

LimagitoX FileMover - Move your files from anywhere to anywhere

Overview

Overview



[Introduction](#)



[License](#)



[Revision History](#)

About

File Mover Software from Limagito.com

LimagitoX FileMover - Move your files from anywhere to anywhere

LimagitoX filemover software is an all-in-one automated file mover solution handling everything from moving, deleting to copying files. LimagitoX is a powerful business automation tool that puts you firmly in control. Discover our features:

You can set file and directory filters based on the file name, date and size. Also rename, encrypt or decrypt files (including PGP) and rename directories (using regular expressions) when moving them to the new destination. Create directories based on the file name or date and check if the file already exists. The file-mover can move files from/to local folders as well as FTP, SFTP, FTPS directories and to SMTP.

This software offers quite a few features that make the program very flexible and useful for a variety of file management tasks as well as file backups. LimagitoX runs in the system tray and automatically monitors the selected folders for any additions that match your file moving rules. You can set up as many working threads as wanted (Full Version), each with individual settings. Other features include detailed logging, support for subdirectory scanning, command-line options and much more.

License

License Information

For the LimagitoX file mover software is a Lite, Single User, Site and Corporate License available. The file mover Lite edition is free but is restricted to a single moving rule. A single user license grants you the right to install and use LimagitoX on a single machine. A single License key is generated for a specific hostname (= not transferable). A site license allows you the right to install and use LimagitoX file mover across multiple machines in your organization at a single site. A corporate license allows you the right to install and use LimagitoX file mover across multiple machines in your organization regardless of location.

LimagitoX file mover licensing

After payment you will receive a zipped License.xml file by mail. We typically process most orders within a few hours. However in some cases it can take up to 2 business days.

Refund Policy

We provide a free Lite version to let you fully evaluate our product(s) before purchasing. Unlike physical goods, electronically distributed software and software licenses can be duplicated. Once a license has been issued, it is unfortunately not possible for us to recall all copies. Therefore, Limagito.com does not accept product returns or exchanges. It is your responsibility to familiarize yourself with this refund policy. By placing an order, you are supposed to have read this refund policy, agreed with and fully accepted the terms of this refund policy. If you do not agree with or fully accept the terms of this refund policy, please do not purchase our product.

Revision History



LimagitoX Help v2013.08.25 (draft)



LimagitoX Help v2013.08.26

EULA

END-USER LICENSE AGREEMENT

IMPORTANT! BE SURE TO CAREFULLY READ AND UNDERSTAND ALL OF THE RIGHTS AND RESTRICTIONS SET FORTH IN THIS END-USER LICENSE AGREEMENT ("EULA").

This EULA is a binding legal agreement between you and www.limagito.com (hereinafter "Licensor") for the materials accompanying this EULA, including the accompanying computer software, legal forms, associated media, printed materials and any "online" or electronic documentation (hereinafter the "Software"). By installing the Software, you agree to be bound by the terms of this EULA. If you do not agree to the terms of this EULA, do not install or attempt to use the Software.

1. Grant of License

The Software and legal forms are protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The Software and forms are licensed, not sold.

This EULA grants you the following rights:

- A. A single user license grants you the right to install and use LimagitoX on a single machine. A Single User License key is generated for a specific hostname (= not transferable).
A site license allows you the right to install and use LimagitoX across multiple machines in your organization at a single site.
A corporate license allows you the right to install and use LimagitoX across multiple machines in your organization regardless of location.
- B. Your license rights under this EULA are non-exclusive. All rights not expressly granted herein are reserved by Licensor.
- D. You may not sell, transfer or convey the Software to any third party without Licensor's prior express written consent.

2. Replacement, Modification and/or Upgrades

Licensor may, from time to time, and for a fee, replace, modify or upgrade the Software. When accepted by you, any such replacement or modified Software code or upgrade to the Software will be considered part of the Software and subject to the terms of this EULA (unless this EULA is superceded by a further EULA accompanying such replacement or modified version of or upgrade to the Software).

3. Termination

You may terminate this EULA at any time by destroying all your copies of the Software. Your license to the Software automatically terminates if you fail to comply with the terms of this agreement. Upon termination, you are required to remove the Software from your computer and destroy any copies of the Software in your possession.

4. Copyright

A. All title and copyrights in and to the Software (including but not limited to any images, photographs, animations, video, audio, music and text incorporated into the Software), the accompanying printed materials, and any copies of the Software, are owned by Licensor or its suppliers. This EULA grants you no rights to use such content. If this Software contains documentation that is provided only in electronic form, you may print one copy of such electronic documentation. Except for any copies of this EULA, you may not copy the printed materials accompanying the Software.

B. You may not to reverse engineer, de-compile, disassemble, alter, duplicate, modify, rent, lease, loan, sublicense, make copies of, create derivative works from, distribute or provide others with the Software in whole or part, transmit or communicate the application over a network.

5. Disclaimer of Warranties

LICENSOR AND ITS SUPPLIERS PROVIDE THE SOFTWARE "AS IS" AND WITH ALL FAULTS, AND HEREBY DISCLAIM ALL OTHER WARRANTIES AND CONDITIONS, EITHER EXPRESS, IMPLIED OR STATUTORY, INCLUDING BUT NOT LIMITED TO ANY (IF ANY) IMPLIED WARRANTIES OR CONDITIONS OF MERCHANTABILITY, OF FITNESS FOR A PARTICULAR PURPOSE, OF LACK OF VIRUSES, AND OF LACK OF NEGLIGENCE OR LACK OF WORKMANLIKE EFFORT. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, OF QUIET ENJOYMENT, OR OF NONINFRINGEMENT. THE ENTIRE RISK ARISING OUT OF THE USE OR PERFORMANCE OF THE SOFTWARE IS WITH YOU.

6. Limitation of Damages

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT WILL LICENSOR OR ITS SUPPLIERS BE LIABLE FOR ANY CONSEQUENTIAL, INCIDENTAL, DIRECT, INDIRECT, SPECIAL, PUNITIVE OR OTHER DAMAGES WHATSOEVER ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE AND WHETHER BASED ON CONTRACT, TORT, NEGLIGENCE, STRICT LIABILITY OR OTHERWISE, EVEN IF LICENSOR OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. THIS EXCLUSION OF DAMAGES WILL BE EFFECTIVE EVEN IF ANY REMEDY FAILS OF ITS ESSENTIAL PURPOSE.

7. Arbitration

This Agreement is made under, shall be governed by and construed in accordance with the laws of Belgium.

8. Severability

If any term of this EULA is found to be unenforceable or contrary to law, it will be modified to the least extent necessary to make it enforceable, and the remaining portions of this Agreement will remain in full force and effect.

9. No Waiver

No waiver of any right under this EULA will be deemed effective unless contained in writing signed by a duly authorized representative of the party against whom the waiver is to be asserted, and no waiver of any past or present right arising from any breach or failure to perform will be deemed to be a waiver of any future rights arising out of this EULA.

10. Entire Agreement

This EULA constitutes the entire agreement between the parties with respect to its subject matter, and supersedes all prior agreements, proposals, negotiations, representations or communications relating to the subject matter. Both parties acknowledge that they have not been induced to enter

into this EULA by any representations or promises not specifically stated herein.

Options

Application

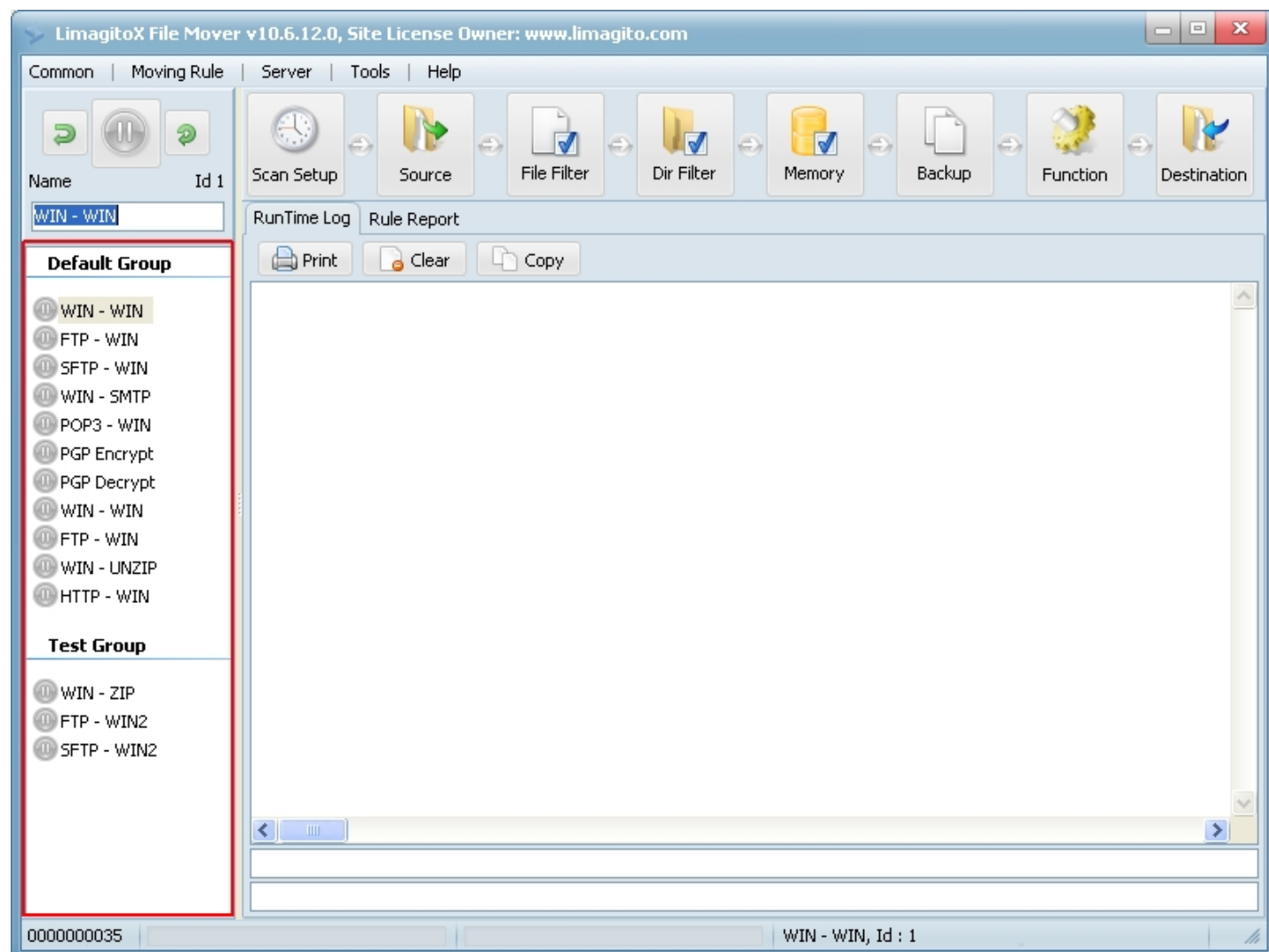
-  [GUI Introduction](#)
-  [Common](#)
-  [Moving Rule](#)
-  [Server](#)
-  [Tools](#)
-  [Help](#)
-  [Source Options](#)
-  [Destination Options](#)
-  [Service Options](#)

GUI

Application GUI Introduction

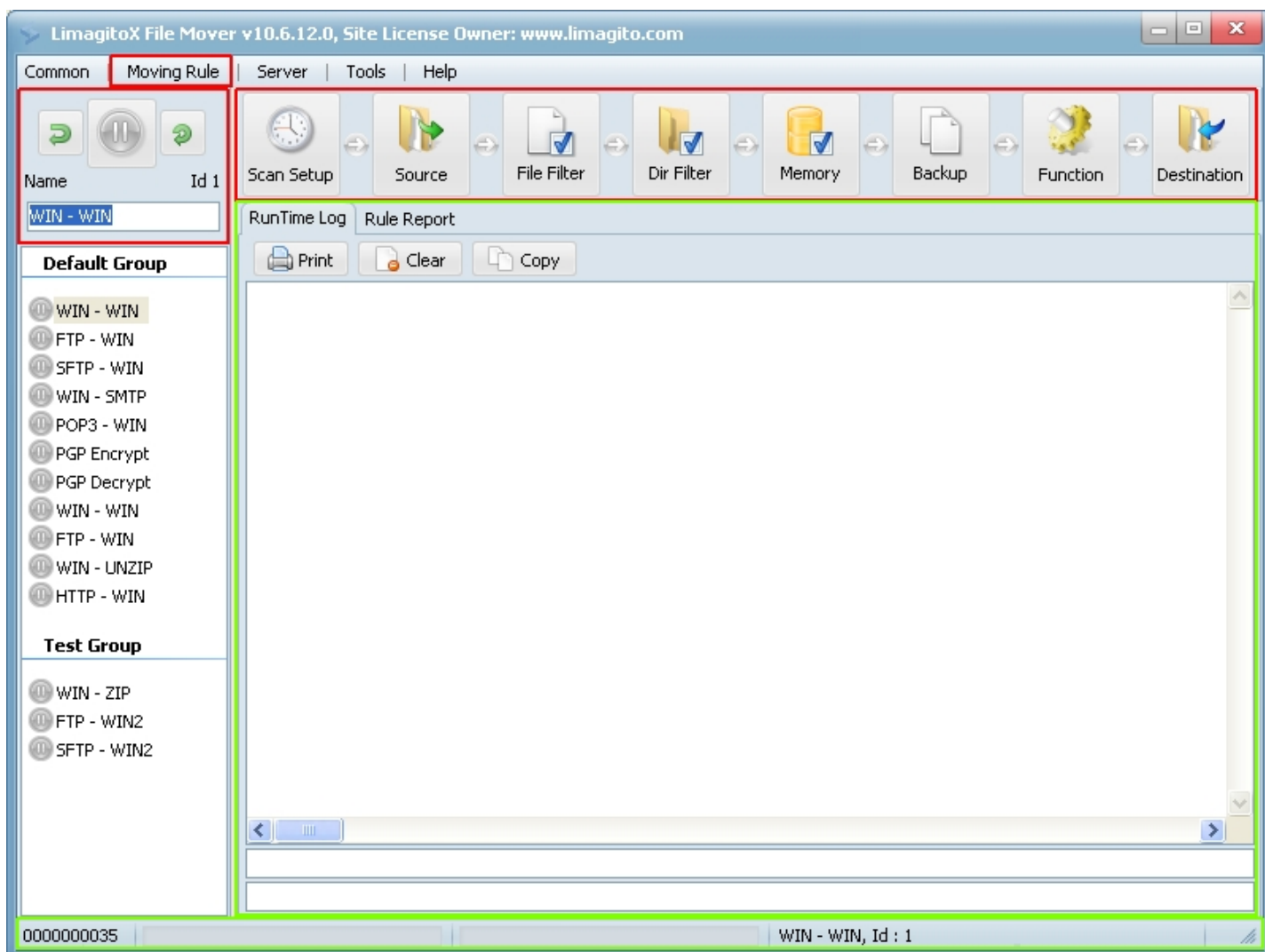
When using LimagitoX you'll often see the term 'rule'. A rule is like a kind of mini application running within the LimagitoX GUI or Service. Each rule has it's own settings and uses the GUI to show it's status. Theoretically you can add 999 rules. Our advice is to use a maximum of 500 rules with one instance of our file mover.

The list view, marked with red, on the left side contains the available rules. Left click to select one of the rules.

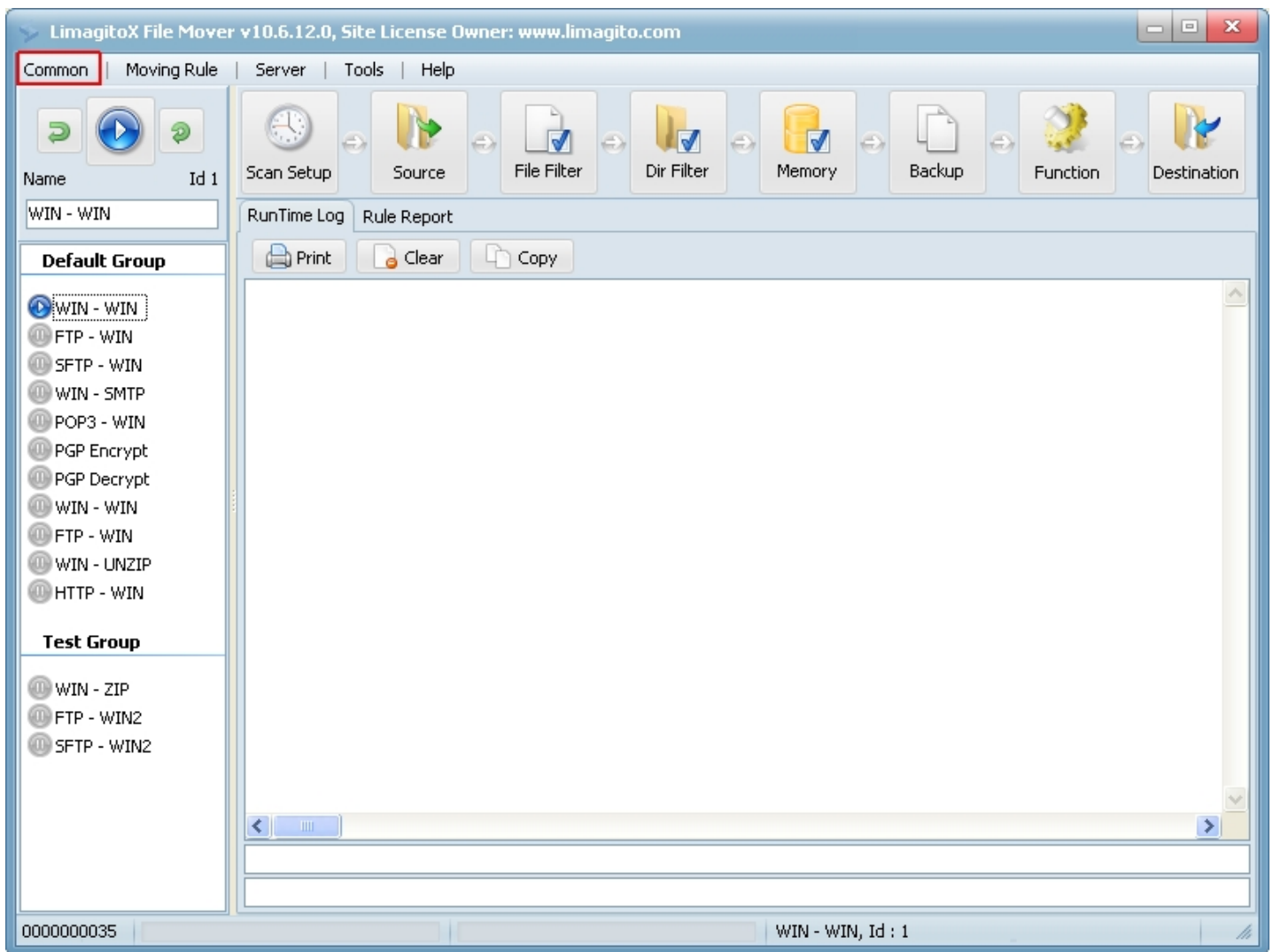


In the following screenshot we've marked some areas related to a single rule:

- the red parts are used to setup the selected rule
- the green parts provides you with status information of the selected rule

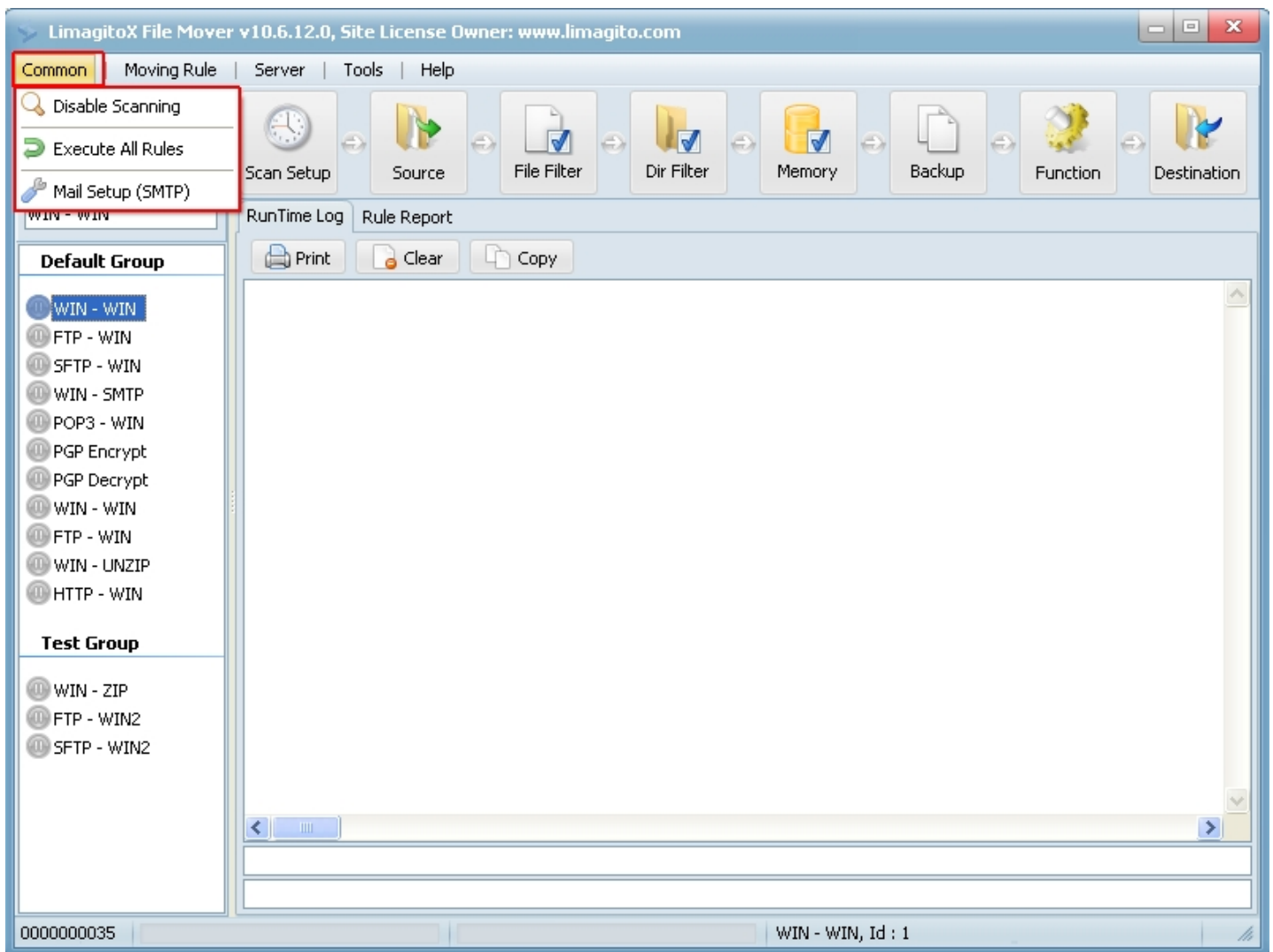


In the 'Common' menu you can find options that are used by all rules. This is what we refer to as common options.



Common Options

Common Options (Common for all rules)



- ▶ **Disable / Enable Scanning:** Disable / Enable scanning source of all enabled moving rules.

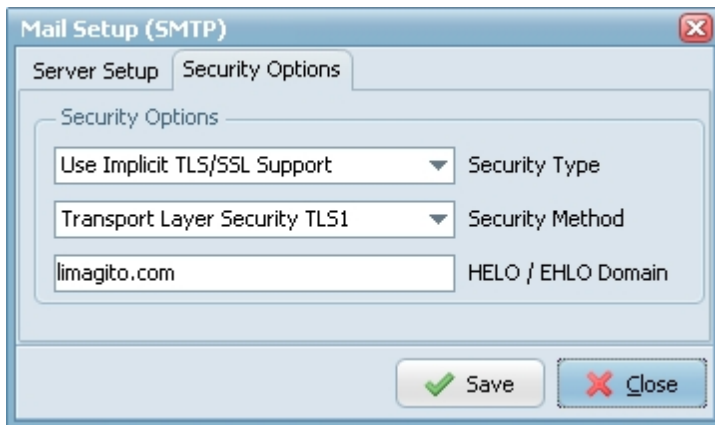
- ▶ **Execute All Rules:** Execute all enabled rules now. With execute we mean that scanning of the source will be triggered one time.

Mail Setup (SMTP)

Server Setup

Common mail settings. Can be used in the 'Rule Events' option. This way you only need to setup the Mail Server once instead of doing this for each Moving Rule.

Security Options

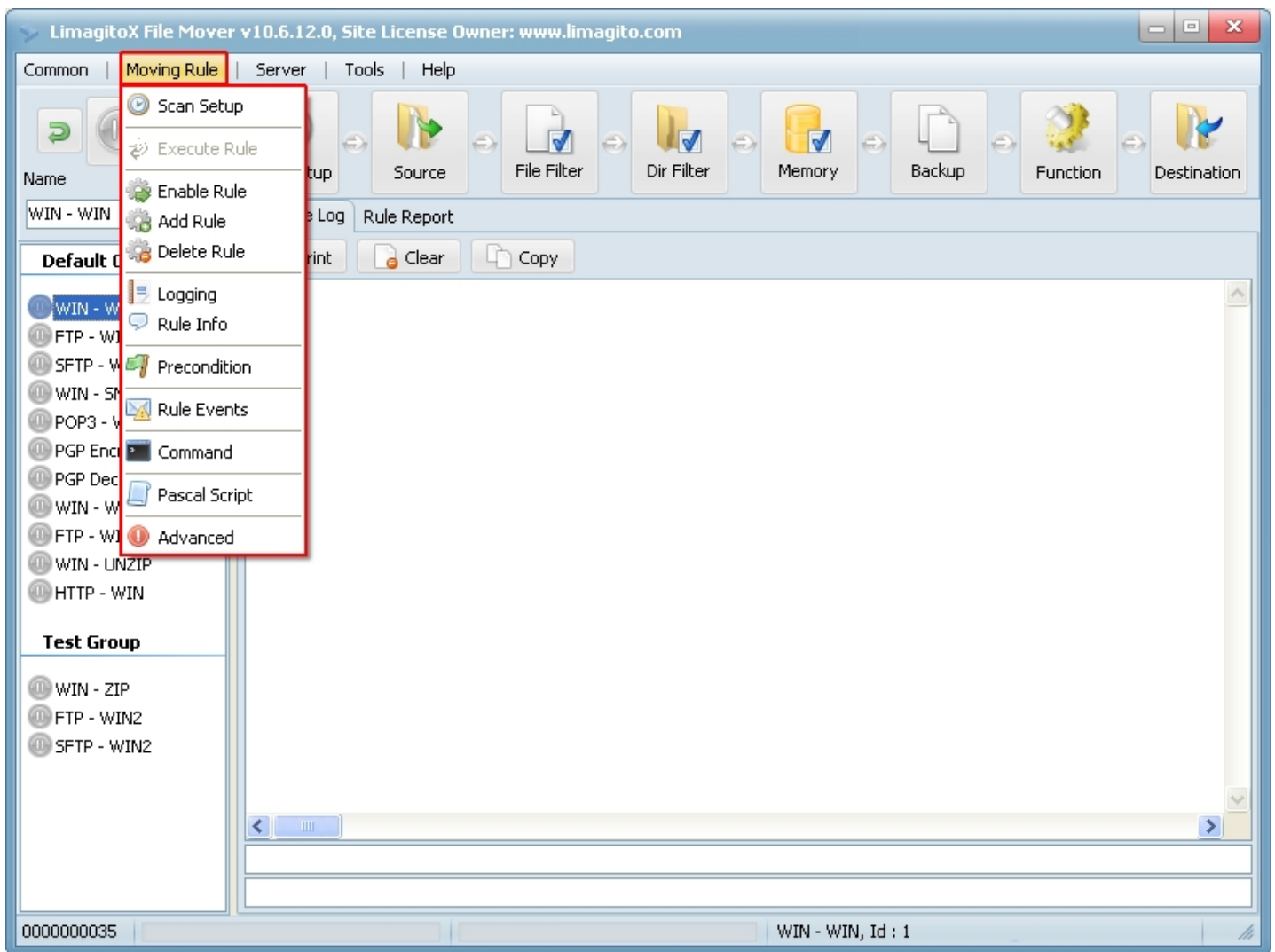


- ▶ With the security options you can enable TLS/SSL support for SMTP.
- ▶ HELO/EHLO Domain: Ask the server for the SMTP extensions that the server supports, by using the EHLO greeting of the Extended SMTP specification (RFC 1870). Fall back to HELO only if the server does not respond to EHLO.

Rule Options

Moving Rule (Unique for each rule)

-  [Scan Setup](#)
-  [Logging](#)
-  [Rule Info](#)
-  [Precondition](#)
-  [Rule Events](#)
-  [Command](#)
-  [Pascal Script](#)
-  [Advanced](#)

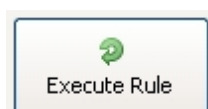


Toggle switch: Enable/Disable the selected moving rule.

Name

1. Win - Sntp

Short name (description) for the selected moving rule.



Execute selected rule now. The selected rule must be enabled. The button is only visible if the rule is enabled.

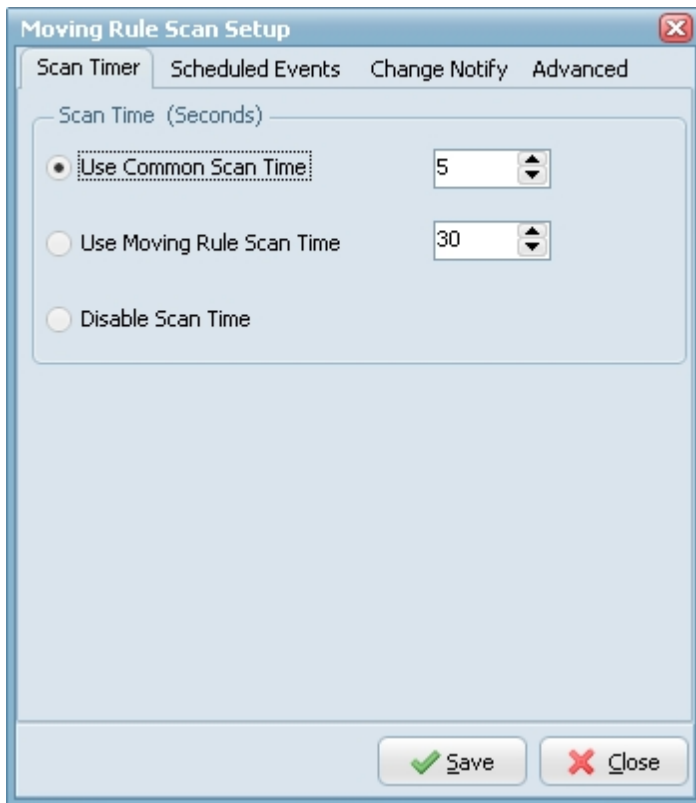
Scan Setup

Scan Setup

A trigger is an event that executes a rule. The default 'trigger' for a new rule is the common scan time. Next to the manual trigger we have three automatic triggers available for each moving rule:

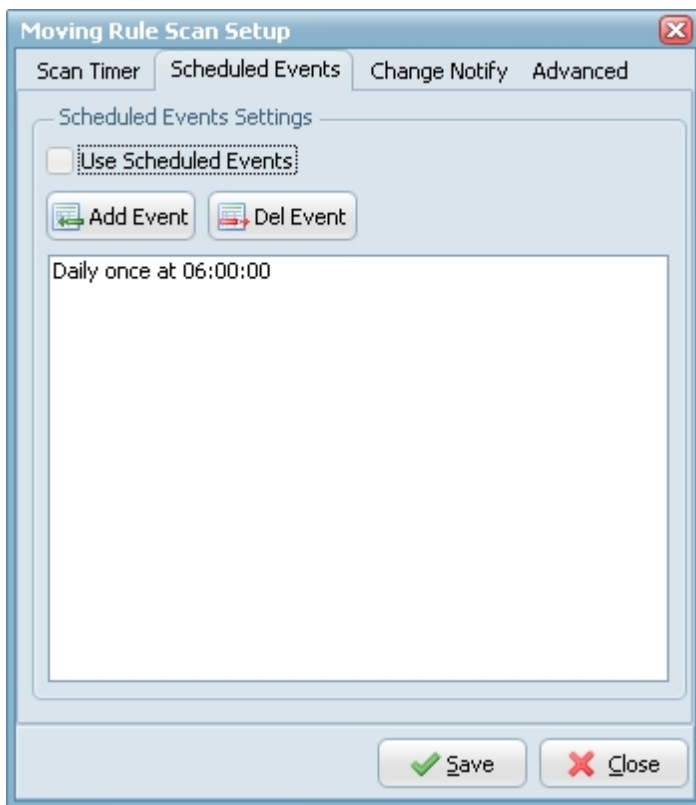
- 1) Scan Timer
- 2) Scheduled Events
- 3) Change Notify (WIN as Source)

Scan Timer

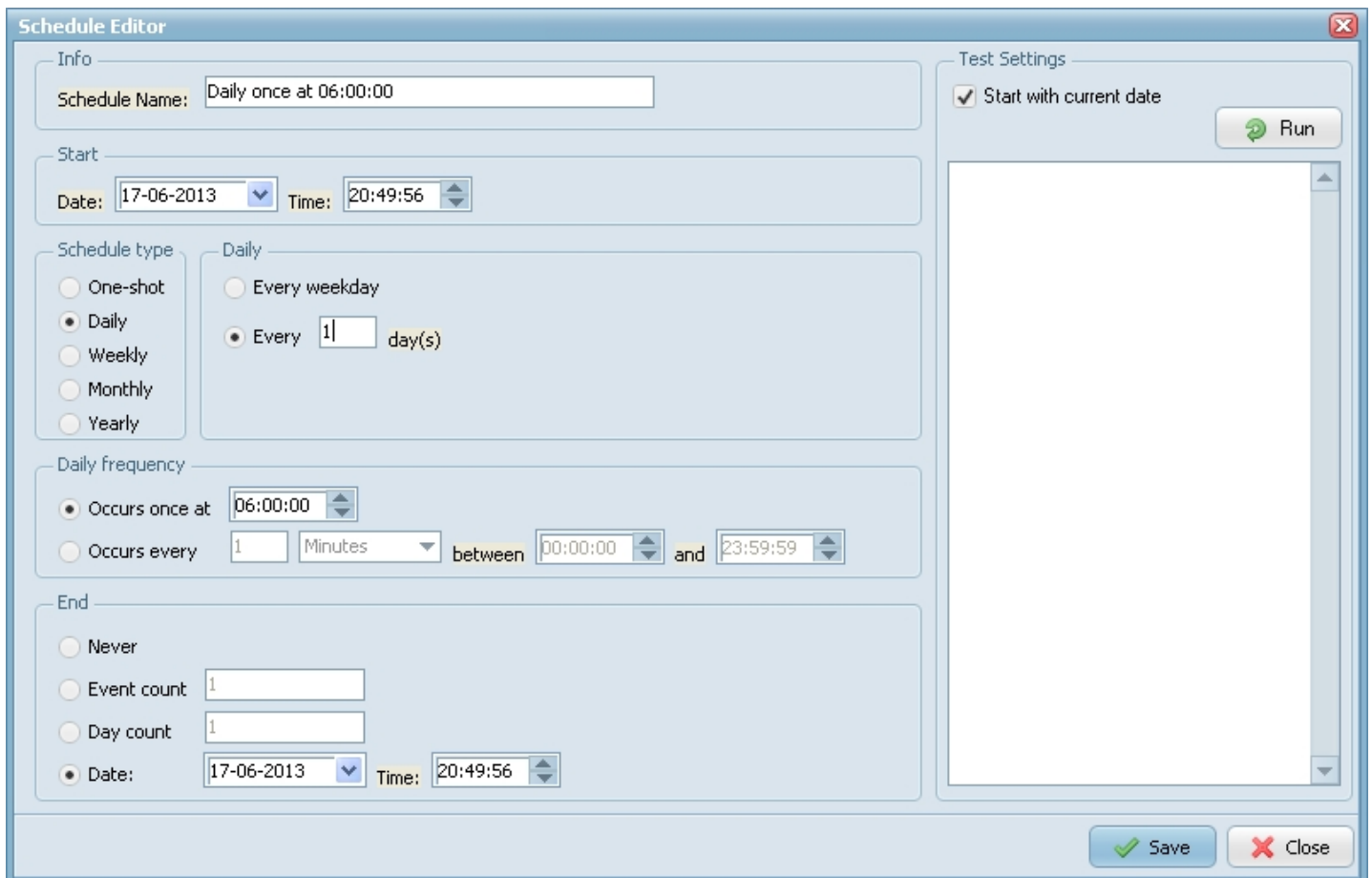


- ▶ Use Common Scan Time: The common scan time can be used by multiple moving rules. Changing the value of this timer will reflect on all rules where this timer is enabled.
- ▶ Use Moving Rule Scan Time: Use a different scan time for each moving rule. The moving rule scan time is used by the selected moving rule only. If 'Use Moving Rule Scan Time' is enabled then the common scan time is ignored (for the selected moving rule).
- ▶ Disable Scan Time: This will disable the scan time function for the selected moving rule. Useful if you only want to use Scheduled Events.

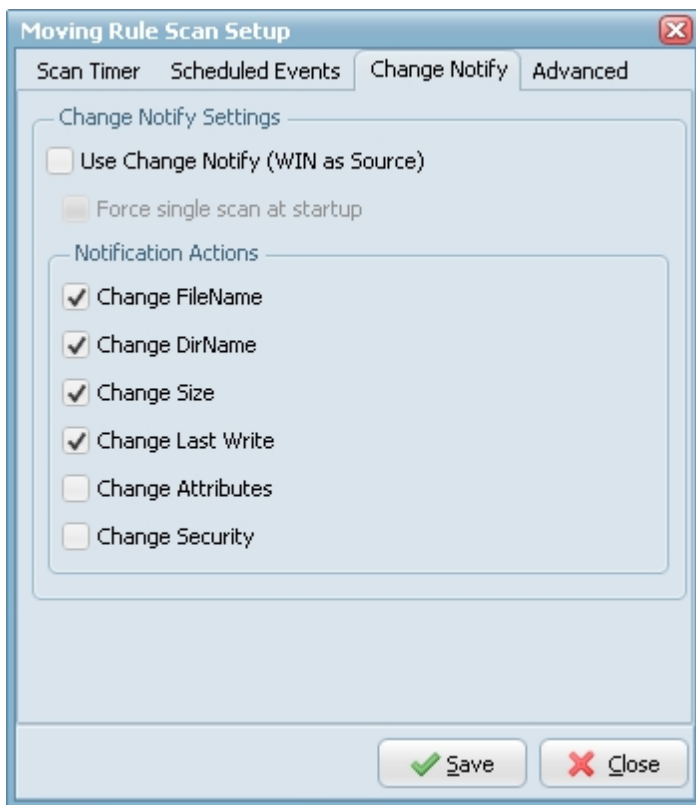
Scheduled Events



- Use Scheduled Events: Use Scheduled Events to trigger the selected moving rule.

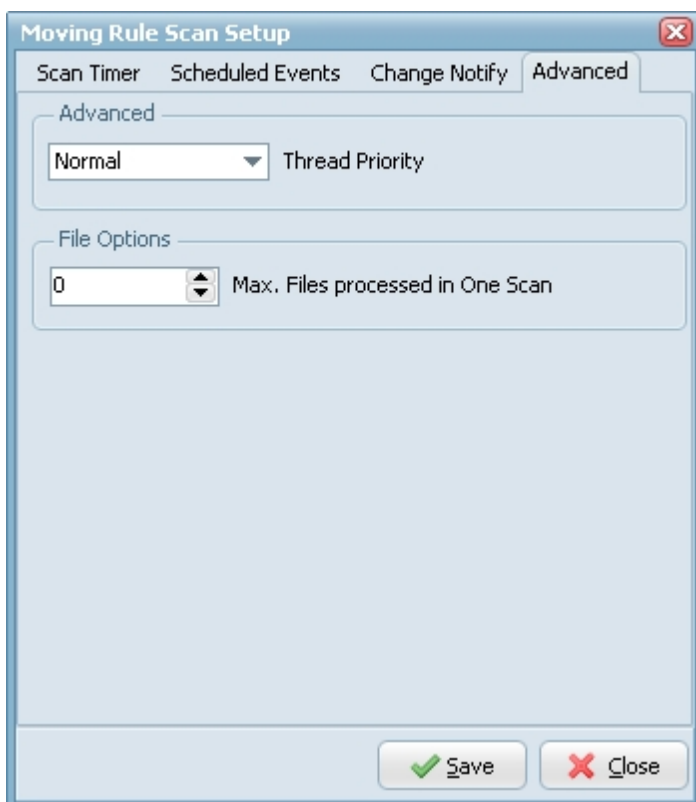


Change Notify



- **Use Change Notify (WIN as Source):** Use the OS change notify event to trigger the moving rule. Only for WIN as source.
- **Force single scan at startup:** This will trigger the rule at startup even if we don't get an notify event from the OS.

Advanced







- **Thread Priority:** Priority indicates how much preference the thread gets when the operating system schedules CPU time among all the threads in your application. Use a high priority thread to handle time critical tasks, and a low priority thread to perform other tasks.

- ▶ Max. Files at Once: Maximum files that LimagitoX will pickup during a scan (default = 0 = No Limit)

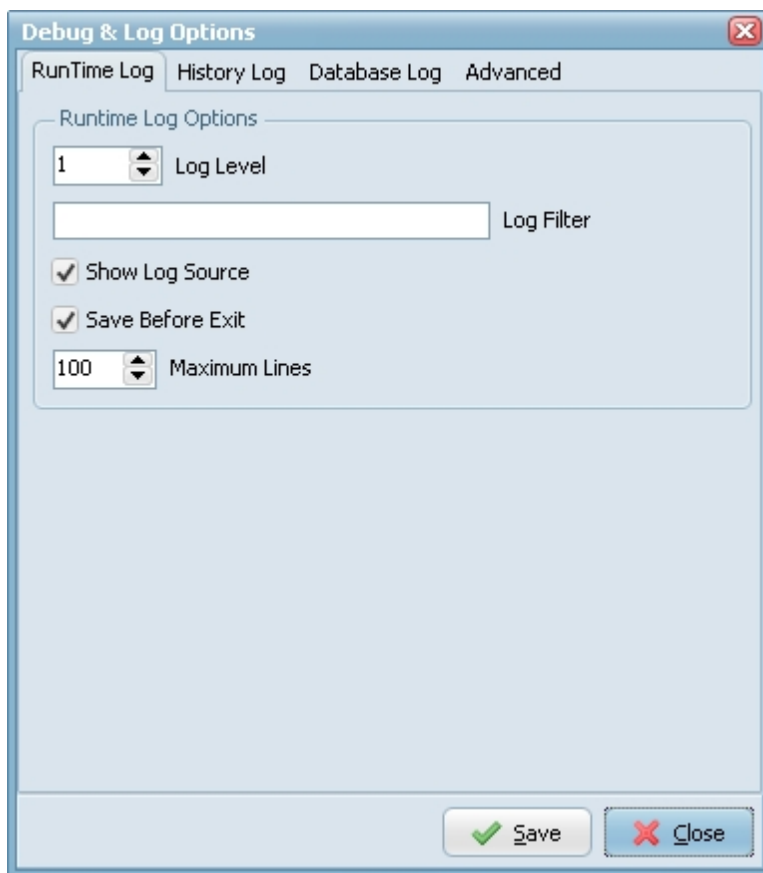
Logging

Logging

-  [RunTime Log](#)
-  [History Log](#)
-  [Database Log](#)
-  [Advanced](#)

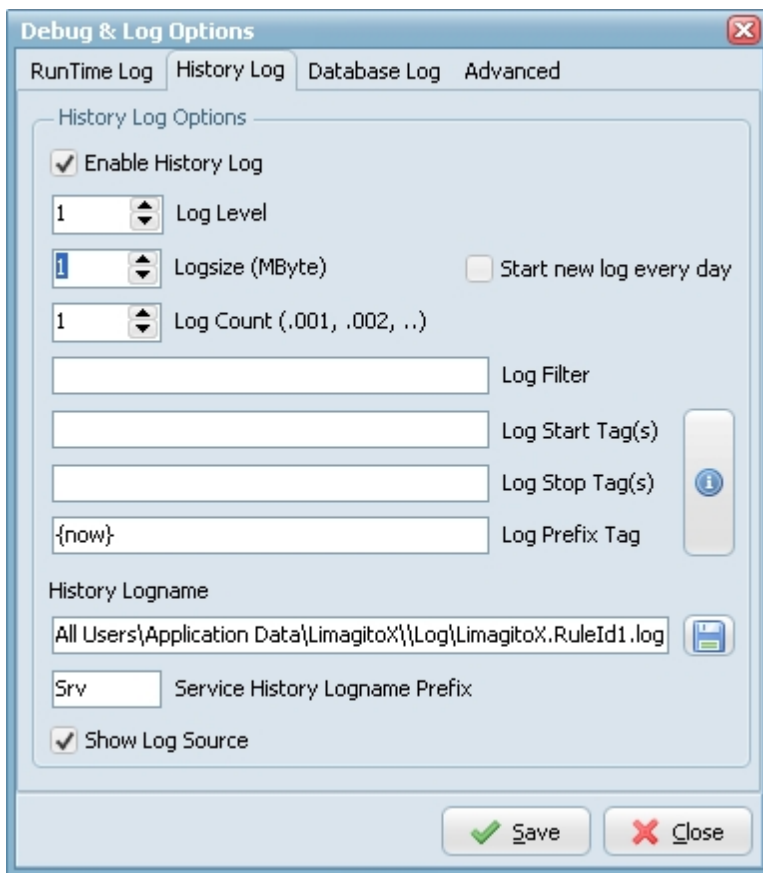
RunTime Log


Runtime Log



History Log

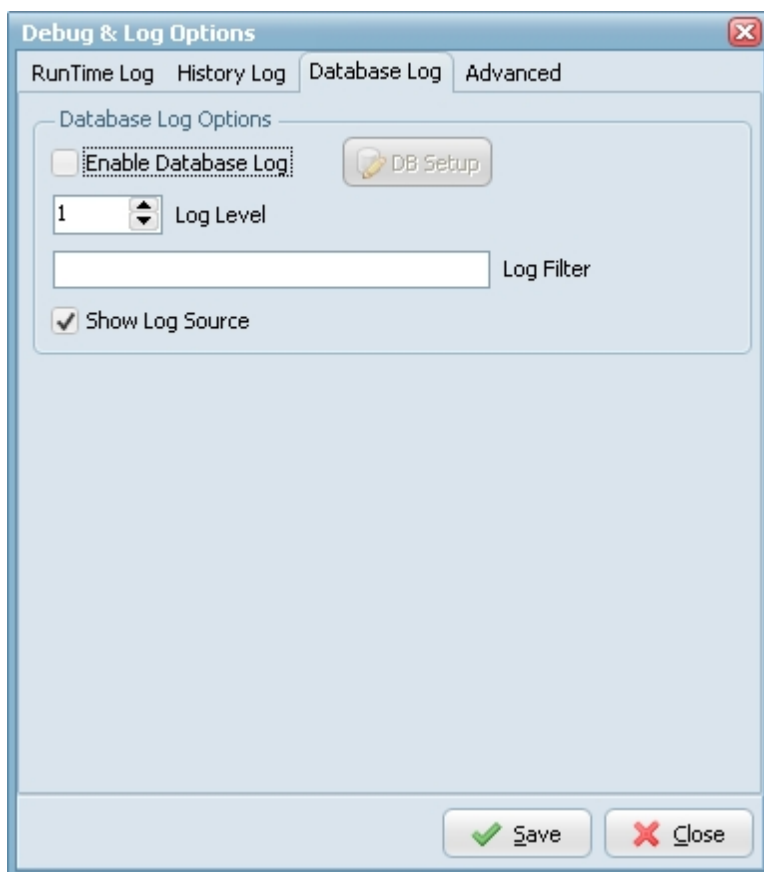
History Log



- ▶ Enable History Log: Enable logging to file for the selected thread (moving rule).
- ▶ Setup Log: Setup log options for the selected Limagito thread.
- ▶ Logging Level 1-10: Increase the log level if you need more 'debug' information (default 1). Don't use level 10 during production, only for testing.
- ▶ Log Size: Set the maximum size for the log file.
- ▶ Log History Count: If log size is reached then the .log file will be renamed to .001. With this option you can set the amount of history files.
- ▶ History Log Filter: You can add more then one Log Filter each separated by ';' (i.e. error;exception). This will limit the information in the History Log.
- ▶ RunTime Log Filter: You can add more then one RunTime Log Filter each separated by ';' (i.e. error;exception). This will limit the information in the RunTime Log.
- ▶ Log Start Tag(s): 
- ▶ Log Stop Tag(s):
- ▶ Log Prefix Tag:
- ▶ Log Filename: Select the filename for the log file.
- ▶ Save: Save log setup.

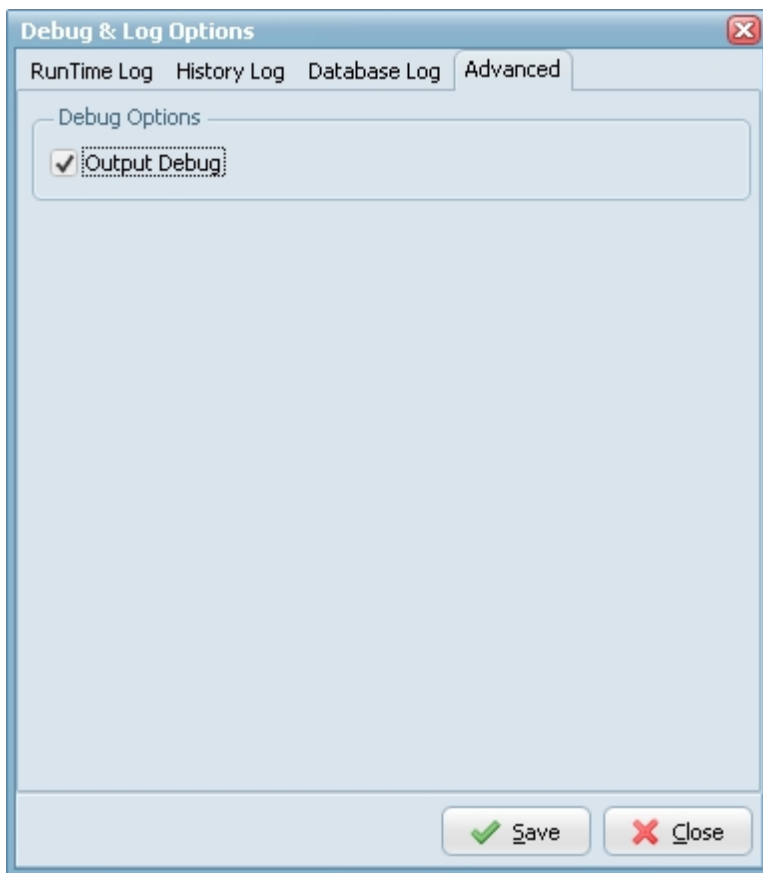
Database Log

Database Log



Advanced

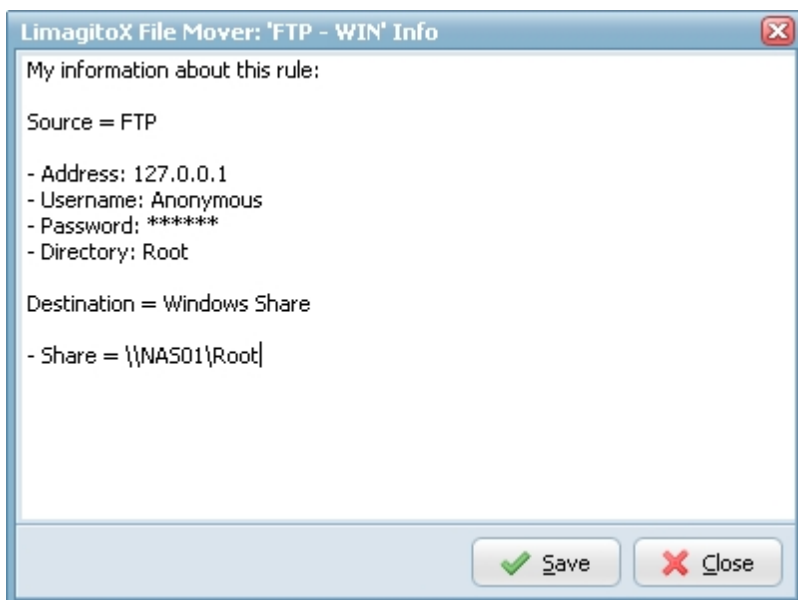
Advanced



- ▶ **Output Debug:** Output debug information for the selected rule. This gives you full debug capability when using a debug monitor (DebugView, freeware at <http://technet.microsoft.com/en-us/sysinternals/default.aspx>).

