



Installing the SSH Client v3.2.2 For Microsoft Windows

OVERVIEW	1
SYSTEM REQUIREMENTS	2
INSTALLING THE SSH PACKAGE	2
STARTING THE PROGRAMS	5
USING THE SHELL CLIENT	8
USING THE FILE TRANSFER CLIENT	9
HOW TO START SSH SECURE FILE TRANSFER	9
SIMPLE UPLOADING AND DOWNLOADING	10
UN-INSTALLING THE SSH PACKAGE	11
GETTING MORE HELP WITH SSH	11

Overview

Many people use the Telnet program (e.g.: QVT/Term) to connect to a remote machine, like `uhunix2.its.hawaii.edu`. During the Telnet session, a lot of information passes between the PC and the remote machine, including your password, the contents of your email messages and basically anything that can be viewed on the screen or typed in at the keyboard. This information could potentially be read by malicious people on your network using specialized tools. FTP (File Transfer Protocol) is also vulnerable to hackers. For this reason, Telnet and FTP programs are not considered secure.

There are several secure alternatives to Telnet and FTP. One alternative is the SSH Secure Shell for Workstations package, by SSH Communications. It has 2 components: the Shell Client (a secure replacement for Telnet) and the File Transfer Client (a secure replacement for FTP).

These programs encrypt all data passing between the PC and the remote machine, including passwords. The SSH package has become the de facto standard for secure logins.

System Requirements

The SSH client does not have any special hardware or software requirements. SSH client is compatible with any computer running Microsoft Windows 95, Windows 98 or 98 SE, Windows ME, Windows NT 4, Windows 2000, or Windows XP.

The SSH client installation requires a minimum of 4 megabytes of disk space. However, the default installation will take about 12 megabytes of disk space.

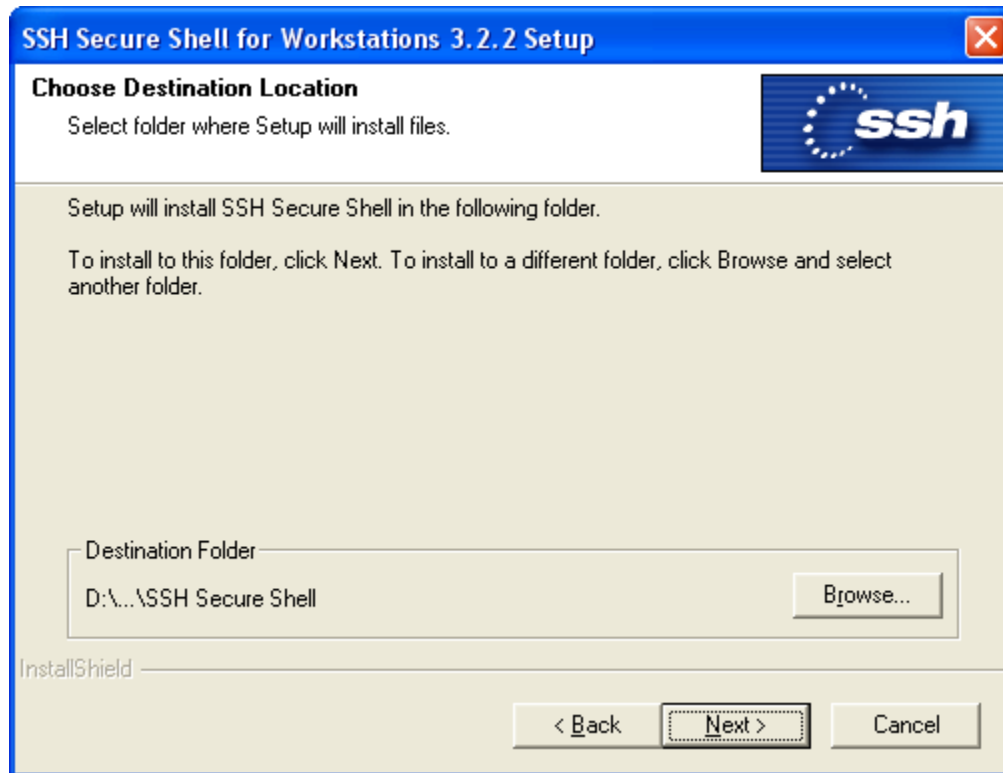
Installing the SSH package

1. SSH can be downloaded from <ftp://ftp.hawaii.edu/pub/dss/ibmpc/ssh322win.exe>. When downloading the installation file, save it on the Desktop for easy access.
2. Exit from all other programs before installing the SSH package.
3. When download is completed, go to the Desktop and open the installation file.
4. The *SSH Setup Wizard* will start. Click **Next**.

