University of Bristol Information Services

Uploading files to a web server using SSH Secure Shell 3.2.9

Practical workbook

Aims and Learning Objectives

By the end of this course you will be able to:

- Upload your documents (for example HTML files) from a local PC to your personal web space;
- Set the required access permission of these files.

Document information

Course files

This document and any associated practice files (if needed) are available on the web. To find these, go to www.bristol.ac.uk/is/learning/resources and in the **Keyword** box, type the document code given in brackets at the top of this page.

Related documentation

Other related documents are available from the web at:

http://www.bristol.ac.uk/is/learning/resources

Format conventions

The following format conventions are used in this document:

Computer input that you type is shown in a **`bold Courier font`**	**`http://www.bristol.ac.uk`**
Computer output, menu names and options, buttons, URLs are shown in a `Courier font`	`Save, Go to, Refresh`
Text that you must replace is shown in *italics*	Enter your *username*
Computer keys that you must press are in a **`bold Courier font`** and enclosed in angle brackets	**`<Enter>, <n>, <N>, </>`**
Instructions for users of other software versions are displayed in a boxed area.	Example text like this

Contents

Introduction

You are strongly recommended to use SSH Secure Shell Client for connecting interactively and for file transfer whenever possible, especially when connecting from outside the University.

The SSH Secure Shell Client program allows you to connect to systems that have implemented the appropriate server software using the protocol SSH which provides secure, encrypted communications across networks. You can also use SSH Secure Shell Client to transfer files securely to and from these systems.

Use of SSH ensures that your username and password cannot be "sniffed" and captured by malicious people while you are connecting to the remote system (a very common way for hackers to find out usernames and passwords that they can use to facilitate misuse of computers).

You can use SSH Secure Shell Client to connect to any of the centrally-administered Unix systems in the University and to an increasing number of departmental Unix systems.

To ensure full functionality, please upgrade to the latest version of the software: SSH Secure Shell Client 3.2.9 (ftp://ftp.bristol.ac.uk/pub/ibmpc/ssh/)

Prerequisites

This document assumes that you are familiar with the use of a computer keyboard and mouse, Microsoft Windows based products and the use of a web browser, such as Mozilla or Microsoft Internet Explorer.

Task 1 Publishing to the web (sftp)

Objectives To publish documents to the web.

Method You will use the SSH secure shell file transfer protocol.

Comments This task assumes that files will be stored on the staff interactive system seis.bris.ac.uk which provides a modest space (up to 30mb) for web pages.

An alternative method, using a system called Samba, is also available for members of the University using the central web server. See document **smb-i1** (Accessing files on the central Web server using Samba), at the URL in the **Related documents** section for further information.

1.1 Open SSH File Transfer Client. Assuming you are working in one of the IS training rooms, the path from the `Start` menu is `Programs` / `Telnet & FTP` / `Secure Shell File Transfer Client`.

For installations outside the Computer Centre training rooms, use the `SSH Secure Shell` menu rather than the `Network` menu (see Figure 1).

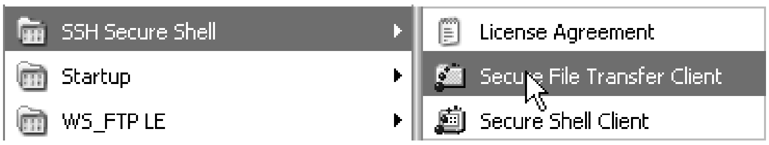


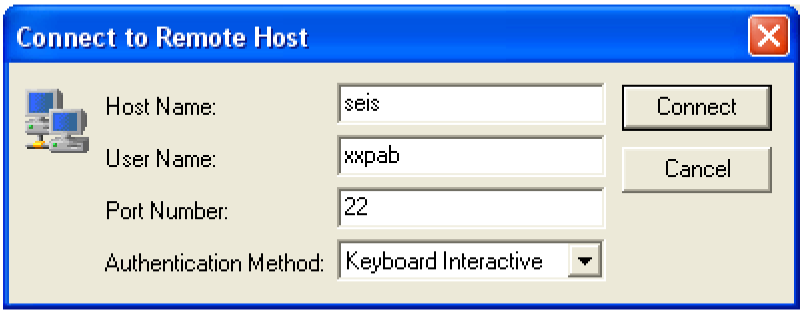
Figure 1 – opening the secure file transfer client

1.2 If a New Items dialog box appears, click on `Yes`.

1.3 Click on the Quick Connect menu button (alternatively, go to `File/Quick Connect`)

1.4 Fill in the `Connect to Remote Host` dialog box as follows:

- In the `Host Name` box, type in the name of the remote system you want to connect to (e.g. **`seis`**, **`info`** or other).
  If you connect from outside the University (from home for instance) you need to include the full path to the host name, for example: **`seis.bristol.ac.uk`** or **`info.bristol.ac.uk`**.
- In the `User Name` box, type in your username (i.e. the username you use to access your email account).
- Leave the `Port Number` box as it is (i.e. set to `22`).
- In the `Authentication Method` dropdown box, select `Keyboard Interactive` if connecting to `seis`, and `Password` if connecting to `info`.