Rule Info

Rule Info



Here can can add your own information about the selected rule. It will be stored in the settings database.

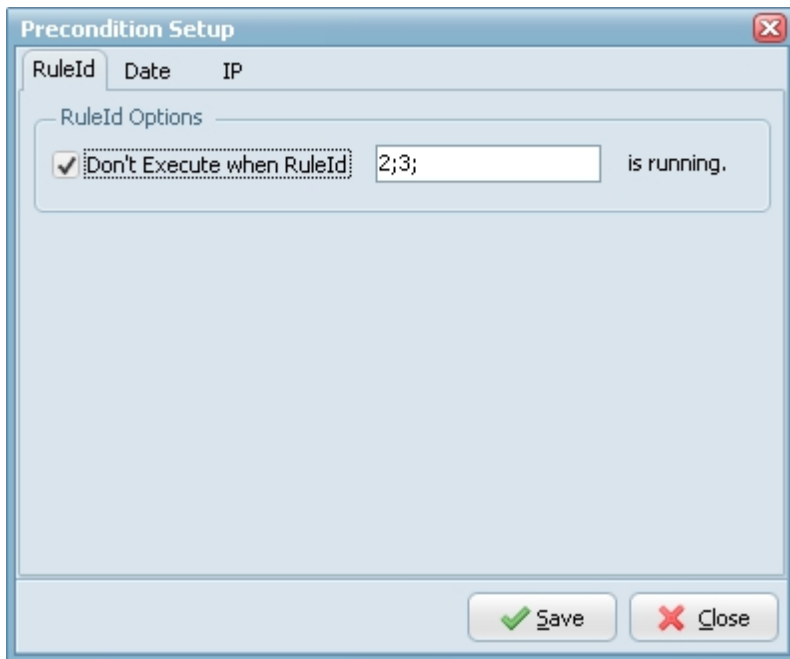
Precondition

Precondition

The precondition option let's you decide whether or not to execute the rule. When a rule is triggered it will check the

preconditions first. If they are valid then the rule will continue, otherwise it will wait on the next scan trigger. At this moment we have 3 preconditions that you can use.

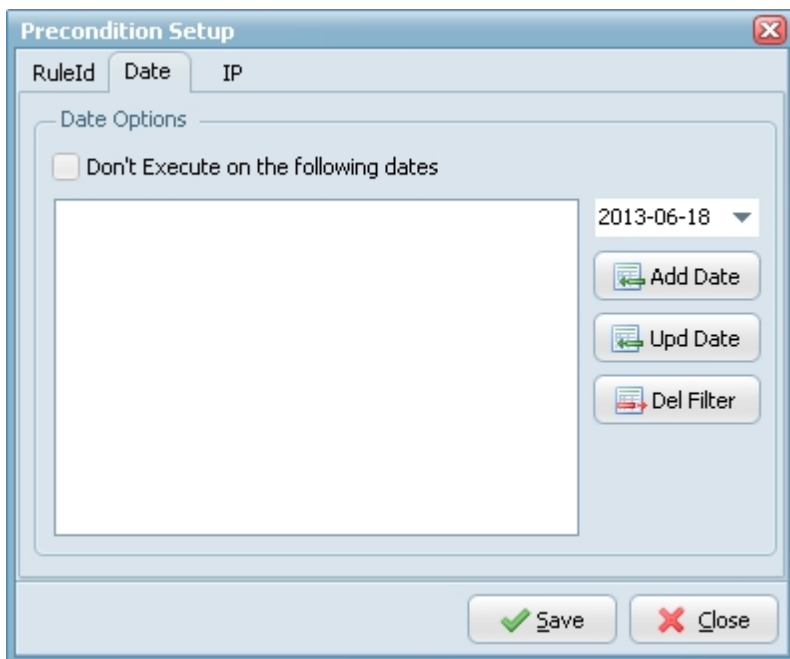
1. RuleId



- ▶ Don't Execute when RuleId ? is running: You can use this precondition when you need to be sure that other rule(s) aren't running. In the example above the rule won't run when rule with Id 2 or Id 3 is running. You can find the rule Id next to the rule name.

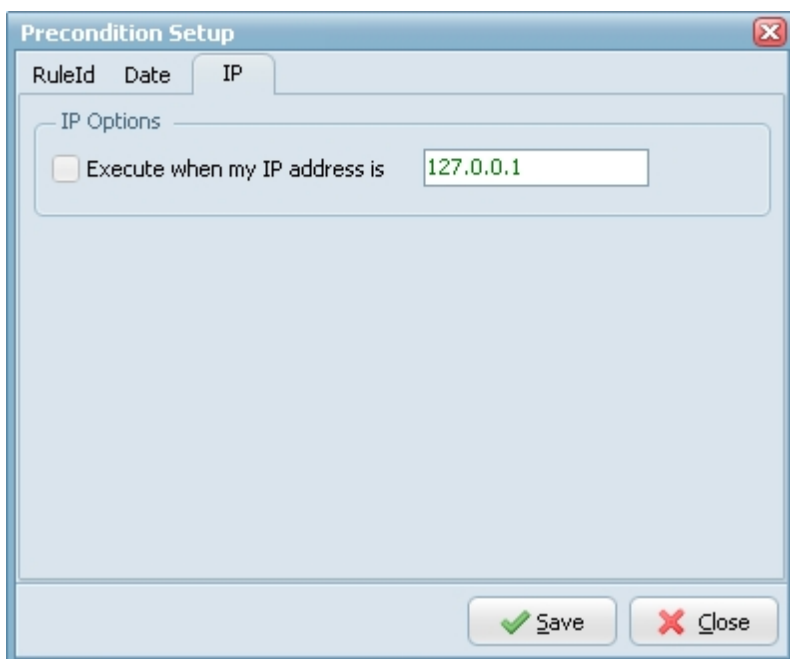


2. Date



- ▶ Don't Execute on the following dates: The rule won't run on the added dates.

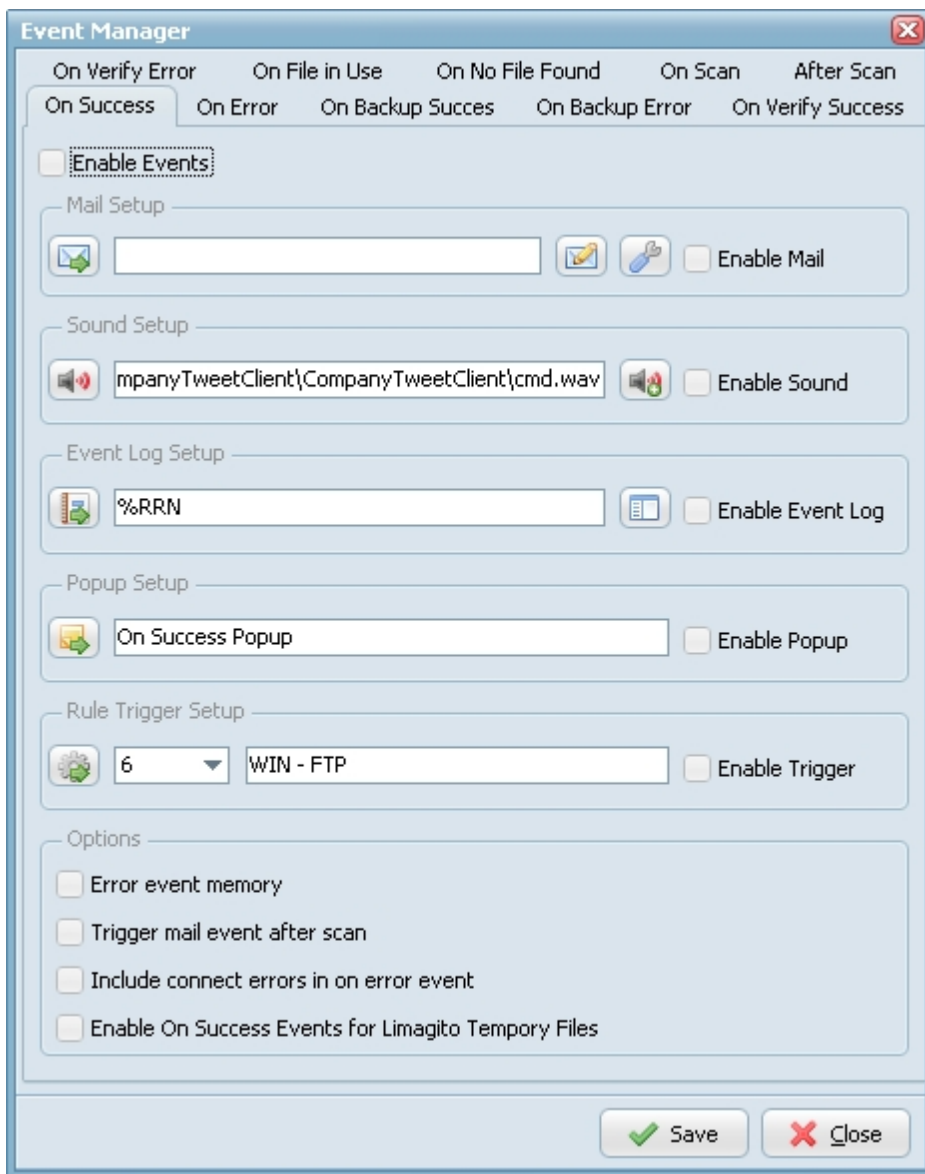
3. IP



- ▶ Execute when my IP address is ?: The rule will check the IP address of the host. If this isn't correct then the rule won't start. Often used when LimagitoX is installed on 2 servers. One of the servers is the active server, the other one is the backup server. The active server gets a common IP address. The rule only needs to run on the active server.

Rule Events

Rule Events

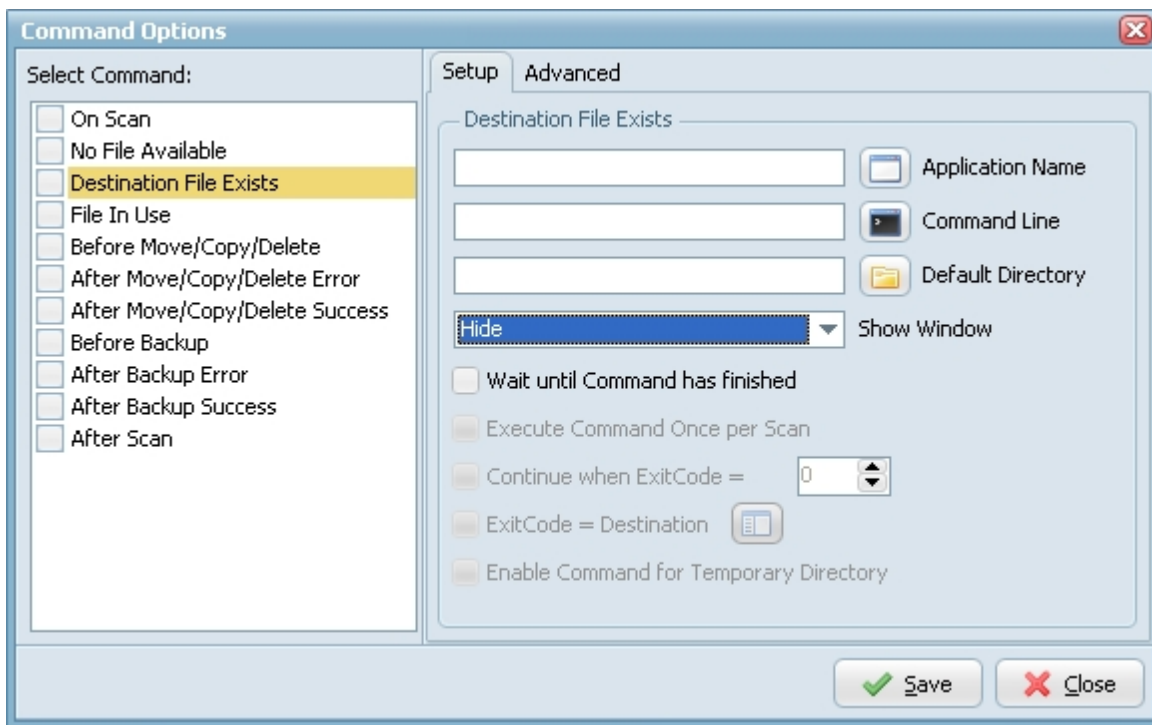


- ▶ Error event memory: Trigger error events only once for the same file.
- ▶ Trigger mail events after scan: Trigger mail events after scan instead of for each file. When this option is enabled only mail parameter %FN (Filename) can be used.

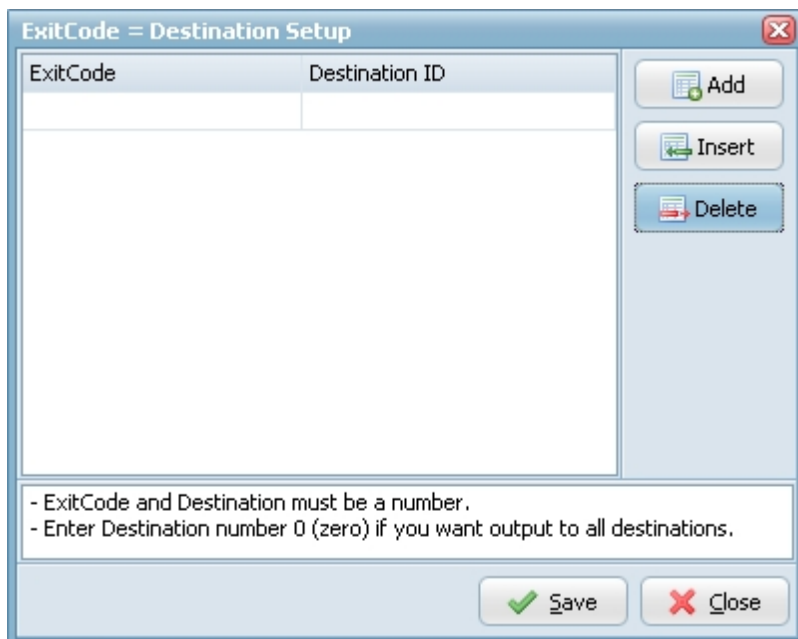
Command

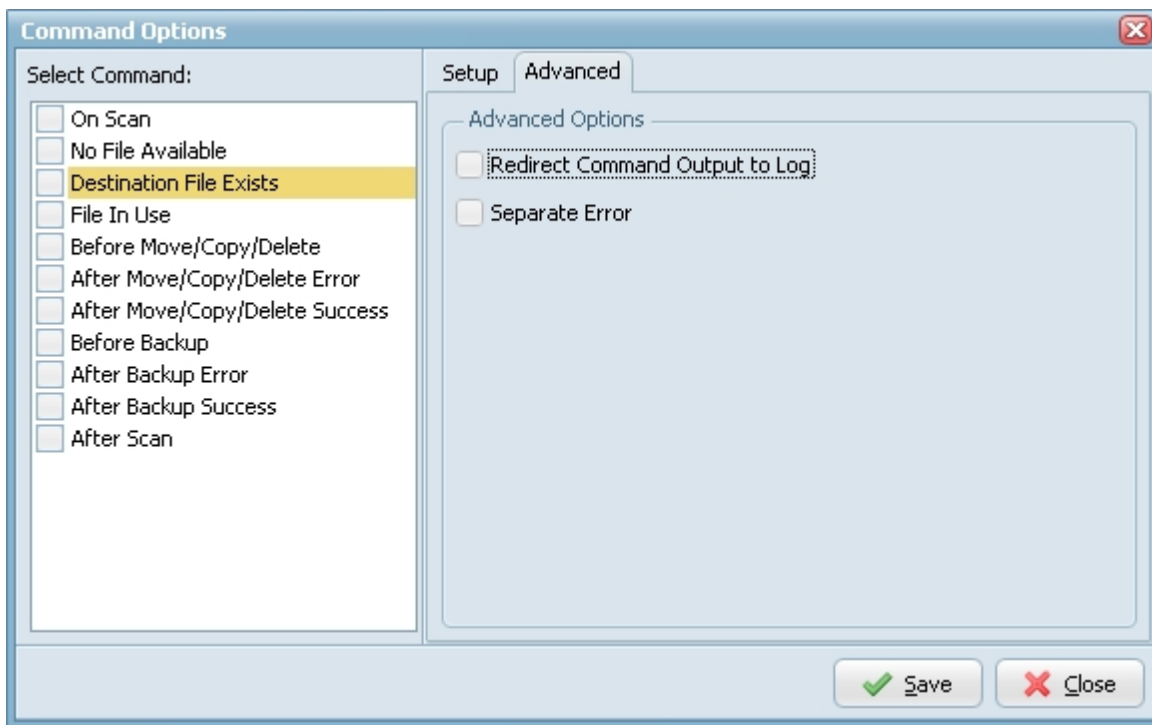
Command

Use the Command option to execute an external (command line) application.



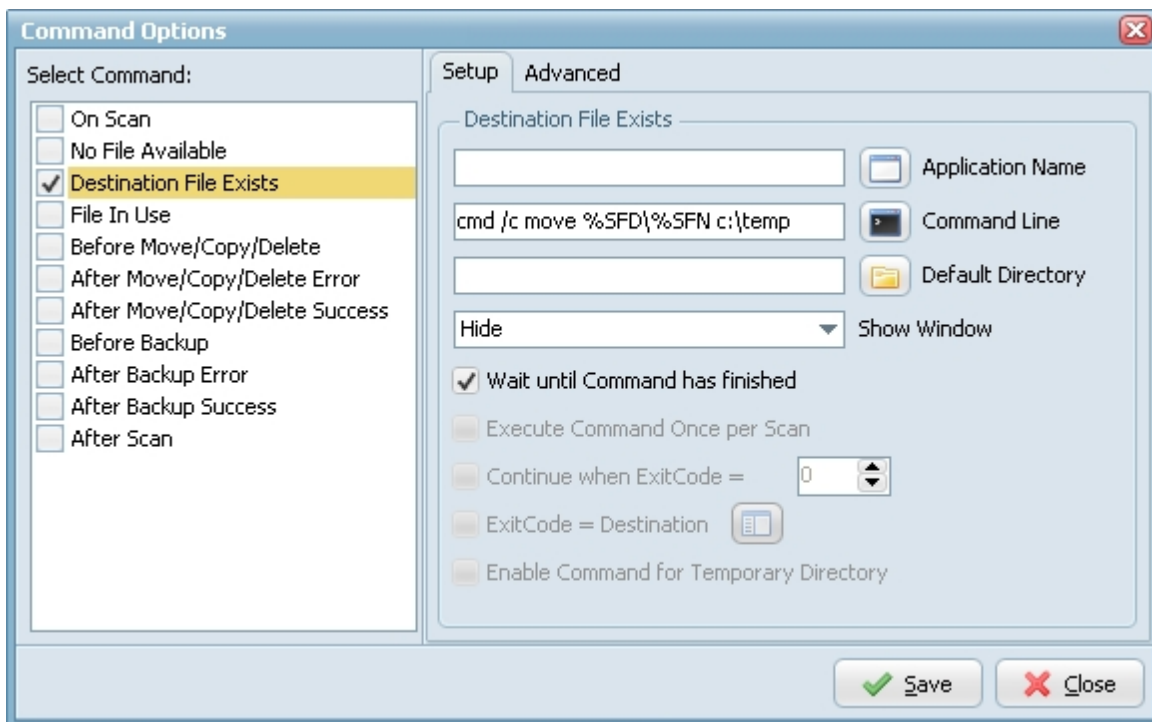
- ▶ Wait until command has finished: The rule will only continue when the (command line) application is finished.
- ▶ Execute command once per scan: The (command line) application will only be executed once during a scan (not with every source file).
- ▶ Continue when ExitCode is: Check the ExitCode of the (command line) application and decide if you want to continue.
- ▶ ExitCode = Destination: Let the ExitCode of the (command line) application decide which destination the rule will use.





- ▶ Enable command for temporary directory:
- ▶ Redirect Command Output to Log:
- ▶ Separate Error:

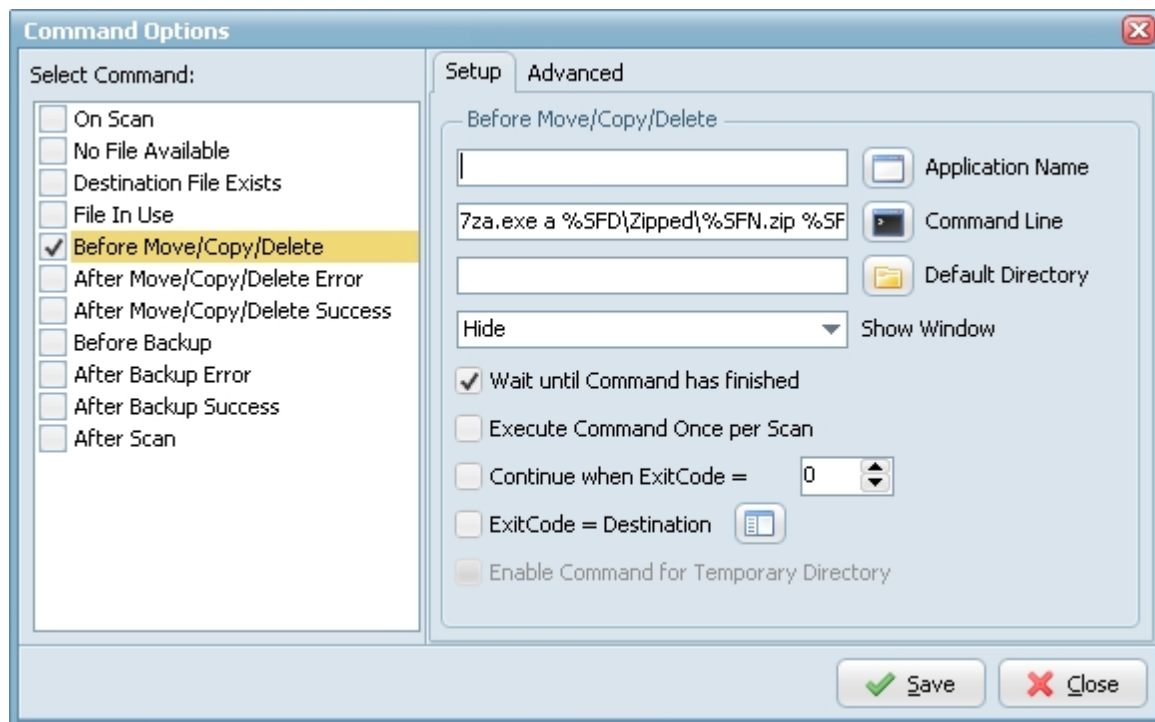
First example:



In the first example we're going to move the source file to a temp directory if this file exists in the destination directory. We are using the 'Destination File Exists' command option. The 'Application name' is empty. This depends on what you are going to execute. We are using a command line instruction.

Command: `cmd /c move %SFD%\%SFN c:\temp`

cmd /c	Carries out the command and then terminates
move	Moves files and renames files and directories.
%SFD%\%SFN	Source (Source file directory + filename)

Second example:

In this example we're going to zip the source file using the command line version of 7zip. (7za.exe download at <http://www.7-zip.org>). We are going to use the 'Before Move/Copy/Delete' command option. The 'Application Name' is empty. This depends on what you are going to execute. We are using a command line application.

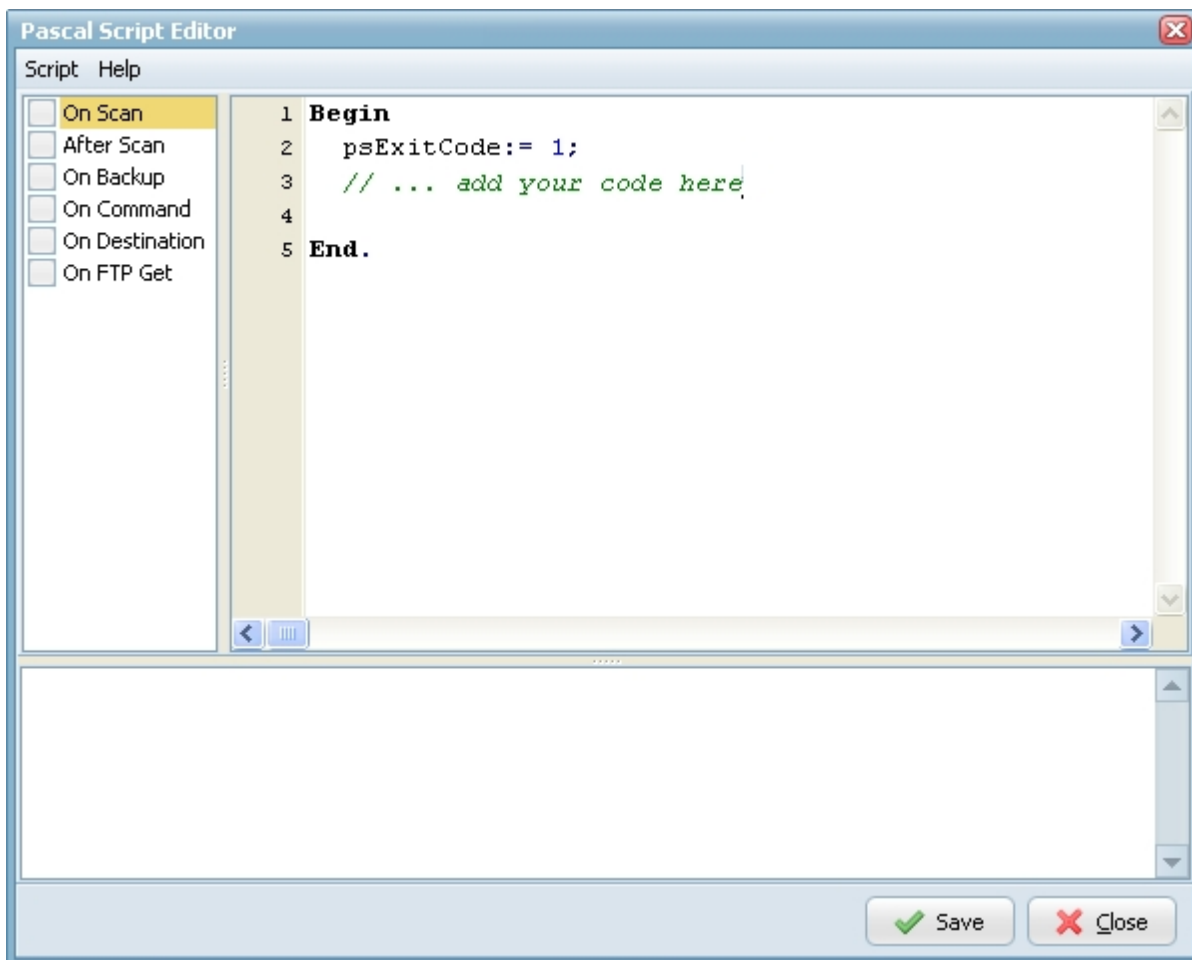
Command: **7za.exe a %SFD\Zipped\%SFN.zip %SFD%FN**

7za.exe	7Zip Command line exe file
a	7Zip archive command
%SFD\Zipped\%SFN.zip	Destination, Zipped filename (Destination directory + filename)
%SFD%SFN	Source, Unzipped filename (Source directory + filename)

Input files are zipped into the subfolder 'zipped'. The extension .zip is added to the original filename.

Pascal Script

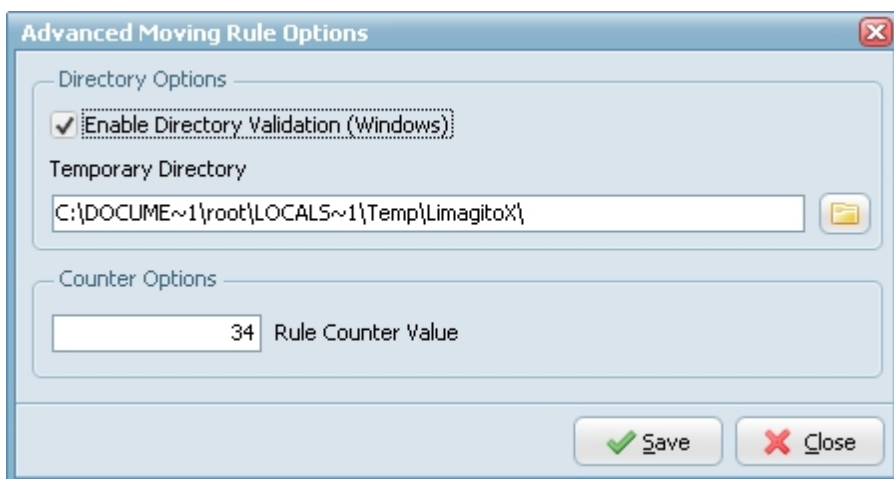
Pascal Script



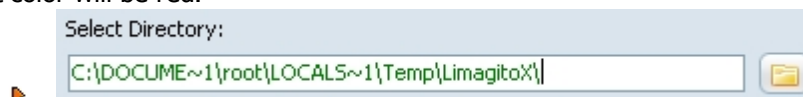
With Pascal Script we (and you as user) can create customized options. It helps us to create options that are user specific. We can not add all user request as a new option within our application. Only available with a Site or Corporate license.

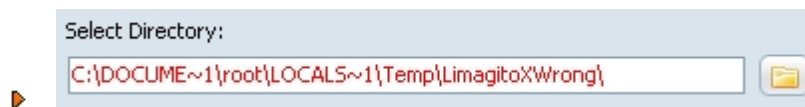
Advanced

Advanced



- ▶ **Enable Directory Validation (Windows):** When a selected directory is valid the font color will be green, when not the font color will be red.



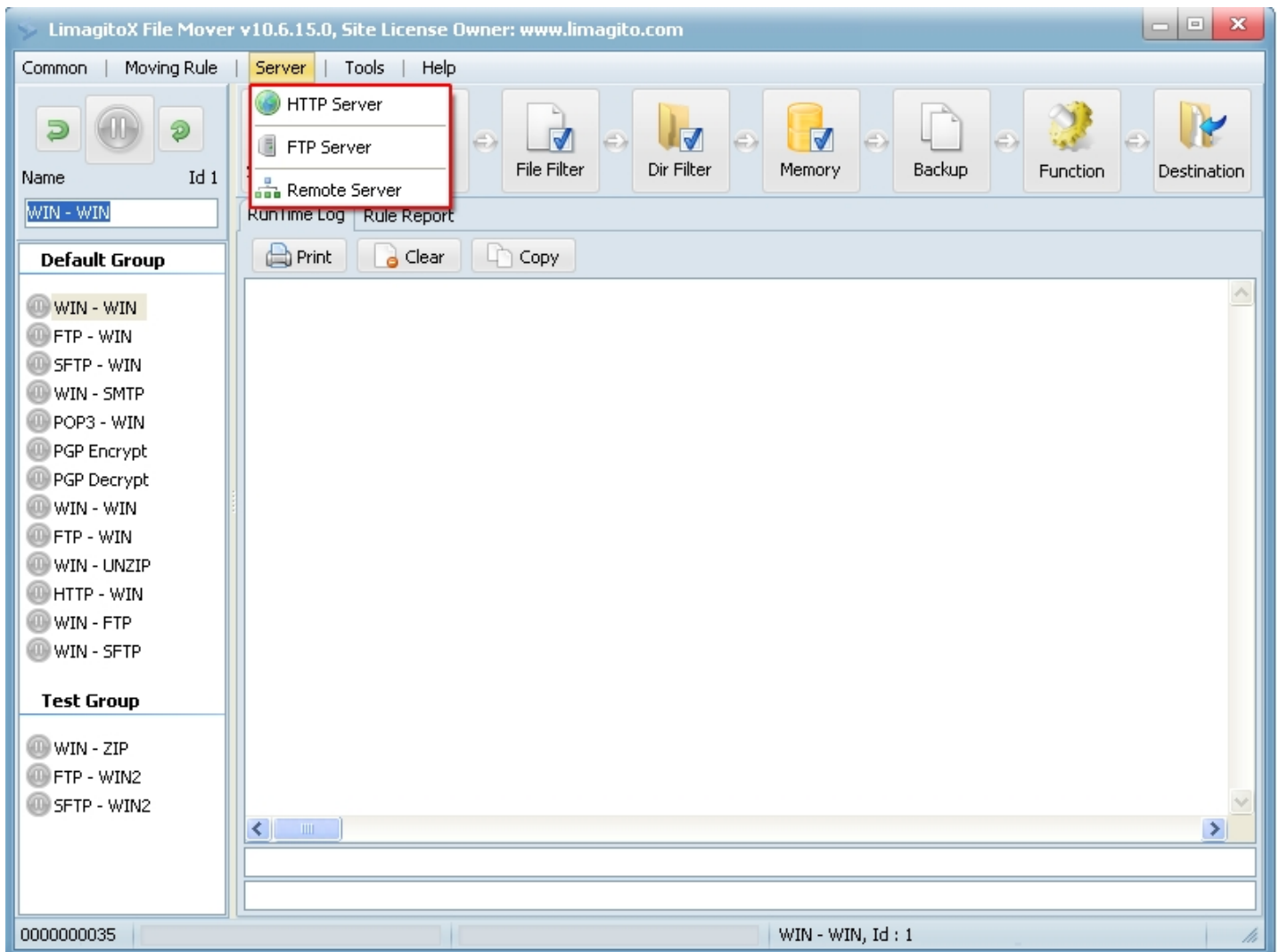


- ▶ Temporary Directory: Temporary directory created and used by LimagitoX.
- ▶ Counter Options: With this option you can change the current value of the rule counter.

Server Options

Server

- [HTTP Server](#)
- [FTP Server](#)
- [Remote Server](#)



HTTP Server

HTTP Server

With the built in HTTP server you can consult the RunTime log using a web browser. Often used when using LimagitoX as a service. This way you can monitor what the service is doing without the need to open log files.

Http Server Setup - Rule : WIN - WIN

Server Setup HTML HEAD HTML BODY TOP HTML BODY BOTTOM

☐ Enable Http Server

Http Server Setup

127.0.0.1 IP

8080 Port

☐ Enable Http Root Directory (Everyone Read-Only)

C:\DOCUME~1\root\LOCALS~1\Temp\ 

Http RunTime Log Setup

Global Username

Global Password

Http RunTime Log Rule Setup

Rule Username

Rule Password

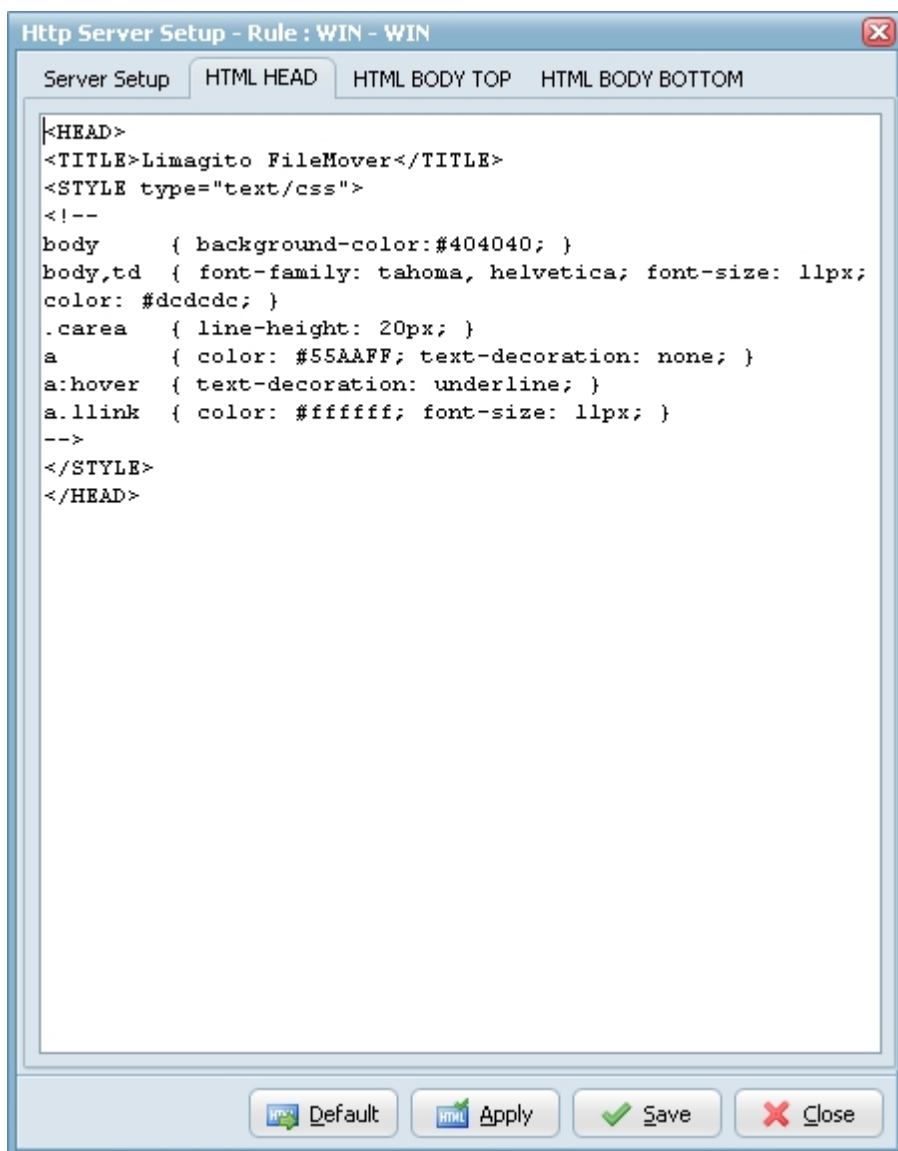
☒ Enable Execute ☐ Enable Clear All RunTime Logs

☐ Enable Hold ☐ Hide Moving Rule

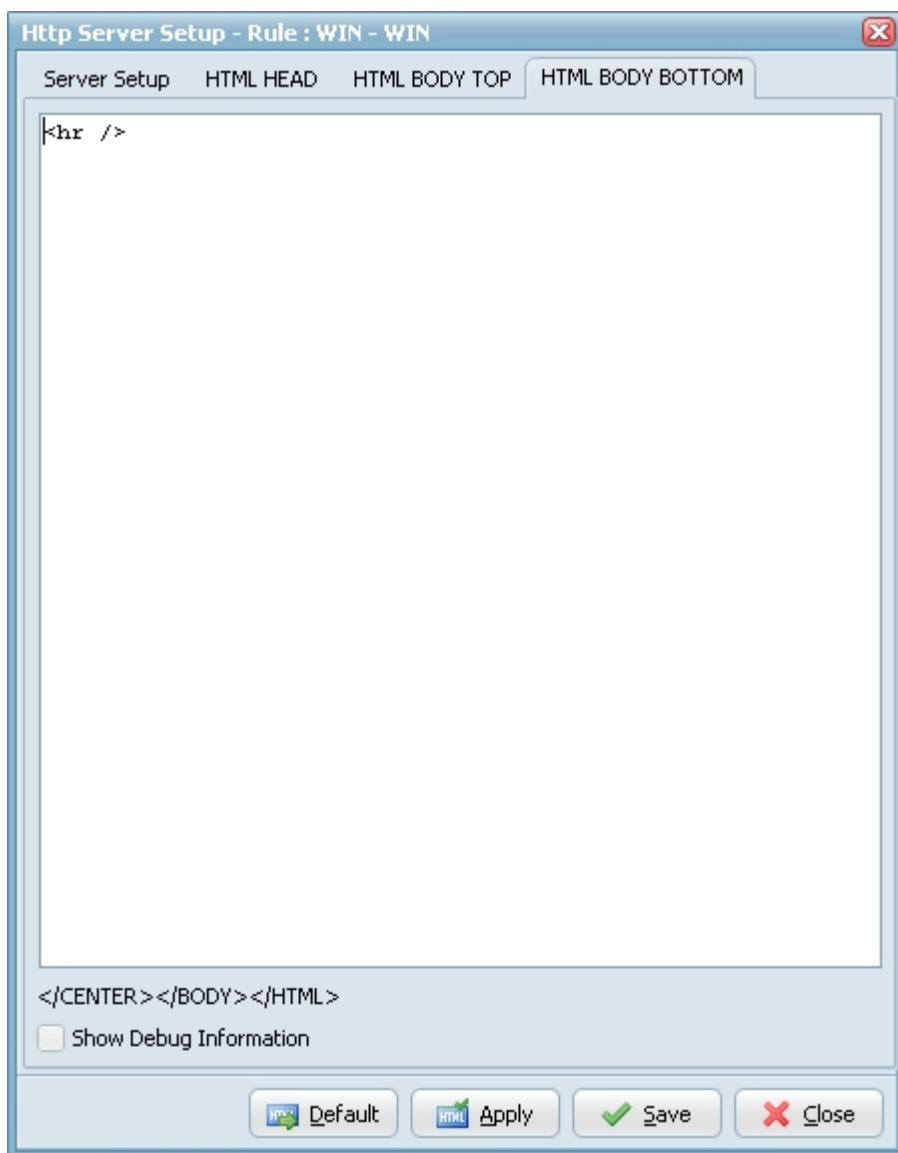
☐ Enable Clear RunTime Log

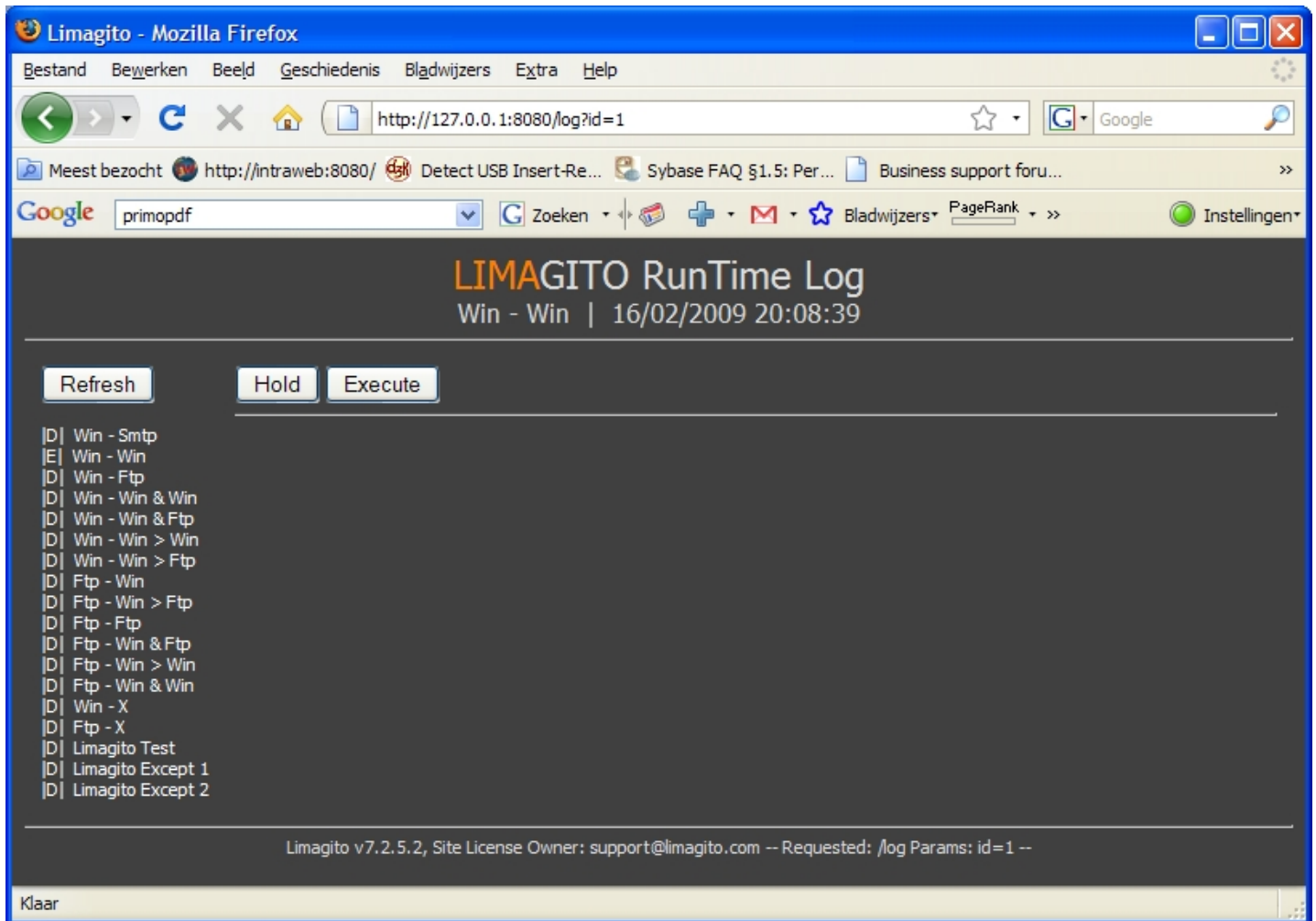
 Default  Apply  Save  Close

- ▶ Enable Http Server: enable build-in Http server for RunTime log.
- ▶ IP: Host name or IP address of Http server.
- ▶ Port: Port used by Http server.
- ▶ Global Username: Username to log into the Http server (= all rules).
- ▶ Global Password: Password to log into the Http server (= all rules).
- ▶ Rule Username en Rule Password: Extra Http Username and Password field for each moving rule. Now you can setup a different username and password for each moving rule http runtime log.
- ▶ Enable Execute, this will show the Execute button on the Limagito RunTime page.
- ▶ Enable Hold, this will show the Hold button on the Limagito RunTime page.









FTP Server

Work in progress

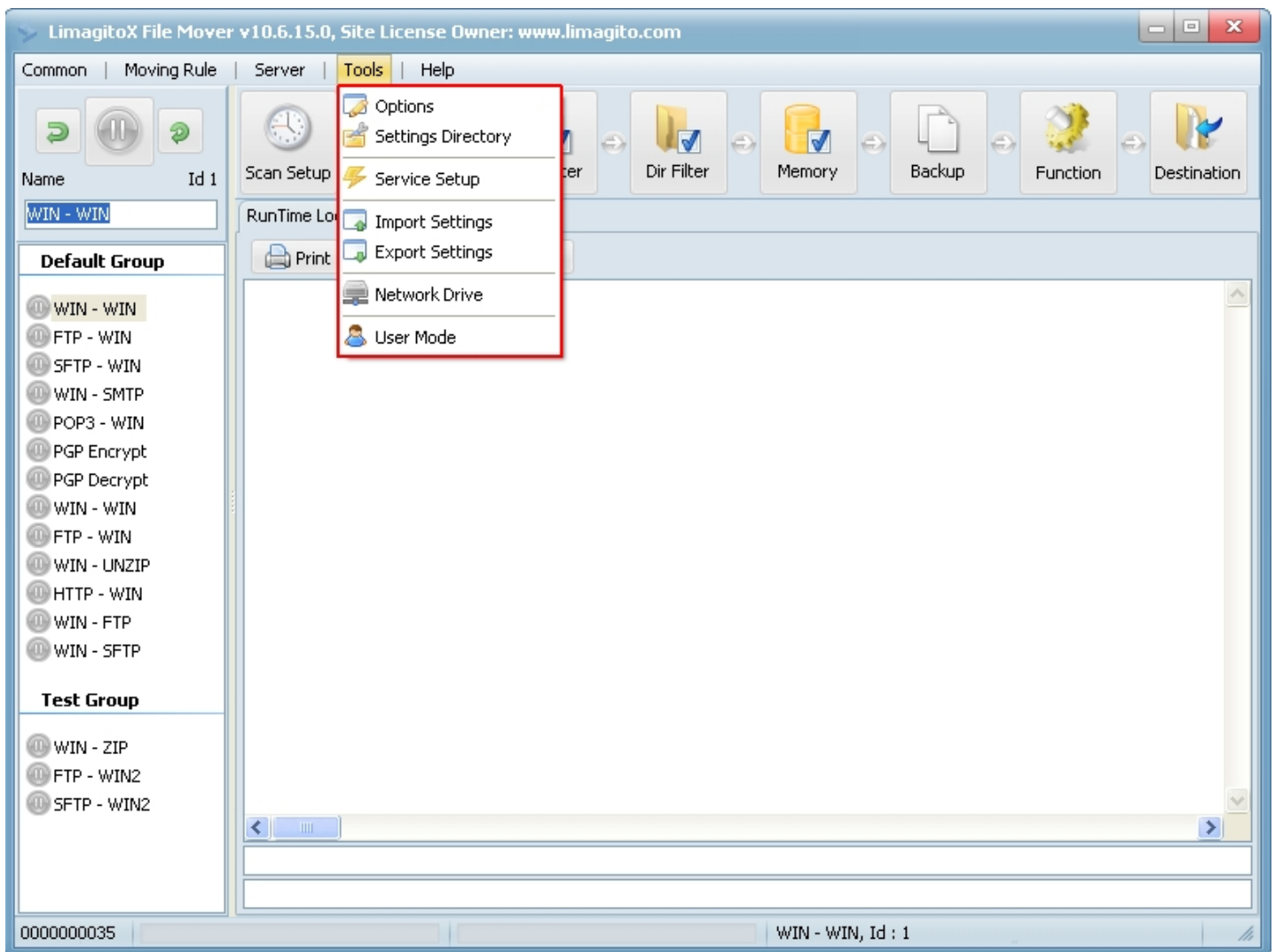
Remote Server

Work in progress

Application Options

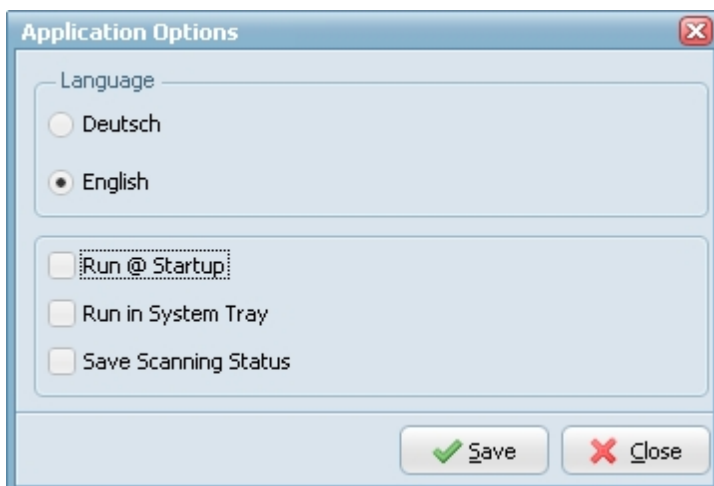
Tools

- [Options](#)
 - [Settings Directory](#)
 - [Service Setup](#)
 - [Import Settings](#)
 - [Export Settings](#)
 - [Network Drive](#)
 - [User Mode](#)



Options

Options



- ▶ Run @ Startup: LimagitoX will automatically run at windows startup (entry in the HKLM registry).
- ▶ Run in System Tray: LimagitoX will minimize into the system tray at startup.
- ▶ Save Scanning Status: Scanning of all rules can be disabled manually using the ['Disable/Enable Scanning'](#) option. When this option is enabled, LimagitoX will use the last status at startup.



