SPEEDEserver™

Key File Generation

November 14, 2017

National Student Clearinghouse®

2300 Dulles Station Blvd., Suite 220, Herndon, VA 20171

SPEEDEserver™

Table of Contents

Introduction

You must generate public and private keys to use the SPEEDE Server. This guide provides step-by-step instructions on using PuTTY to generate your key file, including how to:

- install PuTTY,
- generate the keys, and
- configure PuTTY to work withSPEEDE.

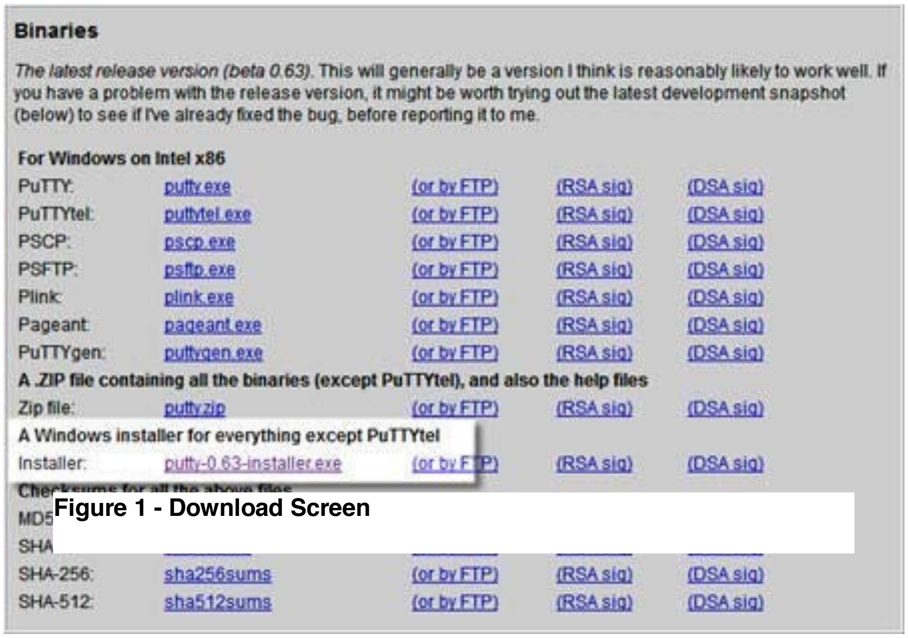
PuTTY Installation

Install the PuTTY package, which you can download from: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html.

Select the download listed under **A Windows installer for everything except PuTTYtel**.

The installer version may vary (currently 0.63). Always select the newest version.

In Windows Explorer, go to the **Downloads** folder and click **putty-x.xx-installer.exe** to begin the install process.



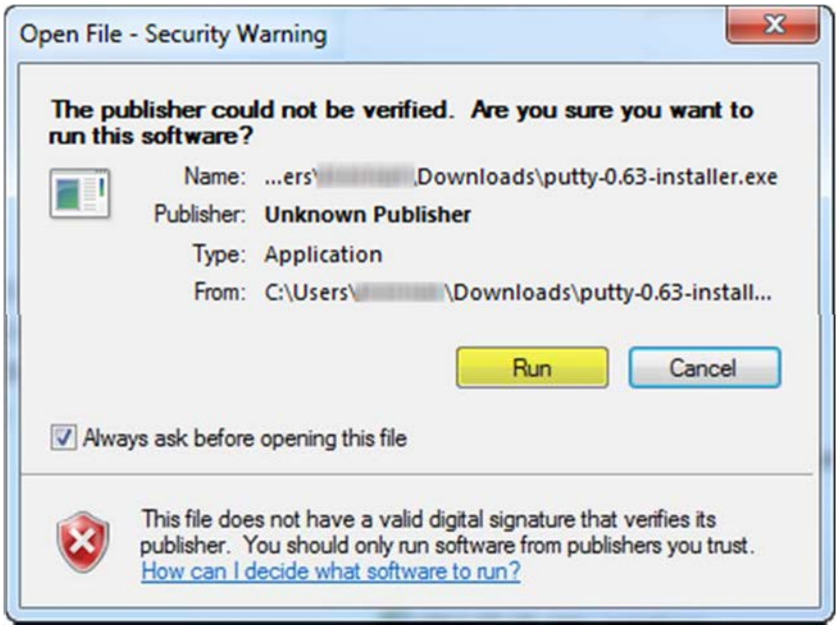
Binaries

The latest release version (beta 0.63). This will generally be a version I think is reasonably likely to work well. If you have a problem with the release version, it might be worth trying out the latest development snapshot (below) to see if I've already fixed the bug, before reporting it to me.

For Windows on Intel x86				
PuTTY:	putty.exe	(or by FTP)	(RSA sig)	(DSA sig)
PuTTYtel:	puttytel.exe	(or by FTP)	(RSA sig)	(DSA sig)
PSCP:	pscp.exe	(or by FTP)	(RSA sig)	(DSA sig)
PSFTP:	psftp.exe	(or by FTP)	(RSA sig)	(DSA sig)
Plink:	plink.exe	(or by FTP)	(RSA sig)	(DSA sig)
Pageant:	pageant.exe	(or by FTP)	(RSA sig)	(DSA sig)
PuTTYgen:	puttygen.exe	(or by FTP)	(RSA sig)	(DSA sig)
A .ZIP file containing all the binaries (except PuTTYtel), and also the help files				
Zip file:	putty.zip	(or by FTP)	(RSA sig)	(DSA sig)
A Windows installer for everything except PuTTYtel				
Installer:	putty-0.63-installer.exe	(or by FTP)	(RSA sig)	(DSA sig)
Checksums for all the above files				
MD5				
SHA				
SHA-256:	sha256sums	(or by FTP)	(RSA sig)	(DSA sig)
SHA-512:	sha512sums	(or by FTP)	(RSA sig)	(DSA sig)

Figure 1 - Download Screen

When the Security Warning appears, click **Run**.



Open File - Security Warning

The publisher could not be verified. Are you sure you want to run this software?

Name: ...ers\[redacted]Downloads\putty-0.63-installer.exe

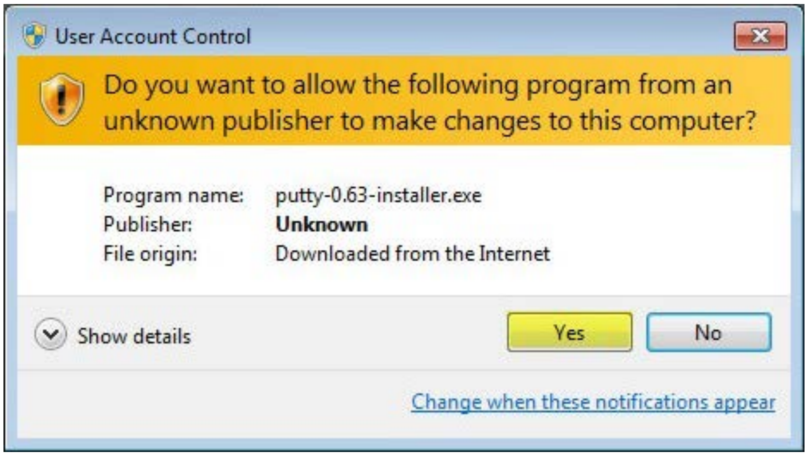
Publisher: **Unknown Publisher**

Type: Application

From: C:\Users\[redacted]\Downloads\putty-0.63-install...

