

# **SFTP*Plus***

Version 1.1

Mike Protts

mikep@proatria.com

Pro:Atria Ltd,

The Old Exchange,

South Cadbury,

Yeovil,

Somerset,

BA22 7ET UK

Tel: +44 (0)1963 441311

Fax: +44 (0)1963 441312

sales@proatria.com

technicalsupport@proatria.com

<http://www.proatria.com>

February 23, 2006

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	Copyright . . . . .	1
1.2	Trademarks . . . . .	1
1.3	Notices . . . . .	2
1.4	Licensing . . . . .	2
<b>2</b>	<b>Installation</b>	<b>3</b>
2.1	Pre-installation notes . . . . .	3
2.1.1	Windows . . . . .	3
2.2	Installation . . . . .	3
<b>3</b>	<b>Configuration</b>	<b>4</b>
3.1	Database Configuration . . . . .	4
3.1.1	Starting the database . . . . .	4
3.2	http server configuration . . . . .	5
3.2.1	Configuring IIS - optional . . . . .	5
3.2.2	Starting the http server . . . . .	5
3.3	sftp server configuration . . . . .	5
3.3.1	Locally authenticated users . . . . .	6
3.3.2	SFTPPlus authenticated users . . . . .	6
3.3.3	Starting the sftp server . . . . .	6
3.4	ftp server configuration . . . . .	6
3.4.1	Starting the ftp server . . . . .	6
<b>4</b>	<b>Administration</b>	<b>7</b>
4.1	Adding servers . . . . .	7
4.2	Adding users . . . . .	7
4.2.1	Create home directory . . . . .	7
4.3	HTTP transfers . . . . .	8

---

4.3.1	Example scenario . . . . .	8
<b>5</b>	<b>Messages</b>	<b>9</b>
5.1	Message routing . . . . .	9
5.2	Messages . . . . .	9

# Chapter 1

## Introduction

SFTPPlus server - a tool for secure file transfers

SFTPPlus server utilises open standards to implement secure file transfer with controls and audit suitable for the enterprise.

SFTPPlus includes an openssh server with modifications for authentication and audit, and additionally we provide Apache and mysql as packaged by the Xampp project.

The web interface provides a single point of administration, authentication and audit for multiple transfer servers, including sftp, http and ftp transfer. The benefits of this include being able to provide sftp access without giving a native OS userid and password, and maintaining the audit trail to see what files have been transferred.

As all protocols are standards based, any client may be chosen.

### 1.1 Copyright

This product is Copyright (C) Pro:Atria Ltd 2005. ALL RIGHTS RESERVED.

Portions of this product are copyright as follows

Regina Copyright (C) 1992-1994 Anders Christensen

PuTTY is copyright 1997-2005 Simon Tatham

Regutils Copyright (c) 1998, 2001 Patrick TJ McPhee

md5sum Copyright (C) 2002 Free Software Foundation, Inc.

openssl \*\*\* TODO openssh \*\*\* TODO cygwin \*\*\* TODO curl \*\*\* TODO apache \*\*\* TODO mysql \*\*\*  
TODO

Please contact Pro:Atria Ltd for the further details.

### 1.2 Trademarks

All products and company names mentioned herein are the marks of their respective owners, including but not limited to PuTTY, Regina, HP, IBM, Intel, Linux, Microsoft, Solaris, Sun, Tivoli, Netview, UNIX and Windows. \*\*\* TODO

## 1.3 Notices

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)

The software is supplied with full source code available, and may be modified as required. Pro:Atria Ltd fully supports the original software and approved modifications, according to the license agreement. Any modification that has not been approved by Pro:Atria Ltd will be supported on a best effort basis.

## 1.4 Licensing

SFTPPlus is licensed for use according to this documentation, in conjunction with the license agreement.

## Chapter 2

# Installation

### 2.1 Pre-installation notes

SFTPPlus is supplied as a zip file which will be unpacked into a single directory. There are no changes to any system directories.

#### 2.1.1 Windows

SFTPPlus is also provided as an install package. SFTPPlus does have to make some registry changes:

1. Uninstall entries
2. Installing as a service
3. Event log definitions
4. Entries made by the putty program

To run the service, the user that will run the SFTPPlus services must have 'Log on as a service' right. The installation of Apache, mysql and openssh will assign the appropriate rights.