Settings Directory

Settings Directory

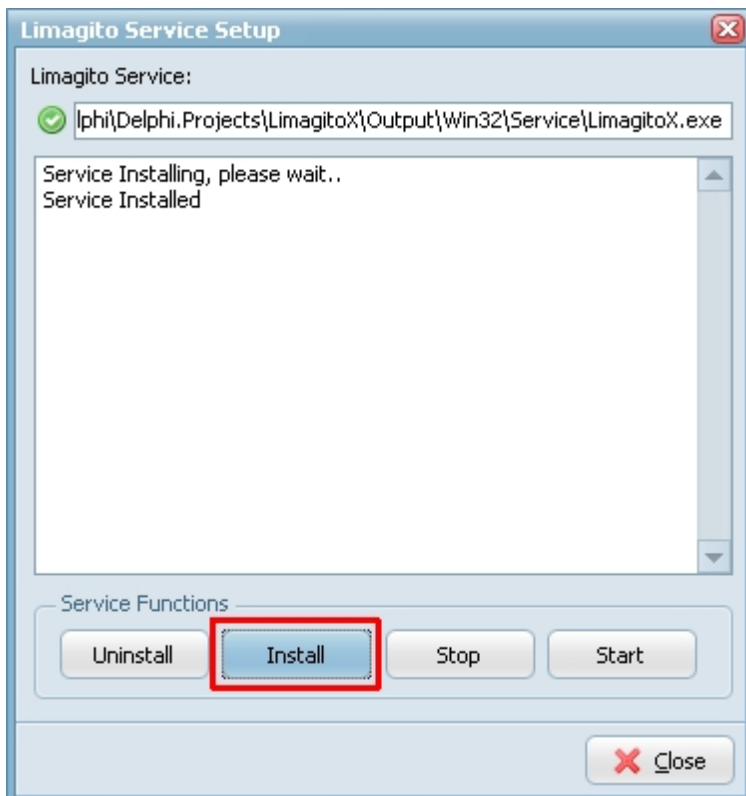
- ▶ Use the 'Settings Directory' option to find where LimagitoX FileMover stores its settings. You can find all settings, except the Run @ Startup, in this directory. The Run @ Startup option is stored in the Windows registry. The settings directory depends on the OS you're using and should contain the following subdirectories:
 - ▶ \Bak : Contains 7 backups of "LimagitoX.sqlite". LimagitoX.sqlite contains most settings of LimagitoX.exe (Application and Service version).
 - ▶ \Log : Default Log Directory of LimagitoX File Mover.

Service Setup

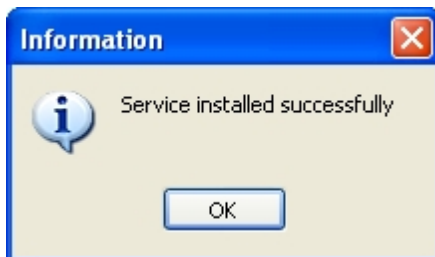
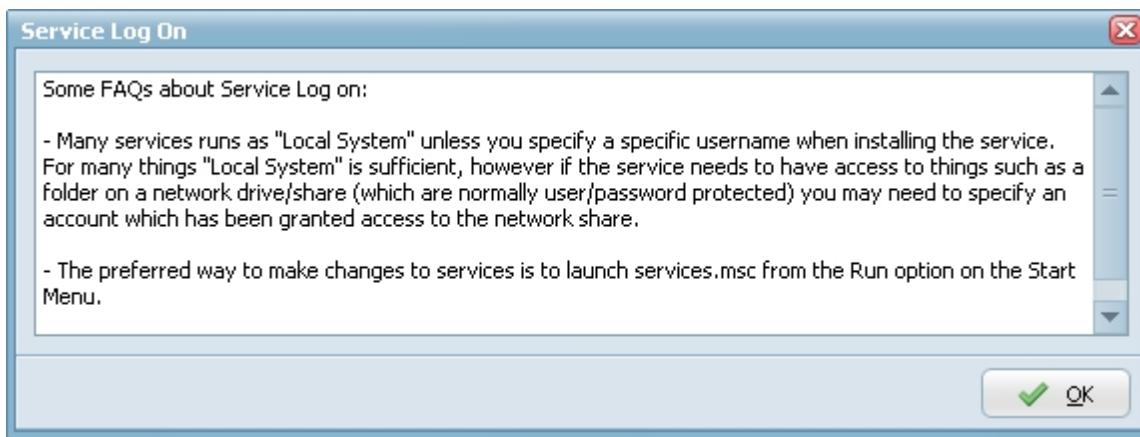
Service Setup

With the service setup you can install, uninstall, start and stop the LimagitoX service.

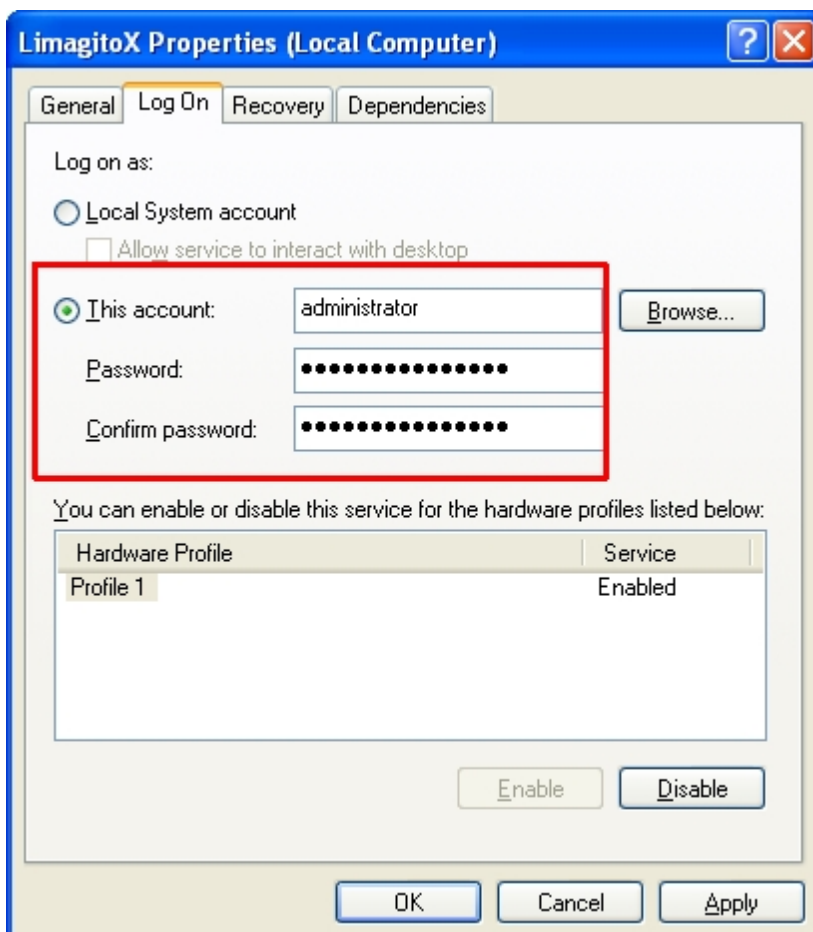
Install LimagitoX as a service using the 'Install' button.



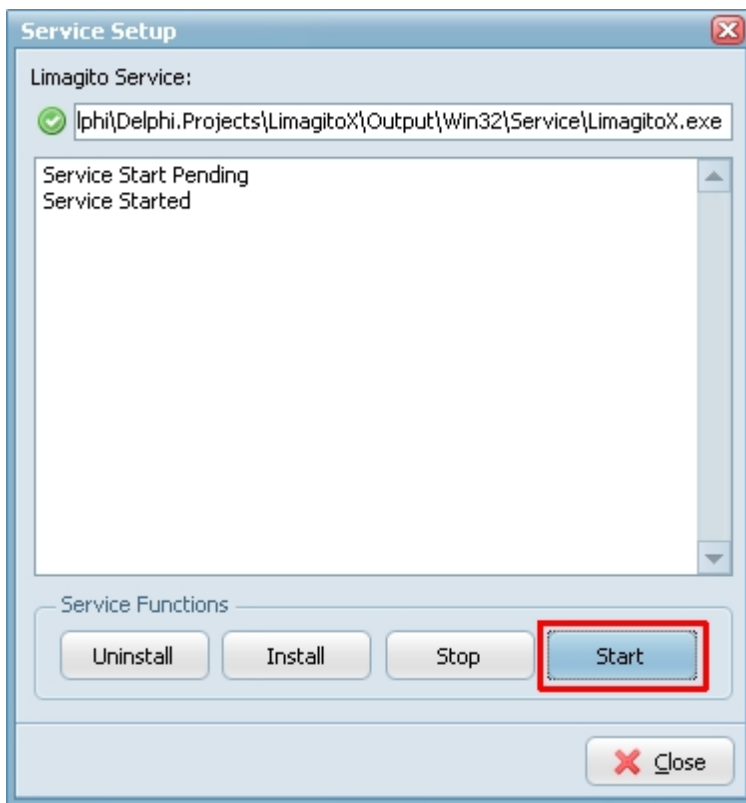
"Please read the following information carefully"



Adjust the "Log on as" account settings:



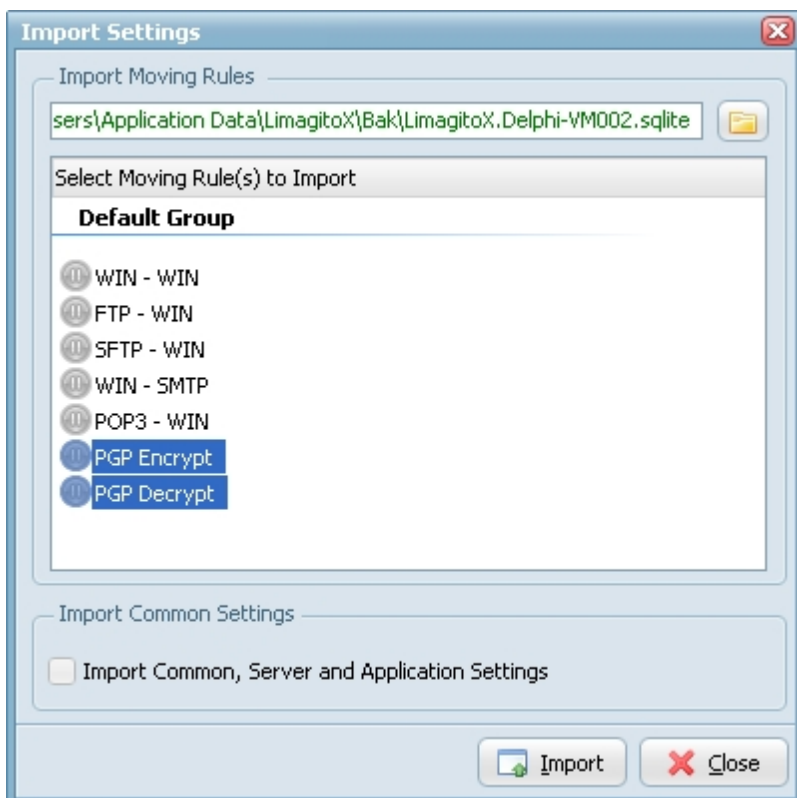
Start the LimagitoX service:



Exit the LimagitoX application. We don't want the application version to interfere with the running LimagitoX service.

Import Settings

Import Settings

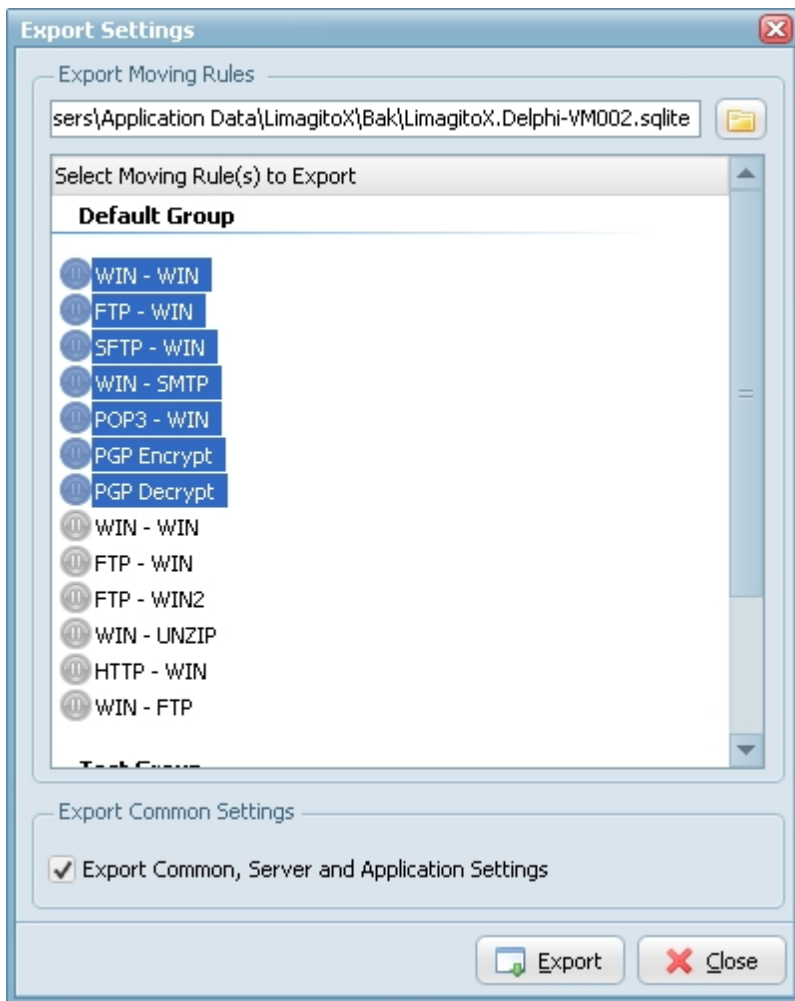


- First: Select the moving rule export file (.sqlite).
- Second: Select the moving rules you want to import.
- Third: Select if you want to import the common, server and application too (if they exist in the export .sqlite file).

- ▶ Last: Click on 'Import' button
- ▶ Done

Export Settings

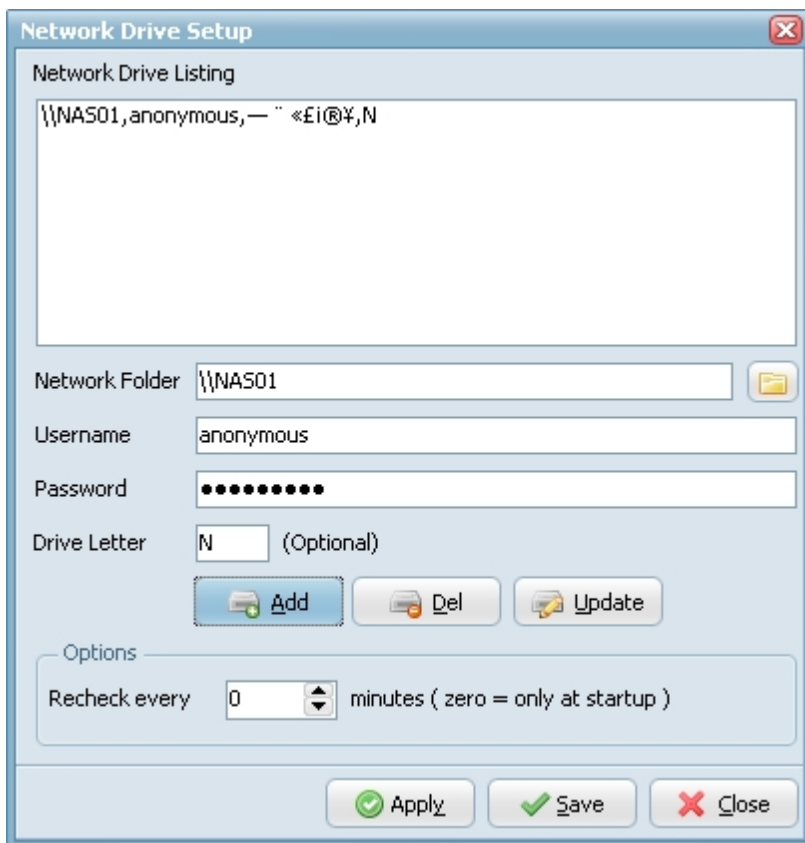
Export Settings



- ▶ First: Select the directory where you want to put the export file.
- ▶ Second: Select the moving rules you want to export.
- ▶ Third: Enable 'Export Common, Server and Application Settings' if you also want to export common, server and application options.
- ▶ Last: Click on 'Export' button.

Network Drive

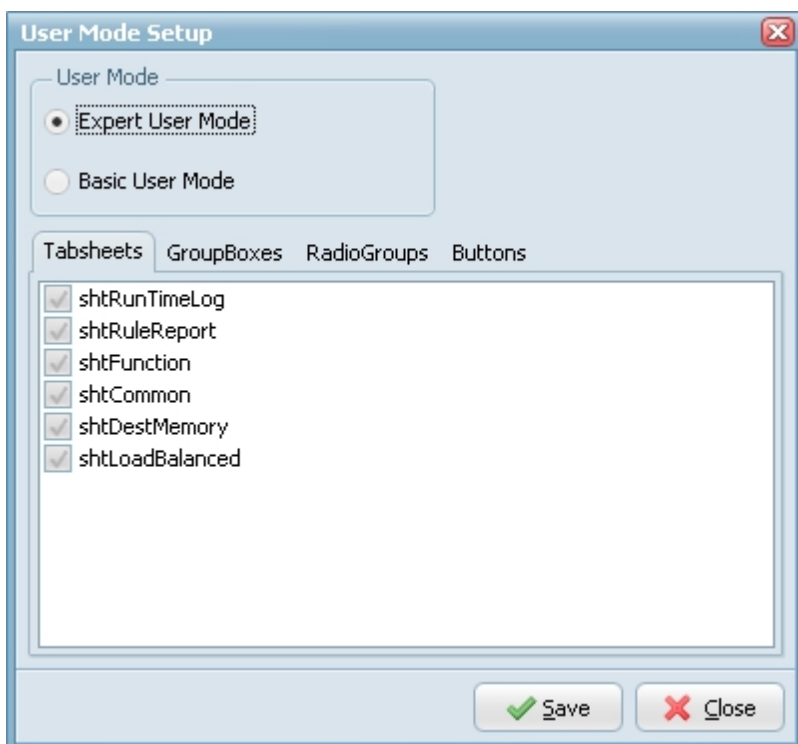
Network Drive



- ▶ Network Folder: network share you want to connect
- ▶ Username: username you need to provide when connecting to the share
- ▶ Password: password you need to provide when connecting to the share
- ▶ Drive Letter: the share will be available as the given drive letter (optional)
- ▶ Recheck every x minutes: check the availability of the share every x minutes (default = 0 = only at LimagitoX startup)

User Mode

User Mode

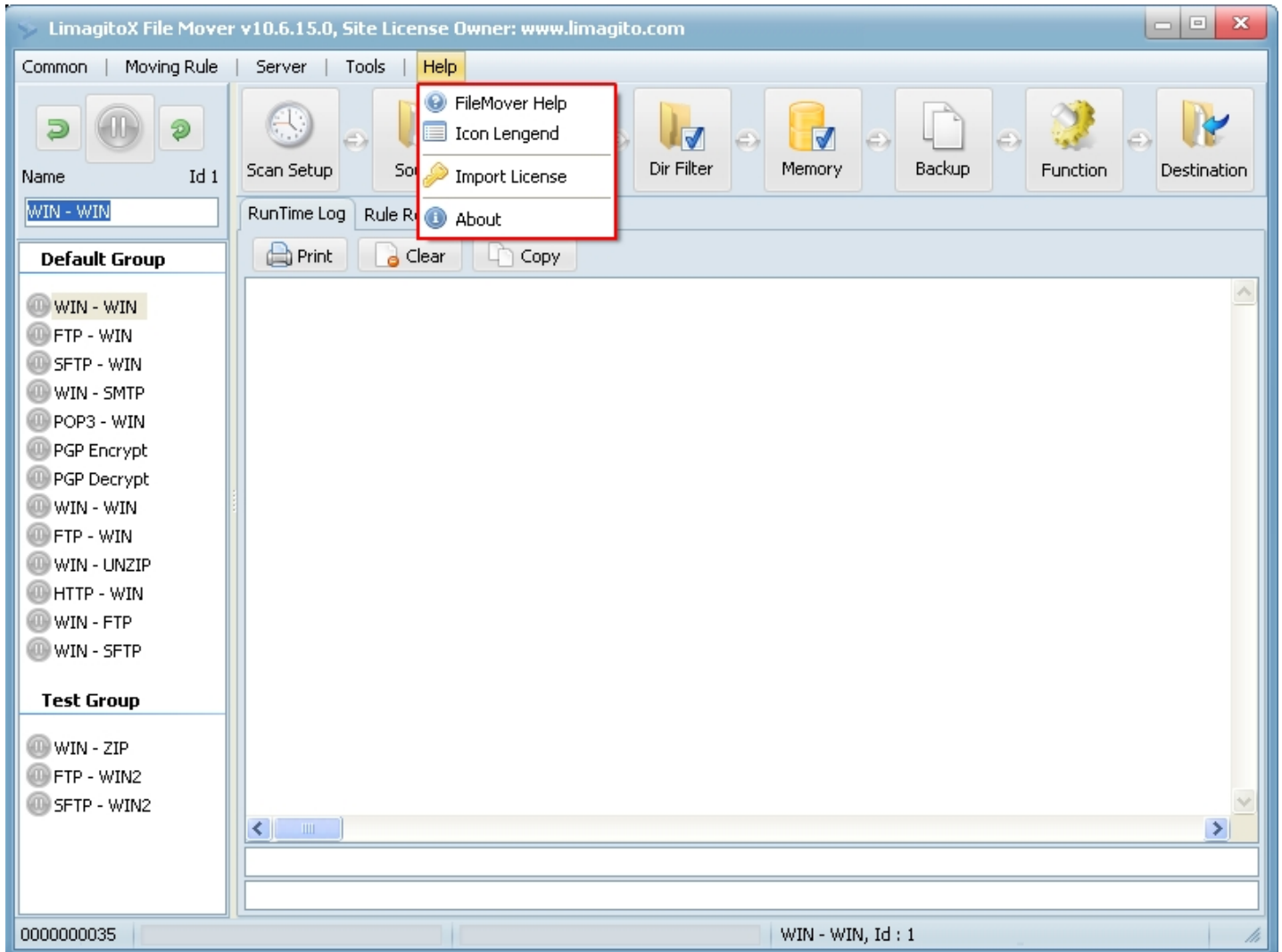


Disable Tabsheets, Groupboxes, Radiogroups and Buttons to create a Basic User Mode.

- ▶ Basic User Mode, Adjustable Setup
- ▶ Expert User Mode, Fixed Setup (all enabled)

Help Options

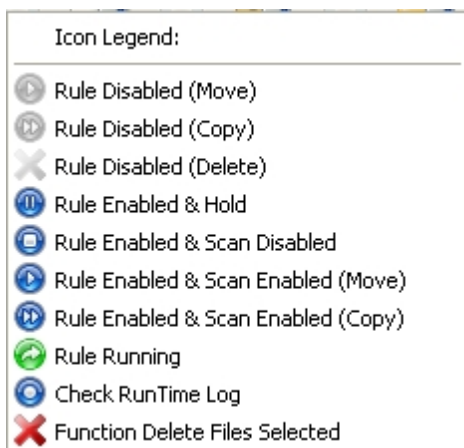
Help Options



FileMover Help

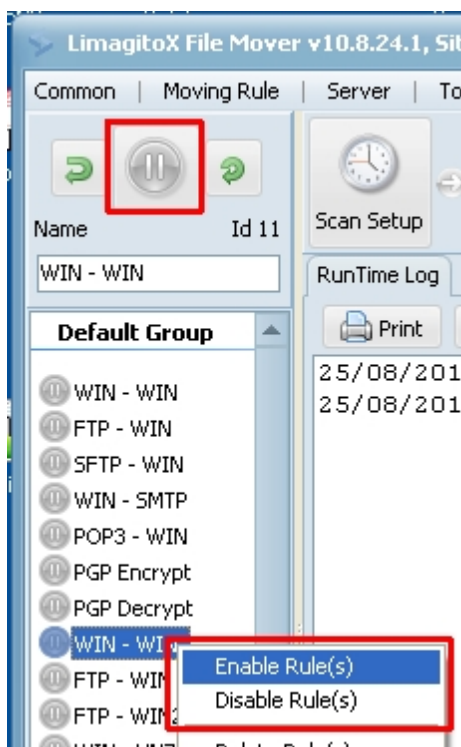
Open LimagitoX help file (help.chm).

Icon Legend

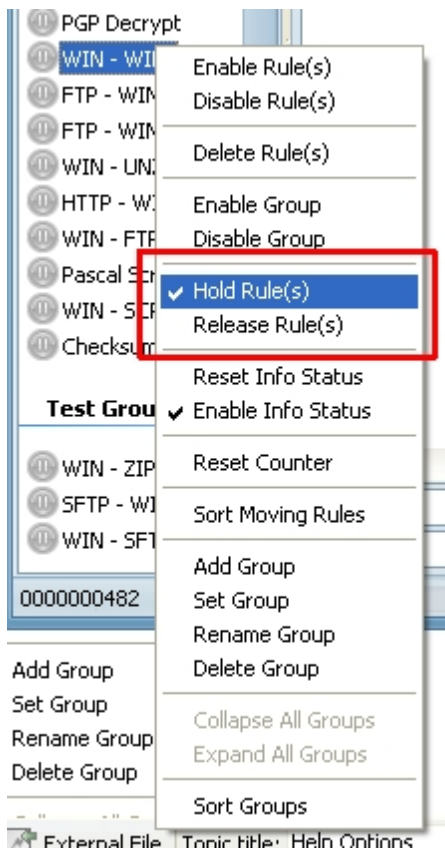


Possible Moving Rule status.

- ▶ Rule Disabled, the rule is inactive. The rule won't run even when you trigger it manually. Right click on the selected rule to 'Enable' or 'Disable' or click on the large status icon in the upper left corner to toggle it's status.



- ▶ Rule Enabled & Hold. The rule is enabled but in Hold status. An enabled rule can be put in hold or release status. This can be done using the integrated http server (web interface) or by right click on the selected rule and selecting 'Hold Rule' or 'Release Rule'. An enabled rule in hold won't run even when you trigger it manually.



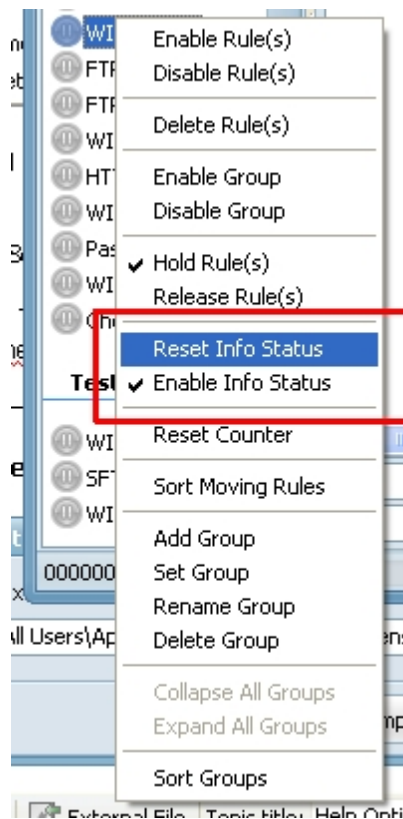
- ▶ Rule Enabled & Scan Disabled. Can be two reasons.

1. Scanning was disabled manually using the ['Disable/Enable Scanning'](#) option.

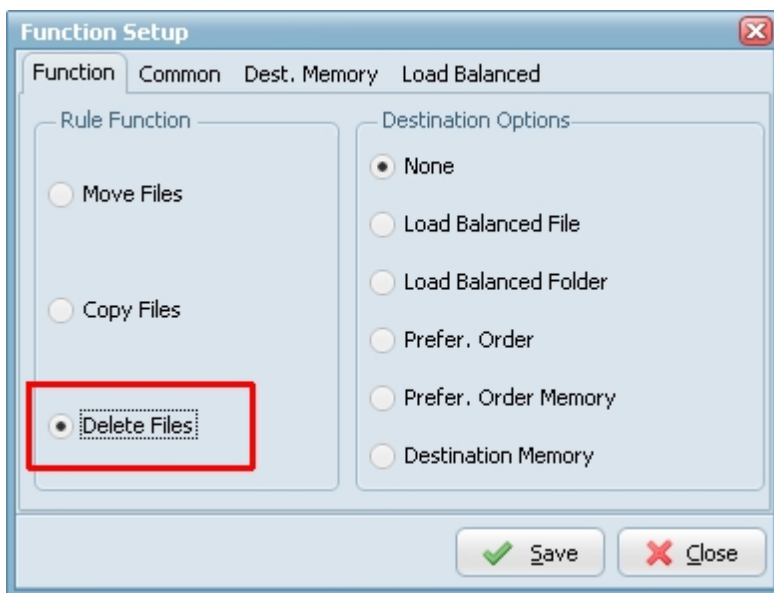


2. When you start the LimagitoX application and the LimagitoX service is running then the rules in the application version will automatically go into this status. They will only accept manual triggers. We don't want the application version to interfere with the running LimagitoX service.

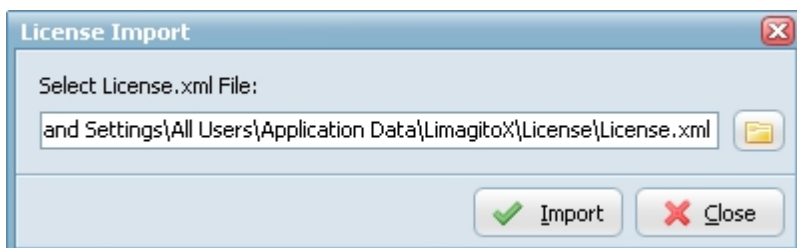
- ▶ Rule Enabled & Time Schedule. No longer used, obsolete.
- ▶ Rule Enabled & Scan Enabled. In this status the rule will accept scan triggers. It's ready to run.
- ▶ Rule Running. The rule was triggered and is running now. As long as the rule thread is running it will have this status.
- ▶ Check RunTime Log. An error occurred while the rule was running. This is a kind of memory info status. It doesn't mean that the 'problem' still exists. Right click on the selected rule in the listview and select 'Reset Info Status' to reset this status. You can also disable this option here.



- Function Delete Files Selected: 'Delete Files' is selected as function for this rule. A separate icon in the rule list view to indicate which rules are doing a delete function.



Import License



After payment you will receive a zipped License.xml file by mail. Please unzip and export this License.xml file using the 'Import License' option.

About

Information about the LimagitoX version you are using. The License hostname is important for the Single License.



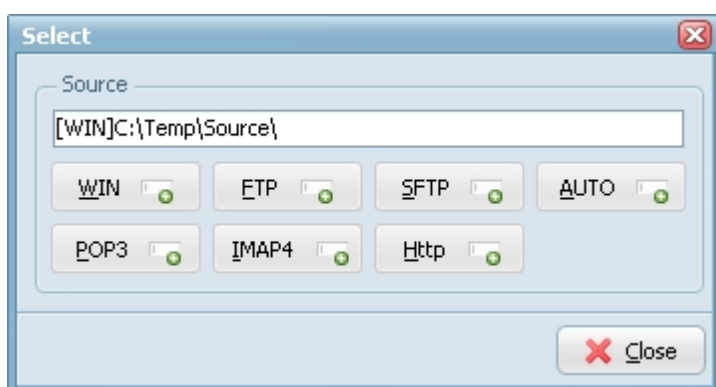
Rule Setup

Rule Setup

-  [Source](#)
-  [File Filter](#)
-  [Dir Filter](#)
-  [Memory](#)
-  [Backup](#)
-  [Function](#)
-  [Destination](#)

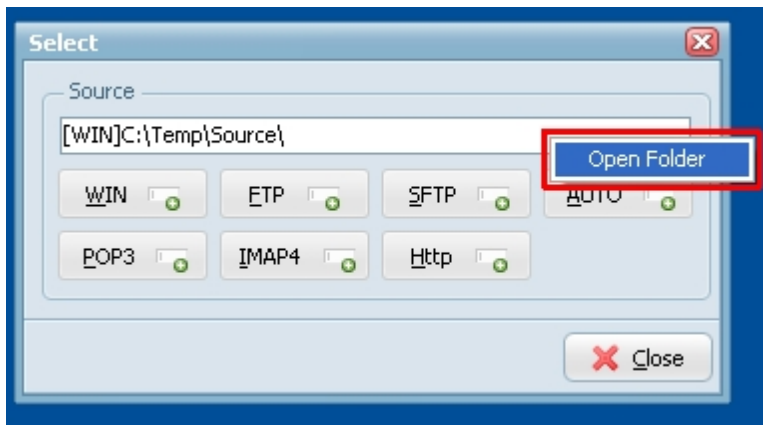
Source Options

Source Selection



LimagitoX Source selection possibilities:

- ▶ [WIN](#)
- ▶ [FTP](#)
- ▶ [SFTP](#)
- ▶ [AUTO](#)
- ▶ [POP3](#)
- ▶ [IMAP4](#)
- ▶ [HTTP](#)



Right click on the selected source to:

- ▶ open and explore the source folder (WIN, FTP, SFTP)

WIN Source

WIN Source Setup

Add / Update WIN as Source.



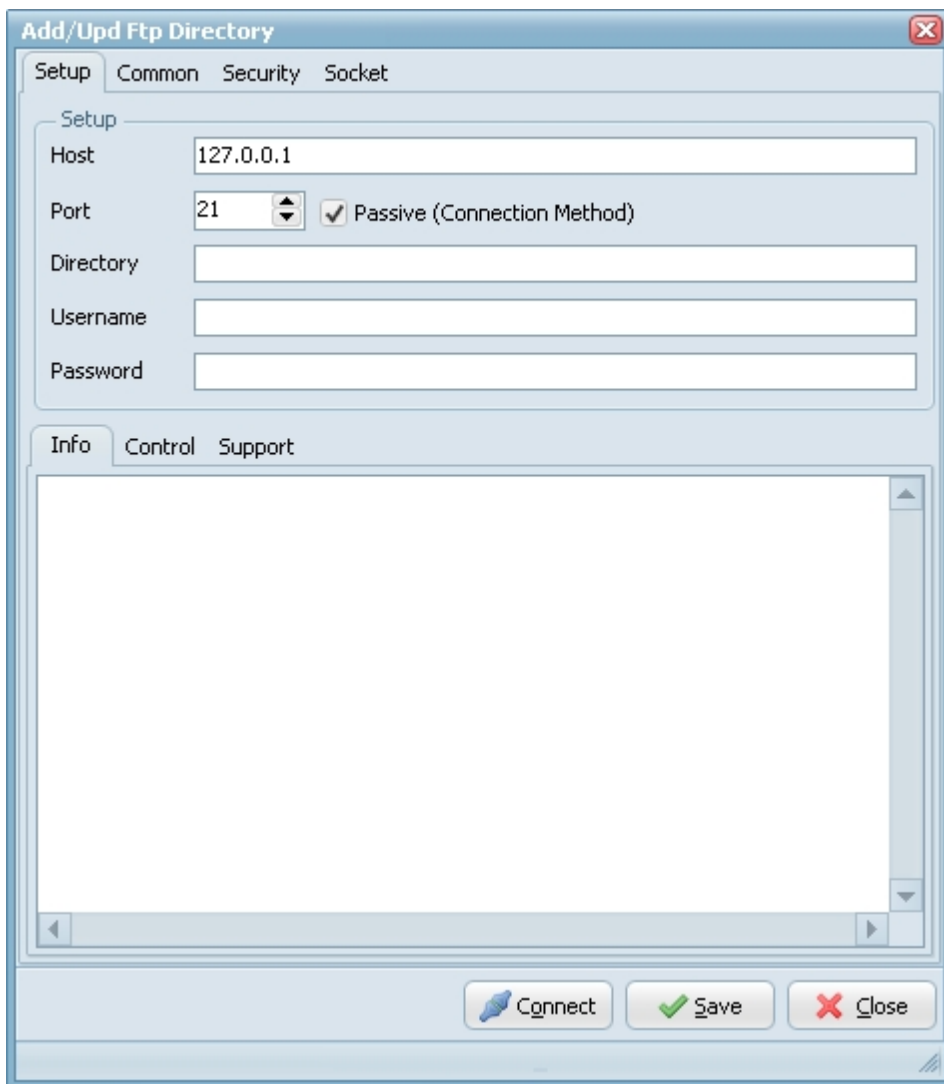
- ▶ You can drag and drop the folder into the window.

FTP Source

FTP (FTP & FTPS) Source Setup

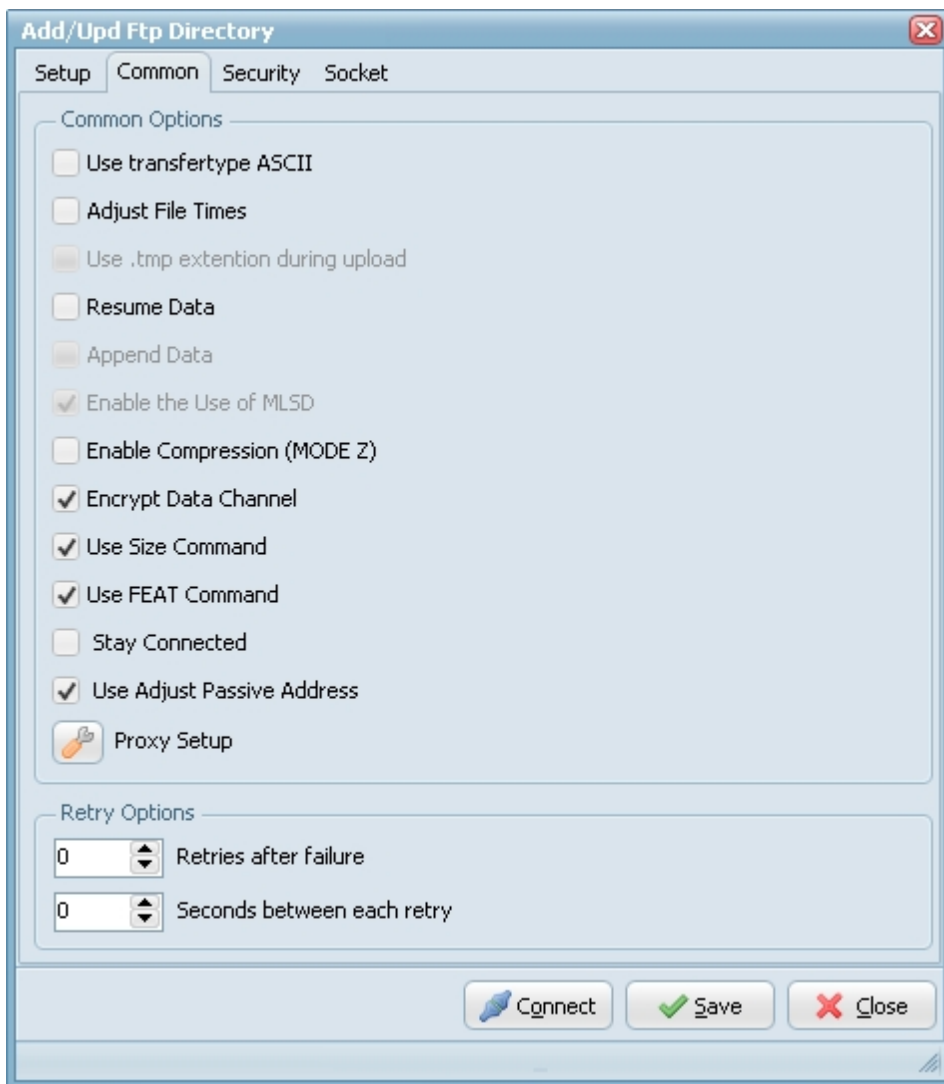
Add / Update FTP as Source.

Setup Options



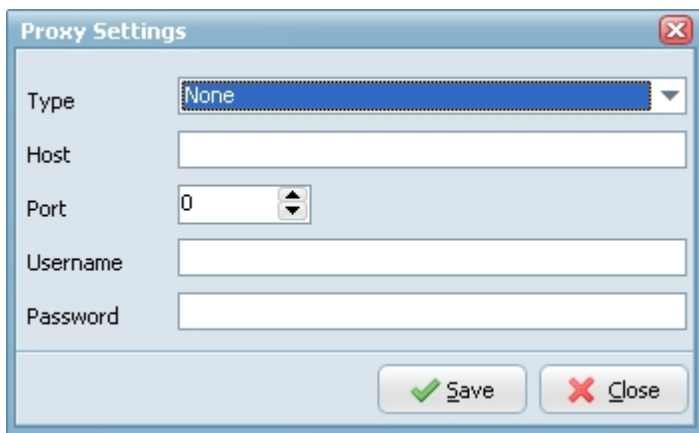
- ▶ Host: This option specifies the address of the host to connect to.
- ▶ Port: Port number on the host to connect to (Default value is 21).
- ▶ Passive: Active connections (or when Passive is disabled) indicates that the FTP server will open the connection for the data channel. In other words, the FTP client will listen for the server to open a connection for the data channel.
- ▶ Directory: Directory on the server file system.
- ▶ Username: Authentication identity used when logging in to the server (example: Anonymous).
- ▶ Password: Authentication credentials used when logging into the server.
- ▶ Connect: Check connection setup.

Common Options



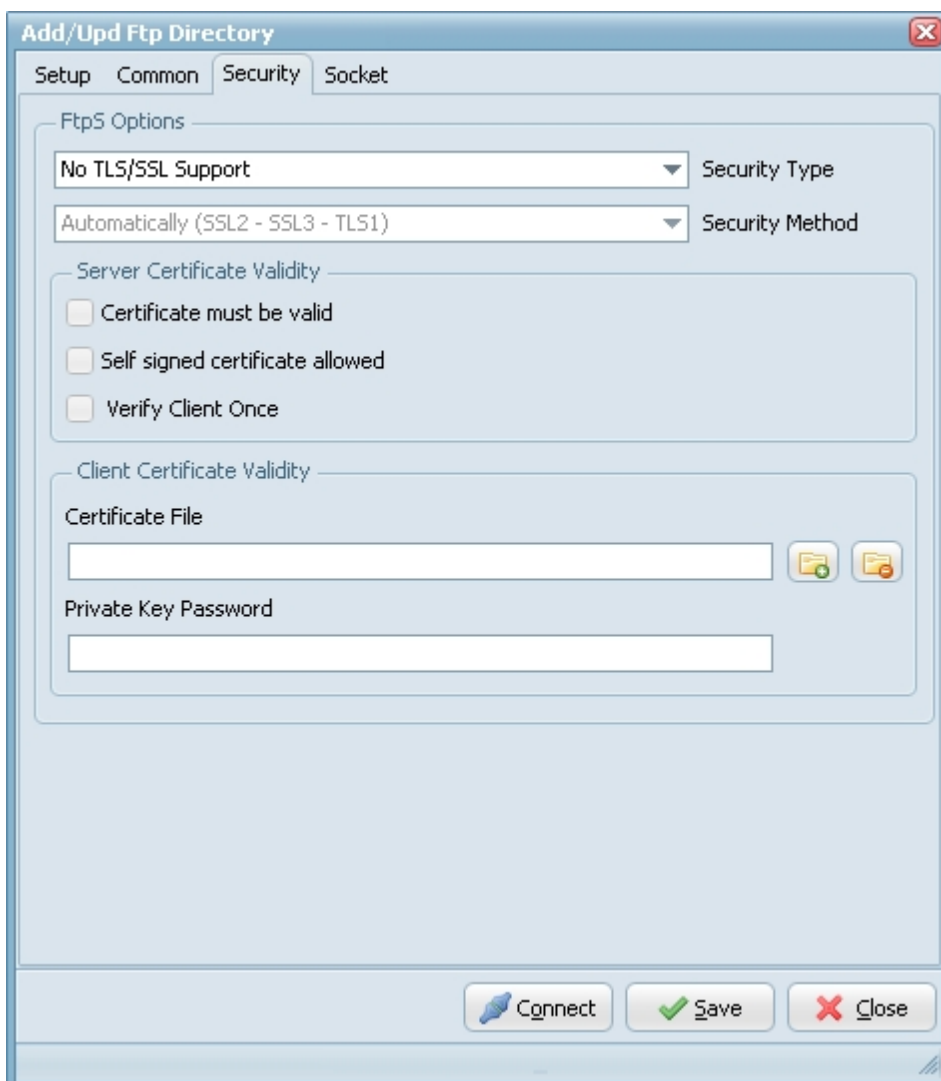
- ▶ Use transfertype ASCII: Use transfertype ASCII instead of Binary.
- ▶ Adjust File Times: File times will be adjusted after upload/download operation.
- ▶ Resume Data: When Resume contains True, the destination file will be opened and positioned to the end of the existing file data before retrieving new data.
- ▶ Append Data: When Append contains True, the FTP server will append data from the transfer to the end of a file which already exists on the FTP server.
- ▶ Enable Compression (MODE Z): Enable MODE Z Compression.
- ▶ Encrypt Data Channel: If this option is enabled the channel used for data transfer (files, directory listings) will be encrypted, otherwise only command channel will be encrypted.
- ▶ Use Size Command: Use this option to specify, whether SIZE command is sent when the data is downloaded. Use of this command lets the component report correct total size in OnProgress event, when the size of the data to be downloaded was not specified. Note, that some servers behave unexpectedly when SIZE command is used.
- ▶ Use FEAT Command: Use this option to specify, whether FEAT command is to be sent to the server. This command requests supported security mechanisms from FTPS server. Although server is not obliged to respond to it.
- ▶ Stay Connected: Don't disconnect the connection between scans.
- ▶ Use Adjust Passive Address: If this option is enabled, in passive mode data transfer, we will automatically set the address of the remote host to that from the control connection.

Proxy Settings



- ▶ Type: Use this option to specify type of the proxy server.
 - ▶ no proxy
 - ▶ user site proxy
 - ▶ site proxy
 - ▶ open proxy
 - ▶ userpath proxy
 - ▶ transparent proxy
- ▶ Host: Use this option to specify proxy server address.
- ▶ Port: Use this option to specify port on the proxy server.
- ▶ Username: Use this option to specify username.
- ▶ Password: Use this option to specify password.

Security Options



FTPS (also known as FTP Secure and FTP-SSL) is an extension to the commonly used File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols. FTPS should not be confused with the SSH File Transfer Protocol (SFTP), an incompatible secure file transfer subsystem for the Secure Shell (SSH) protocol. It is also different from Secure FTP, the practice of tunneling FTP through an SSH connection.

Security Type:

- ▶ Use Implicit TLS/SSL Support: Negotiation is not allowed with implicit FTPS configurations. A client is immediately expected to challenge the FTPS server with a TLS/SSL ClientHello message. If such a message is not received by the FTPS server, the server should drop the connection.
- ▶ Use Explicit TLS/SSL Support: In explicit mode (also known as FTPES), an FTPS client must "explicitly request" security from an FTPS server and then step-up to a mutually agreed encryption method. If a client does not request security, the FTPS server can either allow the client to continue insecure or refuse/limit the connection.

Security Method:

- ▶ Secure Sockets Layer SSLv2
- ▶ Secure Sockets Layer SSLv23
- ▶ Secure Sockets Layer SSLv3
- ▶ Transport Layer Security TLSv1
- ▶ Transport Layer Security TLSv1.1
- ▶ Transport Layer Security TLSv1.2

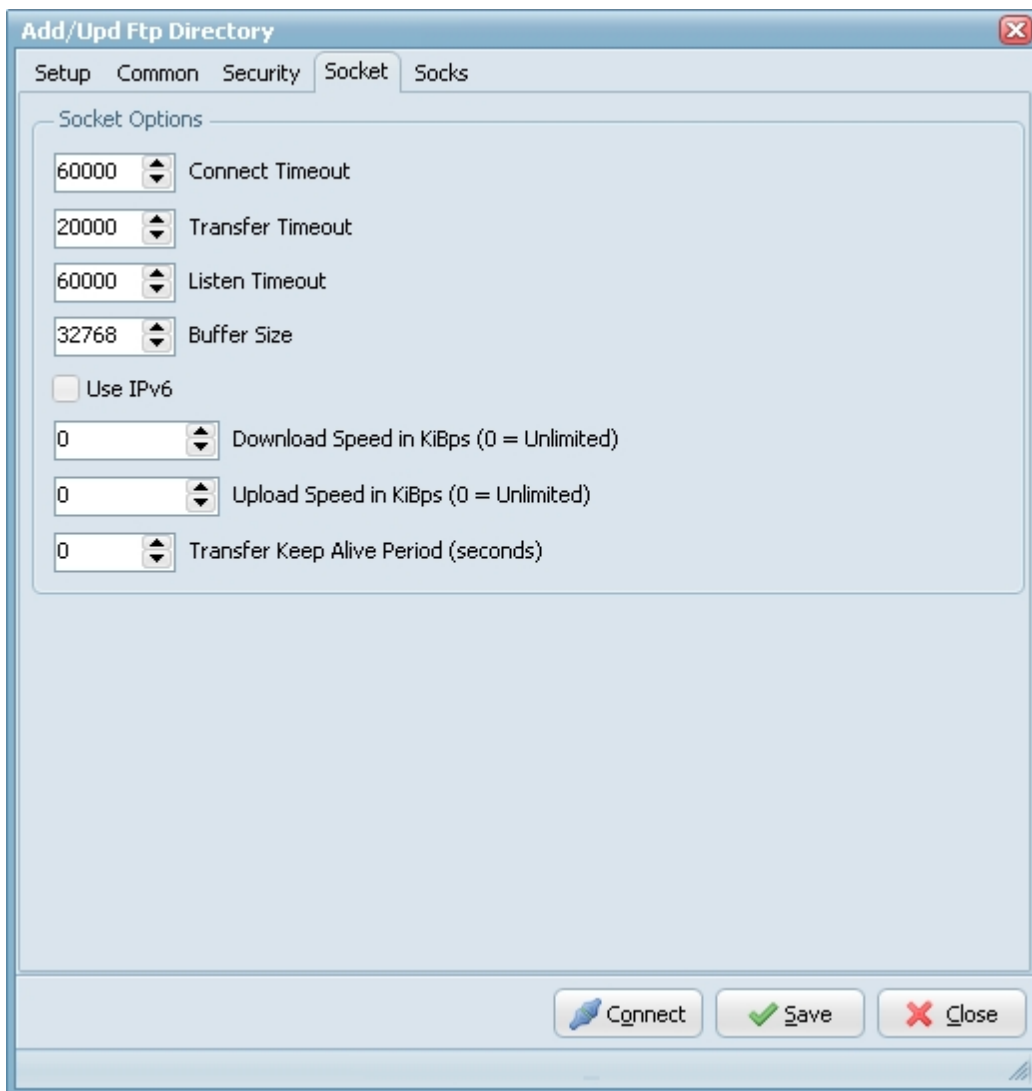
Server Certificate Validity

- ▶ Certificate must be valid: Certificate was validated successfully and is valid.
- ▶ Self signed certificate allowed: A self signed certificate is allowed.
- ▶ Verify client once:

Client Certificate Validity

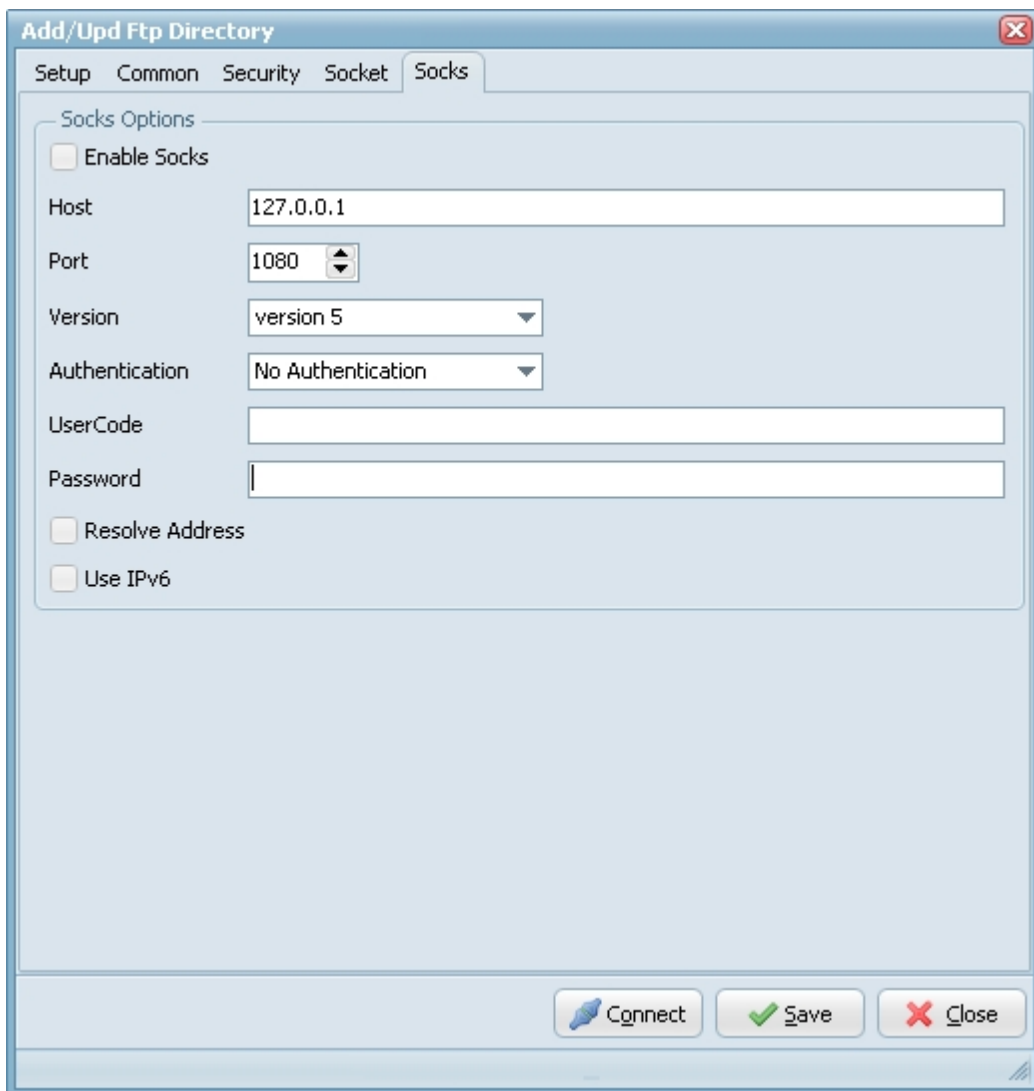
- ▶ Certificate File: For authentication FTPS (or, to be more precise, SSL/TLS protocol under FTP) uses X.509 certificates.
- ▶ Private Key Password: Needed when your private key is encrypted with a passphrase.