☑ Always ask before opening this file

This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?



User Account Control

Do you want to allow the following program from an unknown publisher to make changes to this computer?

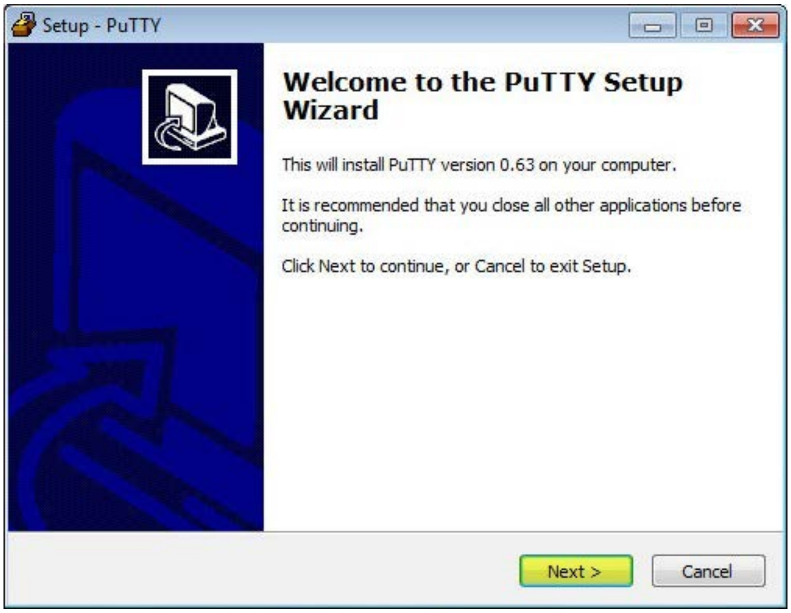
Program name: putty-0.63-installer.exe

Publisher: **Unknown**

File origin: Downloaded from the Internet

If a pop-up warning from Window's User Account Control displays, click **Yes** to continue.

When the Welcome screen appears, click **Next**.



Setup - PuTTY

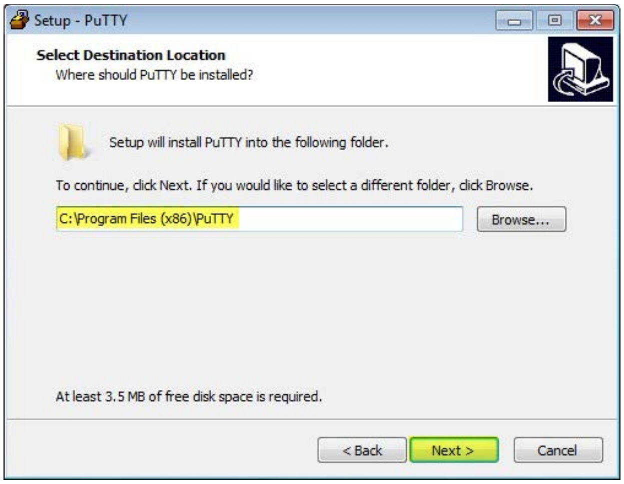
Welcome to the PuTTY Setup Wizard

This will install PuTTY version 0.63 on your computer.

It is recommended that you close all other applications before continuing.

Click Next to continue, or Cancel to exit Setup.

In the Setup screen, save PuTTY to the default destination Location. Select **Next** to continue.



Setup - PuTTY

Select Destination Location

Where should PuTTY be installed?

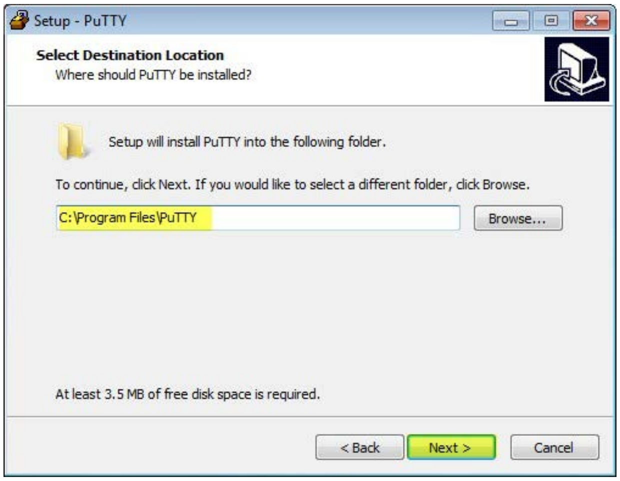
Setup will install PuTTY into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files (x86)\PuTTY

At least 3.5 MB of free disk space is required.

64-bit Machine



Setup - PuTTY

Select Destination Location

Where should PuTTY be installed?

Setup will install PuTTY into the following folder.

To continue, click Next. If you would like to select a different folder, click Browse.

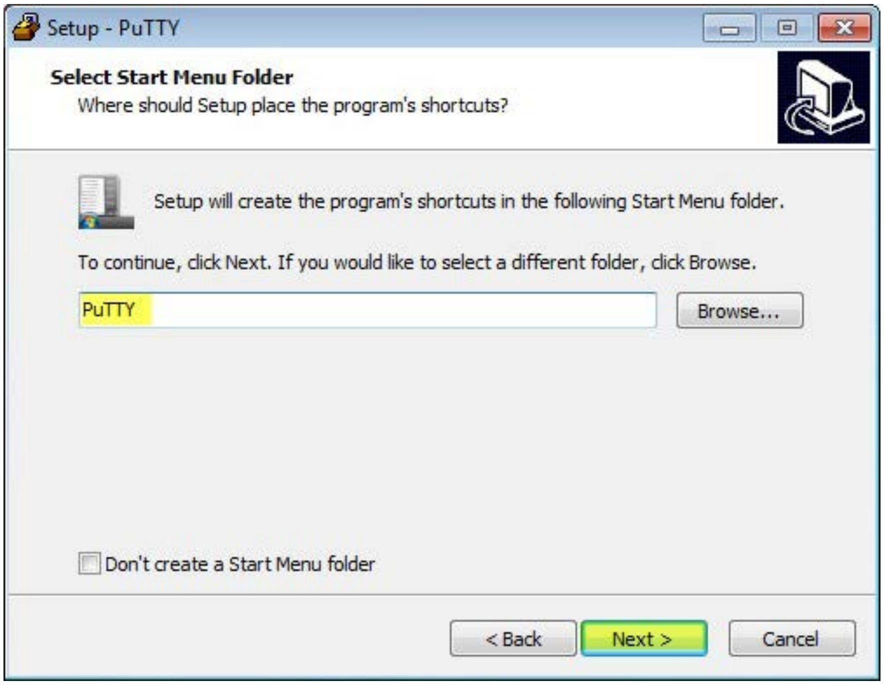
C:\Program Files\PuTTY

At least 3.5 MB of free disk space is required.