### 2.2 Installation

Unzip SFTPPlus.zip into a suitable directory, eg c:\SFTPPLUS (Windows) or /usr/local/SFTPPlus(Linux/Unix). The files must be accessible to the user that will run the SFTPPlus service.

The windows installer default directory is c:\SFTPPLUS

Once the files have been installed, then the product must be configured for use.

# Chapter 3

## Configuration

There are a number of items that need to be configured.

1. Client (optional - see client documentation)
2. database
3. http server
4. sftp server
5. ftp server

### 3.1 Database Configuration

A mysql database for authentication and audit is provided in a pre-initialised form. If you are using this database then you can start the database with no further configuration. If the database will be on a different machine to the web server, then the database permissions and connection information will have to be changed.

If you are planning to use an existing database, then the sql statements for initialising are contained in the SFTPPlus/admin/htdocs/SFTPPlusDatabase.sql file. This can be changed to suit site requirements.

The supplied database has a root password set as SFTPPlus - this should be changed.

The sql file has the passwords for the required users, the grant statements need to be changed as appropriate.

The files auditdb.php, usersdb.php and admindb.php (in the SFTPPlus/admin/htdocs/ directory) need to be updated for the correct database.

If you are using a non-standard port for the database then this also needs to be changed in the config files.

#### 3.1.1 Starting the database

If you are using the supplied database, then the mysql server needs to be started.

For Windows mysql will first be installed as a service, then the service started. The service is installed and started by clicking start/all programs/SFTPPlus/database/Install Service.

For UNIX and Linux, the mysql server is started with SFTPPlus/admin/mysql/bin/mysqld, or as a daemon as normal.

## 3.2 http server configuration

You can use any http server that supports php, or the supplied apache can be used.

If you wish to use the supplied apache server and you already have an existing http server on this machine, you will need to change the ports used for SFTPPlus.

The http server is configured using the files http.conf and ssl.conf in the SFTPPlus/admin/apache directory. The supplied configuration is set to use the standard ports 80 for http and 443 for https. These can be changed as required. For example, the http port might be changed from 80 to 18080, and the ssl port from 443 to 18443. To change these, edit http.conf and change all occurrences of 80 to the chosen value, then edit ssl.conf and change all occurrences of 443 to the chosen value.

### 3.2.1 Configuring IIS - optional

If you prefer to use IIS as a web server, then it needs to be configured for PHP. The directory SFTPPlus\admin\htdocs\SFTPPlus should be configured as virtual directory /SFTPPlus.

1. Enable php (depends on version - may not be needed) In IIS admin add new web service extension php with required file: c:\SFTPPlus\admin\php\php5isapi.dll and set as allowed.
2. Map .php extension (this will be global - if only for SFTPPlus you can perform this after step 3 for the SFTPPlus virtual directory) Right click on Default web site (or SFTPPlus directory) Select home directory Click configuration Add .php with executable c:\SFTPPlus\admin\php\php5isapi.dll
3. Add new virtual directory for SFTPPlus using c:\SFTPPlus\admin\htdocs\SFTPPlus
4. Add c:\sftpplus\admin\php and c:\sftpplus\admin\php\ext to the PATH variable (may need server restart - IIS seems reluctant to pick this up!) \*\*\* Note that if a dll is not found the message will be popped up on the console - you may have to use mstsc /console option to clear it \*\*\* . An alternative is to copy the dll's from the php \nd php\ext directory to system32.
5. Allow read/write/execute access for Internet Guest Account to c:\sftpplus\admin\tmp
6. copy php\php.ini to c:\windows
7. Restart IIS

### 3.2.2 Starting the http server

If you are using the supplied apache server, it's service can be installed and started from the start menu: start/all programs/SFTPPlus/web/Install Service

## 3.3 sftp server configuration

The sftp server has some extra steps for Windows installations. This allows the mapping of UNIX style files and paths to the Windows filesystem.