Socket Options



- ▶ **Connect Timeout:** Milliseconds to wait for successful completion of a connection attempt (default 60000). Default value is 60000 ms (1 min).
- ▶ **Listen Timeout:** Use this option to specify maximal time during which the listening socket will be opened in the active mode. If there is no connection request from server during this time the transfer operation will be canceled. Default value is 60000 ms (1 min).
- ▶ **Transfer Timeout:** In active mode, specifies a time period that a client should wait for incoming data connection (when file or directory listing is to be transferred). If no data connection is accepted during this period, the data connection will be cancelled. Default value is 60000 ms (1 min).
- ▶ **Buffer Size:** Use this option to specify the size of the chunk used during datatransfer. Changing the chunk size may increase (or, on the contrary, decrease) the speed of file download/upload. Default value is 32768 bytes.
- ▶ **Use IPv6:** This option defines whether IP protocol version 6 should be used.
- ▶ **Download Speed:** Use this option to specify the maximum number of KiBps that FTP client may receive. The value of 0 (zero) means "no limitation".
- ▶ **Upload Speed:** Use this option to specify the maximum number of KiBps that FTP client may send. The value of 0 (zero) means "no limitation".
- ▶ **Transfer Keep Alive Period:** Use keep-alive to prevent command channel from being closed by NATs during long data transfer. Keep-alive is enabled by setting the Keep Alive Period option to a non-zero value (300 is a great value for keep-alives). Note, that not all servers handle keep-alives correctly.

Socks Options



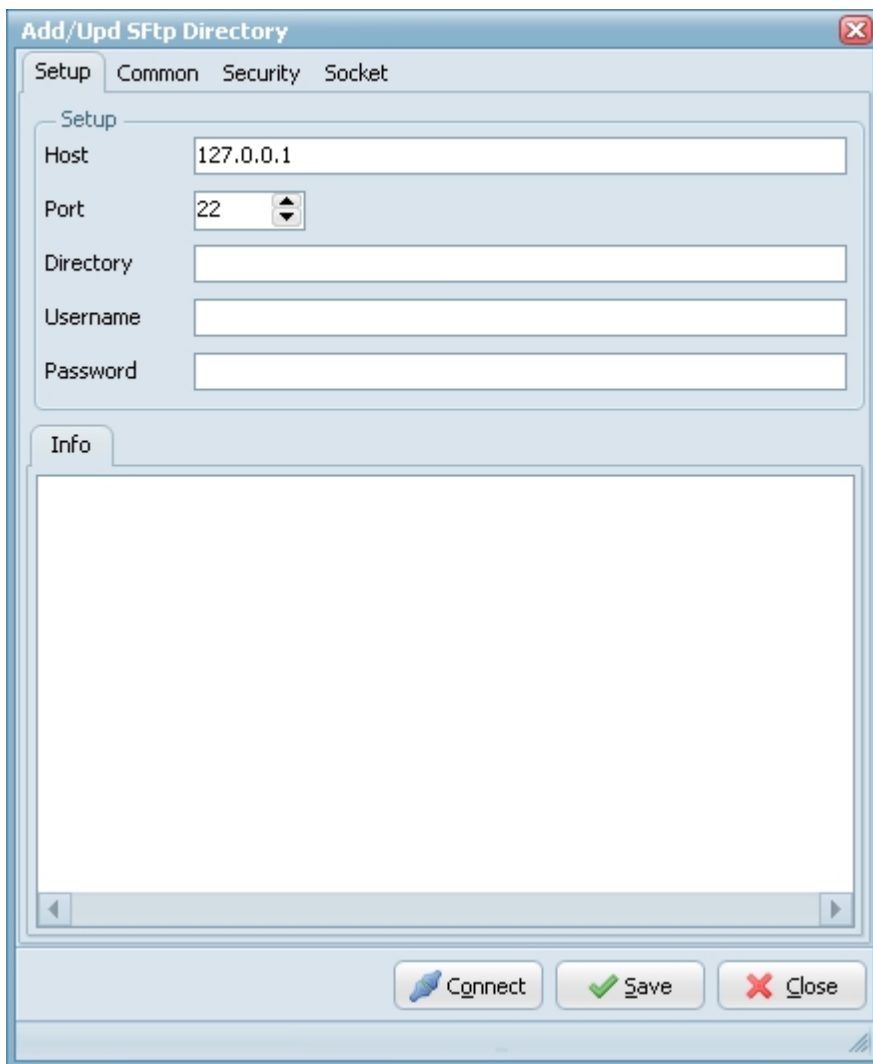
- ▶ **Enable Socks:** This option defines whether the connection is established directly (Enable Socks is disabled) or via SOCKS server (Enable Socks is enabled).
- ▶ **Host:** This property specifies the IP address or host name of the SOCKS server.
- ▶ **Port:** Specifies the port that SOCKS server is bound to. Default value is 1080.
- ▶ **Version:** This option specifies the version of SOCKS protocol to be used with the SOCKS server. Default value is version 5.
- ▶ **Authentication:** This option specifies the method of authentication to use with the SOCKS server. The methods supported are "No Authenticate" and "UserCode".
- ▶ **UserCode:** This property specifies the user code (username) to access the SOCKS server.
- ▶ **Password:** This property specifies the password to access the SOCKS server.
- ▶ **Resolve Address:** Specifies whether the address of destination host is resolved or passed to SOCKS server for resolving. Usually the host name is resolved on the client system. However some policy can forbid DNS operations on client computers. Then the client needs to pass the host name to the SOCKS server unresolved (SOCKS server is supposed to resolve it itself).
- ▶ **Use IPv6:** This option defines whether IP protocol version 6 should be used.

SFTP Source

SFTP Source Setup

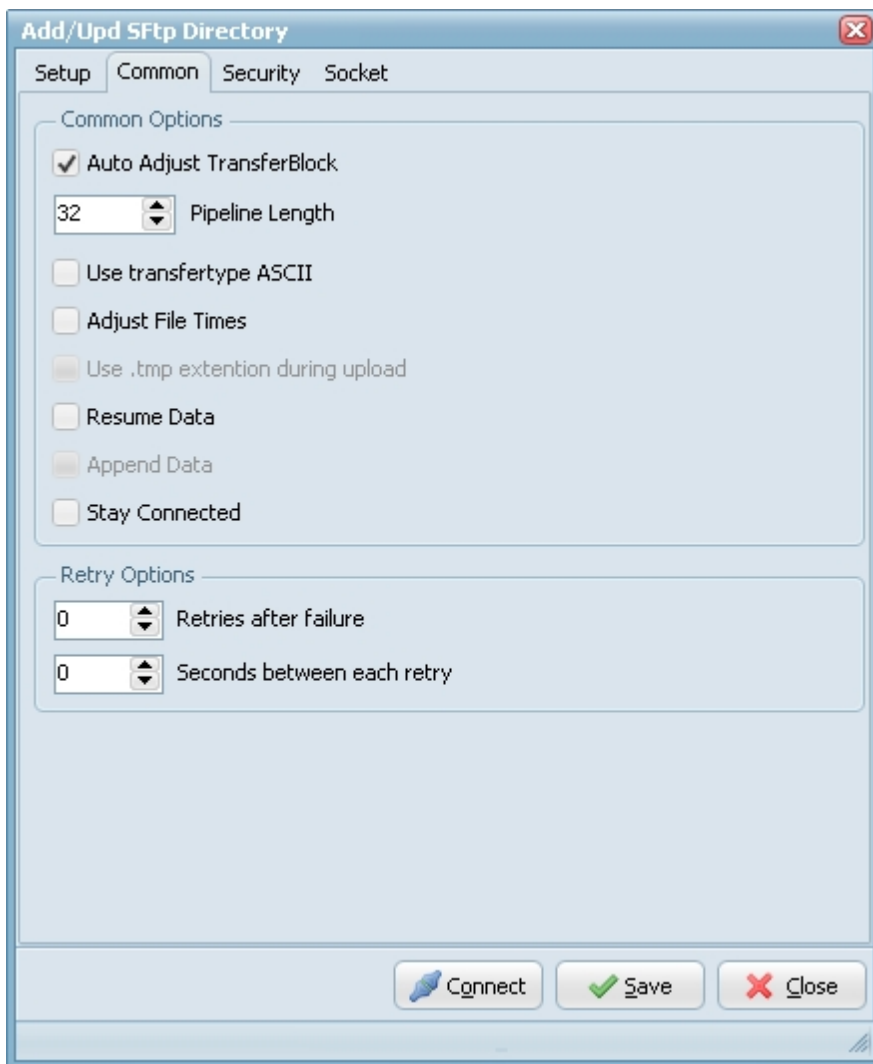
Add / Update SFTP as Source.

Setup Options



- ▶ Host: This option specifies the address of the host to connect to.
- ▶ Port: Port number on the host to connect to (Default value is 22).
- ▶ Directory: Directory on the server file system.
- ▶ Username: Authentication identity used when logging in to the server (example: Anonymous).
- ▶ Password: Authentication credentials used when logging into the server.
- ▶ Connect: Check connection setup.

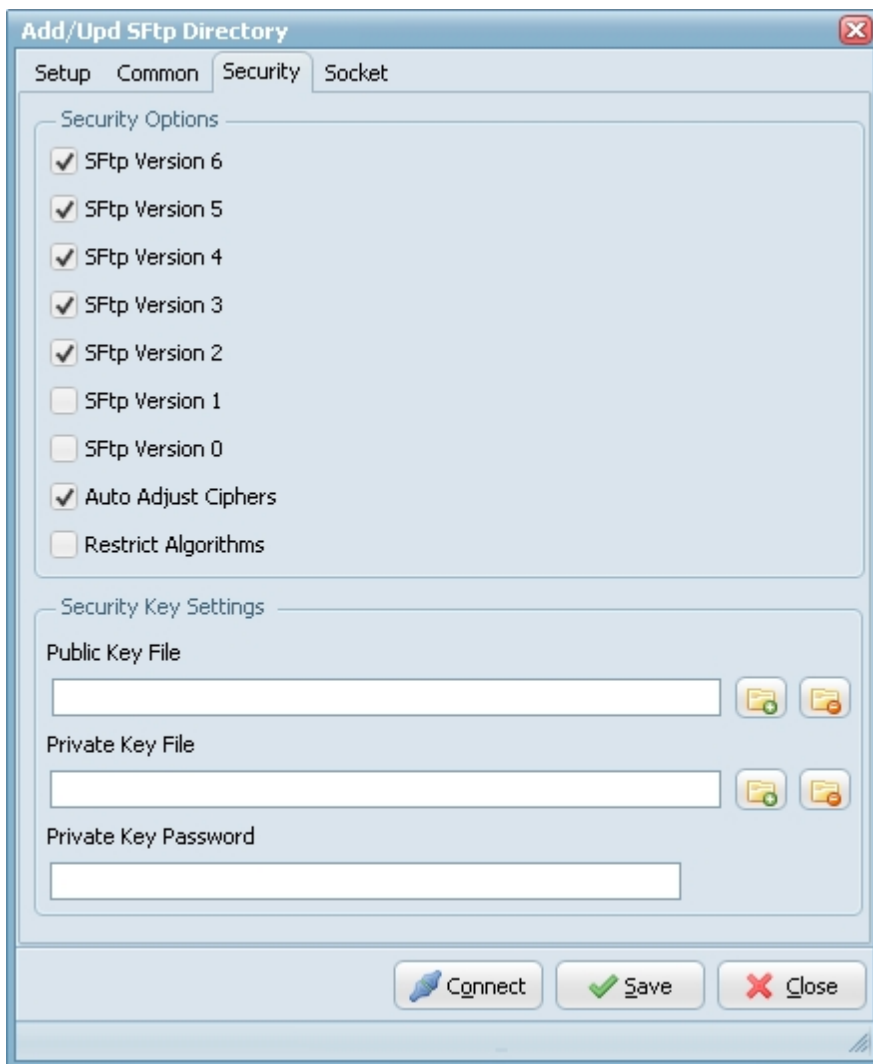
Common Options



Common Options

- ▶ **Auto Adjust Transferblock:** Use this option to enable or disable automatic adjustment of pipeline length and block sizes. By default automatic adjustment is enabled, and normally you don't need to disable it.
- ▶ **Pipeline Length:** Use this property to specify the number of upload or download requests sent before waiting for all requests to complete. The more requests are sent, the faster the transfer is. However, in case of error, all requests are discarded. Also, more pending requests means more memory used, so if speed is not critical and memory consumption is, set PipelineLength to 1. Default value is 32.
- ▶ **Use transfertype ASCII:** Use transfertype ASCII instead of Binary.
- ▶ **Adjust File Times:** File times will be adjusted after upload/download operation.
- ▶ **Resume Data:** When Resume contains True, the destination file will be opened and positioned to the end of the existing file data before retrieving new data.
- ▶ **Stay Connected:** Don't disconnect the connection between scans.

Security Options



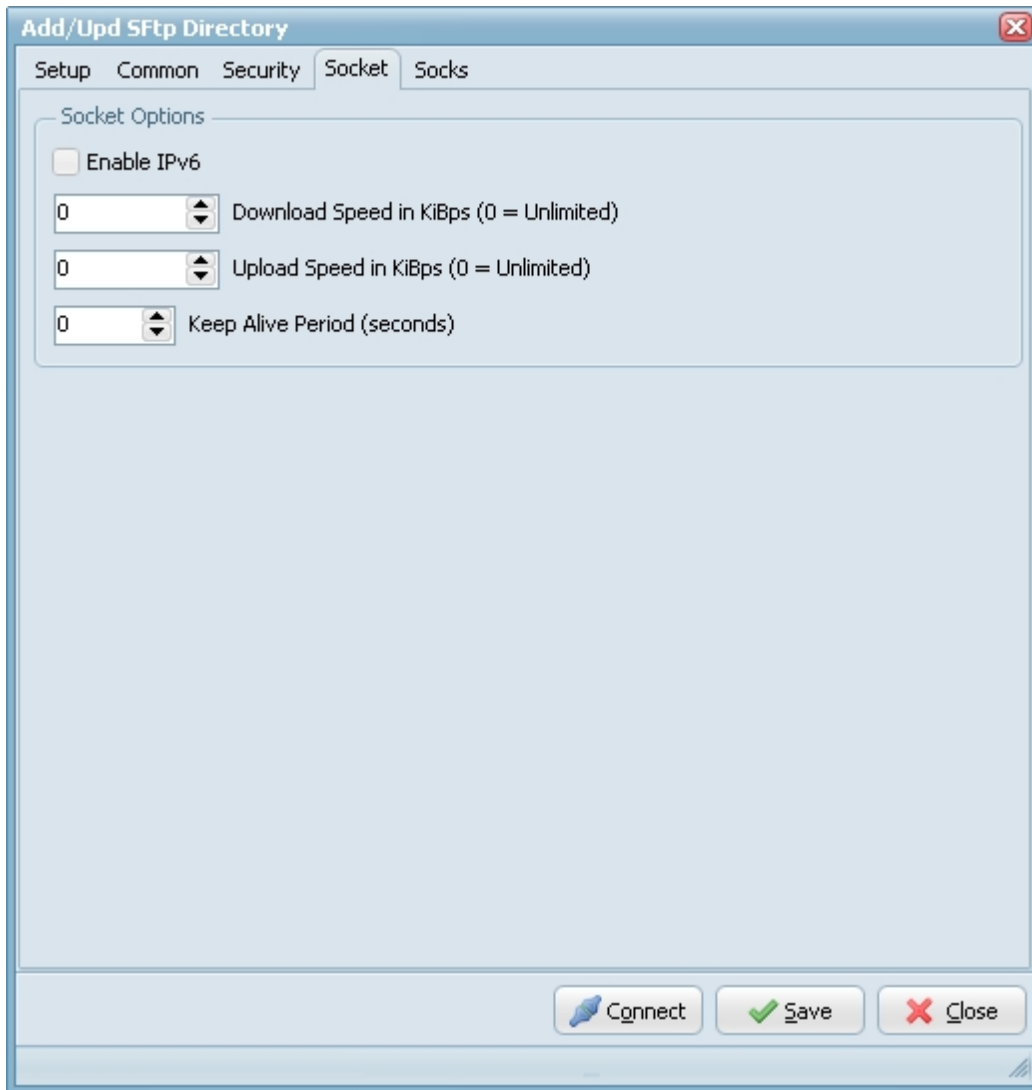
Security Options

- ▶ **SFTP Versions:** Use this option to specify SFTP versions which can be used during the connection.

Security Key Options

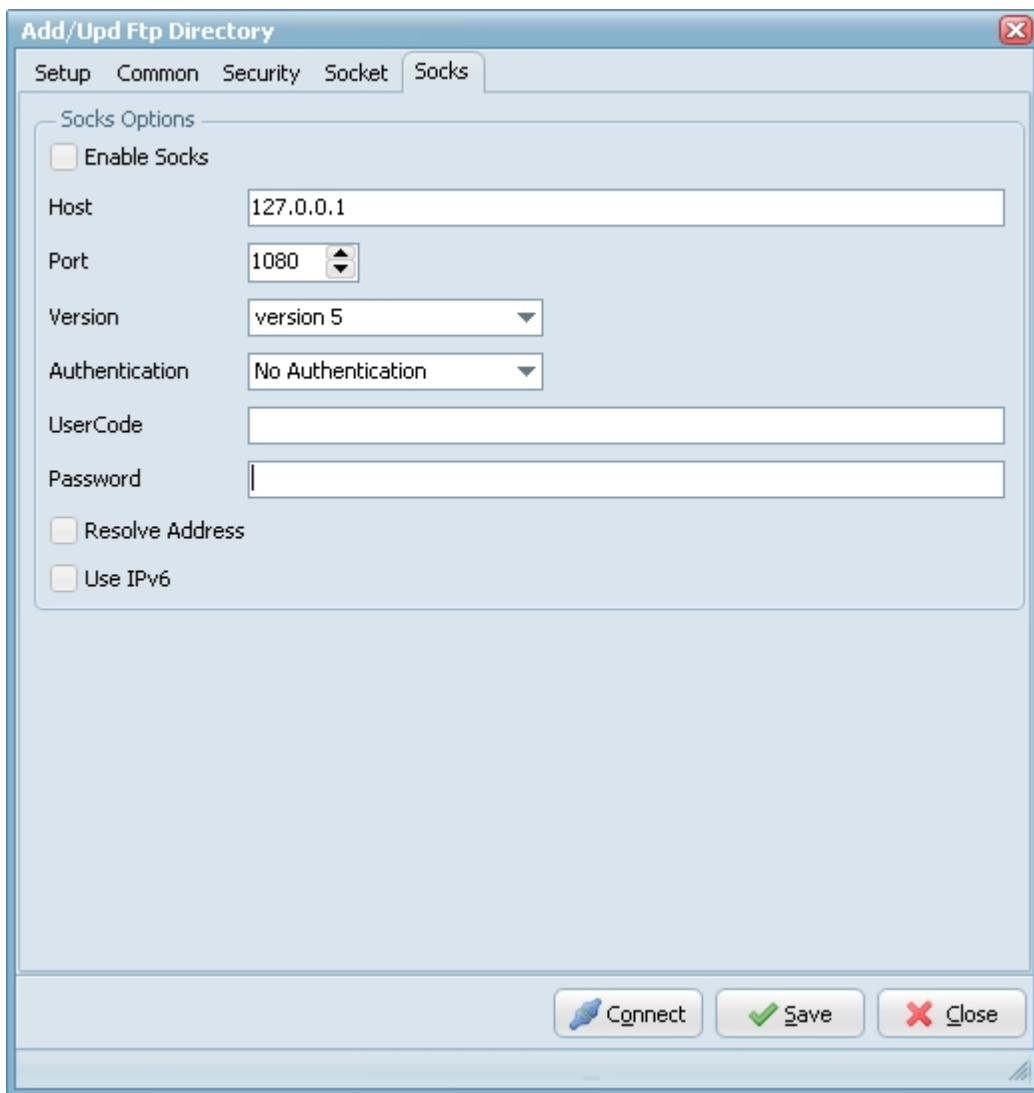
- ▶ **Public Key File:** When you authenticate with a public/private key pair, the server to which you are connecting should have a copy of your public key. This public key is safe for anyone to have. It doesn't contain any information about the owner of the key. Neither it contains information that lets one reliably validate the integrity and authenticity.
- ▶ **Private Key File:** When you authenticate with a public/private key pair, you should have a private key that only you have access to. When you log in using your key pair, the server sends a challenge, encrypted with your public key. The only key that will decrypt the challenge is your private key.
- ▶ **Private Key Password:** Needed when your private key is encrypted with a passphrase. Everyone recommends that you protect your private key with a passphrase (otherwise anybody who steals the file from you can log into everything you have access to).

Socket Options



- ▶ **Use IPv6:** This option defines whether IP protocol version 6 should be used.
- ▶ **Download Speed:** Use this option to specify the maximum number of KiBps that SFTP client may receive. The value of 0 (zero) means "no limitation".
- ▶ **Upload Speed:** Use this option to specify the maximum number of KiBps that SFTP client may send. The value of 0 (zero) means "no limitation".
- ▶ **Keep Alive Periods:** Use this option to specify tunnel inactivity period (in seconds), after which the keep-alive signal will be sent. Default value is 0 (no keep-alive signals).

Socks Options

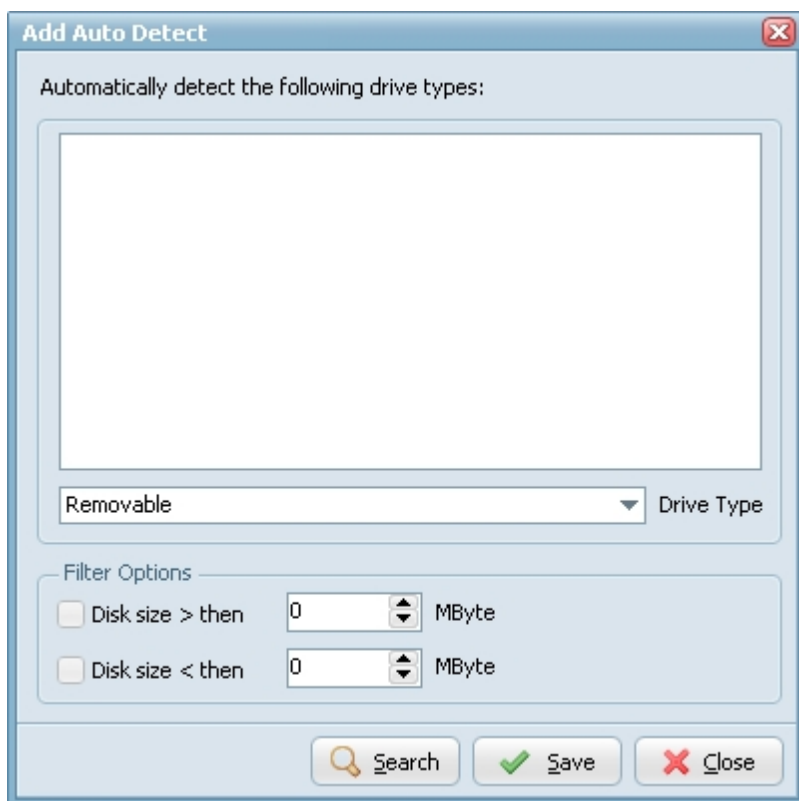


- ▶ **Enable Socks:** This option defines whether the connection is established directly (Enable Socks is disabled) or via SOCKS server (Enable Socks is enabled).
- ▶ **Host:** This property specifies the IP address or host name of the SOCKS server.
- ▶ **Port:** Specifies the port that SOCKS server is bound to. Default value is 1080.
- ▶ **Version:** This option specifies the version of SOCKS protocol to be used with the SOCKS server. Default value is version 5.
- ▶ **Authentication:** This option specifies the method of authentication to use with the SOCKS server. The methods supported are "No Authenticate" and "UserCode".
- ▶ **UserCode:** This property specifies the user code (username) to access the SOCKS server.
- ▶ **Password:** This property specifies the password to access the SOCKS server.
- ▶ **Resolve Address:** Specifies whether the address of destination host is resolved or passed to SOCKS server for resolving. Usually the host name is resolved on the client system. However some policy can forbid DNS operations on client computers. Then the client needs to pass the host name to the SOCKS server unresolved (SOCKS server is supposed to resolve it itself).
- ▶ **Use IPv6:** This option defines whether IP protocol version 6 should be used.

AUTO Source

AUTO Source Setup

Add / Update AUTO as Source.

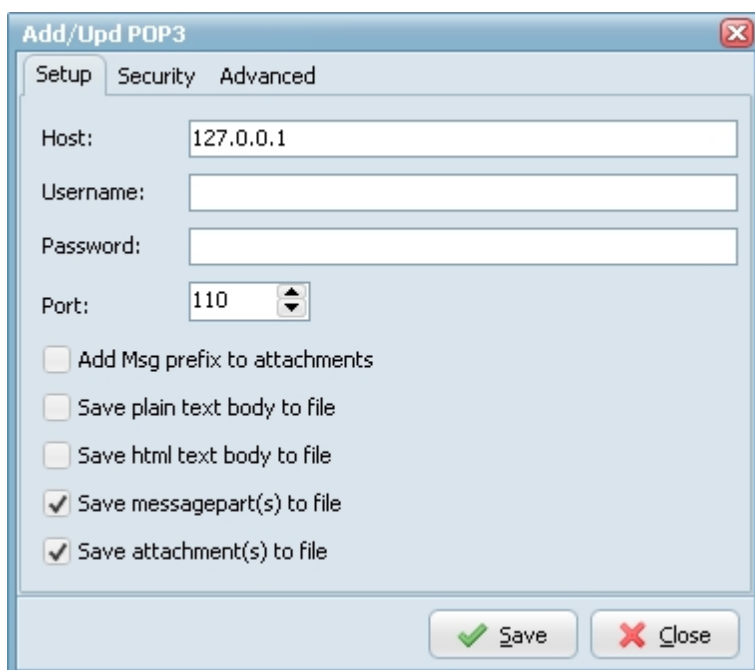


POP3 Source

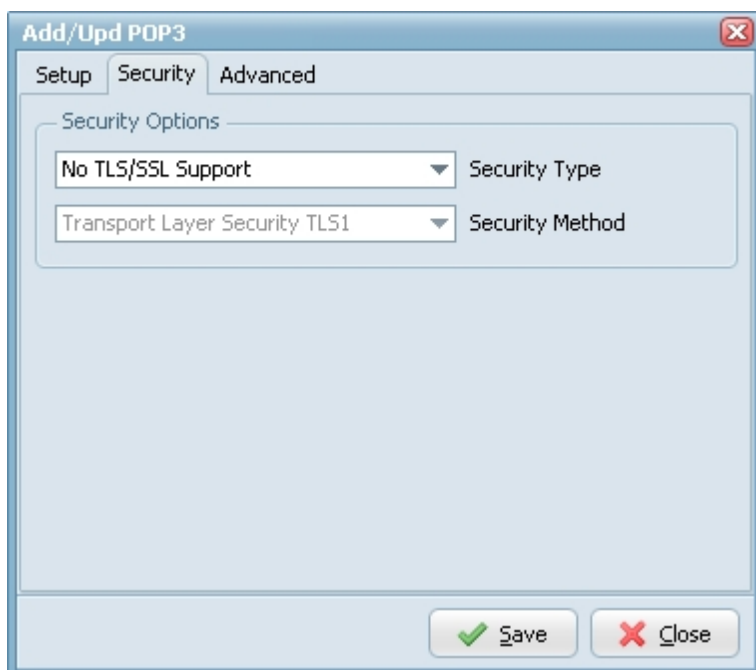
POP3 Source Setup

Add / Update POP3 as Source.

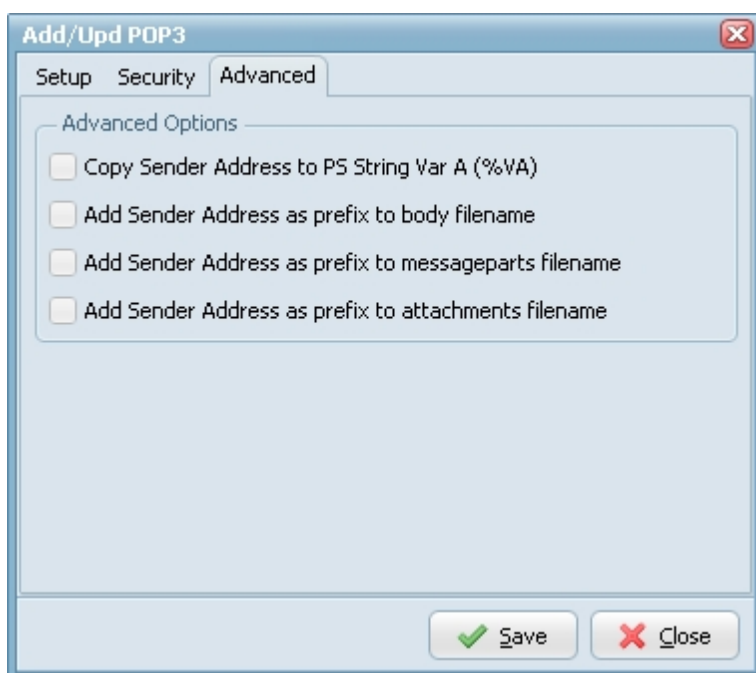
Setup Options



Security Options



Advanced Options



IMAP Source

IMAP Source Setup

Add / Update IMAP as Source.

Setup Options

Add/Upd IMAP4

Setup Security Advanced

Host: 127.0.0.1

Username:

Password:

MailBox: INBOX

Port: 143

☐ Add Msg prefix to attachments

☐ Save plain text body to file

☐ Save html text body to file

Advanced

☐ Move to mailbox on success

Save Close

Security Options

Add/Upd IMAP4

Setup Security Advanced

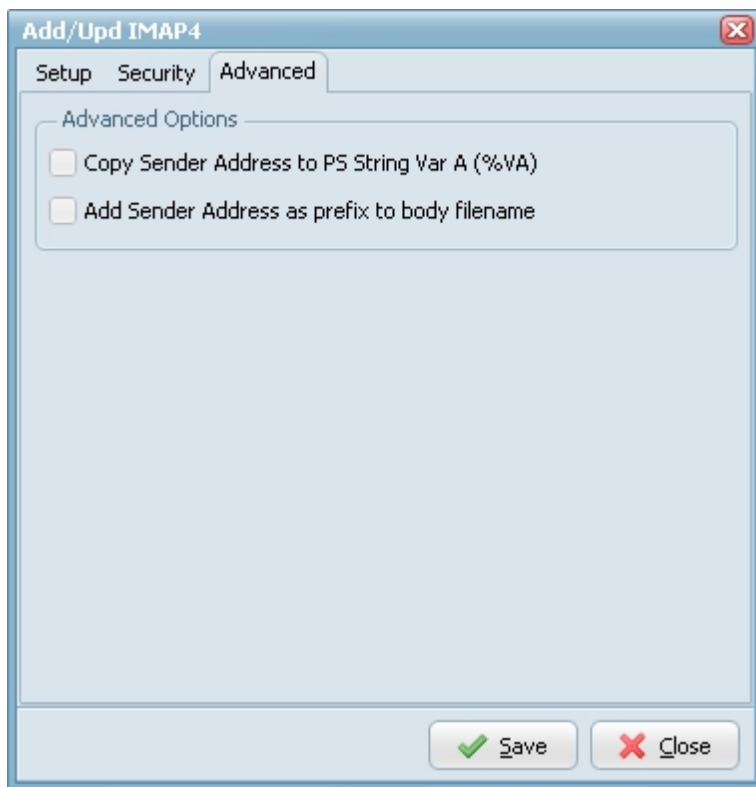
Security Options

No TLS/SSL Support Security Type

Transport Layer Security TLSv1 Security Method

Save Close

Advanced Options

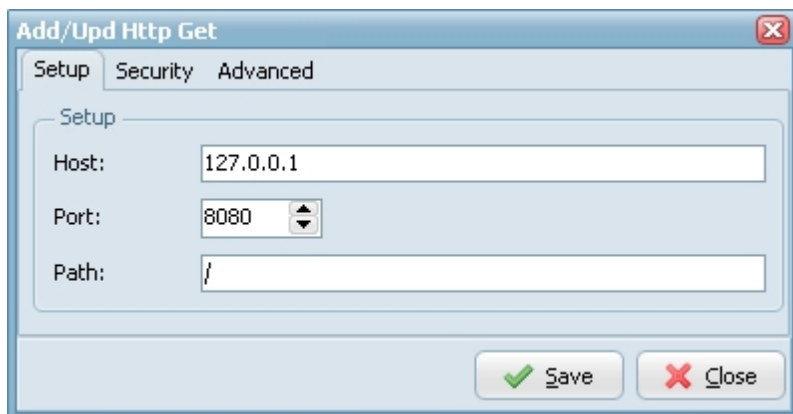


HTTP Source

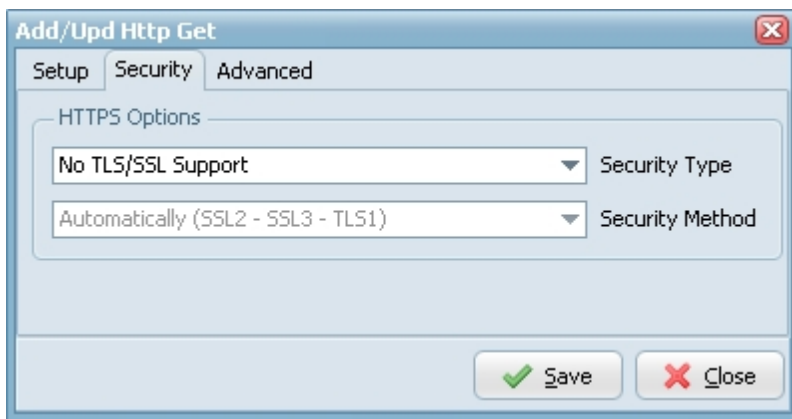
HTTP Source Setup

Add / Update HTTP as Source.

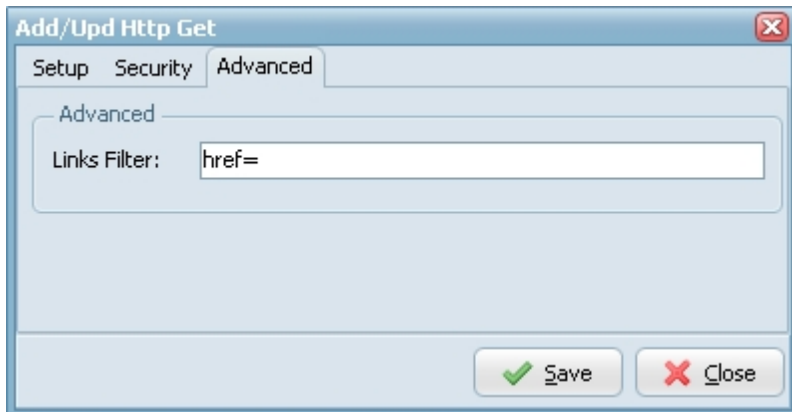
Setup Options



Security Options

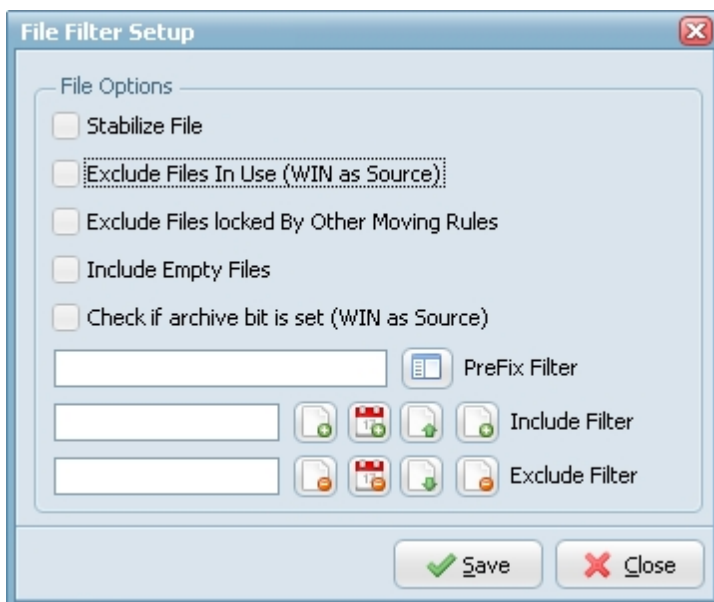


Advanced Options



File Filter

File Filter Setup



- ▶ **Stabilize File:** Scan will wait until the file is stabilized (not growing). An extra scan is needed to if the file is still growing. This will double the actual scan time.
- ▶ **Exclude Files in Use:** Do not copy/move/delete files that are locked by another process (WIN source only).
- ▶ **Exclude Files locked by other moving rules.** Only enable this option if multiple rules are scanning the same directory. Enable this option in all the rules the are scanning this same source.
- ▶ **Include Empty Files:** Scan will also pick up empty files (0 bytes).
- ▶ **Check if archive bit is set (WIN as Source):** On Windows when a file is created or modified, the archive bit is set, and when the file has been backed up, the archive bit is cleared. It is by use of the archive bit that incremental backups are

implemented.

- ▶ File PreFix Filter: Scan will only pick up files starting with this prefix.

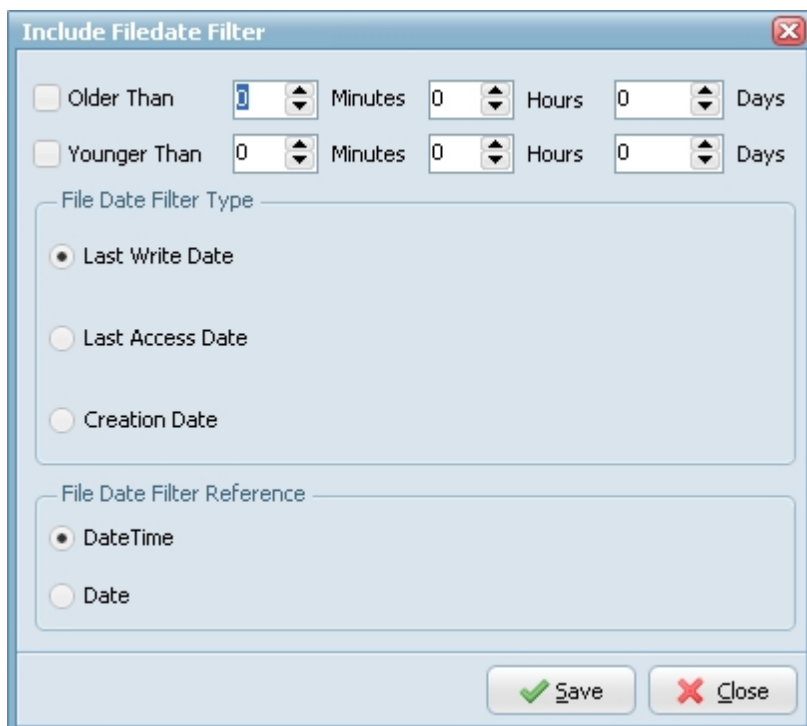
Filename Include Filter



The 'Include Filename Filter' dialog box has a title bar with a close button. It contains a 'Filename Filter' text box with the text '*.pdf;*.tiff'. Below this is an 'Add/Del Filter' section with a list box containing '*.pdf' and '*.tiff', and two buttons: 'Add Filter' and 'Del Filter'. At the bottom, there is a 'Check Filename' text box with the text 'MyFilename.pdf' and two buttons: 'Save' (with a green checkmark) and 'Close' (with a red X).

- ▶ Scan will only pick up files using this filter(s).

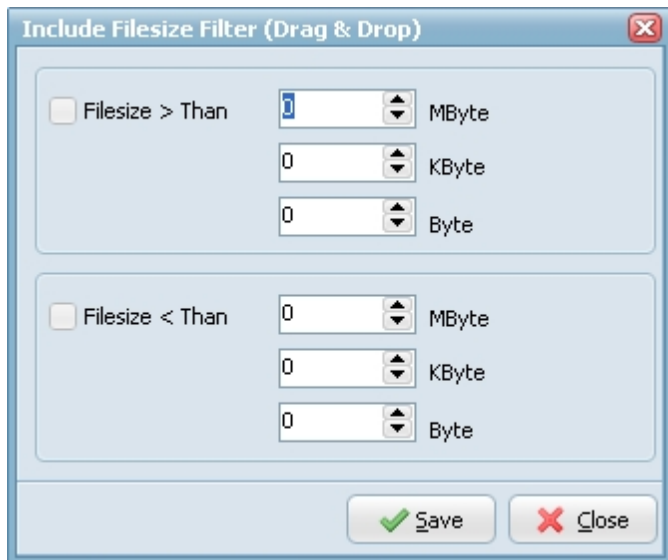
Filedate Include Filter



The 'Include Filedate Filter' dialog box has a title bar with a close button. It contains two sections: 'Older Than' and 'Younger Than'. Each section has a checkbox, a spinner box, and labels for 'Minutes', 'Hours', and 'Days'. Below these is a 'File Date Filter Type' section with three radio buttons: 'Last Write Date' (selected), 'Last Access Date', and 'Creation Date'. At the bottom is a 'File Date Filter Reference' section with two radio buttons: 'DateTime' (selected) and 'Date'. At the very bottom are two buttons: 'Save' (with a green checkmark) and 'Close' (with a red X).

- ▶ Scan will only pick up files using this date filter(s).

Filesize Include Filter



Include Filesize Filter (Drag & Drop)

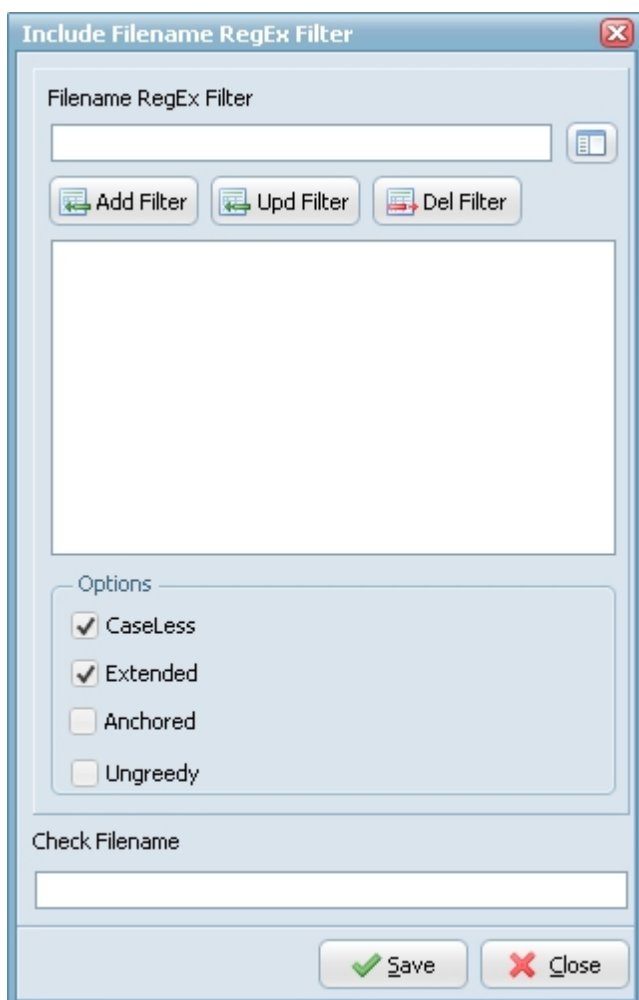
☐ Filesize > Than MByte
 KByte
 Byte

☐ Filesize < Than MByte
 KByte
 Byte

☒ Save ☐ Close

► Scan will only pick up files using this size filter(s).

Filename RegEx Include Filter



Include Filename RegEx Filter

Filename RegEx Filter

☒ Add Filter ☒ Upd Filter ☒ Del Filter

Options

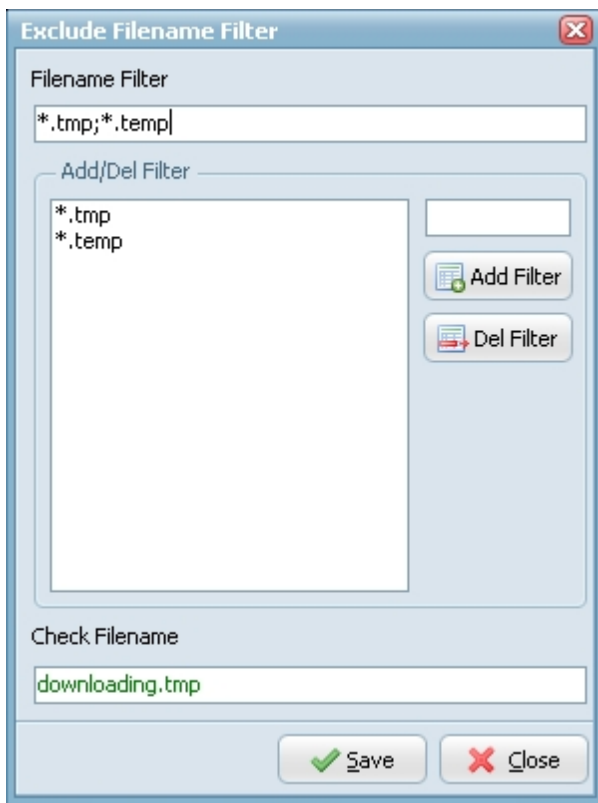
☒ CaseLess
☒ Extended
☐ Anchored
☐ Ungreedy

Check Filename

☒ Save ☐ Close

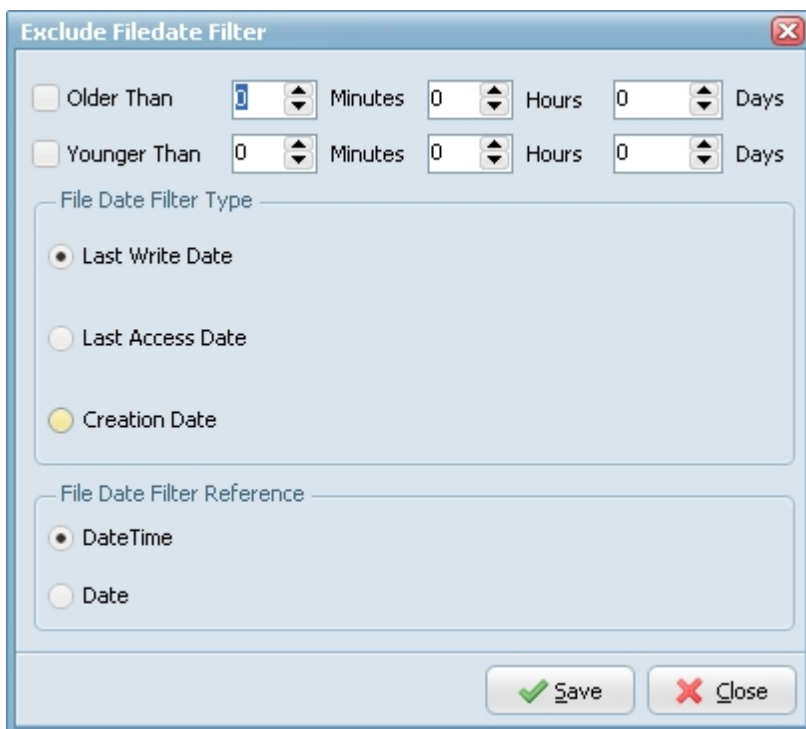
► Scan will only pick up files using this RegEx filter(s).

Filename Exclude Filter



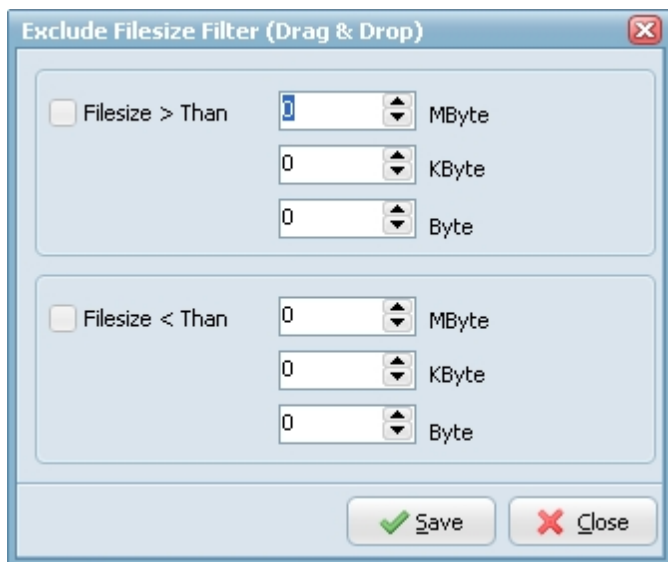
- ▶ Scan will not pick up files using this filter(s).

Filedate Exclude Filter



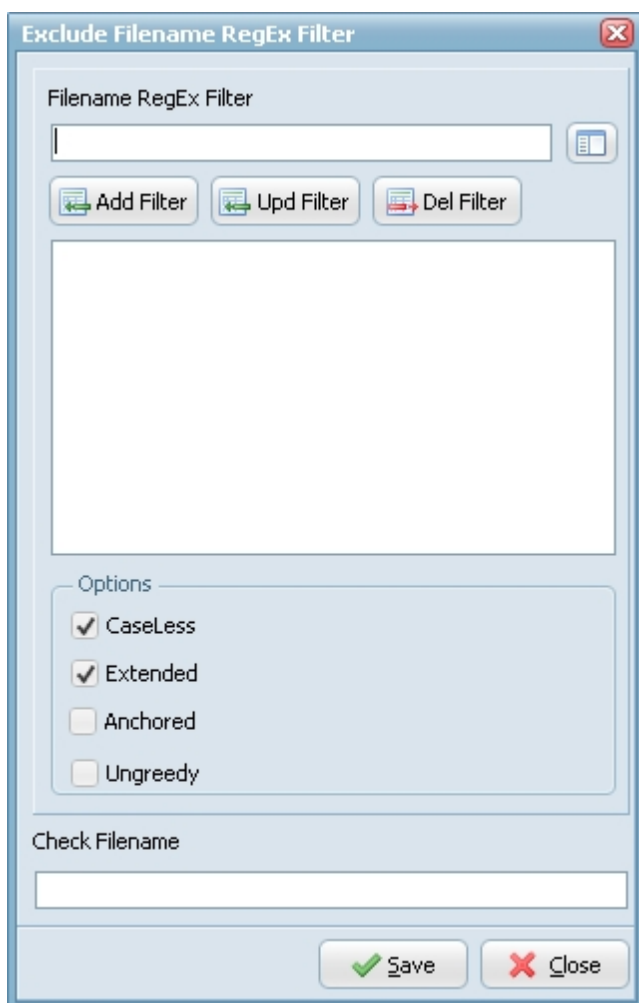
- ▶ Scan will not pick up files using this date filter(s).

