

# SSH Tutorial: Windows

Last Updated Wednesday, 03 September 2008

## Quick Reference

- SSH - Secure Shell
- SFTP - Secure File Transfer Protocol    What is SSH?

From the SSH help files:

"The SSH Secure Shell for Workstations (SSH2 client) is a program that allows secure network services over an insecure network. SSH Secure Shell for Workstations replaces other, insecure terminal applications, such as Telnet and FTP. It allows you to securely login to remote host computers, to execute commands safely on a remote computer, and to provide secure encrypted and authenticated communications between two hosts in an untrusted network. X11 connections and arbitrary TCP/IP ports can also be forwarded over the secure channel, expanding SSH Secure Shell for Workstations's usability even further."

Basically, SSH is a protocol that protects your computer as well as the remote host from possible security risks. With SSH, scp, and sftp you can replace all of the insecure tools. Those tools are considered insecure because they make no attempt to encrypt your password or your data.

Why should I use it?

SSH should be used to replace the following applications currently in use at the center:

- telnet
- WS\_FTP
- ftp (Unix and Windows command line clients)
- Unix r-commands (rcp, rlogin, rsh)

SSH allows you to satisfy all your communication and file transfer needs in the same suite of software and also provides an intuitive interface to do it. I will not delve into all the features of the SSH software nor will I give a lesson on public and private key encryption. The purpose of this tutorial is to teach people who currently use the above tools on how to use the SSH software.

## Windows Setup and Use

### Downloading

SSH can be downloaded at the following locations:

- <ftp://ftp.cis.rit.edu/support/software>

The SSH we use is the non-commercial version for workstations. This version is the same as the commercial version except for a licensing difference and the non-commercial does not support PKI or PKCS functionality.

Once at the download site:

- Click "SSHSecureShellClient-3.2.9.exe" \* Please note that version numbers are reflective of the time this tutorial was written
- Select "Save to Disk" -> Hit "Ok"

### Installing

Find where the setup file is saved:

- Open the file "SSHSecureShellClient-3.2.9.exe".
- Follow the prompts, leave all the defaults.
- Two icons should appear on the desktop labeled:
  - SSH Secure Shell Client
  - SSH Secure File Transfer
- Installation is complete

### Using the Windows SSH Secure Shell Client

This topic will be divided into two sections:

- The first is a brief overview of the SSH window.
- The second will go over quick connecting to a remote host. This will not require the use of profiles or any advanced

features.

Before anything else, SSH must be started. This can be done by either:

- Open the icon that was placed on the desktop named "SSH Secure Shell Client"
- Go to "Start" -> "Programs" -> "SSH Secure Shell" -> "SSH Secure Shell Client"

#### Window Overview

- Quick Connect: Execute a quick connect. You will be prompted for a remote host name and your username. ( It will also prompt for a port and authentication method, but these are set by defaults. )
- Profiles: Brings up a menu that allows you to edit, add or select a profile.
- Connection Buttons: The first button brings up a quick connect dialog. When connected the second button can be used to disconnect from the remote host.
- Program Buttons: The first button launches another client window. The second button launches a new FTP window.
- Help Button: Brings up the help libraries. Very useful.
- Terminal Window: This is the terminal window. Once connected, all commands are done in here.

#### Quick Connect

The quickest way to connect to a remote-host is by using the quick connect button. (1, above.)

When you click the quick connect button, the following dialog will appear:

The Hostname and Username fields will be empty so they must be filled in.

In this case I'm using a fictional machine, grissom:

- Enter remote-host name
- Enter user name
- Click Connect

#### Host Identification

If this is the first time you are connecting to this particular remote-host, you will receive the following dialog:

This dialog is the remote-host sending you it's public key. This is used in the encryption scheme of SSH. The dialog offers to save the public key to the local database so you won't have to confirm the public key each time you connect to that particular remote-host from your current machine. It is not vital to save it to the local database, but if you SSH into the same remote-host with the same machine often, it is recommended.

- Yes: Saves the public key to the local database, connection to remote-host continues.
- No: Does not save the public key, connection to remote-host continues.
- Cancel: Does not save the public key, connection closes.
- Help: Opens the SSH help files.

#### Password

You will then be prompted for a password:

- Enter your password
- Click Ok

If the connection was successful you will see a prompt in the terminal window like the one you received using telnet or putty. You can now execute commands and anything else you need to do.

#### Disconnecting

Click the button that has a red slash through it (3) or close the SSH window.  
(FTP)

Using SSH Secure File Transfer Client

This topic will be divided into two sections:

- The first is a brief overview of the FTP window.
- The second will go over quick connecting to a remote host. This will not require the use of profiles or any advanced features.

Before anything else, the FTP client must be started. This can be done by either:

- \* Open the icon that was placed on the desktop named "SSH Secure File Transfer Client"
- \* Go to "Start" -> "Programs" -> "SSH Secure Shell" -> "SSH Secure File Transfer Client"

#### FTP Window Overview

- Quick Connect: Execute a quick connect. You will be prompted for a remote host name and your username. ( It will also prompt for a port and authentication method, but these are set by defaults. )
- Profiles: Brings up a menu that allows you to edit, add or select a profile.
- Connection Buttons: The first button brings up a quick connect dialog. When connected the second button can be used to disconnect from the remote host.
- Program Buttons: The first button launches another client window. The second button launches a new FTP window.
- Help Button: Brings up the help libraries. Very useful.
- Local Host: This window displays the directory structure of the machine you are currently using. It navigates just like Windows.
- Remote Host: This window displays the directory structure of the machine you are connecting to. It also navigates like Windows.
- Transfer Window: All pending, current and past transfers between hosts will be displayed in this window

#### FTP Quick Connect

Quick connecting is identical to quick connecting in the SSH Secure Shell Client.

So refer to the quick connect instructions in the previous portion of this document.

#### Transferring Files

Transferring files is as easy as moving files on your local machine:

- Select the files you want to transfer.
- Drag them to their destination.

You don't even have to find the file in the directory structure(6 & 7) to transfer them. You can simply drag something from your desktop or anywhere else to the remote-host and likewise.