Ftp Schedular Pro User Interface
Revised 12th May 2007

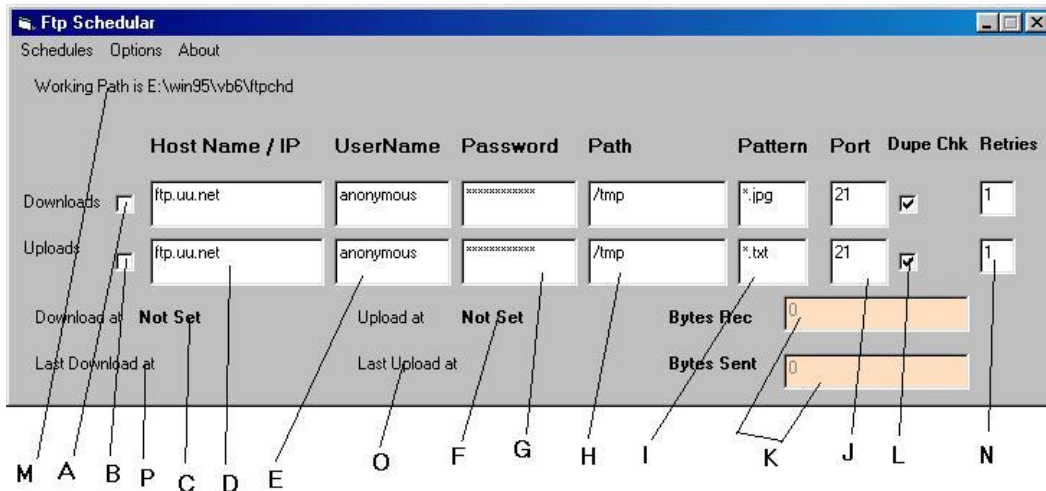**Topic**   **Page**

Standard Version

Fig I
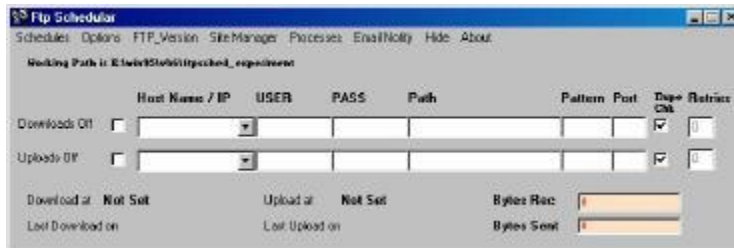
A – Activate Timer for DownLoader
B – Activate Timer for Uploader
C – Status and Time of Schedule for Download
D- Ftp Server Name / IP
E – UserName
F - Status and Time of Schedule for Upload
G – Password (Hidden)
H – Path on Ftp Server
I – Wildcard Pattern to list to Upload
J – Port of Ftp Server
K – Bytes being Sent
L – Checking to ensure no duplicate files are uploaded
  (By Name, See other menu options to include Size check)
M – Change path where files are to be stored or sent from
N – Number of retries to attempt if a transfer failed
O- Last date an upload ftp transfer was transacted/attempted schedule
P- Last date an download ftp transfer was transacted/attempted schedule

Pro Version

The following pages will illustrate the features of the Professional version of the FTP Client.

PRO Form View

Standard Form View

Above shows the before and after Menu layout when you toggle between the Standard and Pro versions.

Each site entered (Download/Upload) can be configured separately with respect to the following key areas:
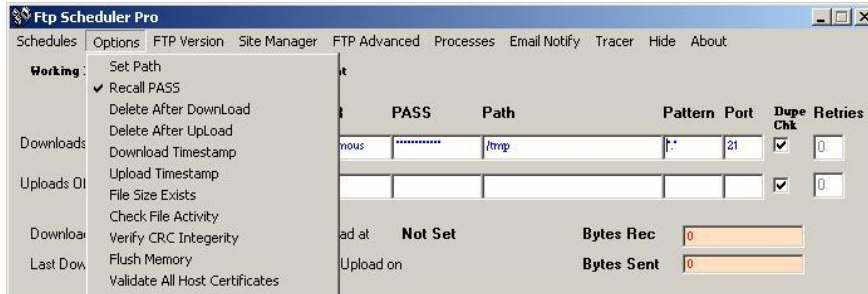
- ❑ Time
- ❑ FXP On/Off
- ❑ Security On/Off
- ❑ Process Launcher On/Off

Key features to be illustrated are as follows:

- ➤ **FXP**

- ➤ **Secure FTP**
    - o **Private/Public Key**
    - o **Certificate**

- ➤ **Shell Processes**

- ➤ **Email Configuration**

- ➤ **File Analysis**
    - o **Spider Search**

- ➤ **Registered Version**

FXP

The FXP works on the principal of launching the FTP site set for download. The scheduling then traverses through all the Upload sites to determine which of those sites have been set for FXP. The files matching the wildcard pattern in the Download site configuration are transferred to the Upload sites.
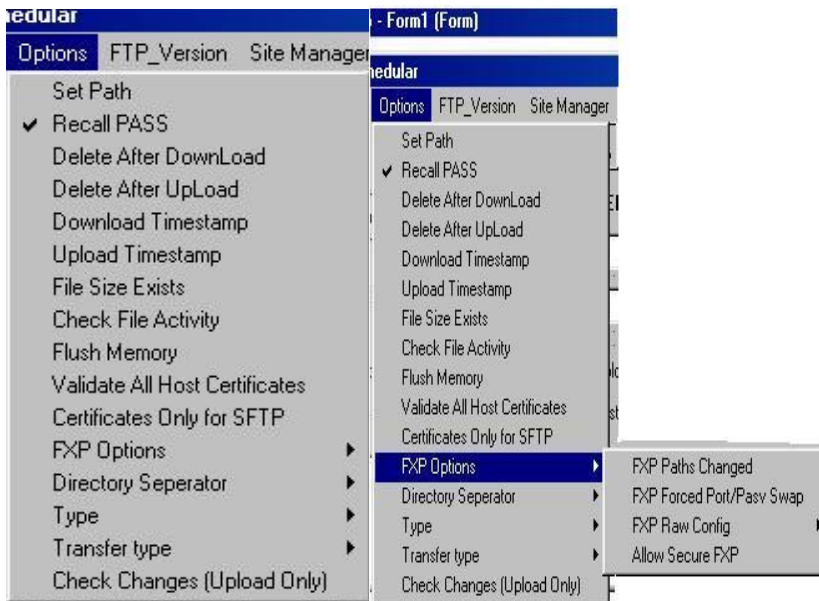