The installation is slightly different depending on the version of Windows - for Windows 2003 the service has to be run as a Windows account, whereas Windows XP, NT and 2000 can use the Local System account. There is also a separate account created for 'privilege separation' - which ensures that a low privilege account can be used.

To setup the sshd configuration, use the start menu option: start/all programs/SFTPPlus/sftp server/Install Service. This will prompt you for required information. The service will not start at this point - to allow for further configuration.

Now the sftp service needs to be configured for authentication - if you are running the web server on the local system with port 80, then there is no further configuration required, but if not the SFTPPlusAuthentication parameter in SFTPPlus/server/etc/sshd\_config will need updating. Then the service can be started from the start menu with start/all programs/SFTPPlus/sftp server/Start Service

### 3.3.1 Locally authenticated users

To be used by standard users, with authentication to the OS, users must exist in /etc/passwd (or SFTPPlus\server\etc\passwd for Windows).

For Windows users, the users can be added using the mkpasswd command as follows:

1. open a command prompt (start/run/cmd)
2. change directory to sftpplus\server
3. issue the command bin\mkpasswd -l -uUSERID » etc\passwd
4. edit the file etc\passwd
5. change the end of the last line from /bin/bash to /bin/sh
6. create the home directory for the user SFTPPlus\client\inbox\USERID

### 3.3.2 SFTPPlus authenticated users

To allow sftpplus authentication, a user alias is used - this is a standard account on the operating system which is used to restrict access to the filesystem. This account will not be used directly. The windows installation will create an account 'sftpuser' automatically. For UNIX and Linux an account will need to be created, although it does not need to be able to logon.

More information on users is in the administration chapter.

### 3.3.3 Starting the sftp server

The service can be started from the start menu with start/all programs/SFTPPlus/sftp server/Start Service

## 3.4 ftp server configuration

### 3.4.1 Starting the ftp server

## Chapter 4

# Administration

The administration system is accessed via a web browser `http://HOSTNAME/SFTPPlus` or `http://HOSTNAME:PORT/SFTPPlus`, eg if using the local machine with the http server port set to 18080, use `http://localhost:18080/SFTPPlus`. The administration userid and password can be set in the `SFTPPlusDatabase.sql` file, or if the database is used as provided, you can logon with userid mike, password=password.

### 4.1 Adding servers

Click on the servers link and you will see a list of servers - there are a couple of examples which can be deleted later. Click on NEW to add the server - this should be identified by it's hostname.

Each server can be enabled for sftp, http, https, ftp and ftps transfers. Additionally the authentication can be based on native os or sftpplus authentication, and for sftp the use of public/private key or passwords.

Also the users who can access the server can be selected from the list.

### 4.2 Adding users

Now you can add users. For initial testing there are already some users set up. The user test has a password whatever, and the user anotheruser has a password ahem. To enable use of these for sftp you need to select the sftp checkbox, use sftpuser as alias, use /home/test as the home directory and select the server(s) that you will be using.

Each server can be enabled for sftp, http, https, ftp and ftps transfers. Additionally the authentication can be based on native os or sftpplus authentication, and for sftp the use of public/private key or passwords.

Also the servers that the user can access can be selected from the list.

The user and server access must match, eg both the user and the server must have http selected to allow http access.

#### 4.2.1 Create home directory

You will need to create the home directory for the user - please note that the home directory must belong to the alias account.

For Windows, the home directory will be created under `SFTPPlus\client\inbox\`

eg if the SFTPPlus userid is usera and then the home directory would be `c:\SFTPPlus\client\inbox\usera`, but the owner would be `sftpuser`.

You can create the home directory using the Explore link, as described in the next section.

## 4.3 HTTP transfers

The http transfer facility allows users to transfer files using http and https. This uses standard browser facilities. From the administrative panels the screens can be accessed by clicking on the Explore link. A transfer user will only see their own home directory, whereas an administrative user can see them all.

For transfer user access, the url is `http://SERVER/SFTPPlus/explore`

The transfer browser interface is designed to be straightforward to use for anyone familiar with a browser.

### 4.3.1 Example scenario

- 1.

## Chapter 5

# Messages

The messages issued by SFTPPlus are listed here as a convenience. Please note that the file message.conf contains the most up to date set of messages.

