

# SSH on Windows

[SSH at Rockefeller University](#)

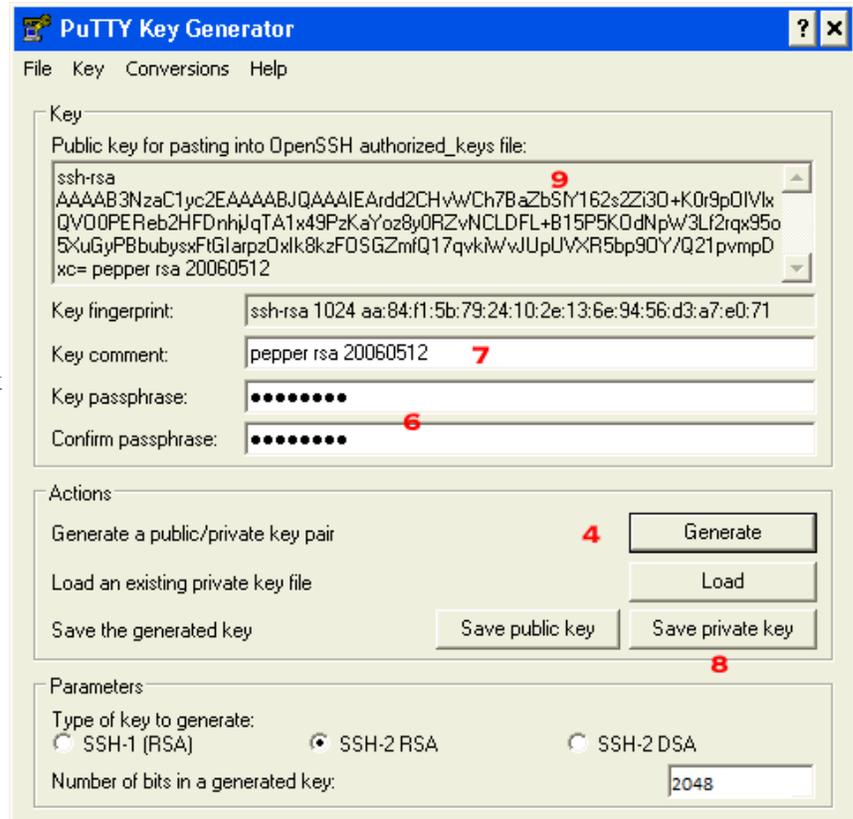
[SSH on Windows](#)

[OpenSSH \(UNIX & Mac OS X\)  
makekeys.sh UNIX script](#)

[SSH Details & Tips](#)

## Part I: Create a Private/Public Key Pair with PuTTYgen

1. Create a folder on your PC for SSH keys.
2. Download the latest Installer from [the PuTTY Download Page](http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html) <<http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>>; (you may need to scroll down for the "Windows installer for everything except PuTTYtel" download file). Run the installer and accept the "Unknown Publisher" warning. If you wish, create a QuickLaunch icon (in the Start bar).
3. Run PuTTYgen (**Start > All Programs > PuTTY > PuTTYgen**).
4. At the bottom of the window, click **Generate**.
5. *Wave the mouse around inside the **PuTTYgen** window* until the bar reaches the end of the window. It uses mouse motion as a source of randomness.
6. In the "Key passphrase" field, type a passphrase to encrypt this key with. It must be a [good password](#) (at least 8 characters, not all letters or numbers, etc.); type it again in the "Confirm passphrase" field.
7. Set a "Key comment" -- we suggest adding your login name to the default.
8. Click the "Save private key" button to save an encrypted file containing your private and public key in PuTTY format. Make sure the filename includes your RU login



name, the date, and the .ppk suffix,

*e.g.*,

`id_rsa.pepper.20061108.ppk.`

Save the file to the folder you created in step 1. ***This file must be protected as if it was your password. It should not be made available to others, and should NOT be sent via email.***

9. Save/Export your Public Key - Select the whole "Public key for pasting into OpenSSH authorized\_keys file:" from the box at the top of PuTTYgen's window and **Copy** it (using `ctrl-C` or the right mouse button). Open Notepad, **Paste** the key in, and **Save** the file to the directory you created in step 1. Make sure the filename includes your RU login name, the date, and the .pub suffix, *e.g.*,

`id_rsa.pepper.20061108.pub.`

10. If you need Rockefeller University IT to install your key on a University-maintained unix machine, email the Public Key file created in the previous step to [wizards@rockefeller.edu](mailto:wizards@rockefeller.edu). Indicate your user name and the machine you need to connect to in your request. Do NOT email the private (ppk) file.

