

SFTP for DMA downloads

Important information for those subscribers who currently download the tps, ctps, mps, bmps or fps files via ftp.

What's Happening?

The ftp server for the DMA file downloads is being replaced with a more secure sftp server. The sftp server uses the SSH2 protocol which encrypts all information transferred between the server and client.

When is it Happening?

The sftp service is running now to allow changeover for current subscribers from ftp to sftp and time to test and implement the new protocol up to the previously mentioned January 16th changeover date. The existing ftp server will continue to run up to this date and for at least the first month from this date to allow subscribers to continue to download the files whilst testing and implementing any new sftp clients.

What will I need?

Using sftp is very similar to ftp, you just require a sftp client.

The important thing is that the client must support sftp using the SSH2 protocol. Some clients only use the older (and less secure) SSH1 protocol, the server used for the DMA file downloads does **not** support SSH1.

Which client to use depends on how you currently download via ftp whether manually via a client with a graphical user interface, manually via a command line interface or automatically in a batch file. The operating system used also determines which client can be used.

The server uses the default port for SSH which is port 22. Subscribers may have to arrange their Firewalls to allow this port to be used.

There are many sftp clients available both freeware and commercial, with a Graphical User Interface (GUI) or a command line interface (console). A list is given below.

List of SFTP clients

Open Source

- [Cyber duck](#) (OS X, GUI)
- [FileZilla](#) (Windows, GUI)
- [Fugu](#) (OS X, GUI)
- [gFTP](#) (portable, console and GUI)
- [OpenSSH](#) (portable, console)
- [Putty PSFTP](#) (portable, console)
- [WinSCP](#) (Windows, GUI and console)
- [Yafc](#) (portable, console)
- [Perl](#) (portable, console)

Proprietary

- [Bitwise Tunnelier](#) (Windows, GUI and console) free for individual use
- [Captain FTP](#) (Mac OS X, GUI and automation)
- [Commander FTP](#)
- [CoreFTP](#)
- [CuteFTP](#)
- [Fetch](#) (Mac OS X, GUI)
- [FastTrackFTP](#)
- [FTP Voyager Secure](#)
- [Interarchy](#) (Mac OS X, GUI)
- [Pragma FortressSSH](#) (Windows and PDAs, GUI and console)
- [Private Shell](#) (Windows, GUI and console)
- [RBrowser](#) (Mac OS X, GUI)
- [Servant Salamander](#) (Windows, GUI)
- [SFTPPlus](#) (Multiplatform)
- [SftpDrive](#) (Windows, maps drive letter to SFTP)
- [SmartFTP](#)
- [SSH Tectia](#) (Multiplatform)
- [Transmit](#) (Mac OS X, GUI)
- [WebDrive](#) (Windows, maps drive letter to SFTP)
- [WS FTP Pro](#)

Connecting for the first time

The first time you connect via sftp, the server sends the following encryption key to the client.

```
bc:40:a8:ac:8f:8b:dd:04:97:97:05:b3:a4:9f:49:2b
```

The client will ask if you wish to accept this key, after which it will remember this key for the DMA sftp site.

Important: If you are intending to use the sftp client from a automated batch job, you will need to go through the above authentication routine first before running the batch job, otherwise the batch job may hang waiting for confirmation of acceptance of the key. Therefore the user should manually invoke the sftp client first, log on and accept the key.

SFTP in Batch Mode

Many subscribers automate their ftp downloads using a batch file job. The clients mentioned above marked 'console' allow for automatic batch processing of scripts. However, there are some issues regarding password authentication in sftp mode. Some command-line clients (e.g. puTTY, winSCP and Tunellier) allow the username and password to be entered as command line arguments.

Unix systems

Most systems based on Unix have an sftp client installed based on the openSSH standard. Details are contained in the 'man sftp' page. It can be used interactively or in conjunction with a batchfile containing the commands to download the required files.

OpenSSH, however, requires a ‘non-interactive authentication’ method if used with the batchmode option set in the config file. This can cause problems when the server asks for the users password.

The solution to this is to use an alternative client (e.g. puTTY) which allows password authentication in batch mode, or, it can be arranged to use authentication using a client generated private-public key pair.

To generate a public-private key pair in openSSH the ssh-keygen program is used. Full details are contained in the Unix documentation for ssh-keygen.

Note, the key generated must be either rsa or dsa type 2 not rsa type 1

Use ssh-keygen -trsa, or ssh-keygen =tdsa

The public key that is generated needs to be set up on our server while the private key remains on the client machine. The generated public key should be emailed as an attachment to TPS-HelpDesk@gb.co.uk together with your username and it will be set up. You will then be informed when it is ready so you can test the authentication.

Before trying the authentication in batchmode refer to the **connecting for the first time** section above.

To use sftp using key based authentication requires the ‘batchmode=yes’ option and the ‘identityfile’ option to point to the private key file. These can be passed as either command line arguments or set in the ssh_config file. The Unix documentation on sftp, ssh-keygen and ssh_config give full details.

FTP-SFTP Bridge

The Bitvise Tunnelier product (<http://www.bitvise.com>) (which is free for up to four users in a single environment) comes with an FTP-SFTP bridge. This allows ftp clients to access the sftp server by translating from one protocol to the other. A connection is defined between the client and the sftp server to provide the sftp connection but the software listens for *ftp* connections on the machine on which it is running. Therefore ftp clients can connect to this machine which then translates the ftp protocol to sftp and relays the commands to our server. Any current ftp software just needs to connect to the machine running the FTP-SFTP bridge.

Any Other Questions?

Contact

TPS-HelpDesk@gb.co.uk

0870 036 1204