### 5.1 Message routing

**\*\*TODO\*\***

### 5.2 Messages

- – MessageId - 0
  - Severity - I
  - Text -
  - Help - Messages issued before processing the global.conf file
  
- – MessageId - 1
  - Severity - I
  - Text - Configuration read, startup continues
  - Help - The global.conf file has been processed and startup continues
  
- – MessageId - 2
  - Severity - S
  - Text - Unable to find conf files
  - Help - SFTPPlus has failed to find the required configuration files. Consult message.log and check the runtime path. This may also indicate a problem with semaphore locking.
  
- – MessageId - 3
  - Severity - E

- Text - STDERR
  - Help - Error output from a command issued.
- - MessageId - 4
  - Severity - I
  - Text - STDOUT
  - Help - Output from a command issued
- - MessageId - 5
  - Severity - I
  - Text - Config file
  - Help - Configuration file is being read
- - MessageId - 6
  - Severity - I
  - Text - Setting:
  - Help - Setting from a configuration file
- - MessageId - 7
  - Severity - E
  - Text - Definition | disabled - ignoring
  - Help - The definition is specifically disabled in the configuration file. The definition should be removed if not needed. It can be left as disabled if it may be required in future.
- - MessageId - 8
  - Severity - E
  - Text - Unable to scan | - ignoring
  - Help - A defined directory was not able to be scanned. Check the directory exists and is accessible to the SFTPPlus service
- - MessageId - 9
  - Severity - E
  - Text - command was
  - Help - Command used to test a directory
- - MessageId - 10
  - Severity - I
  - Text - Adding | to monitoring list

- Help - The definition listed has been added to the list of active definitions
  
- - MessageId - 11
  - Severity - E
  - Text - Missing subdir parameter in |, ignoring
  - Help - A definition has no subdir parameter. Add the correct subdir parameter to the definition. This must point to a sub-directory of inbox
  
- - MessageId - 12
  - Severity - I
  - Text - Using server | for
  - Help - The server specified for a transfer
  
- - MessageId - 13
  - Severity - E
  - Text - Missing server parameter |, ignoring
  - Help - No server was specified for a transfer - the target server must be specified
  
- - MessageId - 14
  - Severity - I
  - Text - Using port | for
  - Help - The port specified for a transfer
  
- - MessageId - 15
  - Severity - I
  - Text - Using port 22 for
  - Help - Using the default port (22) for sftp
  
- - MessageId - 16
  - Severity - I
  - Text - Using user | for
  - Help - The user specified for the remote system for a transfer
  
- - MessageId - 17
  - Severity - E
  - Text - Missing user parameter
  - Help - A userid must be specified for the target system
  
- - MessageId - 18

- Severity - I
  - Text - Using password provided for
  - Help - The password provided will be used.
- - MessageId - 19
  - Severity - E
  - Text - Missing password parameter
  - Help - No password has been provided for the remote system. This must be the password for the specified user on the remote system.
- - MessageId - 20
  - Severity - I
  - Text - Using saved profile | for
  - Help - The specified PuTTY profile will be used.
- - MessageId - 21
  - Severity - E
  - Text - Missing savedprofile parameter
  - Help - No PuTTY profile has been specified. The profile will be created by using the putty.exe gui, and saving a connection definition
- - MessageId - 22
  - Severity - I
  - Text - Using target directory | for
  - Help - The remote directory where transferred files will be placed.
- - MessageId - 23
  - Severity - E
  - Text - Missing targetdir parameter
  - Help - A remote directory must be specified for storing transferred files.
- - MessageId - 24
  - Severity - I
  - Text - Using response file | for
  - Help - A response file as specified will be retrieved after a transfer
- - MessageId - 25
  - Severity - E
  - Text - Missing responsein parameter

- Help - A response file name must be specified. This can include %FNAME% and %FTYPE% for filename and type
  
- - MessageId - 26
  - Severity - I
  - Text - Using response directory | for
  - Help - The response file will be retrieved from the specified remote directory.
  
- - MessageId - 27
  - Severity - E
  - Text - Missing respondedir parameter
  - Help - A remote directory where the response file will be found must be specified.
  
