LimagitoXI File Mover

Overview

Overview

About

File Mover Software from Limagito.com

LimagitoX File Mover - Move your files from anywhere to anywhere

The product name is LimagitoX File Mover. The current version is XI.

LimagitoX File Mover 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 feautures:

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, AWSS3, WEBDAV 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

- LimagitoXI Help v2016.05.27 (draft)
- LimagitoXI Help v2016.05.30

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

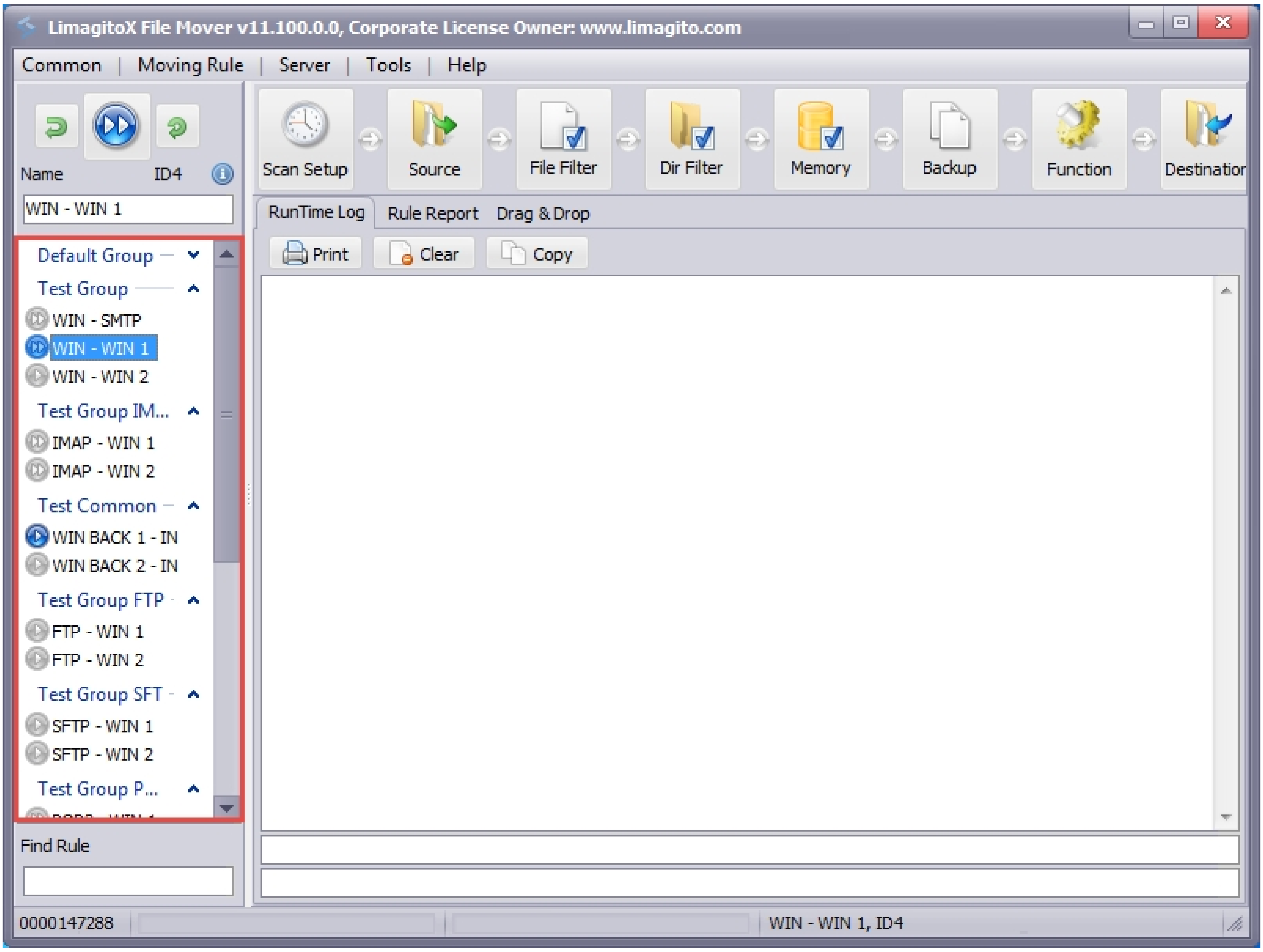
- GUI Introduction
- Common
- Moving Rule
- Server
- Tools
- Help
- Source Options
- Destination Options
- Service Options

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.



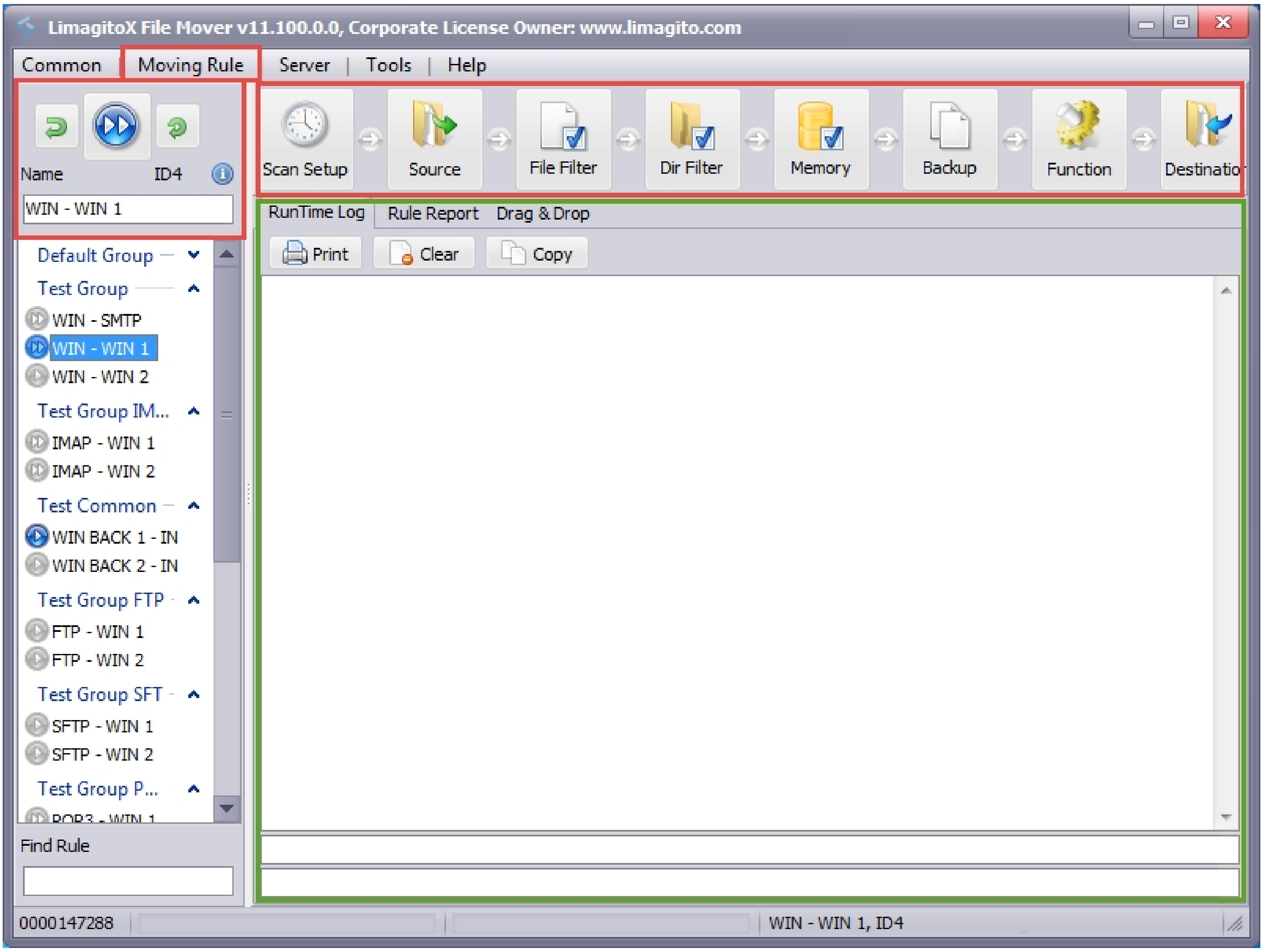
LimagitoX File Mover v11.100.0.0, Corporate License Owner: www.limagito.com

Name: WIN - WIN 1   ID4

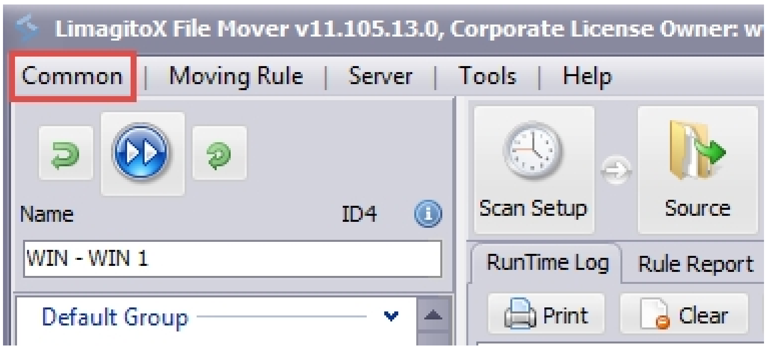
WIN - WIN 1, ID4

0000147288

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

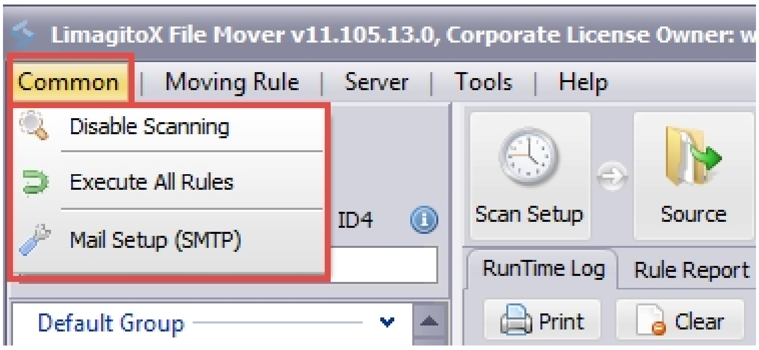


In the 'Common' menu you can find options that are used by all rules. This is what we refer to as common options.



Common Options

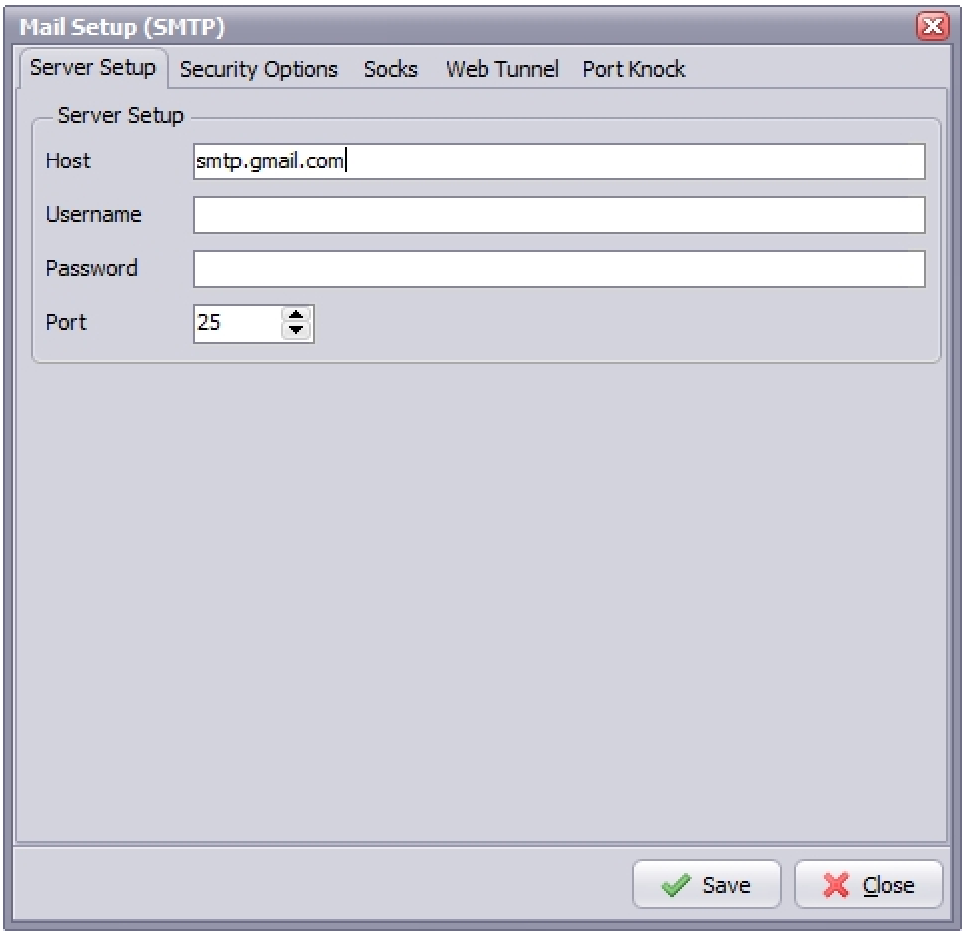
Common Options (Common for all rules)



- 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): 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.

Mail Setup (SMTP)

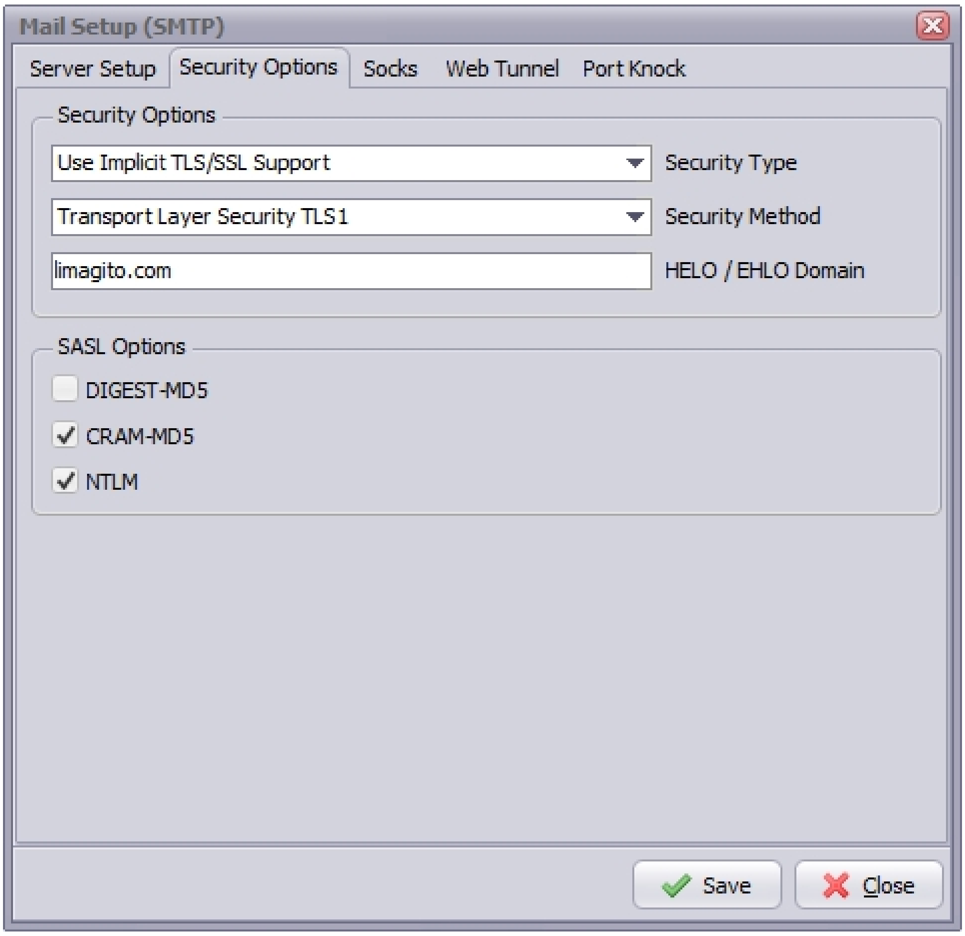
Server Setup



Host: smtp.gmail.com
Username:
Password:
Port: 25

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



Security Options

Use Implicit TLS/SSL Support	Security Type
Transport Layer Security TLS1	Security Method
limagito.com	HELO / EHLO Domain

SASL Options

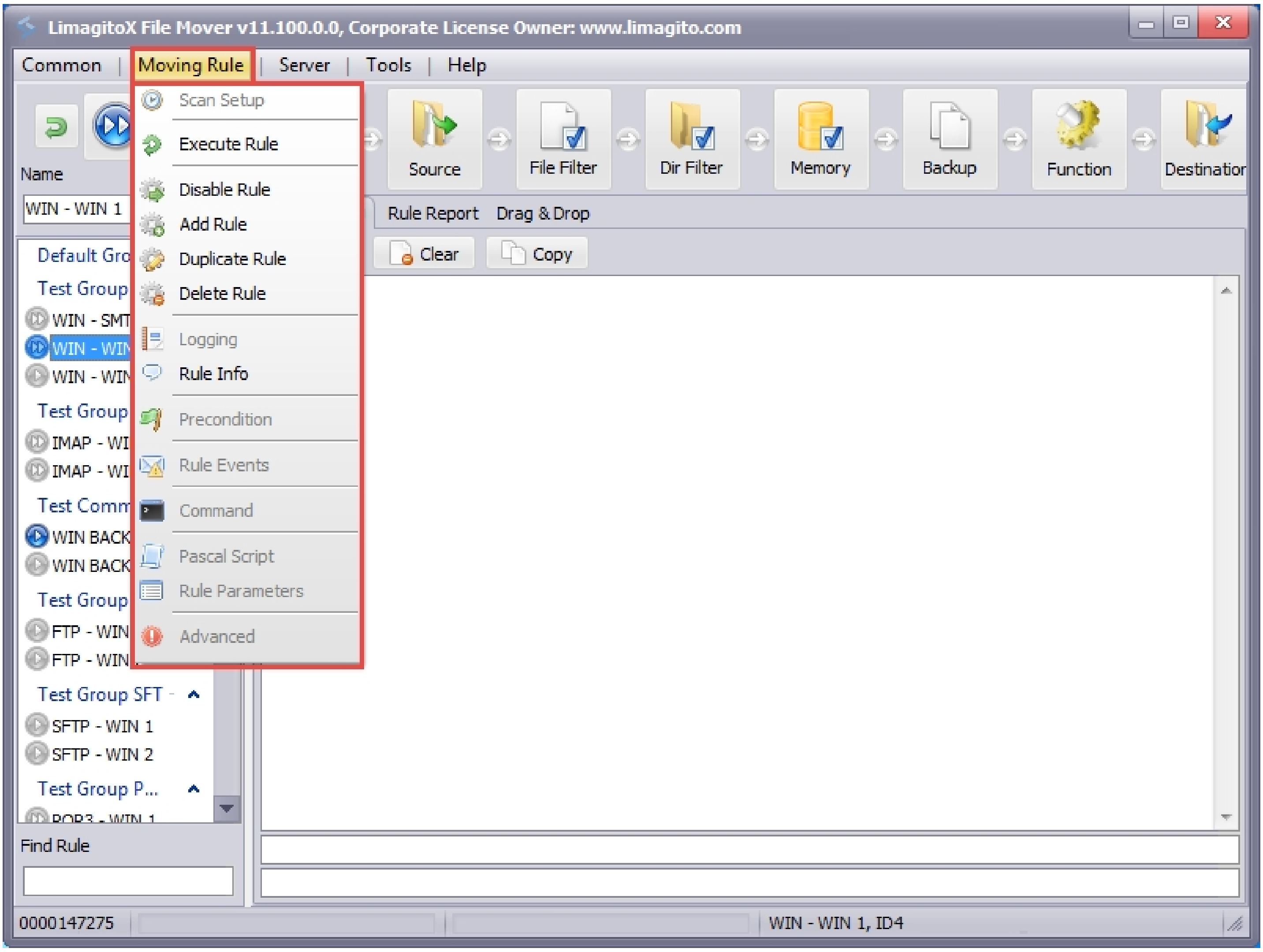
- □ DIGEST-MD5
- ☑ CRAM-MD5
- ☑ NTLM

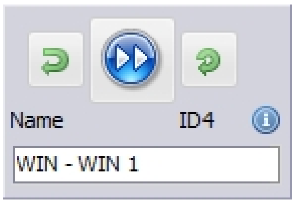
- With the security options you can enable TLS/SSL support for SMTP.
- HELO/EHLO Domain: Ask the server for the SMTP extensions that the server supports, by using the EHLO greeting of the Extended SMTP specification (RFC 1870). Fall back to HELO only if the server does not respond to EHLO.

Rule Options

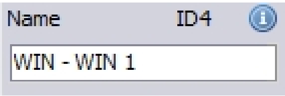
Moving Rule (Unique for each rule)

- Scan Setup
- Logging
- Rule Info
- Precondition
- Rule Events
- Command
- Pascal Script
- Advanced





- Toggle switch: Enable/Disable the selected moving rule.

- 

Short name (description) for the selected moving rule + ID number of the Rule.

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

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

Scan Setup

Scan Setup

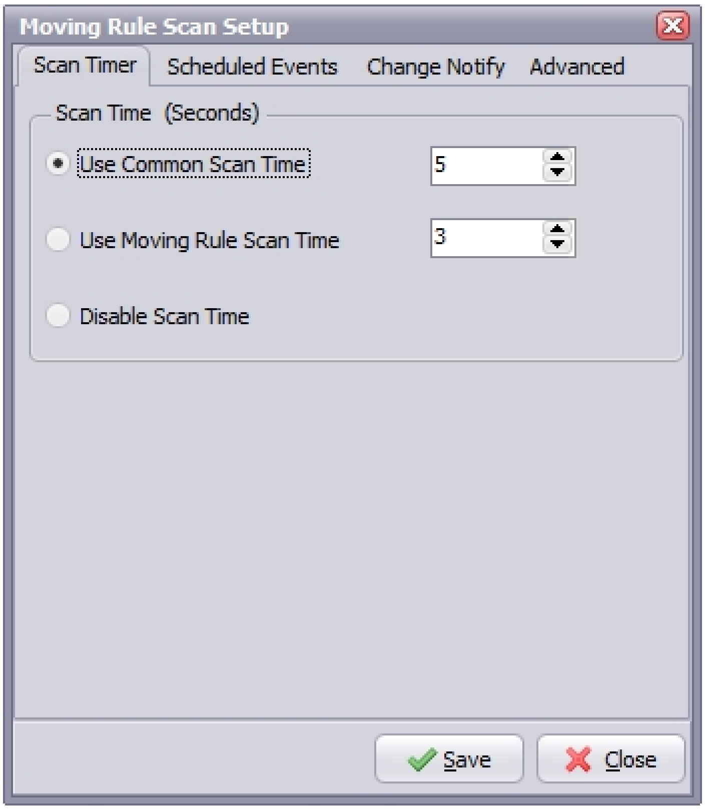
A trigger is an event that executes a rule. The default ‘trigger' for a new rule is the common scan time. Next to the manual trigger we have three automatic triggers available for each moving rule:

1) Scan Timer

2) Scheduled Events

3) Change Notify (WIN as Source)

Scan Timer



Scan Time (Seconds)

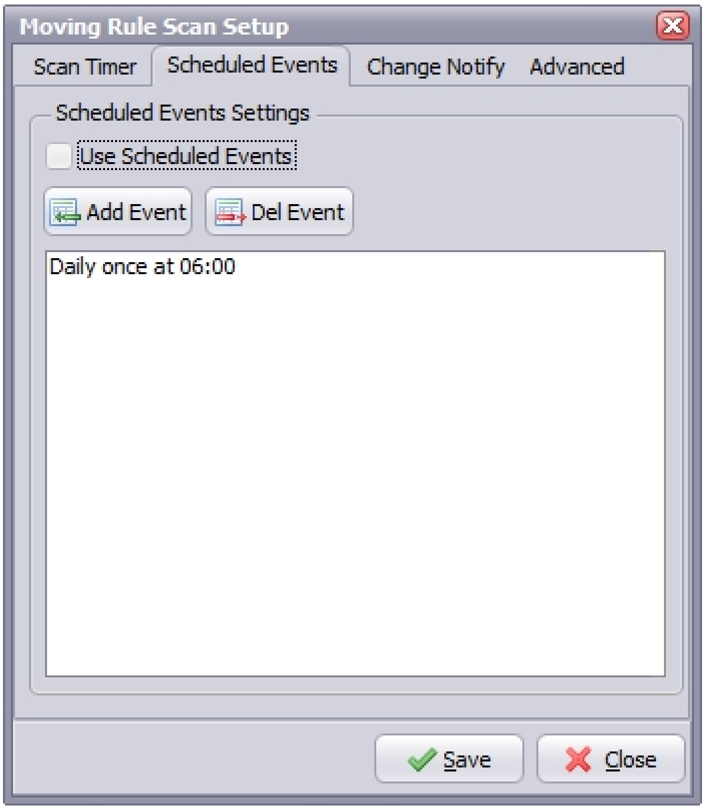
● Use Common Scan Time 5

○ Use Moving Rule Scan Time 3

○ Disable Scan Time

- 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

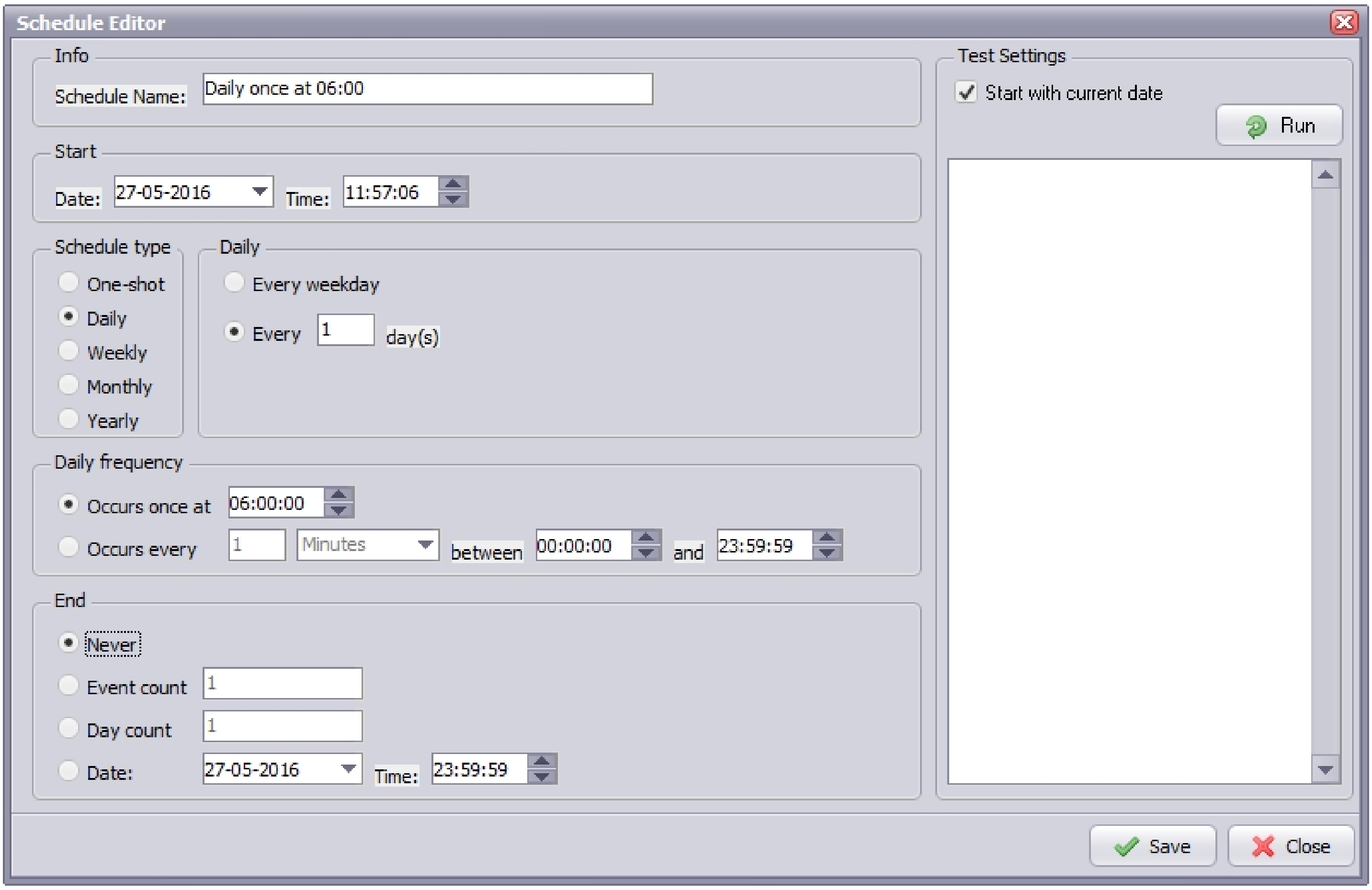


Scheduled Events Settings

□ Use Scheduled Events

Daily once at 06:00

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



Info

Schedule Name: Daily once at 06:00

Start

Date: 27-05-2016 Time: 11:57:06

Schedule type

○ One-shot
● Daily
○ Weekly
○ Monthly
○ Yearly

Daily

○ Every weekday
● Every 1 day(s)

