Windows How-to: Use PuTTY Agent SSH Keys

PuTTY is pretty much the standard SSH client for Windows. However, using SSH keys for automatic authentication isn’t the most obvious.

## Create Your SSH Key

While it is possible to import and (re)use OpenSSH keys with PuTTY, we will assume you are starting from scratch.

1. Open the PuTTY key generator program, which is usually installed in C:\Program Files(x86)\PuTTY\puttygen.exe.
2. Select Generate a public/private key pair. The default is a 2048-bit SSH2-RSA key, which is acceptable for most applications.
3. Move the mouse around in the window to generate randomness.
4. Change the Key comment to make it obvious what the key is for.
5. Create a key passphrase, and enter it twice. Don’t be tempted to leave it blank!
6. Save private key to a folder, such as your Documents directory. You should probably save the public key as well, just for completeness.
7. Type <ALT> + <P> to select the OpenSSH-style public key block, which should be saved to another file. This public key will either be uploaded to the CNS VM hosting site, or manually appended to your $HOME/.ssh/authorized\_keys file, depending on your needs.



## Add the Key to PuTTY Agent on Sign-On

You can set the agent to start up when you sign on your Windows computer, and have it automatically load the key.

1. Open File Explorer (explorer.exe).
2. Enter shell:startup as the folder location.
3. Right-click in the window and select New > Shortcut.
4. Browse to the PuTTY agent executable (C:\Program Files (x86)\PuTTY\pageant.exe).
5. Select Next, and Finish.
6. Right-click on the new shortcut and select Properties.
7. Change the Start in folder to point to where you saved the private key.
8. Append the key name to the Target field. If you have multiple private keys, append each one to the list.
9. Select OK to save your changes.

The PuTTY agent will now start up when you sign on, request your passphrase(s), then manage the keys on behalf of PuTTY, PSFTP, and any other SSH client compatible with PuTTY agent.

