SSH Academy

Using PuTTYgen on Windows to generate SSH key pairs

This page is about PuTTYgen on Windows. For the Linux version, see here.

PuTTYgen is an key generator tool for creating SSH keys for PuTTY. It is analogous to the ssh-keygen tool used in some other SSH implementations.

The basic function is to create public and private key pairs. PuTTY stores keys in its own format in `.ppk` files. However, the tool can also convert keys to and from other formats.

`PuTTYgen.exe` on Windows is a graphical tool. A command-line version is available for Linux.

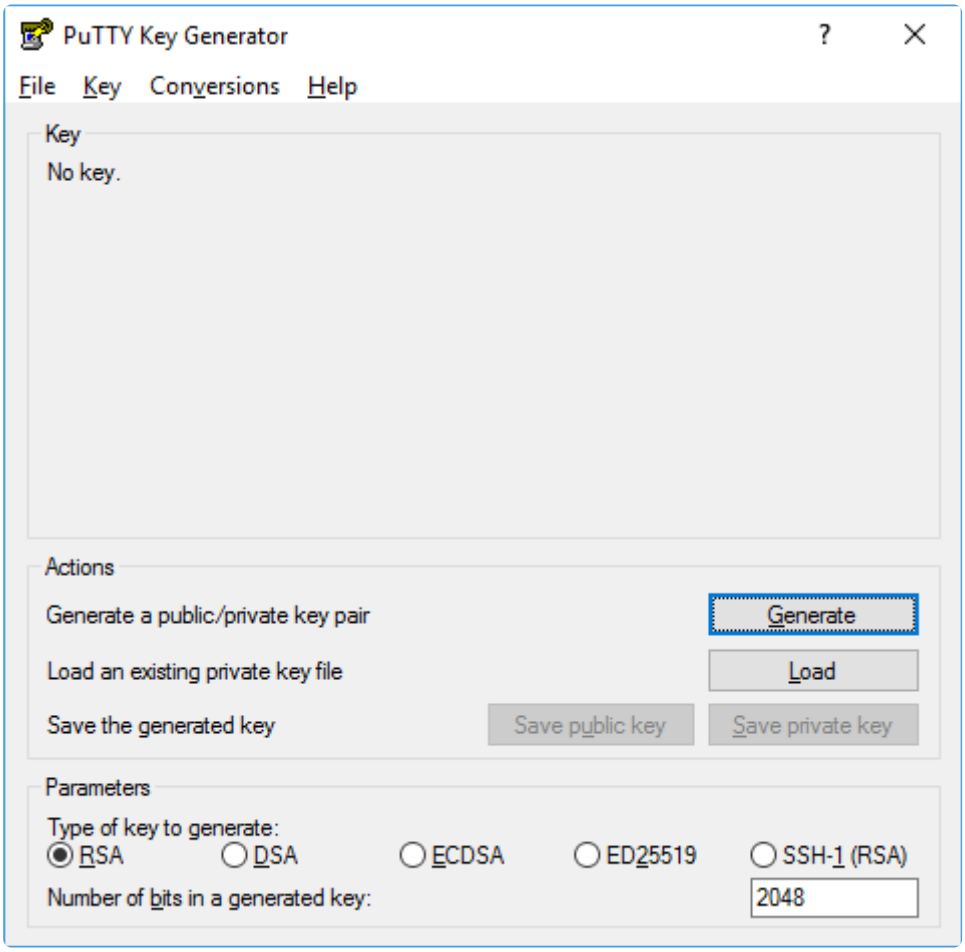
Contents

PuTTYgen download and install

PuTTYgen is normally installed as part of the normal PuTTY `.msi` package installation. There is no need for a separate PuTTYgen download. Download the PuTTY installation package. For detailed installation instructions, see PuTTY installation instructions.

Running PuTTYgen

Go to Windows **Start menu** → **All Programs** → **PuTTY** → **PuTTYgen**.