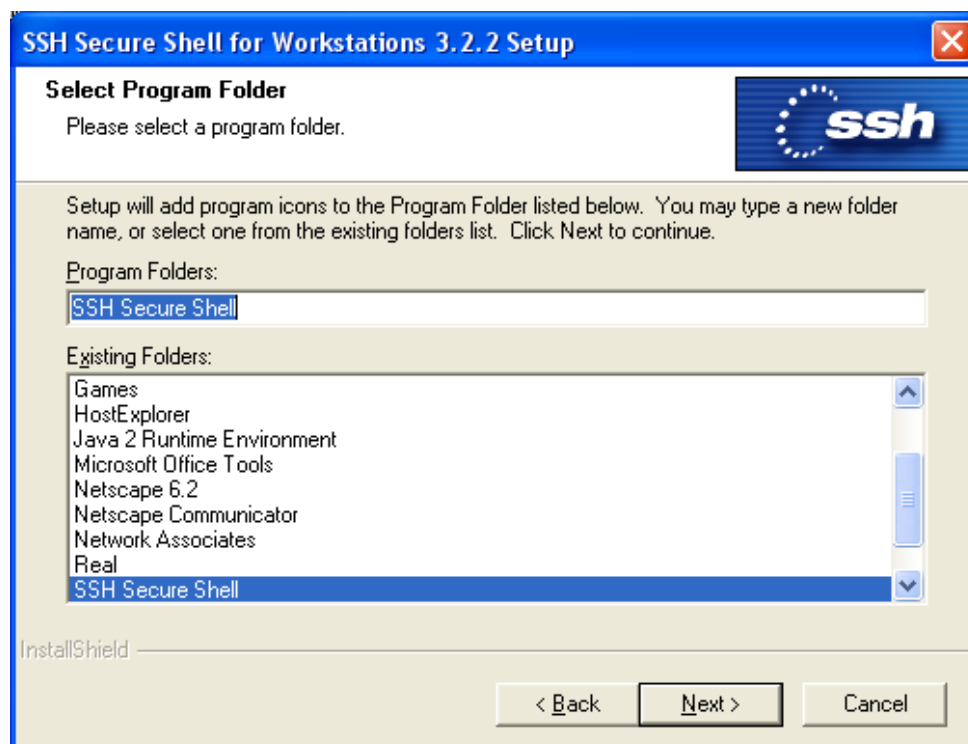


5. The SSH License Agreement screen will come up. Click **Yes** to accept these terms. Click **no** to decline.

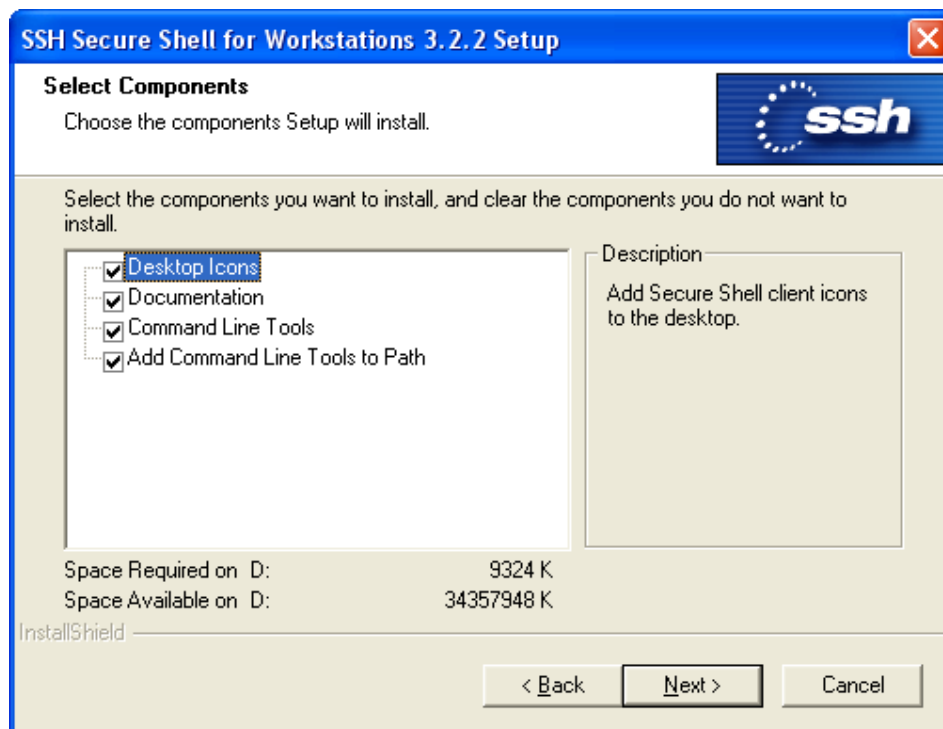
6. The *SetupWizard* will now prompt you to select the installation folder. If Click **Next** to accept the default location or **Browse** to define a different folder.