Daily frequency

● Occurs once at 06:00:00
○ Occurs every 1 Minutes between 00:00:00 and 23:59:59

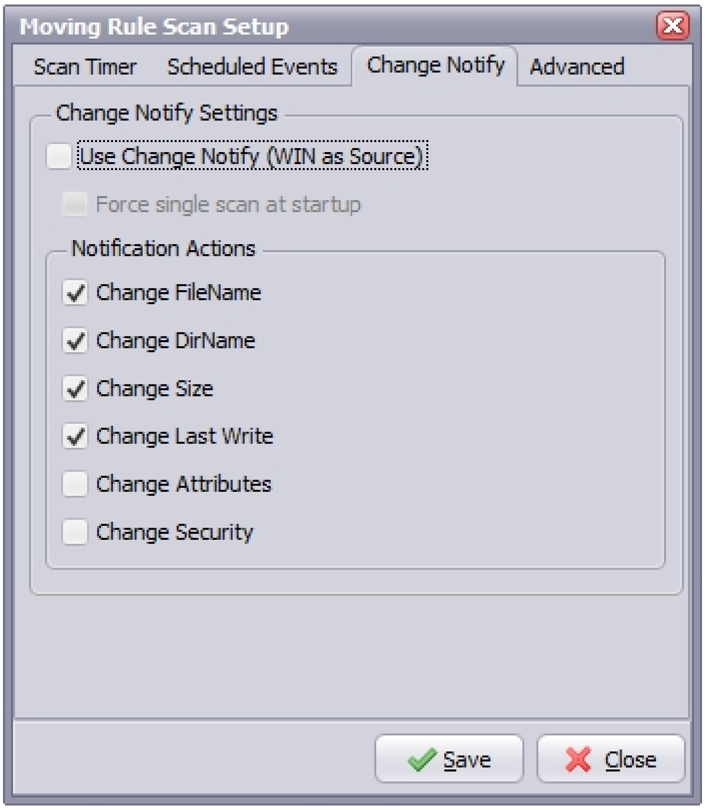
End

● Never
○ Event count 1
○ Day count 1
○ Date: 27-05-2016 Time: 23:59:59

Test Settings

☑ Start with current date

Change Notify



Change Notify Settings

□ Use Change Notify (WIN as Source)

□ Force single scan at startup

Notification Actions

☑ Change FileName

☑ Change DirName

☑ Change Size

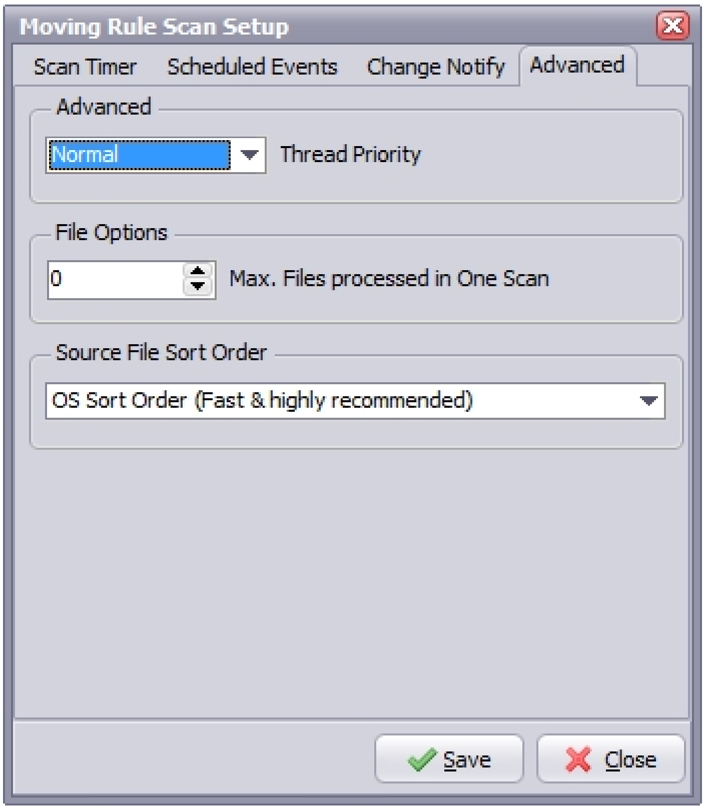
☑ Change Last Write

□ Change Attributes

□ Change Security

- 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



Advanced

Normal — Thread Priority

File Options

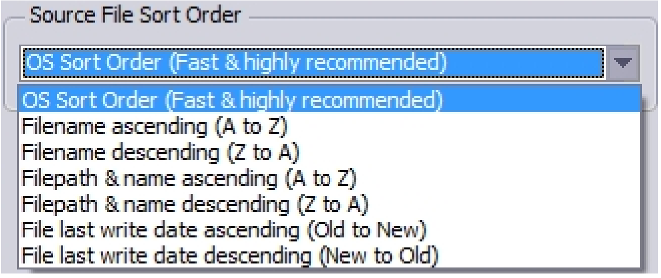
0 — Max. Files processed in One Scan

Source File Sort Order

OS Sort Order (Fast & highly recommended)

- 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).



Source File Sort Order

OS Sort Order (Fast & highly recommended)

- OS Sort Order (Fast & highly recommended)
- Filename ascending (A to Z)
- Filename descending (Z to A)
- Filepath & name ascending (A to Z)
- Filepath & name descending (Z to A)
- File last write date ascending (Old to New)
- File last write date descending (New to Old)

- Source File Sort Order: Let you change the way files are handled during output. (default = OS Sort Order = Fast & highly recommended).

Logging

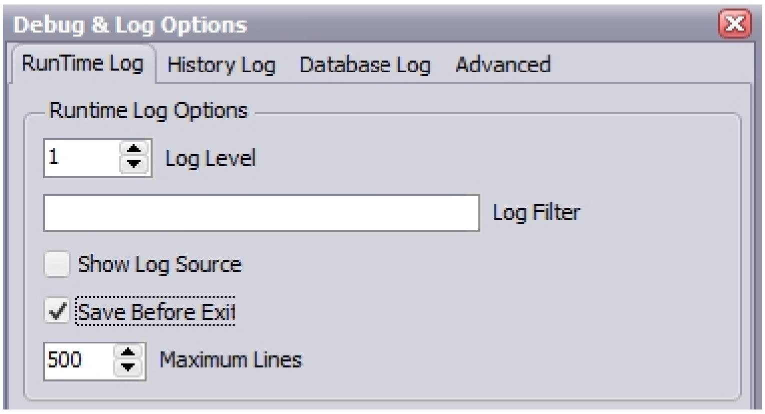
Logging

- RunTime Log
- History Log
- Database Log
- Advanced

RunTime Log

RunTime Log

Logging to the Runtime window in the application



Debug & Log Options

Runtime Log Options

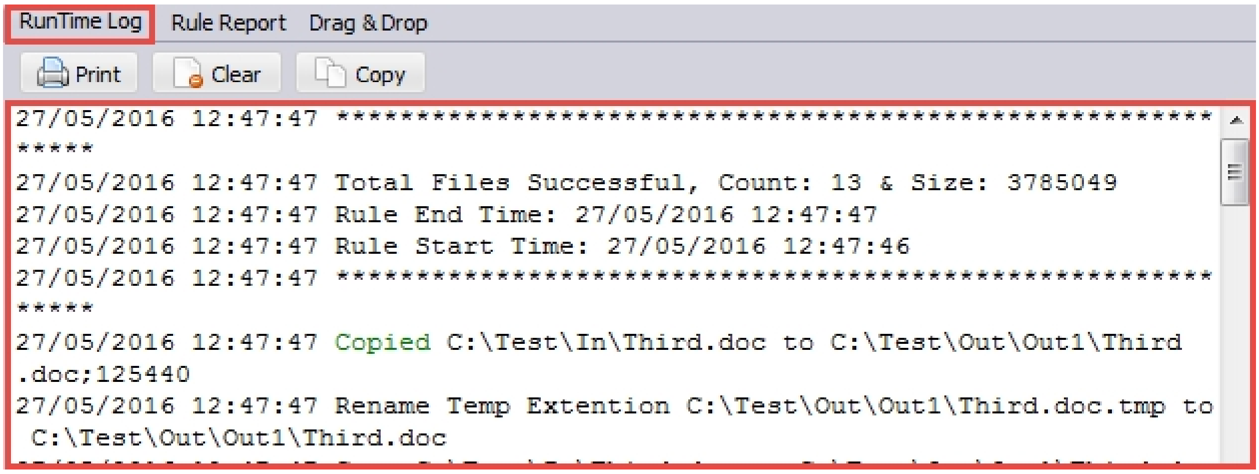
1 Log Level

Log Filter

□ Show Log Source

☑ Save Before Exit

500 Maximum Lines

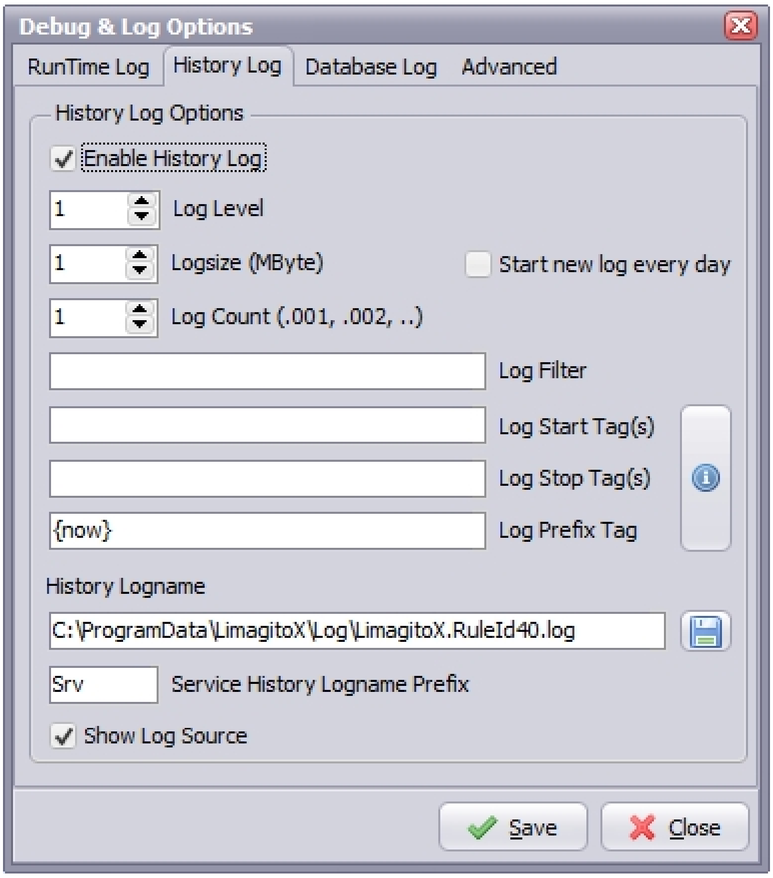


```
27/05/2016 12:47:47 ******************************************************
*****
27/05/2016 12:47:47 Total Files Successful, Count: 13 & Size: 3785049
27/05/2016 12:47:47 Rule End Time: 27/05/2016 12:47:47
27/05/2016 12:47:47 Rule Start Time: 27/05/2016 12:47:46
27/05/2016 12:47:47 ******************************************************
*****
27/05/2016 12:47:47 Copied C:\Test\In\Third.doc to C:\Test\Out\Out1\Third
.doc;125440
27/05/2016 12:47:47 Rename Temp Extention C:\Test\Out\Out1\Third.doc.tmp to
 C:\Test\Out\Out1\Third.doc
```

- Log 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 Filter: You can add more then one Log Filter each separated by ';' (i.e. error;exception). This will limit the information in the RunTime Log.
- Show log Source: Show which object is sending the log information (i.e. File Filter, Dir Filter, ...).
- Save Before Exit: The current content of the RunTime log will be available again after restart of the application.
- Maximum Lines: The maximum amount of lines in the RunTime Log window.

History Log

History Log



History Log Options

☑ Enable History Log

1 Log Level

1 Logsize (MByte)

□ Start new log every day

1 Log Count (.001, .002, ..)

Log Filter

Log Start Tag(s)

Log Stop Tag(s)

{now} Log Prefix Tag

History Logname

C:\ProgramData\LimagitoX\Log\LimagitoX.RuleId40.log

Srv Service History Logname Prefix

☑ Show Log Source

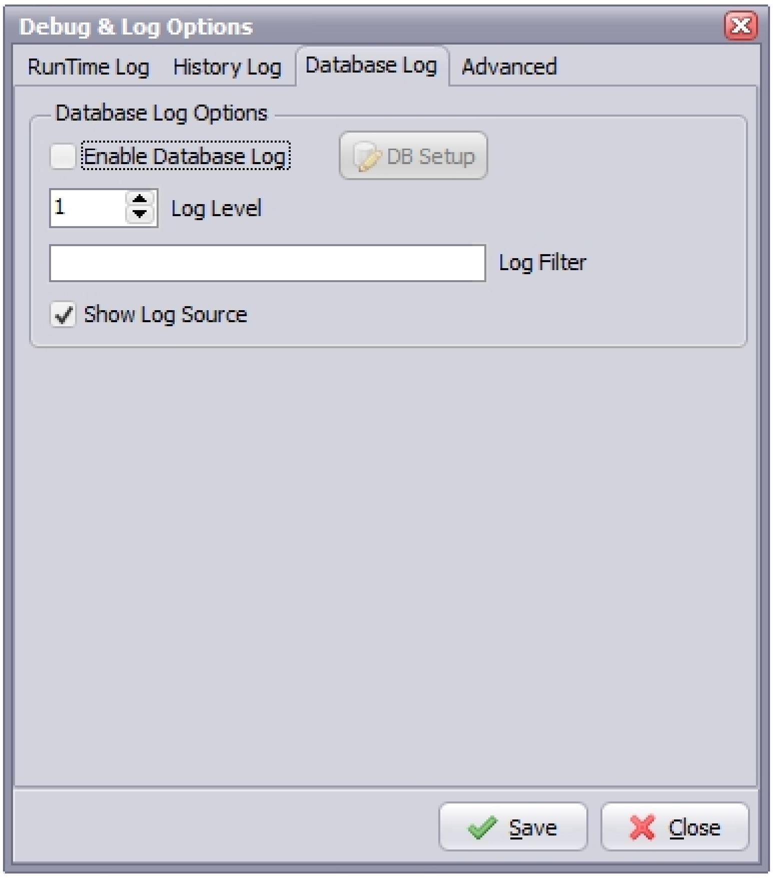
- Enable History Log: Enable logging to file for the selected thread (moving rule).
- Setup Log: Setup log options for the selected Limagito thread.
- Logging Level 1-10: Increase the log level if you need more 'debug' information (default 1). Don't use level 10 during production, only for testing.
- Log Size: Set the maximum size for the log file.
- Log 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.

- Start new log every day: Force new log file each day.
- 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.
- Log Start Tag(s):
- Log Stop Tag(s):
- Log Prefix Tag:
- Log Filename: Select the filename for the log file.
- Show log Source: Show which object is sending the log information (i.e. File Filter, Dir Filter, ...).

Database Log

Database Log



Debug & Log Options

Database Log Options

☐ Enable Database Log

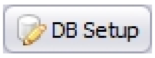
Log Level: 1

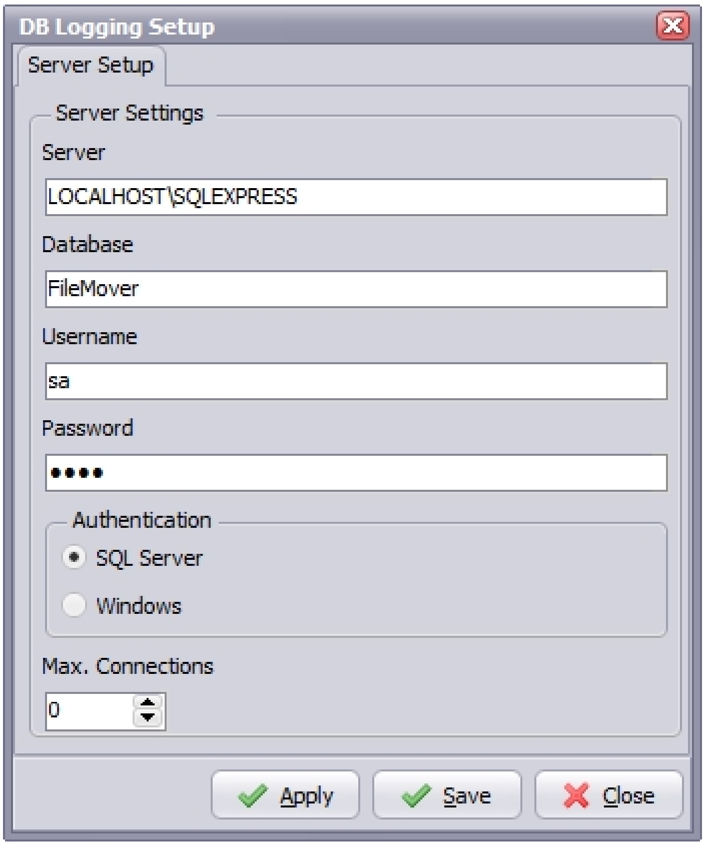
Log Filter:

☑ Show Log Source

- Enable Database Log: Enable logging to a MSSQL database for the selected thread (moving rule).
- DB Setup: Database connection setup
- 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 Filter: You can add more then one Log Filter each separated by ';' (i.e. error;exception). This will limit the information in the database Log.
- Show log Source: Show which object is sending the log information (i.e. File Filter, Dir Filter, ...).

Database connection setup





Server: LOCALHOST\SQLEXPRESS

Database: FileMover

Username: sa

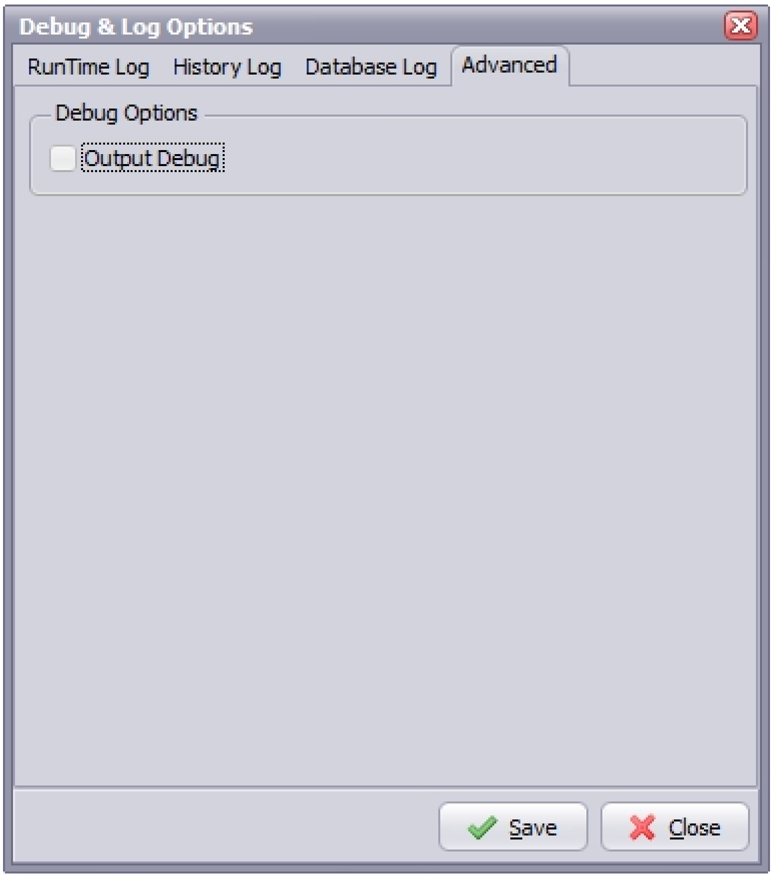
Password: ●●●●

Authentication
● SQL Server
○ Windows

Max. Connections: 0

Advanced

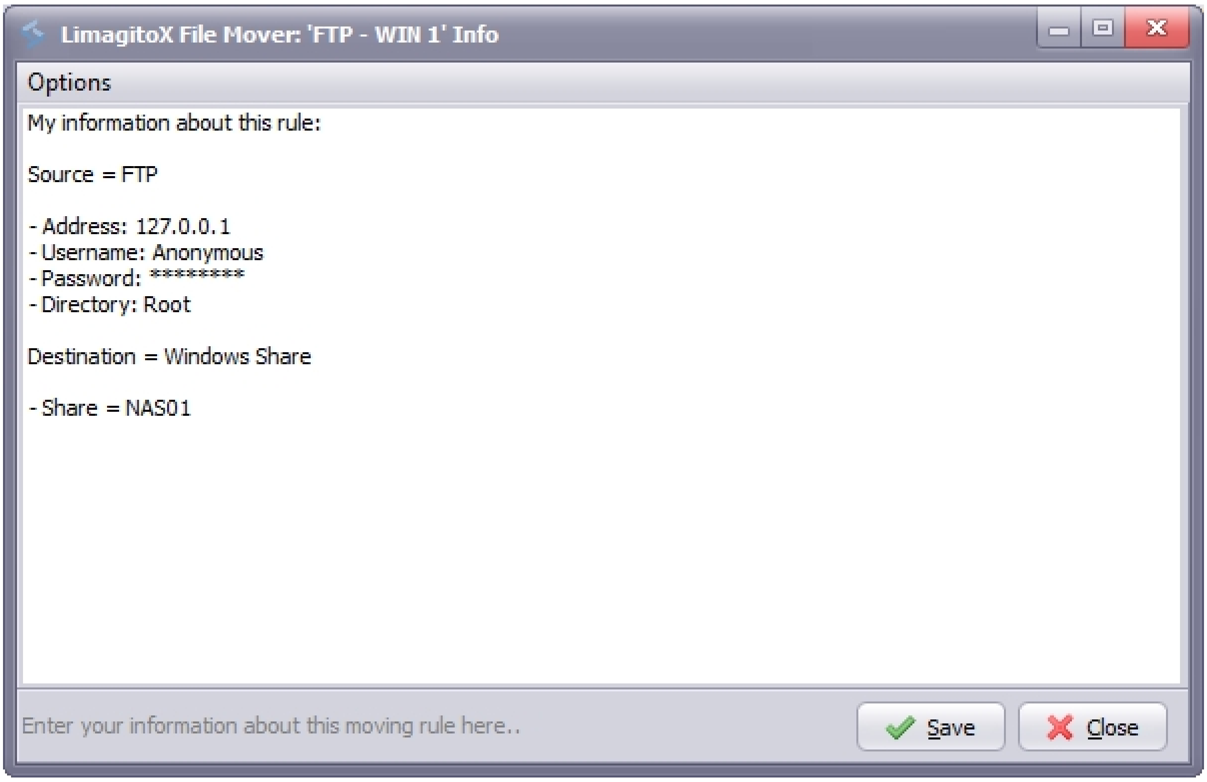
Advanced



- 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


LimagitoX File Mover: 'FTP - WIN 1' Info
Options
Enter your information about this moving rule here..
Save
Close

My information about this rule:

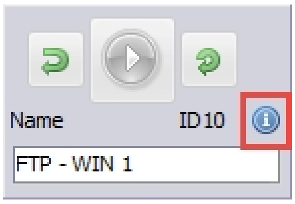
Source = FTP

- Address: 127.0.0.1
- Username: Anonymous
- Password: *********
- Directory: Root

Destination = Windows Share

- Share = NAS01

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



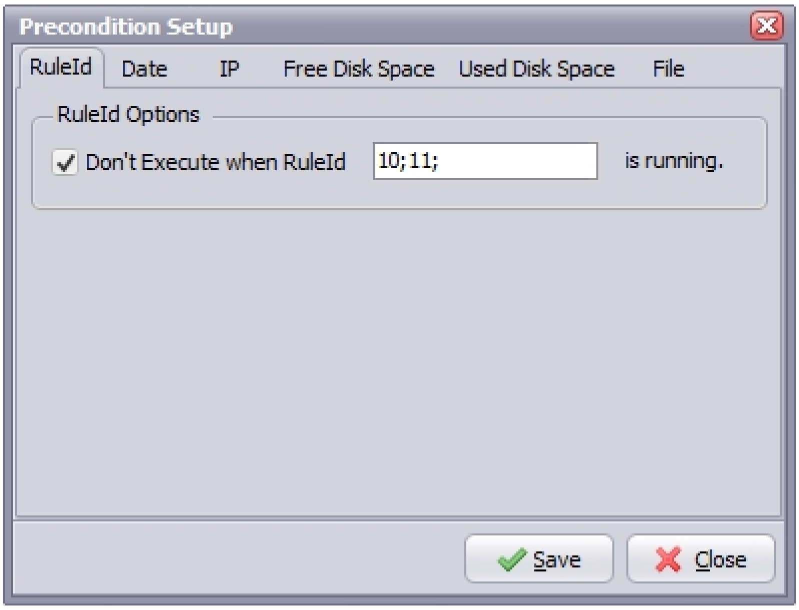
- Shortcut to Rule information.