32-bit Machine

Note: In this example, the install directory includes **Program Files (x86)**. If your machine is 32-bit, only **Program Files** are displayed, as shown above on the right. Make a note of this location, as you will need to know the directory path later.

On the next setup screen, click **Next** to retain the Start Menu Folder's defaults.



Setup - PuTTY

Select Start Menu Folder

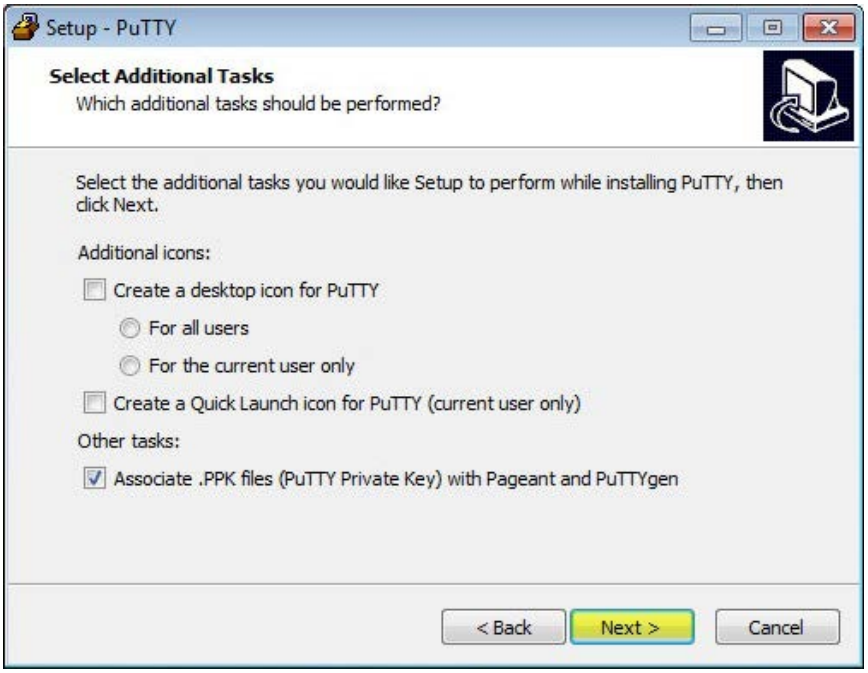
Where should Setup place the program's shortcuts?

Setup will create the program's shortcuts in the following Start Menu folder.

To continue, click Next. If you would like to select a different folder, click Browse.

PuTTY

□ Don't create a Start Menu folder



Setup - PuTTY

Select Additional Tasks

Which additional tasks should be performed?

Select the additional tasks you would like Setup to perform while installing PuTTY, then click Next.

Additional icons:

□ Create a desktop icon for PuTTY

○ For all users

○ For the current user only

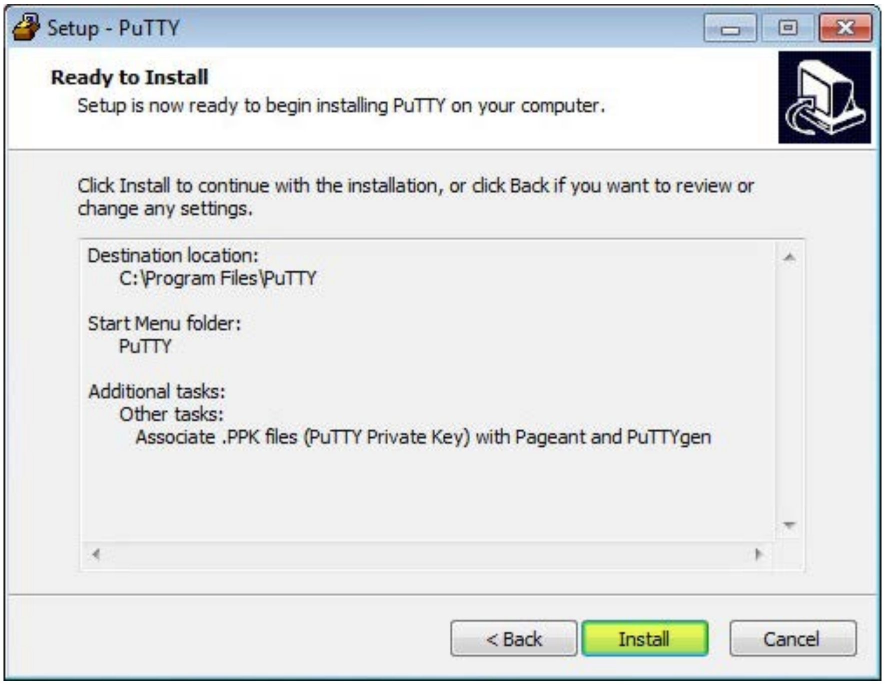
□ Create a Quick Launch icon for PuTTY (current user only)

Other tasks:

☑ Associate .PPK files (PuTTY Private Key) with Pageant and PuTTYgen

On the Select Additional Tasks screen, retain the default selections and click **Next**:

On the Ready to Install screen, verify that the settings are identical to those on the previous screen then select **Install** to continue.



Setup - PuTTY

Ready to Install

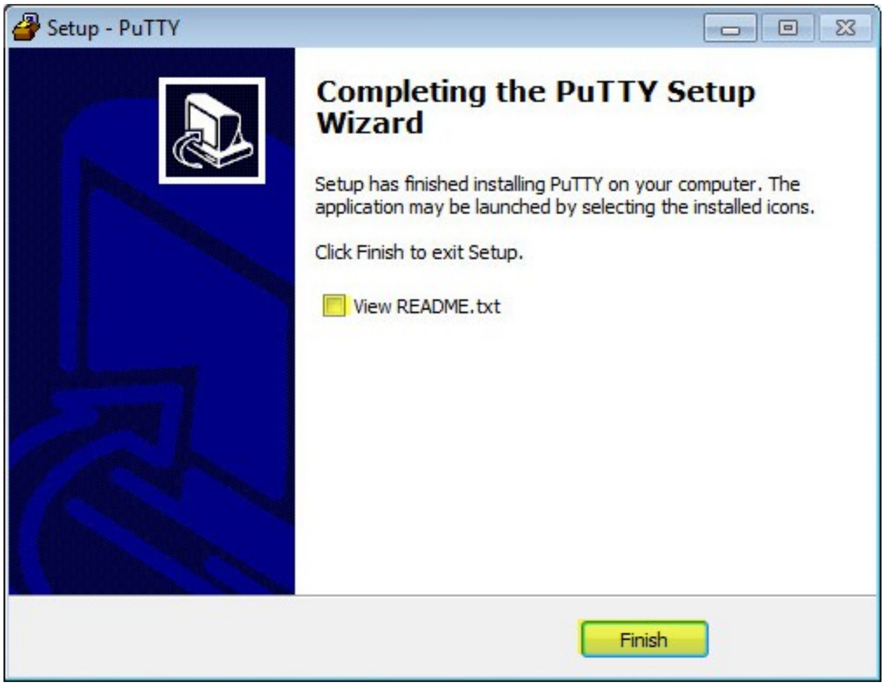
Setup is now ready to begin installing PuTTY on your computer.

Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:
C:\Program Files\PuTTY

Start Menu folder:
PuTTY

Additional tasks:
Other tasks:
Associate .PPK files (PuTTY Private Key) with Pageant and PuTTYgen



Setup - PuTTY

Completing the PuTTY Setup Wizard

Setup has finished installing PuTTY on your computer. The application may be launched by selecting the installed icons.

Click Finish to exit Setup.

□ View README.txt

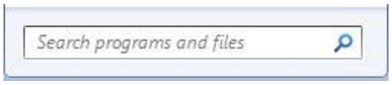
Once the install is complete, uncheck the View README.txt checkbox and click **Finish**.

Key Generation

The next step is to create your public and private keys. These keys contain your password and an encryption certificate to authenticate your files to your destination server.

Once PuTTY is installed, perform the following:

Click the **Start** button. In the Run window, type **c:\Program Files(x86)\PuTTY\puttygen.exe** and hit **Enter**.

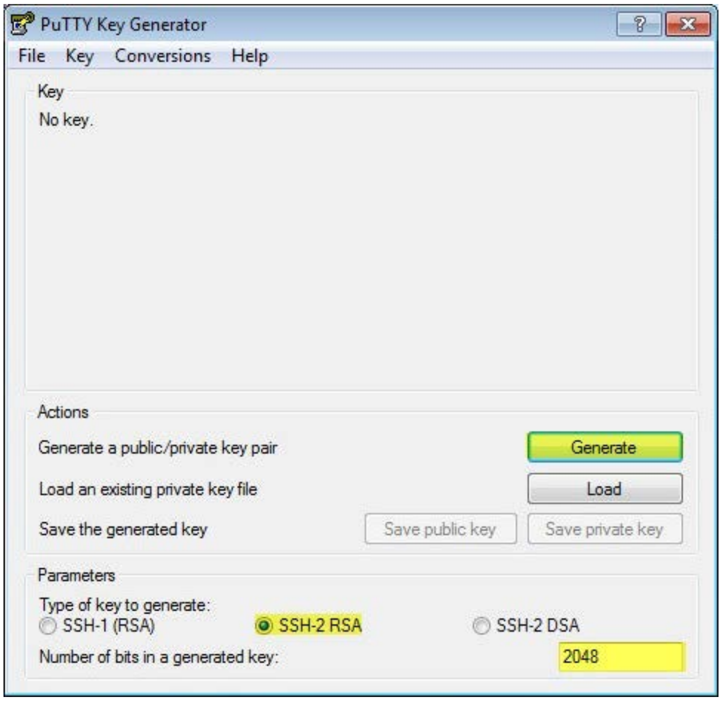


> **Note**: If your Windows install is 32-bit, remove the (x86) text so there is no space between the word "**Files**" and the back slash "\". This format should be similar to the Select Destination Folder screen during the initial PuTTY setup.

The PuTTY Key Generator screen will launch.

- 2048 should appear in the **Number of bits in a generated key** box
- SSH-2 RSA radio button should be selected for **Type of key to generate**

Click **Generate**.



No key.

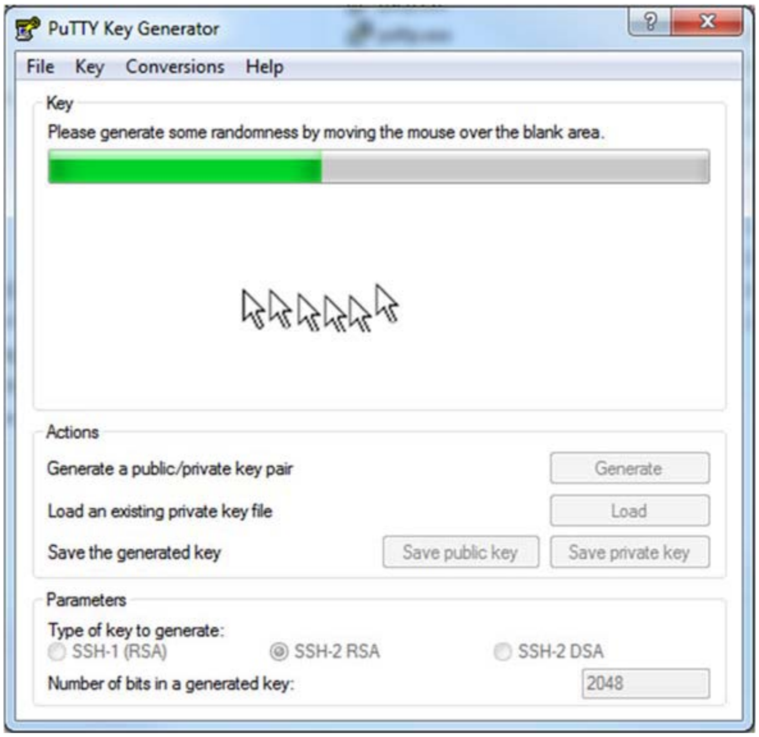
Generate a public/private key pair

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



Key

Please generate some randomness by moving the mouse over the blank area.

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Parameters

Type of key to generate:

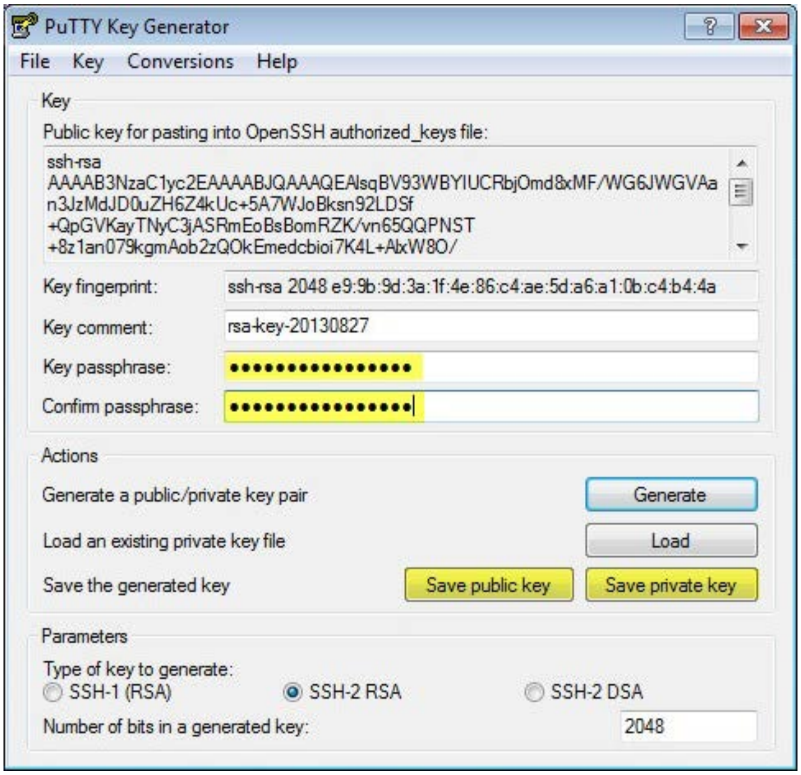
○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 2048