Host Name: seis
User Name: xxpab
Port Number: 22
Authentication Method: Keyboard Interactive

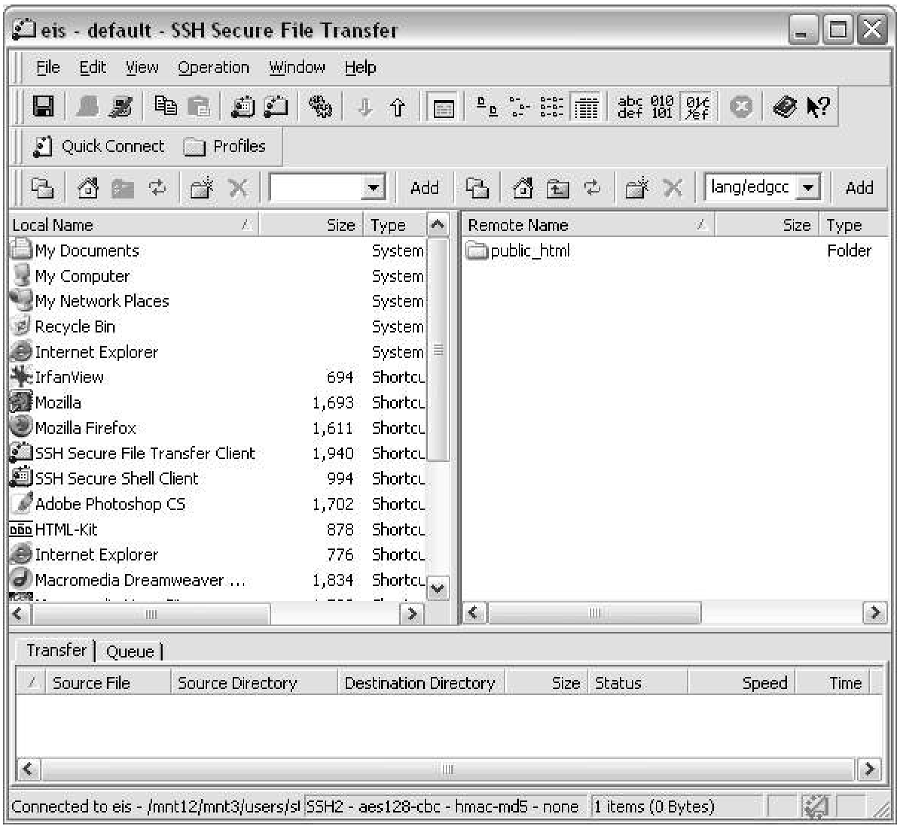
Figure 2 - connect to remote host dialog box

Note *Host Name:* _________________ (the name of the remote system you wish to connect to).
Username: _________________ (replace *xxpab* with your username for that system).

Click on `Connect`.

1.5 When prompted, type in your UOB / Kerberos `password` for that system and press **`<Enter>`**. You are now connected to the remote server (for example, `seis`, `info`, or other)

1.6 On the `interactive server`, personal web documents are published in a directory named `public_html`. Double-click on this folder (in the **right-hand** pane) to open it and display your web files and folders (they will appear in the right-hand pane). Unless you have already uploaded files, this will be empty.



Local Name	Size	Type
My Documents		System
My Computer		System
My Network Places		System
Recycle Bin		System
Internet Explorer		System
IrfanView	694	Shortcu
Mozilla	1,693	Shortcu
Mozilla Firefox	1,611	Shortcu
SSH Secure File Transfer Client	1,940	Shortcu
SSH Secure Shell Client	994	Shortcu
Adobe Photoshop CS	1,702	Shortcu
HTML-Kit	878	Shortcu
Internet Explorer	776	Shortcu
Macromedia Dreamweaver ...	1,834	Shortcu

Remote Name	Size	Type
public_html		Folder

Source File	Source Directory	Destination Directory	Size	Status	Speed	Time

Connected to eis - /mnt12/mnt3/users/sl SSH2 - aes128-cbc - hmac-md5 - none 1 items (0 Bytes)

Figure 3 - local and remote windows in SSH Secure File Transfer

1.7 Click the `Show/Hide Folder` icon to see where you are in the tree structure. A new pane will appear on the far right-hand side, showing the contents of your public_html folder. By default, this should be empty.