7. The *SetupWizard* will now prompt you to add a Program Folder into which it will place the SSH program icons. Click **Next** to accept the default or rename to your preference.

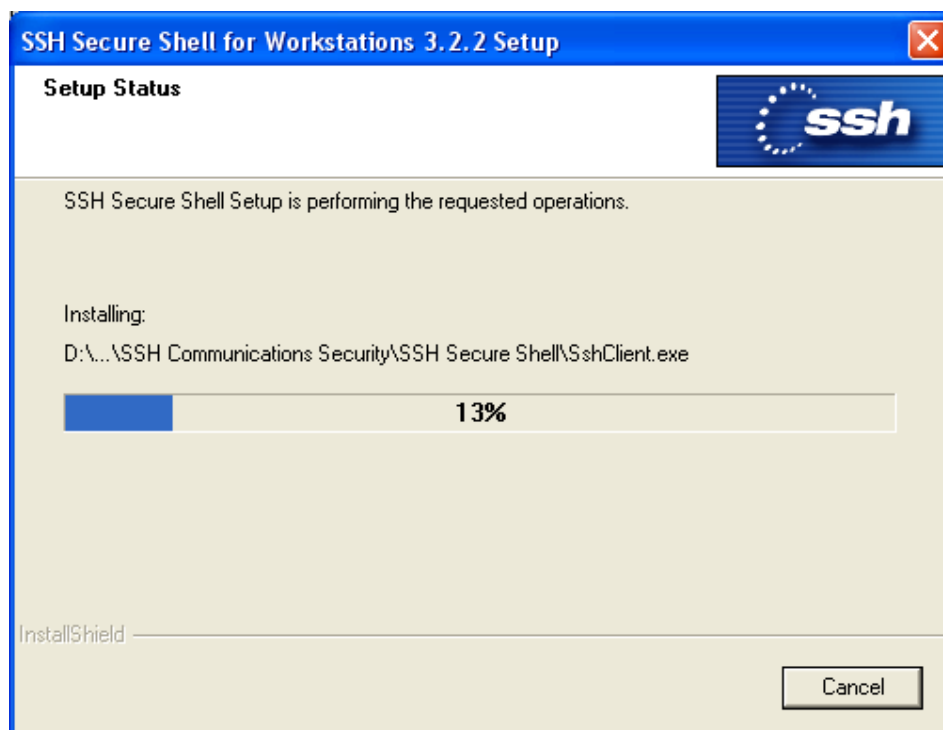


8. The *SetupWizard* prompts you to select which components to install. By default it will install everything. Click **Next** to accept the default or choose components as needed.



9. The *SetupWizard* prompts you to confirm the installation settings. Click **Next** to accept it or click **Back** to make changes.