Filesize Exclude Filter



- ▶ Scan will not pick up files using this size filter(s).

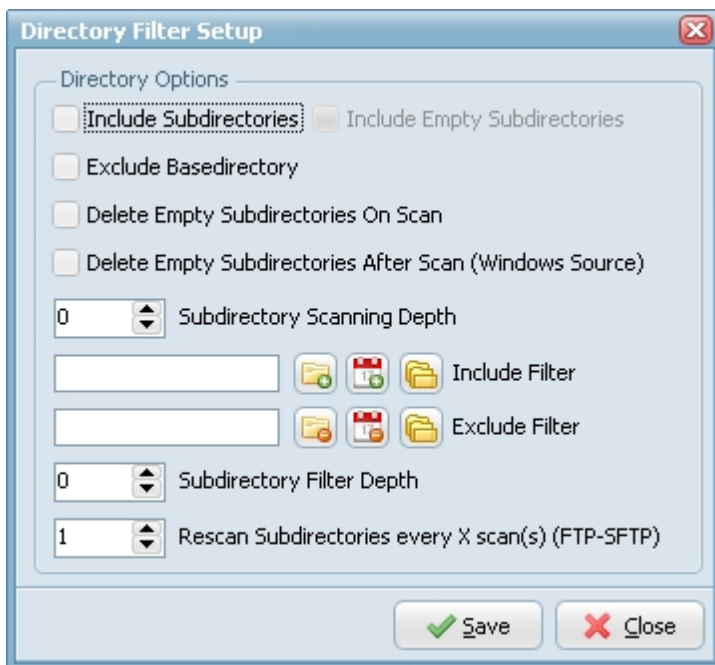
Filename RegEx Exclude Filter



- ▶ Scan will not pick up files using this RegEx filter(s).

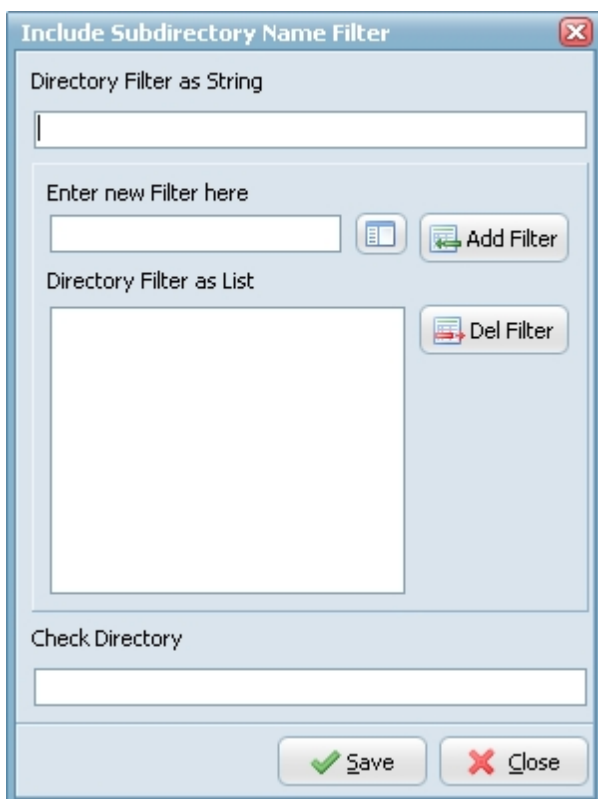
Dir Filter

Directory Filter Setup



- ▶ **Include Subdirectories:** Include source subdirectories when scanning.
- ▶ **Include Empty Subdirectories:** With empty we mean no files or no files found due to file filter. Enable this option if you want to copy the complete folder structure from source to destination.
- ▶ **Exclude Basedirectory:** Exclude base source directory when scanning.
- ▶ **Delete Empty Subdirectories On Scan:** Deletes existing empty subdirectories.
- ▶ **Delete Empty Subdirectories After Scan (WIN as Source):** Deletes existing empty subdirectories after scan (WIN as Source).
- ▶ **Subdirectory Scanning Depth:** Subdirectory Scanning Depth (default 0 = No Limit).
- ▶ **Subdirectory Filter Depth:**
- ▶ **Rescan Subdirectories every X scan(s) (FTP-SFTP):**

Subdirectory Name Include Filter



Subdirectory Date Include Filter

Include Subdirectory Date Filter (Windows)

☐ Older than Minutes Hours Days

☐ Younger than Minutes Hours Days

Directory Date Filter Type

☒ Last Write Date

☐ Last Access Date

☐ Creation Date

Directory Date Filter Reference

☒ DateTime

☐ Date

☒ Save ☐ Close

Subdirectory Size Include Filter

Include Directory Size Filter (Windows)

☐ Dirsize > then MByte

KByte

Byte

☐ Dirsize < then MByte

KByte

Byte

☒ Save ☐ Close

Subdirectory Name Exclude Filter

Exclude Subdirectory Name Filter

Directory Filter as String

Enter new Filter here

Directory Filter as List

Check Directory

Save Close

Subdirectory Date Exclude Filter

Exclude Subdirectory Date Filter (Windows)

☐ Older than Minutes Hours Days

☐ Younger than Minutes Hours Days

Directory Date Filter Type

☒ Last Write Date

☐ Last Access Date

☐ Creation Date

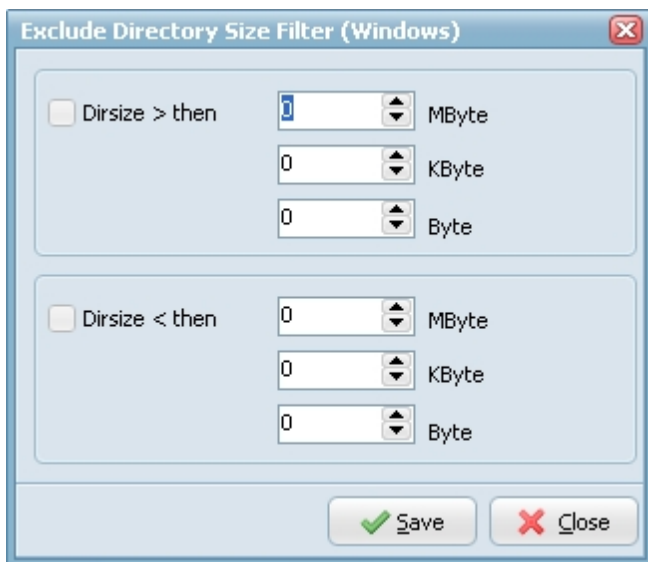
Directory Date Filter Reference

☒ DateTime

☐ Date

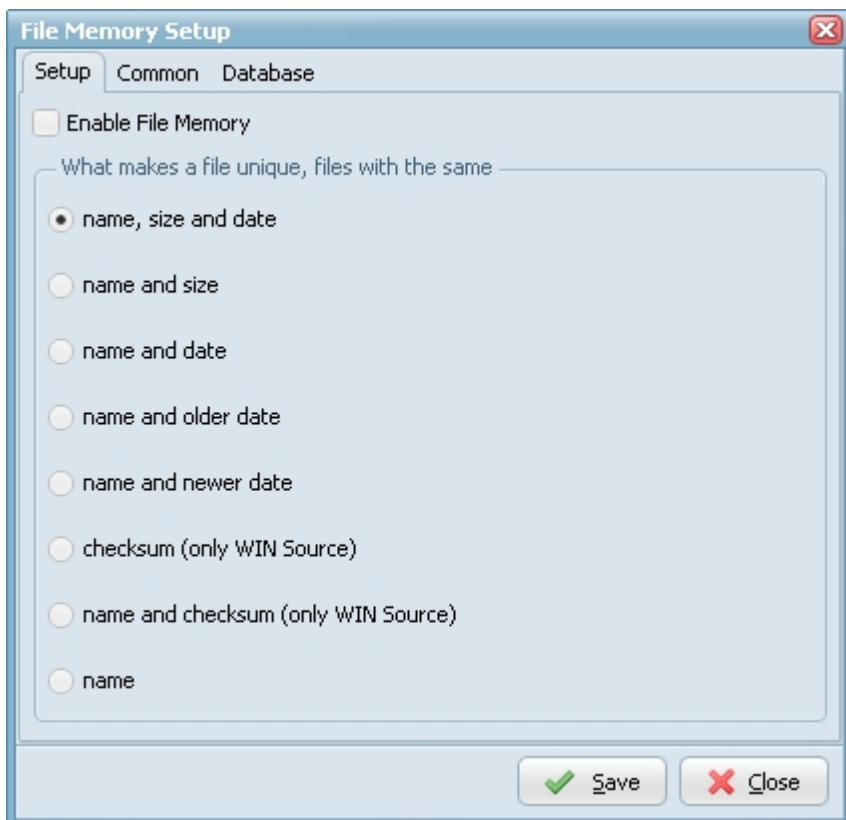
Save Close

Subdirectory Size Exclude Filter

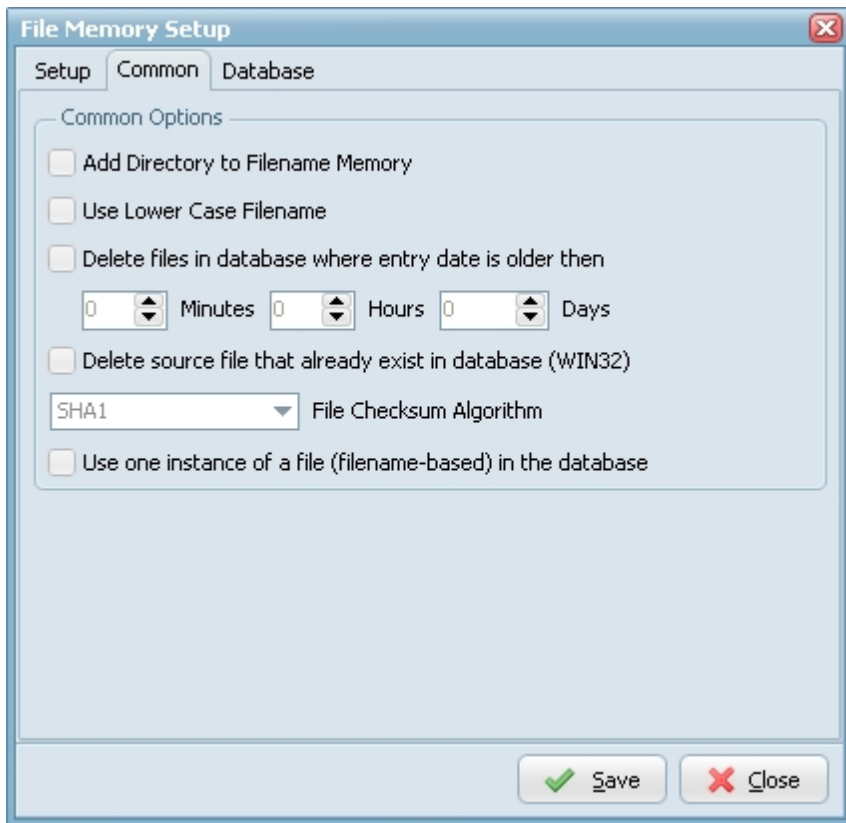


Memory

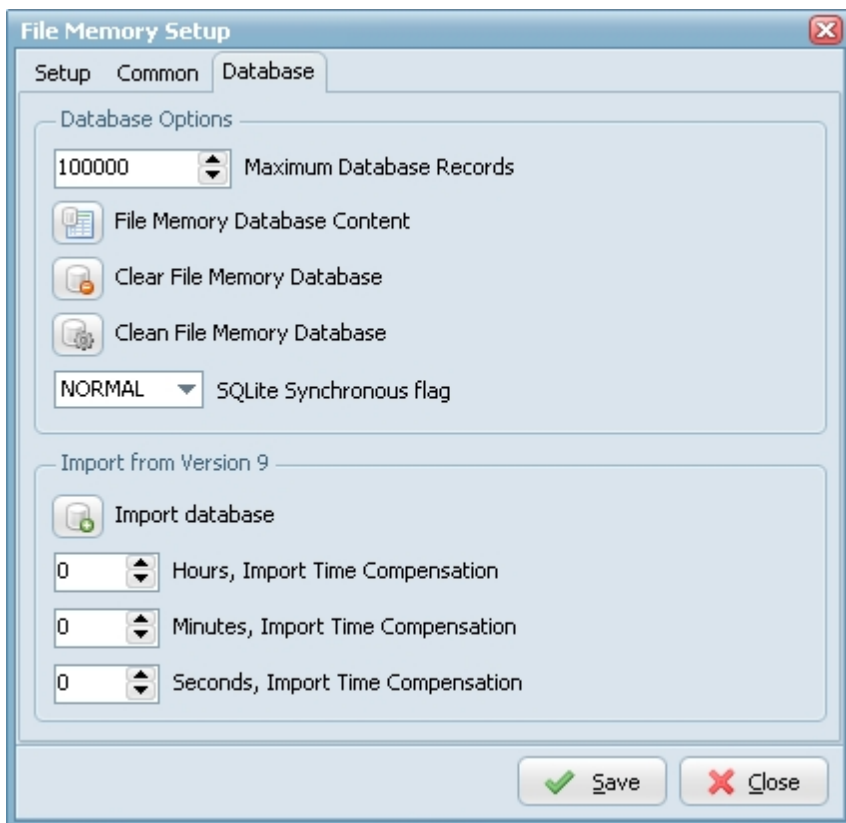
Memory Setup



- ▶ Enable File Memory: Mostly used with 'Copy File' as Rule Function to create a one way sync rule.
- ▶ What makes a file unique, files with the same:
 - ▶ name, size and date => files with the same name, size and date will be moved/copied/deleted once.
 - ▶ name and size => files with the same name and size will be moved/copied/deleted once.
 - ▶ name and date => files with the same name and date will be moved/copied/deleted once.
 - ▶ name and older date => Only older files will be moved/copied/deleted.
 - ▶ name and newer date => Only newer files will be moved/copied/deleted.
 - ▶ checksum (WIN as Source) => files with the same checksum will be moved/copied/deleted once.
 - ▶ name and checksum (WIN as Source) => files with the same name and checksum will be moved/copied/deleted once.
 - ▶ name => files with the same name will be moved/copied/deleted once.



- ▶ Add Directory to Filename Memory: Add Directory to Filename Memory Field (Default value is False).
- ▶ Use Lower Case Filename: Use Lower Case in Filename Memory Field (Default value is False).
- ▶ Delete files in database where entry date is older then: This will delete all files in the file memory database where the entry data (data when file was added to this database) is older then.
- ▶ Delete source file that already exist in database: Source file will be delete if the file is already available in the file memory database (WIN as Source Only).
- ▶ File Checksum Algorithm: Checksum algorithm used for file checksum.
- ▶ Use one instance of a file (filename-based) in the database: Use one instance of a file (filename-based) in the database (Default False).

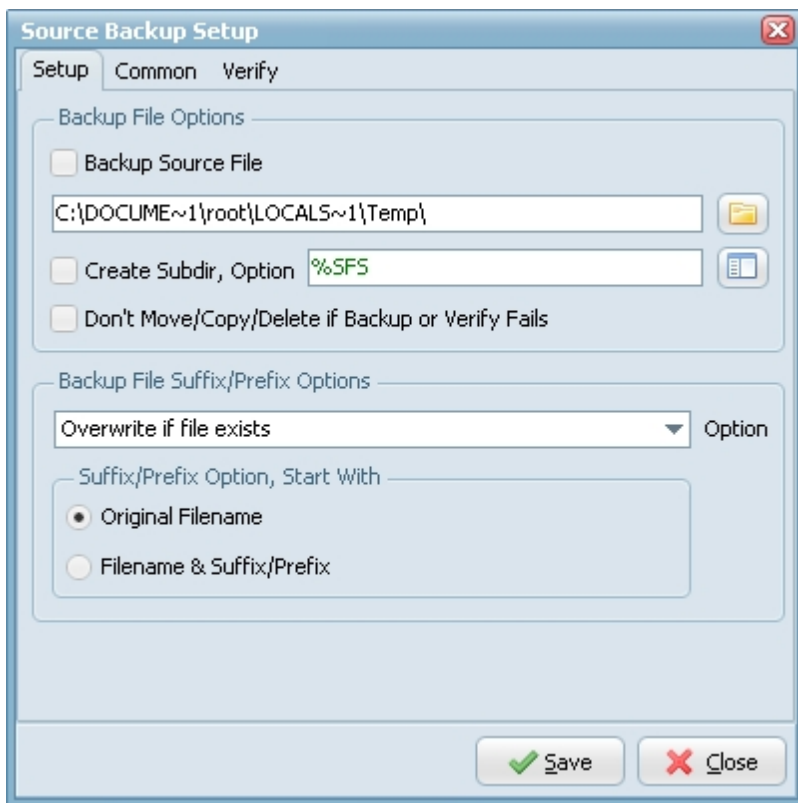


- ▶ **File Memory Database Content:** Shows the files already copied, moved or deleted by LimagitoX.
- ▶ **Clear File Memory Database:** Clear all information in the file Memory.
- ▶ **Clean File Memory Database:** This cleans the file memory database by copying its contents to a temporary database file and reloading the original database file from the copy. This eliminates free pages, aligns table data to be contiguous, and otherwise cleans up the database file structure.
- ▶ **SQLite Synchronous flag:** When synchronous is FULL (2), the SQLite database engine will pause at critical moments to make sure that data has actually been written to the disk surface before continuing. This ensures that if the operating system crashes or if there is a power failure, the database will be uncorrupted after rebooting. FULL synchronous is very safe, but it is also slower. When synchronous is NORMAL (1), the SQLite database engine will still pause at the most critical moments, but less often than in FULL mode. There is a very small (though non-zero) chance that a power failure at just the wrong time could corrupt the database in NORMAL mode. But in practice, you are more likely to suffer a catastrophic disk failure or some other unrecoverable hardware fault. With synchronous OFF (0), SQLite continues without pausing as soon as it has handed data off to the operating system. If the application running SQLite crashes, the data will be safe, but the database might become corrupted if the operating system crashes or the computer loses power before that data has been written to the disk surface. On the other hand, some operations are as much as 50 or more times faster with synchronous OFF.

Backup

Source Backup Setup

Setup Options

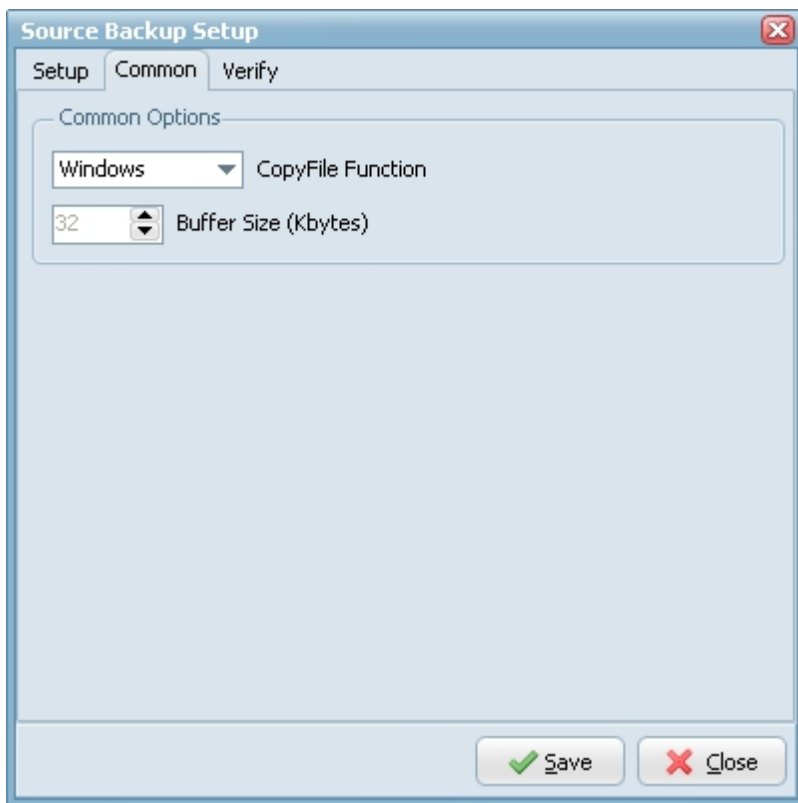


- ▶ Backup Source File: Enable this to backup the original source file before doing the actual function.
- ▶ Don't Move/Copy/Del if Backup or Verify Fails: No move/copy/delete to destination in case of backup or verify error. The actual function won't be triggered.

Backup File Suffix/Prefix Options

- ▶ Overwrite if file exists: Backup file will be overwritten.
- ▶ Only Newer Files: Only newer files will be backed up.
- ▶ Skip if file exists: Skip backup if backup file already exists.
- ▶ Fail if file exists: Error if backup file already exists.
- ▶ Add version number suffix if file exists: Version number suffix will be added if backup file already exists (i.e. "filename.btx.1").
- ▶ Add version number (pre-ext) suffix if file exists: Version number (pre-ext) suffix will be added if backup file already exists (i.e. "filename.1.btx").
- ▶ Add version number prefix if file exists: Version number prefix will be added if backup file already exists (i.e. "1.filename.btx").
- ▶ Add date time suffix if file exists: Date time suffix will be added if backup file already exists (i.e. "filename.btx.20131116114801"). Format date time used: "YYYYMMDDHHNNSS".
- ▶ Add date time (pre-ext) suffix if file exists: Date time (pre-ext) suffix will be added if backup file already exists (i.e. "filename.20131116114801.btx"). Format date time used: "YYYYMMDDHHNNSS".
- ▶ Add date time prefix if file exists: Date time prefix will be added if backup file already exists (i.e. "20131116114801.filename.btx"). Format date time used: "YYYYMMDDHHNNSS".
- ▶ Suffix/Prefix Option, Start With
 - ▶ Original Filename: First backup will be the original filename when suffix/prefix option is chosen (i.e. "filename.btx").
 - ▶ Filename & Suffix/Prefix: First backup will be the original filename & suffix/prefix when suffix/prefix option is chosen (i.e. "filename.btx.1").

Common Options

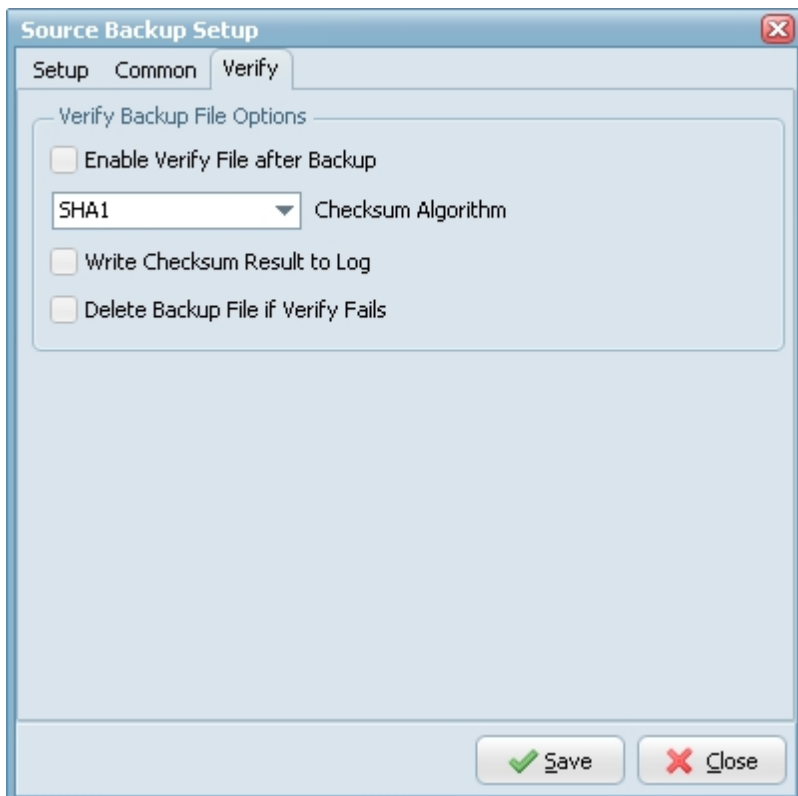


► CopyFile Function:

- Windows (default): use the windows CopyFile API.
- Chunks: copy the file in chunks. With chunks you can terminate the copy/move process anytime you like. The progressbar will only work with the Chunks CopyFile Function.

► Buffer Size: Size chunks in Kbytes (Default value is 32 Kbytes).

Verify Options

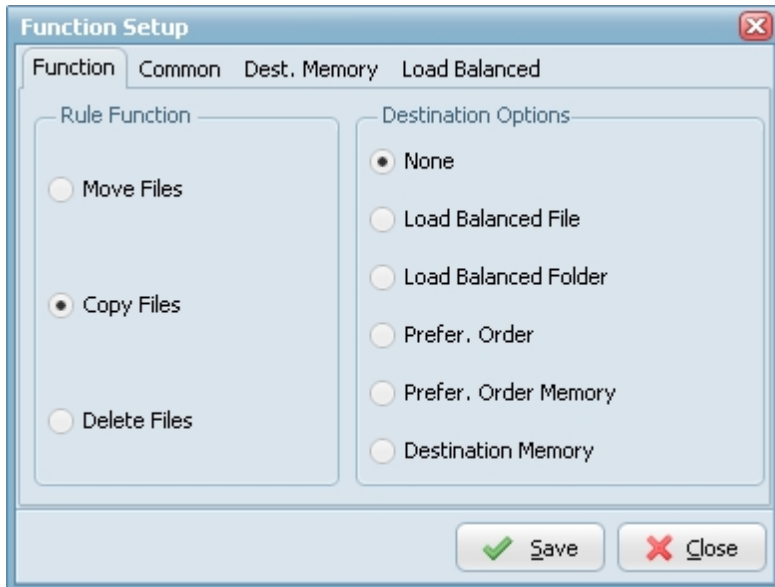


- ▶ Enable Verify File after Backup: Compares source and backup files for verified transfer integrity.
- ▶ Checksum Algorithm: Checksum Algorithm used for verified WIN transfer integrity (SHA1, MD5, ...).
- ▶ Write Checksum Result to Log: The Checksum result will be written to the log file.
- ▶ Delete Backup File if Verify Fail: The backup file will be deleted if verification fails.

Function

Function Setup

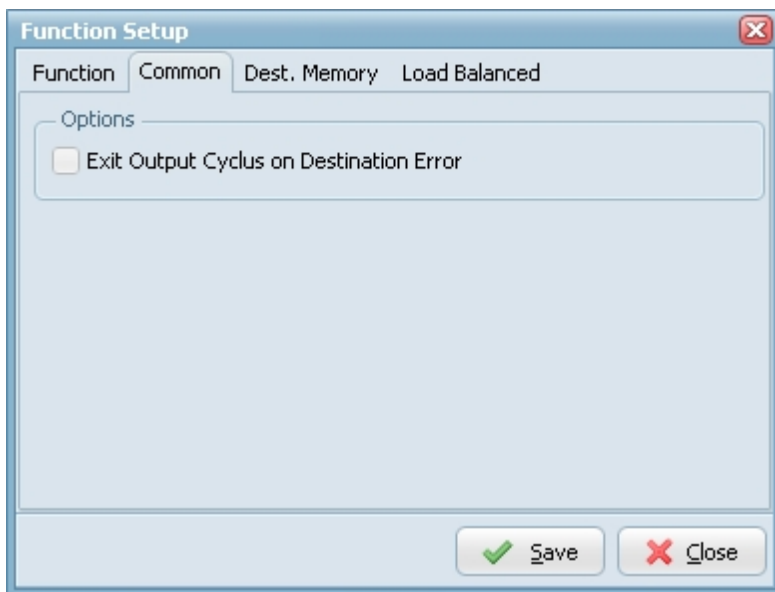
Function Options



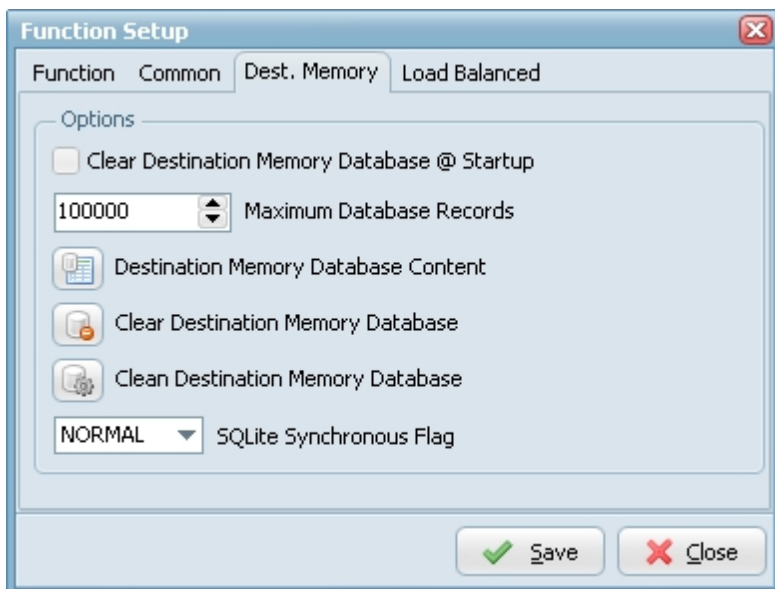
Destination Options:

- ▶ Load Balanced File: Use load balancing technique with destinations. You need more than one destination when you want to use this option. Example with two destinations: The first source file will go to the first destination. The second source file will go to the second destination. The third source file will go to the first destination ...
- ▶ Load Balanced Folder: Use load balancing technique with destinations. You need more than one destination when you want to use this option. Example with two destinations: The files from the first source subdirectory will go to the first destination. The files from the second source subdirectory will go to the second destination. The files from the third source subdirectory will go to the first destination ...
- ▶ Prefer. Order: Use preference technique with destinations. You need more than one destination when you want to use this option. Example with two destinations: The first file will go to the first destination if this destination is available. If not then the first file will go to the second destination. The second file will go to the first destination if this destination is available. If not then this second file will go to the second destination.
- ▶ Destination Memory: Use destination memory technique with destinations. You need more than one destination when you want to use this option. LimagitoX will remember if copy/move to one of the destinations fails and will try to copy/move the file during the next scan. It will only try to copy/move the file again to this destination where there was an error.

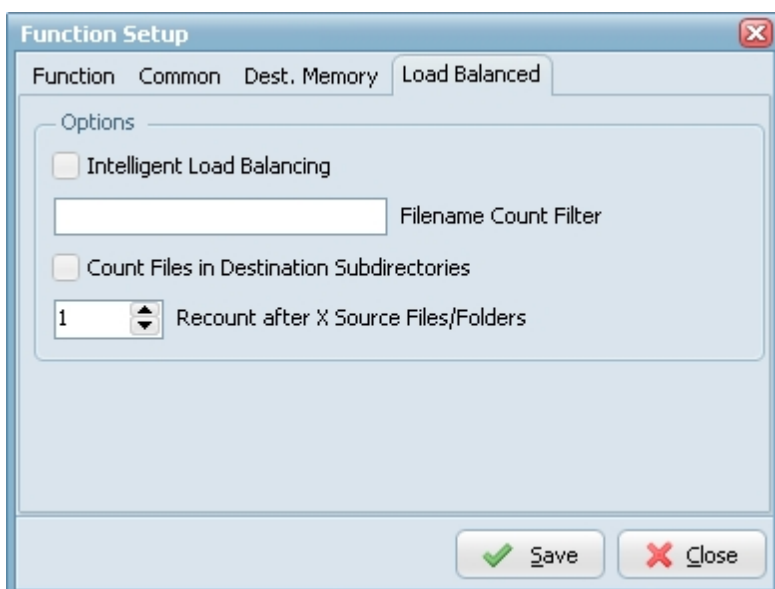
Common Options



Destination Memory Options

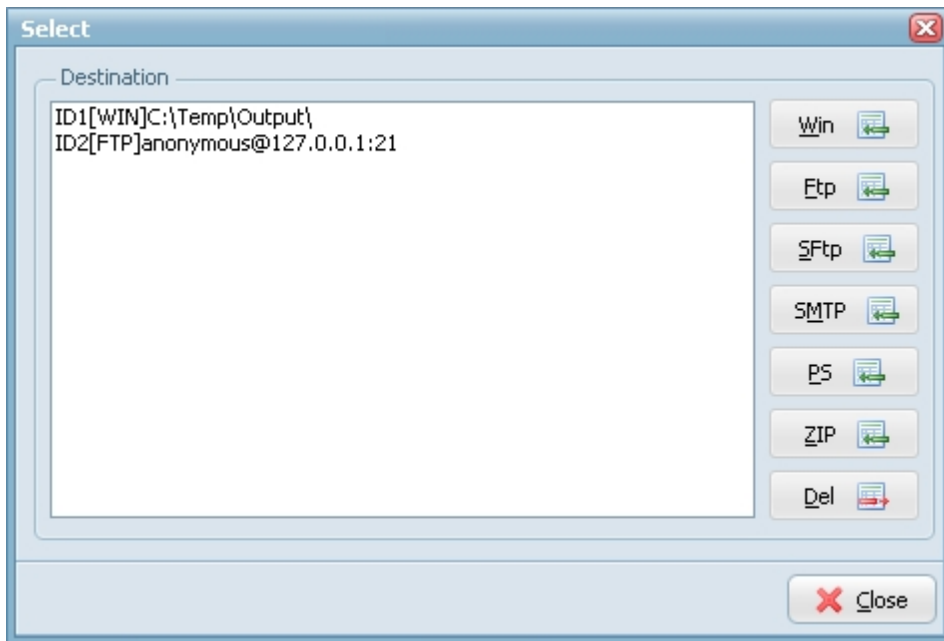


Load Balancing Options



Destination Options

Destination Selection



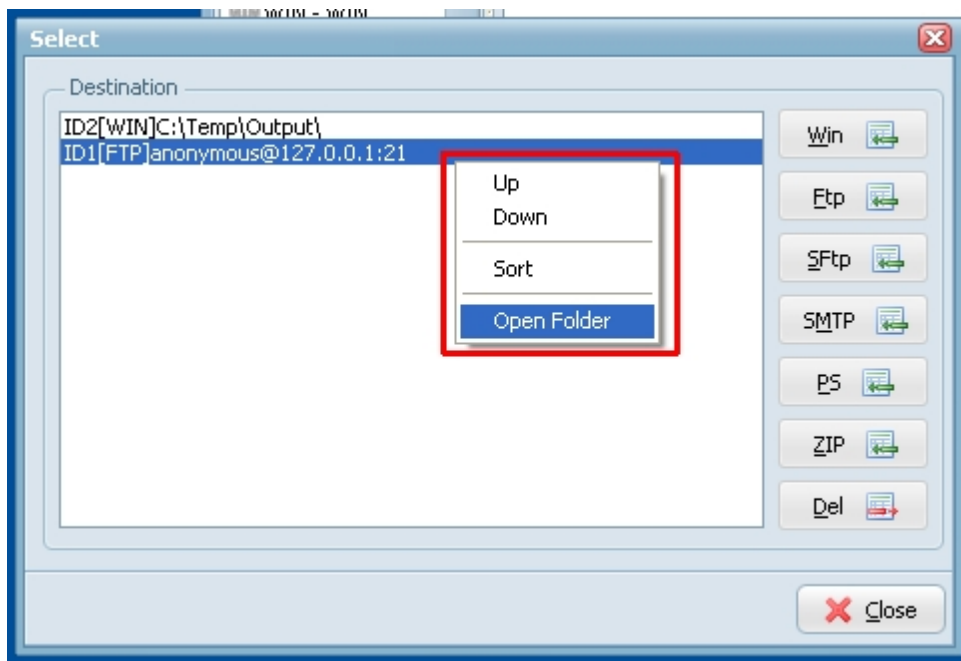
LimagitoX Destination selection possibilities:

- ▶ [WIN](#)
- ▶ [FTP](#)
- ▶ [SFTP](#)
- ▶ [SMTP](#)
- ▶ [PS](#)
- ▶ [ZIP](#)

You can use multiple destinations each using their own settings. Double click on a destination to open it's setup form.



Select the destination you want to remove and select the DEL button (Delete).



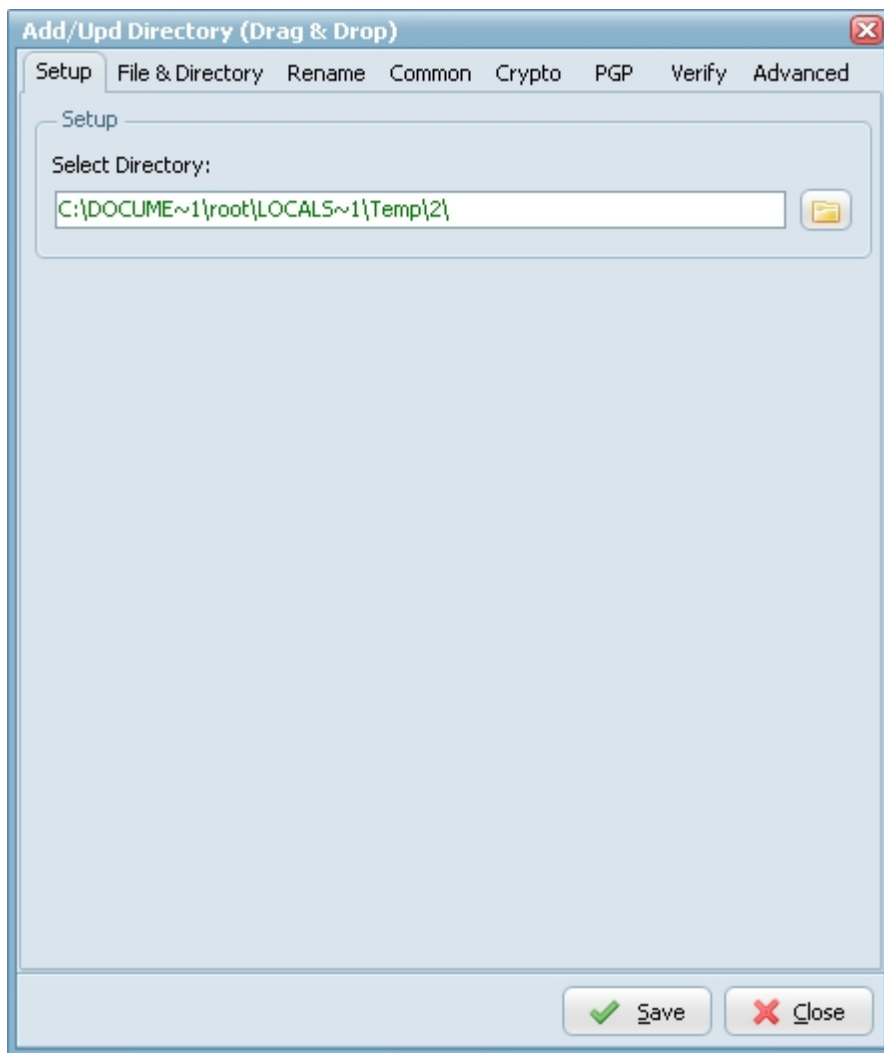
Right click on the selected destination to:

- ▶ change it's position in the destination list view
- ▶ sort the destination list view
- ▶ open and explore the destination folder (WIN, FTP, SFTP)

WIN Destination

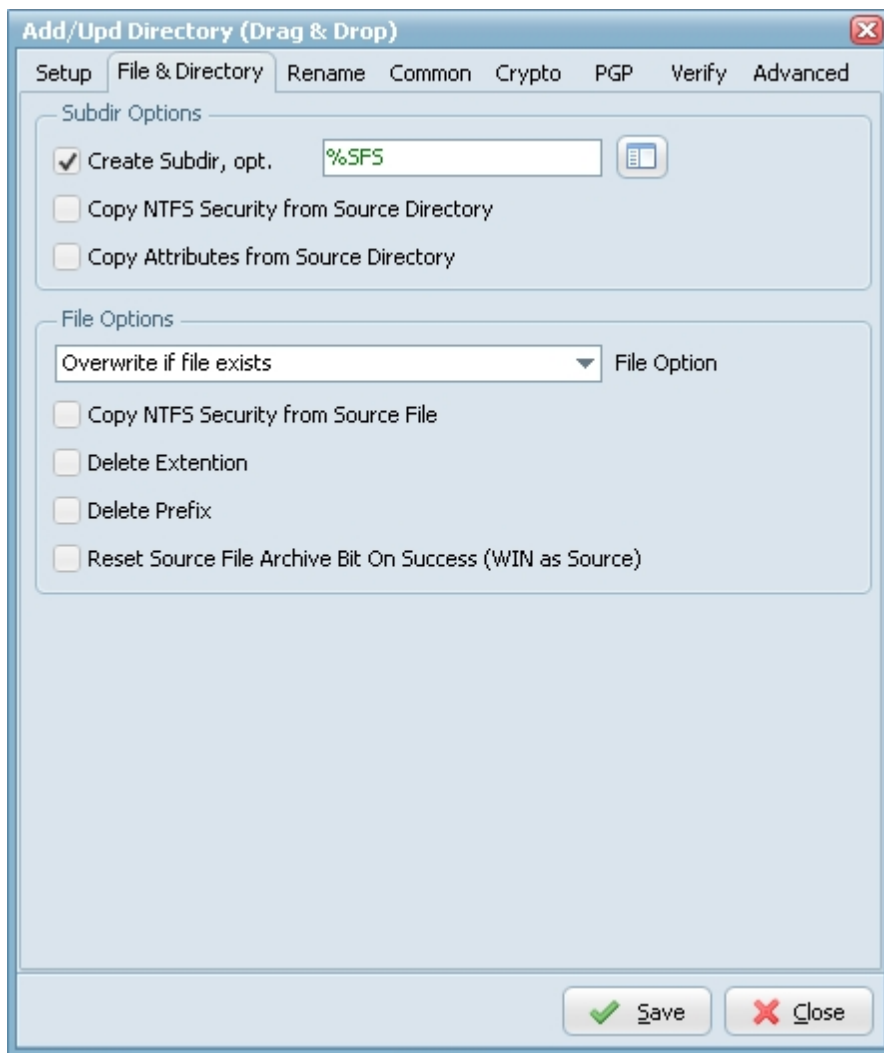
WIN Destination Setup

Setup Options



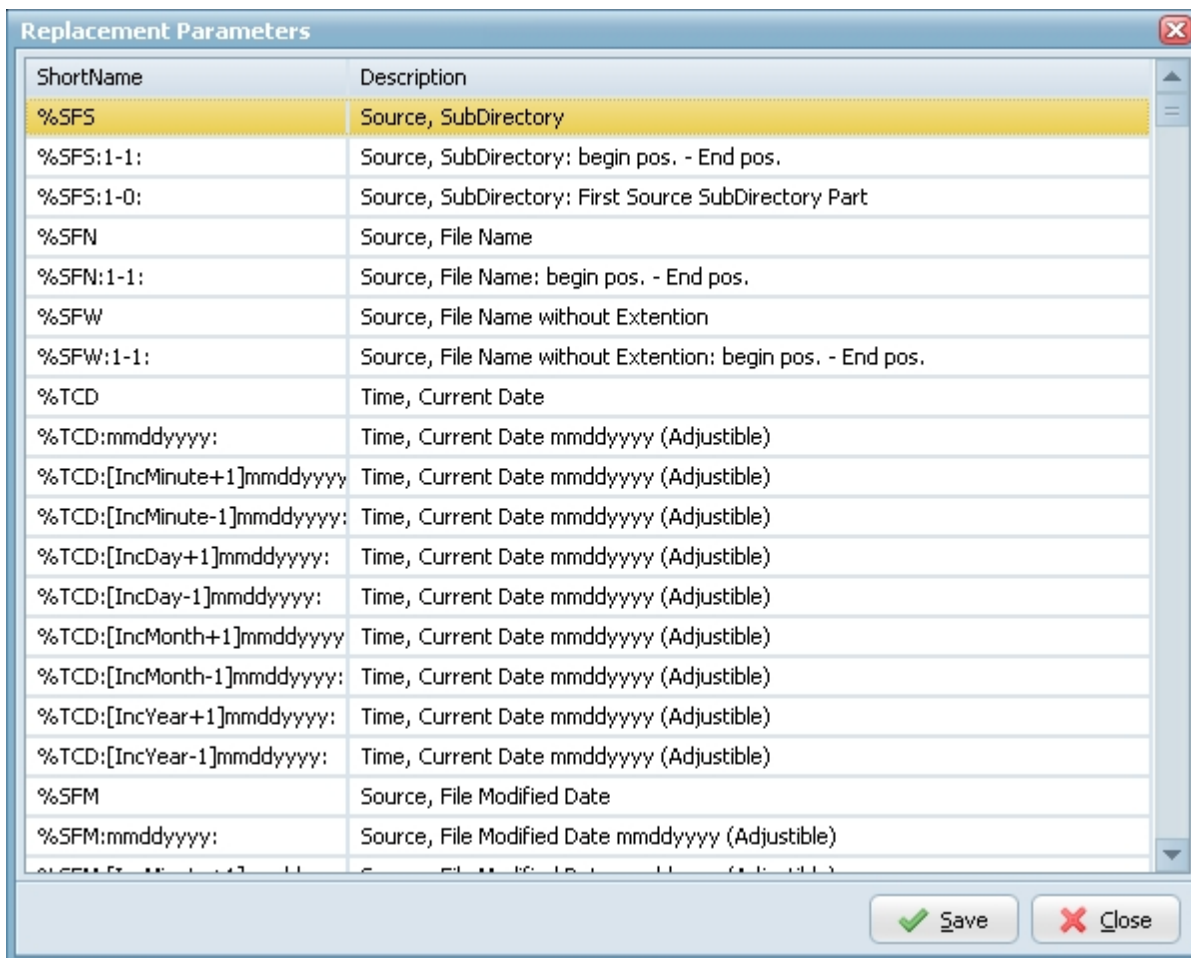
- ▶ Select Directory: Windows destination directory (folder or share).

File & Directory Options



Subdir Options

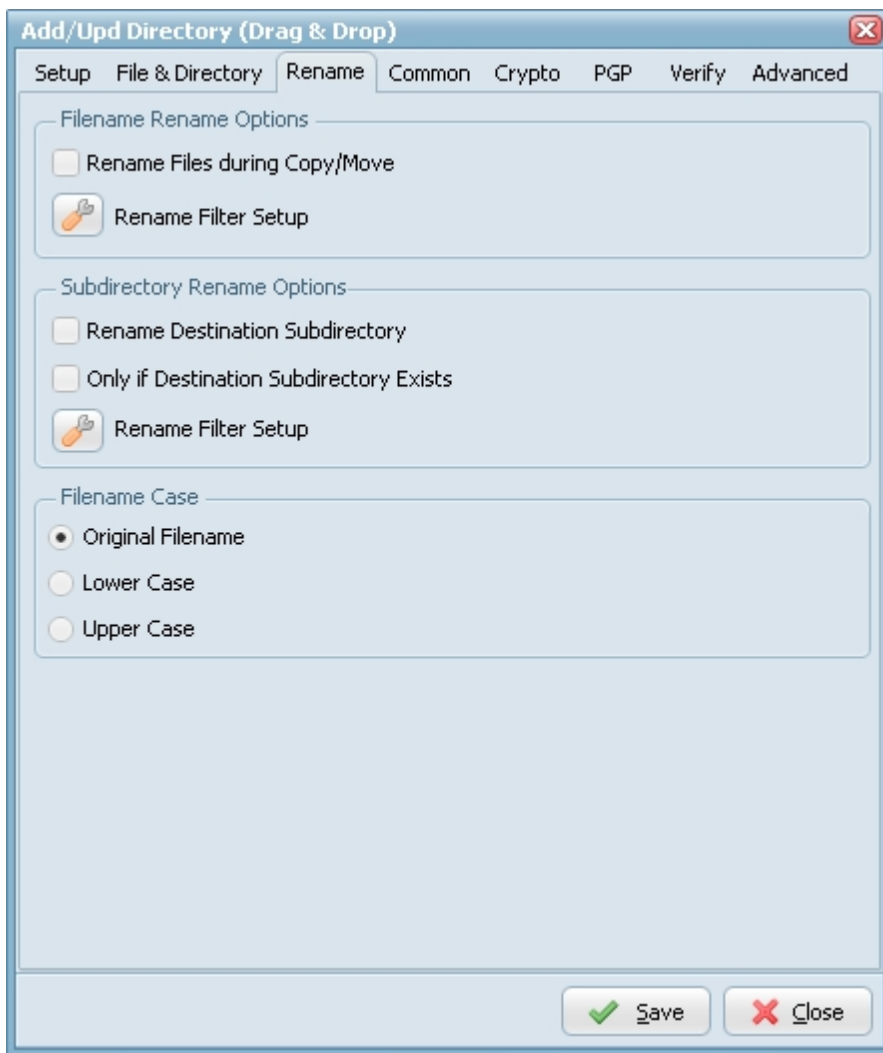
- ▶ Create Subdir: Create Subdirectory for the Windows destination.
- ▶ Create Subdir, option: Different parameters can be used to create the destination directory.