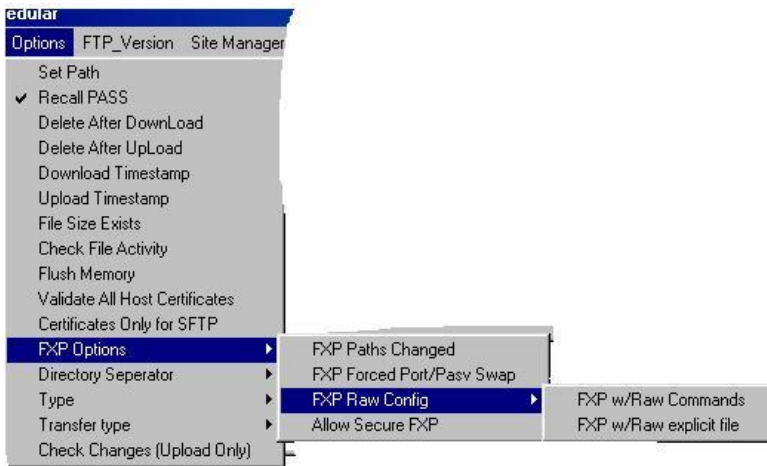Configuring the scheduler for FXP, you must set the following features:

FXP Paths Changed (Optional)
FXP Forced Port/Swap Swap (Optional if implicit PASV fails)
Allow FXP Secure (Optional if attempting to FXP between Secure FTP sites)

FXP w/Raw Commands – Toggles between the two (2) algorithms used to initiate FXP. Choose On/Off (Ticked or UnTicked) to determine which works best.

edular

| Options | FTP_Version | Site Manager |

Set Path
✔ Recall PASS
Delete After DownLoad
Delete After UpLoad
Download Timestamp
Upload Timestamp
File Size Exists
Check File Activity
Flush Memory
Validate All Host Certificates
Certificates Only for SFTP
FXP Options   ▶
Directory Seperator   ▶
Type   ▶
Transfer type   ▶
Check Changes (Upload Only)

FXP Paths Changed
FXP Forced Port/Pasv Swap
FXP Raw Config   ▶
Allow Secure FXP

FXP w/Raw Commands
FXP w/Raw explicit file

The following dialog allows you to set the time to run a FTP process. You can now set the Hour and Minutes precisely. If you leave the minutes setting to Zero(0) then the schedule initiates any part of the hour as was the default setting of the older FTP Scheduler.

Download/Upload dialog is selected by the following actions:

- o   Double Clicking Time/Not Set label
- O   Sub Menu Item Download/Upload from the Schedules Menu Item

The checkbox 'Active' denotes if a site will be included in the scheduled sites to initiate connection. If left unchecked then the site would be omitted.

The checkbox 'FXP On' denotes if a site will be included in the scheduled sites to initiate FXP type transfers.
The Frequency determines if a transfer will initiate Daily or Hourly (Registered Version Only!)

*N.B. The **'Active'** checkbox must be checked for each site for the site to flagged as active during the schedule process*

*'**Check every 0 Minutes**' is only applicable for Registered Version. **Freq** should be set to Hourly when this functionality is required.*

Security

There are 5 protocols for the FTP client:

- o FTP Standard (Unsecure)
- o SFTP (Secure FTP – Public / Private Key)
- o FTP Secure No data encrypt (Public Key/Certificate Authenticate)
- o FTP Secure data encrypt (Public Key/Certificate Authenticate)
- o FTP Implicit (Public Key/Certificate Authenticate)

N.B. Upon configuring the Site information when dealing with public/private key or certification encryption you must always save the Key or Certificate after you load or generate it the 1st time so the system will create a file so when the scheduler triggers it will load the appropriate file for that site.
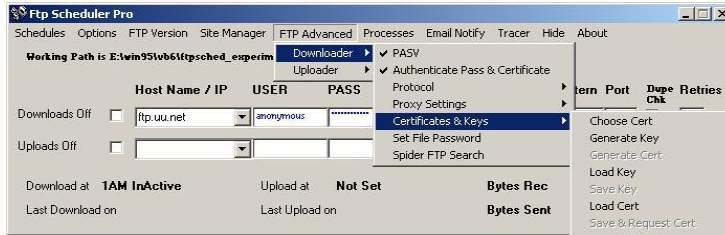

Proxy server settings:

- o Active – Sets transfer to be re-routed through a proxy to bypass firewall restrictions
- o FXP Inactive – Disables FXP to permit access to FTP sites with strict NAT settings
- o Proxy Host – Dialog to set the Hostname / IP of the proxy server

