloud.com/products/backup/\)](https://upcloud.com/products/backup/)

[SDN Private Networks](https://upcloud.com/products/software-defined-networking/)

[\(https://upcloud.com/products/software-defined-networking/\)](https://upcloud.com/products/software-defined-networking/)

[Network Transfer Pool](https://upcloud.com/products/network-transfer-pool/)

[\(https://upcloud.com/products/network-transfer-pool/\)](https://upcloud.com/products/network-transfer-pool/)

[Private Cloud](https://upcloud.com/products/private-cloud/)

[\(https://upcloud.com/products/private-cloud/\)](https://upcloud.com/products/private-cloud/)

Community

[**\(https://upcloud.com/community/\)**](https://upcloud.com/community/)

[Overview](https://upcloud.com/community/) [\(https://upcloud.com/community/\)](https://upcloud.com/community/)

[Use cases](https://upcloud.com/community/stories/)

[\(https://upcloud.com/community/stories/\)](https://upcloud.com/community/stories/)

[Events](https://upcloud.com/community/events/)

[\(https://upcloud.com/community/events/\)](https://upcloud.com/community/events/)

[Newsletter](https://upcloud.com/sign-up-newsletter/) [\(https://upcloud.com/sign-up-newsletter/\)](https://upcloud.com/sign-up-newsletter/)

[**\(https://upcloud.com\)**](https://upcloud.com/)

[**Compare**](https://upcloud.com/compare/) [**\(https://upcloud.com/compare/\)**](https://upcloud.com/compare/)

[AWS EC2](https://upcloud.com/compare/aws-ec2/) [\(https://upcloud.com/compare/aws-ec2/\)](https://upcloud.com/compare/aws-ec2/)

[Azure](https://upcloud.com/compare/azure/) [\(https://upcloud.com/compare/azure/\)](https://upcloud.com/compare/azure/)

[DigitalOcean](https://upcloud.com/compare/digitalocean/)

[\(https://upcloud.com/compare/digitalocean/\)](https://upcloud.com/compare/digitalocean/)

[Linode](https://upcloud.com/compare/linode/) [\(https://upcloud.com/compare/linode/\)](https://upcloud.com/compare/linode/)

[Vultr](https://upcloud.com/compare/vultr/) [\(https://upcloud.com/compare/vultr/\)](https://upcloud.com/compare/vultr/)

Resources

[Resources](https://upcloud.com/community/resources/)

[\(https://upcloud.com/community/resources/\)](https://upcloud.com/community/resources/)

[Tutorials](https://upcloud.com/community/tutorials/)

[\(https://upcloud.com/community/tutorials/\)](https://upcloud.com/community/tutorials/)

[Documentation](https://upcloud.com/docs/upcloud-services/) [\(https://upcloud.com/docs/upcloud-services/\)](https://upcloud.com/docs/upcloud-services/)

[API](https://developers.upcloud.com/1.3/) [\(https://developers.upcloud.com/1.3/\)](https://developers.upcloud.com/1.3/)

[Status page](https://status.upcloud.com/) [\(https://status.upcloud.com/\)](https://status.upcloud.com/)

[FAQ](https://upcloud.com/faq/) [\(https://upcloud.com/faq/\)](https://upcloud.com/faq/)

Company

About UpCloud (<https://upcloud.com/about/>)

Blog & News (<https://upcloud.com/blog/>)

Partners (<https://upcloud.com/partners/>)

Careers (<https://upcloud.com/careers/>)

Brand Assets (<https://upcloud.com/brand-assets/>)

Contact us (<https://upcloud.com/contact/>)

Using OpenSSH to generate a key pair

Using PuTTYTray to generate a key pair

<https://upcloud.com>)

Turn off password authentication

UpCloud Ltd © 2020. All rights reserved.

[Terms of service \(/terms-of-service/\)](/terms-of-service/) [Privacy policy \(/privacy-policy/\)](/privacy-policy/)

Conclusions

[_ \(https://www.facebook.com/UpCloudLtd\)](https://www.facebook.com/UpCloudLtd) [_ \(https://twitter.com/upcloud\)](https://twitter.com/upcloud)

[_ \(https://github.com/UpCloudLtd\)](https://github.com/UpCloudLtd) [_ \(https://www.linkedin.com/company/upcloud/\)](https://www.linkedin.com/company/upcloud/)

[_ \(https://www.instagram.com/upcloud/\)](https://www.instagram.com/upcloud/)

[_ \(https://www.youtube.com/channel/UCkIkxF5pBTBLYgYHXDIUUuw\)](https://www.youtube.com/channel/UCkIkxF5pBTBLYgYHXDIUUuw)