Precondition

Precondition

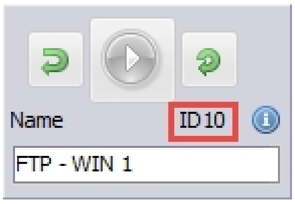
The precondition option let's you decide whether or not to execute the rule. When a rule is triggered it will check the preconditions first. If they are valid then the rule will continue, otherwise it will wait on the next scan trigger. At this moment we have 3 preconditions that you can use. Each moving rule will check its own preconditions.

1. RuleId

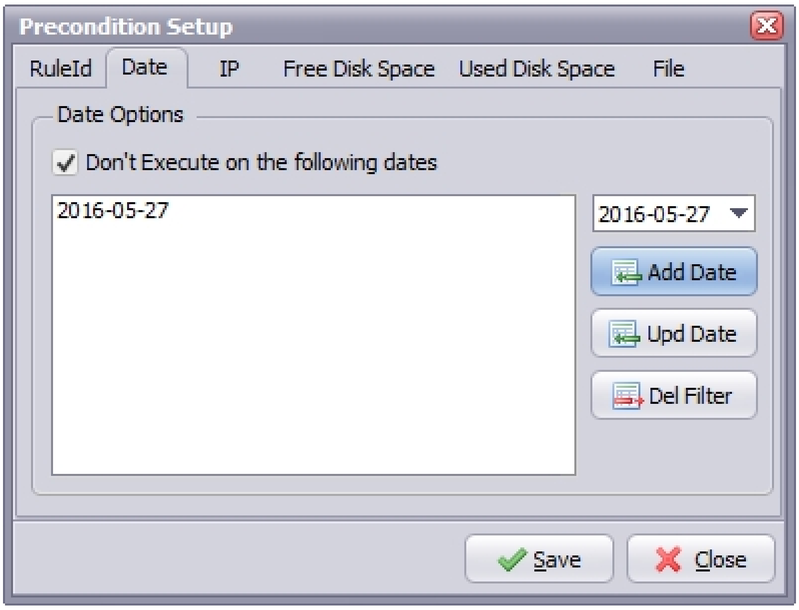


☑ Don't Execute when RuleId 10;11; is running.

- 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 10 or ID 11 is running. You can find the rule ID next to the rule name.



2. Date



Date Options

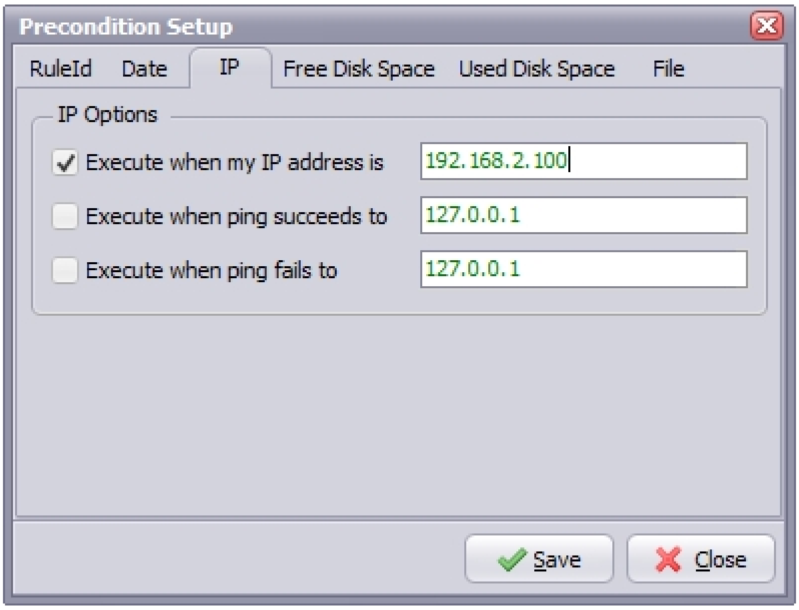
☑ Don't Execute on the following dates

2016-05-27

2016-05-27

- The trigger will not continue on the following dates: The rule won't run on the added dates.

3. IP



IP Options

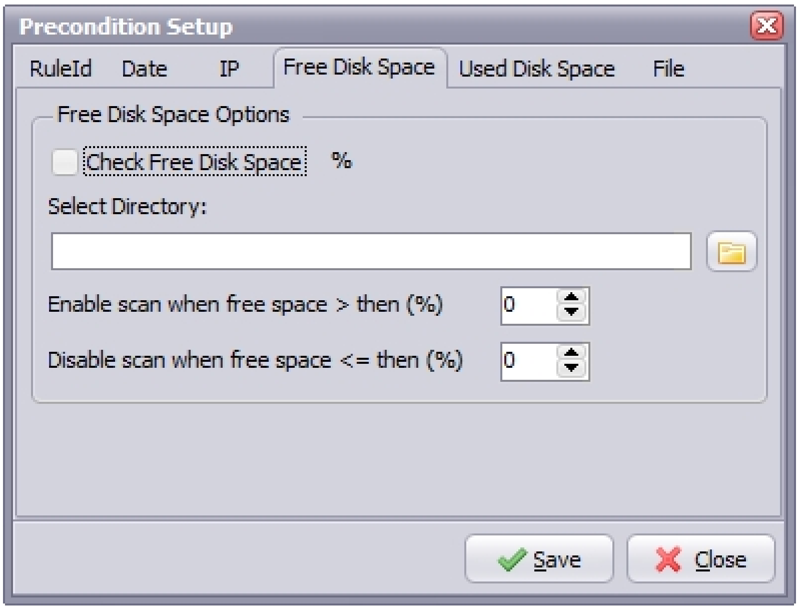
☑ Execute when my IP address is 192.168.2.100

☐ Execute when ping succeeds to 127.0.0.1

☐ Execute when ping fails to 127.0.0.1

- Execute when my IP address is ?: The rule will check the IP address of the host. If this isn't correct than the rule trigger will not continue. 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.
- Execute when ping succeeds to ?: The rule trigger will continue when the ping succeeds. You can add more then one address each separated by ';' (i.e. 192.168.2.201;192.168.2.202). In this case they all need to succeed.
- Execute when ping fails to ?: The rule trigger will continue when the ping fails. You can add more then one address each separated by ';' (i.e. 192.168.2.203;192.168.2.204). In this case they all need to fail.

4. Free Disk Space



□ Check Free Disk Space %

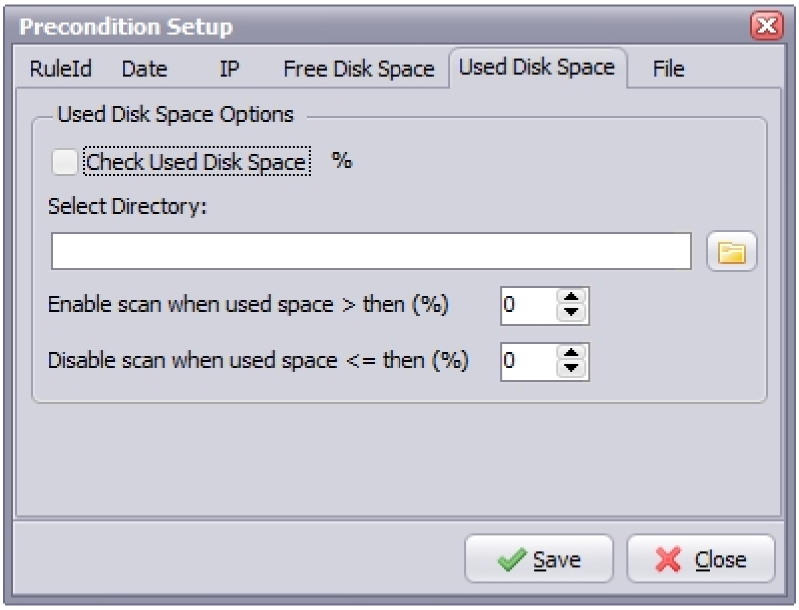
Select Directory:

Enable scan when free space > then (%) 0

Disable scan when free space <= then (%) 0

- Check Free Disk Space: Enable checking of free disk space to continue/exit the trigger.
- Select Directory: Directory that will we used during the 'Free Disk Space' check.
- Enable scan when free space > then (%): Continue trigger when free space is larger then setup.
- Disable scan when free space <= then (%): Exit trigger when free space is below setup.

5. Used Disk Space



□ Check Used Disk Space %

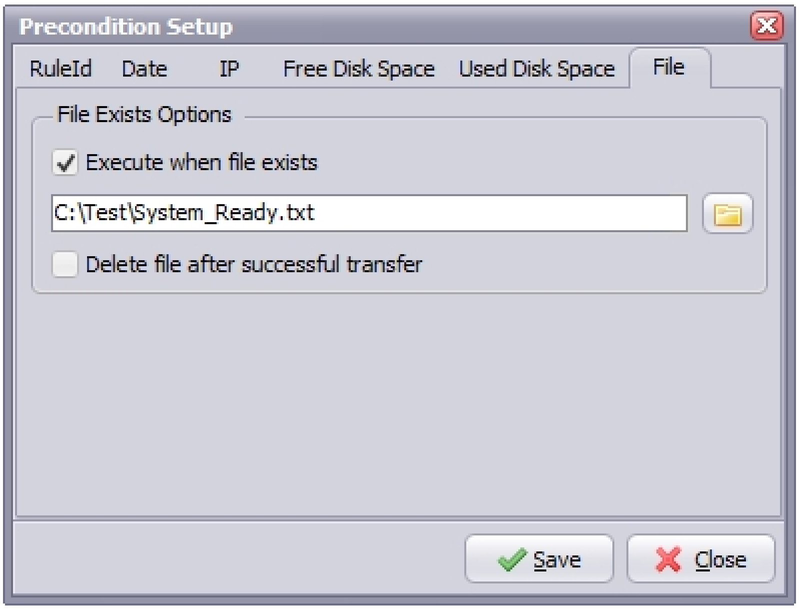
Select Directory:

Enable scan when used space > then (%) 0

Disable scan when used space <= then (%) 0

- Check Used Disk Space: Enable checking of used disk space to continue/exit the trigger.
- Selected Directory: Directory that will we used during the 'Used Disk Space' check.
- Enable scan when used space > then (%): Continue trigger when used space is larger then setup.
- Disable scan when used space <= then (%): Exit trigger when used space is below setup.

6. File



File Exists Options

☑ Execute when file exists

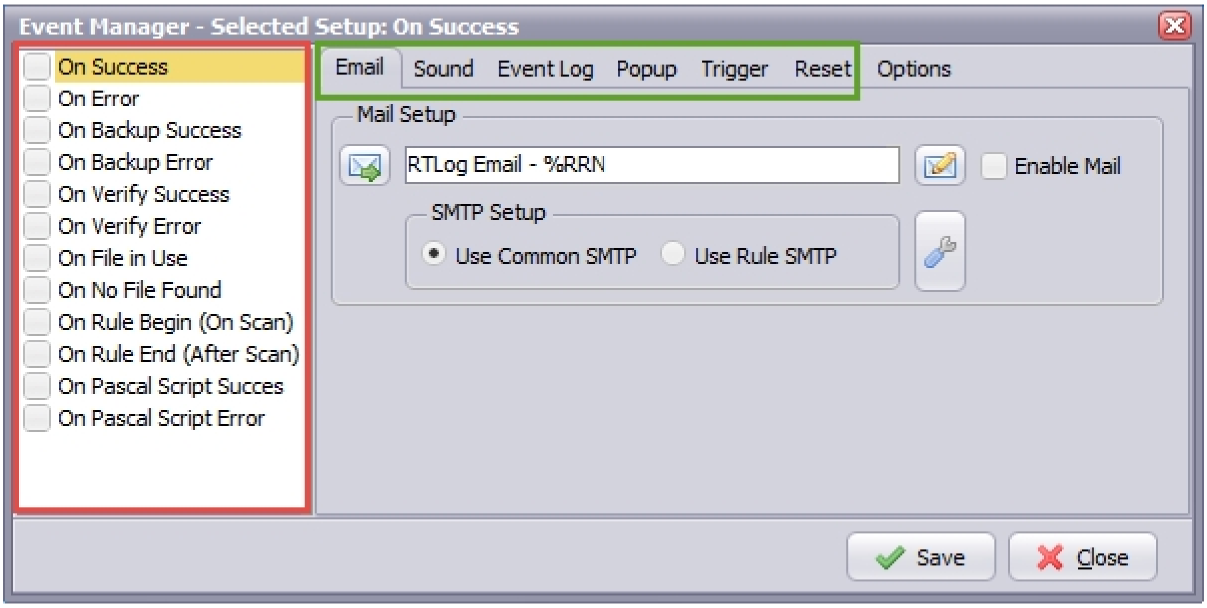
C:\Test\System_Ready.txt

□ Delete file after successful transfer

- Execute when file exists: Trigger will continue when selected file exists.
- Selected File: File that will we used during the 'File Exists Option'.
- Delete file after successful transfer: Selected file will be deleted after successful transfer of the Source files.

Rule Events

Rule Events



□ On Success
□ On Error
□ On Backup Success
□ On Backup Error
□ On Verify Success
□ On Verify Error
□ On File in Use
□ On No File Found
□ On Rule Begin (On Scan)
□ On Rule End (After Scan)
□ On Pascal Script Succes
□ On Pascal Script Error

Mail Setup

RTLog Email - %RRN

□ Enable Mail

SMTP Setup

● Use Common SMTP ○ Use Rule SMTP

With this option you can trigger procedure(s) (marked green) at different application events (marked red). Important, each event will use its own procedure setup. So select the event on the left and change the setup of the procedures on the right. You need to repeat this for every enabled event.

Current supported events:

- On Success
- On Error
- On Backup Success
- On Backup Error
- On Verify Success
- On Verify Error
- On File in Use
- On No File Found

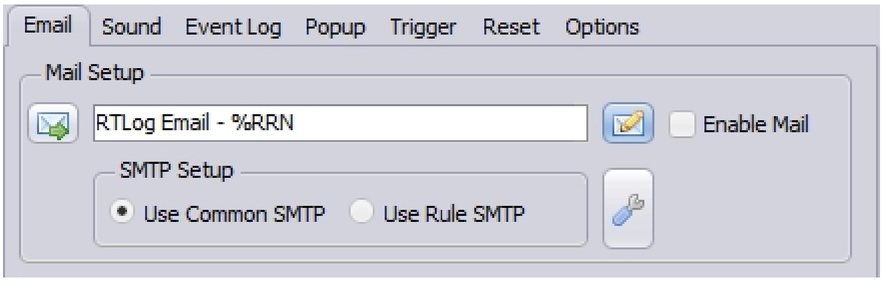
On Rule Begin (On Scan)	First event when the rule is triggered, sequence is started.
On Rule End (After Scan)	Last event of the rule sequence.
On Pascal Script Succes	
On Pascal Script Error	

Current supported procedures:

- 'Email' (SMTP)
- 'Sound'
- Windows 'Event Log'
- 'Popup'
- 'Trigger' Rule
- 'Reset' Rule Scan Timer

---

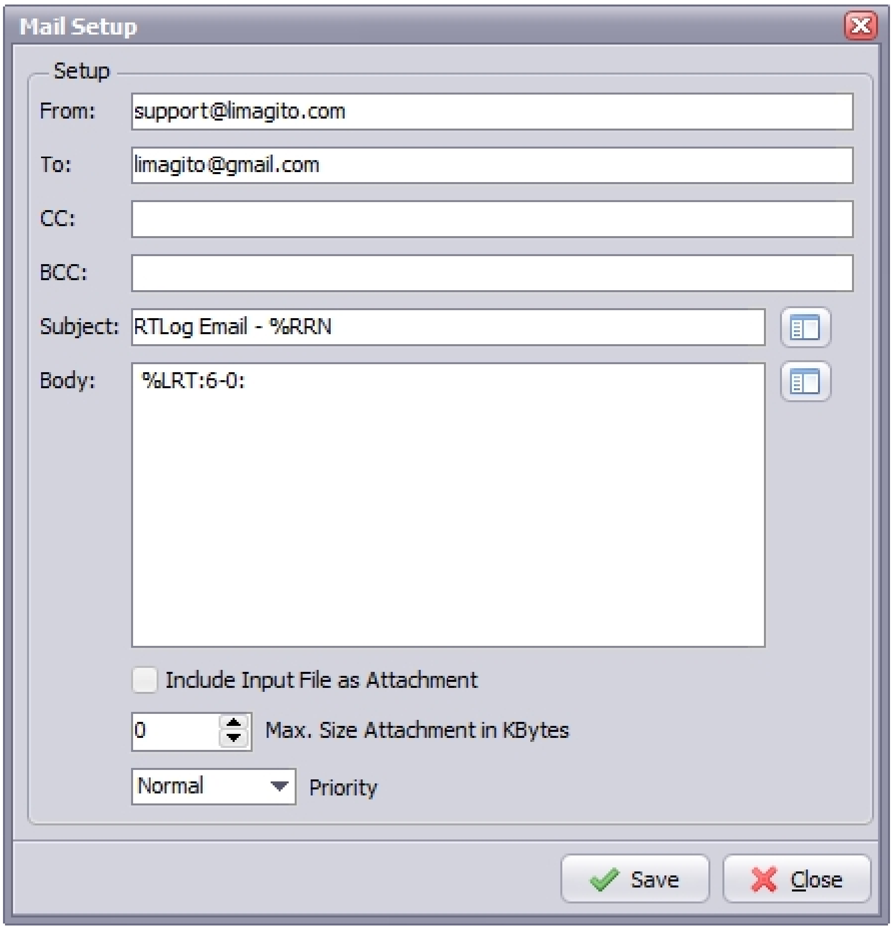
1. Email



RTLog Email - %RRN

□ Enable Mail

● Use Common SMTP ○ Use Rule SMTP



From: support@limagito.com

To: limagito@gmail.com

CC:

BCC:

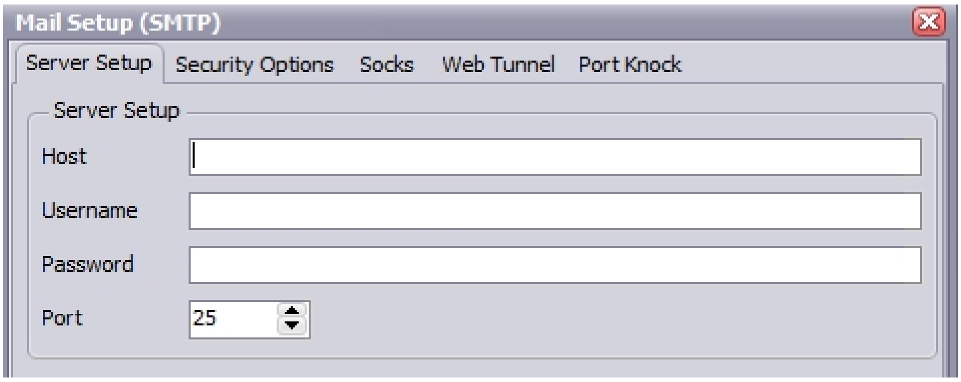
Subject: RTLog Email - %RRN

Body: %LRT:6-0:

□ Include Input File as Attachment

0 Max. Size Attachment in KBytes

Normal Priority



Server Setup

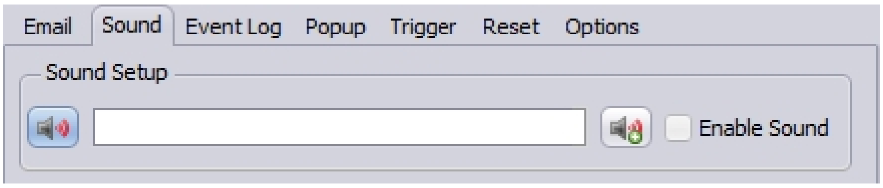
Host

Username

Password

Port 25

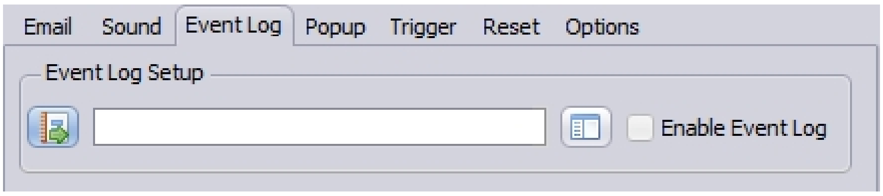
2. Sound



Sound Setup

□ Enable Sound

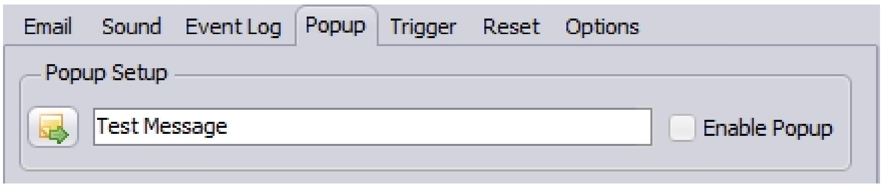
3. Event Log



Event Log Setup

□ Enable Event Log

4. Popup

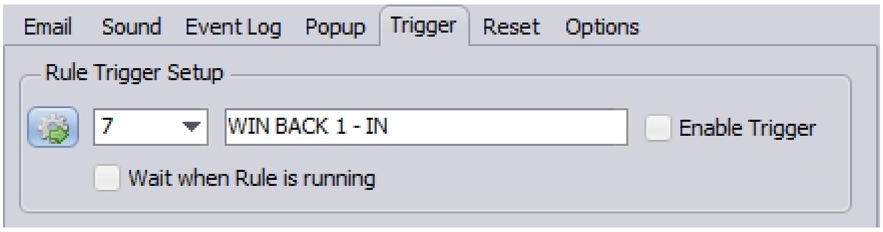


Popup Setup

Test Message

□ Enable Popup

5. Trigger



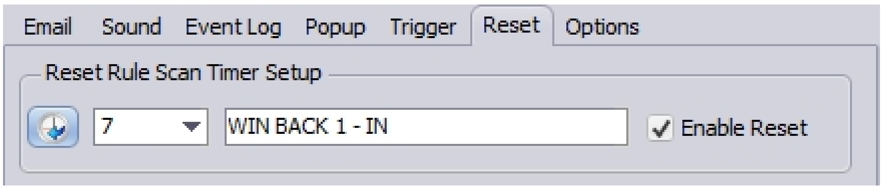
Rule Trigger Setup

7 WIN BACK 1 - IN

□ Enable Trigger

□ Wait when Rule is running

6. Reset

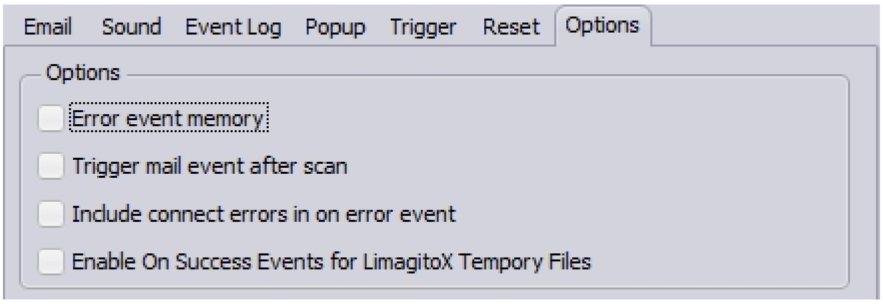


Reset Rule Scan Timer Setup

7 WIN BACK 1 - IN

☑ Enable Reset

7. Options



Options

□ Error event memory

□ Trigger mail event after scan

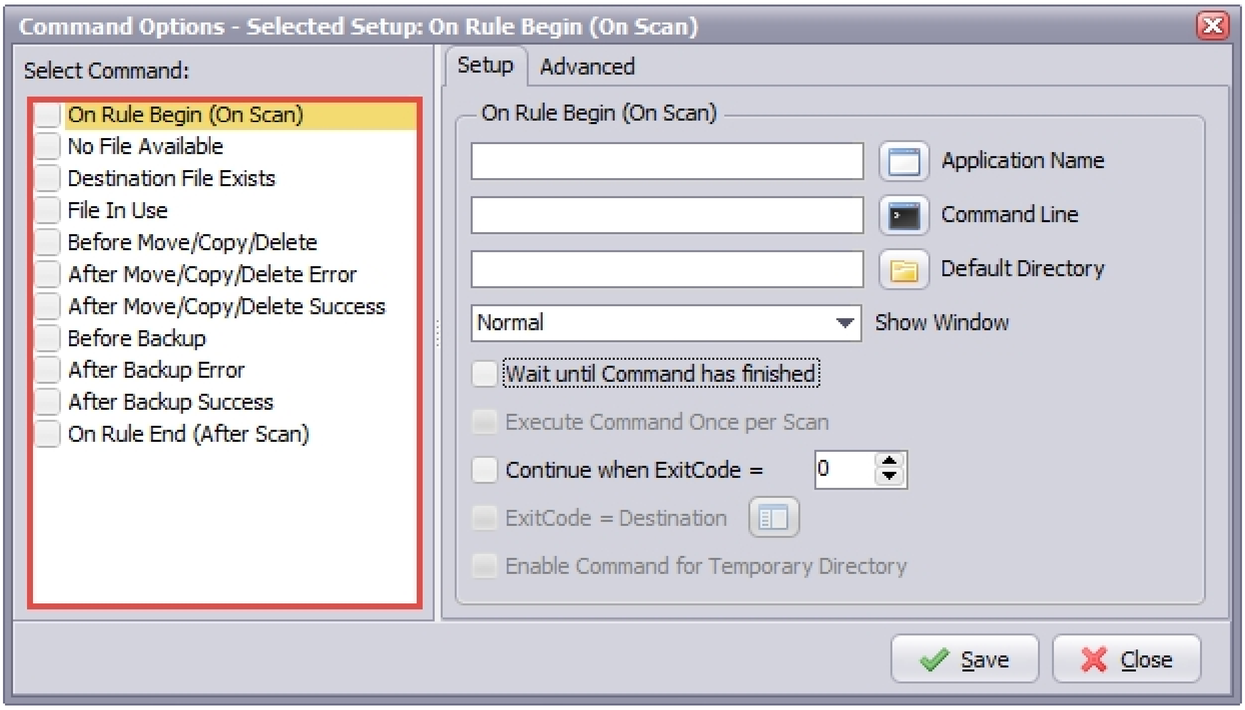
□ Include connect errors in on error event

□ Enable On Success Events for LimagitoX Tempory Files

- 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



Select Command:

□ On Rule Begin (On Scan)
□ No File Available
□ Destination File Exists
□ File In Use
□ Before Move/Copy/Delete
□ After Move/Copy/Delete Error
□ After Move/Copy/Delete Success
□ Before Backup
□ After Backup Error
□ After Backup Success
□ On Rule End (After Scan)

On Rule Begin (On Scan)

Application Name:

Command Line:

Default Directory:

Show Window: Normal

□ Wait until Command has finished

□ Execute Command Once per Scan

□ Continue when ExitCode = 0

□ ExitCode = Destination

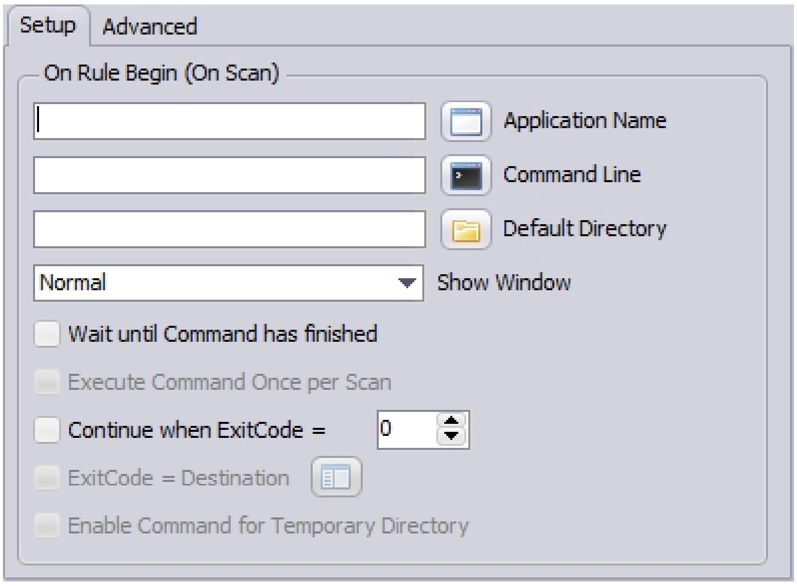
□ Enable Command for Temporary Directory

Use the Command option to execute an external (command line) application at different application events (marked red). Important, each event will use its own Command setup. So select the event on the left and change the setup of the Command on the right. You need to repeat this for every enabled event.