Choosing / Setting the type of encryption for Secure FTP protocols (SFTP , FTPS etc)
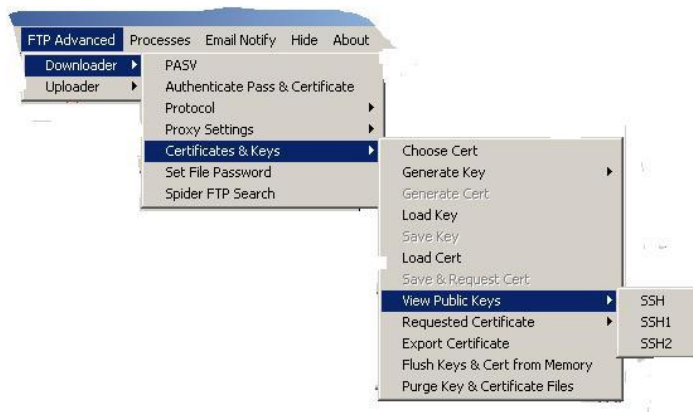
- o Choose Certificate – Select Certificates from windows registry
- o Generate Key – Generate Public/Private key for SFTP & FTPS protocols
- o Generate Certificate – Generate Certificate for LAN use
- o Load Key – Load Key saved on previous occasion
- o Save Key – Save Key in memory to file
- o Load Certificate – Load Certificate previously saved
- o Save / Request Certificate – Save Certificate or Request one from 3rd party for internet use
- o Flush Keys/Certificates – Purge all Keys and Certificates set previously for the Download/Upload Site

Viewing the Public Keys in different data formats that exists for a Download/Upload site.
N.B. Key must be Generated or Saved before attempting to view public Keys
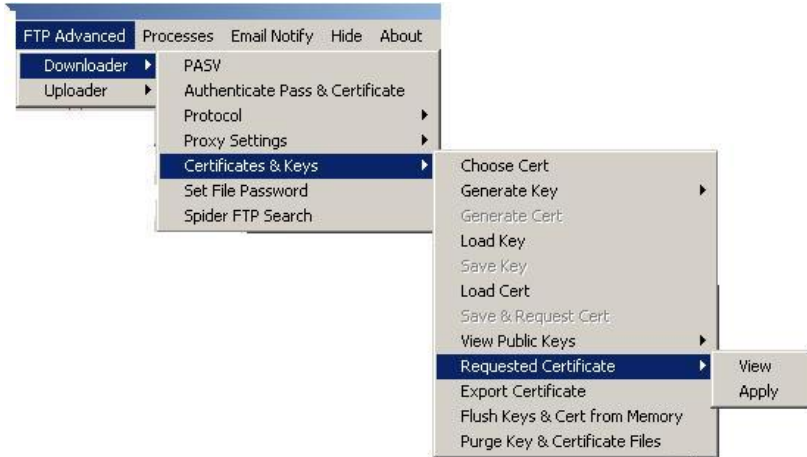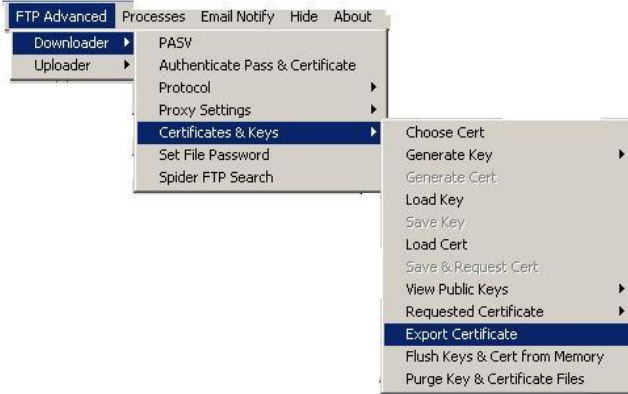
- o SSH
- o SSH1
- o SSH2

View certificate request / Apply Certificate returned from 3rd Party
N.B. Certificate must be Generated or Saved before attempting to view Requested/Saved Certificate

- o   View – Request Certificate saved as a file previously
- o   Apply – Implement Certificate from 3rd Party via a load dialog

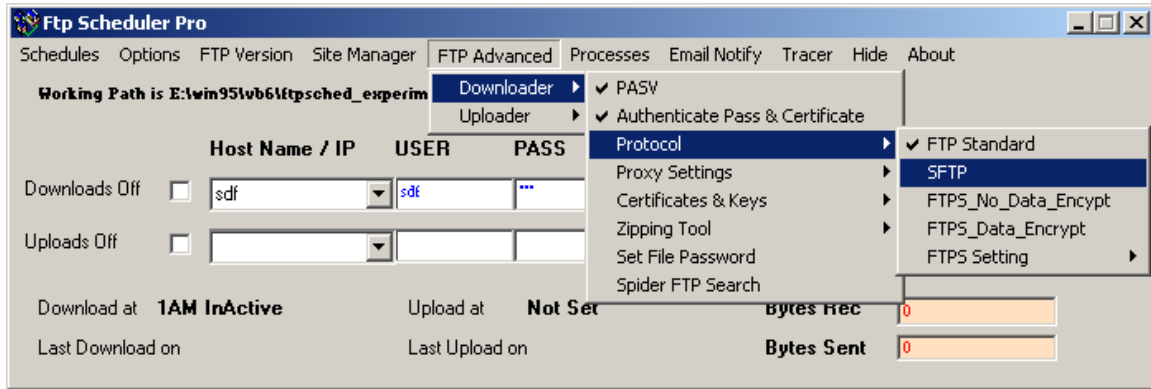Export Certificate for easy import into Windows Registry.

The status of the export is shown to the user in a popup prompt.