While the key is generating, move the cursor repeatedly over the blank area of the window until the key generation is complete.

The PuTTY Key Generator screen will change to display other fields, including **Key Passphrase** boxes.

The key passphrase requires a strong password. Follow your organization's recommendations for strong passwords and enter it in the **Key passphrase** and **Confirm passphrase** boxes.



Key

Public key for pasting into OpenSSH authorized_keys file:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABJQAAAQEAlsqBV93WBYIUCRbjOmd8xMF/WG6JWGVAa
n3JzMdJD0uZH6Z4kUc+5A7WJoBksn92LDSf
+QpGVKayTNyC3jASRmEoBsBomRZK/vn65QQPNST
+8z1an079kgmAob2zQOkEmedcbioi7K4L+AlxW8O/
```

Key fingerprint: ssh-rsa 2048 e9:9b:9d:3a:1f:4e:86:c4:ae:5d:a6:a1:0b:c4:b4:4a

Key comment: rsa-key-20130827

Key passphrase: •••••••••••••••••

Confirm passphrase: •••••••••••••••••

Actions

Generate a public/private key pair

Load an existing private key file

Save the generated key

Parameters

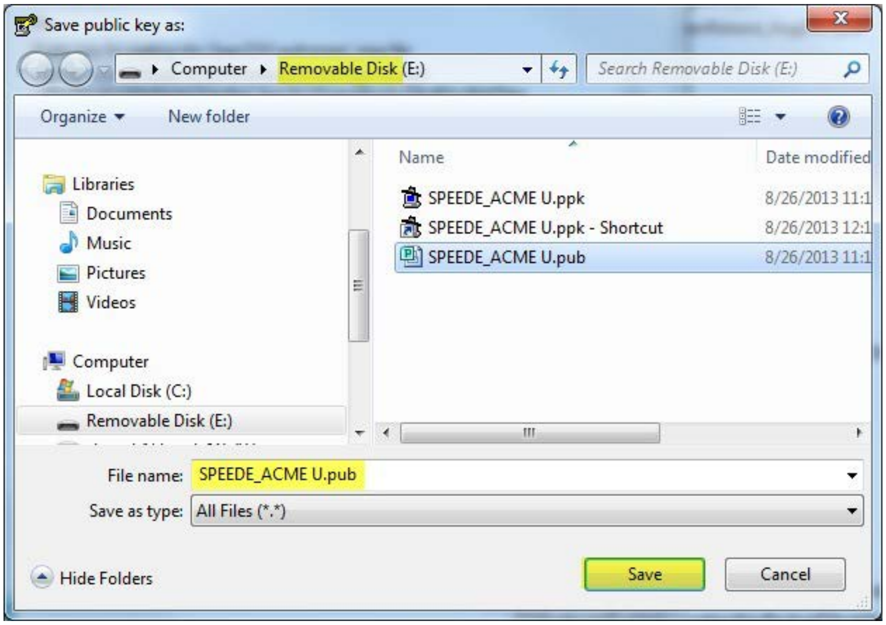
Type of key to generate:

○ SSH-1 (RSA) ● SSH-2 RSA ○ SSH-2 DSA

Number of bits in a generated key: 2048

Save the public and private keys to a safe location, such as a new USB drive (which should not be used for any other purpose) that you can lock in a secure area or a password-protected drive. Name the public key ***SPEEDE_{school name}.pub*** and the private key ***SPEEDE_{school name}.ppk***, as shown below for ***ACME U***.

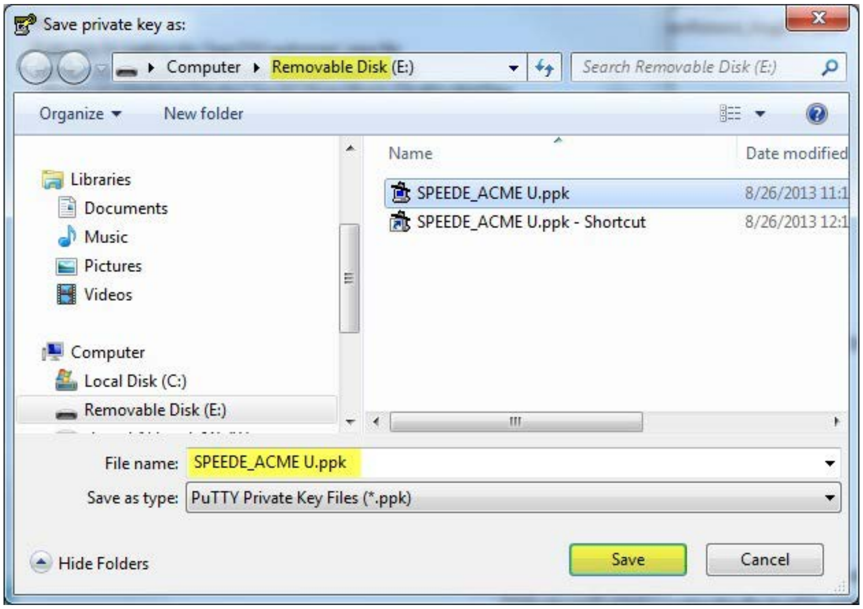
Click **Save Public Key** to open Windows Explorer and name the public key **SPEEDE_{school name}.pub**. Click **Save**.



Name	Date modified
SPEEDE_ACME U.ppk	8/26/2013 11:1
SPEEDE_ACME U.ppk - Shortcut	8/26/2013 12:1
SPEEDE_ACME U.pub	8/26/2013 11:1

File name: SPEEDE_ACME U.pub

Save as type: All Files (*.*)



Name	Date modified
SPEEDE_ACME U.ppk	8/26/2013 11:1
SPEEDE_ACME U.ppk - Shortcut	8/26/2013 12:1

File name: SPEEDE_ACME U.ppk

Save as type: PuTTY Private Key Files (*.ppk)

Repeat this step for the **Save Private key** (you'll need to add the passphrase again) and name it **SPEEDE_{school name}.ppk** for the private key. Click **Save**.