10. The *SetupWizard* will now install SSH onto your computer.

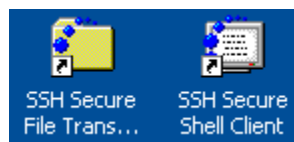


11. Click **Finish** to complete the installation.

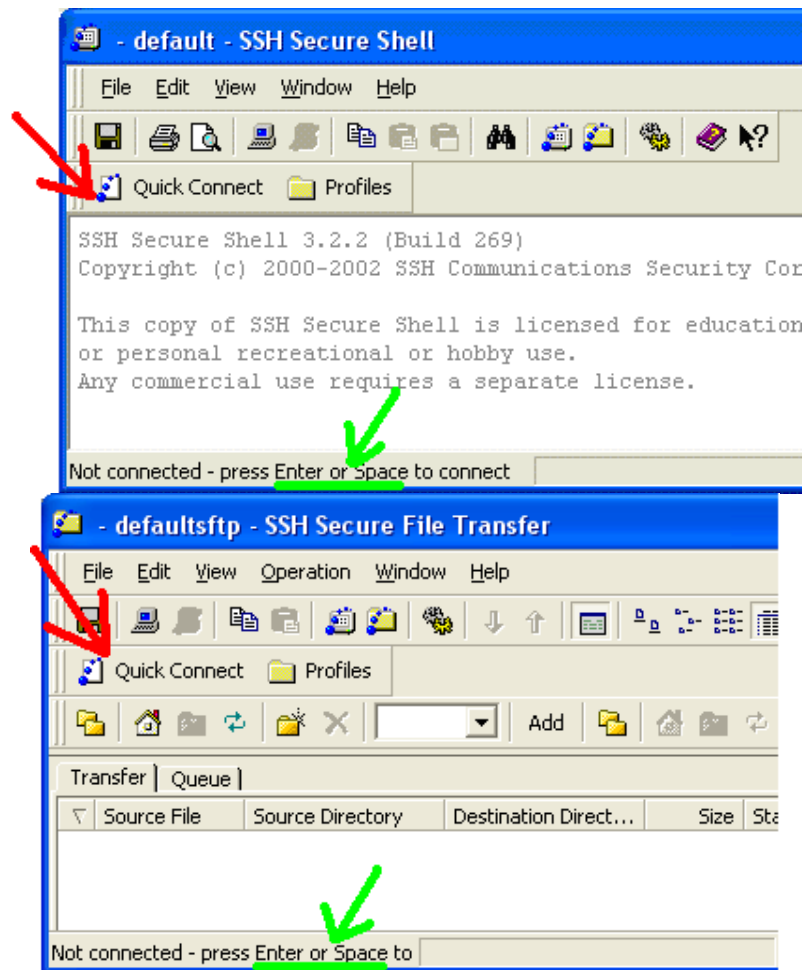


Starting the Programs

1. After the installation, you will find two new icons on your desktop: one for SSH Secure Shell Client and one for SSH Secure File Transfer Client. To start one of these programs, double-click the appropriate icon on the desktop.

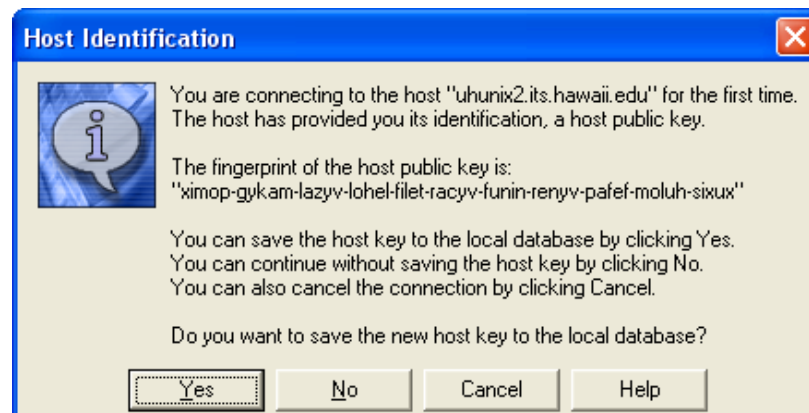


Now, to connect to a remote computer, click the **Quick Connect** button on the tool bar in the program window.

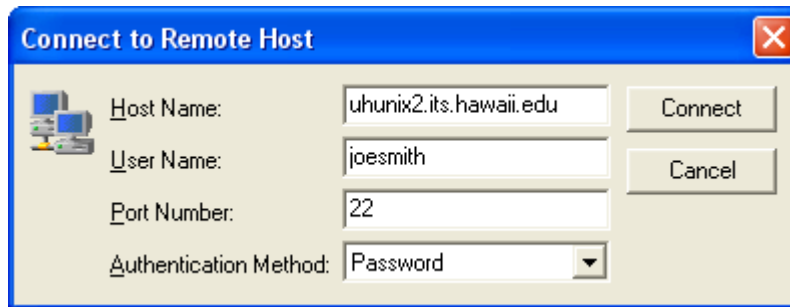


The **Connect to Remote Host** window will appear.