Current supported events:

On Rule Begin (On Scan)	First event when the rule is triggered, sequence is started.
No File Available	
Destination File Exists	
File In Use	
Before Move/Copy/Delete	
After Move/Copy/Delete Error	
After Move/Copy/Delete Success	
Before Backup	
After Backup Error	
After Backup Success	
On Rule End (After Scan)	Last event of the rule sequence.

1. Setup



On Rule Begin (On Scan)

Application Name:

Command Line:

Default Directory:

Show Window: Normal

□ Wait until Command has finished

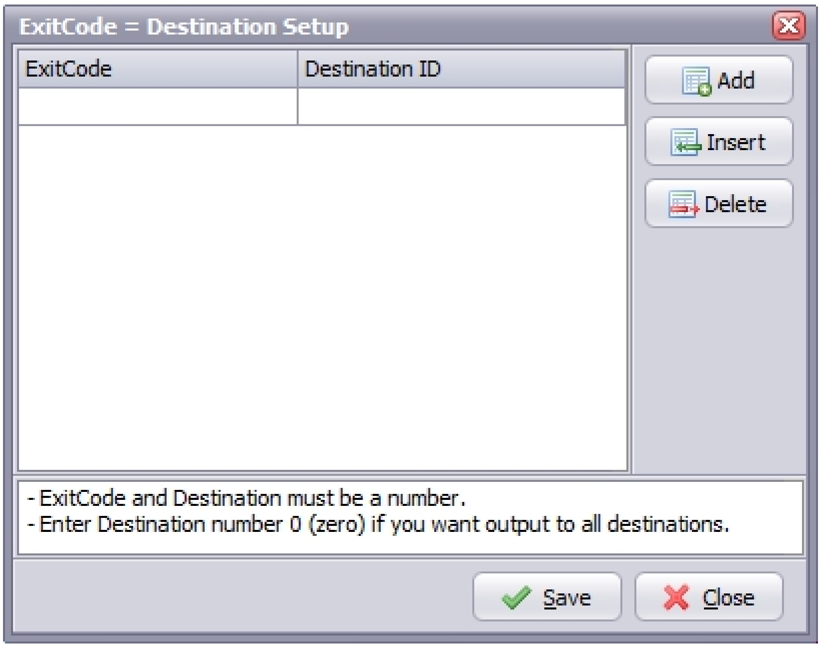
□ Execute Command Once per Scan

□ Continue when ExitCode = 0

□ ExitCode = Destination

□ Enable Command for Temporary Directory

- 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.

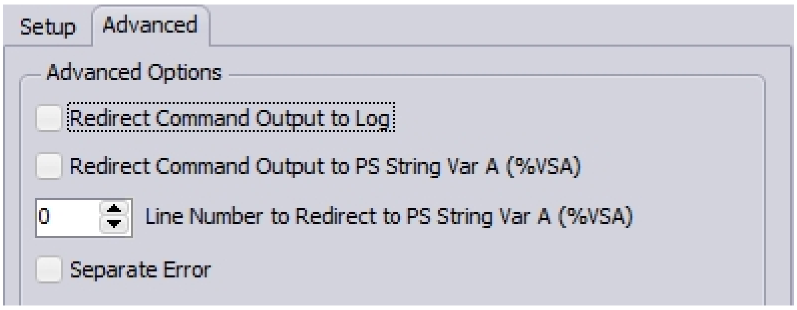


ExitCode = Destination Setup

ExitCode	Destination ID

- ExitCode and Destination must be a number.
- Enter Destination number 0 (zero) if you want output to all destinations.

2. Advanced



Advanced Options

□ Redirect Command Output to Log

□ Redirect Command Output to PS String Var A (%VSA)

0 Line Number to Redirect to PS String Var A (%VSA)

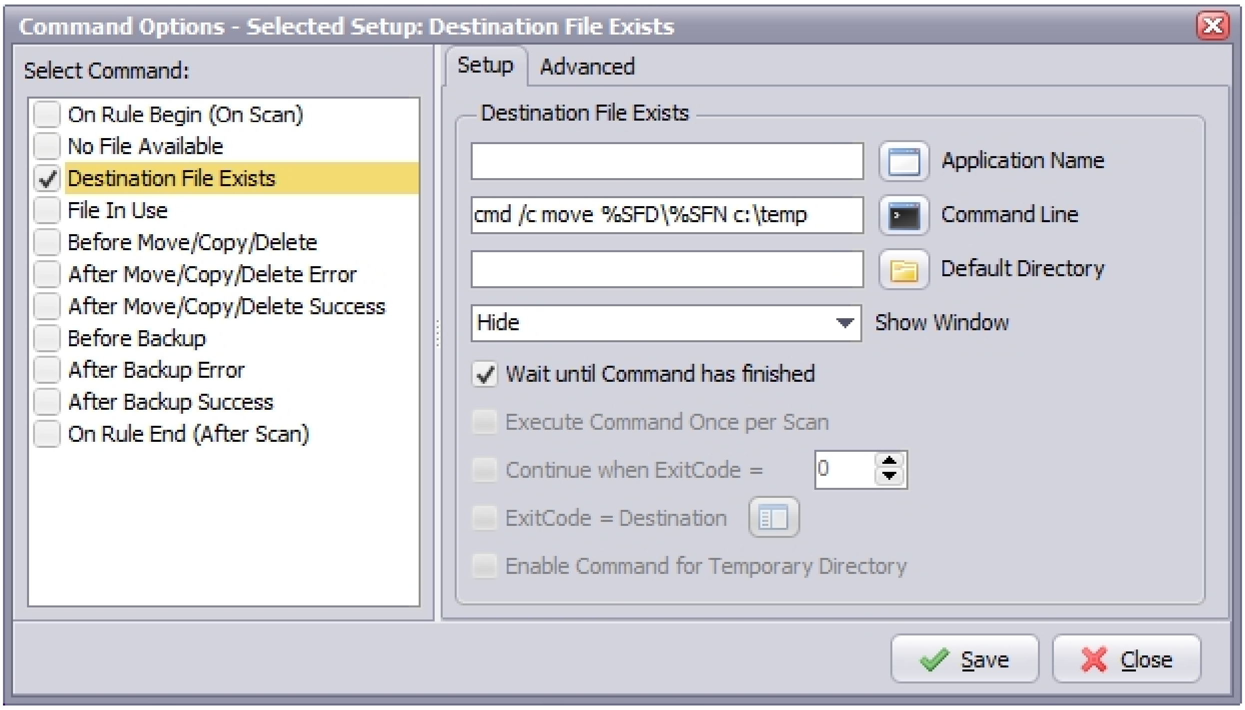
□ Separate Error

- Enable command for temporary directory:

- Redirect Command Output to Log:
- Separate Error:

3. Examples

3.1 First example



Command Options - Selected Setup: Destination File Exists

Select Command:

- □ On Rule Begin (On Scan)
- □ No File Available
- ☑ Destination File Exists
- □ File In Use
- □ Before Move/Copy/Delete
- □ After Move/Copy/Delete Error
- □ After Move/Copy/Delete Success
- □ Before Backup
- □ After Backup Error
- □ After Backup Success
- □ On Rule End (After Scan)

Destination File Exists

	Application Name
cmd /c move %SFD\%SFN c:\temp	Command Line
	Default Directory
Hide	Show Window

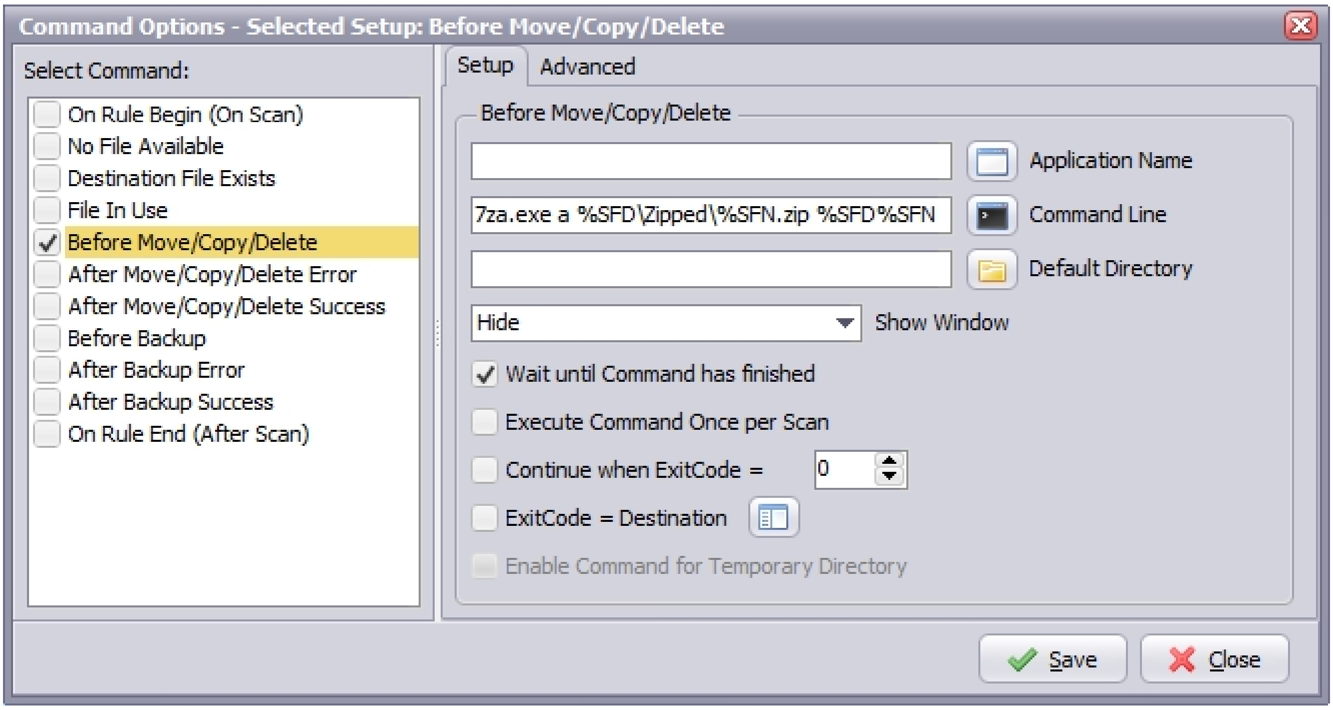
- ☑ Wait until Command has finished
- □ Execute Command Once per Scan
- □ Continue when ExitCode = 0
- □ ExitCode = Destination
- □ Enable Command for Temporary Directory

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)
c:\temp	Destination

3.2 Second example



Select Command:

- □ On Rule Begin (On Scan)
- □ No File Available
- □ Destination File Exists
- □ File In Use
- ☑ Before Move/Copy/Delete
- □ After Move/Copy/Delete Error
- □ After Move/Copy/Delete Success
- □ Before Backup
- □ After Backup Error
- □ After Backup Success
- □ On Rule End (After Scan)

Before Move/Copy/Delete

Application Name:

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

Default Directory:

Show Window: Hide

☑ Wait until Command has finished

□ Execute Command Once per Scan

□ Continue when ExitCode = 0

□ ExitCode = Destination

□ Enable Command for Temporary Directory

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.

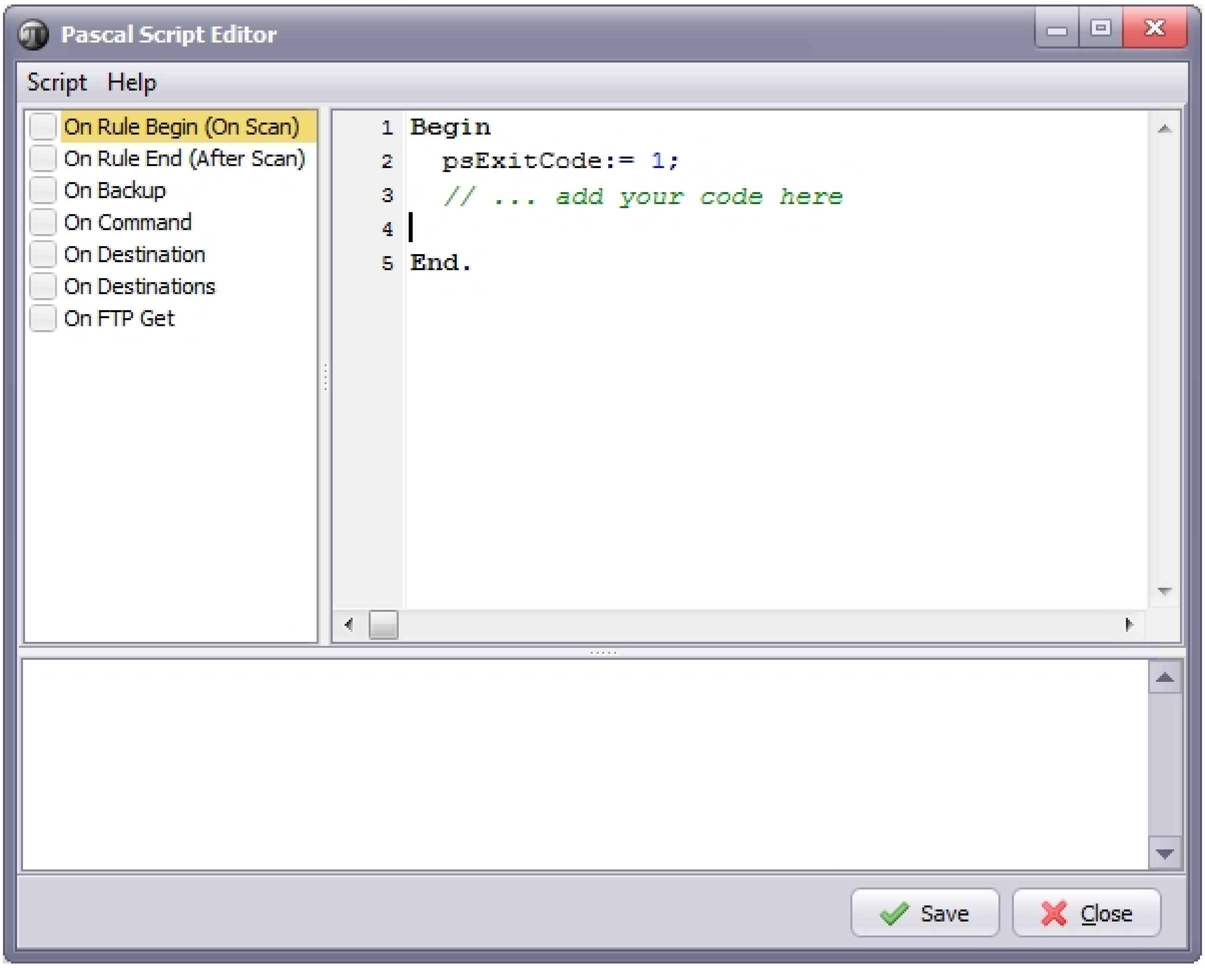
Command: 7za.exe a %SFD\Zipped\%SFN.zip %SFD%SFN

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 extention .zip is added to the original filename.

Pascal Script

Pascal Script



```
Begin
  psExitCode:= 1;
  // ... add your code here

End.
```

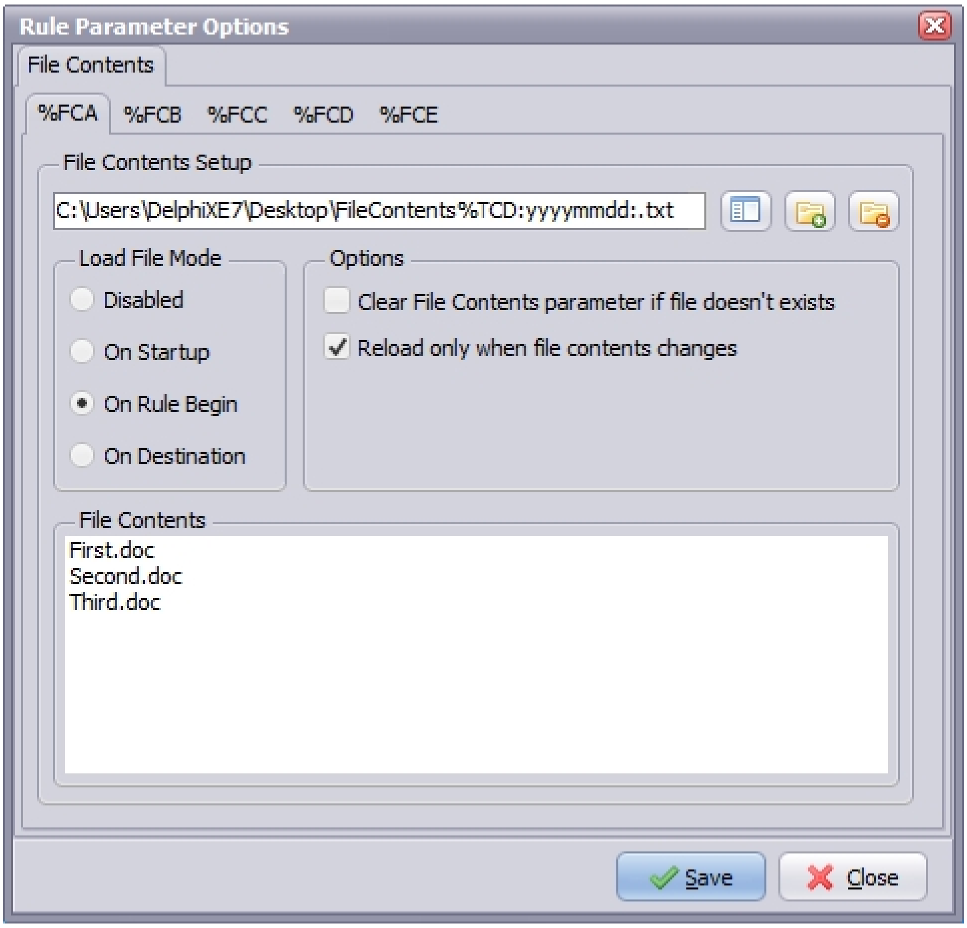
With Pascal Script we (and you as user) can can create customized options. It helps us to create options that are user specific.

▶ psExitCode := 1;	Rule cyclus will continue.
▶ psExitCode := 0;	This will break the rule cyclus. The Script will return an error as result.
▶ psExitCode := -1;	This will break the rule cyclus without returning an error.

Rule Parameters

Rule Parameters

File Contents Parameter



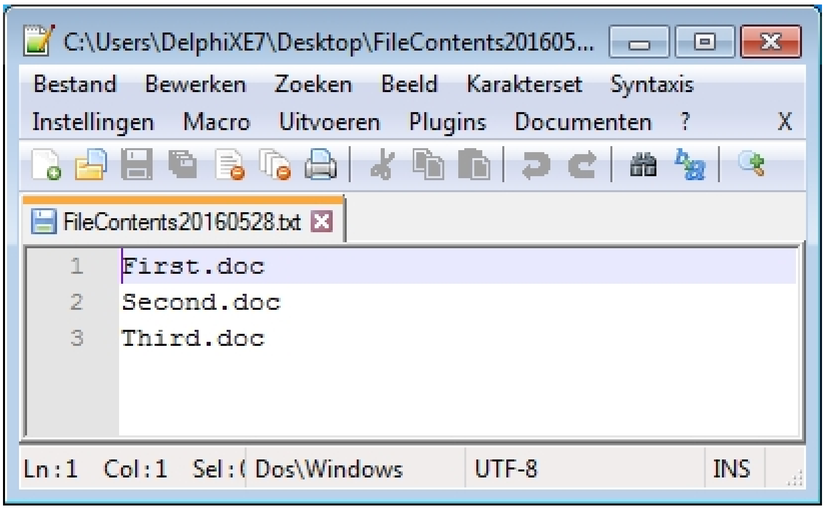
C:\Users\DelphiXE7\Desktop\FileContents%TCD:yyyymmdd:.txt

Load File Mode
- ○ Disabled
- ○ On Startup
- ● On Rule Begin
- ○ On Destination

Options
- □ Clear File Contents parameter if file doesn't exists
- ☑ Reload only when file contents changes

File Contents

```
First.doc
Second.doc
Third.doc
```

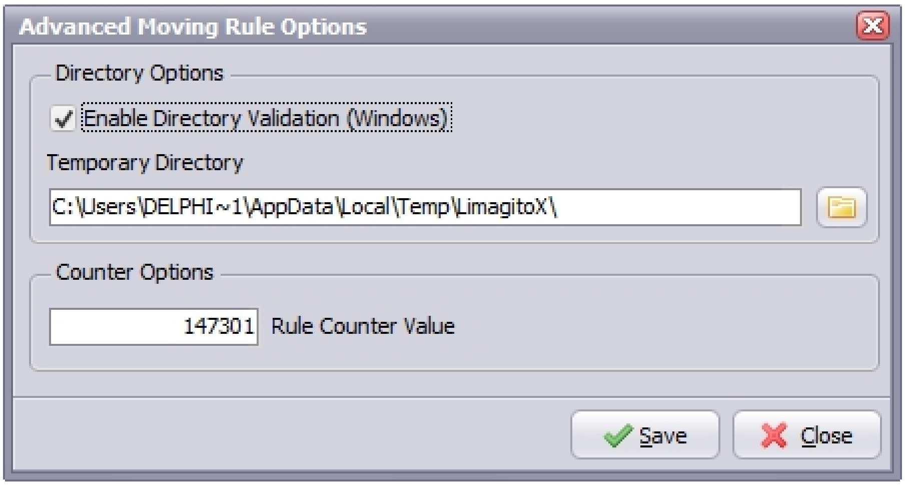


```
First.doc
Second.doc
Third.doc
```

These Rule Parameters you be used throughout the application. We've also added an extra file filter option called 'File Contents Filter'. This filter is used together with the File Contents parameters.