After the standard Site configuration is complete please follow these steps to create a secure FTP Site session:
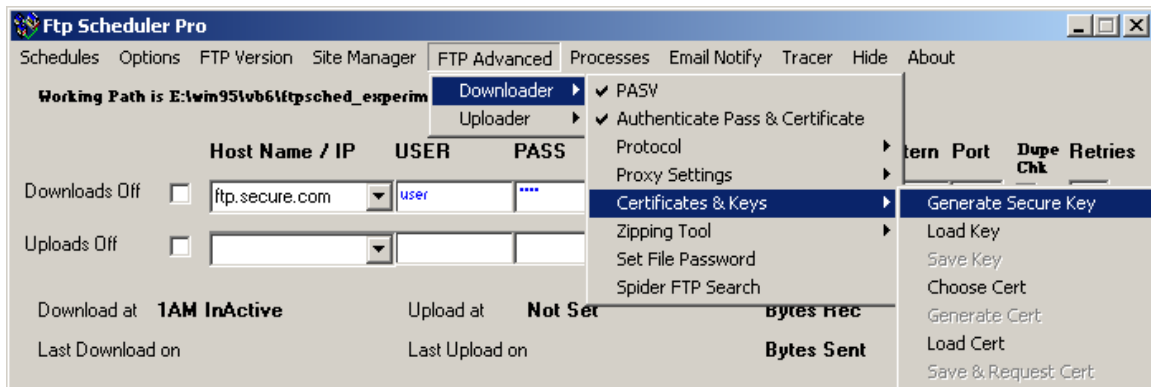
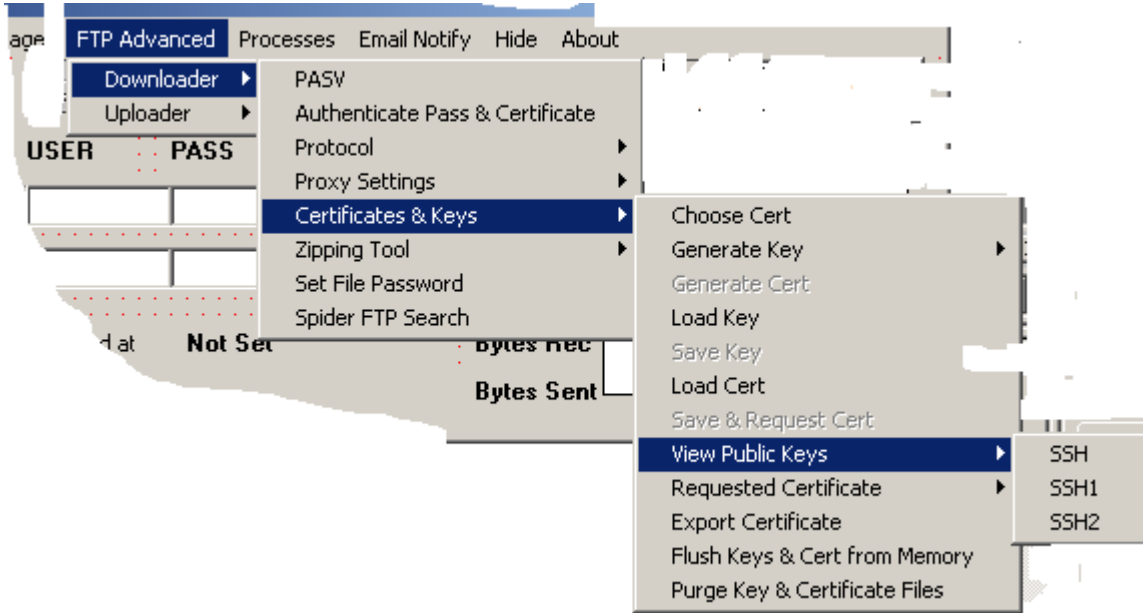**Step 1**

Select SFTP Protocol menu option as shown below:

Step 2

Generate a public/private Key as shown below: That's it you are set for Secure Connections. Loading of Keys or Certificates is if provided by external parties.
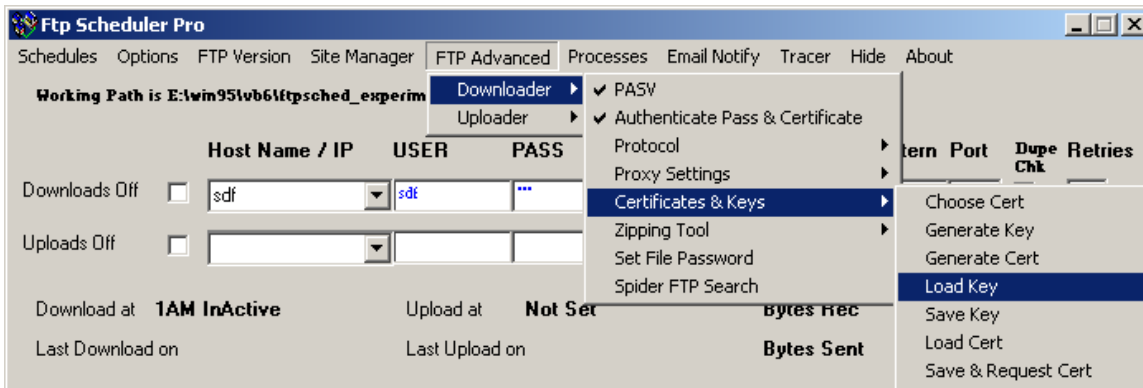
Step 3(Optional)

The site session is now configured for a secure connection to the siteTo register the 'Key' with a public organization such as 'Verisign' the step is to submit the public key. This is achieved by pasting the public key in the publicssh file on the FTP Server (Ask site administrator to assist in placing in right file/area). This is achieved by selecting the option below to view the respective public key.

Step 4 (Optional)

In the event you closed the application before step 4, you can 'Load Key' as shown below then follow step 4 to achieve the same result.
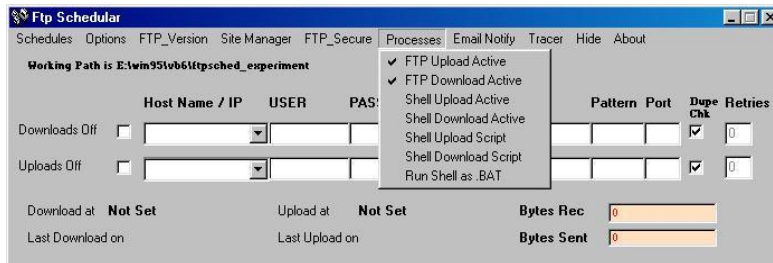

N.B. Do not 'Generate Key' unless you intend to create a new Private/Public key for a site. Please follow step 5 if a key was generated previously for a particular site. Each site session requires you to follow steps 1 through 5.