*Note that the private key file is effectively your password, so be careful with it!*

Most commercial SSH software uses different key formats than OpenSSH. If you need assistance with a server which doesn't use `authorized_keys`, please open a UNIX Software ticket with the Help Desk ([helpdesk@rockefeller.edu](mailto:helpdesk@rockefeller.edu), x8940).

## Part II: Configure pageant

If desired, pageant may be used to cache your passphrase. Pageant is not required, but may make the use of PuTTY more convenient.

**Note:** pageant is an [SSH agent/keychain](#) which adds an icon  to the Windows taskbar. It offers two functions. First, pageant can cache keys (like `ssh-agent/keychain`). Second, right-clicking on the

pageant icon brings up a menu to launch frequently-used PuTTY sessions. To avoid username prompts when using **Saved Sessions**, set the "Auto-login username" under **PuTTY Configuration > Connection**; you may also wish to "Enable X11 forwarding" under **PuTTY Configuration > Connection > SSH > Tunnels**.

1. Locate your private key (.ppk file), saved in Part I.
2. Right-click the key, and select **Copy**.
3. Right-click on **Start**, and select **Open**; this opens your "Start Menu" folder.
4. Open Programs\Startup (inside "Start Menu").
5. Right-click inside Startup, and select "Paste Shortcut".
6. Double-click the .ppk shortcut.
7. In the **Windows cannot open this file:** dialog, choose "Select the program from a list" and click **OK**.
8. In the **Open With** dialog, click **Browse** and select pageant.exe (normally C:\Program Files\PuTTY\pageant.exe).
9. Double-click the .ppk shortcut to confirm it opens in pageant, and that your password works to decrypt and cache the encrypted key contained in the file.
10. Right-click on pageant in the **Start** bar, select View Keys, and verify your private key is shown in the **Pageant Key List** window.

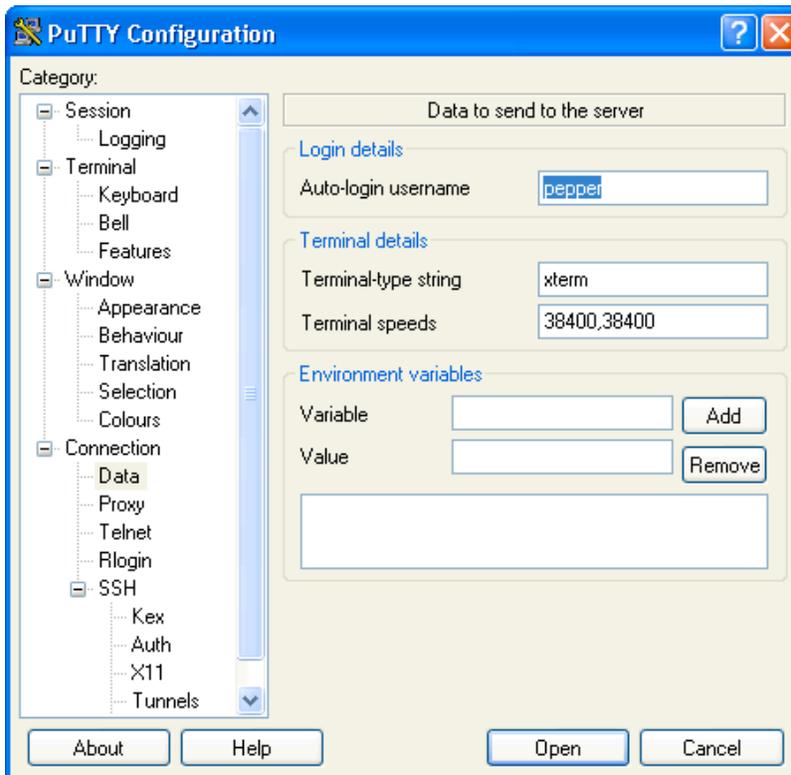
On login, pageant will prompt for a password to decrypt the private key(s) in your .ppk file(s) into memory. At logout, pageant will exit and forget the keys.