1.8 To upload your files from your local hard drive:

In the local (left-hand) panel, browse to the local folder containing the files you want to upload into your remote `public_html` directory.

Note Local folder: ____ (for example, `C:\User\WWW\` in the training rooms or A: if you saved your files on a floppy disk).

1.9 Select the files and/or folders you want to upload.

Note To select a group of files/folders, click on the first one, hold the **`<Shift>`** key and click on the last file/folder. Release the **`<Shift>`** key.
To select several non-consecutive files/folders, hold the **`<Ctrl>`** key and click on each of the files/folders you want to select. Release the **`<Ctrl>`** key.

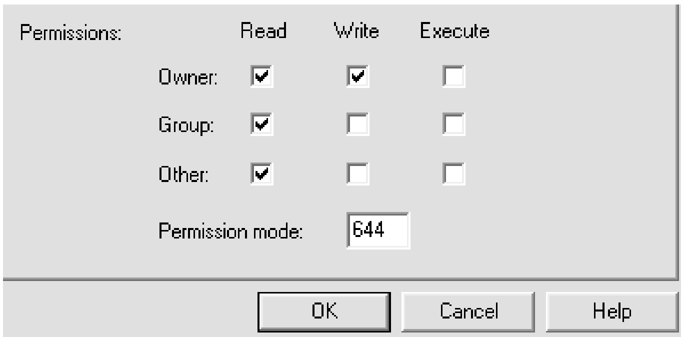
1.10 Drag them across and drop them into your `public_html` folder, in the right-hand pane.

Note There is another way to upload files in SSH Secure Shell 3.2. You can use the `Upload Dialog` window, which you open from the `Operation` menu (or its short cut icon ⇧ on the toolbar). A window representing your local hard drive (for example `C:`) will appear. As in the previous method, browse to the local folder containing the files you want to upload into your remote `public_html` directory, select the files and/or folders you want to upload and click on the `Upload` button in the lower right hand corner of the window.

1.11 Select all the files (not folders) in the `public_html` folder in the right-hand pane.

Using the right-mouse button, click and select `Properties` (you can also select `Properties` from the `Operation` menu).

Check that the permissions are set to **`644`** in the `Permission Mask` box (as in Figure 4). If not, use the tick boxes to select the correct permissions.



Permissions:	Read	Write	Execute
Owner:	☑	☑	□
Group:	☑	□	□
Other:	☑	□	□

Permission mode: 644

Figure 4 - file transfer properties (permissions)

Click on `OK`.

1.12 If you have uploaded any folders (e.g. images), select them one by one and set their permissions to **`755`** rather than `644` (i.e. give `Execute` permissions to all – `Owner`, `Group` and `Other`).

Don't forget then to set the permissions of the files within these folders to `644`.

Note To help understand the file permissions, try to remember that **Read=4**, **Write=2** and **execute=1**. As the owner of a file, the permission 6 is derived from adding Read and Write together (i.e. 4 + 2 = 6). To make folders executable, simply add 1 to the value assigned to each party (see task 1.11)

If others (defined in Unix terms as a **Group**) have been given password protected access to the files, the file permissions should be set to **664** and folders to **775** This is only appropriate for shared departmental pages.

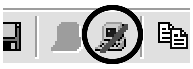
1.13 Switch to a web browser and view the documents you have just published.

For example, enter the URL `http://seis.bristol.ac.uk/~`*`xxpab`*`/` (replacing *xxpab* with your username).

Note You will also need to include the name of the document you wish to display if you have not created an index file (for example `index.html` or `welcome.html`).

Course document: ____
(if you are using these notes as part of a structured course).

1.14 To logout:

From the `File` menu, select `Disconnect`, or click on the  icon.

Click on `Yes` to confirm this action.

Go to `File/Exit` to close the `SSH Secure File Transfer` window (alternatively press **`<F4>`** or click on the ☒ icon in the top right corner).

Note To log into the University's Central Web Server, log in as per tasks 1.1 – 1.7. From the `Operation` menu select `Go to Folder`. A dialogue box will appear; add the following address: `/info/www/Depts/`*`yourdept`*`/` replacing *yourdept* with the top-level folder name of your department or unit. The far right-hand pane will show the next level of subfolders. Double-clicking a subfolder will display its contents.