Advanced

Advanced



Directory Options

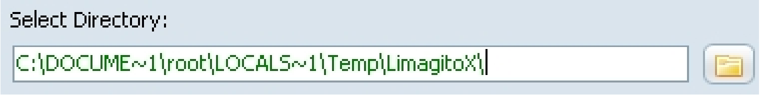
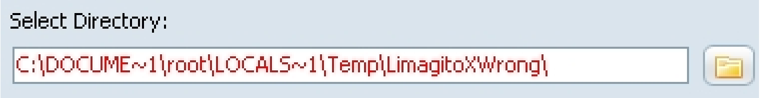
☑ Enable Directory Validation (Windows)

Temporary Directory

C:\Users\DELPHI~1\AppData\Local\Temp\LimagitoX\

Counter Options

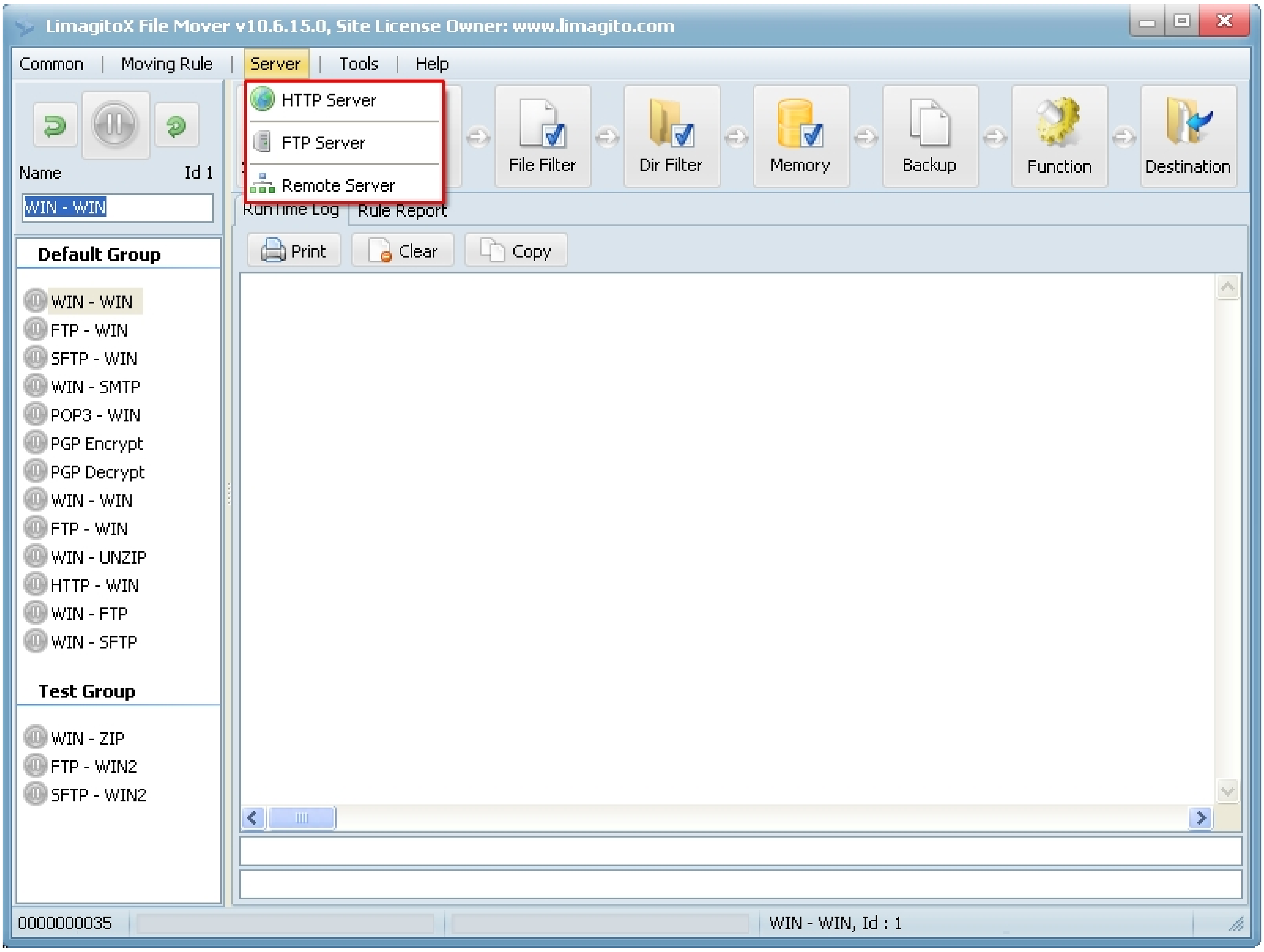
147301 Rule Counter Value

- Enable Directory Validation (Windows): When a selected directory is valid the font color will be green, when not the font color will be red.
  - 
    Select Directory:
    C:\DOCUME~1\root\LOCALS~1\Temp\LimagitoX\
  - 
    Select Directory:
    C:\DOCUME~1\root\LOCALS~1\Temp\LimagitoXWrong\
- 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

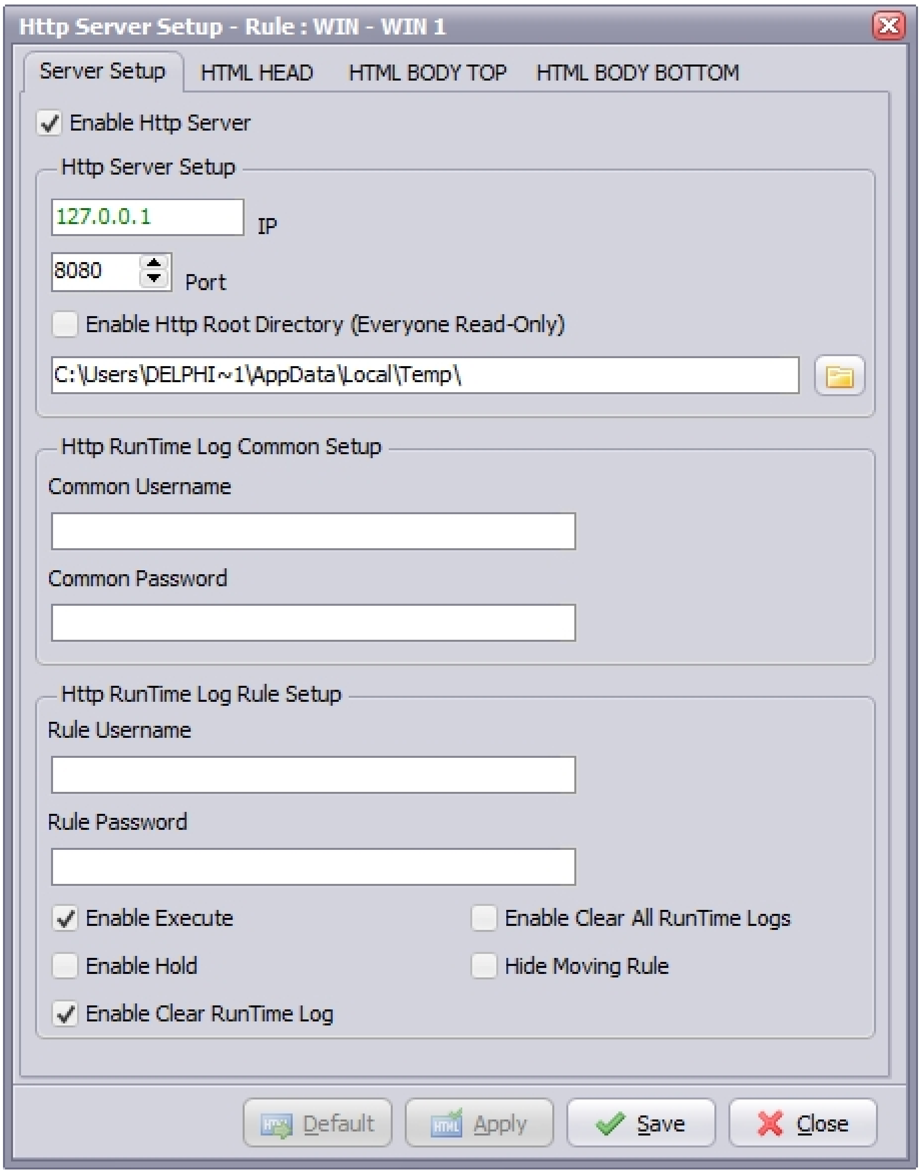
- HTTP Server
- FTP Server
- Remote Server



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 1

Server Setup | HTML HEAD | HTML BODY TOP | HTML BODY BOTTOM

☑ Enable Http Server

Http Server Setup

IP: 127.0.0.1

Port: 8080

☐ Enable Http Root Directory (Everyone Read-Only)

C:\Users\DELPHI~1\AppData\Local\Temp\

Http RunTime Log Common Setup

Common Username

Common Password

Http RunTime Log Rule Setup

Rule Username

Rule Password

☑ Enable Execute

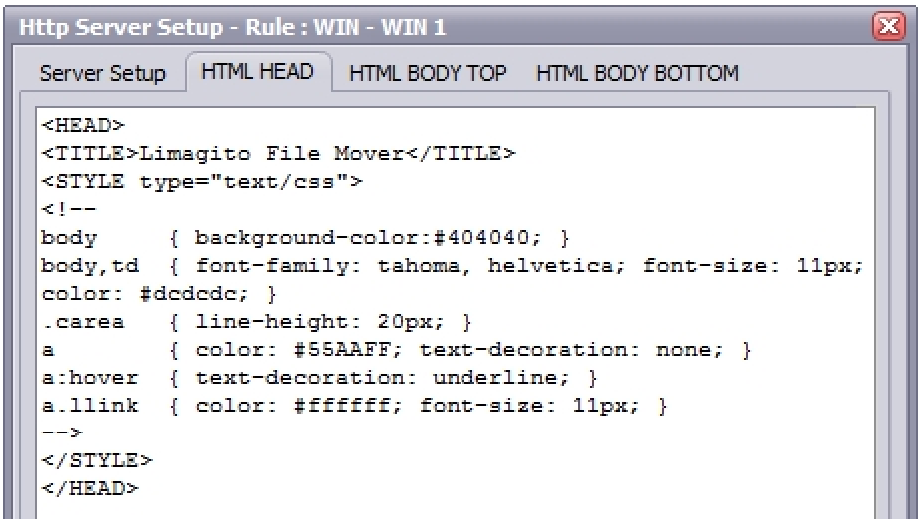
☐ Enable Clear All RunTime Logs

☐ Enable Hold

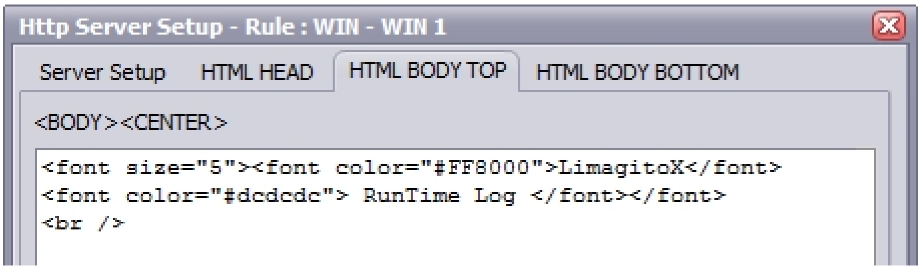
☐ Hide Moving Rule

☑ Enable Clear RunTime Log

- 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.
- Enable Clear RunTime log
- Enabke Clear All RunTime Logs
- Hide Moving Rule

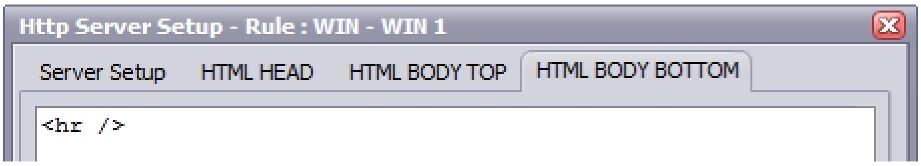


```
<HEAD>
<TITLE>Limagito File Mover</TITLE>
<STYLE type="text/css">
<!--
body     { background-color:#404040; }
body,td  { font-family: tahoma, helvetica; font-size: 11px;
color: #dcdcdc; }
.carea   { line-height: 20px; }
a        { color: #55AAFF; text-decoration: none; }
a:hover  { text-decoration: underline; }
a.llink  { color: #ffffff; font-size: 11px; }
-->
</STYLE>
</HEAD>
```

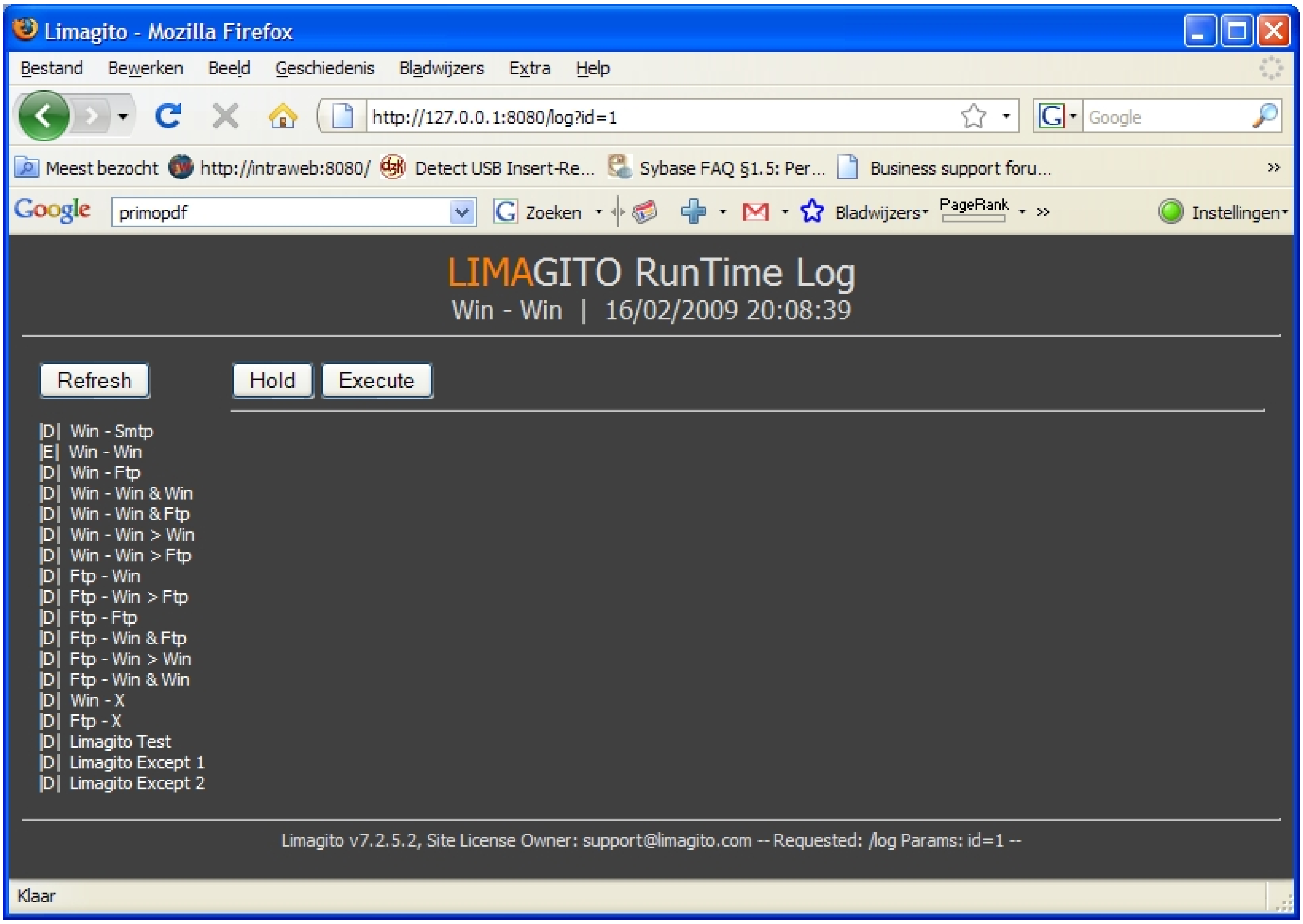


<BODY><CENTER>

```
<font size="5"><font color="#FF8000">LimagitoX</font>
<font color="#dcdcdc"> RunTime Log </font></font>
<br />
```



```
<hr />
```



LIMAGITO RunTime Log

Win - Win | 16/02/2009 20:08:39

```
|D| Win - Smtp
|E| Win - Win
|D| Win - Ftp
|D| Win - Win & Win
|D| Win - Win & Ftp
|D| Win - Win > Win
|D| Win - Win > Ftp
|D| Ftp - Win
|D| Ftp - Win > Ftp
|D| Ftp - Ftp
|D| Ftp - Win & Ftp
|D| Ftp - Win > Win
|D| Ftp - Win & Win
|D| Win - X
|D| Ftp - X
|D| Limagito Test
|D| Limagito Except 1
|D| Limagito Except 2
```

Limagito v7.2.5.2, Site License Owner: support@limagito.com -- Requested: /log Params: id=1 --

FTP Server

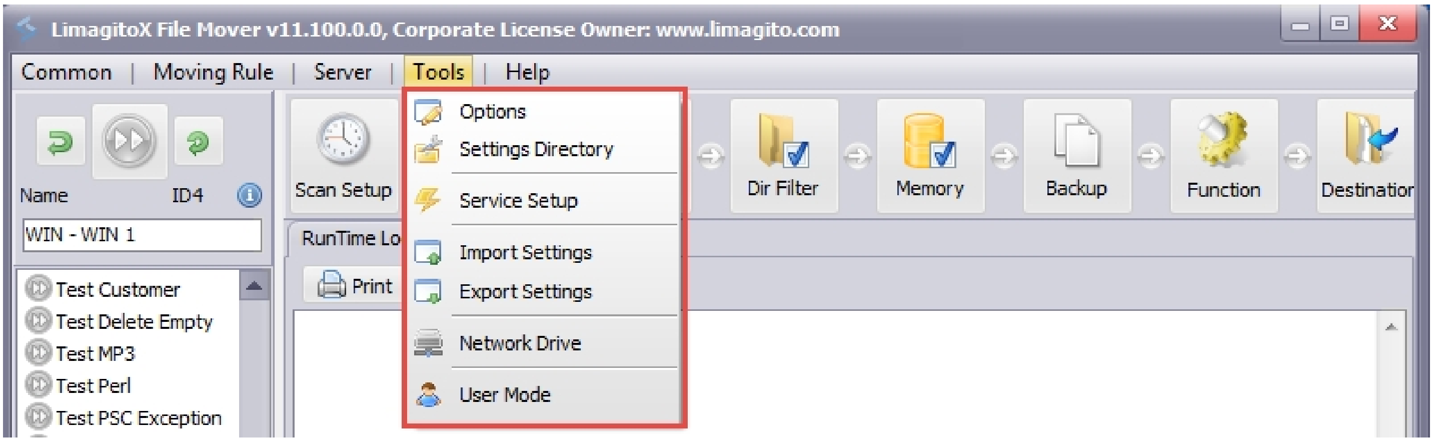
FTP Server

FTP Server is obsolete. Will be remove in the next version of LimagitoX.

Application Options

Tools

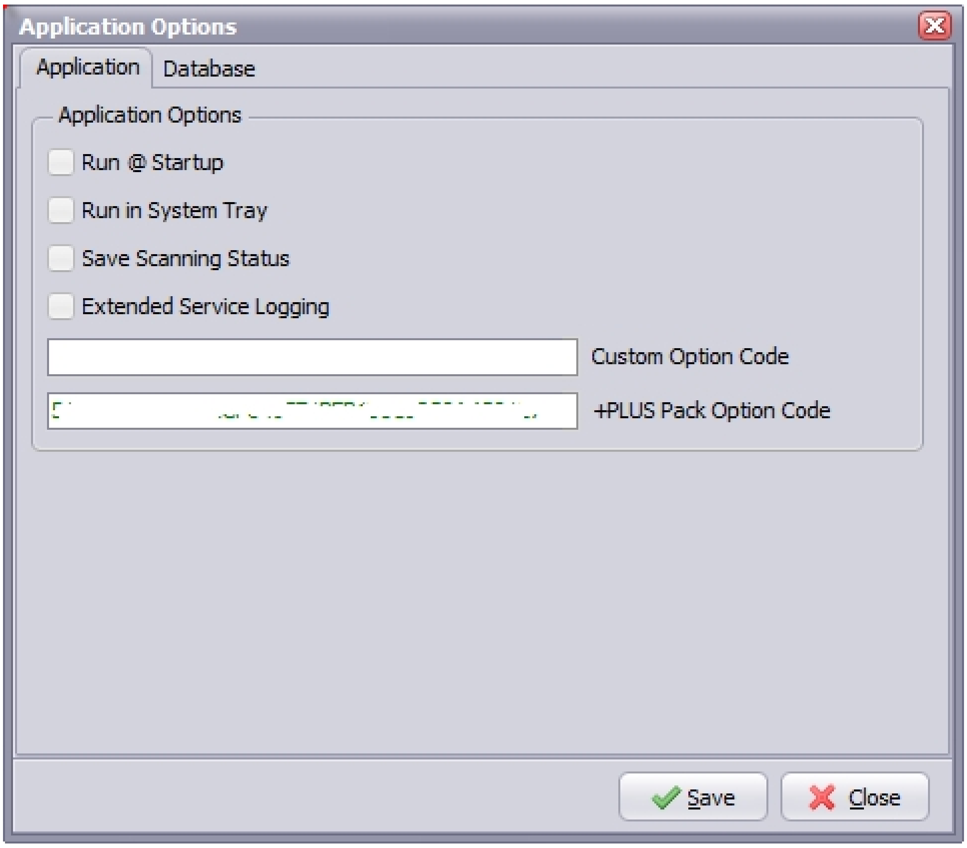
- Options
- Settings Directory
- Service Setup
- Import Settings
- Export Settings
- Network Drive
- User Mode



Options

Options

1. Application


Application Options

Application | Database

Application Options

☐ Run @ Startup

☐ Run in System Tray

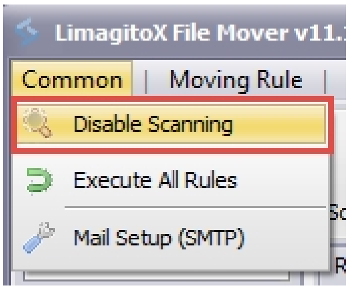
☐ Save Scanning Status

☐ Extended Service Logging

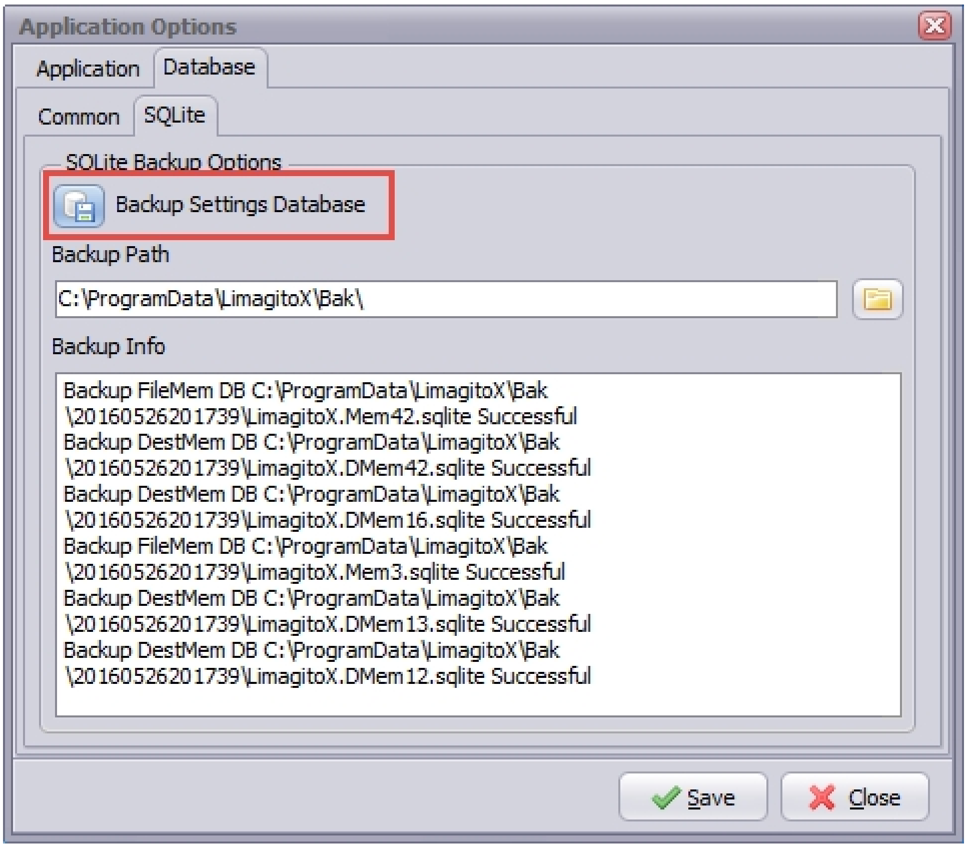
Custom Option Code

+PLUS Pack Option Code

- 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.



2. Database



Backup Path: C:\ProgramData\LimagitoX\Bak\

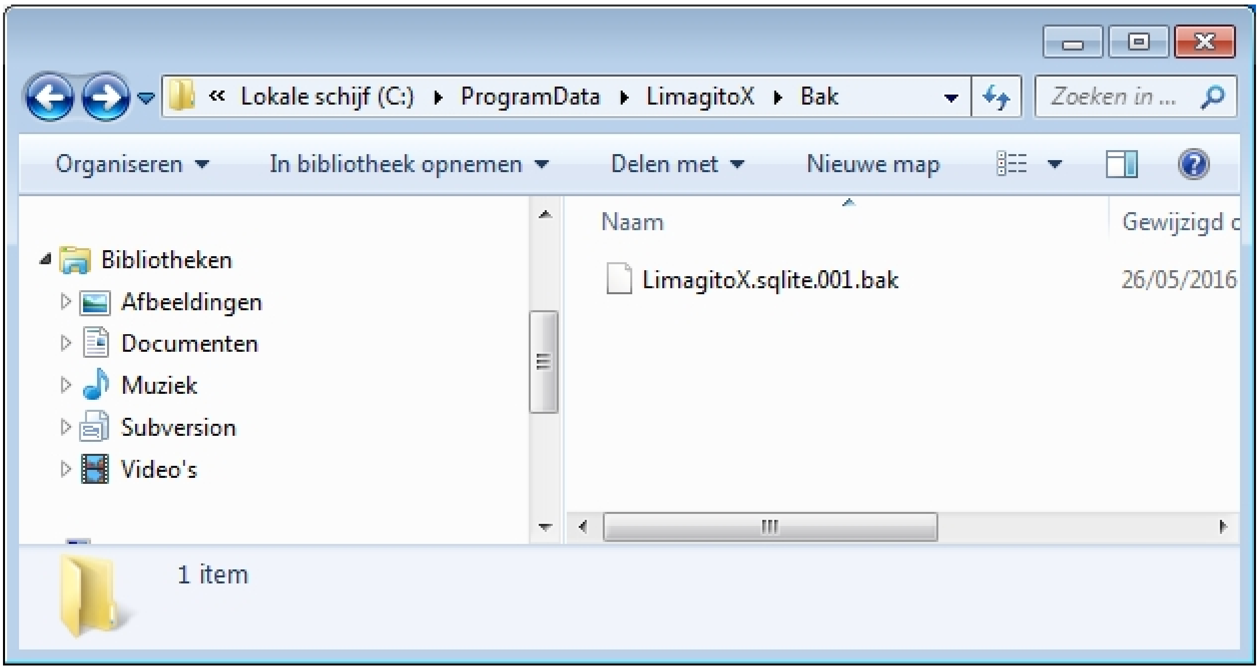
```
Backup FileMem DB C:\ProgramData\LimagitoX\Bak
\20160526201739\LimagitoX.Mem42.sqlite Successful
Backup DestMem DB C:\ProgramData\LimagitoX\Bak
\20160526201739\LimagitoX.DMem42.sqlite Successful
Backup DestMem DB C:\ProgramData\LimagitoX\Bak
\20160526201739\LimagitoX.DMem16.sqlite Successful
Backup FileMem DB C:\ProgramData\LimagitoX\Bak
\20160526201739\LimagitoX.Mem3.sqlite Successful
Backup DestMem DB C:\ProgramData\LimagitoX\Bak
\20160526201739\LimagitoX.DMem13.sqlite Successful
Backup DestMem DB C:\ProgramData\LimagitoX\Bak
\20160526201739\LimagitoX.DMem12.sqlite Successful
```

- Backup Settings Database: A manual option to backup the settings database.
- Backup Path: Folder where the files of the manual database backup will be stored.
- Backup Info: Information about the files that are copied during the backup.