If you use pageant, it is *very important* to always lock your screen when away; Windows can do this automatically with the screen saver (**Start > Control Panel > Display > ScreenSaver**; in Windows XP, the option is "On resume, display Welcome screen").

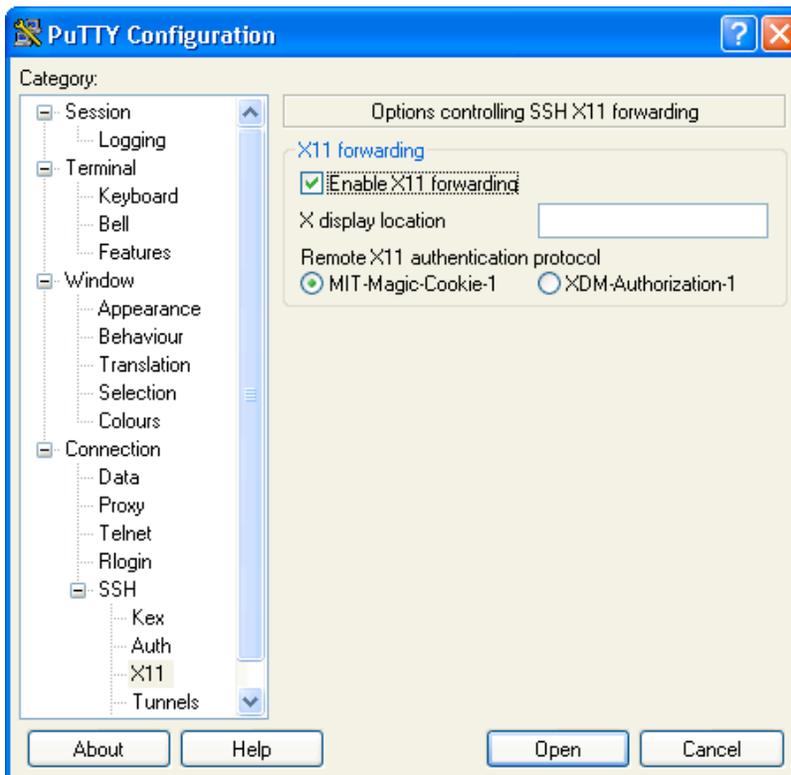
When using pageant, do not specify a key file in PuTTY or WinSCP -- both automatically try all keys from pageant. Additionally, any "Saved Sessions" from PuTTY are automatically available in pageant's menu.

## Part III: Configure PuTTY

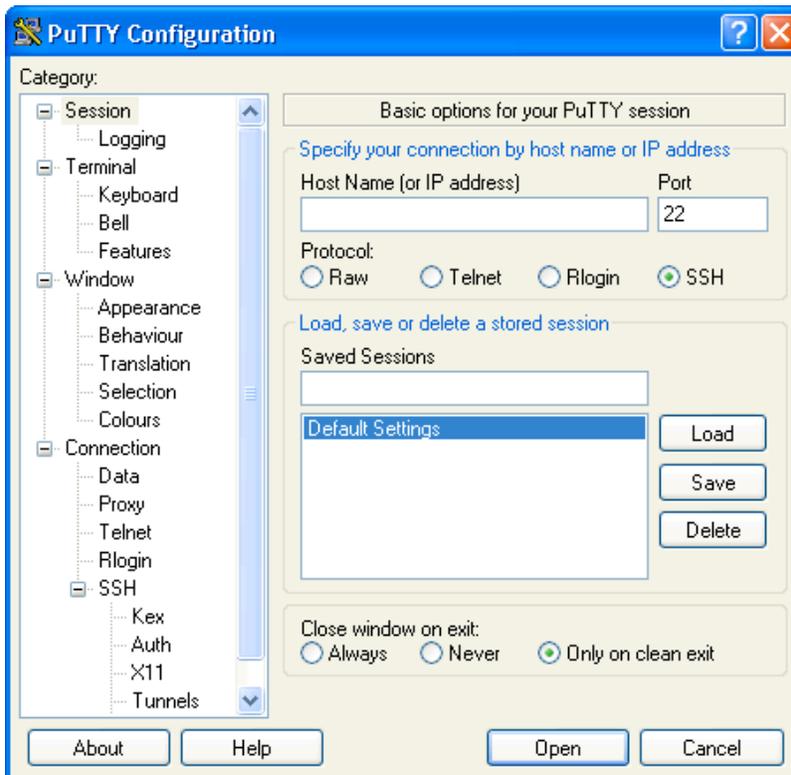
1. Start PuTTY (**Start > All Programs > PuTTY > PuTTY**).