*The first time you connect to a new host, you will receive a **Host Identification** message informing you that an encryption key for this remote machine is being created. Click **Yes** to accept this key and continue.*

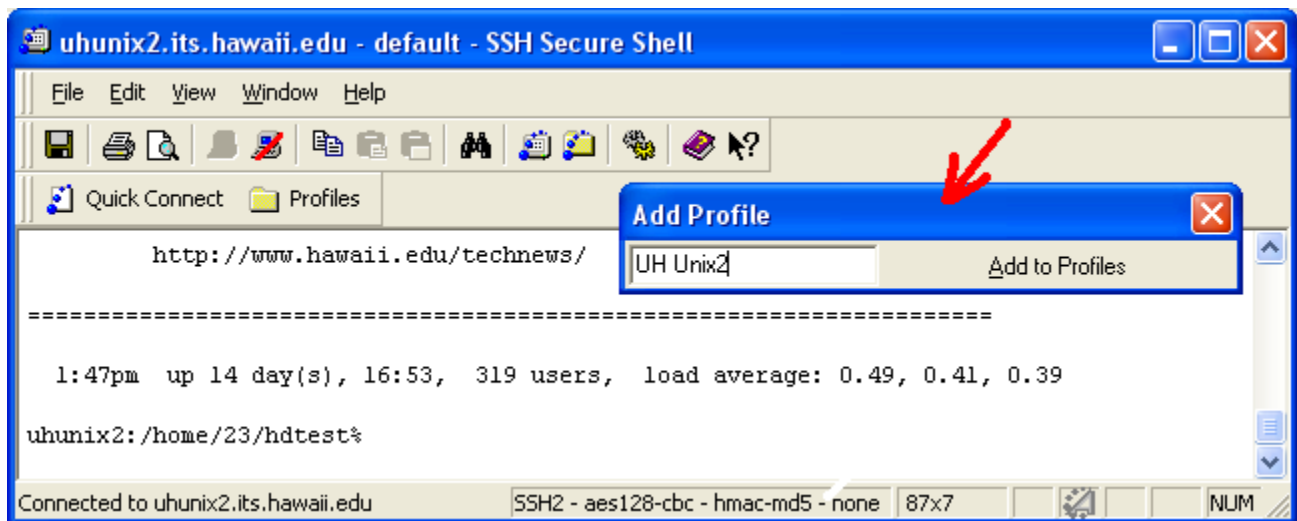


2. Type in a host name (for example: `uhunix2.its.hawaii.edu`) and your ITS username. Do not change the Port Number or Authentication Method. Click **Connect**.



4. You are now prompted for your ITS password. Enter it and click **OK**. You are now able to use the programs.

5. (Optional) The **Add Profiles** window will appear. Type a name for this profile. (It is a good idea to name the profile something like "UH unix 2 Terminal" or "UH unix 2 File Transfer".) Click **Add the Current Connection to Profiles**.



You have now saved your choice of remote host (e.g.: `uhunix2.its.hawaii.edu`) and your ITS username (e.g.: `joesmith`) as a profile (perhaps named "UH unix2").

From now on, when you start the program, you can click the **Profiles** button and select the profile you just created. All the configuration information will be recalled and you will then be prompted for your ITS password.