Settings Directory

Settings Directory

- Use the 'Settings Directory' option to find where LimagitoX FileMover stores it's 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 : Will contains up to 7 backups of "LimagitoX.sqlite". This is done automatically. Limagito.sqlite contains most settings of LimagitoX.exe (application and service version).



LimagitoX.sqlite.001.bak 26/05/2016

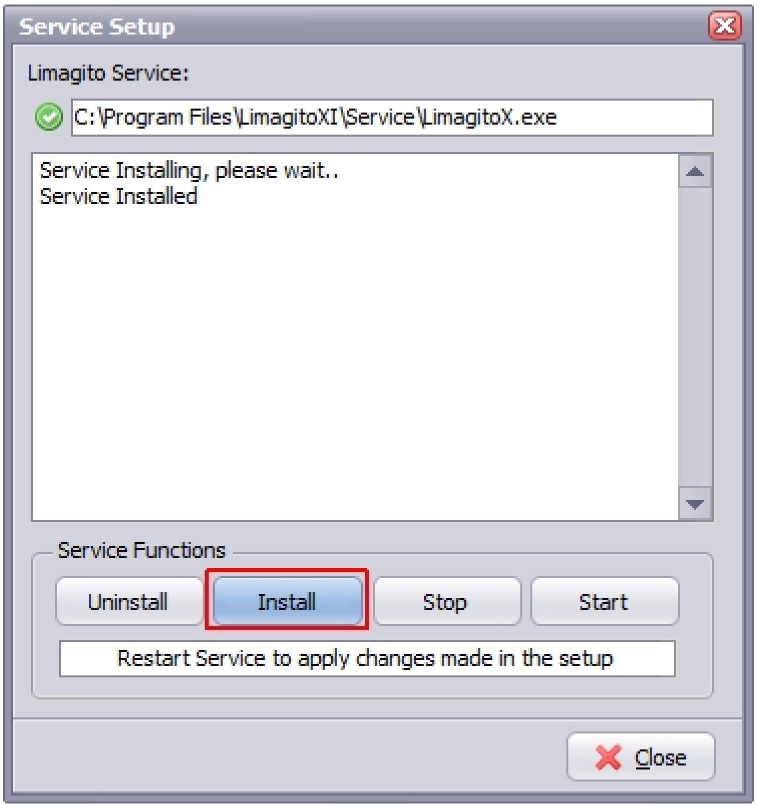
- \LOG : Default Log Directory of LimagitoX File Mover.

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.

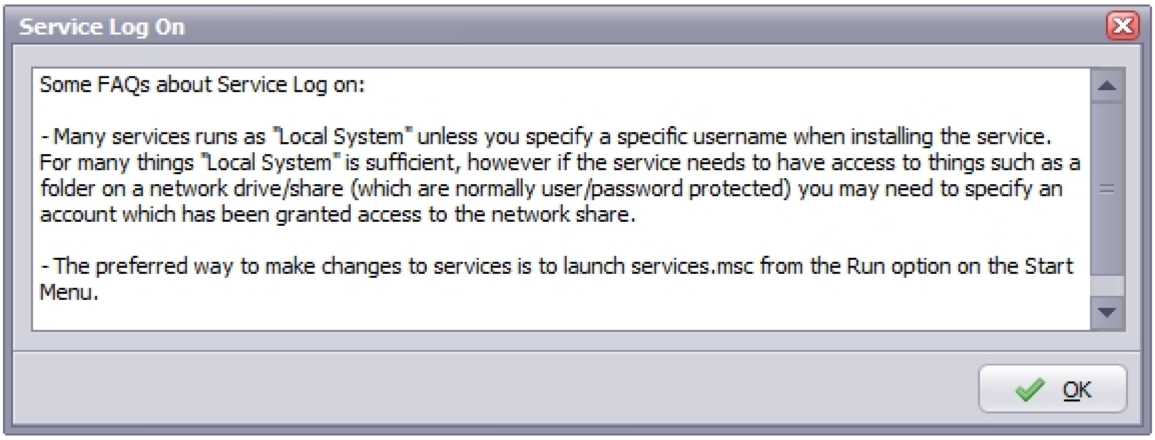


C:\Program Files\LimagitoXI\Service\LimagitoX.exe

```
Service Installing, please wait..
Service Installed
```

Restart Service to apply changes made in the setup

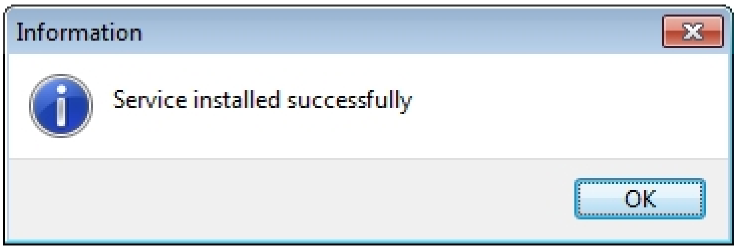
"Please read the following information carefully"



Some FAQs about Service Log on:

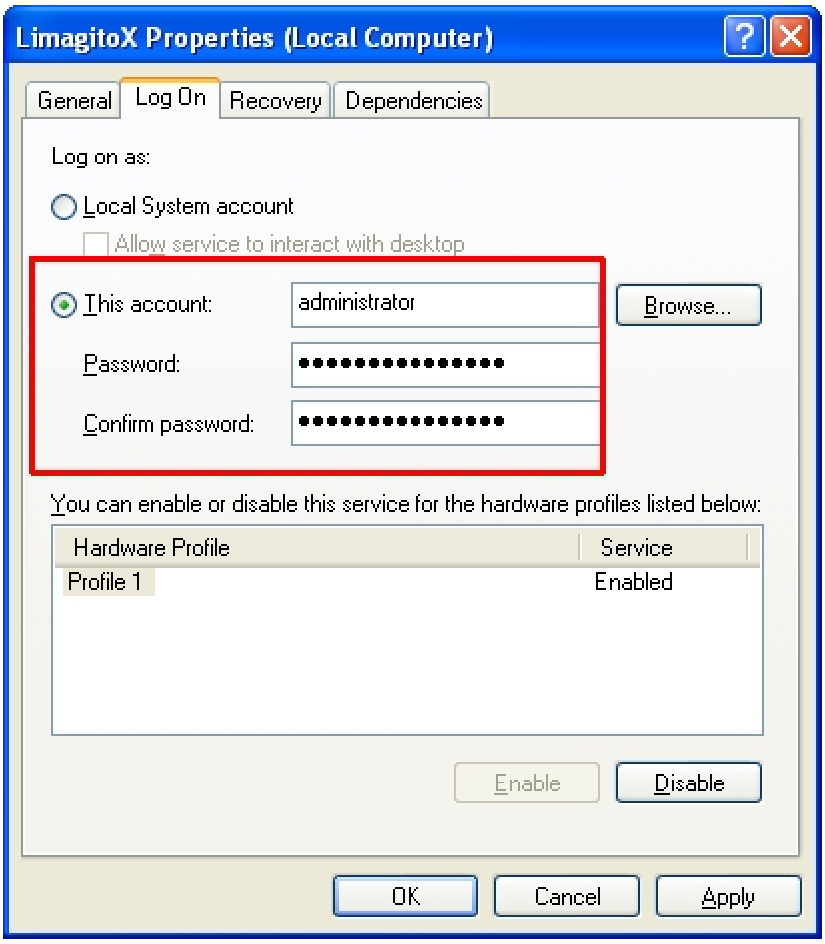
- Many services runs as "Local System" unless you specify a specific username when installing the service. For many things "Local System" is sufficient, however if the service needs to have access to things such as a folder on a network drive/share (which are normally user/password protected) you may need to specify an account which has been granted access to the network share.

- The preferred way to make changes to services is to launch services.msc from the Run option on the Start Menu.



Service installed successfully

Adjust the "Log on as" account settings:



Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: administrator

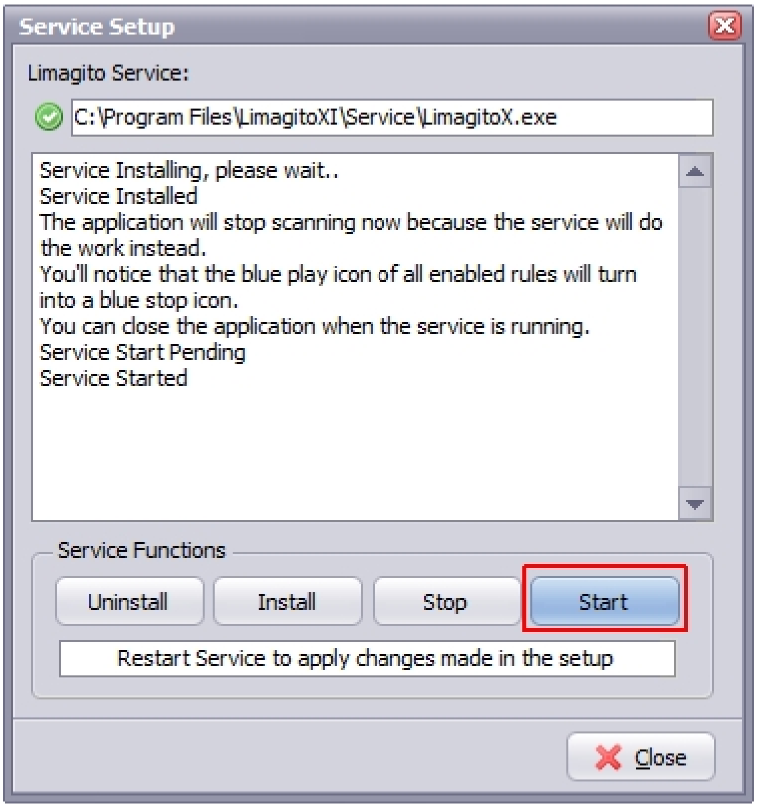
Password: ●●●●●●●●●●●●●●●

Confirm password: ●●●●●●●●●●●●●●●

You can enable or disable this service for the hardware profiles listed below:

Hardware Profile	Service
Profile 1	Enabled

Start the LimagitoX service:


Service Setup

Limagito Service:

C:\Program Files\LimagitoXI\Service\LimagitoX.exe

```
Service Installing, please wait..
Service Installed
The application will stop scanning now because the service will do
the work instead.
You'll notice that the blue play icon of all enabled rules will turn
into a blue stop icon.
You can close the application when the service is running.
Service Start Pending
Service Started
```

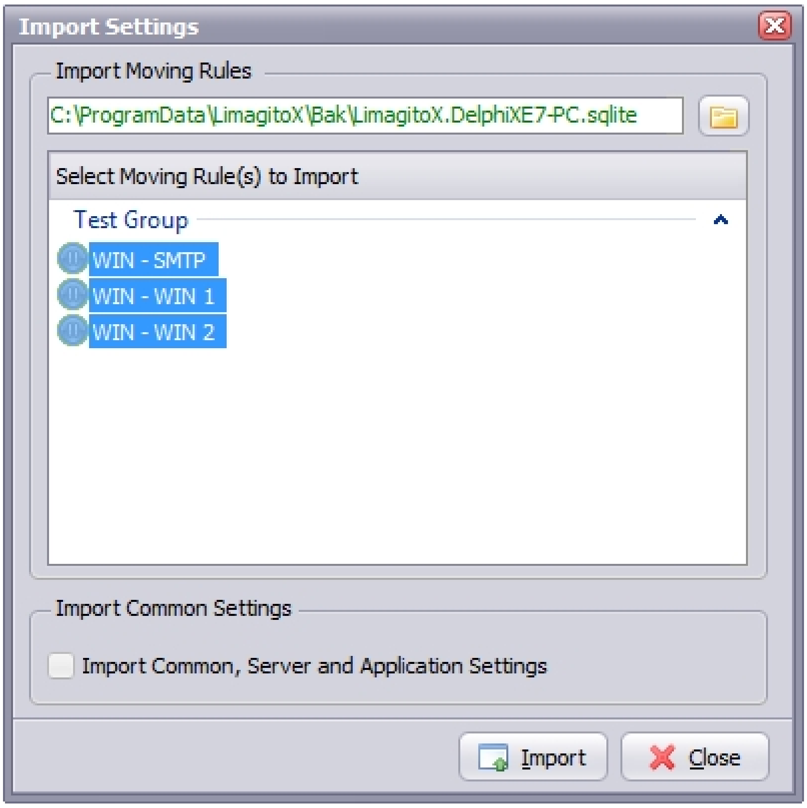
Service Functions

Restart Service to apply changes made in the setup

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

Import Settings

Import Settings


Import Settings

Import Moving Rules

C:\ProgramData\LimagitoX\Bak\LimagitoX.DelphiXE7-PC.sqlite

Select Moving Rule(s) to Import

Test Group

- WIN - SMTP
- WIN - WIN 1
- WIN - WIN 2

Import Common Settings

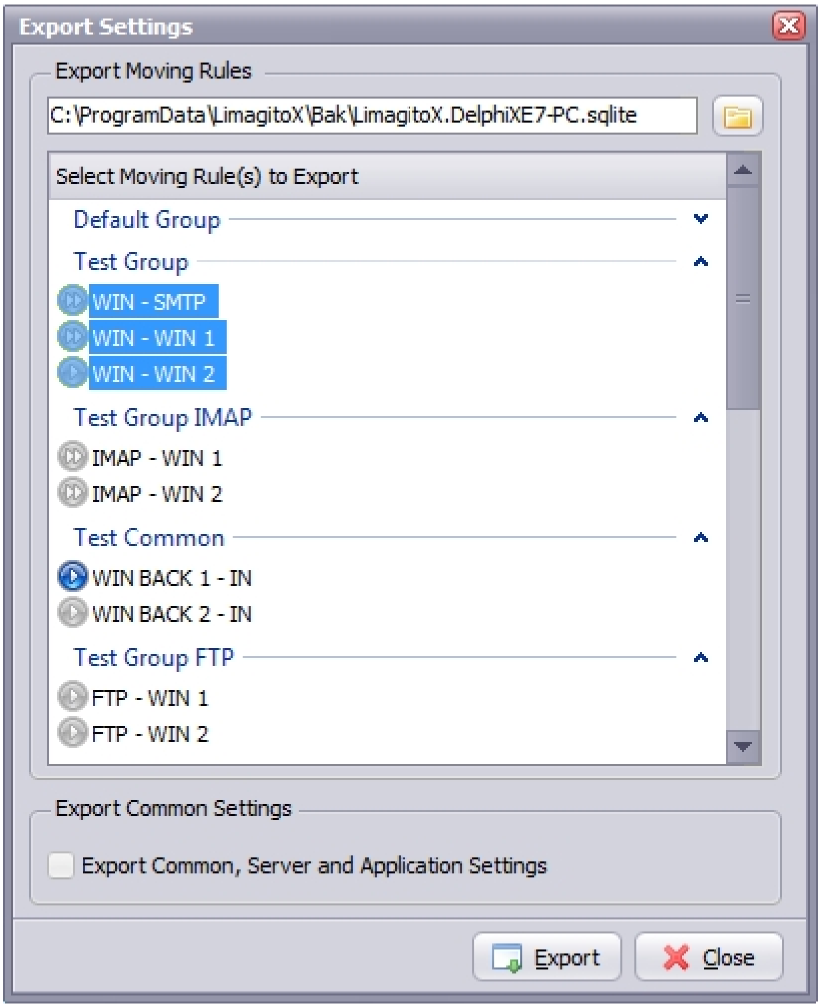
□ Import Common, Server and Application Settings

1. Select the moving rule export file (.sqlite).
2. Select the moving rules you want to import.
3. Select if you want to import the common, server and application too (if they exist in the export .sqlite file).

4. Click on 'Import' button.
5. Done.

Export Settings

Export Settings



Export Settings

Export Moving Rules

C:\ProgramData\LimagitoX\Bak\LimagitoX.DelphiXE7-PC.sqlite

Select Moving Rule(s) to Export

Default Group

Test Group

WIN - SMTP

WIN - WIN 1

WIN - WIN 2

Test Group IMAP

IMAP - WIN 1

IMAP - WIN 2

Test Common

WIN BACK 1 - IN

WIN BACK 2 - IN

Test Group FTP

FTP - WIN 1

FTP - WIN 2

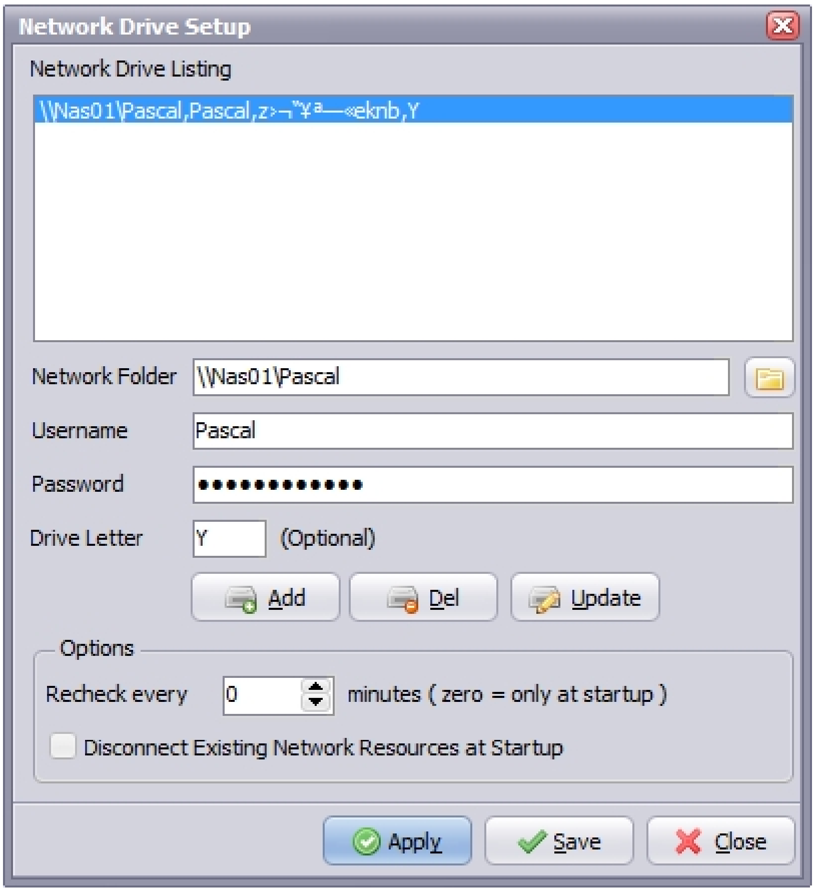
Export Common Settings

□ Export Common, Server and Application Settings

1. Select the directory where you want to put the export file.
2. Select the moving rules you want to export.
3. Enable 'Export Common, Server and Application Settings' if you also want to export common, server and application options.
4. Click on 'Export' button.
5. Done.

Network Drive

Network Drive



Network Drive Setup

Network Drive Listing

\\Nas01\Pascal,Pascal,z›¬˜¥ª—«eknb,Y

Network Folder \\Nas01\Pascal

Username Pascal

Password ●●●●●●●●●●●●

Drive Letter Y (Optional)

Options

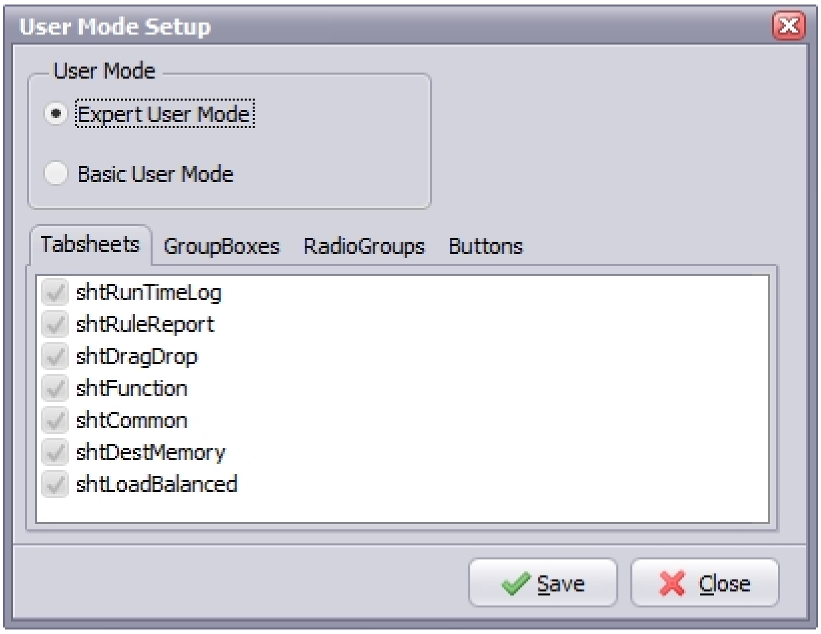
Recheck every 0 minutes (zero = only at startup)

□ Disconnect Existing Network Resources at Startup

- 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)
- Disconnect Existing Network Resource at Startup: When LimagitoX is started it will first disconnect existing resources before connecting to the Network Drives.

User Mode

User Mode



User Mode Setup

User Mode

● Expert User Mode

○ Basic User Mode

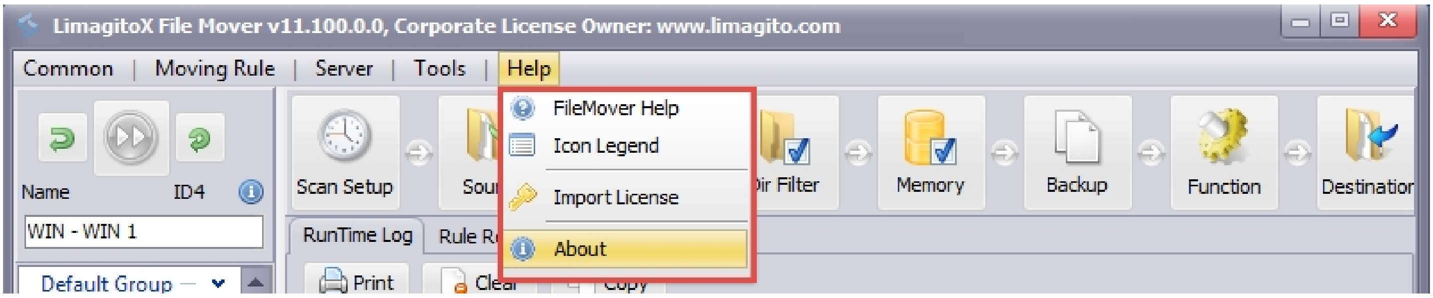
☑ shtRunTimeLog
☑ shtRuleReport
☑ shtDragDrop
☑ shtFunction
☑ shtCommon
☑ shtDestMemory
☑ shtLoadBalanced

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

- Expert User Mode, All enabled (= default)
- Basic User Mode, Adjustible setup

Help Options

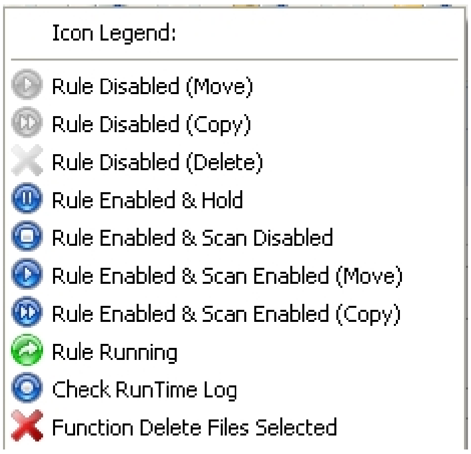
Help Options



FileMover Help

Open LimagitoX help file (help.chm).