2. On the left side, select **Connection > Data**, and on the right enter your account name under "Auto-Login username".

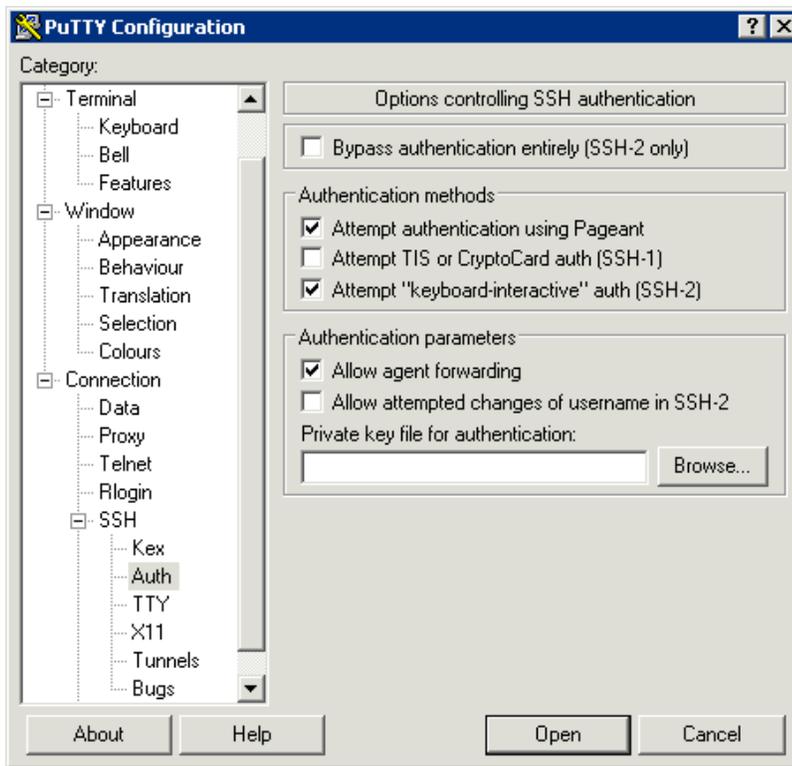


3. *If you will be using X11: (Hummingbird Exceed, WRQ Reflections, or X-Win 32),* on the left side select **Connection > SSH > X11**, and on the right check "Enable X11 forwarding".



4. On the left side, select **Session**; on the right click "Default Settings" (or provide an alternate name). Click the **Save** button.

At this point, PuTTY is ready to go. Now it's time to install the *public* key on SSH servers you use, and create "Saved Sessions" for convenient access.



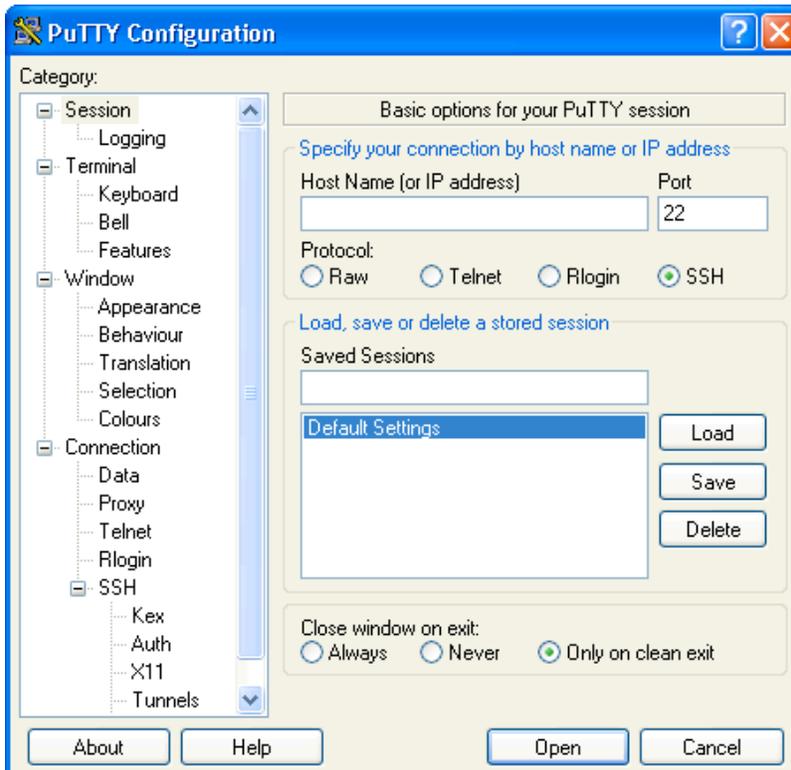
If you access any servers which are not directly accessible, such as cluster nodes, create a Saved Session for the accessible intermediate server (typically the head node), and in that session, check "Allow agent forwarding" under Connection:SSH:Auth. This will allow you to log into the inaccessible nodes using a public key with the head node as your intermediary.