File Options

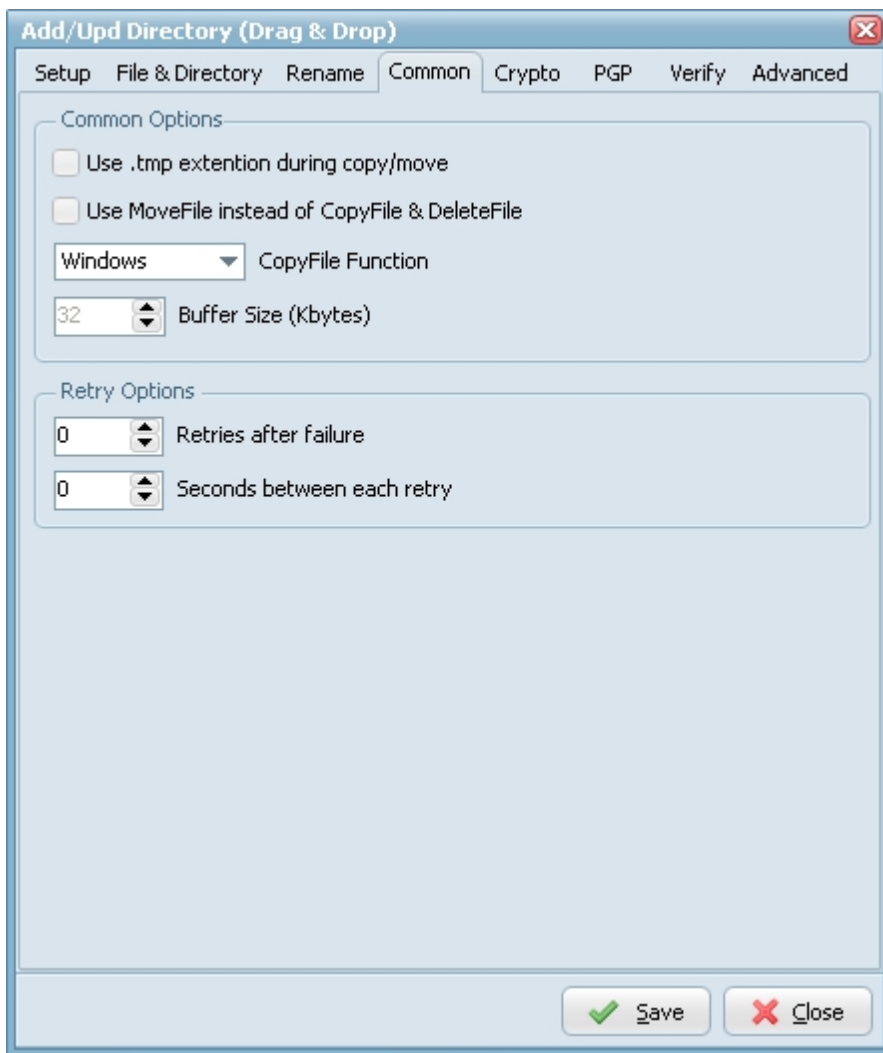
- ▶ Overwrite if file exists: Destination file will be overwritten.
- ▶ Only Newer Files: Only newer files will be processed to the destination.
- ▶ Skip if file exists: Skip if destination file already exists.
- ▶ Fail if file exists: Error if destination file already exists.
- ▶ Add version number suffix if file exists: Version number suffix will be added if destination file already exists (i.e. "filename.txt.1").
- ▶ Add version number (pre-ext) suffix if file exists: Version number (pre-ext) suffix will be added if destination file already exists (i.e. "filename.1.txt").
- ▶ Add version number prefix if file exists: Version number prefix will be added if destination file already exists (i.e. "1.filename.txt").
- ▶ Add date time suffix if file exists: Date time suffix will be added if destination file already exists (i.e. "filename.txt.20131116114801"). Format date time used: "YYYYMMDDHHNNSS".
- ▶ Add date time (pre-ext) suffix if file exists: Date time (pre-ext) suffix will be added if destination file already exists (i.e. "filename.20131116114801.txt"). Format date time used: "YYYYMMDDHHNNSS".
- ▶ Add date time prefix if file exists: Date time prefix will be added if destination file already exists (i.e. "20131116114801.filename.txt"). Format date time used: "YYYYMMDDHHNNSS".
- ▶ Copy NTFS Security from Source File: By default, creating a file in a destination on an NTFS partition, the destination file takes on the security and access control settings of the destinations parent folder. This option will copy the original security/ACL settings to the destination file.
- ▶ Delete Extension: Delete the extension of the destination filename.
- ▶ Delete Prefix: Delete the prefix (see file prefix filter source option) of the destination filename.
- ▶ Reset Source File Archive Bit On Success (WIN as Source): On Windows when a file is created or modified, the archive bit is set, and when the file has been backed up, the archive bit is cleared. It is by use of the archive bit that incremental backups are implemented.

Rename Options



- ▶ Rename Files during Copy/Move: Use regular expressions to rename the destination filename. A very good site with information about regular expressions is <http://www.regular-expressions.info/>
- ▶ Rename Destination Subdirectory: Use regular expressions to rename the destination subdirectory.
- ▶ Only if Destination Subdirectory Exists: Rename only if destination subdirectory already exists.
- ▶ Filename Case: Use original filename, lower case or upper case for the destination filenames.

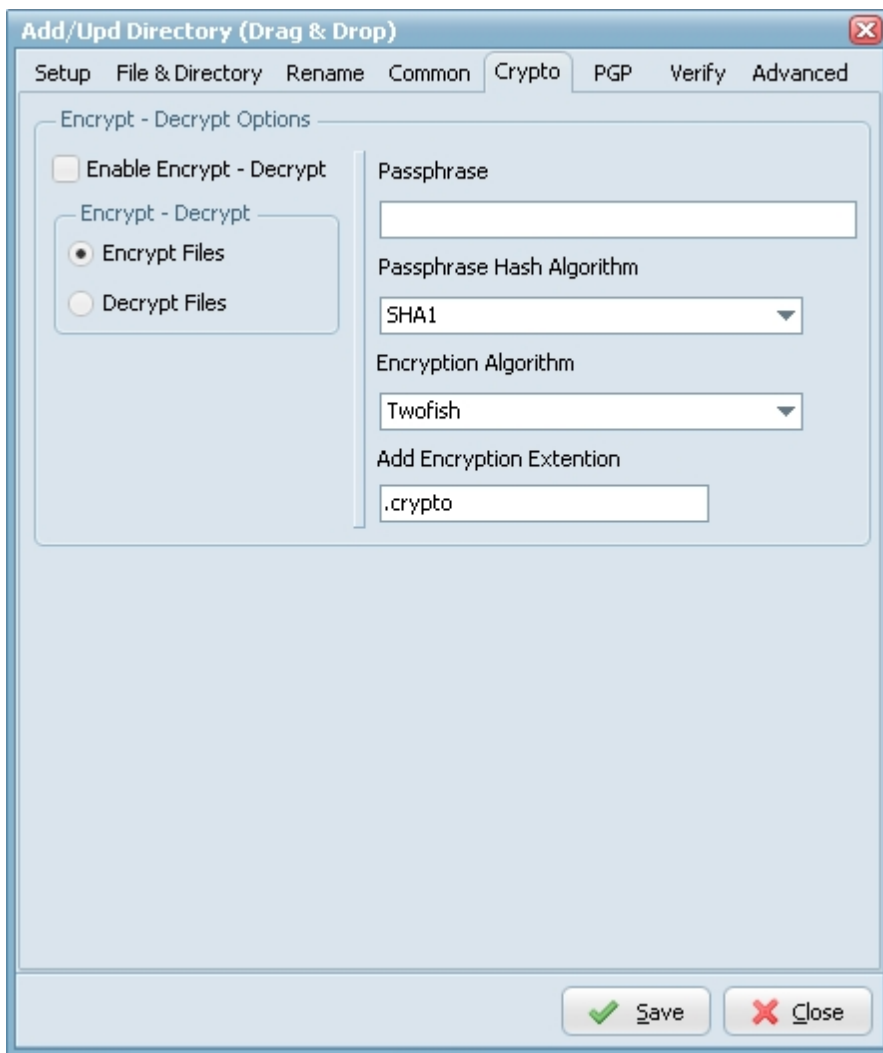
Common Options



Common Options

- ▶ Use MoveFile instead of CopyFile & DeleteFile (WIN as Source): If you have a single (WIN) destination and the destination path is on the same drive as the source path (WIN as Source) then you can use this option. This will speedup the move function.
- ▶ CopyFile Function:
 - ▶ Windows (default): use the windows CopyFile API.
 - ▶ Chunks: copy the file in chunks. With chunks you can terminate the copy/move process anytime you like. The progressbar will only work with the Chunks CopyFile Function.
- ▶ Buffer Size: Size chunks in Kbytes (Default value is 32 Kbytes).

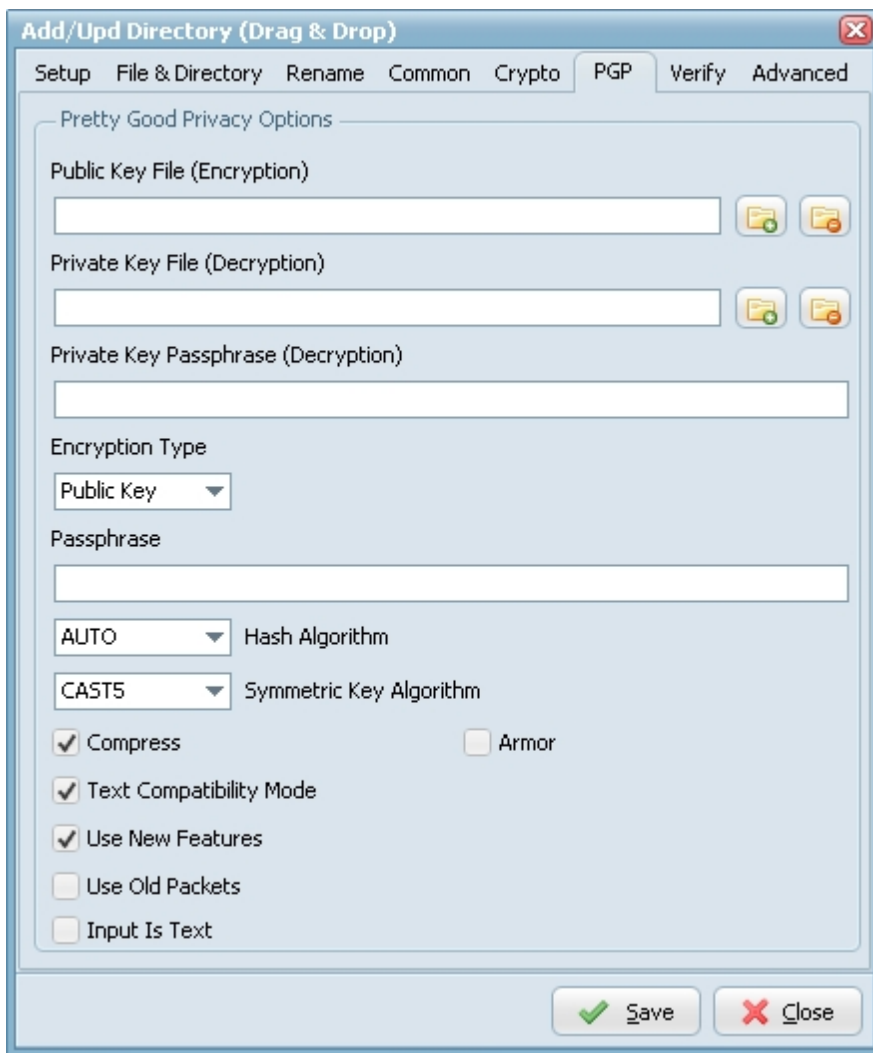
Crypto Options



Encrypt - Decrypt Options

- ▶ Encryption & Decryption using the following Encryption algorithms: Blowfish, Cast 128, Cast 256, DES, 3DES, Ice, Thin Ice, Ice2, IDEA, Mars, Misty1, RC2, RC4, RC5, RC6, Rijndael (the new AES), Serpent, Tea, Twofish and PGP (Pretty Good Privacy). You can use the following Hash Algorithms for the password: Haval, MD4, MD5, RipeMD-128, RipeMD-160, SHA-1, SHA-256, SHA-384, SHA-512, Tiger. LimagitoX uses a 64 bit Salt. Salt = Random data that is included as part of a session key. When added to a session key, the plaintext salt data is placed in front of the encrypted key data. Salt values are added to increase the work required to mount a brute-force (dictionary) attack against data encrypted with a symmetric-key cipher.
- ▶ Encryption & Decryption available in Site and Corporate License. Encryption available in Lite and Single License.

PGP Options

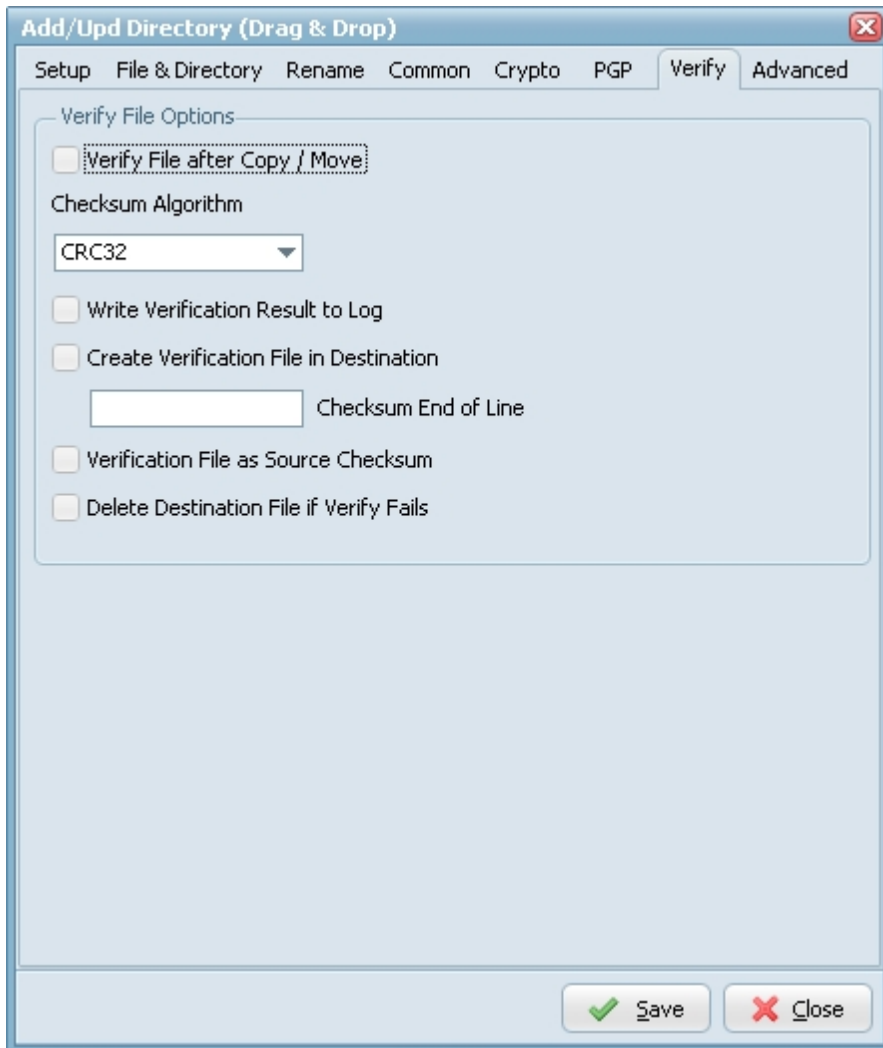


To enable PGP you need to set the Encryption Algorithm to PGP (check the Crypto Tab).

- ▶ **Public Key File:** Use this option to set the keyring with keys for data encryption.
- ▶ **Private Key File:** Use this option to determine keyring with keys for decryption.
- ▶ **Private Key Passphrase:** This option specifies password that will be used when trying to decrypt the private (secret) key used for file encryption.
- ▶ **Encryption Type:**
 - ▶ Both: both public key and password will be used for encryption. It implies, that decryption can be performed by either the password or the private (secret) key.
- ▶ **Passphrase:** This property specifies the password that will be tried to use when decrypting the file, which was previously encrypted using symmetric algorithm (not with a public key).
- ▶ **Hash Algorithm:** Use this option to set algorithm that will be used for hash calculation.
- ▶ **Symmetric Key Algorithm:** Specifies the symmetric algorithm for data encryption.
- ▶ **Compress:** Data will be compressed before encryption.
- ▶ **Text Compatibility Mode:** Several versions of PGP have bug in their implementations that results in creation of incorrect text signatures. The following paragraph is taken from RFC 2440: «PGP 2.6.X and 5.0 do not trim trailing whitespace from a "canonical text" signature. They only remove it from cleartext signatures. These signatures are not OpenPGP compliant -- OpenPGP requires trimming the whitespace. If you wish to interoperate with PGP 2.6.X or PGP 5, you may wish to accept these non-compliant signatures.» One can say that this bug also exists in PGP6.5 and PGP8.0 implementations. It is a good idea to enable this property if you want to interoperate with those versions of PGP. Disable this option if you need to create OpenPGP-compliant messages.
- ▶ **Use New Features:** Use this option for compatibility with old versions of PGP-compatible software. If this option is enabled, then newer and stronger algorithms will be used. In this case ClearTextSign and Sign will be compatible with PGP 2.6.x, while Encrypt and EncryptAndSign will not. If the option is disabled, then the result will be compatible with PGP 2.6.x, while the keys are compatible (i.e. don't use features not supported by PGP 2.6.x).
- ▶ **Use Old Packets:** If this option is enabled only packets of old format will be used in order for compatibility with PGP 2.6.x.
- ▶ **Input Is Text:** Use this option when you want to specify that input data must be interpreted as text.

- ▶ **Armor:** Use this option to determine if resulting data should be armored, i.e. wrapped into base64-cover. ASCII armor is a binary-to-textual encoding converter. ASCII armor is a feature of a type of encryption called pretty good privacy (PGP). ASCII armor involves encasing encrypted messaging in ASCII so that they can be sent in a standard messaging format such as email.

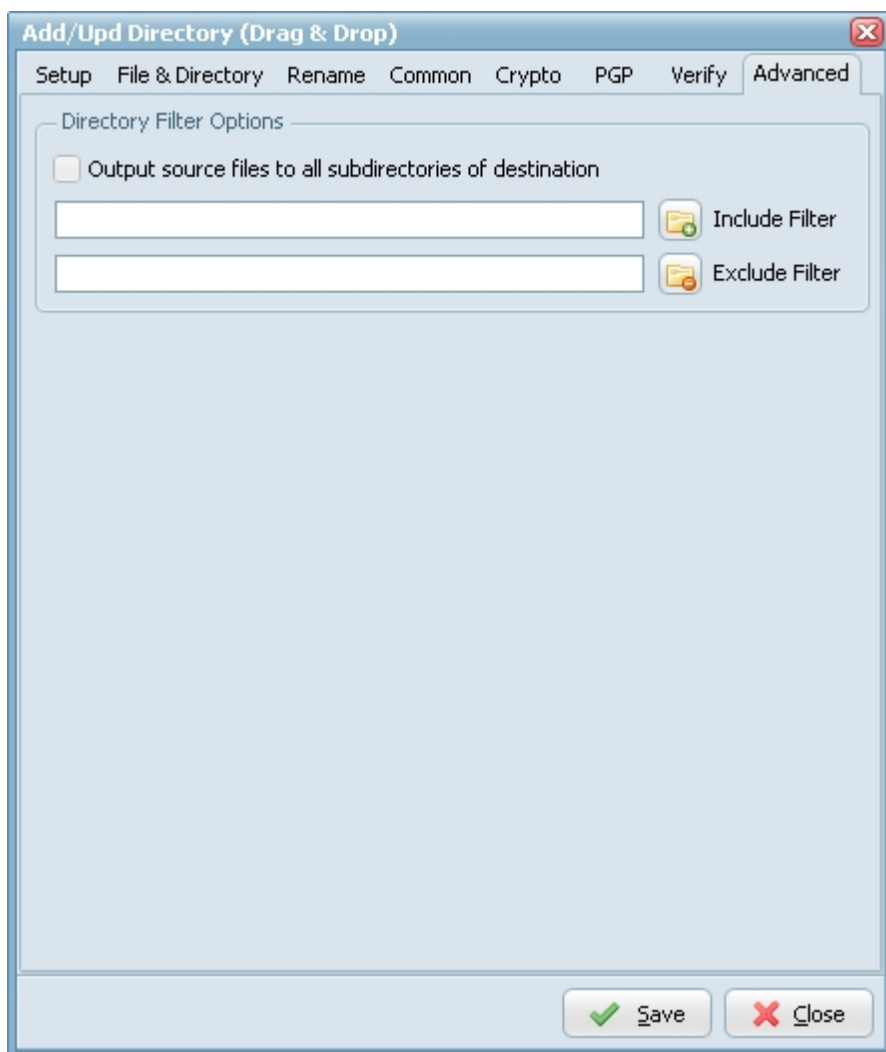
Verify Options



Verify File Options

- ▶ **Verify File after Copy/Move:** Compares source and destination file for verified transfer integrity.
- ▶ **Checksum Algorithm:** Checksum Algorithm used for verified transfer integrity.
- ▶ **Write Checksum result to Log:** Checksum result will be written into the Log file.
- ▶ **Create Verification File in Destination:** Will create a verification file in the destination directory with the checksum of the file.
- ▶ **Checksum End of Line:** Info will be added after the actual checksum. Add %CWS*%DFN for original unix interchange.
 - ▶ %CWS = Char WhiteSpace
 - ▶ %DFN = Destination FileName
- ▶ **Verification File as Source Checksum:** If verification file exists then use this file as source checksum otherwise calculate source checksum.
- ▶ **Delete Destination File if Verify Fail:** Destination file will be deleted if verification fails.

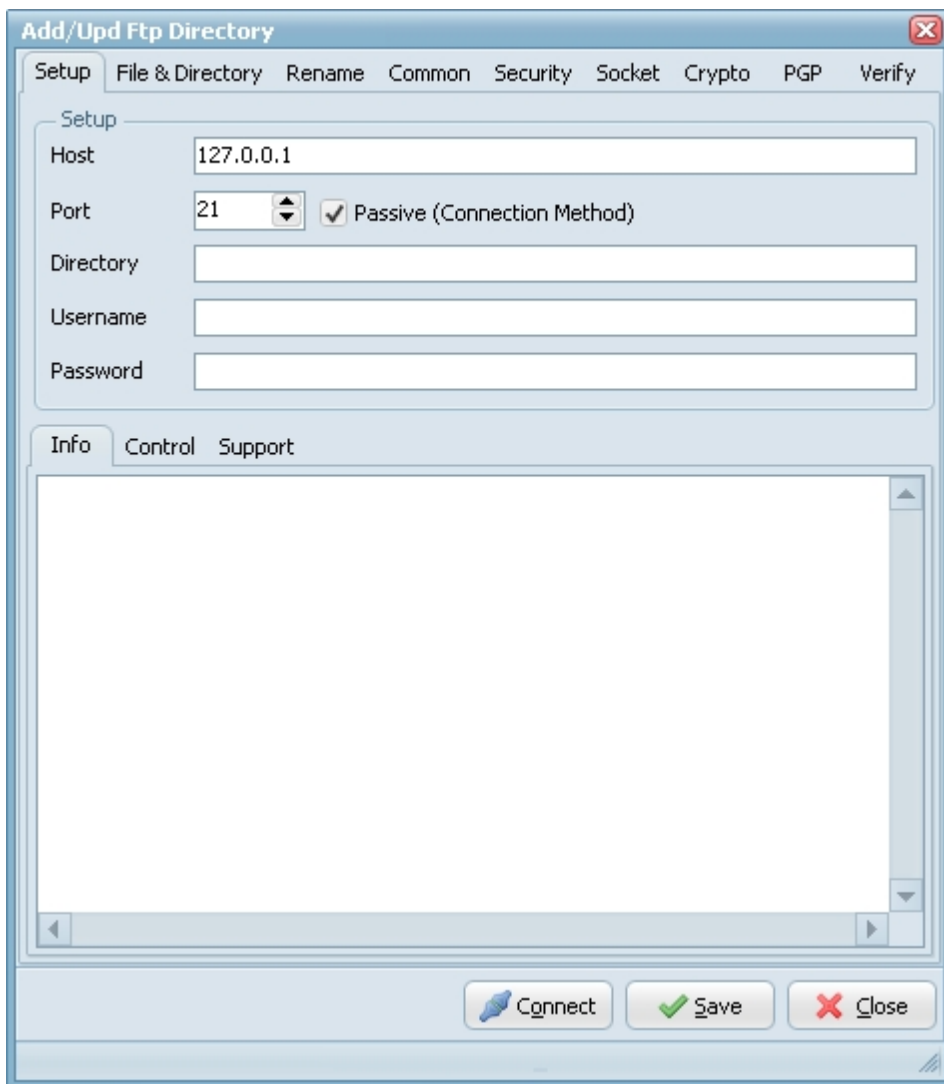
Advanced Options



FTP Destination

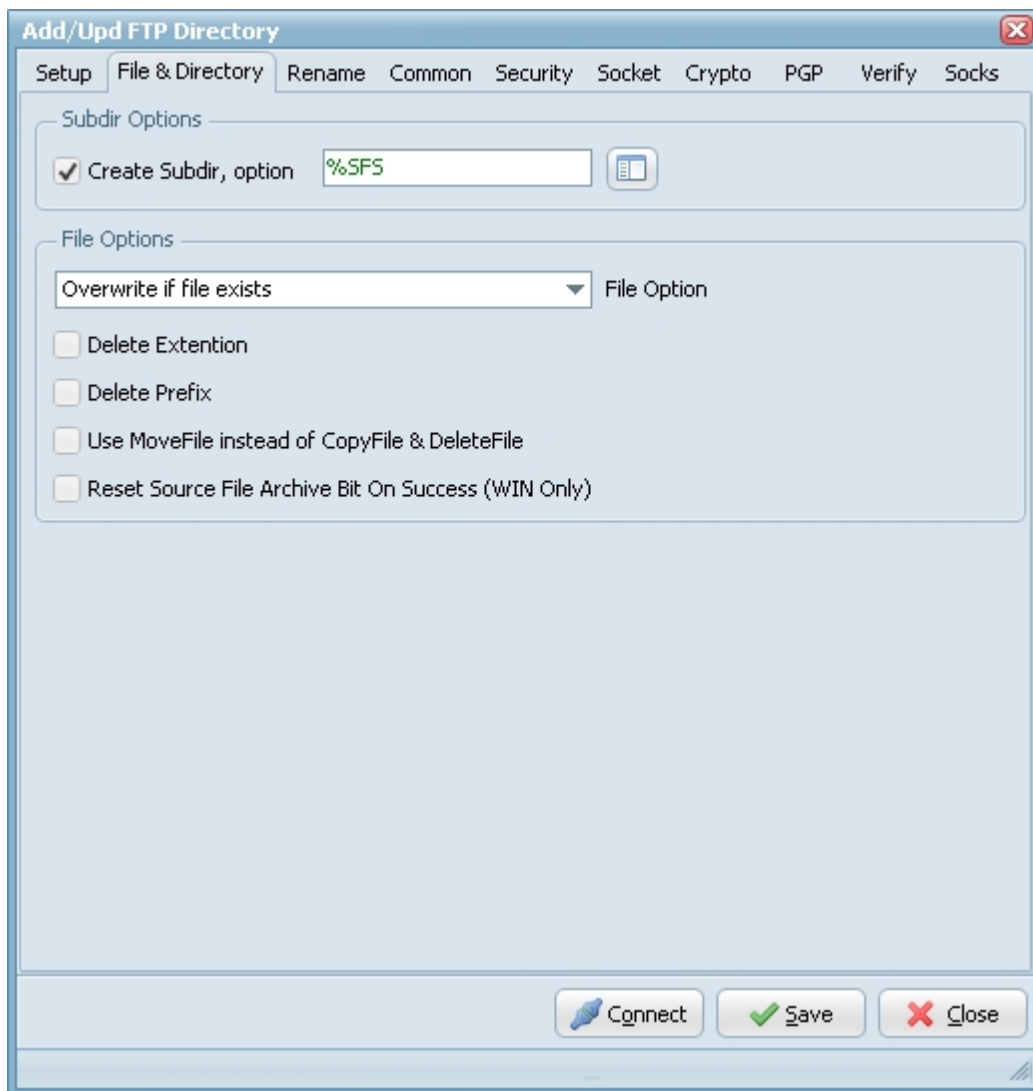
FTP Destination Setup

Setup Options



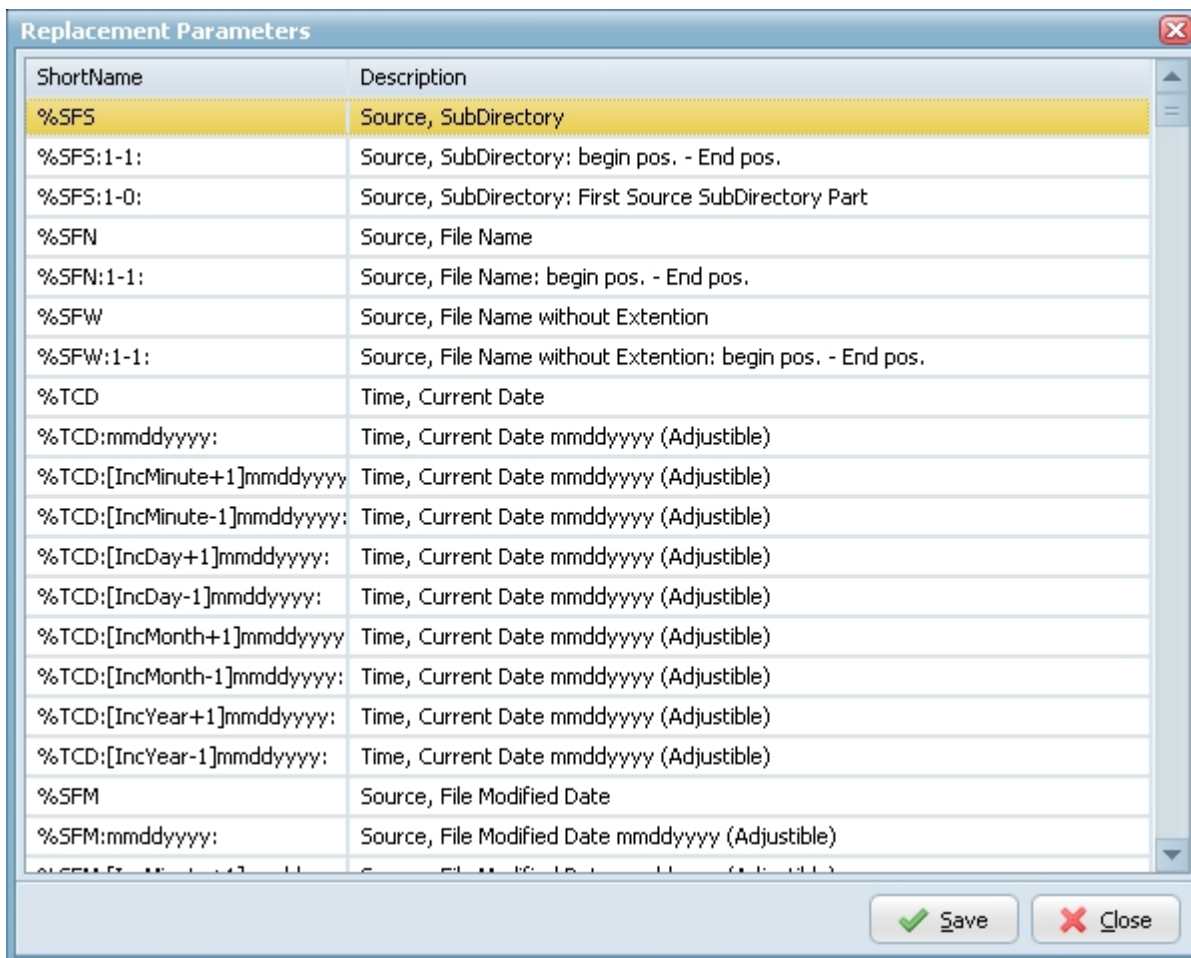
- ▶ Host: This option specifies the address of the host to connect to.
- ▶ Port: Port number on the host to connect to (Default value is 21).
- ▶ Passive: Active connections (or when Passive is disabled) indicates that the FTP server will open the connection for the data channel. In other words, the FTP client will listen for the server to open a connection for the data channel.
- ▶ Directory: Directory on the server file system.
- ▶ Username: Authentication identity used when logging in to the server (example: Anonymous).
- ▶ Password: Authentication credentials used when logging into the server.
- ▶ Connect: Check connection setup.

File & Directory Options



Subdir Options

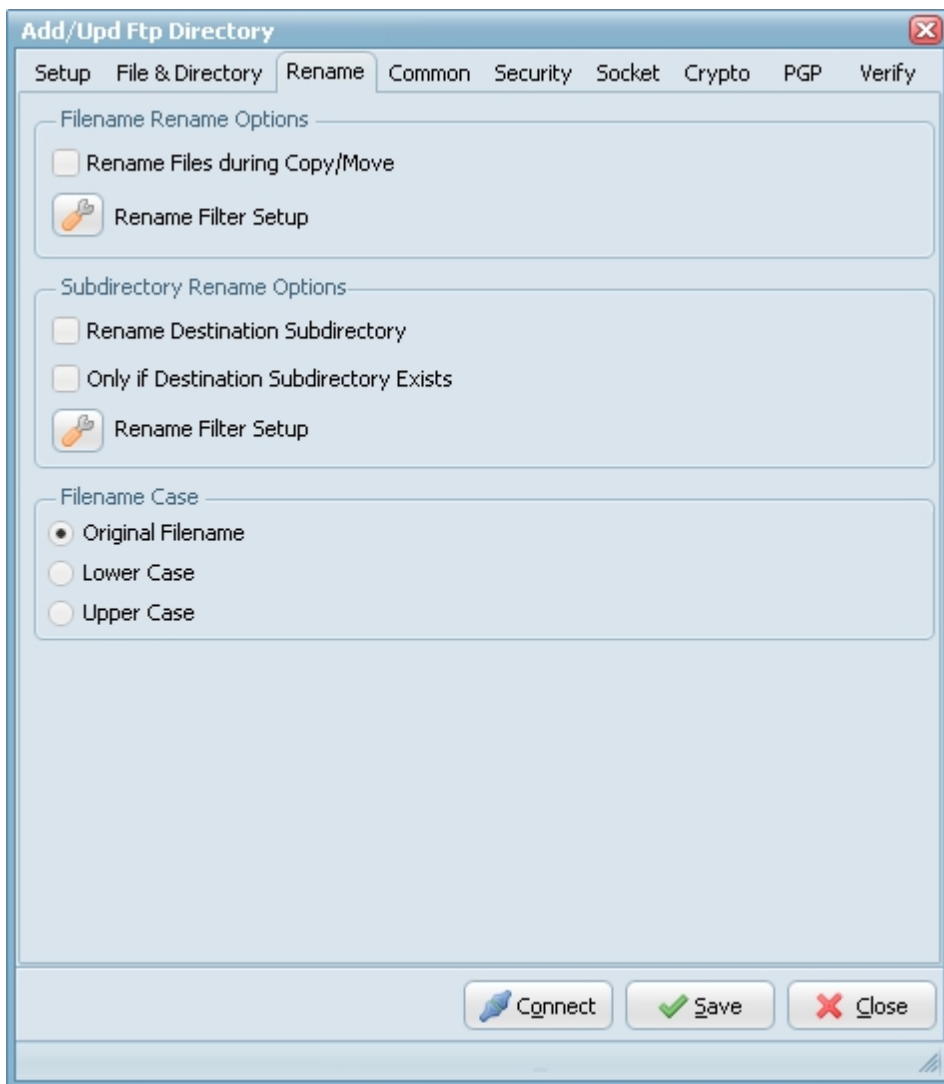
- ▶ Create Subdir: Create Subdirectory for the Windows destination.
- ▶ Create Subdir, option: Different parameters can be used to create the destination directory.



File Options

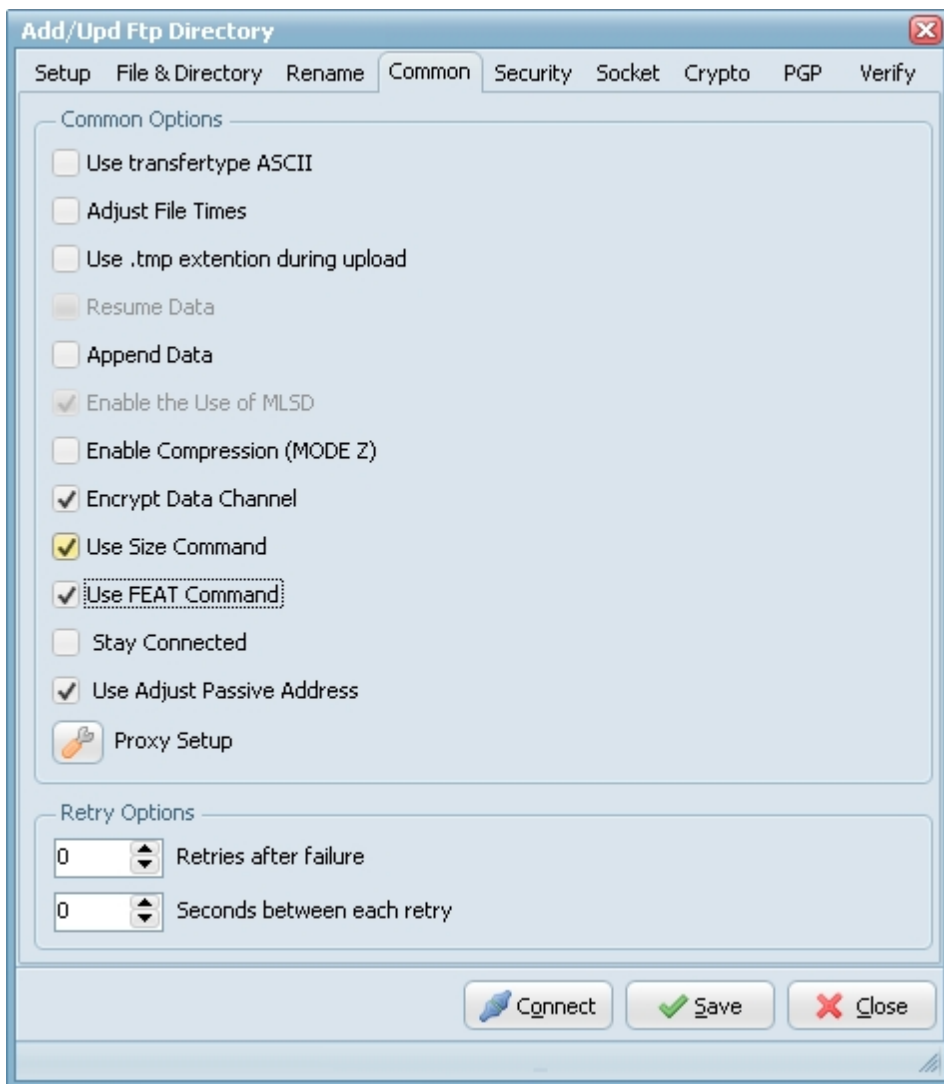
- ▶ Overwrite if file exists: Destination file will be overwritten.
- ▶ Only Newer Files: Only newer files will be processed to the destination.
- ▶ Skip if file exists: Skip if destination file already exists.
- ▶ Fail if file exists: Error if destination file already exists.
- ▶ Add version number suffix if file exists: Version number suffix will be added if destination file already exists (i.e. "filename.txt.1").
- ▶ Add version number (pre-ext) suffix if file exists: Version number (pre-ext) suffix will be added if destination file already exists (i.e. "filename.1.txt").
- ▶ Add version number prefix if file exists: Version number prefix will be added if destination file already exists (i.e. "1.filename.txt").
- ▶ Add date time suffix if file exists: Date time suffix will be added if destination file already exists (i.e. "filename.txt.20131116114801"). Format date time used: "YYYYMMDDHHNNSS".
- ▶ Add date time (pre-ext) suffix if file exists: Date time (pre-ext) suffix will be added if destination file already exists (i.e. "filename.20131116114801.txt"). Format date time used: "YYYYMMDDHHNNSS".
- ▶ Add date time prefix if file exists: Date time prefix will be added if destination file already exists (i.e. "20131116114801.filename.txt"). Format date time used: "YYYYMMDDHHNNSS".
- ▶ Delete Extension: Delete the extension of the destination filename.
- ▶ Delete Prefix: Delete the prefix (see file prefix filter source option) of the destination filename.
- ▶ Reset Source File Archive Bit On Success (WIN as Source): On Windows when a file is created or modified, the archive bit is set, and when the file has been backed up, the archive bit is cleared. It is by use of the archive bit that incremental backups are implemented.

Rename Options



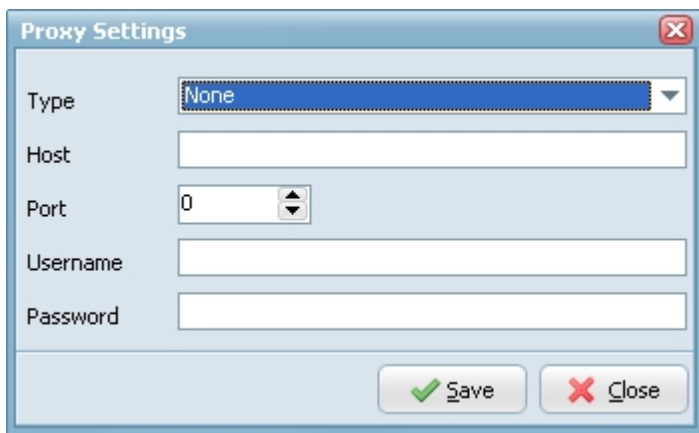
- ▶ **Rename Files during Copy/Move:** Use regular expressions to rename the destination filename. A very good site with information about regular expressions is <http://www.regular-expressions.info/>
- ▶ **Rename Destination Subdirectory:** Use regular expressions to rename the destination subdirectory.
- ▶ **Only if Destination Subdirectory Exists:** Rename only if destination subdirectory already exists.
- ▶ **Filename Case:** Use original filename, lower case or upper case for the destination filenames.

Common Options



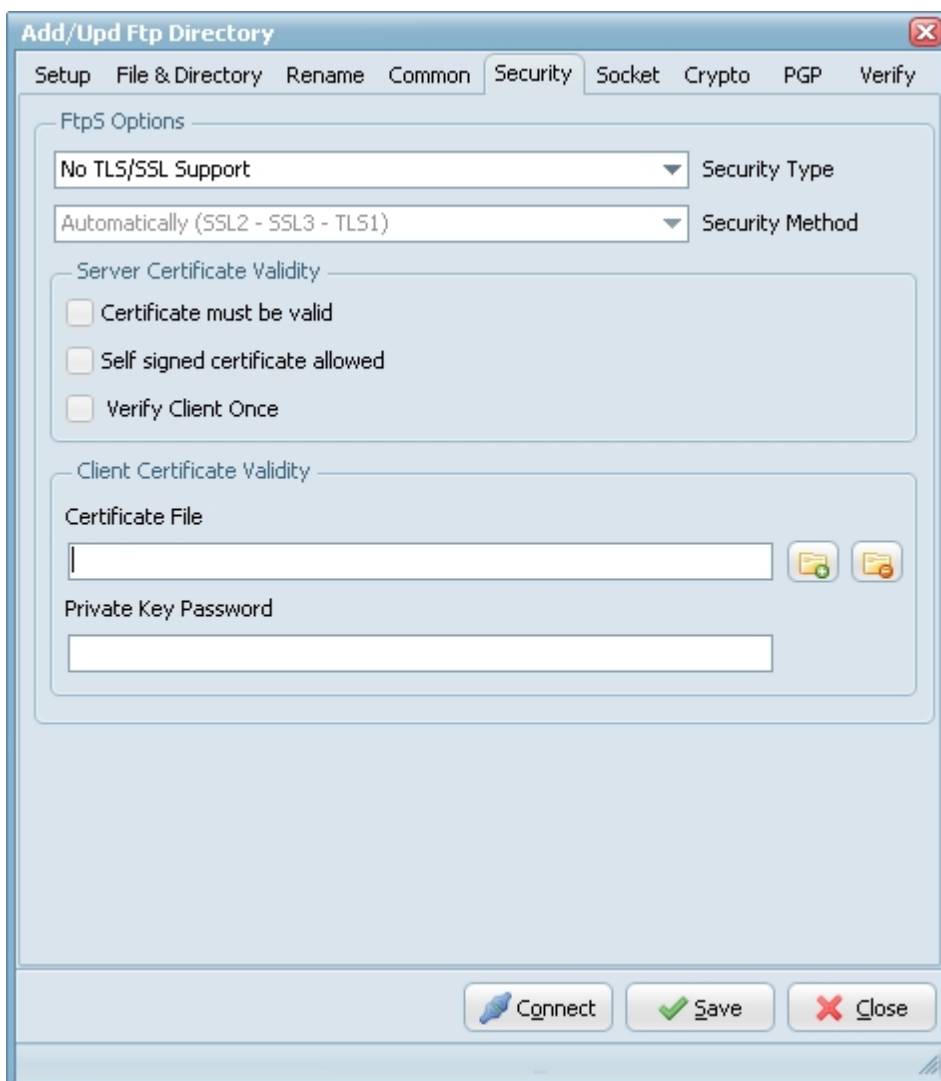
- ▶ Use transfertype ASCII: Use transfertype ASCII instead of Binary.
- ▶ Adjust File Times: File times will be adjusted after upload/download operation.
- ▶ Resume Data: When Resume contains True, the destination file will be opened and positioned to the end of the existing file data before retrieving new data.
- ▶ Append Data: When Append contains True, the FTP server will append data from the transfer to the end of a file which already exists on the FTP server.
- ▶ Enable Compression (MODE Z): Enable MODE Z Compression.
- ▶ Encrypt Data Channel: If this option is enabled the channel used for data transfer (files, directory listings) will be encrypted, otherwise only command channel will be encrypted.
- ▶ Use Size Command: Use this option to specify, whether SIZE command is sent when the data is downloaded. Use of this command lets the component report correct total size in OnProgress event, when the size of the data to be downloaded was not specified. Note, that some servers behave unexpectedly when SIZE command is used.
- ▶ Use FEAT Command: Use this option to specify, whether FEAT command is to be sent to the server. This command requests supported security mechanisms from FTPS server. Although server is not obliged to respond to it.
- ▶ Stay Connected: Don't disconnect the connection between scans.
- ▶ Use Adjust Passive Address: If this option is enabled, in passive mode data transfer, we will automatically set the address of the remote host to that from the control connection.

Proxy Settings



- ▶ Type: Use this option to specify type of the proxy server.
 - ▶ no proxy
 - ▶ user site proxy
 - ▶ site proxy
 - ▶ open proxy
 - ▶ userpath proxy
 - ▶ transparent proxy
- ▶ Host: Use this option to specify proxy server address.
- ▶ Port: Use this option to specify port on the proxy server.
- ▶ Username: Use this option to specify username.
- ▶ Password: Use this option to specify password.

Security Options



FTPS (also known as FTP Secure and FTP-SSL) is an extension to the commonly used File Transfer Protocol (FTP) that adds support for the Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols. FTPS should not be confused with the SSH File Transfer Protocol (SFTP), an incompatible secure file transfer subsystem for the Secure Shell (SSH) protocol. It is also different from Secure FTP, the practice of tunneling FTP through an SSH connection.

Security Type:

- ▶ Use Implicit TLS/SSL Support: Negotiation is not allowed with implicit FTPS configurations. A client is immediately expected to challenge the FTPS server with a TLS/SSL ClientHello message. If such a message is not received by the FTPS server, the server should drop the connection.
- ▶ Use Explicit TLS/SSL Support: In explicit mode (also known as FTPES), an FTPS client must "explicitly request" security from an FTPS server and then step-up to a mutually agreed encryption method. If a client does not request security, the FTPS server can either allow the client to continue insecure or refuse/limit the connection.

Security Method:

- ▶ Secure Sockets Layer SSLv2
- ▶ Secure Sockets Layer SSLv23
- ▶ Secure Sockets Layer SSLv3
- ▶ Transport Layer Security TLSv1
- ▶ Transport Layer Security TLSv1.1
- ▶ Transport Layer Security TLSv1.2

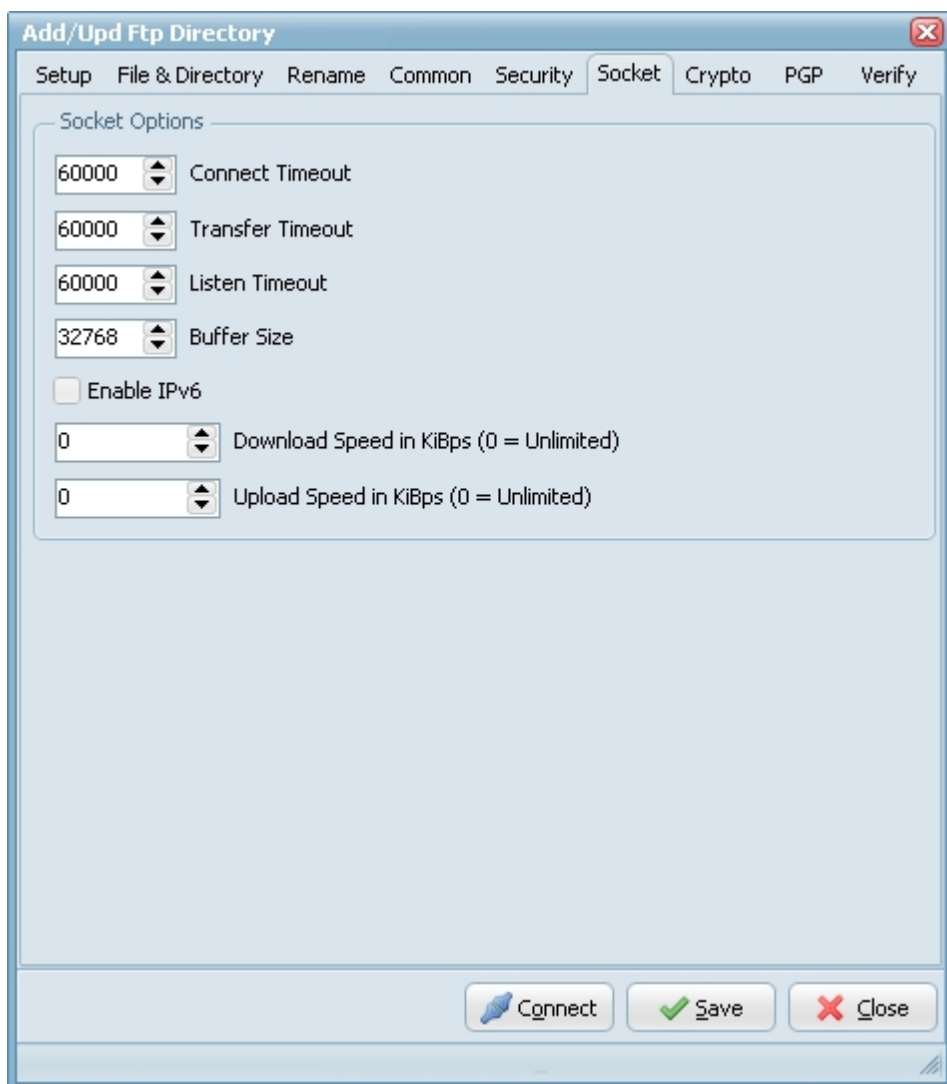
Server Certificate Validity

- ▶ Certificate must be valid: Certificate was validated successfully and is valid.
- ▶ Self signed certificate allowed: A self signed certificate is allowed.
- ▶ Verify client once:

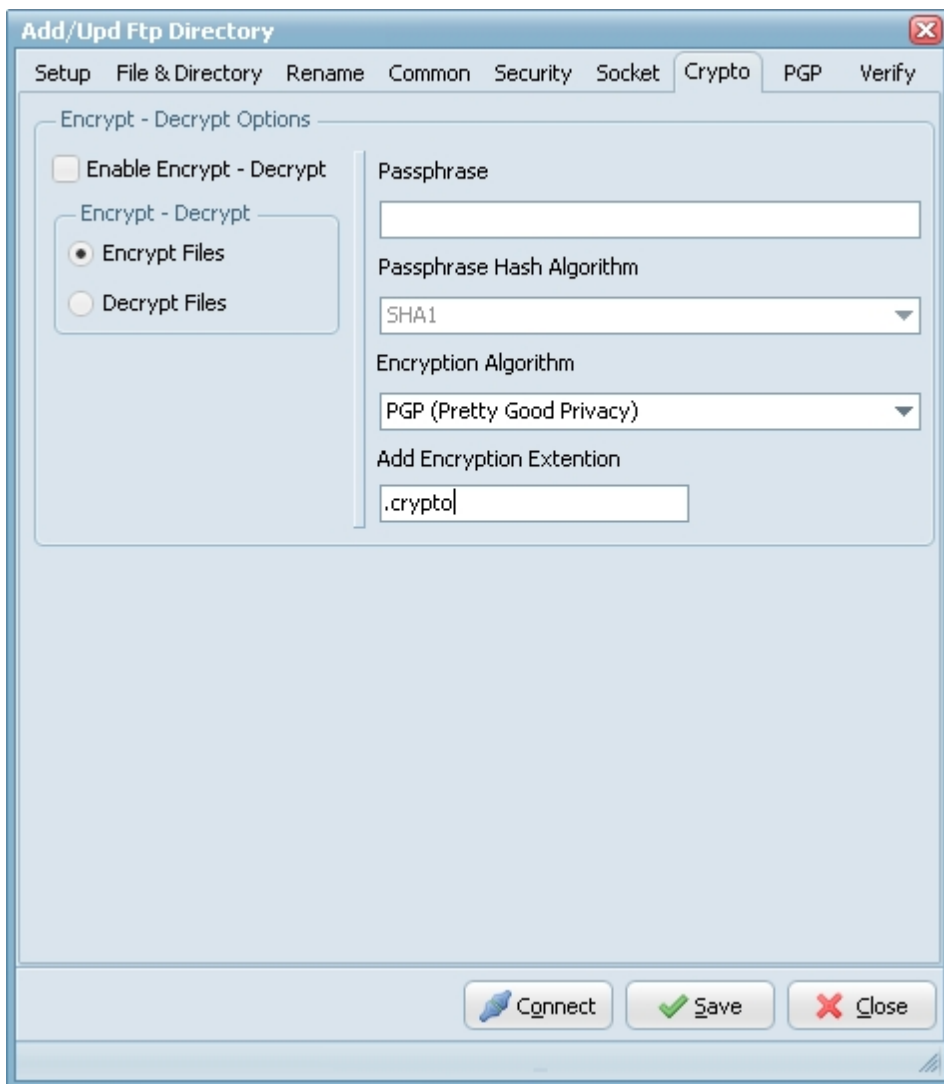
Client Certificate Validity

- ▶ Certificate File: For authentication FTPS (or, to be more precise, SSL/TLS protocol under FTP) uses X.509 certificates.
- ▶ Private Key Password: Needed when your private key is encrypted with a passphrase.