Icon Legend

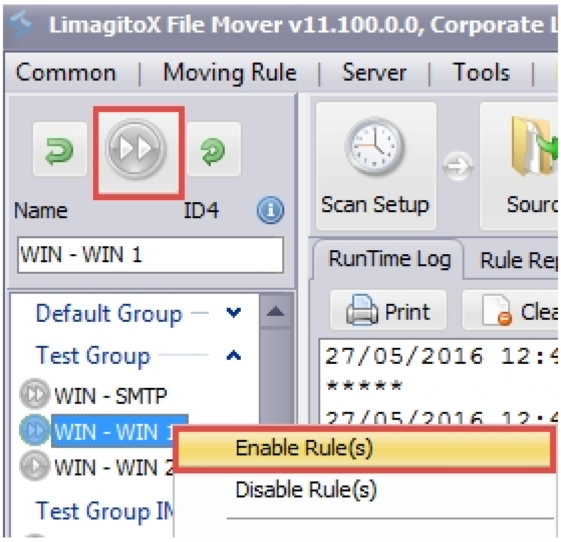


Icon Legend:

- Rule Disabled (Move)
- Rule Disabled (Copy)
- Rule Disabled (Delete)
- Rule Enabled & Hold
- Rule Enabled & Scan Disabled
- Rule Enabled & Scan Enabled (Move)
- Rule Enabled & Scan Enabled (Copy)
- Rule Running
- Check RunTime Log
- Function Delete Files Selected

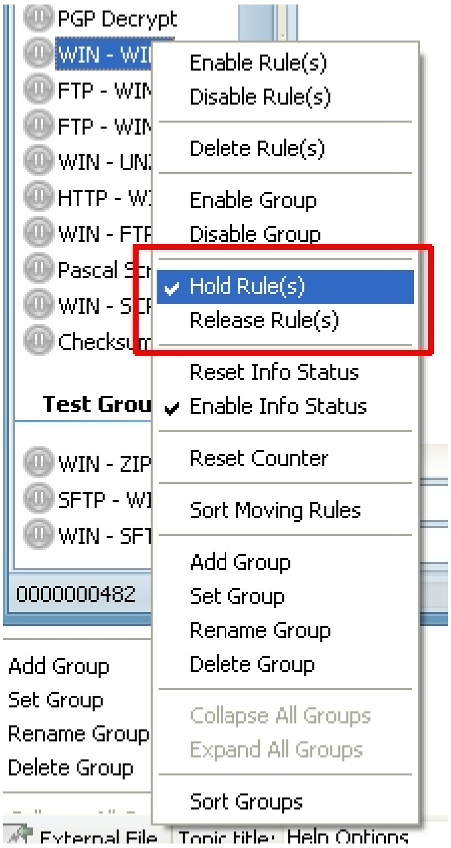
Possible Moving Rule status.

- 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.



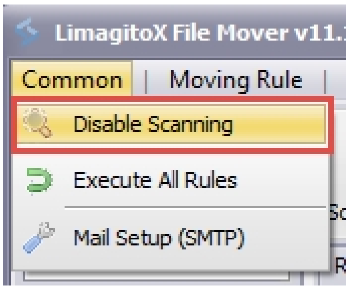
27/05/2016 12:4
*****
27/05/2016 12:4

- Rule Enabled & Hold. The rule is enabled but in Hold status. An enabled rule can be put in hold or release status. This can de 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.



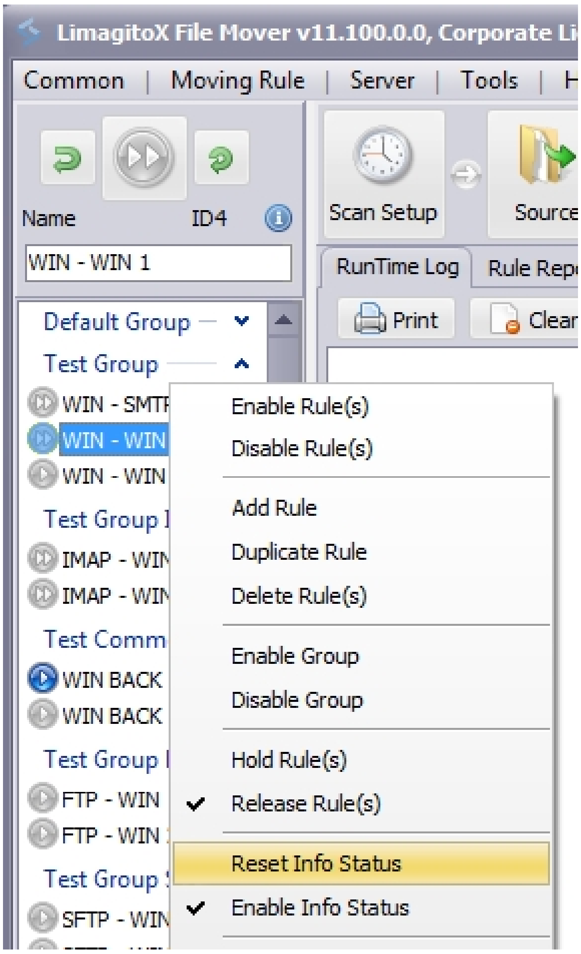
2. When you start the LimagitoX application and the LimagitoX service is running then the rules in the application version will automatically go into this status. They will only accept manual triggers. We don't want the application version to interfere with the running LimagitoX service.

- Rule Enabled & Time Schedule. No longer used, obsolete.

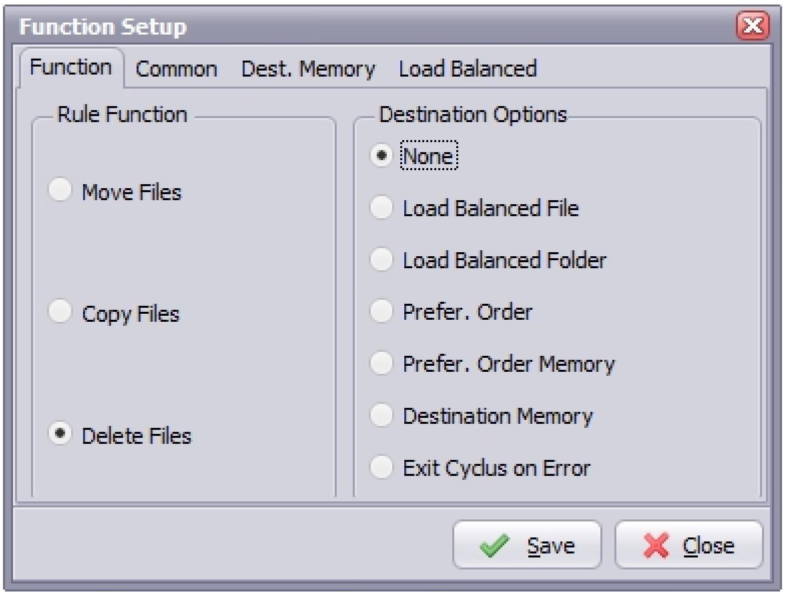
- Rule Enabled & Scan Enabled. In this status the rule will accept scan triggers. It's ready to run.

- 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.



Function Setup

Rule Function

○ Move Files

○ Copy Files

● Delete Files

Destination Options

● None

○ Load Balanced File

○ Load Balanced Folder

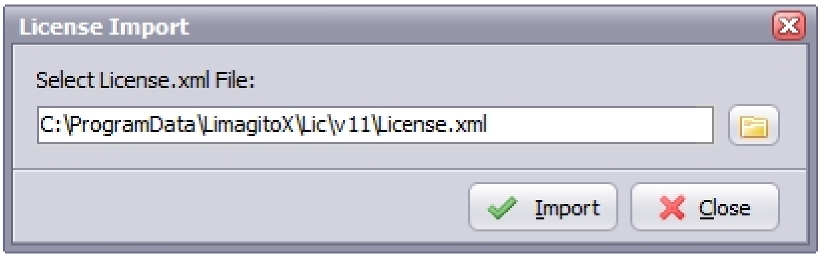
○ Prefer. Order

○ Prefer. Order Memory

○ Destination Memory

○ Exit Cyclus on Error

Import License



License Import

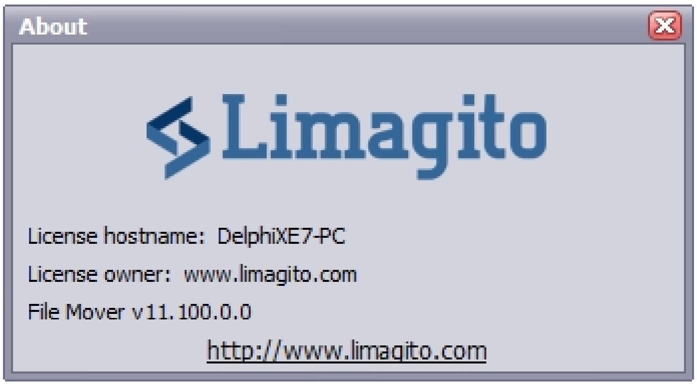
Select License.xml File:

C:\ProgramData\LimagitoX\Lic\v11\License.xml

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.



About

License hostname: DelphiXE7-PC

License owner: www.limagito.com

File Mover v11.100.0.0

http://www.limagito.com

Rule Setup

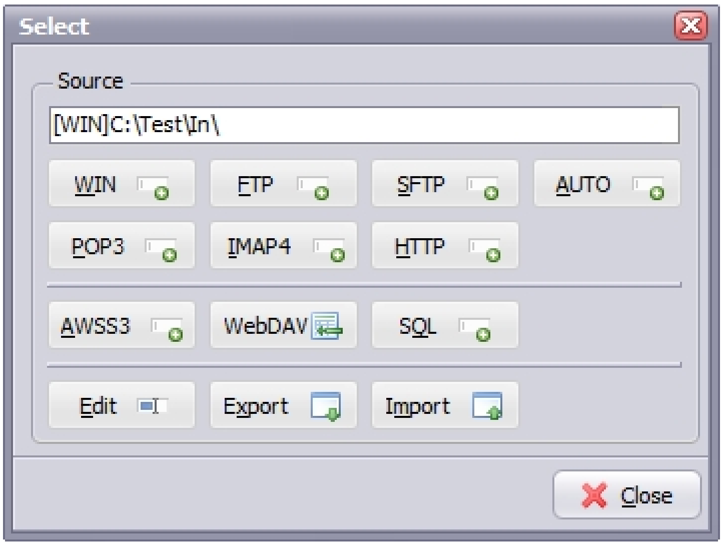
Rule Setup

- Source
- File Filter
- Dir Filter

- Memory
- Backup
- Function
- Destination

Source Options

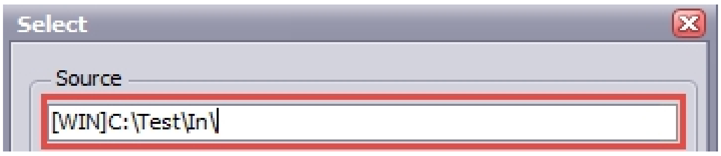
Source Selection



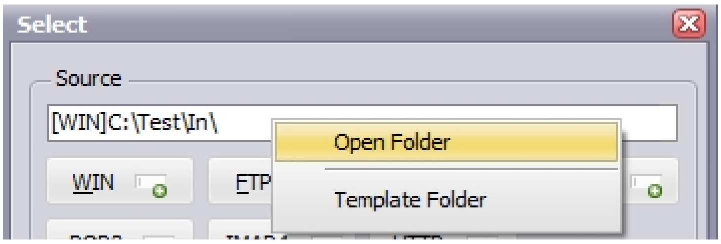
LimagitoX Source possibilities:

- WIN
- FTP
- SFTP
- AUTO
- POP3
- IMAP4
- HTTP
- AWSS3
- WebDAV
- SQL

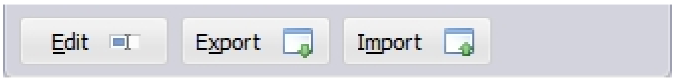
AWSS3, WebDAV and SQL are part of the +PLUS Option Pack License. All three are available in the Free Lite version so they can be fully evaluated before purchasing.

- 

Double click on the selected source to open its current setup screen.

- 

Right click on the selected source to:
  - Open and explore the source folder (WIN, FTP, SFTP)
  - Open and explore the template folder (Export Folder)

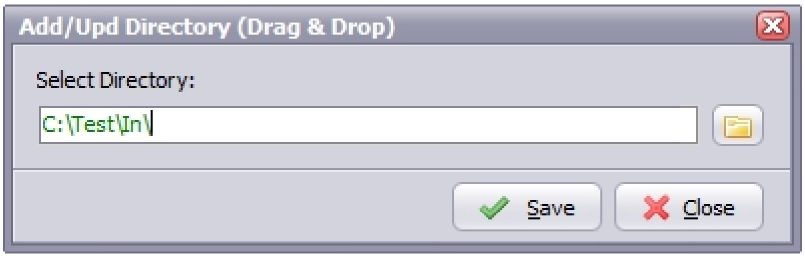


- Select 'Edit' to open the setup screen of the current Source.
- Select 'Export' to export the setup of the current Source (template as ini file).
- Select 'Import' to replace the current Source setup using an ini template file.

WIN Source

WIN Source Setup

Add / Update WIN as Source.



Select Directory: C:\Test\In\

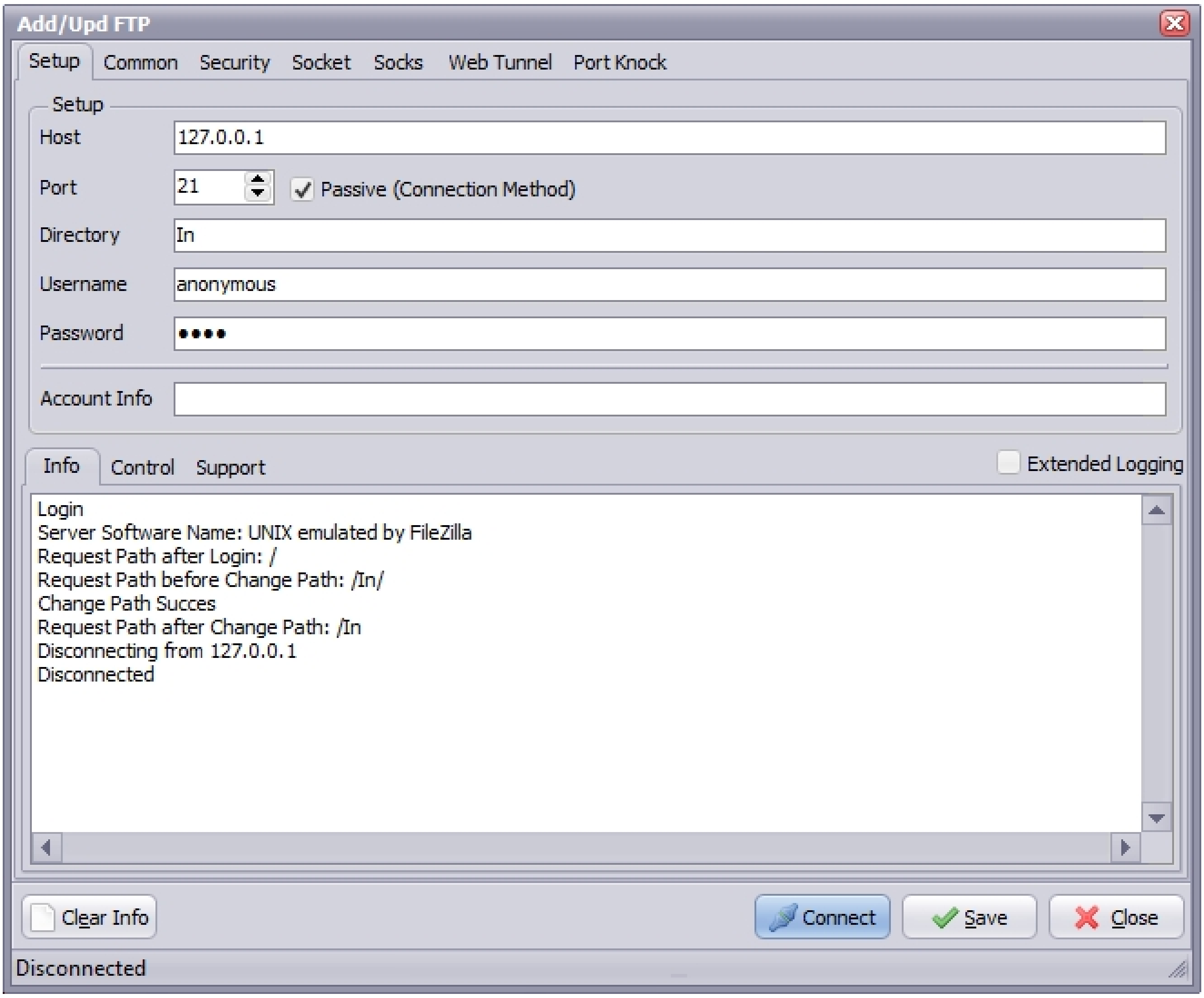
- You can drag and drop the folder into the window.

FTP Source

FTP (FTP & FTPS) Source Setup

Add / Update FTP as Source.

Setup Options



Host: 127.0.0.1

Port: 21 ☑ Passive (Connection Method)

Directory: In

Username: anonymous

Password: ●●●●

Account Info:

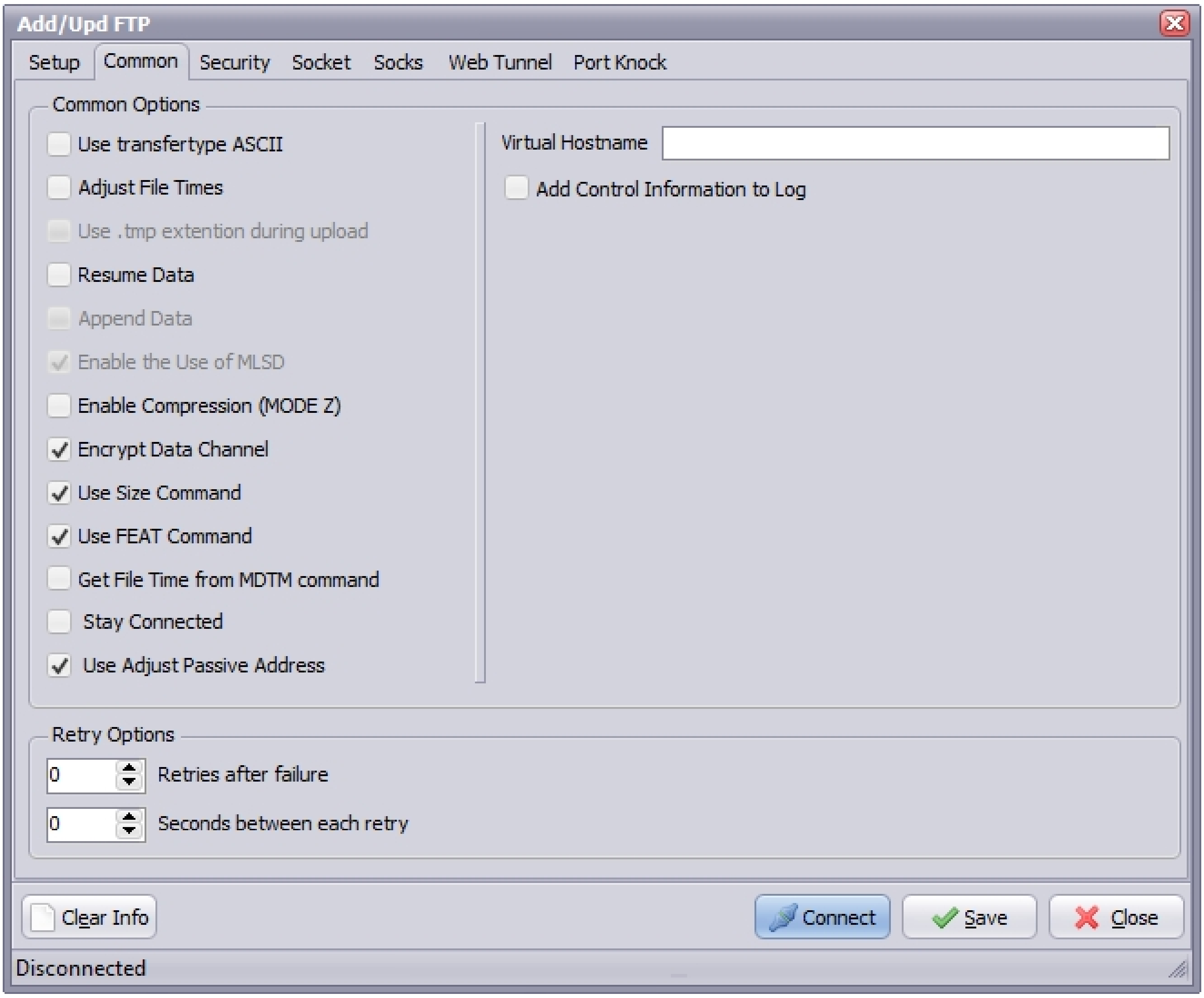
□ Extended Logging

```
Login
Server Software Name: UNIX emulated by FileZilla
Request Path after Login: /
Request Path before Change Path: /In/
Change Path Succes
Request Path after Change Path: /In
Disconnecting from 127.0.0.1
Disconnected
```

Disconnected

- 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.
- Account Info: Here you can enter your own information about this FTP connection. It's an information text field.
- Extended Logging: To extend the log information in the Info window.
- Connect: Check connection setup.

Common Options



Common Options

☐ Use transfertype ASCII
☐ Adjust File Times
☐ Use .tmp extention during upload
☐ Resume Data
☐ Append Data
☑ Enable the Use of MLSD
☐ Enable Compression (MODE Z)
☑ Encrypt Data Channel
☑ Use Size Command
☑ Use FEAT Command
☐ Get File Time from MDTM command
☐ Stay Connected
☑ Use Adjust Passive Address

Virtual Hostname

☐ Add Control Information to Log

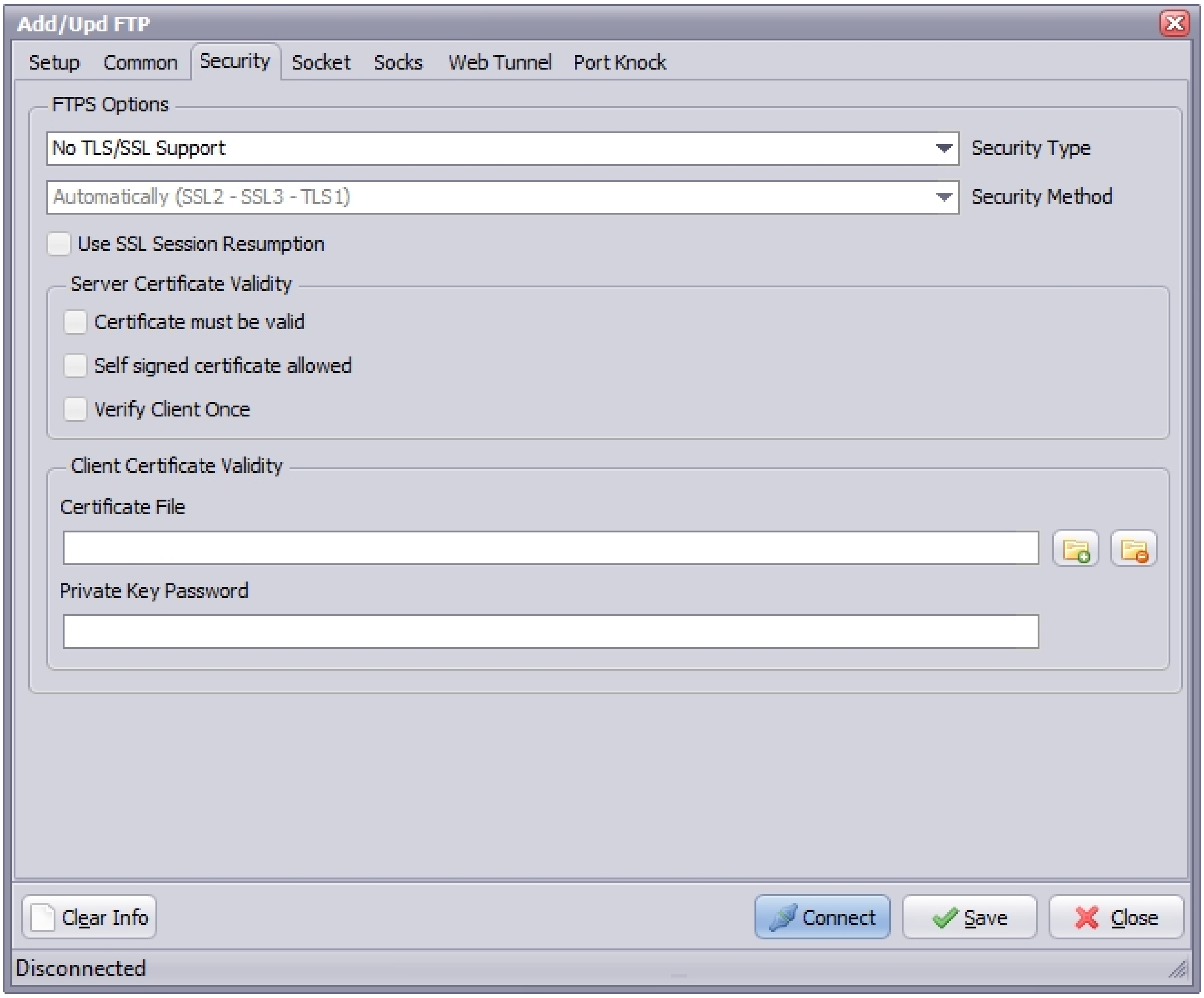
Retry Options

0 Retries after failure
0 Seconds between each retry

Disconnected

- 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 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.
- Virtual Hostname: Use this option to allow a server-FTP process to determine to which of possibly many virtual hosts the File Mover wishes to connect.
- Add Control Information to log: Add FTP specific control information to the log.
- Retries after failure: Amount of retries after a copy/move failure.
- Seconds between each retry: Seconds that the rule will wait between each retry.

Security Options



FTPS Options

Security Type: No TLS/SSL Support

Security Method: Automatically (SSL2 - SSL3 - TLS1)

□ Use SSL Session Resumption

Server Certificate Validity

□ Certificate must be valid

□ Self signed certificate allowed

□ Verify Client Once

Client Certificate Validity

Certificate File:

Private Key Password:

Disconnected

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.