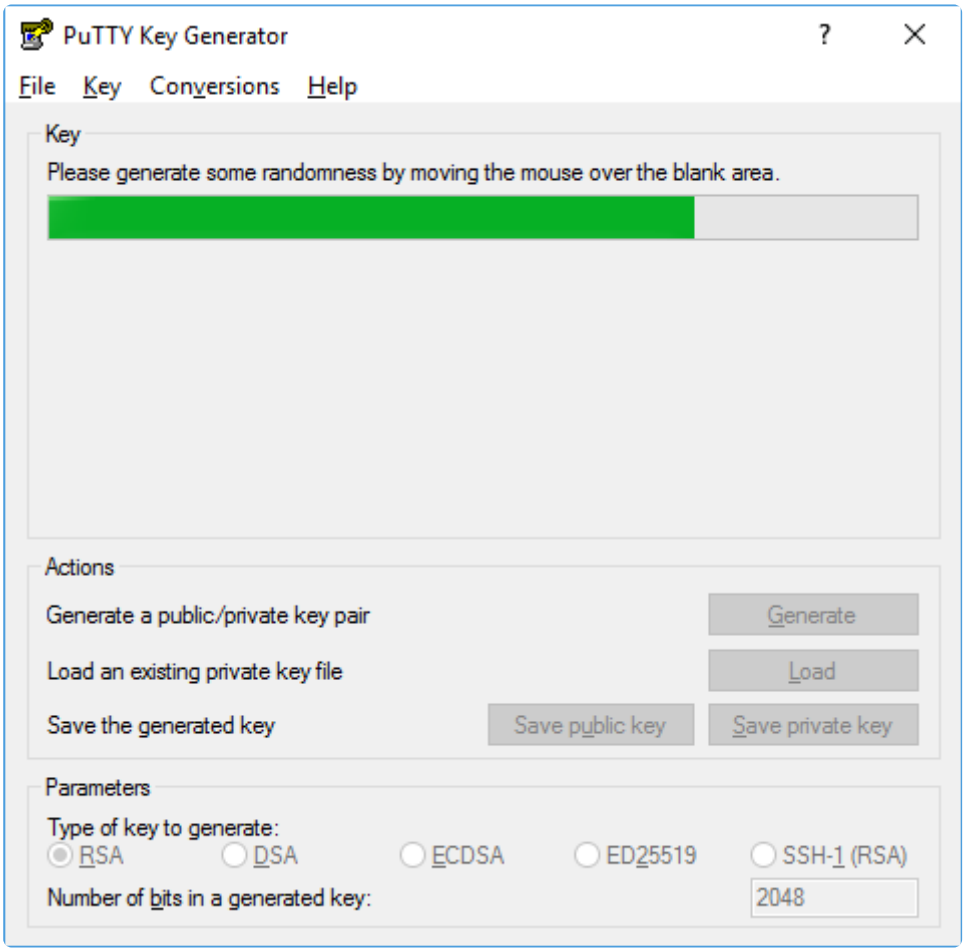
Creating a new key pair for authentication

To create a new key pair, select the type of key to generate from the bottom of the screen (using SSH-2 RSA with 2048 bit key size is good for most people; another good well-known alternative is ECDSA).

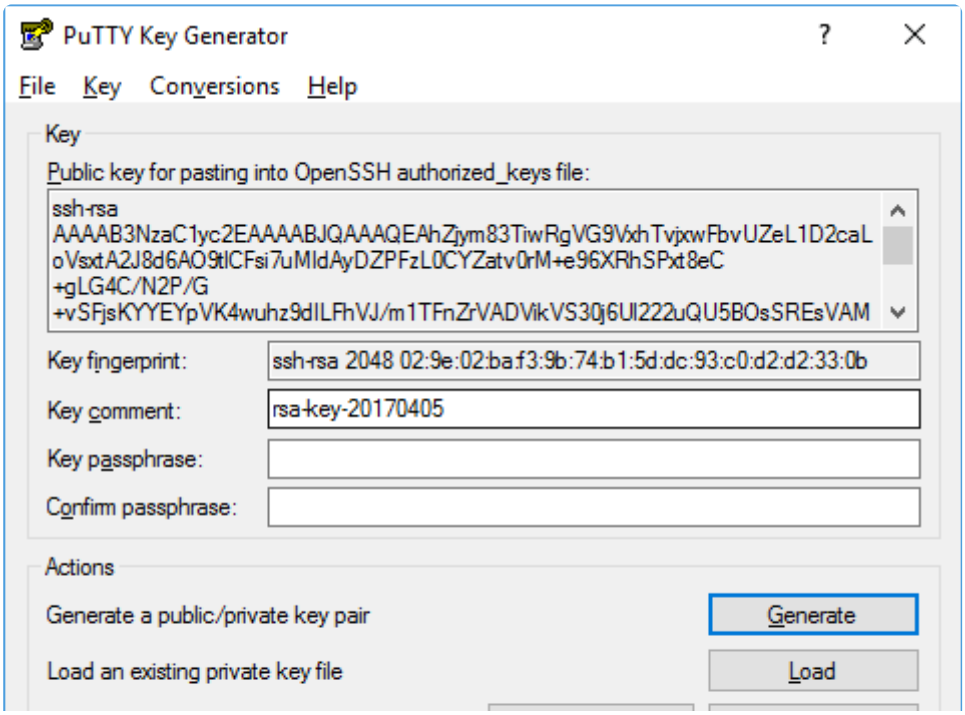
Then click **Generate**, and start moving the mouse within the Window. Putty uses mouse movements to collect randomness. The exact way you are going to move your mouse cannot be predicted by an external attacker. You may need to move the mouse for some time, depending on the size of your key. As you move it, the green progress bar should advance.