## Part IV: Install Your Public Key

*Note: Information Technology Staff can install your key on University-maintained servers. To request such installation, email the contents of your Public Key file to [helpdesk@rockefeller.edu](mailto:helpdesk@rockefeller.edu) and [wizards@rockefeller.edu](mailto:wizards@rockefeller.edu). Indicate your user name and the machine you need to connect to in your request. Do NOT email the private (ppk) file.*

The following steps are provided for those who would like to install their public keys on self-maintained machines. Follow the steps below for each OpenSSH server you connect to via `ssh`, `sftp`, or `scp`. The OpenSSH page includes [a more complete explanation](#).

### 1. Start PuTTY.



2. Type the computer's DNS name under "Host Name (or IP address)".
3. Type the same name under the "Saved Sessions" box.
4. Click **Save** to create a saved session, like a bookmark, for this server. It will pick up the username and X11 settings you made to the default. Saved Sessions are also available directly from pageant (below).
5. Click the **Open** button to connect to the server shown.
6. PuTTY will prompt for your UNIX password, because the public key isn't installed yet. Enter it to login.
7. Type `mkdir -p .ssh` to be sure you have a `~/ .ssh` directory.
8. Type `echo "` (one double-quote; do not hit `Enter`)
9. Switch back to your public key (the `.pub` file) in notepad, select the whole thing (wrapped to several lines), and **Copy** it.
10. Return to your PuTTY session and **Paste** the public key.
11. Type `" >> .ssh/authorized_keys` (another double-quote) to finish the command line, and hit `Enter`. The command should look something like:
 

```
echo "ssh-rsa AAAA... pepper@rockefeller.edu 20061108" >> .ssh/authorized_keys
```
12. Right-click on the PuTTY title bar of the logged-in window, and select "Duplicate Session" from the pop-up menu.
13. If pageant is working and the key was installed successfully, you should get a new session window without any username or authentication prompting.

You can now right-click on pageant's icon in the **Start** bar, select "Saved Sessions", and pick a session from the list to

log in.

Repeat Part IV as needed to install your key onto other servers.

## Part V: Install & Configure WinSCP

1. Download and run the [WinSCP Installation Package](#). Ignore the advertisements and scroll down to find the Installation Package of the latest version. The filename should resemble winscp516setup.exe, from <http://download.winscp.net>. You can ignore the "Unknown Publisher" warning, and accept most of the installation defaults, but uncheck PuTTYgen & pageant -- they were already installed with PuTTY.
2. Launch WinSCP.
3. Optional: in the **WinSCP Login** window, click **Tools... > Import...** to load PuTTY's Saved Sessions into WinSCP.
4. Once the Saved Sessions are imported, you may want to set "Remember last used directory" in WinSCP's Directories configuration area.
5. Log in to confirm WinSCP is getting the keys from pageant successfully -- you should not see a password prompt.

If you are replacing an old key, after you have confirmed the new one works, remove the old public key from `~/.ssh/authorized_keys`.

## X11 Note

To enable X11 forwarding in PuTTY, activate **Connection > SSH > Tunnels > Enable X11 forwarding**. For `xauth` to work properly, your X11 application (Exceed, Reflections, or X-Win 32) must be running *before* establishing the `ssh` connection.

---

[Up](#)