At this point, your private and public keys are generated. If you are using PuTTY to FTP your files to SPEEDE, continue with the next section. Otherwise, use these keys with any application you use to connect to the SPEEDE server over the supported protocol.

Close the PuTTY Key Generator, which is no longer needed.

Configuring PuTTY for SPEEDE Use

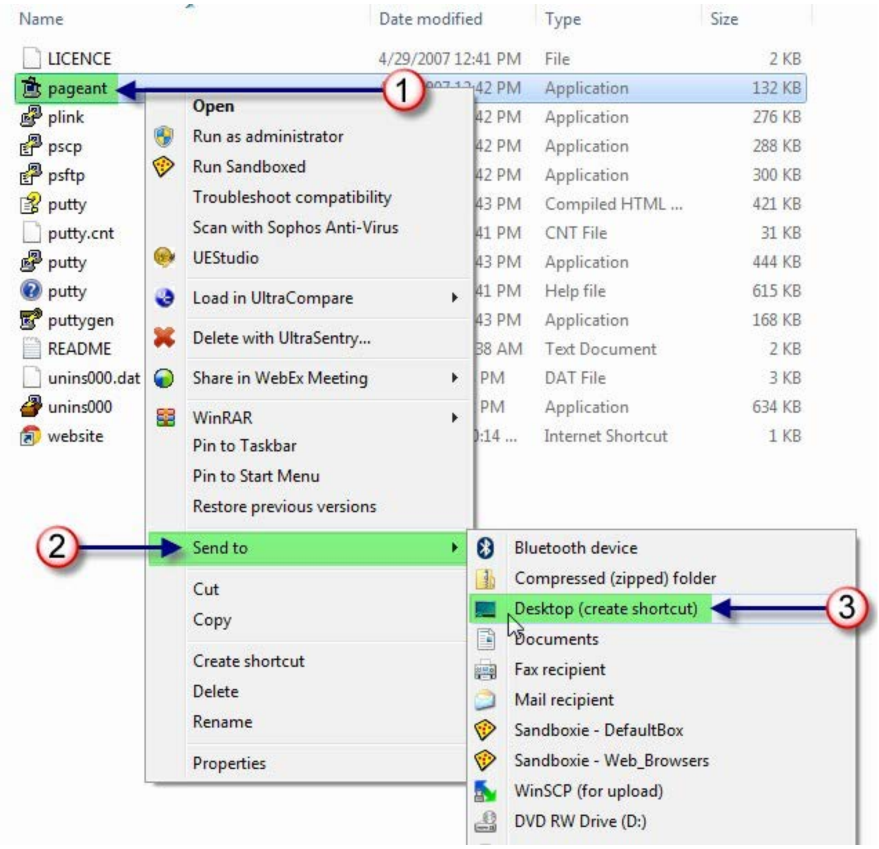
Load PuTTY Private Key on Logon to Windows

This section deals with getting your computer to load the private key into memory on system startup, so you will not need to load it each time you connect to SPEEDE.

Insert the USB drive that contains your public and private keys into your computer or go to the password-protected drive where you stored your public and private keys.

Click the Start button and type **explorer.exe** in the Run window, then hit **Enter** or open Windows Explorer. Select ***Computer***, ***Local Disk (C:)***, ***Program Files*** (or ***Program Files (x86)***), ***PuTTY*** (or select the password-protected drive where you stored your public and private keys).

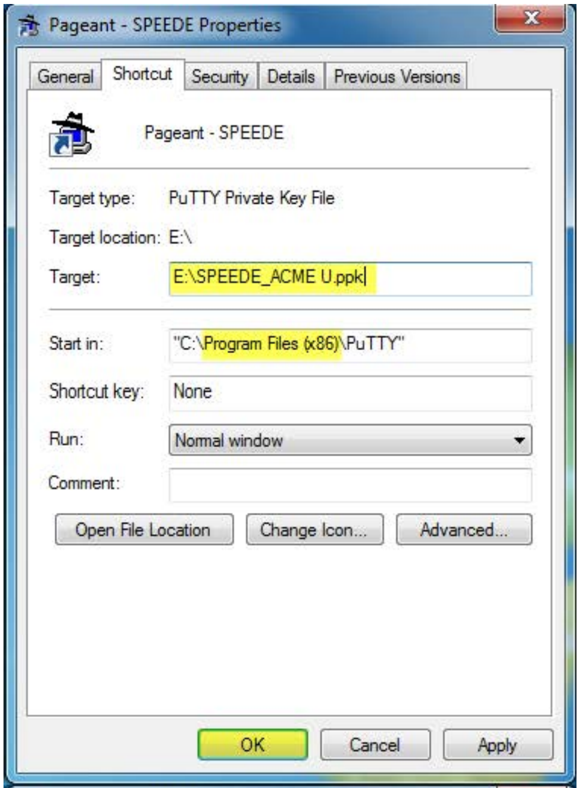
1) Right click the file ***pageant.exe***. 2) select ***Send to***, then 3) choose ***Desktop***.



Name	Date modified	Type	Size
LICENCE	4/29/2007 12:41 PM	File	2 KB
pageant	12:42 PM	Application	132 KB
plink	42 PM	Application	276 KB
pscp	42 PM	Application	288 KB
psftp	42 PM	Application	300 KB
putty	43 PM	Compiled HTML ...	421 KB
putty.cnt	41 PM	CNT File	31 KB
putty	43 PM	Application	444 KB
putty	41 PM	Help file	615 KB
puttygen	43 PM	Application	168 KB
README	38 AM	Text Document	2 KB
unins000.dat	PM	DAT File	3 KB
unins000	PM	Application	634 KB
website	:14 ...	Internet Shortcut	1 KB

Minimize all screens on your Desktop so you can see the icon you just created. Right click the icon and select ***Properties***.

64-bit Machine



Pageant - SPEEDE Properties

Pageant - SPEEDE

Target type: PuTTY Private Key File

Target location: E:\

Target: E:\SPEEDE_ACME U.ppk

Start in: "C:\Program Files (x86)\PuTTY"

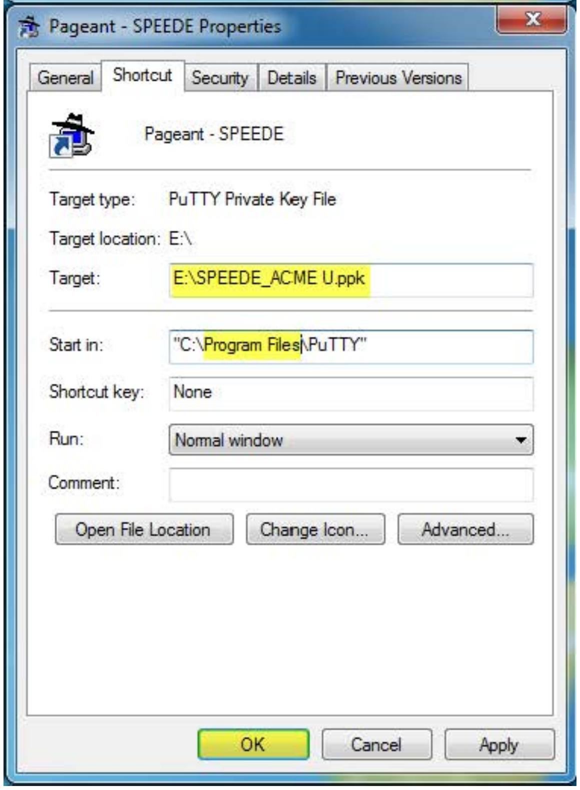
Shortcut key: None

Run: Normal window

Comment:

In the ***Target*** box, enter the path to the private key you created. When you are done, click **OK**.

32-bit Machine



Pageant - SPEEDE Properties

Pageant - SPEEDE

Target type: PuTTY Private Key File

