Portal > Knowledgebase > Technical > Infrastructure > SSH Access

SSH Access

Jem Camba - 2019-03-06 - in Infrastructure

> *Use SSH to securely access your Packet servers.*

SSH keys are one of the most secure ways to access a web server, since it requires authentication beyond a simple password. While each new Packet server has a root password assigned, it is removed from the customer portal after 24 hours - after which point you’ll need to leverage SSH or need to have added a new root password to the machine.

Generating SSH Keys

The Mac/Linux Way

This is pretty simple. The first step is to create a key pair on your local machine or your work station. Open a Command line and type:

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

Once you have entered the ssh-keygen command, you will go through with these questions.

```
Enter file in which to save the key (/home/name/.ssh/id_rsa):
```

You can use the default name and destination if this is your first ssh key.

```
Enter passphrase (empty for no passphrase):
```

Usually, System Administrators/DevOps do not use passphrase on their keys -- well admit it, one reason we use ssh key is to gain a secure, passwordless login to the server, right?

But if you feel the need of extra layer security, you may go ahead and key in your passphrase (make sure you safe keep your passphrase!)

Once you are done, **id_rsa.pub** is the key that you need to upload to Packet Portal. It should go without saying, but we'll say it anyway, do not share your private key *(located here /home/yourname/.ssh/id_rsa)* with anyone!

Your public SSH key is commonly located here */home/yourname/.ssh/id_rsa.pub* and you can display your public SSH key with the following command:

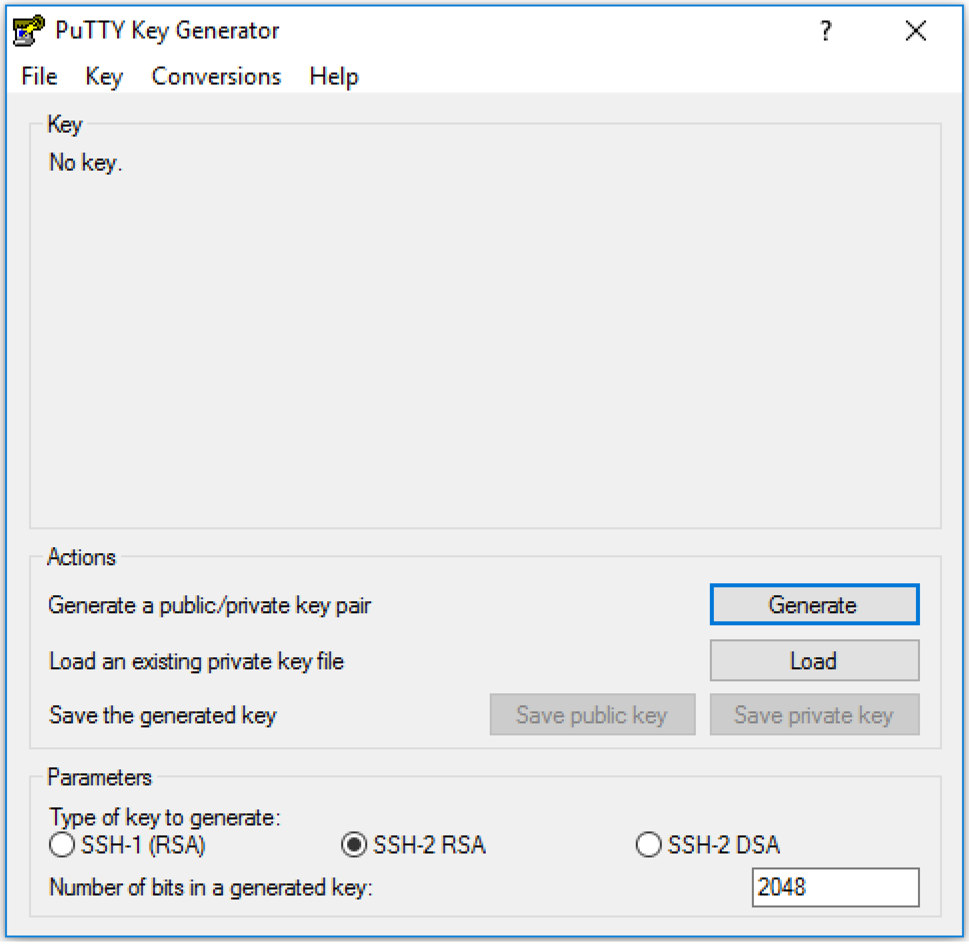
```
cat ~/.ssh/id_rsa.pub
```

The PuTTY Way (Windows)

First, Download PuTTY. The two binaries you will need are:

- PuTTY (the SSH and Telnet client itself)
- PuTTYgen (an RSA and DSA key generation utility)

Next, open PuTTYgen.exe which will look like this:



No key.