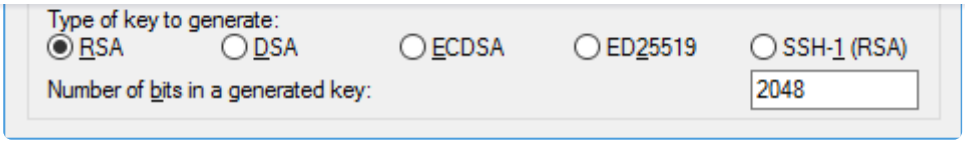
Once the progress bar becomes full, the actual key generation computation takes place. This may take from several seconds to several minutes. When complete, the public key should appear in the Window. You can now specify a passphrase for the key.

You should save at least the private key by clicking **Save private key**. It may be advisable to also save the public key, though it can be later regenerated by loading the private key (by clicking **Load**).



We strongly recommended using a passphrase be for private key files intended for interactive use. If keys are needed for automation (e.g., with **WinSCP**, then they may be left without a passphrase.





Installing the public key as an authorized key on a server

With both Tectia SSH and OpenSSH servers, access to an account is granted by adding the public key to a ~/.ssh/authorized_keys file on the server.

To install the public key, Log into the server, edit the `authorized_keys` file with your favorite editor, and cut-and-paste the public key output by the above command to the `authorized_keys` file. Save the file. Configure PuTTY to use your private key file (here `keyfile.ppk`). Then test if login works. See configuring public key authentication for PuTTY.

Managing SSH keys

In larger organizations, the number of SSH keys on servers and clients can easily grow to tens of thousands, in some cases to millions of keys. In large quantities, SSH keys can become a massive security risk and they can violate compliance requirements.

Universal SSH Key Manager can manage PuTTY keys in addition to OpenSSH and Tectia keys. It works with legacy keys on traditional servers as well as dynamic and keyless elastic environments in the cloud. Any larger organization should ensure they have proper provisioning and termination processes for SSH keys as part of their Identify and Access Management (IAM) practice.

Changing the passphase of a key

It is recommended that all SSH keys be regenerated and changed periodically. The Universal SSH Key Manager can automate this. Just changing the passphrase is no substitute, but it is better than nothing. These instructions can also be used to add a passphrase to a key that was created without one.

To change the passphrase, click on **Load** to load an existing key, then enter a new passphrase, and click **Save private key** to save the private key with the new passphrase. Be sure to properly destroy and wipe the old key file. Creating a new file with a new passphrase will not help if the old file remains available.

Videos illustrating use of PuTTYgen

Using PuTTYgen to generate an SSH key

Using PuTTYgen to generate an SSH key

How to set up PuTTY SSH keys for passwordless logins

Together with our customers, our mission is to secure their digital business on on-premises, cloud, and hybrid ecosystems cost-efficiently, at scale, and without disruptions to their operations or business continuity.

Solutions

Digital transformation
Secure file transfer
Pass IT audits
OT and M2M connections
Credential risk mitigation

Products

PrivX™
UKM™
NQX™
Tectia™
Tectia™ z/OS

Services

SSH Risk assessment™
Professional Services
Support
Contact

Resources

References
Downloads
Manuals
Events & Webinars
Blog

Company

About us
Investors
Partners
Analysts
Press

Stay on top of the latest in cyber security

Be the first to know about SSH.COM's new solutions and features