Target location: E:\

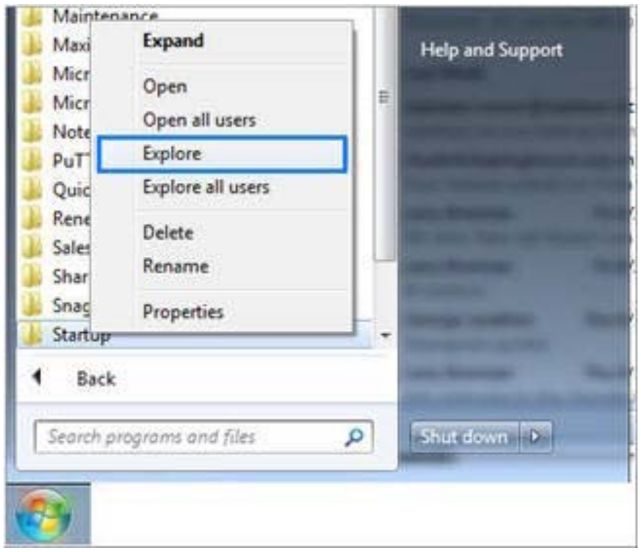
Target: E:\SPEEDE_ACME U.ppk

Start in: "C:\Program Files\PuTTY"

Shortcut key: None

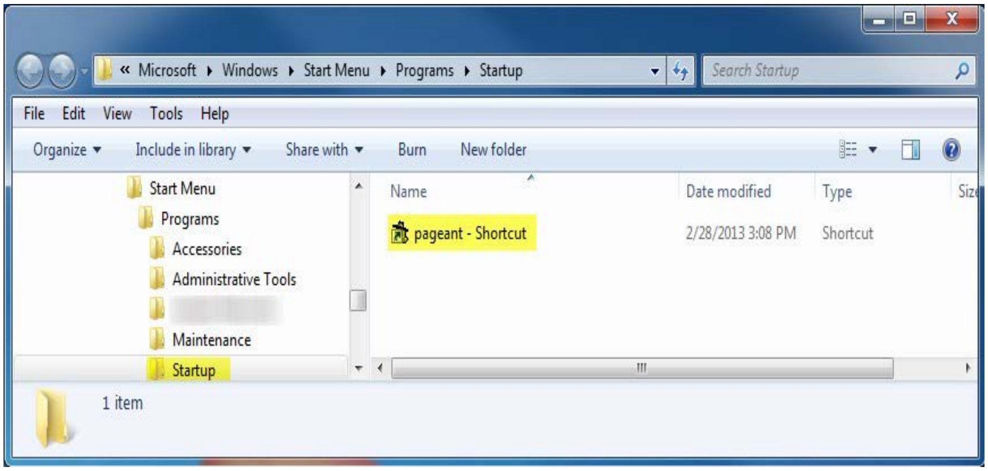
Run: Normal window

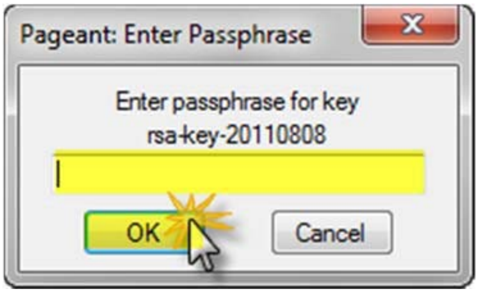
Comment:



Click the Start button and select **All Programs.** Right click on the **Startup** folder and select **Explore**.

This opens the Startup folder in Windows Explorer. Drag the **Pageant** shortcut from your desktop into the Startup folder. Once the shortcut is in place, double click it to test it.





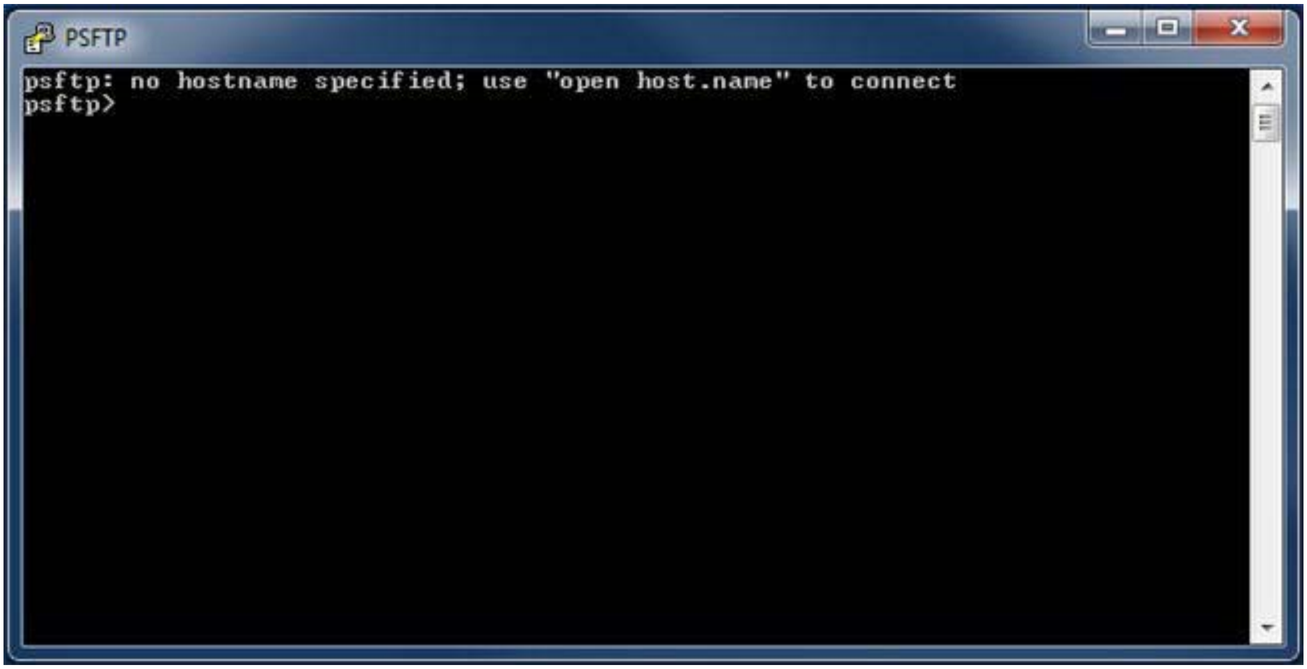
Enter passphrase for key rsa-key-20110808

A small passphrase box will display. Enter the private key password you created when storing the original private key and click **OK**.

Remember, every time you log into your workstation, you should plug in your USB drive or go to the password-protected drive where you stored your public and private keys so this box will appear. All you need to do is enter your private key password. You don't need to worry about loading your private key password each time you open a session to the server.

Using PuTTY's PSFTP

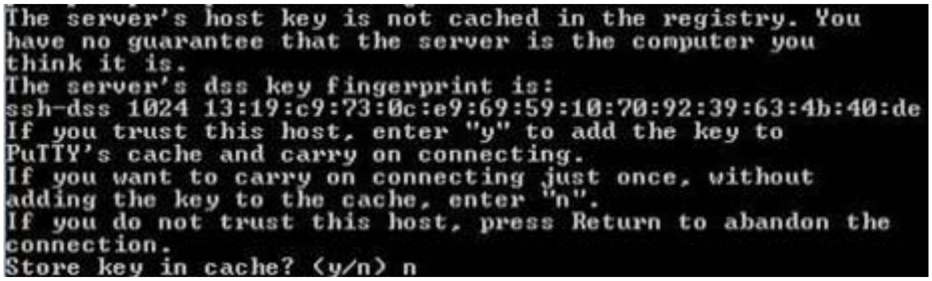
To use PSFTP, click the **Start** button, select **All Programs** and then select **PuTTY**. Click the **PSFTP** icon . The PSFTP window will display.



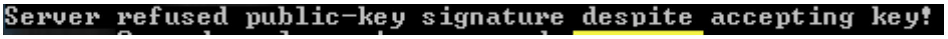
```
psftp: no hostname specified; use "open host.name" to connect
psftp>
```

At the prompt (psftp>), type **open SPEEDE.nslc.org** and press **Enter**.

When prompted with **login as,** enter your assigned SPEEDE user name and password and hit **Enter**. On initial connection, several things happen.



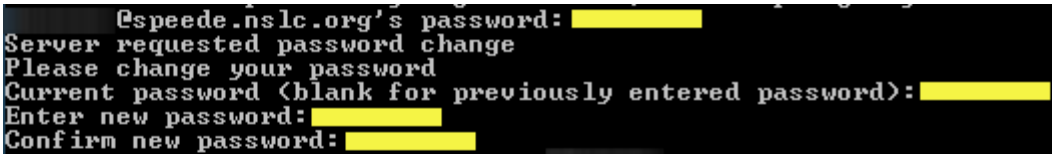
```
The server's host key is not cached in the registry. You
have no guarantee that the server is the computer you
think it is.
The server's dss key fingerprint is:
ssh-dss 1024 13:19:c9:73:0c:e9:69:59:10:70:92:39:63:4b:40:de
If you trust this host, enter "y" to add the key to
PuTTY's cache and carry on connecting.
If you want to carry on connecting just once, without
adding the key to the cache, enter "n".
If you do not trust this host, press Return to abandon the
connection.
Store key in cache? (y/n) n
```



