

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	<code>http://www.bristol.ac.uk</code>
Computer output, menu names and options, buttons, URLs are shown in a <code>Courier font</code>	<code>Save, Go to, Refresh</code>
Text that you must replace is shown in <i>italics</i>	Enter your <i>username</i>
Computer keys that you must press are in a bold Courier font and enclosed in angle brackets	<code><Enter></code> , <code><n></code> , <code><N></code> , <code></></code>
Instructions for users of other software versions are displayed in a boxed area.	<div style="border: 1px solid black; padding: 2px; display: inline-block;">Example text like this</div>

Contents

Format conventions

Related documentation

Task 1 Publishing to the web (sftp).....1

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.

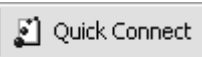
An alternative method, using a system called Samba, is also available for members of the University using the central web server. See document **smb-11** (Accessing files on the central Web server using Samba), at the URL in the **Related documents** section for further information.

-
- 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.

[Click here to download full PDF material](#)