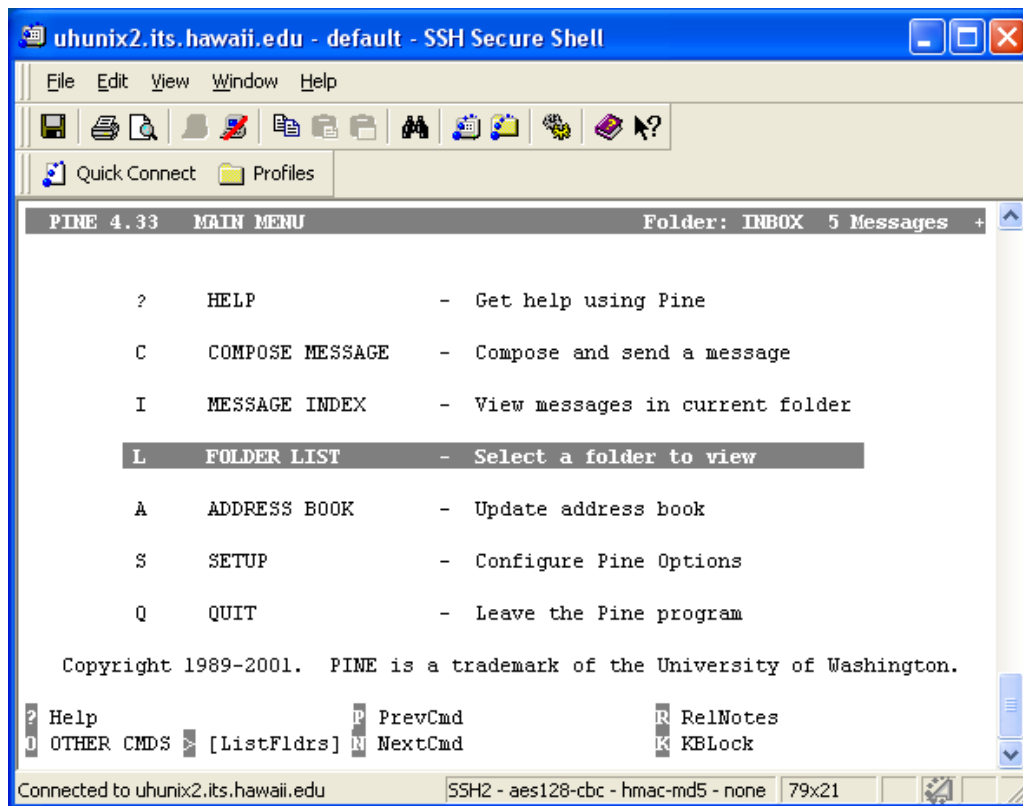
You can create many different profiles, each of which could have different combination of host name, user name, fonts, keyboard layouts, colors, etc.

Note: To make a secure connection using SSH, you must connect to a machine running the SSH server, such as uhunix2.its.hawaii.edu. If you try to use the SSH client to connect to a machine not running SSH server, you will not be able to make a secure connection. To make a non-secure connection, use Telnet or FTP instead.

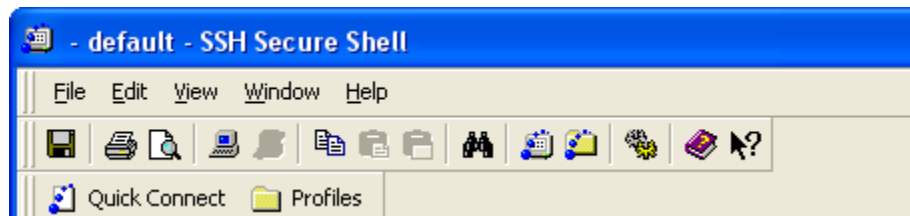
Both the Shell Client and the File Transfer Client use host profiles. These instructions also apply to both programs. You go through the same steps for each: connecting to the remote host, creating a profile with a host name and a user name, save the profile, etc. The File Transfer Client will be covered more in detailed later in this document.

Using the Shell Client

If you followed the steps above using the Shell Client and entered your ITS password, you should now be logged into your uhunix account. The Shell Client is very similar to other Telnet programs in most respects. You can use all Unix commands in SSH Shell Client the same way you that you use in you Telnet program. For example, you can type “**pine**” and press “**enter**” on the keyboard to use the pine email client.



The Secure Shell window has a toolbar with several buttons. If you are not certain what a button does, move the mouse over the button for a few seconds and a short description of the button will appear. It is good practice to familiarize yourself with the different functions of the program.



Hint: If someone mails you the URL to a web-site, just click on the text of that URL and SSH will automatically open a web-browser to that site.

Note to Pine users: This version of the SSH Secure Shell Client does allow you to print to a locally attached printer from Pine. (Earlier versions did not allow this.)

When you finish using your session, log out as you normally would (by typing **logout**) and close the Shell Client.