Socket Options



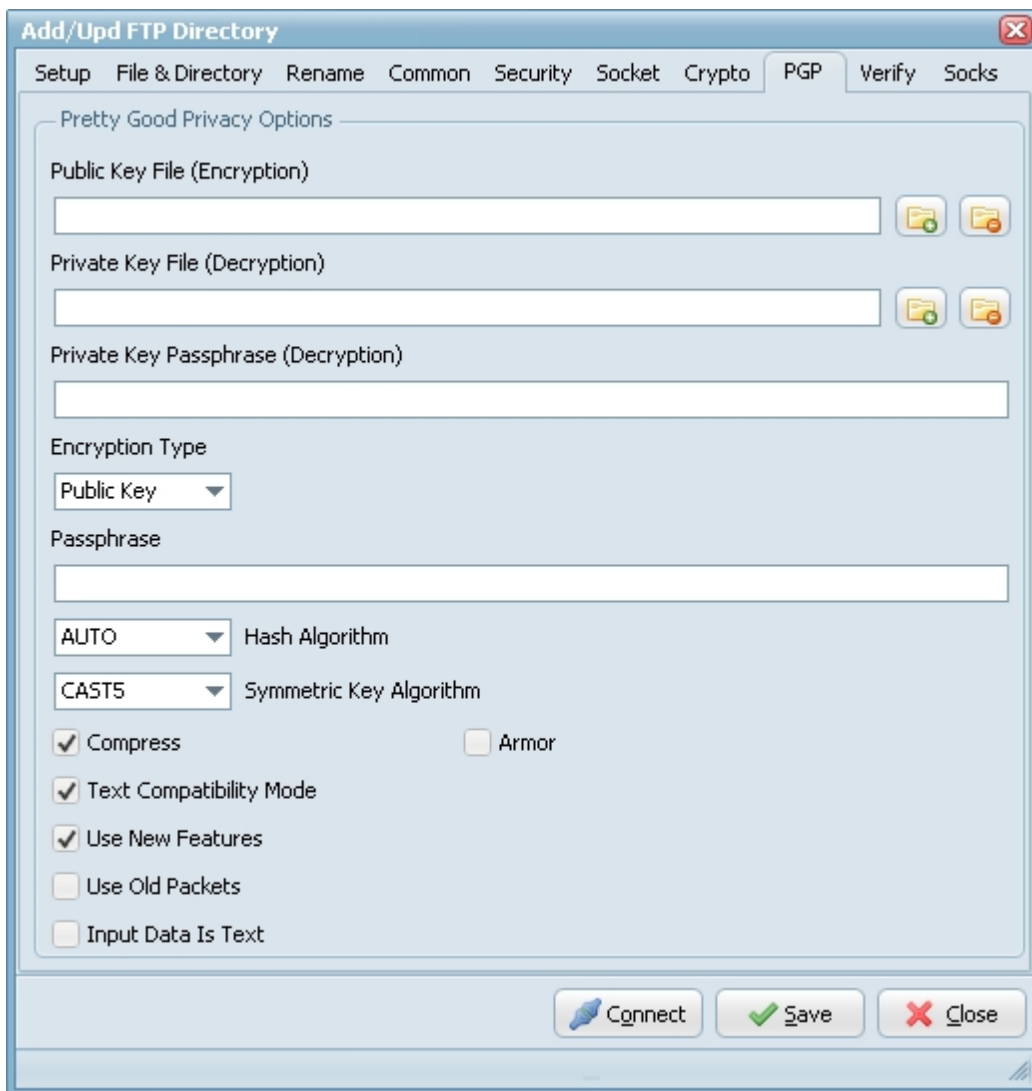
Crypto Options



Encrypt - Decrypt Options

- Encryption & Decryption using the following Encryption algorithms: Blowfish, Cast 128, Cast 256, DES, 3DES, Ice, Thin Ice, Ice2, IDEA, Mars, Misty1, RC2, RC4, RC5, RC6, Rijndael (the new AES), Serpent, Tea, Twofish and PGP (Pretty Good Privacy). You can use the following Hash Algorithms for the password: Haval, MD4, MD5, RipeMD-128, RipeMD-160, SHA-1, SHA-256, SHA-384, SHA-512, Tiger. LimagitoX uses a 64 bit Salt. Salt = Random data that is included as part of a session key. When added to a session key, the plaintext salt data is placed in front of the encrypted key data. Salt values are added to increase the work required to mount a brute-force (dictionary) attack against data encrypted with a symmetric-key cipher.
- Encryption & Decryption available in Site and Corporate License. Encryption available in Lite and Single License.

PGP Options



To enable PGP you need to set the Encryption Algorithm to PGP (check the Crypto Tab).

- ▶ Public Key File: Use this option to set the keyring with keys for data encryption.
- ▶ Private Key File: Use this option to determine keyring with keys for decryption.
- ▶ Private Key Passphrase: This option specifies password that will be used when trying to decrypt the private (secret) key used for file encryption.
- ▶ Encryption Type:
 - ▶ Both: both public key and password will be used for encryption. It implies, that decryption can be performed by either the password or the private (secret) key.
- ▶ Passphrase: This property specifies the password that will be tried to use when decrypting the file, which was previously encrypted using symmetric algorithm (not with a public key).
- ▶ Hash Algorithm: Use this option to set algorithm that will be used for hash calculation.
- ▶ Symmetric Key Algorithm: Specifies the symmetric algorithm for data encryption.
- ▶ Compress: Data will be compressed before encryption.
- ▶ Text Compatibility Mode: Several versions of PGP have bug in their implementations that results in creation of incorrect text signatures. The following paragraph is taken from RFC 2440: «PGP 2.6.X and 5.0 do not trim trailing whitespace from a "canonical text" signature. They only remove it from cleartext signatures. These signatures are not OpenPGP compliant -- OpenPGP requires trimming the whitespace. If you wish to interoperate with PGP 2.6.X or PGP 5, you may wish to accept these non-compliant signatures.» One can say that this bug also exists in PGP6.5 and PGP8.0 implementations. It is a good idea to enable this property if you want to interoperate with those versions of PGP. Disable this option if you need to create OpenPGP-compliant messages.
- ▶ Use New Features: Use this option for compatibility with old versions of PGP-compatible software. If this option is enabled, then newer and stronger algorithms will be used. In this case ClearTextSign and Sign will be compatible with PGP 2.6.x, while Encrypt and EncryptAndSign will not. If the option is disabled, then the result will be compatible with PGP 2.6.x, while the keys are compatible (i.e. don't use features not supported by PGP 2.6.x).
- ▶ Use Old Packets: If this option is enabled only packets of old format will be used in order for compatibility with PGP 2.6.x.

- ▶ **Input Is Text:** Use this option when you want to specify that input data must be interpreted as text.
- ▶ **Armor:** Use this option to determine if resulting data should be armored, i.e. wrapped into base64-cover. ASCII armor is a binary-to-textual encoding converter. ASCII armor is a feature of a type of encryption called pretty good privacy (PGP). ASCII armor involves encasing encrypted messaging in ASCII so that they can be sent in a standard messaging format such as email.

Verify Options



Verify File Options

- ▶ **Verify File after Copy/Move:** Compares source and destination file for verified transfer integrity.
- ▶ **Checksum Algorithm:** Checksum Algorithm used for verified transfer integrity. Automatic: select the algorithm using the following preferred order: 1. SHA1, 2. MD5, 3. CRC32
- ▶ **Write Checksum result to Log:** Checksum result will be written into the Log file.
- ▶ **Delete Destination File if Verify Fail:** Destination file will be deleted if verification fails.

Socks Options

Add/Upd FTP Directory

Setup File & Directory Rename Common Security Socket Crypto PGP Verify Socks

Socks Options

☐ Enable Socks

Host

Port

Version

Authentication

UserCode

Password

☐ Resolve Address

☐ Use IPv6

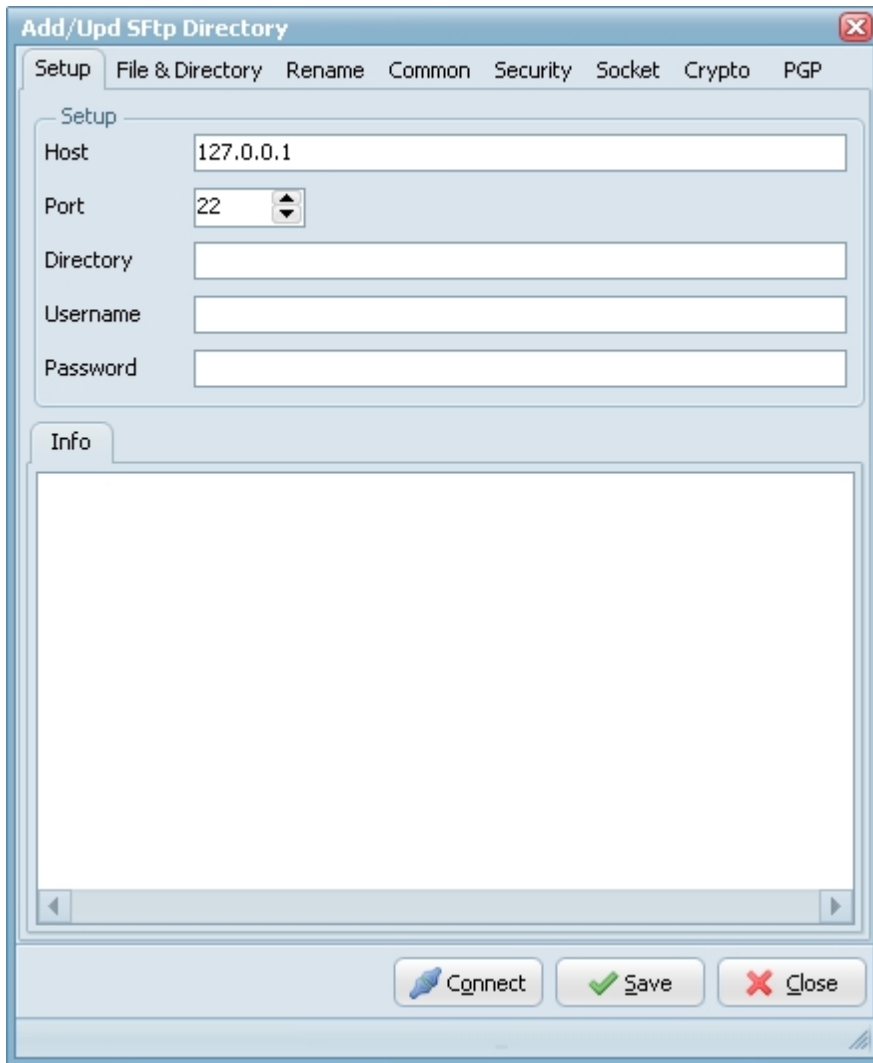
Connect Save Close

- ▶ **Enable Socks:** This option defines whether the connection is established directly (Enable Socks is disabled) or via SOCKS server (Enable Socks is enabled).
- ▶ **Host:** This property specifies the IP address or host name of the SOCKS server.
- ▶ **Port:** Specifies the port that SOCKS server is bound to. Default value is 1080.
- ▶ **Version:** This option specifies the version of SOCKS protocol to be used with the SOCKS server. Default value is version 5.
- ▶ **Authentication:** This option specifies the method of authentication to use with the SOCKS server. The methods supported are "No Authenticate" and "UserCode".
- ▶ **UserCode:** This property specifies the user code (username) to access the SOCKS server.
- ▶ **Password:** This property specifies the password to access the SOCKS server.
- ▶ **Resolve Address:** Specifies whether the address of destination host is resolved or passed to SOCKS server for resolving. Usually the host name is resolved on the client system. However some policy can forbid DNS operations on client computers. Then the client needs to pass the host name to the SOCKS server unresolved (SOCKS server is supposed to resolve it itself).
- ▶ **Use IPv6:** This option defines whether IP protocol version 6 should be used.

SFTP Destination

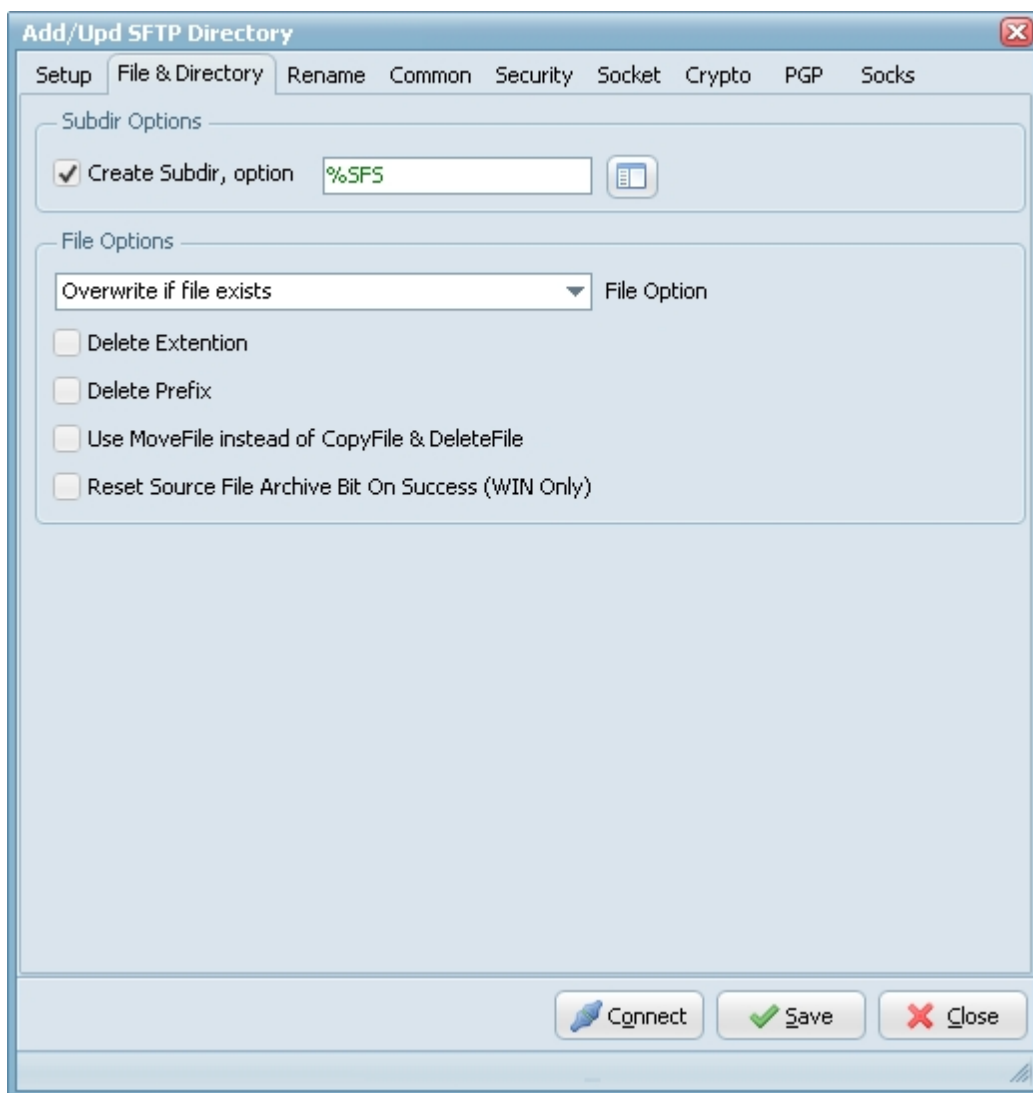
SFTP (FTP & FTPS) Destination Setup

Setup Options



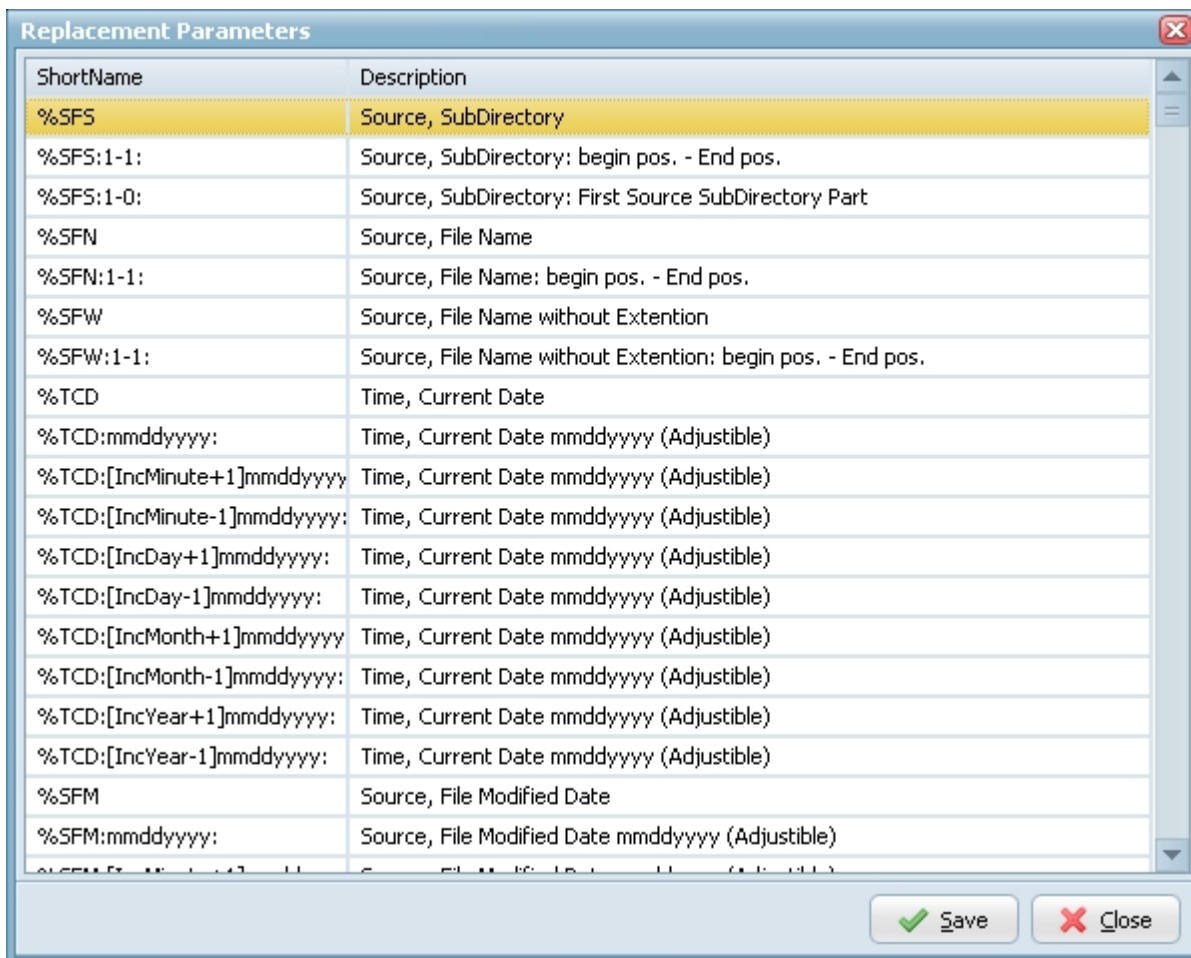
- ▶ Host: This option specifies the address of the host to connect to.
- ▶ Port: Port number on the host to connect to (Default value is 22).
- ▶ Directory: Directory on the server file system.
- ▶ Username: Authentication identity used when logging in to the server (example: Anonymous).
- ▶ Password: Authentication credentials used when logging into the server.
- ▶ Connect: Check connection setup.

File & Directory Options



Subdir Options

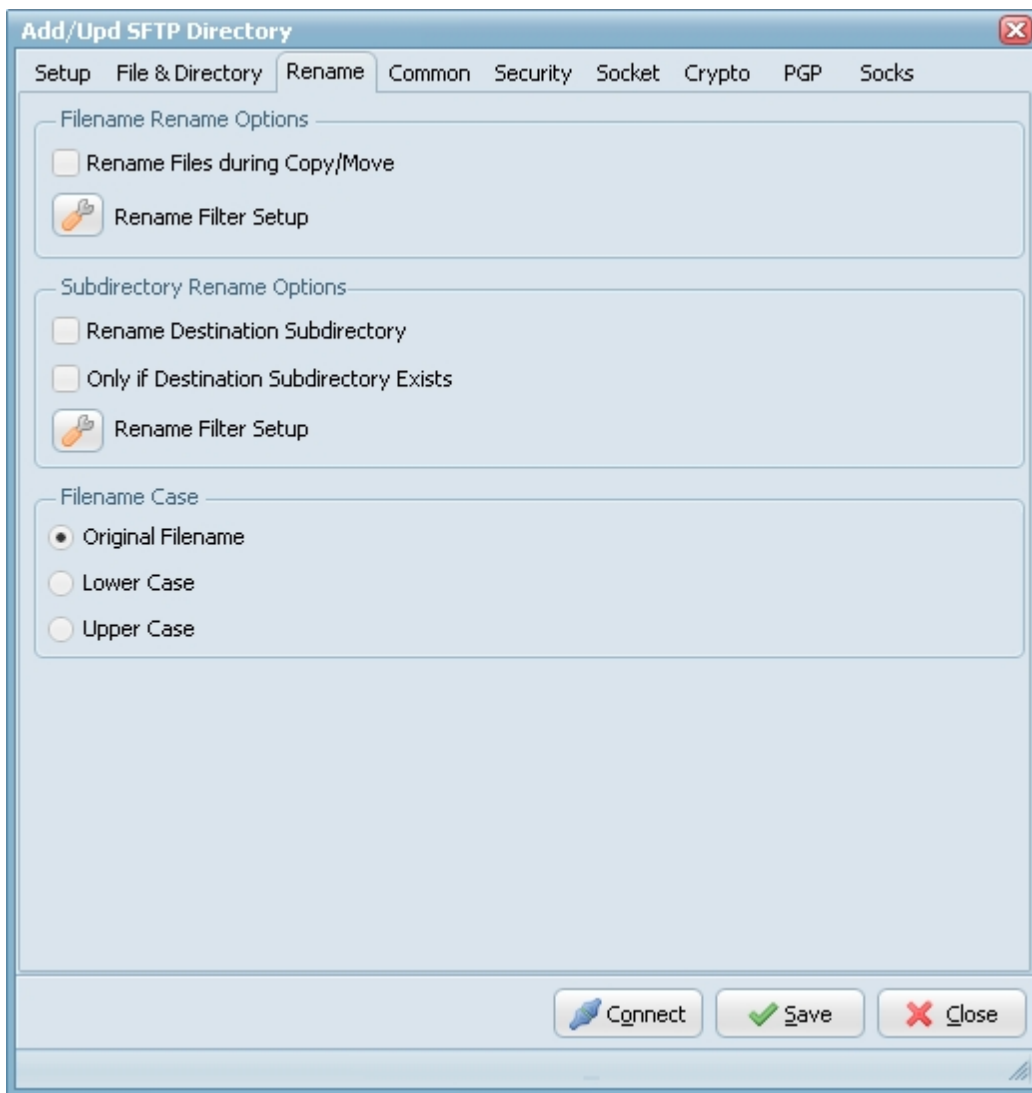
- ▶ Create Subdir: Create Subdirectory for the Windows destination.
- ▶ Create Subdir, option: Different parameters can be used to create the destination directory.



File Options

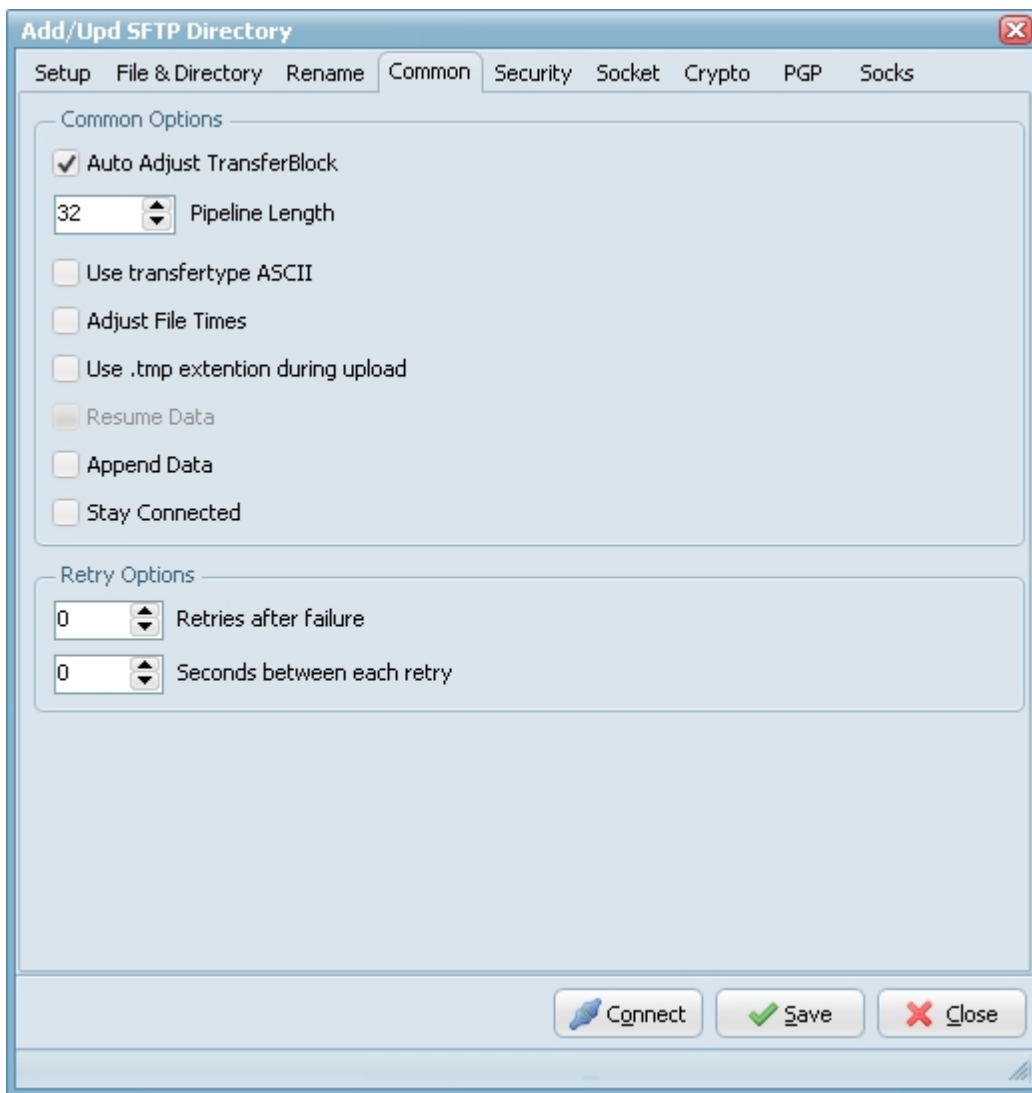
- ▶ Overwrite if file exists: Destination file will be overwritten.
- ▶ Only Newer Files: Only newer files will be processed to the destination.
- ▶ Skip if file exists: Skip if destination file already exists.
- ▶ Fail if file exists: Error if destination file already exists.
- ▶ Add version number suffix if file exists: Version number suffix will be added if destination file already exists (i.e. "filename.txt.1").
- ▶ Add version number (pre-ext) suffix if file exists: Version number (pre-ext) suffix will be added if destination file already exists (i.e. "filename.1.txt").
- ▶ Add version number prefix if file exists: Version number prefix will be added if destination file already exists (i.e. "1.filename.txt").
- ▶ Add date time suffix if file exists: Date time suffix will be added if destination file already exists (i.e. "filename.txt.20131116114801"). Format date time used: "YYYYMMDDHHNNSS".
- ▶ Add date time (pre-ext) suffix if file exists: Date time (pre-ext) suffix will be added if destination file already exists (i.e. "filename.20131116114801.txt"). Format date time used: "YYYYMMDDHHNNSS".
- ▶ Add date time prefix if file exists: Date time prefix will be added if destination file already exists (i.e. "20131116114801.filename.txt"). Format date time used: "YYYYMMDDHHNNSS".
- ▶ Delete Extension: Delete the extension of the destination filename.
- ▶ Delete Prefix: Delete the prefix (see file prefix filter source option) of the destination filename.
- ▶ Reset Source File Archive Bit On Success (WIN as Source): On Windows when a file is created or modified, the archive bit is set, and when the file has been backed up, the archive bit is cleared. It is by use of the archive bit that incremental backups are implemented.

Rename Options



- ▶ Rename Files during Copy/Move: Use regular expressions to rename the destination filename. A very good site with information about regular expressions is <http://www.regular-expressions.info/>
- ▶ Rename Destination Subdirectory: Use regular expressions to rename the destination subdirectory.
- ▶ Only if Destination Subdirectory Exists: Rename only if destination subdirectory already exists.
- ▶ Filename Case: Use original filename, lower case or upper case for the destination filenames.

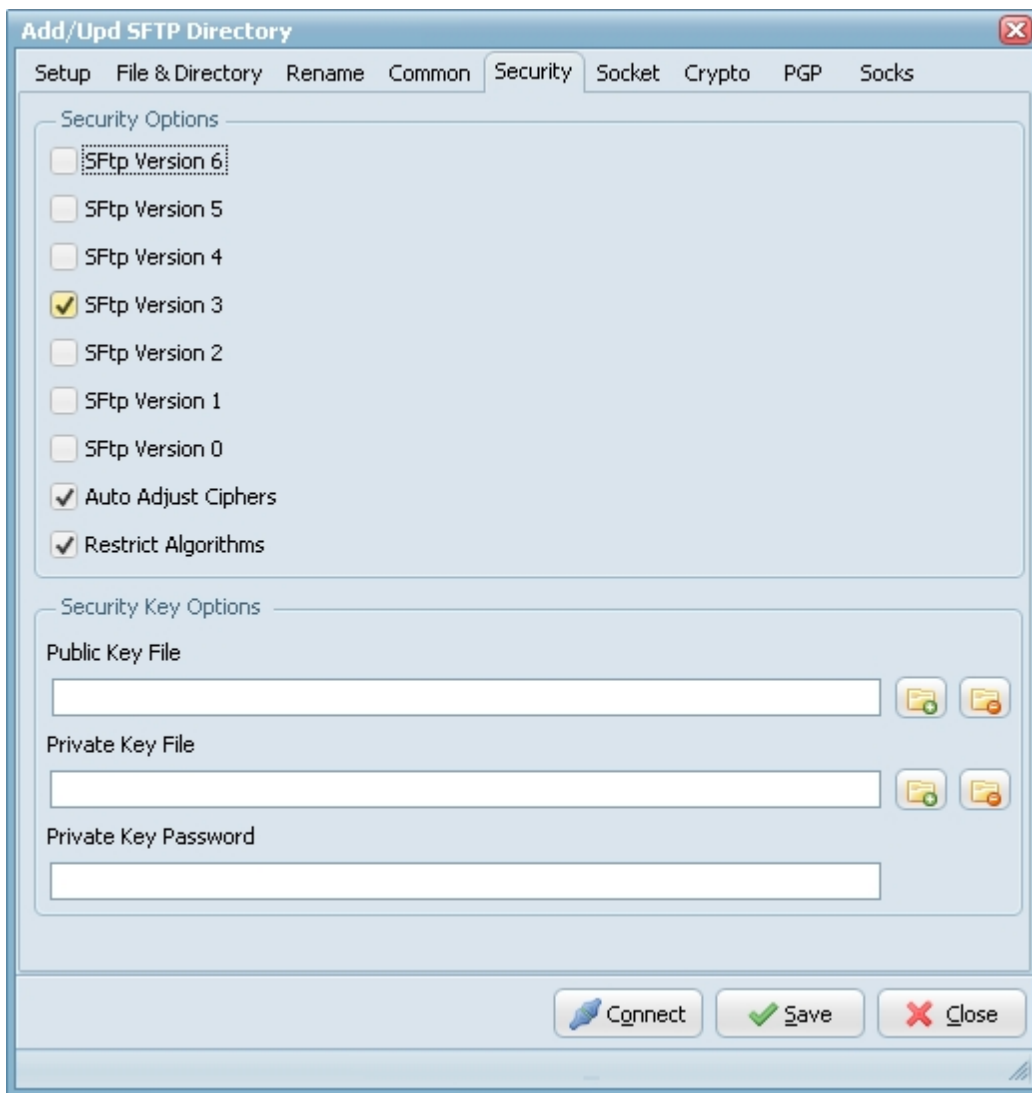
Common Options



Common Options

- ▶ **Auto Adjust Transferblock:** Use this option to enable or disable automatic adjustment of pipeline length and block sizes. By default automatic adjustment is enabled, and normally you don't need to disable it.
- ▶ **Pipeline Length:** Use this property to specify the number of upload or download requests sent before waiting for all requests to complete. The more requests are sent, the faster the transfer is. However, in case of error, all requests are discarded. Also, more pending requests means more memory used, so if speed is not critical and memory consumption is, set PipelineLength to 1. Default value is 32.
- ▶ **Use transfertype ASCII:** Use transfertype ASCII instead of Binary.
- ▶ **Adjust File Times:** File times will be adjusted after upload/download operation.
- ▶ **Resume Data:** When Resume contains True, the destination file will be opened and positioned to the end of the existing file data before retrieving new data.
- ▶ **Stay Connected:** Don't disconnect the connection between scans.

Security Options



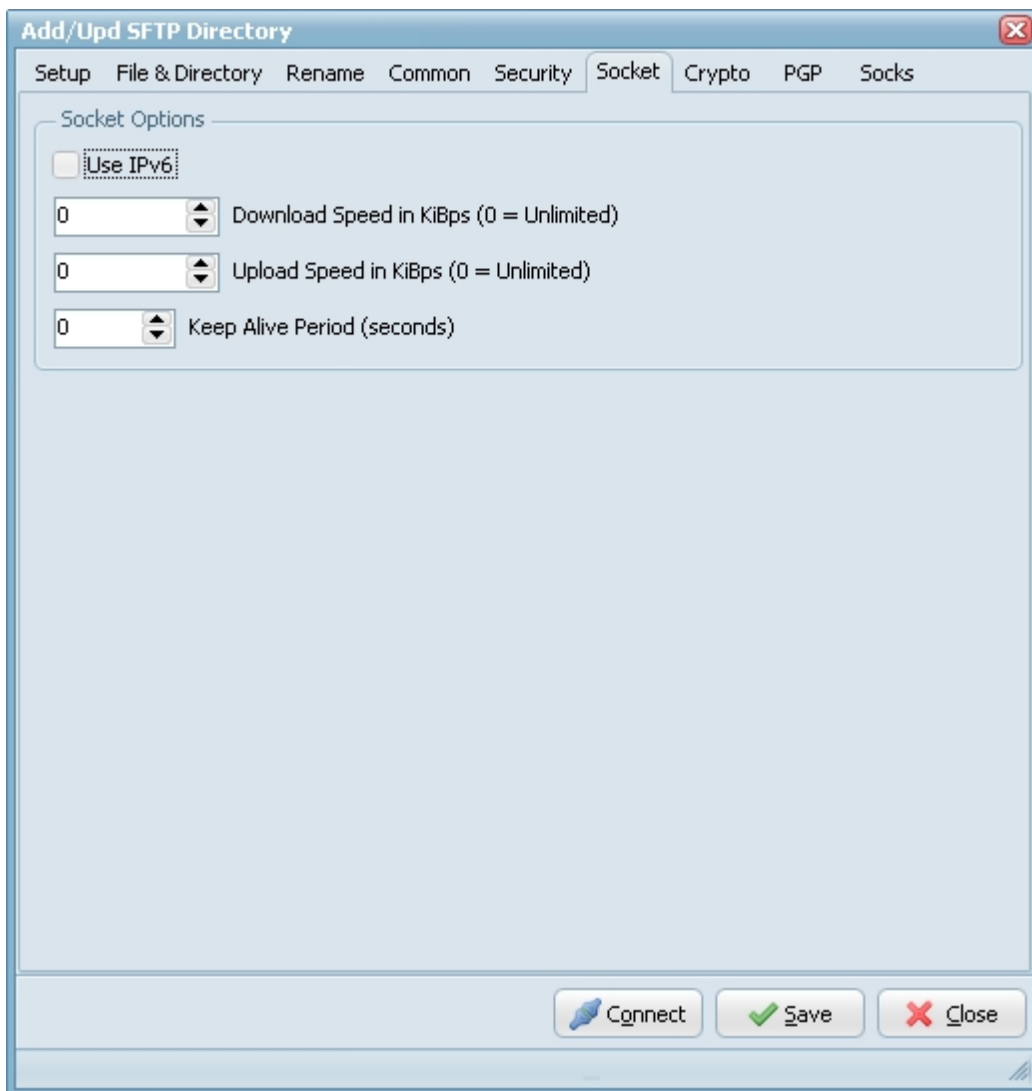
Security Options

- ▶ **SFTP Versions:** Use this option to specify SFTP versions which can be used during the connection.

Security Key Options

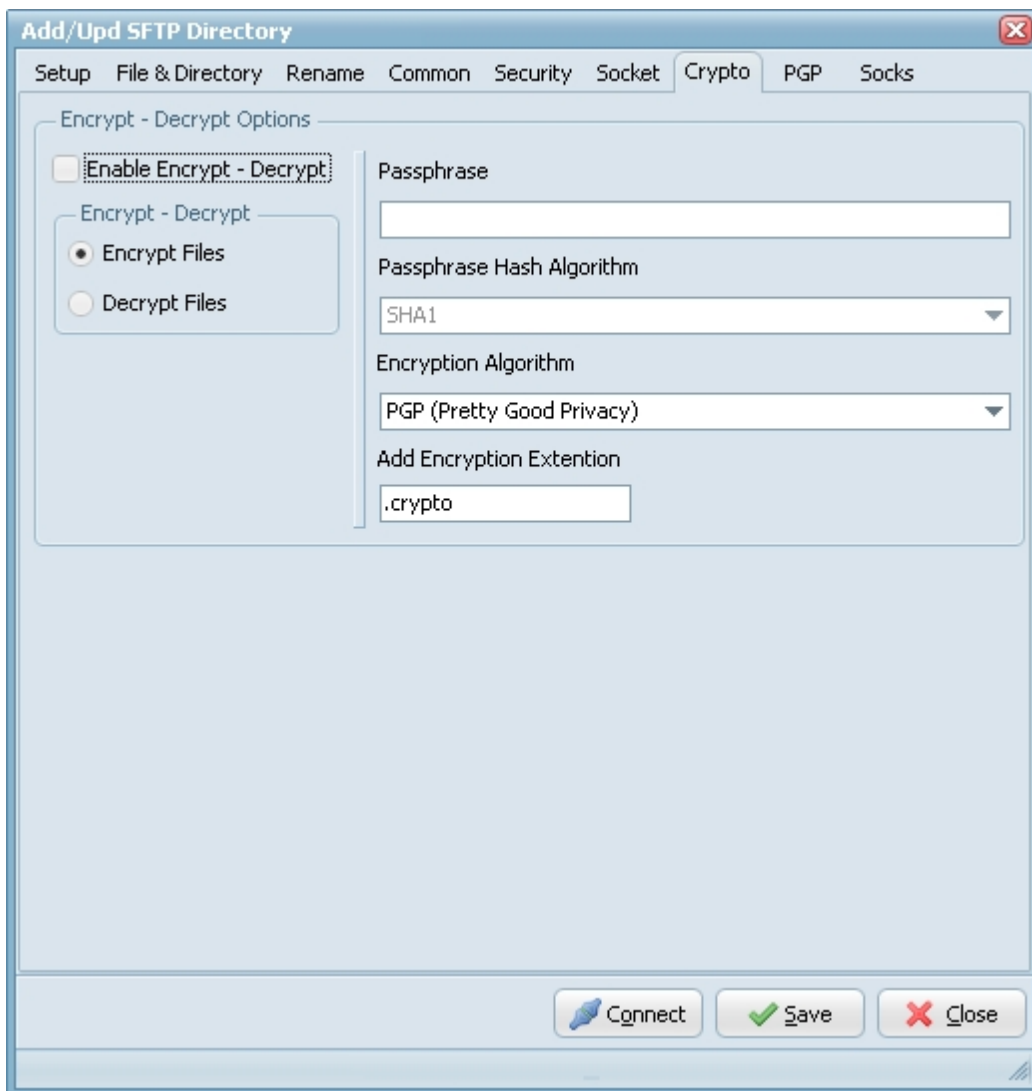
- ▶ **Public Key File:** When you authenticate with a public/private key pair, the server to which you are connecting should have a copy of your public key. This public key is safe for anyone to have. It doesn't contain any information about the owner of the key. Neither it contains information that lets one reliably validate the integrity and authenticity.
- ▶ **Private Key File:** When you authenticate with a public/private key pair, you should have a private key that only you have access to. When you log in using your key pair, the server sends a challenge, encrypted with your public key. The only key that will decrypt the challenge is your private key.
- ▶ **Private Key Password:** Needed when your private key is encrypted with a passphrase. Everyone recommends that you protect your private key with a passphrase (otherwise anybody who steals the file from you can log into everything you have access to).

Socket Options



- ▶ **Use IPv6:** This option defines whether IP protocol version 6 should be used.
- ▶ **Download Speed:** Use this option to specify the maximum number of KiBps that SFTP client may receive. The value of 0 (zero) means "no limitation".
- ▶ **Upload Speed:** Use this option to specify the maximum number of KiBps that SFTP client may send. The value of 0 (zero) means "no limitation".
- ▶ **Keep Alive Periods:** Use this option to specify tunnel inactivity period (in seconds), after which the keep-alive signal will be sent. Default value is 0 (no keep-alive signals).

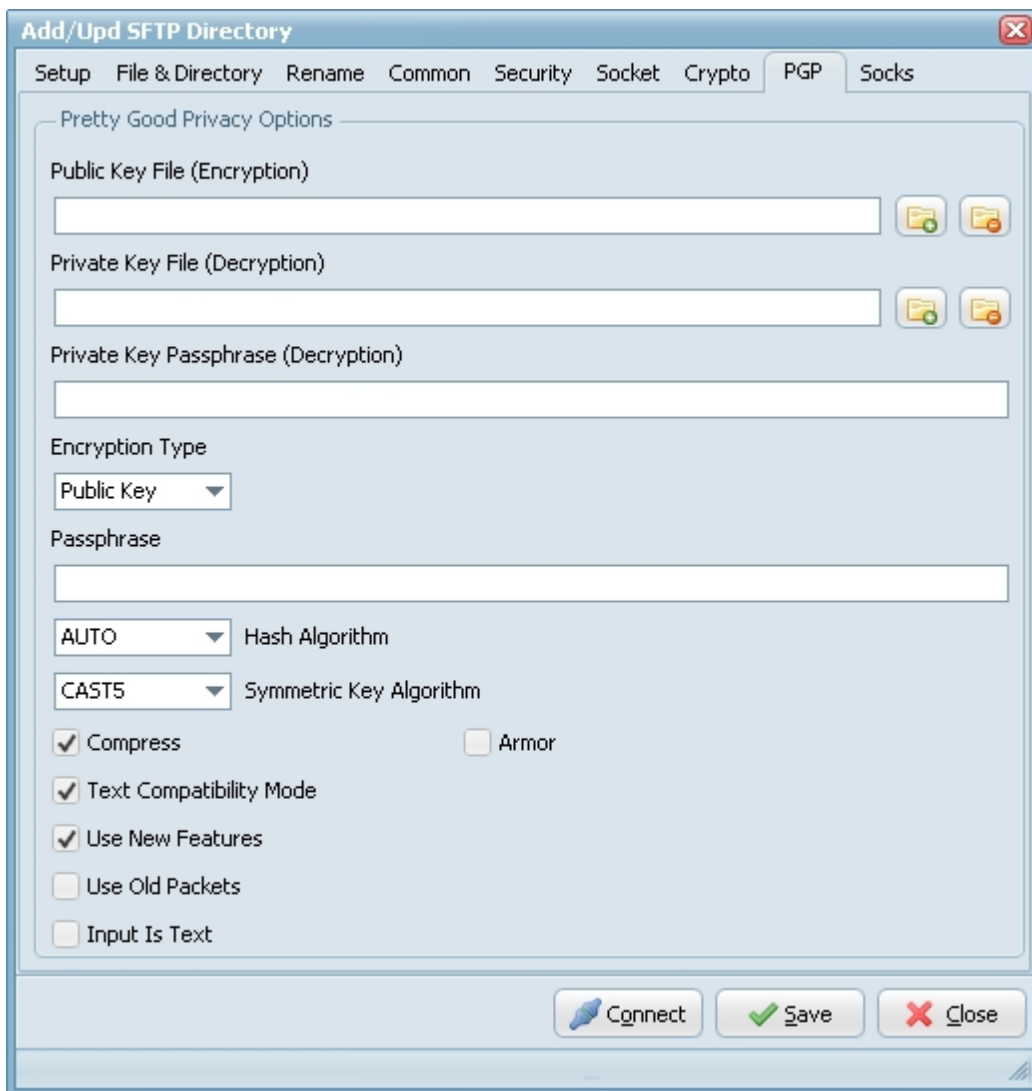
Crypto Options



Encrypt - Decrypt Options

- ▶ Encryption & Decryption using the following Encryption algorithms: Blowfish, Cast 128, Cast 256, DES, 3DES, Ice, Thin Ice, Ice2, IDEA, Mars, Misty1, RC2, RC4, RC5, RC6, Rijndael (the new AES), Serpent, Tea, Twofish and PGP (Pretty Good Privacy). You can use the following Hash Algorithms for the password: Haval, MD4, MD5, RipeMD-128, RipeMD-160, SHA-1, SHA-256, SHA-384, SHA-512, Tiger. LimagitoX uses a 64 bit Salt. Salt = Random data that is included as part of a session key. When added to a session key, the plaintext salt data is placed in front of the encrypted key data. Salt values are added to increase the work required to mount a brute-force (dictionary) attack against data encrypted with a symmetric-key cipher.
- ▶ Encryption & Decryption available in Site and Corporate License. Encryption available in Lite and Single License.

PGP Options



To enable PGP you need to set the Encryption Algorithm to PGP (check the Crypto Tab).

- ▶ Public Key File: Use this option to set the keyring with keys for data encryption.
- ▶ Private Key File: Use this option to determine keyring with keys for decryption.
- ▶ Private Key Passphrase: This option specifies password that will be used when trying to decrypt the private (secret) key used for file encryption.
- ▶ Encryption Type:
 - ▶ Both: both public key and password will be used for encryption. It implies, that decryption can be performed by either the password or the private (secret) key.
- ▶ Passphrase: This property specifies the password that will be tried to use when decrypting the file, which was previously encrypted using symmetric algorithm (not with a public key).
- ▶ Hash Algorithm: Use this option to set algorithm that will be used for hash calculation.
- ▶ Symmetric Key Algorithm: Specifies the symmetric algorithm for data encryption.
- ▶ Compress: Data will be compressed before encryption.
- ▶ Text Compatibility Mode: Several versions of PGP have bug in their implementations that results in creation of incorrect text signatures. The following paragraph is taken from RFC 2440: «PGP 2.6.X and 5.0 do not trim trailing whitespace from a "canonical text" signature. They only remove it from cleartext signatures. These signatures are not OpenPGP compliant -- OpenPGP requires trimming the whitespace. If you wish to interoperate with PGP 2.6.X or PGP 5, you may wish to accept these non-compliant signatures.» One can say that this bug also exists in PGP6.5 and PGP8.0 implementations. It is a good idea to enable this property if you want to interoperate with those versions of PGP. Disable this option if you need to create OpenPGP-compliant messages.
- ▶ Use New Features: Use this option for compatibility with old versions of PGP-compatible software. If this option is enabled, then newer and stronger algorithms will be used. In this case ClearTextSign and Sign will be compatible with PGP 2.6.x, while Encrypt and EncryptAndSign will not. If the option is disabled, then the result will be compatible with PGP 2.6.x, while the keys are compatible (i.e. don't use features not supported by PGP 2.6.x).
- ▶ Use Old Packets: If this option is enabled only packets of old format will be used in order for compatibility with PGP 2.6.x.

- ▶ **Input Is Text:** Use this option when you want to specify that input data must be interpreted as text.
- ▶ **Armor:** Use this option to determine if resulting data should be armored, i.e. wrapped into base64-cover. ASCII armor is a binary-to-textual encoding converter. ASCII armor is a feature of a type of encryption called pretty good privacy (PGP). ASCII armor involves encasing encrypted messaging in ASCII so that they can be sent in a standard messaging format such as email.

Socks Options

The screenshot shows a dialog box titled "Add/Upd SFTP Directory" with a close button (X) in the top right corner. The dialog has several tabs: Setup, File & Directory, Rename, Common, Security, Socket, Crypto, PGP, and Socks. The "Socks" tab is selected. Inside the Socks tab, there is a section titled "Socks Options" containing the following controls:

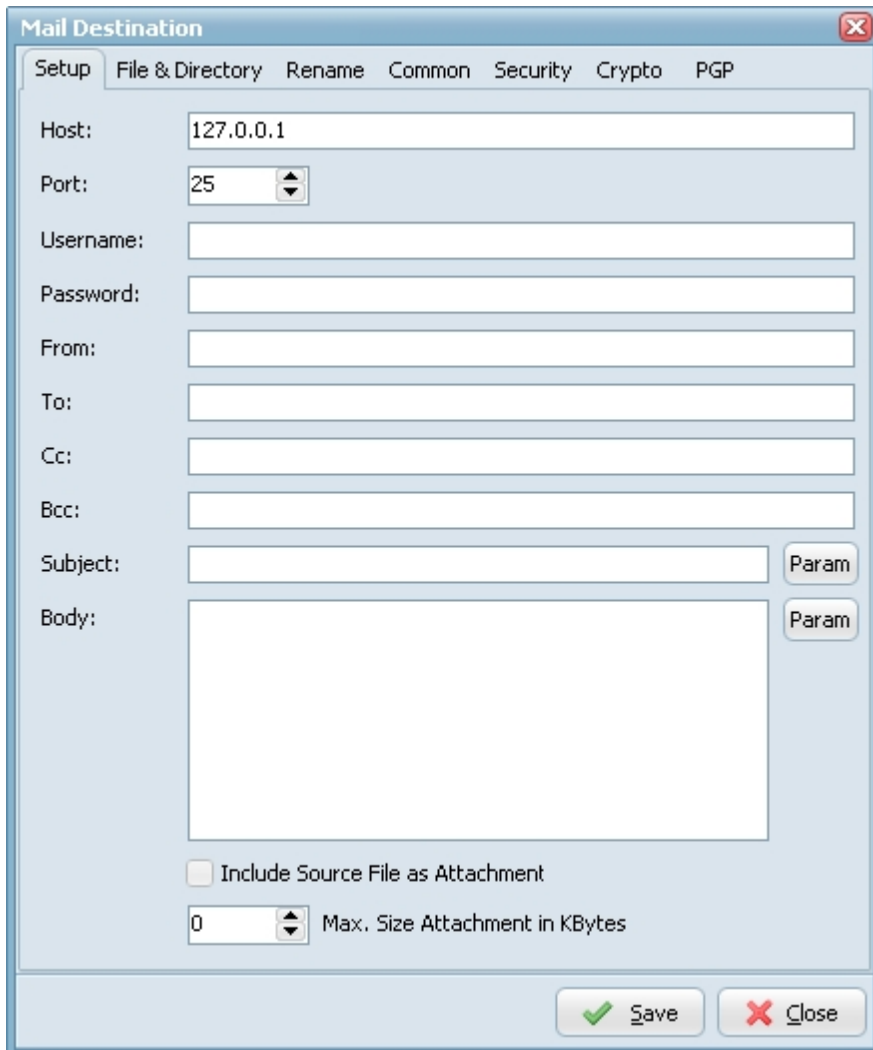
- ☐ **Enable Socks**: A checkbox with a dotted border.
- Host**: A text input field.
- Port**: A spin box with the value 1080.
- Version**: A dropdown menu showing "version 5".
- Authentication**: A dropdown menu showing "No Authentication".
- UserCode**: A text input field.
- Password**: A text input field.
- ☐ **Resolve Address**: A checkbox.
- ☐ **Use IPv6**: A checkbox.