Generate a public/private key pair

Load an existing private key file

Save the generated key

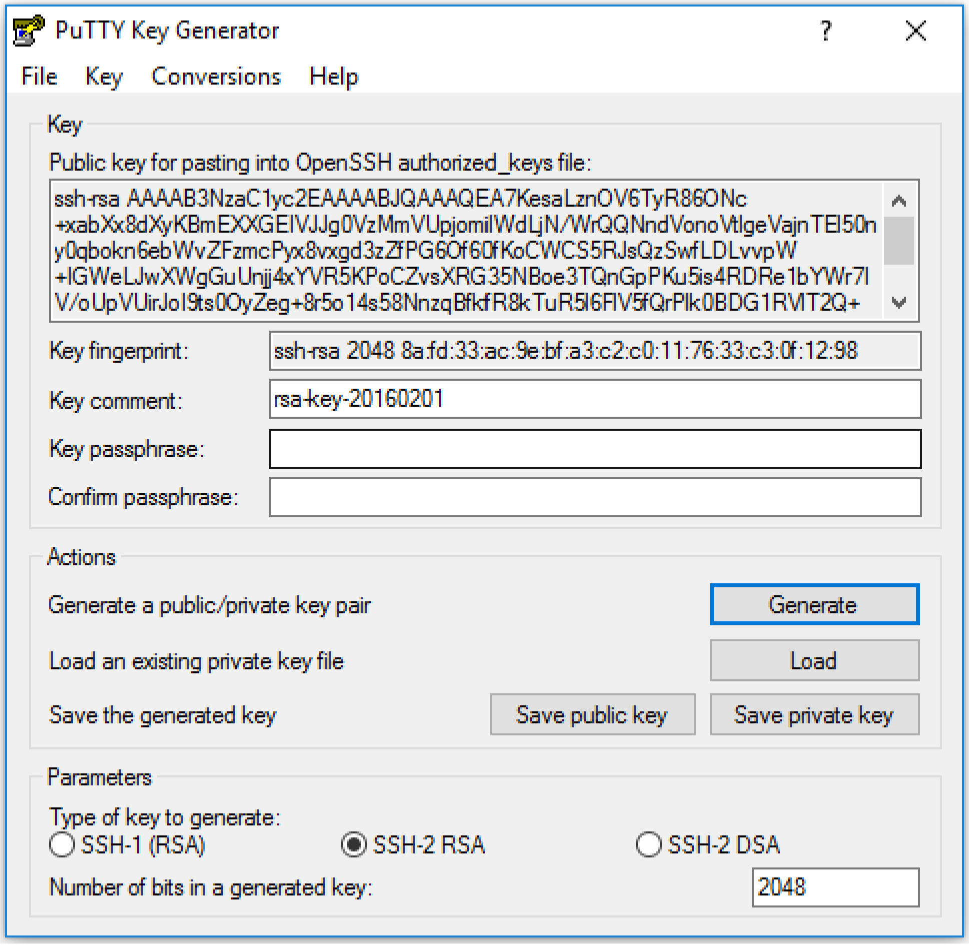
Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 2048

You can change the parameters for your key, even though the default ones are just fine. When you’re ready, click **Generate**.

In order to create a random key, you will be asked to move the cursor around a small empty area on the window. This randomness is called **entropy** and is used to create keys in a secure way that cannot be reproduced by others.

After a few seconds, once the keys are ready, you will be presented with this view:



Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa AAAAB3NzaC1yc2EAAAABJQAAAQEA7KesaLznOV6TyR86ONc
+xabXx8dXyKBmEXXGEIVJJg0VzMmVUpjomilWdLjN/WrQQNndVonoVtlgeVajnTEI50n
y0qbokn6ebWvZFzmcPyx8vxgd3zZfPG6Of60fKoCWCS5RJsQzSwfLDLvvpW
+IGWeLJwXWgGuUnjj4xYVR5KPoCZvsXRG35NBoe3TQnGpPKu5is4RDRe1bYWr7l
V/oUpVUirJol9ts0OyZeg+8r5o14s58NnzqBfkfR8kTuR5l6FlV5fQrPlk0BDG1RVlT2Q+
```

Key fingerprint: ssh-rsa 2048 8a:fd:33:ac:9e:bf:a3:c2:c0:11:76:33:c3:0f:12:98

Key comment: rsa-key-20160201

Key passphrase:

Confirm passphrase:

Generate a public/private key pair

Load an existing private key file

Save the generated key

Type of key to generate:
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 2048

Click the **Save private key** button, name it whatever you like and choose a secure location to save the key with the extension ".ppk".

Repeat the same thing after clicking on **Save public key**. This time, make sure to give it an extension like ".txt", so you can open it later in a regular text editor.

Note! *If you open the public key text file you just saved, you will probably see that it contains something that looks like the following:*

> *---- BEGIN SSH2 PUBLIC KEY ----*
>
> *Comment: "rsa-key-xxxxxx"*
>
> *....*
>
> *---- END SSH2 PUBLIC KEY ----*

Why Putty saves it in this format is unclear, but it is not an accepted form of adding the public key.

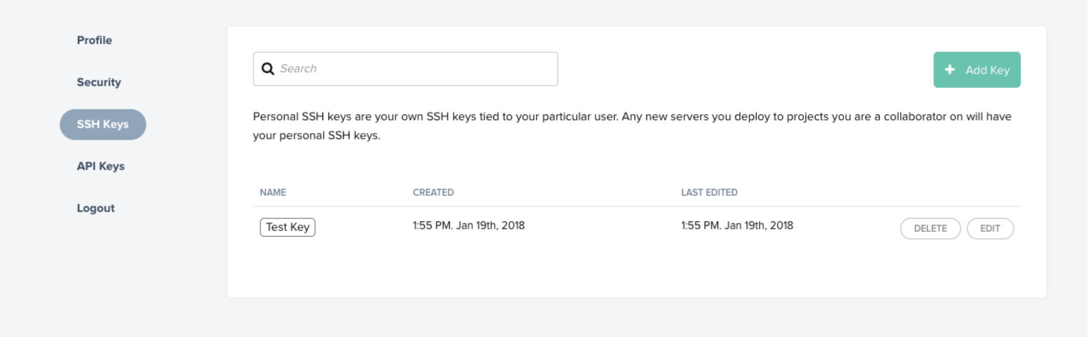
So, for that reason, you might want to copy whatever the Putty Generator shows on the

Public key window and paste it on the document, after deleting everything that was there before.

It should look like: ssh-rsa AAAA...........== rsa-key-xxxxxxx

Adding Your Key to the Packet Portal

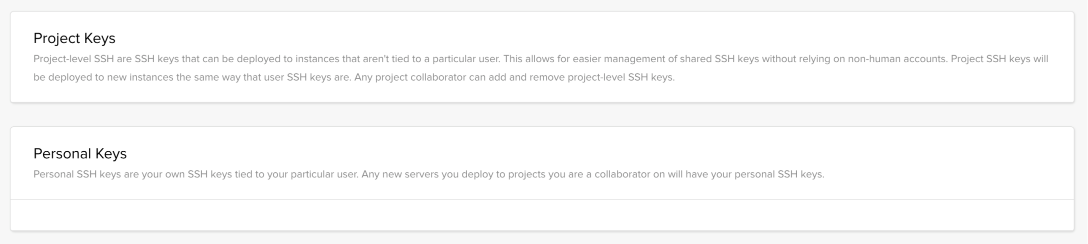
Once you have generated an SSH key pair you can upload the public key to your account. Via the packet portal, go to "SSH Keys" on the left-hand side and click "Add SSH Key" In the lower right-hand corner.



Personal SSH keys are your own SSH keys tied to your particular user. Any new servers you deploy to projects you are a collaborator on will have your personal SSH keys.

NAME	CREATED	LAST EDITED
Test Key	1:55 PM. Jan 19th, 2018	1:55 PM. Jan 19th, 2018

Understanding SSH at Packet -- Personal Keys vs Project Keys
When adding a key in the Packet Portal, you can choose to add either Project Key or a Personal Key.



Project Keys