Using the File Transfer Client

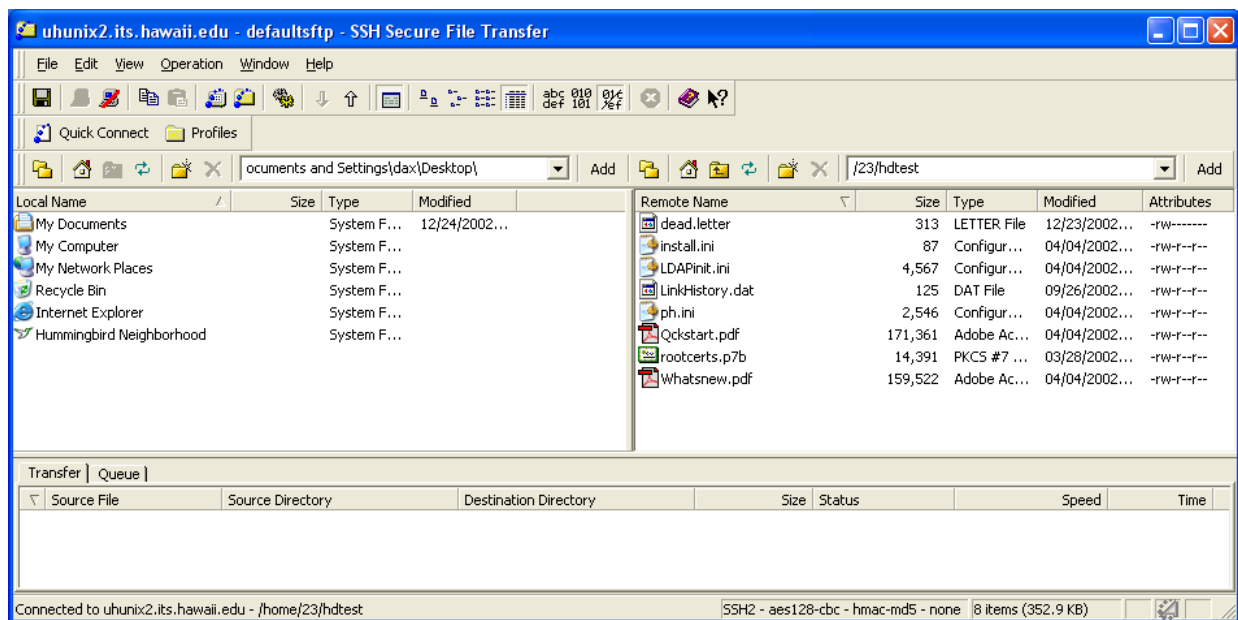
The SSH Secure File Transfer program is a good replacement for FTP. It allows you to transfer files between your local machine and the remote machine quickly, easily and securely. The graphical user interface is very similar to the Microsoft Windows Explorer. For example, you can 'cut' files and folders from your PC and 'paste' to the remote machine, or from remote machine to PC. You can also open a file (like a MS-Word document) on a remote machine by simple clicking on it. (You do not have to download it to work with it.)

HOW TO START SSH SECURE FILE TRANSFER

To Start SSH Secure File Transfer and connect to a remote machine, follow the procedure described in **Starting the Programs**.

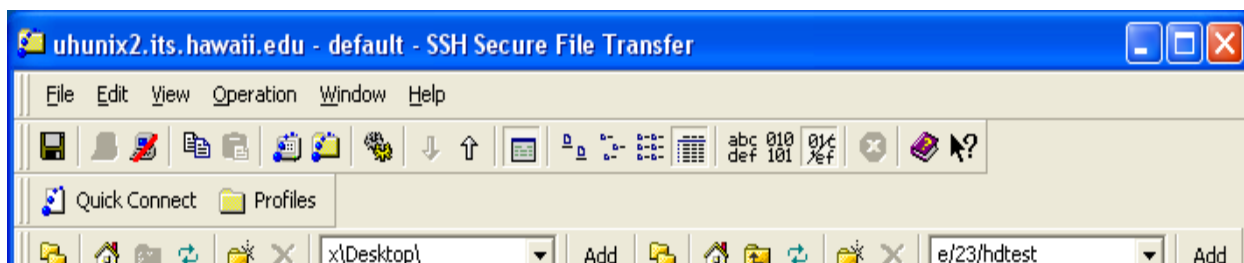
After you open the File Transfer Client and login to the remote machine, you will see a familiar graphical user interface, similar to the Microsoft Windows Explorer. The screen is split in half: the left pane shows the content of the local computer, while the right shows the content of the remote computer.