At the bottom of the dialog, there are three buttons: "Connect" (with a blue arrow icon), "Save" (with a green checkmark icon), and "Close" (with a red X icon).

- ▶ **Enable Socks:** This option defines whether the connection is established directly (Enable Socks is disabled) or via SOCKS server (Enable Socks is enabled).
- ▶ **Host:** This property specifies the IP address or host name of the SOCKS server.
- ▶ **Port:** Specifies the port that SOCKS server is bound to. Default value is 1080.
- ▶ **Version:** This option specifies the version of SOCKS protocol to be used with the SOCKS server. Default value is version 5.
- ▶ **Authentication:** This option specifies the method of authentication to use with the SOCKS server. The methods supported are "No Authenticate" and "UserCode".
- ▶ **UserCode:** This property specifies the user code (username) to access the SOCKS server.
- ▶ **Password:** This property specifies the password to access the SOCKS server.
- ▶ **Resolve Address:** Specifies whether the address of destination host is resolved or passed to SOCKS server for resolving. Usually the host name is resolved on the client system. However some policy can forbid DNS operations on client computers. Then the client needs to pass the host name to the SOCKS server unresolved (SOCKS server is supposed to resolve it itself).
- ▶ **Use IPv6:** This option defines whether IP protocol version 6 should be used.

SMTP Destination Setup

Setup Options

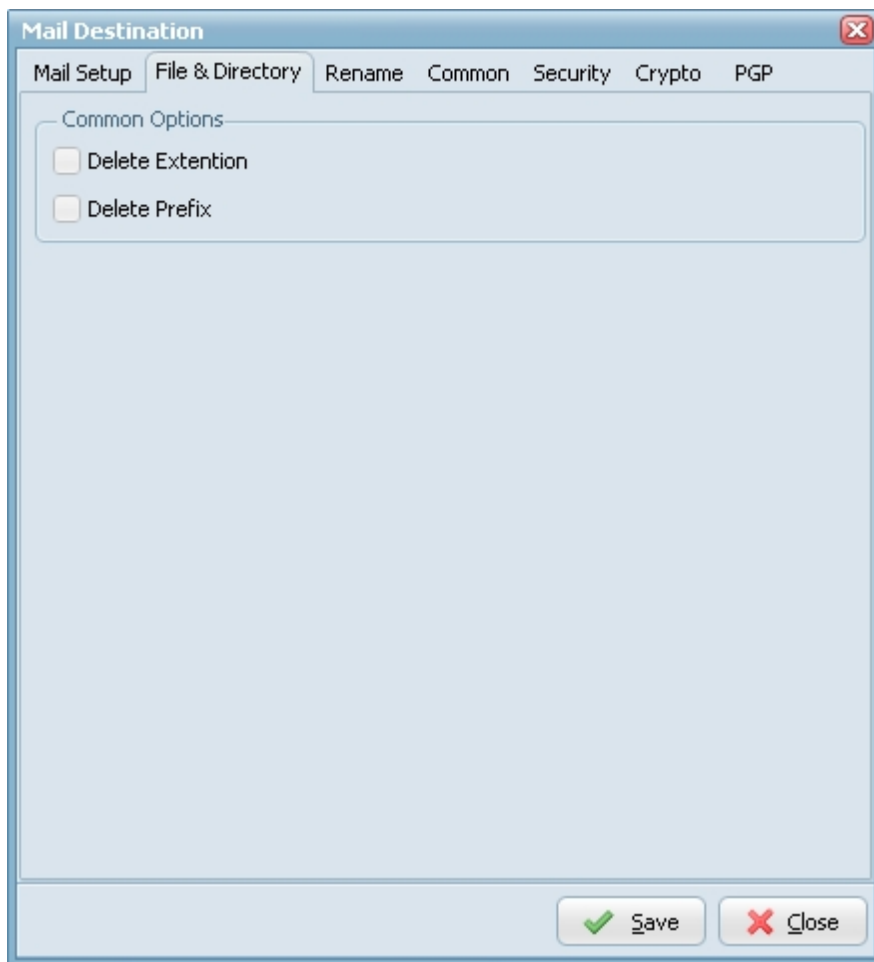


The image shows a 'Mail Destination' dialog box with a tabbed interface. The 'Setup' tab is selected. It contains fields for Host (127.0.0.1), Port (25), Username, Password, From, To, Cc, Bcc, Subject, and Body. There are also checkboxes for 'Include Source File as Attachment' and a spinner for 'Max. Size Attachment in KBytes'. At the bottom are 'Save' and 'Close' buttons.

Field	Value
Host:	127.0.0.1
Port:	25
Username:	
Password:	
From:	
To:	
Cc:	
Bcc:	
Subject:	
Body:	
Include Source File as Attachment	<input type="checkbox"/>
Max. Size Attachment in KBytes	0

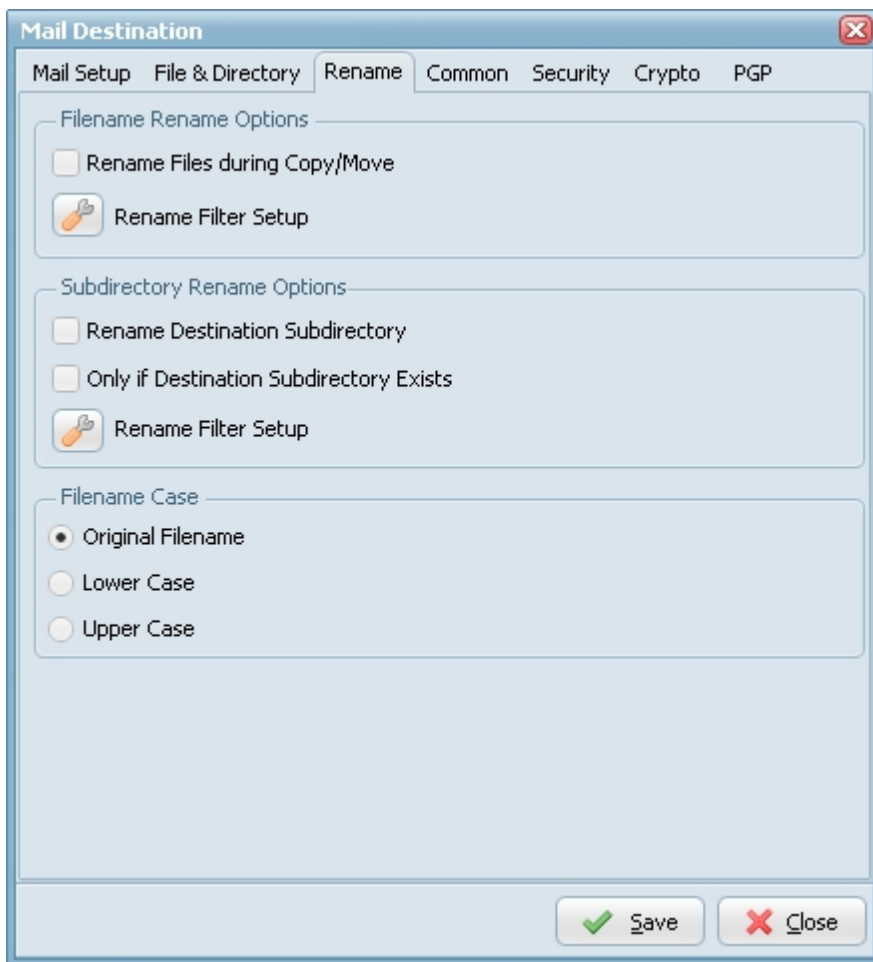
- ▶ Host: This option specifies the address of the host to connect to.
- ▶ Username: Authentication identity used when in to the server.
- ▶ Password: Authentication credentials used when logging into the server.
- ▶ Port: Port number on the host to connect to (Default value is 25).
- ▶ From: Identifies the original author of the message.
- ▶ To: Identifies the recipients of a message.
- ▶ CC: Carbon copy recipients for the message.
- ▶ BCC: Indicates blind carbon copy recipients for the message.
- ▶ Subject: Identifies the subject for the message.
- ▶ Body: Represents the body of the message.
- ▶ Include Input File as Attachment: Source file will be included as attachment.
- ▶ Max. Size Attachment in Kbytes: Maximum size attachment in Kbytes (Default value is zero = Unlimited).

File & Directory Options



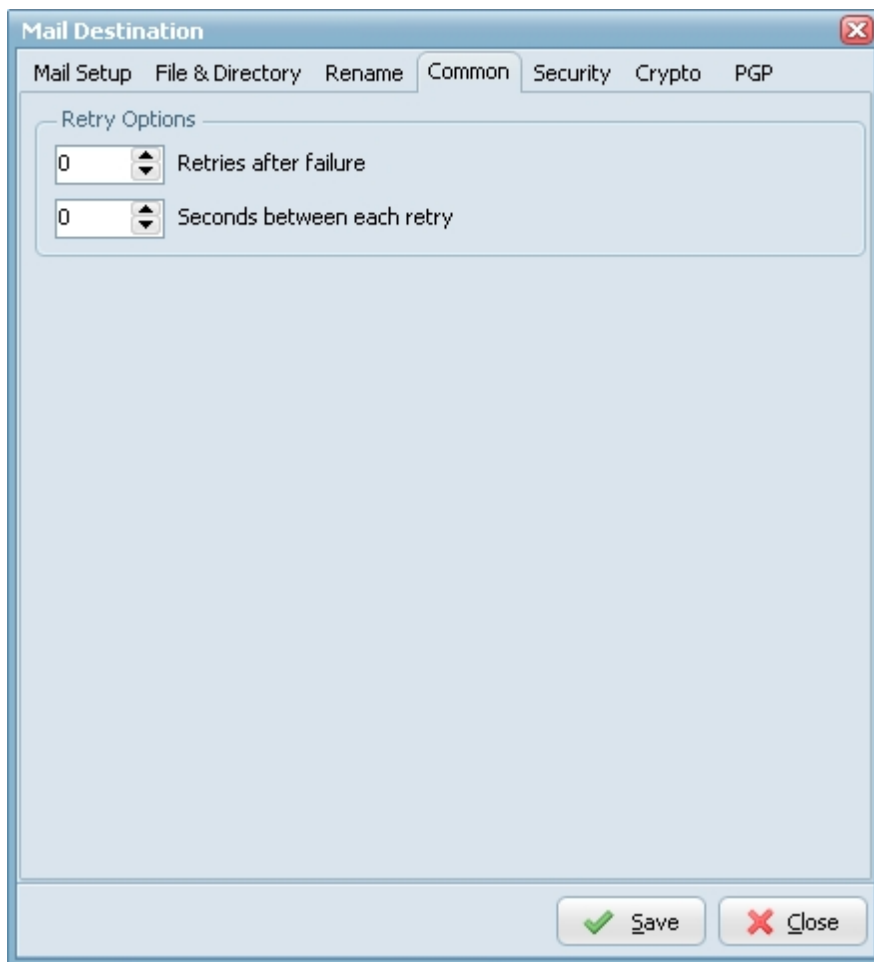
- ▶ Delete Extention: Delete the extention of the destination filename.
- ▶ Delete Prefix: Delete the prefix (see file prefix filter source option) of the destination filename.

Rename Options

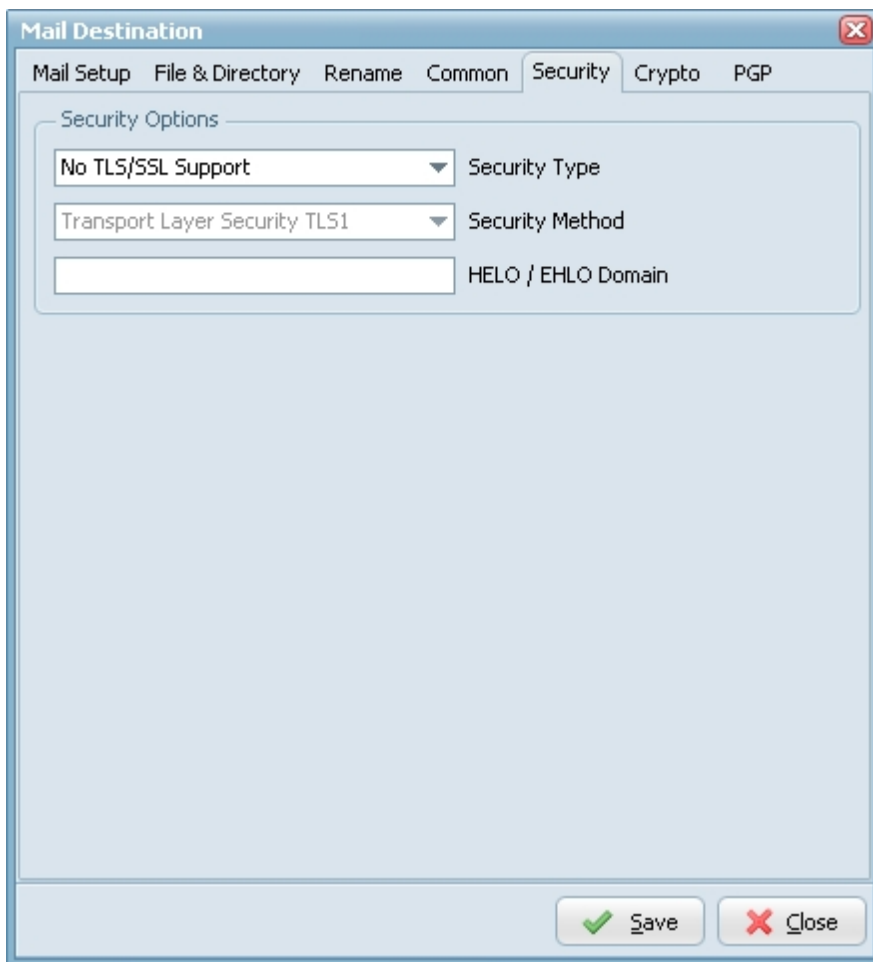


- ▶ **Rename Files during Copy/Move:** Use regular expressions to rename the destination filename. A very good site with information about regular expressions is <http://www.regular-expressions.info/>
- ▶ **Rename Destination Subdirectory:** Use regular expressions to rename the destination subdirectory.
- ▶ **Only if Destination Subdirectory Exists:** Rename only if destination subdirectory already exists.
- ▶ **Filename Case:** Use original filename, lower case or upper case for the destination filenames.

Common Options

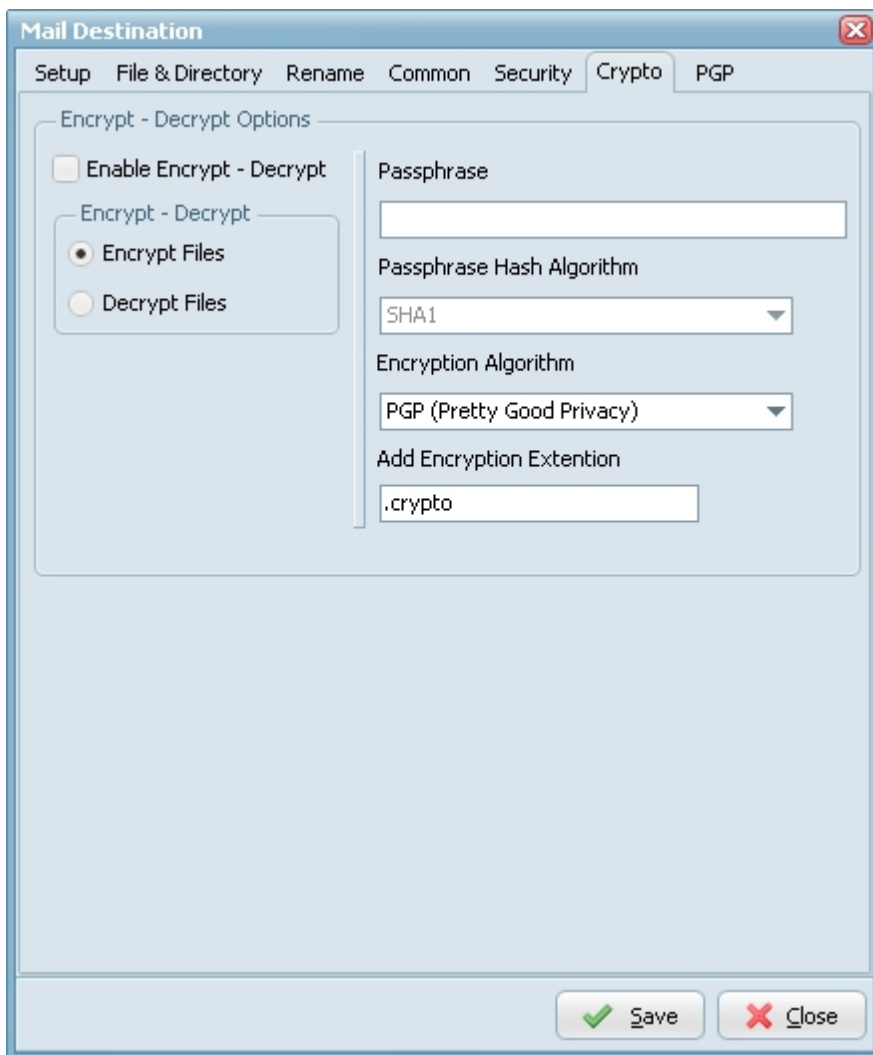


Security Options



- ▶ With the security options you can enable TLS/SSL support.
- ▶ HELO/EHLO Domain: Ask the server for the SMTP extensions that the server supports, by using the EHLO greeting of the Extended SMTP specification (RFC 1870). Fall back to HELO only if the server does not respond to EHLO.

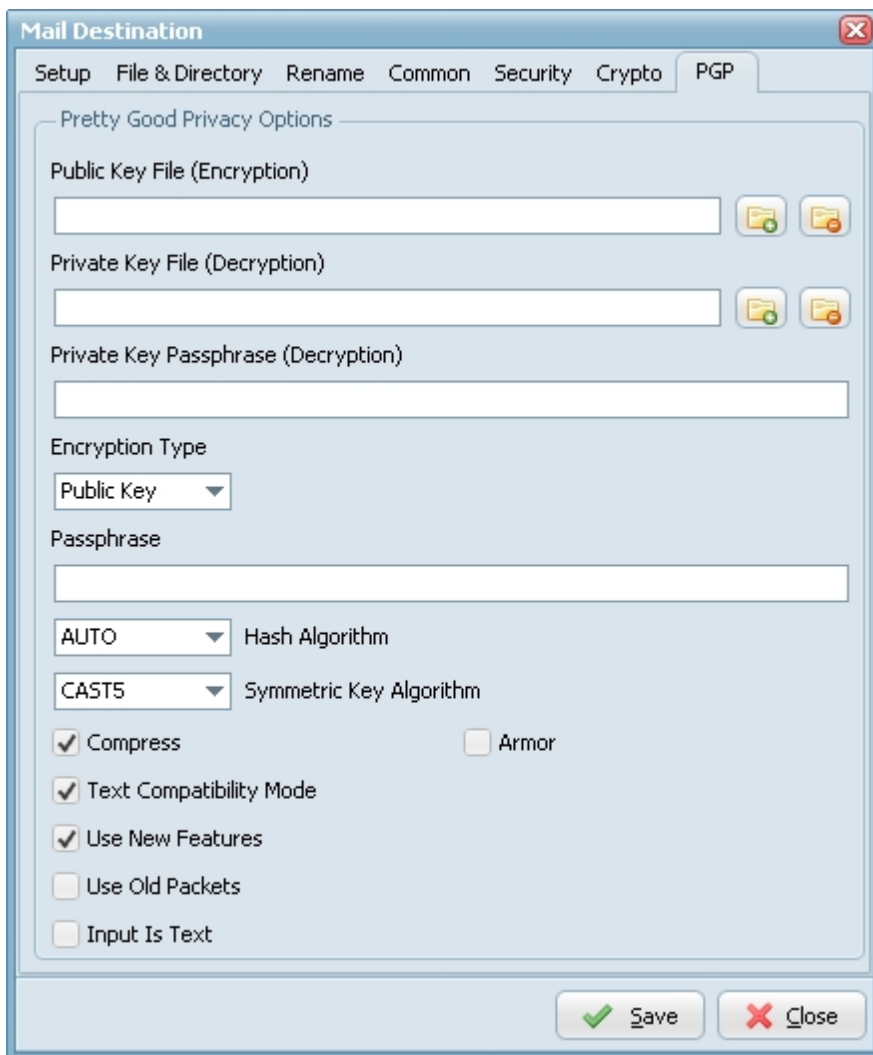
Crypto Options



Encrypt - Decrypt Options

- Encryption & Decryption using the following Encryption algorithms: Blowfish, Cast 128, Cast 256, DES, 3DES, Ice, Thin Ice, Ice2, IDEA, Mars, Misty1, RC2, RC4, RC5, RC6, Rijndael (the new AES), Serpent, Tea, Twofish and PGP (Pretty Good Privacy). You can use the following Hash Algorithms for the password: Haval, MD4, MD5, RipeMD-128, RipeMD-160, SHA-1, SHA-256, SHA-384, SHA-512, Tiger. LimagitoX uses a 64 bit Salt. Salt = Random data that is included as part of a session key. When added to a session key, the plaintext salt data is placed in front of the encrypted key data. Salt values are added to increase the work required to mount a brute-force (dictionary) attack against data encrypted with a symmetric-key cipher.
- Encryption & Decryption available in Site and Corporate License. Encryption available in Lite and Single License.

PGP Options



To enable PGP you need to set the Encryption Algorithm to PGP (check the Crypto Tab).

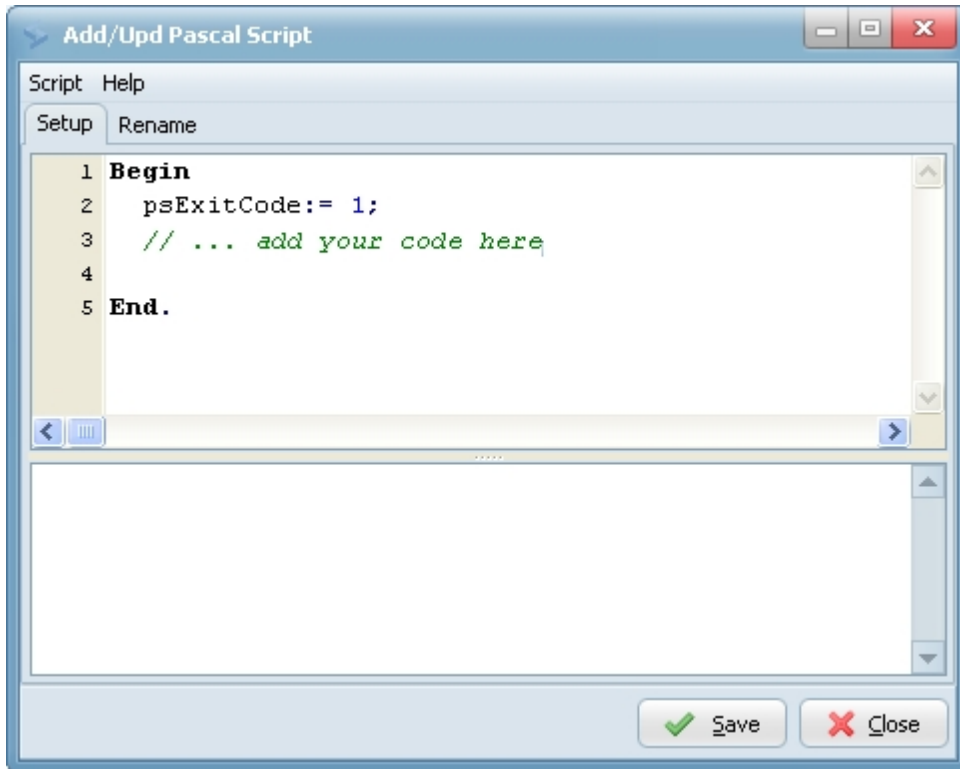
- ▶ Public Key File: Use this option to set the keyring with keys for data encryption.
- ▶ Private Key File: Use this option to determine keyring with keys for decryption.
- ▶ Private Key Passphrase: This option specifies password that will be used when trying to decrypt the private (secret) key used for file encryption.
- ▶ Encryption Type:
 - ▶ Both: both public key and password will be used for encryption. It implies, that decryption can be performed by either the password or the private (secret) key.
- ▶ Passphrase: This property specifies the password that will be tried to use when decrypting the file, which was previously encrypted using symmetric algorithm (not with a public key).
- ▶ Hash Algorithm: Use this option to set algorithm that will be used for hash calculation.
- ▶ Symmetric Key Algorithm: Specifies the symmetric algorithm for data encryption.
- ▶ Compress: Data will be compressed before encryption.
- ▶ Text Compatibility Mode: Several versions of PGP have bug in their implementations that results in creation of incorrect text signatures. The following paragraph is taken from RFC 2440: «PGP 2.6.X and 5.0 do not trim trailing whitespace from a "canonical text" signature. They only remove it from cleartext signatures. These signatures are not OpenPGP compliant -- OpenPGP requires trimming the whitespace. If you wish to interoperate with PGP 2.6.X or PGP 5, you may wish to accept these non-compliant signatures.» One can say that this bug also exists in PGP6.5 and PGP8.0 implementations. It is a good idea to enable this property if you want to interoperate with those versions of PGP. Disable this option if you need to create OpenPGP-compliant messages.
- ▶ Use New Features: Use this option for compatibility with old versions of PGP-compatible software. If this option is enabled, then newer and stronger algorithms will be used. In this case ClearTextSign and Sign will be compatible with PGP 2.6.x, while Encrypt and EncryptAndSign will not. If the option is disabled, then the result will be compatible with PGP 2.6.x, while the keys are compatible (i.e. don't use features not supported by PGP 2.6.x).
- ▶ Use Old Packets: If this option is enabled only packets of old format will be used in order for compatibility with PGP 2.6.x.
- ▶ Input Is Text: Use this option when you want to specify that input data must be interpreted as text.

- ▶ **Armor:** Use this option to determine if resulting data should be armored, i.e. wrapped into base64-cover. ASCII armor is a binary-to-textual encoding converter. ASCII armor is a feature of a type of encryption called pretty good privacy (PGP). ASCII armor involves encasing encrypted messaging in ASCII so that they can be sent in a standard messaging format such as email.

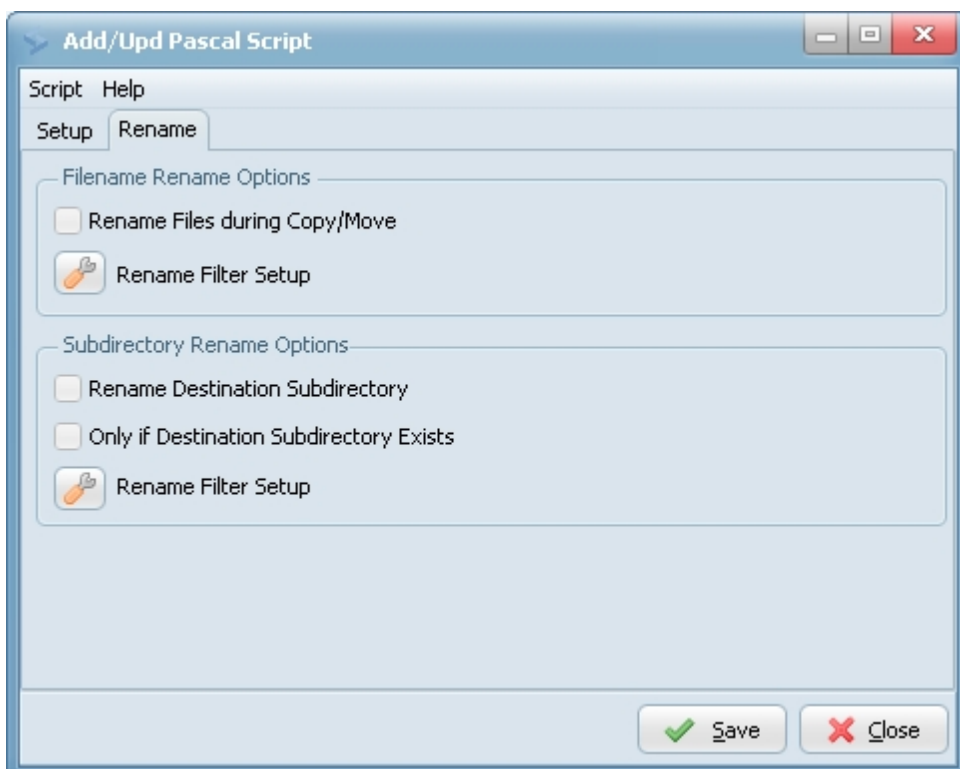
PS Destination

Pascal Script Destination Setup

Setup Options



Rename Options

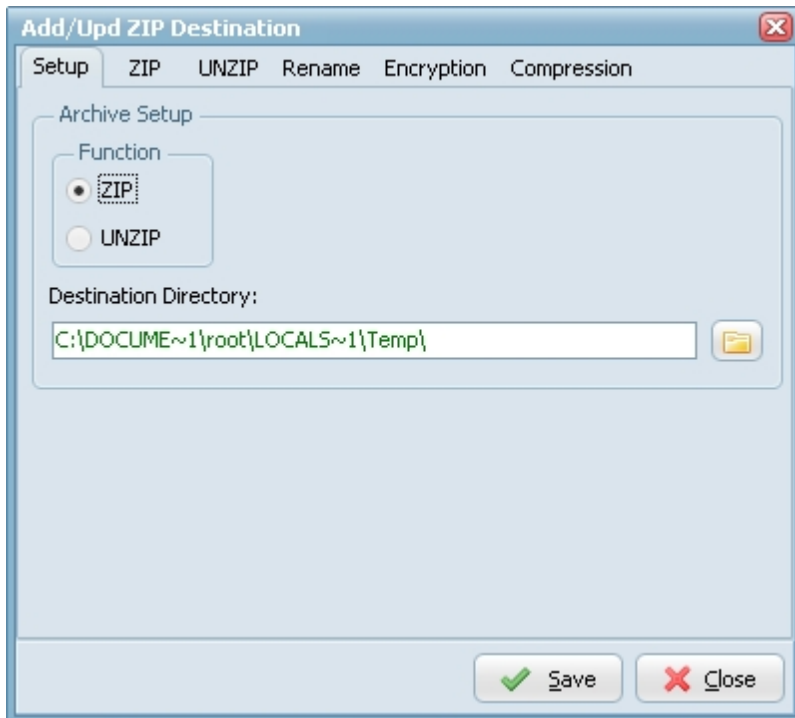


- ▶ Rename Files during Copy/Move: Use regular expressions to rename the destination filename. A very good site with information about regular expressions is <http://www.regular-expressions.info/>
- ▶ Rename Destination Subdirectory: Use regular expressions to rename the destination subdirectory.
- ▶ Only if Destination Subdirectory Exists: Rename only if destination subdirectory already exists.

ZIP Destination

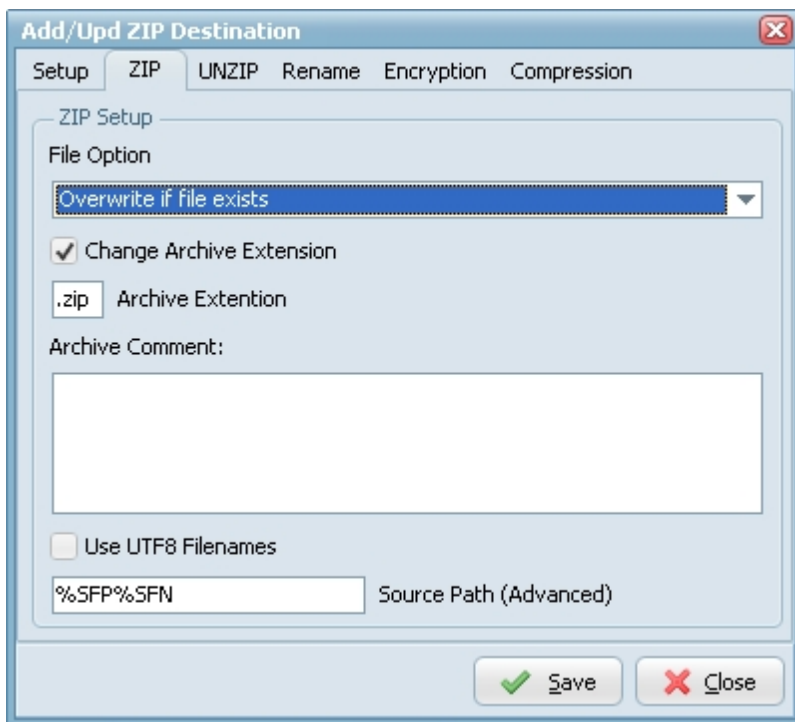
ZIP/UNZIP Destination Setup

Setup Options



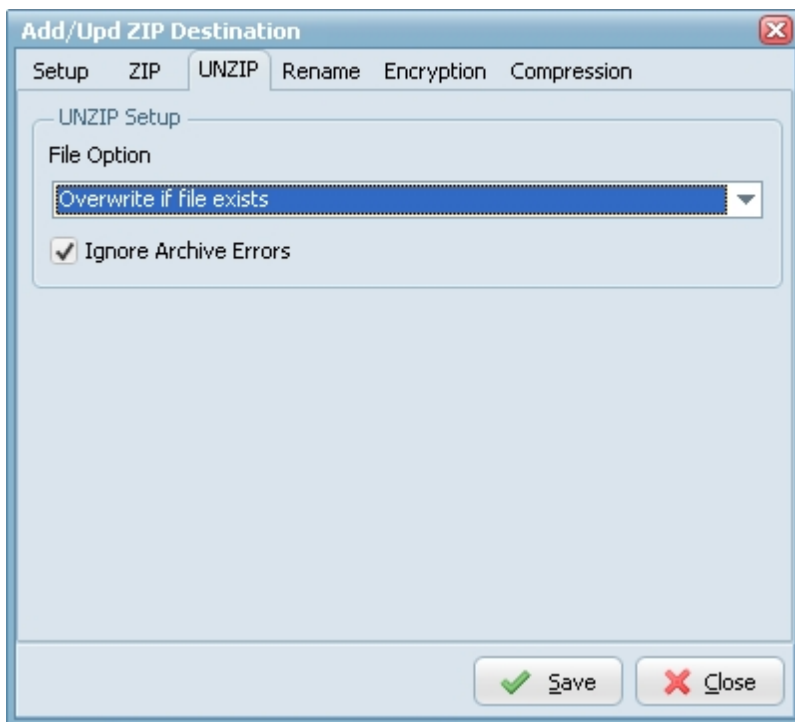
- ▶ Function:
 - ▶ ZIP: Lets you create new archives and modify existing archives.
 - ▶ UNZIP: Lets you read data from existing ZIP archives.
- ▶ Destination Directory: Select Destination Directory, you can use Drag & Drop.

ZIP Options



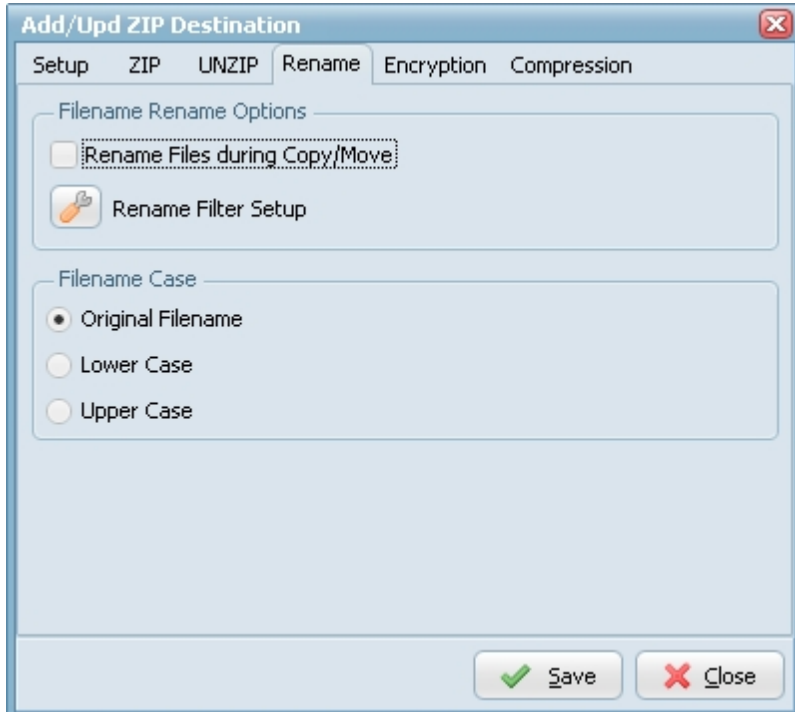
- ▶ **File Option:**
 - ▶ Overwrite if file exists: Destination file will be overwritten.
 - ▶ Only Newer Files: Only newer files will be processed to the destination.
 - ▶ Skip if file exists: Skip if destination file already exists.
 - ▶ Fail if file exists: Error if destination file already exists.
 - ▶ Add version number suffix if file exists: Version number suffix will be added if destination file already exists (i.e. "filename.txt.1").
 - ▶ Add version number (pre-ext) suffix if file exists: Version number (pre-ext) suffix will be added if destination file already exists (i.e. "filename.1.txt").
 - ▶ Add version number prefix if file exists: Version number prefix will be added if destination file already exists (i.e. "1.filename.txt").
 - ▶ Add date time suffix if file exists: Date time suffix will be added if destination file already exists (i.e. "filename.txt.20131116114801"). Format date time used: "YYYYMMDDHHNNSS".
 - ▶ Add date time (pre-ext) suffix if file exists: Date time (pre-ext) suffix will be added if destination file already exists (i.e. "filename.20131116114801.txt"). Format date time used: "YYYYMMDDHHNNSS".
 - ▶ Add date time prefix if file exists: Date time prefix will be added if destination file already exists (i.e. "20131116114801.filename.txt"). Format date time used: "YYYYMMDDHHNNSS".
- ▶ **Change Archive Extension:** Change the extension of the destination filename (i.e. filename.pdf => filename.zip).
- ▶ **Archive Comment:** Contains archive comment.
- ▶ **Use UTF8 Filenames:** Use this option to specify whether we should store file names in UTF8. By default, the file names are stored in OEM encoding. Note that this feature is not supported by most implementations, including 7-Zip, Windows zip folders etc.
- ▶ **Source Path (Advanced):** Defines what will be added to the destination ZIP file (Default value is %SFP%S FN).
 - ▶ %SFP = Source File Path
 - ▶ %S FN = Source File Name

UNZIP Options



- ▶ File Option:
 - ▶ Overwrite if file exists: Destination file will be overwritten.
 - ▶ Only Newer Files: Only newer files will be processed to the destination.
 - ▶ Skip if file exists: Skip if destination file already exists.
 - ▶ Fail if file exists: Error if destination file already exists.
- ▶ Ignore Archive Errors: Specifies if archive errors should be ignored.

Rename Options



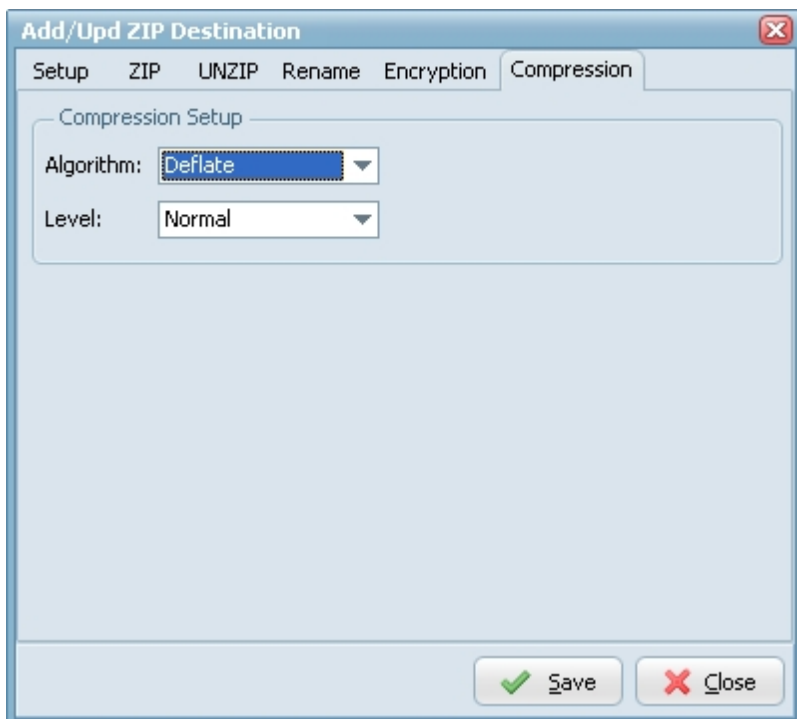
- ▶ Rename Files during Copy/Move: Use regular expressions to rename the destination filename. A very good site with information about regular expressions is <http://www.regular-expressions.info/>
- ▶ Filename Case: Use original filename, lower case or upper case for the destination filenames.

Encryption Options



- ▶ Password: Specifies password to the archive.
- ▶ Encryption:
 - ▶ None
 - ▶ Zip (weak), specifies whether the archive directory entry is encrypted with traditional ZIP encryption.
 - ▶ WinZip AES, specifies whether the archive directory entry is encrypted with WinZip encryption.
 - ▶ PKWare Strong Encryption, specifies if PKWare Strong Encryption should be used.
- ▶ Algorithm:

Compression Options



- ▶ Algorithm: Specifies compression algorithm for the archive entry.
 - ▶ no compression (Stored)
 - ▶ use Deflate compression algorithm
 - ▶ use Deflate64 compression algorithm (supported by PKZip version 2.50 and above)
 - ▶ use bzip2 compression algorithm

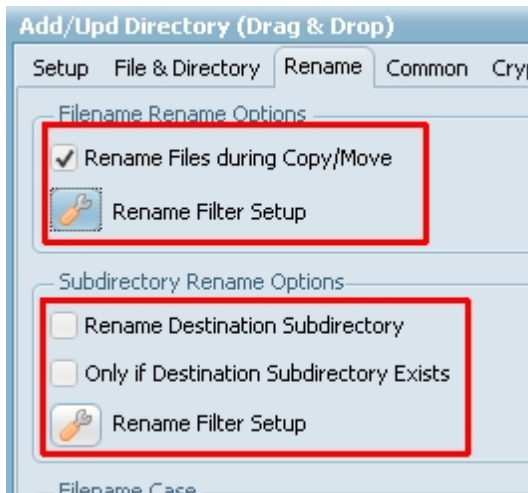
- Level: Specifies compression level for the archive entry.

Renaming

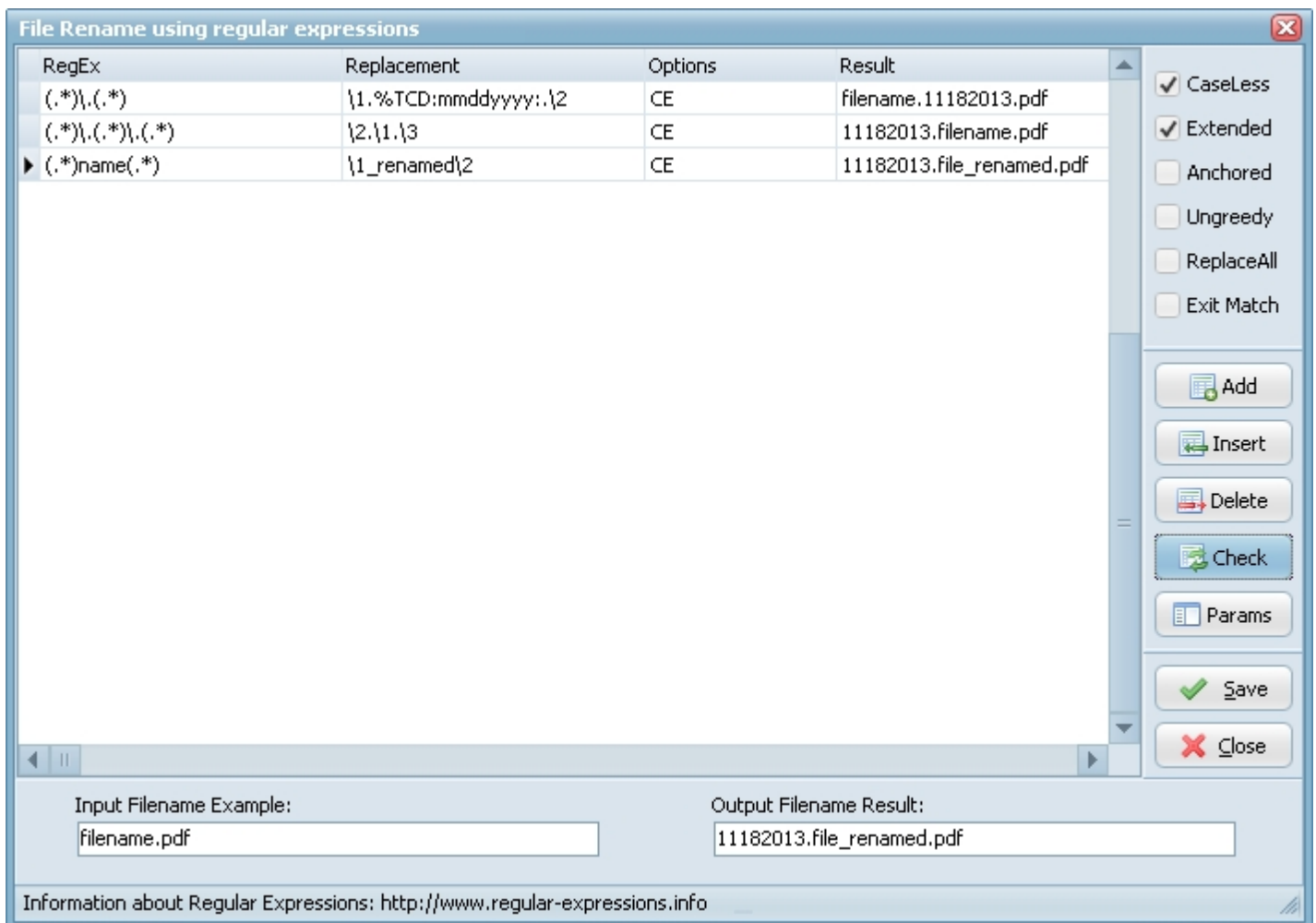
Rename Options

With LimagitoX you can rename destination files and subdirectories. The technique we use is called regular expressions. A regular expression (regex or regexp for short) is a special text string for describing a search pattern. You can think of regular expressions as wildcards on steroids. A very good site with information about regular expressions is <http://www.regular-expressions.info/>

You can find the rename option in the destination 'Rename' tab.



Rename Filter Setup Options



- ▶ Add: Add Regular Expression row.
- ▶ Insert: Insert Regular Expression row.
- ▶ Delete: Delete selected Regular Expression row.
- ▶ Check: Check the Regular Expressions Output Filename Result.
- ▶ Params: Show possible Replacement Parameters. You can add many different parameters like current date, file modified date, ... as a replacement paramter.

Replacement Parameters	
ShortName	Description
%SFS	Source, SubDirectory
%SFS:1-1:	Source, SubDirectory: begin pos. - End pos.
%SFN	Source, File Name
%SFN:1-1:	Source, File Name: begin pos. - End pos.
%SFW	Source, File Name without Extension
%SFW:1-1:	Source, File Name without Extension: begin pos. - End pos.
%TCD	Time, Current Date
%TCD:mmddyyyy:	Time, Current Date mmddyyyy (Adjustable)
%TCD:[IncMinute+1]mmddyyyy	Time, Current Date mmddyyyy (Adjustable)
%TCD:[IncMinute-1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustable)
%TCD:[IncDay+1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustable)
%TCD:[IncDay-1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustable)
%TCD:[IncMonth+1]mmddyyyy	Time, Current Date mmddyyyy (Adjustable)
%TCD:[IncMonth-1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustable)
%TCD:[IncYear+1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustable)
%TCD:[IncYear-1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustable)
%SFM	Source, File Modified Date
%SFM:mmddyyyy:	Source, File Modified Date mmddyyyy (Adjustable)
%SFM:[IncMinute+1]mmddyyyy	Source, File Modified Date mmddyyyy (Adjustable)
%SFM:[IncMinute-1]mmddyyyy:	Source, File Modified Date mmddyyyy (Adjustable)

- The date parameter formatting string (i.e. :mmddyyyy:) can comprise a mix of ordinary characters (that are passed unchanged to the result string), and data formatting characters. The following data formatting character strings can be used:

w

Displays the week without a leading zero (1-53).

ww

Displays the minute with a leading zero (01-53).

c

Displays the date using the format given by the ShortDateFormat global variable, followed by the time using the format given by the LongTimeFormat global variable. The time is not displayed if the date-time value indicates midnight precisely.

d

Displays the day as a number without a leading zero (1-31).

dd

Displays the day as a number with a leading zero (01-31).

ddd

Displays the day as an abbreviation (Sun-Sat) using the strings given by the ShortDayNames global variable.

dddd

Displays the day as a full name (Sunday-Saturday) using the strings given by the LongDayNames global variable.

ddddd

Displays the date using the format given by the ShortDateFormat global variable.

dddddd

Displays the date using the format given by the LongDateFormat global variable.

e

Displays the year in the current period/era as a number without a leading zero (Japanese, Korean, and Taiwanese locales only).

ee

Displays the year in the current period/era as a number with a leading zero (Japanese, Korean, and Taiwanese locales only).

g

Displays the period/era as an abbreviation (Japanese and Taiwanese locales only).

gg

Displays the period/era as a full name (Japanese and Taiwanese locales only).

m

Displays the month as a number without a leading zero (1-12). If the m specifier immediately follows an h or hh specifier, the minute rather than the month is displayed.

mm

Displays the month as a number with a leading zero (01-12). If the mm specifier immediately follows an h or hh specifier, the minute rather than the month is displayed.

mmm

Displays the month as an abbreviation (Jan-Dec) using the strings given by the ShortMonthNames global variable.

mmmm

Displays the month as a full name (January-December) using the strings given by the LongMonthNames global variable.

yy

Displays the year as a two-digit number (00-99).

yyyy

Displays the year as a four-digit number (0000-9999).

h

Displays the hour without a leading zero (0-23).

hh

Displays the hour with a leading zero (00-23).

n

Displays the minute without a leading zero (0-59).

nn

Displays the minute with a leading zero (00-59).

s

Displays the second without a leading zero (0-59).

ss

Displays the second with a leading zero (00-59).

z

Displays the millisecond without a leading zero (0-999).

zzz

Displays the millisecond with a leading zero (000-999).

t

Displays the time using the format given by the ShortTimeFormat global variable.

tt

Displays the time using the format given by the LongTimeFormat global variable.

am/pm

Uses the 12-hour clock for the preceding h or hh specifier, and displays 'am' for any hour before noon, and 'pm' for any hour after noon. The am/pm specifier can use lower, upper, or mixed case, and the result is displayed accordingly.

a/p

Uses the 12-hour clock for the preceding h or hh specifier, and displays 'a' for any hour before noon, and 'p' for any hour after noon. The a/p specifier can use lower, upper, or mixed case, and the result is displayed accordingly.

ampm

Uses the 12-hour clock for the preceding h or hh specifier, and displays the contents of the TimeAMString global variable for any hour before noon, and the contents of the TimePMString global variable for any hour after noon.

/

Displays the date separator character given by the DateSeparator global variable.

:

Displays the time separator character given by the TimeSeparator global variable.