Processes Settings

This menu option allows the user to activate the following processes.
- o Upload Processes (On/Off)   - Permit Upload FTP schedules to initiate
- o Download Processes (On/Off) - Permit Download FTP schedules to initiate
- o Shell Upload Active After   - Permit process to launch Upload **'Batch Script'** After FTP transfer completes
- o Shell Upload Active Before   - Permit process to launch Upload **'Batch Script'** Before FTP transfer Starts
- o Shell Download Active After   - Permit process to launch Download **'Batch Script'** After FTP transfer completes
- o Shell Download Active Before - Permit process to launch Download **'Batch Script'** Before FTP transfer Starts
- o Shell Upload Script   - Dialog to enter Upload Script code to execute
- o Shell Download Script   - Dialog to enter Download Script code to execute
- o Shell Blocking   - Enforce blocking to synchronise the Batch Script with the FTP transfer
- o Run Shell as script   - Toggle On/Off to use code in dialog or use single instruction

Please note that the user has the ability activate shell scripts without having the FTP active.

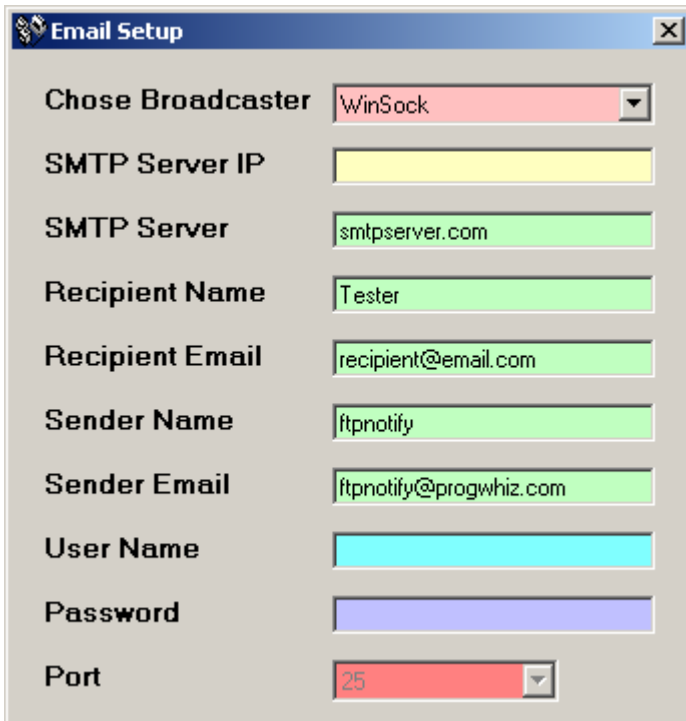Sample of the Shell Script Dialog

N.B. Leave empty if you don't want a script executing after a particular site transfer is completed. This can be useful especially when you have shell scripts active but you don't want or need every site to launch a Batch Script.

Email Configuration

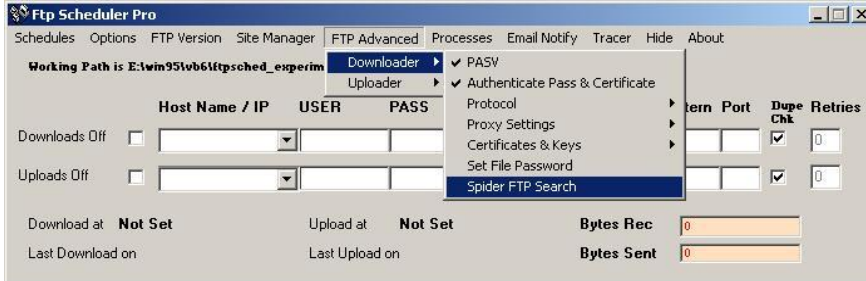Below is the Menu option to configure the email notification module.

Firstly configure the settings shown below applicable to your email client/server. By default the email module will look for Recipient Name and SMTP server settings to change before it permits this moduel to be considered configured properly.
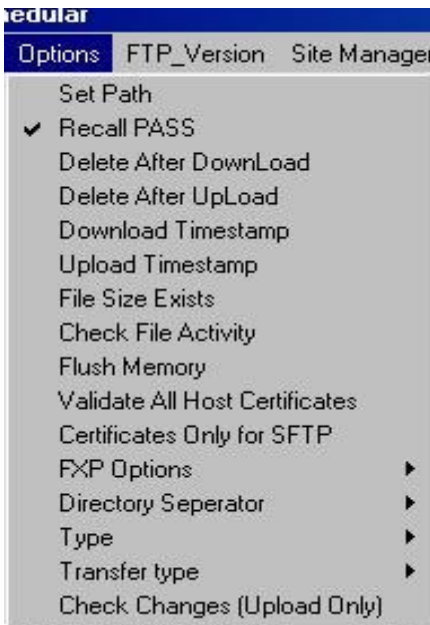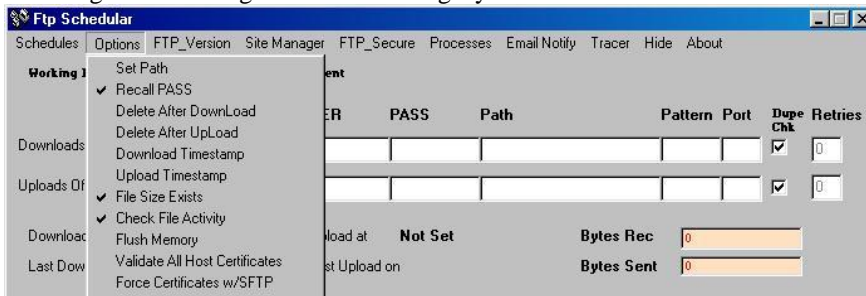
File Analysis