Project-level SSH are SSH keys that can be deployed to instances that aren't tied to a particular user. This allows for easier management of shared SSH keys without relying on non-human accounts. Project SSH keys will be deployed to new instances the same way that user SSH keys are. Any project collaborator can add and remove project-level SSH keys.

Personal Keys
Personal SSH keys are your own SSH keys tied to your particular user. Any new servers you deploy to projects you are a collaborator on will have your personal SSH keys.

As you can see, a Personal Key will be included on all new machines in the projects that you own, or of which you are a collaborator.

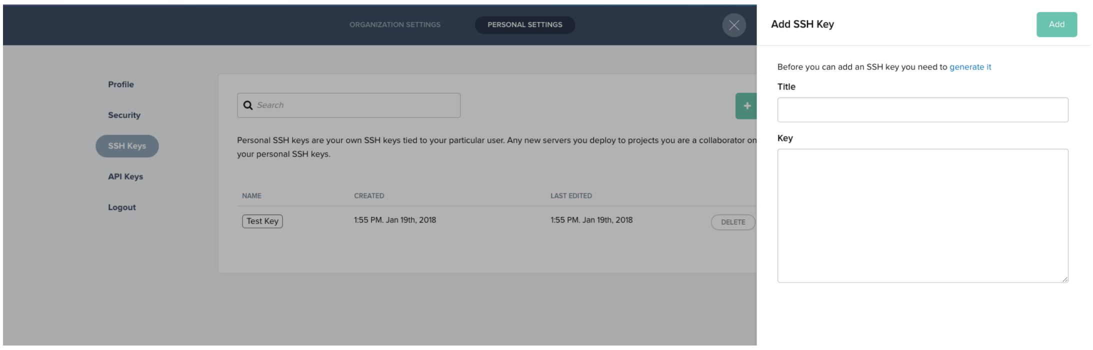
You can also choose to create and manage a key that is specific to a single project (which will be included by default on servers deployed into a particular project). This 2nd option is useful if you don’t want to use a personal key that you leverage in lots of places on a shared box.

Getting Your Key(s) on Your Server(s)

We use our cloud-init service to add all the selected keys (Personal + Project specific + Collaborator) onto each machine at provision time. So as soon as your box is deployed, you can access it via SSH. Nice!

This also means that any keys you (or your collaborators) add via the Packet portal after a server is provisioned won’t be available on the machine automatically. You’ll have to add new keys. Here are a couple of different situations:

Adding New SSH Keys to An Existing Server



Personal SSH keys are your own SSH keys tied to your particular user. Any new servers you deploy to projects you are a collaborator on your personal SSH keys.

NAME	CREATED	LAST EDITED
Test Key	1:55 PM. Jan 19th, 2018	1:55 PM. Jan 19th, 2018

Before you can add an SSH key you need to generate it

Title

Key

Add Your New SSH Key to the Portal:

1. Navigate to the SSH Keys section of the Packet portal.
2. Add your public SSH key. Note that below the key value area, you will see an option to associate this new key with a specific server. You may also select “all of them” if you have many existing servers. Be sure to select the servers that need this new SSH key!

Now that you that the key is added in portal, you need to force add it to your server(s).

Use our SOS service to login with (root + pw) and manually add the new key on the authorized_keys file.

Logging In Via SSH

Mac/Linux

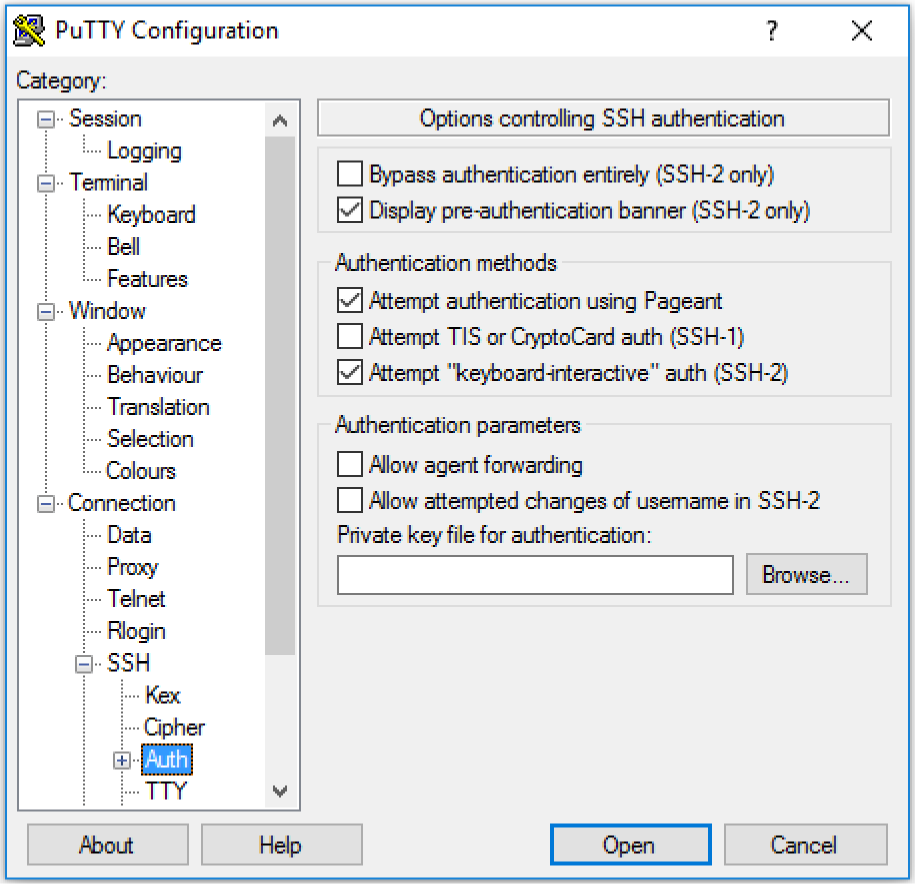
SSH access on Mac and Linux is straightforward. Simply run the command:

```
ssh root@<your_Public IPv4>
```

Windows

Run the PuTTY.exe binary downloaded earlier go to "Data" under "Connection**"**, and add **root** in the field of the username.

Go to Authentication, under SSH, and click the Browse button, to add the private SSH key created earlier.



☐ Bypass authentication entirely (SSH-2 only)

☑ Display pre-authentication banner (SSH-2 only)

Authentication methods

☑ Attempt authentication using Pageant

☐ Attempt TIS or CryptoCard auth (SSH-1)

☑ Attempt "keyboard-interactive" auth (SSH-2)

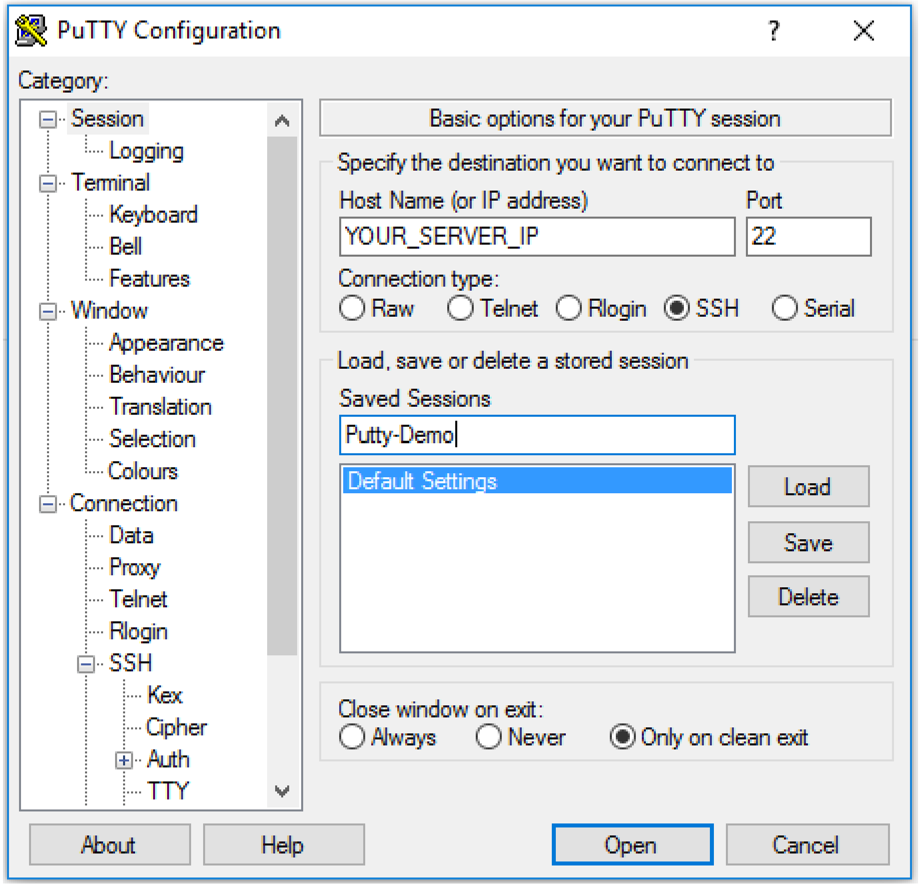
Authentication parameters

☐ Allow agent forwarding

☐ Allow attempted changes of username in SSH-2

Private key file for authentication:

Now go to **Session**, enter the public IP address of your server, give a name to the session, and click **Open**.



Specify the destination you want to connect to

Host Name (or IP address): YOUR_SERVER_IP

Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

Load, save or delete a stored session

Saved Sessions: Putty-Demo

Default Settings

Close window on exit: ○ Always ○ Never ● Only on clean exit

Et voila, you now have SSH access to your server and can continue on with your day.

Tags

ssh keys