- - MessageId - 28
  - Severity - I
  - Text - Using maxtry | for
  - Help - The maximum times a transfer will be attempted before considering as a permanent failure
  
- - MessageId - 29
  - Severity - I
  - Text - Using global maxtry | for
  - Help - Using the global maxtry value for this transfer
  
- - MessageId - 30
  - Severity - I
  - Text - Using waittime | for
  - Help - The time between transfer attempts in seconds
  
- - MessageId - 31
  - Severity - I
  - Text - Using global waittime | for
  - Help - Using the global waittime for this transfer.
  
- - MessageId - 32
  - Severity - I
  - Text - Using initialwait | for
  - Help - The initial wait time before attempting to retrieve a response file. This is intended to allow for processing time between sending a file and the output being created remotely.

- – MessageId - 33
  - Severity - I
  - Text - Using global initialwait | for
  - Help - The global initial waittime will be used for this transfer
  
- – MessageId - 34
  - Severity - I
  - Text - looking for files
  - Help - SFTPPlus is starting a directory scan
  
- – MessageId - 35
  - Severity - I
  - Text - Checking
  - Help - SFTPPlus is checking for files for the specified transfer
  
- – MessageId - 36
  - Severity - E
  - Text - Unable to scan directory
  - Help - SFTPPlus has failed to scan a directory - please check following messages for details
  
- – MessageId - 37
  - Severity - I
  - Text - pausing
  - Help - SFTPPlus is waiting for further files.
  
- – MessageId - 38
  - Severity - S
  - Text - sleep interrupted
  - Help - SFTPPlus has received a signal and will shut down
  
- – MessageId - 39
  - Severity - S
  - Text - unreachable code
  - Help - Debugging information. If this message appears, please contact Technical Support
  
- – MessageId - 40
  - Severity - I
  - Text - Checking file size

- Help - Checking the size of a file before transfer, to ensure that it is not still being written to
- - MessageId - 41
  - Severity - I
  - Text - filesize | bytes
  - Help - Report on the size of a file to be transferred
- - MessageId - 42
  - Severity - I
  - Text - creating checksum
  - Help - The md5sum hash of the file is being created
- - MessageId - 43
  - Severity - I
  - Text - Sending file
  - Help - The file is being sent
- - MessageId - 44
  - Severity - I
  - Text - psftp returned
  - Help - Return code from psftp
- - MessageId - 45
  - Severity - E
  - Text - Secure ftp error - please see
  - Help - An error has occurred in a transfer, and the indicated file will include more information
- - MessageId - 46
  - Severity - I
  - Text - File sent OK.
  - Help - A transfer has completed
- - MessageId - 47
  - Severity - I
  - Text - Adding response to queue
  - Help - A response file will be retrieved at the appropriate time
- - MessageId - 48
  - Severity - I

- Text - Checking for response file for
  - Help - An attempt to retrieve a response file is in progress
- - MessageId - 49
  - Severity - W
  - Text - Failed to obtain response for
  - Help - A response file has not been retrieved. This may indicate insufficient waittime
- - MessageId - 50
  - Severity - I
  - Text - Waiting | for response file for |, | attempts left
  - Help - Information about the number of retries
- - MessageId - 51
  - Severity - I
  - Text - Response file | for | transfer is available
  - Help - A response file has been retrieved successfully
- - MessageId - 52
  - Severity - W
  - Text - File Transfer message:
  - Help - Report from a file transfer session
- - MessageId - 53
  - Severity - I
  - Text - Processing file | as
  - Help - The original filename has had a timestamp added for uniqueness
- - MessageId - 54
  - Severity - I
  - Text - Response received ok
  - Help - A response file has been received
- - MessageId - 55
  - Severity - I
  - Text - Preparing to send for
  - Help - A file is being prepared for transfer
- - MessageId - 56