```
Server refused public-key signature despite accepting key!
```

The message "***Server refused public-key signature despite accepting key!***" will display. This is normal since the system has never seen your public key before. Within 24 hours, an administrator will validate your key and, if no issues present, accept your public key into the SPEEDE system. To request faster processing of your public key, email us at SPEEDEsupport@studentclearinghouse.org or call 703-742-4200. You will know SPEEDE has accepted your public key when the system no longer prompts you for a password.

Secondly, SPEEDE will ask for the initial password provided to you by the SPEEDE team. Once you enter the initial password, you will be prompted to change it.



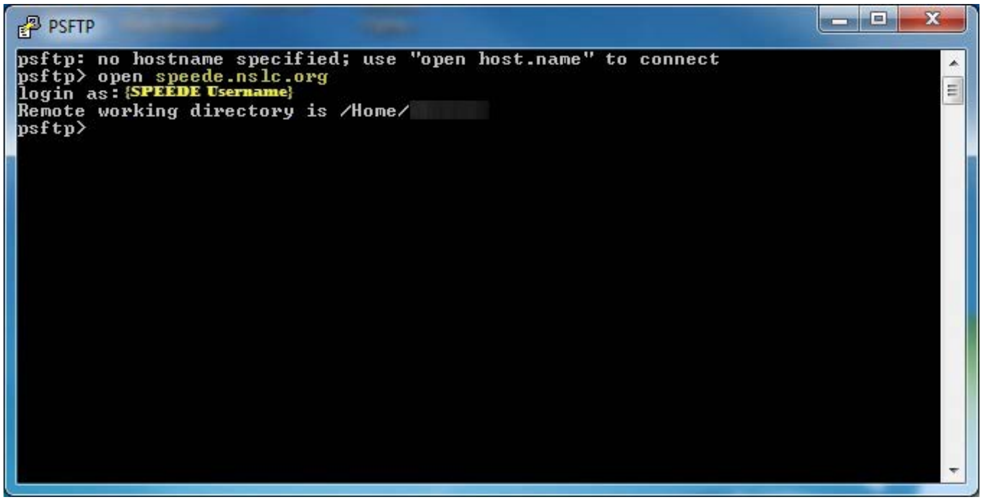
```
[redacted]@speede.nslc.org's password:
Server requested password change
Please change your password
Current password (blank for previously entered password):
Enter new password:
Confirm new password:
```

Hit ***Enter***, for the current password and SPEEDE will use the initial password you just entered. Type your new password twice to set it. Retain this password in a text file on your USB drive that is stored in a secure location or on a password-protected drive. In case anything ever interferes with your keys authenticating you, you can still get onto the system with your username and password.

Password Requirements:

- Passwords cannot resemble usernames
- Password must be at least eight characters long
- Passwords must contain at least one uppercase letter, one lowercase letter, and one number
- Passwords cannot contain common dictionary words
- Passwords must contain at least one special character (such, as $ or !)

If your key is accepted, you will see the screen below and you can begin transferring files knowing your session is protected with 2048-bit RSA encryption.



```
psftp: no hostname specified; use "open host.name" to connect
psftp> open speede.nslc.org
login as:{SPEEDE Username}
Remote working directory is /Home/[redacted]
psftp>
```

To exit from PSFTP, type “bye” or “exit” in all lower case.

You are now ready to **upload** or **download** files via FTP using the “get” and “put” commands. For help, type “**?**” or “**help**.”