FTP site recursive directory search Enabled/Disabled by checking/unchecking the **Spider FTP Search** submenu option

Selecting the following enforces file integrity checks

- o File Exists – Assumes file size response is received from the FTP server
- o Check Changes (Upload Only) – Checks for new files awaiting upload
- o Check File Activity – Verifies the file being transferred is not Busy before permitting transfer to initiate

Registered Version

The 3 key differences between the Unregistered and Registered version is as follows:

	Registered	**Unregistered**
1)	Set # of retries	Only 1 Retry
2)	Set to transfer hourly	N/A
3)	Support 24/7	Support 8/5
4)	Auto Renewal	No Renewal
5)	Free updates	Free updates
6)	Triggered Upload	N/A
7)	Zip/Unzip	Unzip Only
8)	Schedule by Time Difference	N/A

Auditing Features & Log Files

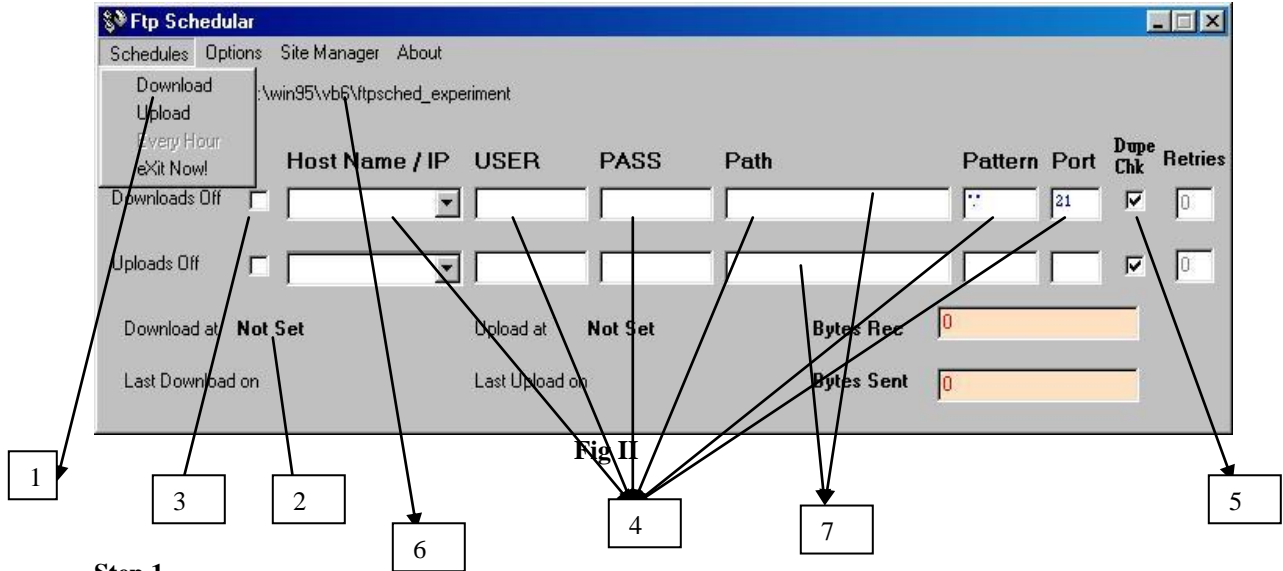| File Name	Description
DL_FILE_SIZE.LOG	Records the Date, Time, Site Name, Name of file received and the size in bytes as well as if the transfer was a FAIL or PASS.
FILEUPL.LOG	Records the Date, Time, Site Name, Name of file sent and the size in bytes as well as if the transfer was a FAIL or PASS.
FILEUPL1.LOG	Name of files uploaded. The files will not be re-uploaded once the dupe-check check box is checked
FILENAME2.LOG	Name of files downloaded. The files will not be re-downloaded once the dupe-check check box is checked
VALUES.LOG	Records the last settings used in the ftp client. The password is encrypted in this file for security measures
ERR_UPLOAD.LOG(Standard Only)	Records the Date & Time the FTP could not connect to the FTP server or Network to initiate an Upload.
ERR_DLOAD.LOG(Standard Only)	Records the Date & Time the FTP could not connect to the FTP server or Network to initiate a Download.
FILEXT.DAT(Professional Only)	Stores all the known ASCII File types. Add or delete to assist the auto transfer detect option in detecting the proper transfer mode
DONE.DAT(Professional Only)	Logging all FTP site Errors
WAITING.CHK	File which is created to denote a shell script is active. When the 'Shell Blocking' is active

Secure FTP Certificates/Keys & Shell/Bat Files

PUBLICDXX.LOG PUBLICUXX.LOG	Public key in RAW format
PUBLICSSHDXX.LOG PUBLICSSHUXX.LOG	Public key in SSH format
PUBLICSSH1DXX.LOG PUBLICSSH1UXX.LOG	Public Key in SSH1 format
PUBLICSSH2DXX.LOG PUBLICSSH2UXX.LOG	Public Key in SSH2 format
CERTDXX.LOG CERTUXX.LOG	Certificate not encrypted format saved in this file
SHELLDL.BAT SHELLUL.BAT	Text file containing single line instruction for BAT process
SHELLDL2.DAT SHELLUL2.DAT	Text file containing script instructions for BAT process
DEFKEYDXX.KEY DEFKEYUXX.KEY	Private key encrypted with pass from '**Set File Password**' submenu option
DEFCERTDXX.CRT DEFCERTUXX.CRT	Certificate encrypted format saved in this file
DEFPFXXX.PFX DEFPF2XXX.PFX	Certificate/Private Key contained in this file
DEFREQXX.CRT DEFREQUXX.CRT	Certificate Request saved in this file

XX- Denotes Site #

N.B. Password Protection for textbox's enforced when Registration Name ends in 'S'

User Guide

Fig II

Step 1

   Enter Data for Receiving (Downloading) – Item (**4**) in Fig II is mandatory

        IP Address or Domain Name of Server
        User Name
        Password
        Path where files are located
        Type of Files to retrieve
        Listening Port of Server

N.B. (**7**) After the site information has been added and 'Activated' the user can double click on this textbox Area to view the Directory contents to verify the path is correct or simply navigate.