- Severity - I
  - Text - Waiting | to send file for |, | attempts left
  - Help - Report on the number of retries for sending a file
- - MessageId - 57
  - Severity - I
  - Text - Adding response to queue for
  - Help - A response file transfer will be queued for later retrieval
- - MessageId - 58
  - Severity - E
  - Text - Failed to send file for
  - Help - A transfer has failed - see following messages
- - MessageId - 59
  - Severity - E
  - Text - Type | not supported, ignoring
  - Help - An invalid transfer type has been specified, the transfer definition will not be used
- - MessageId - 60
  - Severity - E
  - Text - Missing type parameter |, ignoring
  - Help - No transfer type has been specified - the transfer definition will not be used
- - MessageId - 61
  - Severity - I
  - Text - Transfer type | for
  - Help - The specified transfer type will be used
- - MessageId - 62
  - Severity - I
  - Text - md5sum will be sent for
  - Help - The transfer will also include the md5sum file
- - MessageId - 63
  - Severity - I
  - Text - md5sum will not be sent for
  - Help - The transfer will not include the md5sum file

- – MessageId - 64
  - Severity - I
  - Text - preprocess command for | is:
  - Help - The specified command will run before a transfer
  
- – MessageId - 65
  - Severity - I
  - Text - no preprocess command for
  - Help - There is no preprocess for a transfer
  
- – MessageId - 66
  - Severity - I
  - Text - postprocess | command for | is:
  - Help - The specified command will run after a transfer
  
- – MessageId - 67
  - Severity - I
  - Text - no postprocess | command for
  - Help - There is no postprocess for a transfer
  
- – MessageId - 68
  - Severity - I
  - Text - Running | command for | ,
  - Help - The specified command is being run
  
- – MessageId - 69
  - Severity - I
  - Text - Command for | rc 0
  - Help - The command had a return code of 0 (usually good)
  
- – MessageId - 70
  - Severity - W
  - Text - Command for | rc
  - Help - The command had a return other than 0 (usually bad)
  
- – MessageId - 71
  - Severity - I
  - Text - Command for | stdout

- Help - The output for a command
- - MessageId - 72
  - Severity - W
  - Text - Command for | stderr
  - Help - The error messages for a command
- - MessageId - 73
  - Severity - S
  - Text - Program interrupted, shutting down
  - Help - An interrupt signal was received
- - MessageId - 74
  - Severity - S
  - Text - SMTP Socket problem
  - Help - A problem has occurred with a socket command for SMTP messaging. SMTP will be disabled
- - MessageId - 75
  - Severity - W
  - Text - File still changing, postponing
  - Help - A file in an inbox directory is still being updated, it will be retried later
- - MessageId - 76
  - Severity - I
  - Text - Email messages for | will be sent to
  - Help - The specified email address will receive messages related to this transfer
- - MessageId - 77
  - Severity - I
  - Text - Email messages for | will be sent to default
  - Help - The default global email address will receive messages related to this transfer
- - MessageId - 78
  - Severity - S
  - Text - Failure writing file
  - Help - A problem has occurred writing to a file. SFTPPlus will terminate
- - MessageId - 79

- Severity - S
  - Text - Failure reading file
  - Help - A problem has occurred reading from a file. SFTPPlus will terminate
  
- - MessageId - 80
  - Severity - I
  - Text - md5sum will not be created for
  - Help - No md5sum will be created for the transfer. This will reduce CPU load, but prevents use of the md5sum in the audit
  
- - MessageId - 81
  - Severity - I
  - Text - Timestamp will not be used in the target filename
  - Help - The target file name will not include the timestamp. This means that SFTPPlus will not be able to guarantee that files will not be overwritten
  
- - MessageId - 82
  - Severity - I
  - Text - Timestamp will not be used in the local response filename
  - Help - The local response file name will not include the timestamp. This means that SFTPPlus will not be able to guarantee that files will not be overwritten
  
- - MessageId - 83
  - Severity - I
  - Text - Using remote directory | for
  - Help - The remote directory where transfer files will be pulled from.
  
- - MessageId - 84
  - Severity - E
  - Text - Missing remotedir parameter
  - Help - A remote directory must be specified for pulling transfer files.
  
- - MessageId - 85
  - Severity - I
  - Text - Using filename | for
  - Help - The remote filename that will be pulled.
  
- - MessageId - 86
  - Severity - E

- Text - Missing filename parameter
  - Help - A remote filename must be specified for pulling.
- - MessageId - 87
  - Severity - I
  - Text - Using starttime | for
  - Help - The starttime for pulling the file