You can use it like Windows Explorer for most functions—you can delete, copy or rename files and folders on the remote machine the same way you do it in Windows Explorer.



SIMPLE UPLOADING AND DOWNLOADING

The File Transfer Client window has a toolbar with several buttons. If you are not certain what a button does, move the mouse over the button for a few seconds and a short description of the button will appear. It is good practice to familiarize yourself with the different functions of the program.



You can use the File Transfer Client the same way you move files in Windows Explorer. To upload files from the PC to the remote machine, first open the folder on the remote machine (left pane) to specify where to upload the files. Next open the folder that contains the files on your PC. To transfer the files, you can just “drag and drop” the files from the PC to the remote machine, just as if you were copying files between two folders in Windows Explorer.

To download files from the remote machine to your PC, you can follow the same procedure as above—just “drag and drop” files from the remote machine to you PC. This method can be used to transfer folders as well as individual files.

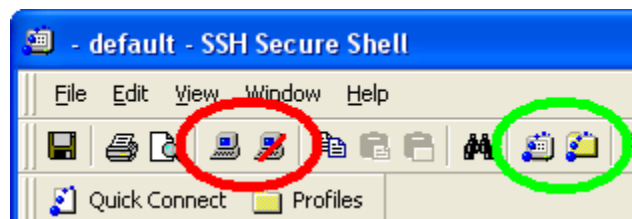
Important note: The program attempts to automatically detect whether the files should be transferred as *ASCII* or as *Binary*. When in doubt, the program transfers files as *ASCII*. If you want to force the program to transfer a file as either *ASCII*, click the **ASCII** button on the toolbar. (The toolbar is pictured above) If you want to force the program to transfer a file as *Binary*, click the **Binary** button on the toolbar. If you want the program to automatically determine whether the file should be transferred as *ASCII* or *Binary*, click the **AUTO** button on the toolbar.

Note that *ASCII* files are simple text files, while *Binary* files are usually executable files, or MS Office files formatted with MS Word, Excel, or Powerpoint.

There are a few small differences between the SSH File Transfer Client and the Windows Explorer:

1. On the remote machine, you can only delete empty folders, not folders that still contain files. Delete or move the files in the folder first before deleting the folder.
2. In Windows, you can paste the same file to a folder several times (and get new files name like “Copy of Resume.doc”.) With the File Transfer Client, file names are not changed during the paste operation on the remote machine. Be careful not to over-write a file you want to keep.

To end your file transfer session and disconnect from the remote machine, click the **Disconnect** button in the File Transfer Client toolbar (an icon of a PC with a slash through it). To open a transfer session again, click on the **Connect** button (an icon of a PC). The icons are circled in red in the picture below.



Note: The Shell Client and the File Transfer Client are very tightly integrated programs. You can open the File Transfer Client from within the Shell Client and vice versa by clicking the appropriate buttons on the toolbar (which look like the icons on the desktop, they are circled in green in picture above).

Un-Installing the SSH package

The SSH Security Shell can be uninstalled using the **Add / Remove Programs** control panel. Select: **Start --> Settings --> Control Panel --> Add/Remove Programs**. Select **SSH Secure Shell** and click **Change / Remove**. Then select **Remove** and click **Next**. SSH is now removed from your machine. Restart your PC to continue.

Getting more help with SSH

SSH has two very useful help resources. The first is the help program that comes with the SSH package. The second is the SSH World Wide Web site found at:

<http://www.ssh.com/products/security/secureshellwks/>

For additional assistance, please phone the ITS Help Desk at (808) 956-8883,
send email to help@hawaii.edu, or fax (808) 956-2108.
Neighbor islands may call the ITS Help Desk's toll-free phone number at (800) 558-2669.

Or see the ITS Help Desk home page at www.hawaii.edu/help
The ITS Help Desk is located in Keller 105 and Keller 213 on the UH Manoa Campus.

The University of Hawai'i is an equal opportunity/affirmative action institution.