Step2

  Set Download Time by selecting option (**1**) or double click on (**2**) as shown in Fig II. Which pulls up
  the following dialog Box, shown below in Fig III.

   i)   Select the time (AM or PM)
   ii)   Select if the transfer starts at a specific number of minutes after the hour (leave at zero(0) if
        desired to start anytime once the hour is reached)
   iii) Set if the transfer starts daily or hourly (Only available in Registered version)
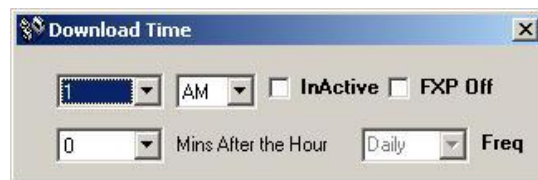   iv) Check the tick box to flag the transfer as active

Fig III

Step3

  Click on option (3) to start the download timer for all the 'Active' download sessions set in Step 2 for
  a specific FTP Site.

Step4

  Activate/Deactivate duplication check safety option (**5**)

Step5
  Set path to which all files are Sent/Received option (**6**)

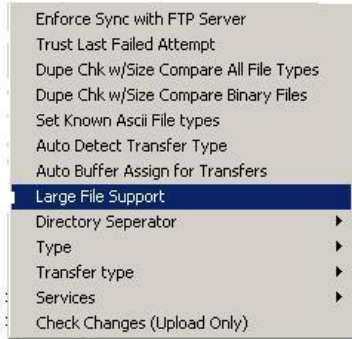P.S. The steps taken to set the Downloading Schedule is to be replicated for Uploading

Special Features

❑ **Aborting Transfers if Network Fails and attempts next file on Queue**

❑ **Adjusts Download/Upload timers if one process takes longer than estimated**

❑ **Automatically retries to receive/send a file upon failure**

❑ **logging even critical errors without causing an application Error**

❑ **Verifying all required fields are populated with valid entries**

❑ **Comprehensive information giving status of current and last transfers**

❑ **Ability to toggle the ability to save the Password (Default is Unchecked)**

❑ **Delete the successfully downloaded file from the FTP Server (Default is Unchecked)**

❑ **Delete file after it is successfully uploaded to the FTP Server (Default is Unchecked)**

❑ **Prevents the application from being exited while a transfer is in process**

❑ **Ability to detect when a transfer ends when the FTP server response is not efficient (File Size known menu property must be checked)**

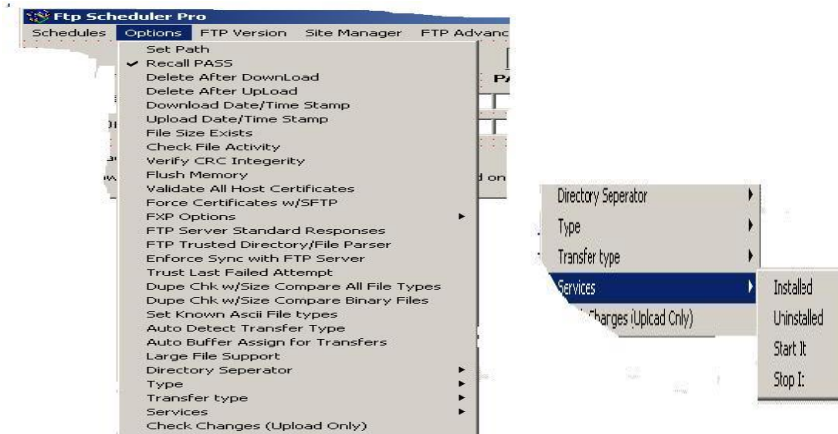❑ **Ability to estimate accurately the duration for a file transfer**

New Features

The following features were added based on user feedback as 'Value Add'. The new features are as follows:
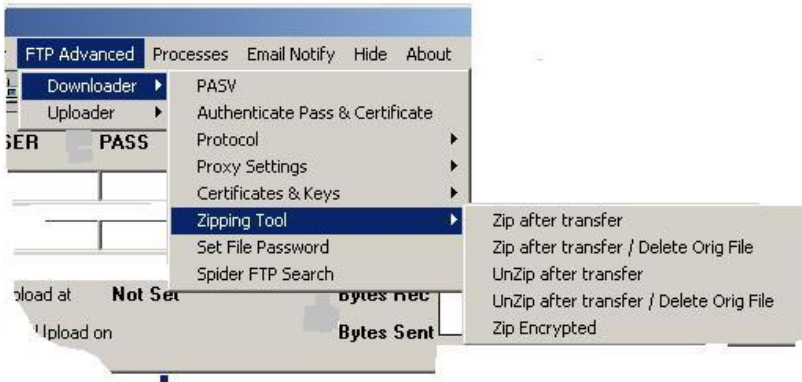
1) Large File support greater than 2.4Gig+

The limitation of most FTP clients is that the size is calculated using a 32Bit value which is limited to 2.4gig Signed or 4.2Gig Unsigned. This new support enables file up to 16000 TeraBytes.
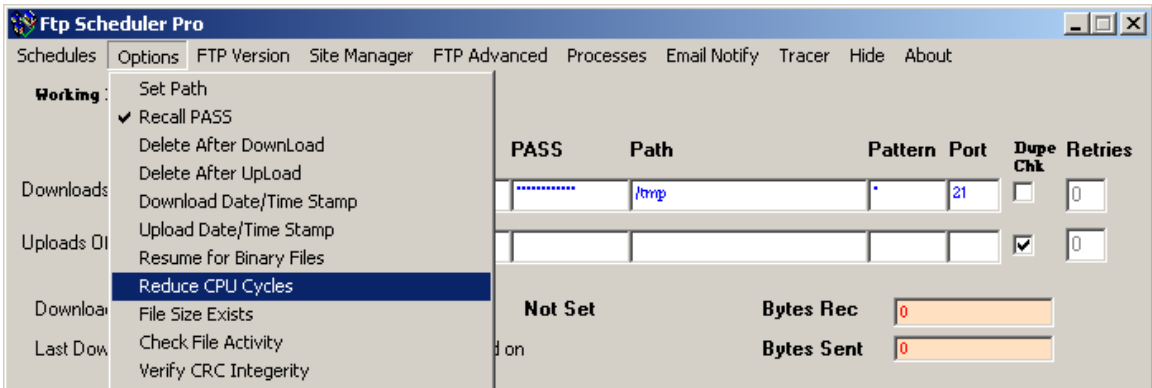
2) Ability to launch as a Windows Service

As the above images shows the FTP Scheduler Pro can be launched as a Windows Service. It is noteworthy to mention that if the Scheduler is not Active the Service will not be allowed to be launched. Also if the service is stopped via the FTP Scheduler Pro it can only be relaunched via the application not Windows Service Manager, this is to ensure full control by the application.

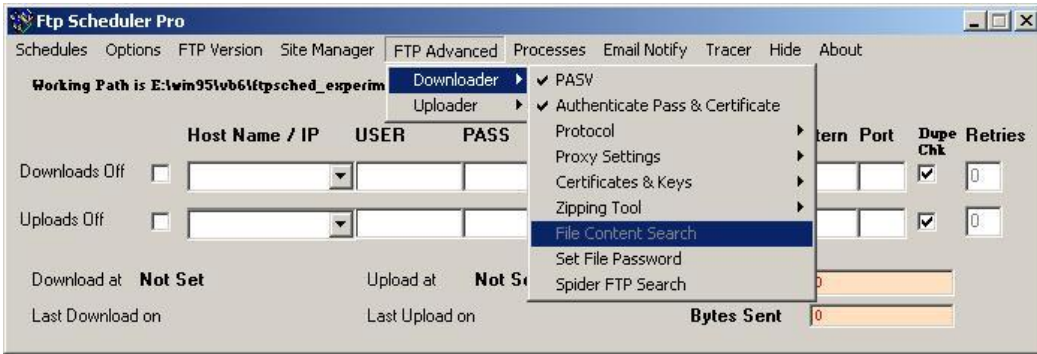3) Ability to Compress/Uncompress Files Post/Pre file transfers using the Zip Algorithm

Both Upload and Download transfers can now denote if to compress a file before or after a transfer respectively. Further to which a file can be uncompressed after a download. Encryption is also supported. *Only the Uncompress option is available in the Unregistered version*.

4) Ability to Reduce CPU Cycles.

5) Ability to search for String/Hex patterns in a file to determine if a file transfer is to take place and/or a file is kept.

Menu option is shown above. The setting is unique to each FTP session created (Upload/Download). Special care must be taken using this option. For instance if the String/Hex is not present a transfer will not be permitted and the system will not attempt to retrieve the file as it would be logged by the system as a file to ignore when the 'Dupe Chk' is set.

Below shows the dialog which permits the user to choose between a String or Hex search:

In addition to the ability to search for String patterns the user can now also search for current **Date/Time** values. This is facilitated by using the following syntax in *the String Search* option:
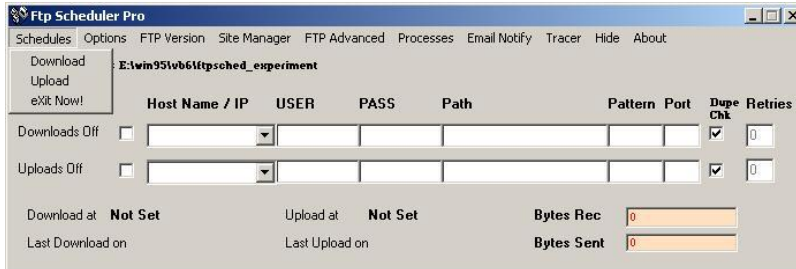
1) $Date(yy/mm/dd)
2) $Date(yyyy/mm/dd)
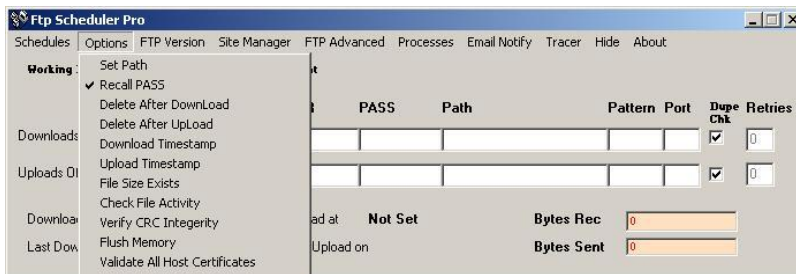3) $Date(yy:mm:dd hh:mm:ss)
4) $Date(mmm dddd)
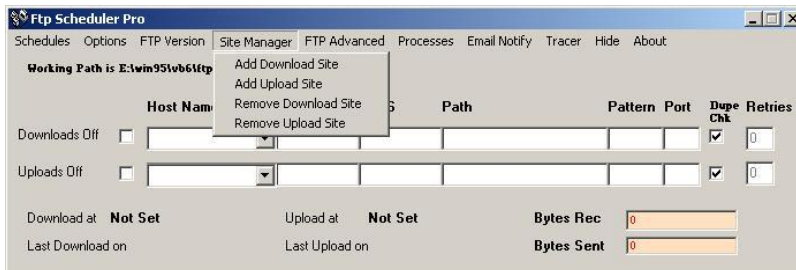
5) Appendix

Menus

Schedules Menu

Options Menu

Site Manager

FTP Advanced Settings

Process Settings