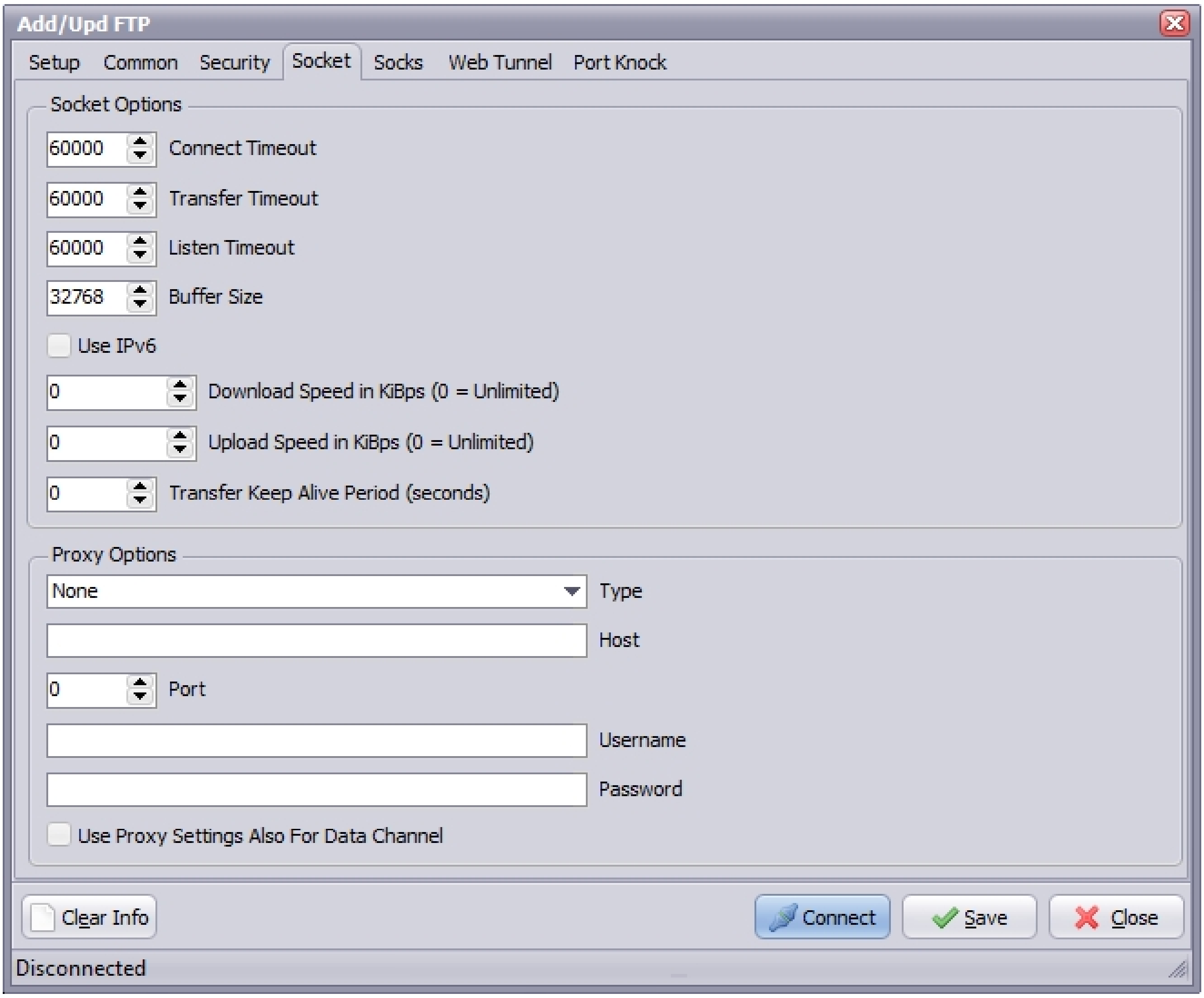
- Self signed certificate allowed: A self signed certificate is allowed.
- Verify client once:

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



Socket Options

60000 Connect Timeout

60000 Transfer Timeout

60000 Listen Timeout

32768 Buffer Size

☐ Use IPv6

0 Download Speed in KiBps (0 = Unlimited)

0 Upload Speed in KiBps (0 = Unlimited)

0 Transfer Keep Alive Period (seconds)

Proxy Options

None Type

Host

0 Port

Username

Password

☐ Use Proxy Settings Also For Data Channel

Disconnected

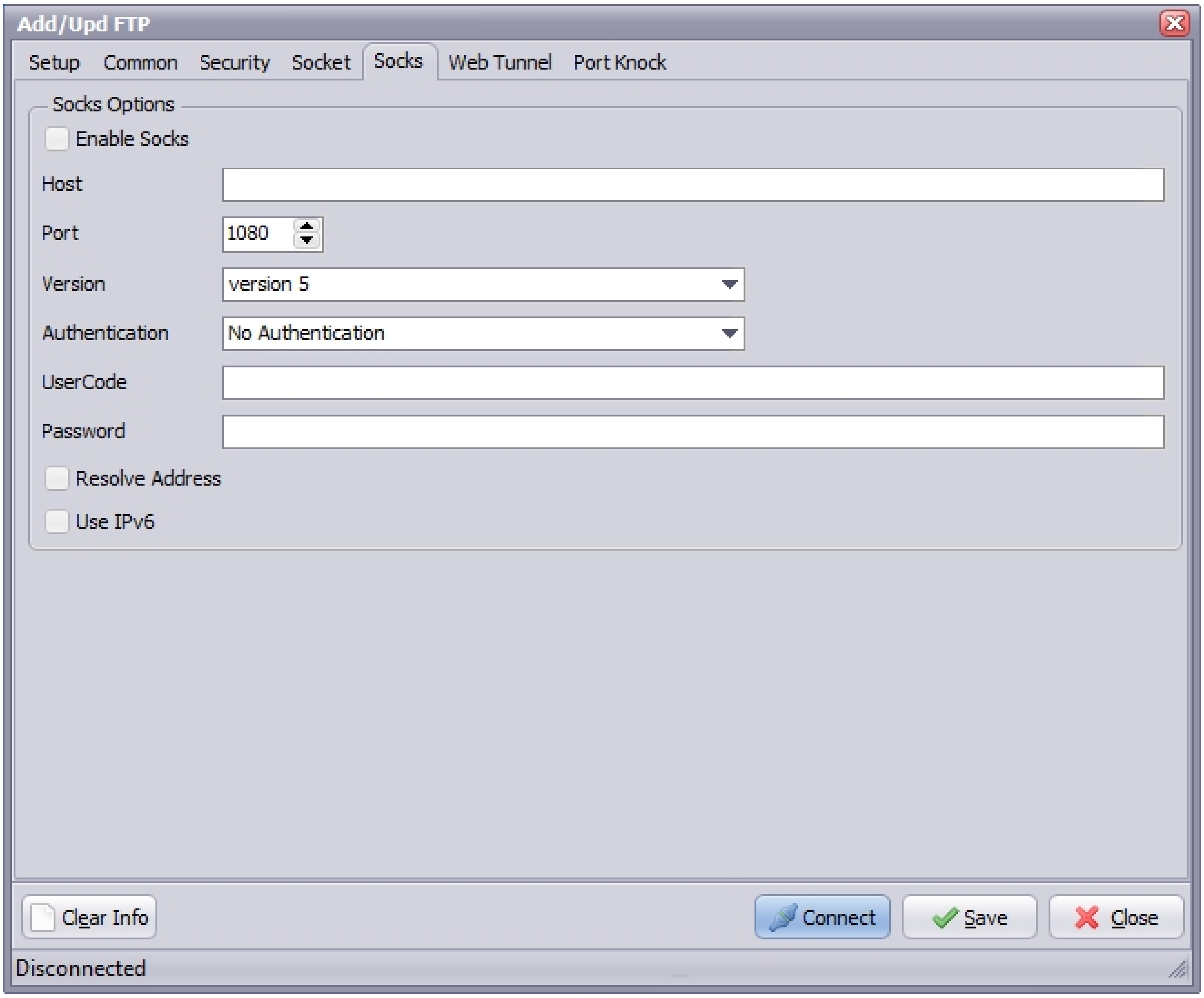
- Connect Timeout: Milliseconds to wait for successful completion of a connection attempt (default 60000). Default value is 60000 ms (1 min).
- Listen Timeout: Use this option to specify maximal time during which the listening socket will be opened in the active mode. If there is no connection request 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.

Proxy Options

- 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.

Socks Options



Socks Options

□ Enable Socks

Host

Port 1080

Version version 5

Authentication No Authentication

UserCode

Password

□ Resolve Address

□ Use IPv6

Disconnected

- Enable Socks: This option defines whether the connection is established directly (Socks is disabled) or via SOCKS server (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".

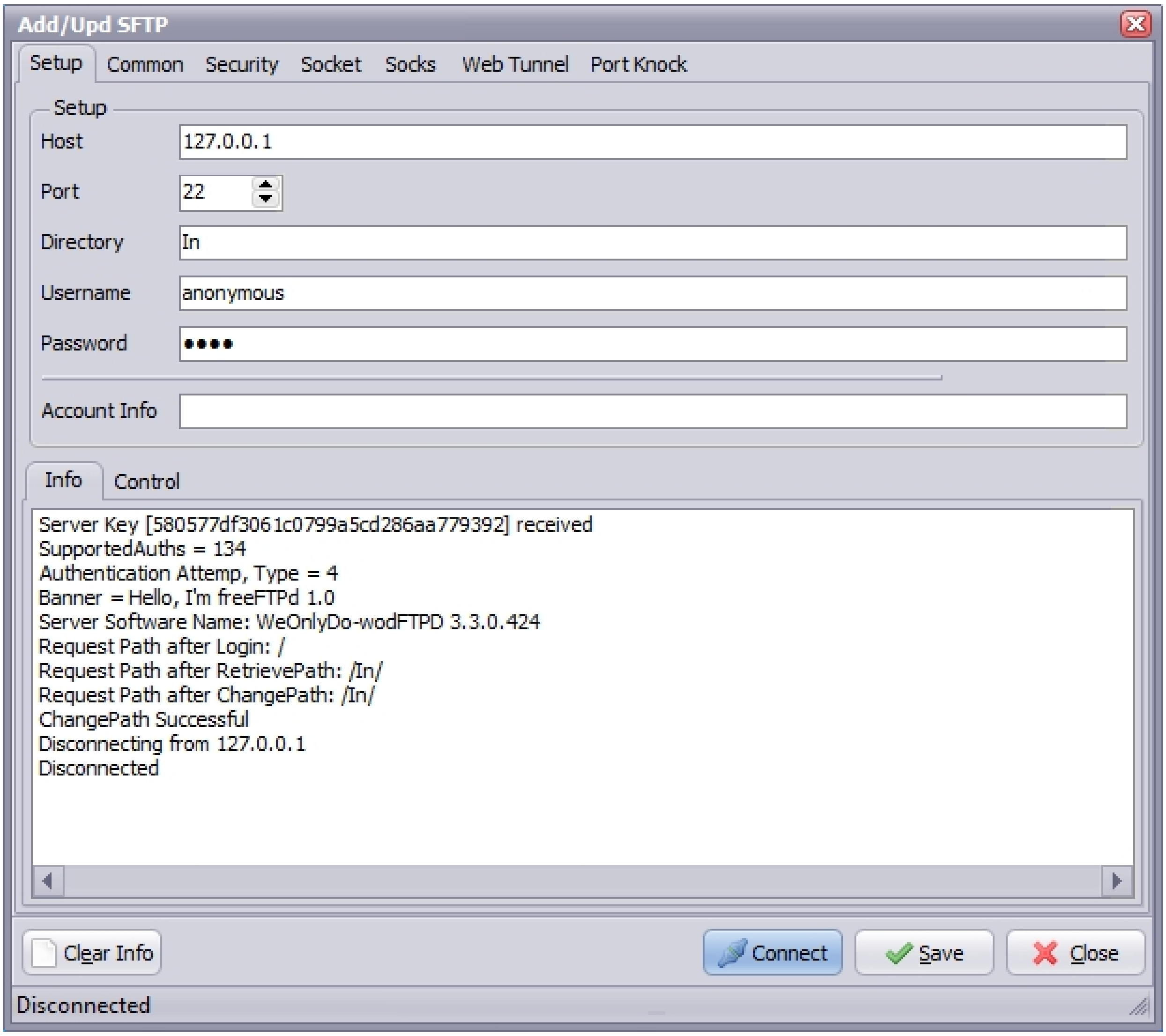
- UserCode: This property specifies the user code (username) to access the SOCKS server.
- Password: This property specifies the password to access the SOCKS server.
- Resolve Address: Specifies whether the address of destination host is resolved or passed to SOCKS server for resolving. Usually the host 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



Setup

Host 127.0.0.1

Port 22

Directory In

Username anonymous

Password ••••

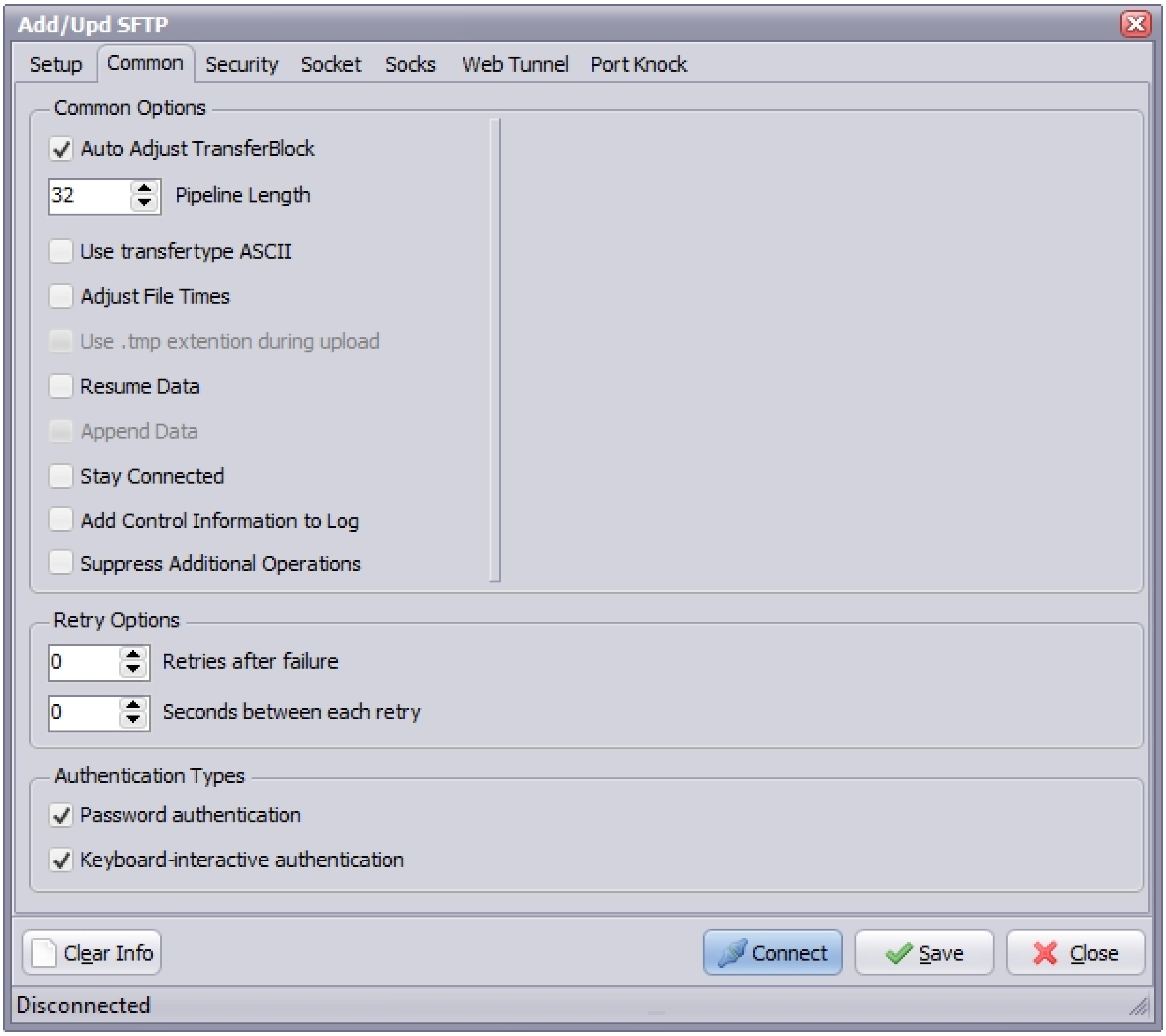
Account Info

```
Server Key [580577df3061c0799a5cd286aa779392] received
SupportedAuths = 134
Authentication Attemp, Type = 4
Banner = Hello, I'm freeFTPd 1.0
Server Software Name: WeOnlyDo-wodFTPD 3.3.0.424
Request Path after Login: /
Request Path after RetrievePath: /In/
Request Path after ChangePath: /In/
ChangePath Successful
Disconnecting from 127.0.0.1
Disconnected
```

Disconnected

- 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

32 Pipeline Length

☐ Use transfertype ASCII

☐ Adjust File Times

☐ Use .tmp extention during upload

☐ Resume Data

☐ Append Data

☐ Stay Connected

☐ Add Control Information to Log

☐ Suppress Additional Operations

Retry Options

0 Retries after failure

0 Seconds between each retry

Authentication Types

☑ Password authentication

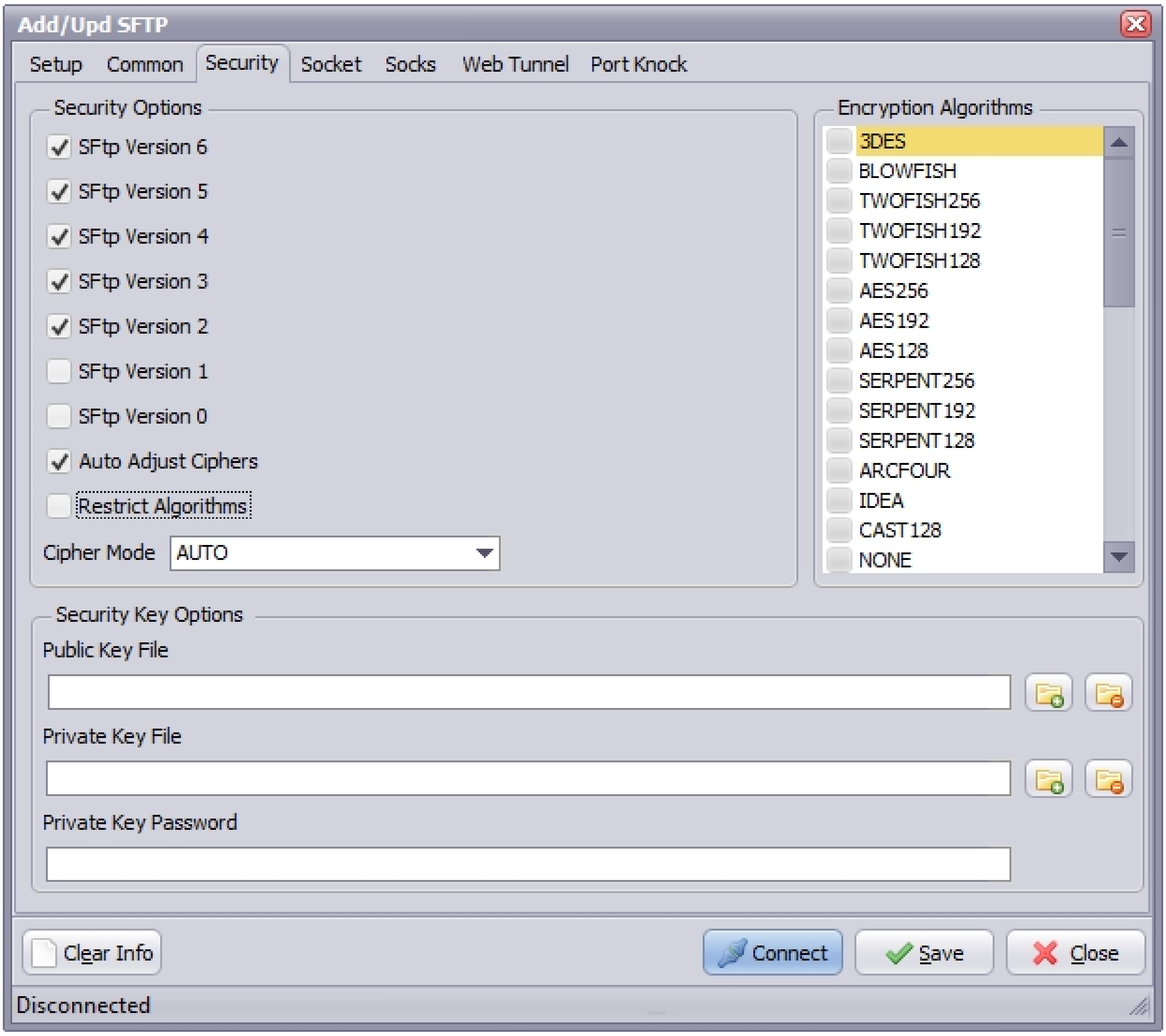
☑ Keyboard-interactive authentication

Disconnected

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 between scans.
- Add Control Information to log: Add SFTP specific control information to the log.
- Suppress Additional Operations: Enable Suppress Additional Operations option to work around buggy SFTP servers.
- Retries after failure: Amount of retries after a copy/move failure.
- Seconds between each retry: Seconds that the rule will wait between each retry.
- Authentication Types: Specify which authentication types SSH client should try to use during the negotiation process.

Security Options



Security Options

- ☑ SFtp Version 6
- ☑ SFtp Version 5
- ☑ SFtp Version 4
- ☑ SFtp Version 3
- ☑ SFtp Version 2
- ☐ SFtp Version 1
- ☐ SFtp Version 0
- ☑ Auto Adjust Ciphers
- ☐ Restrict Algorithms

Cipher Mode: AUTO

Encryption Algorithms

- ☐ 3DES
- ☐ BLOWFISH
- ☐ TWOFISH256
- ☐ TWOFISH192
- ☐ TWOFISH128
- ☐ AES256
- ☐ AES192
- ☐ AES128
- ☐ SERPENT256
- ☐ SERPENT192
- ☐ SERPENT128
- ☐ ARCFOUR
- ☐ IDEA
- ☐ CAST128
- ☐ NONE

Security Key Options

Public Key File:

Private Key File:

Private Key Password:

Disconnected

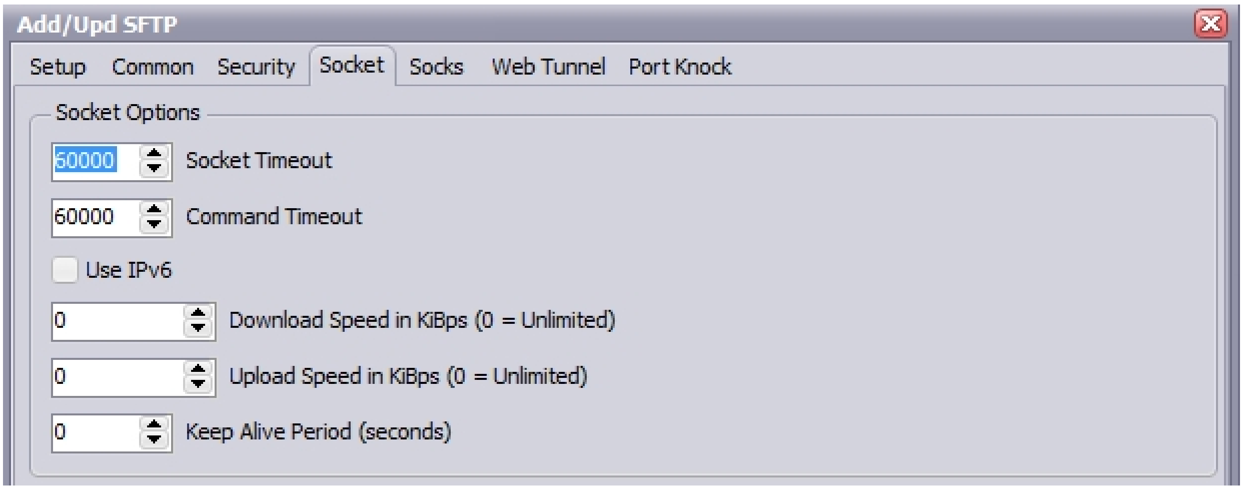
Security Options

- 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



Socket Options

60000 Socket Timeout

60000 Command Timeout

□ Use IPv6

0 Download Speed in KiBps (0 = Unlimited)

0 Upload Speed in KiBps (0 = Unlimited)

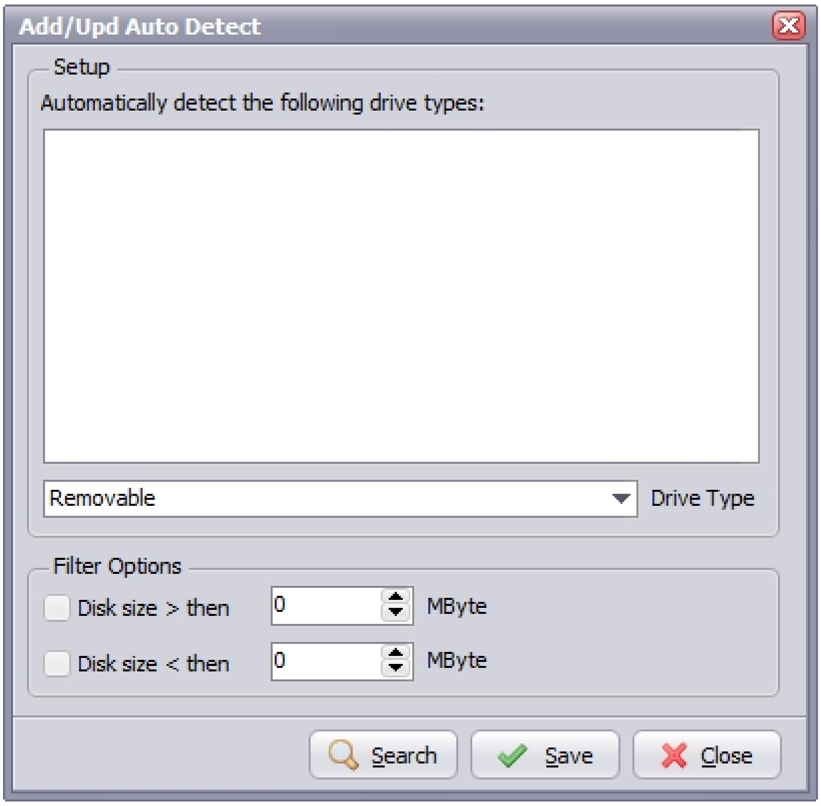
0 Keep Alive Period (seconds)

- Socket Timeout: Specifies maximum time of inactivity after which socket operation is canceled and is considered as expired. If you try to connect, read or write something from/to socket and the attempt is unsuccessful for specified number of milliseconds the operation is canceled with timeout error.
- Command Timeout: Use this option to specify the timeout (in milliseconds) for execution of SSH commands on the server.
- 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).

AUTO Source

AUTO Source Setup

Add / Update AUTO as Source.



Setup

Automatically detect the following drive types:

Removable Drive Type

Filter Options

□ Disk size > then 0 MByte

□ Disk size < then 0 MByte

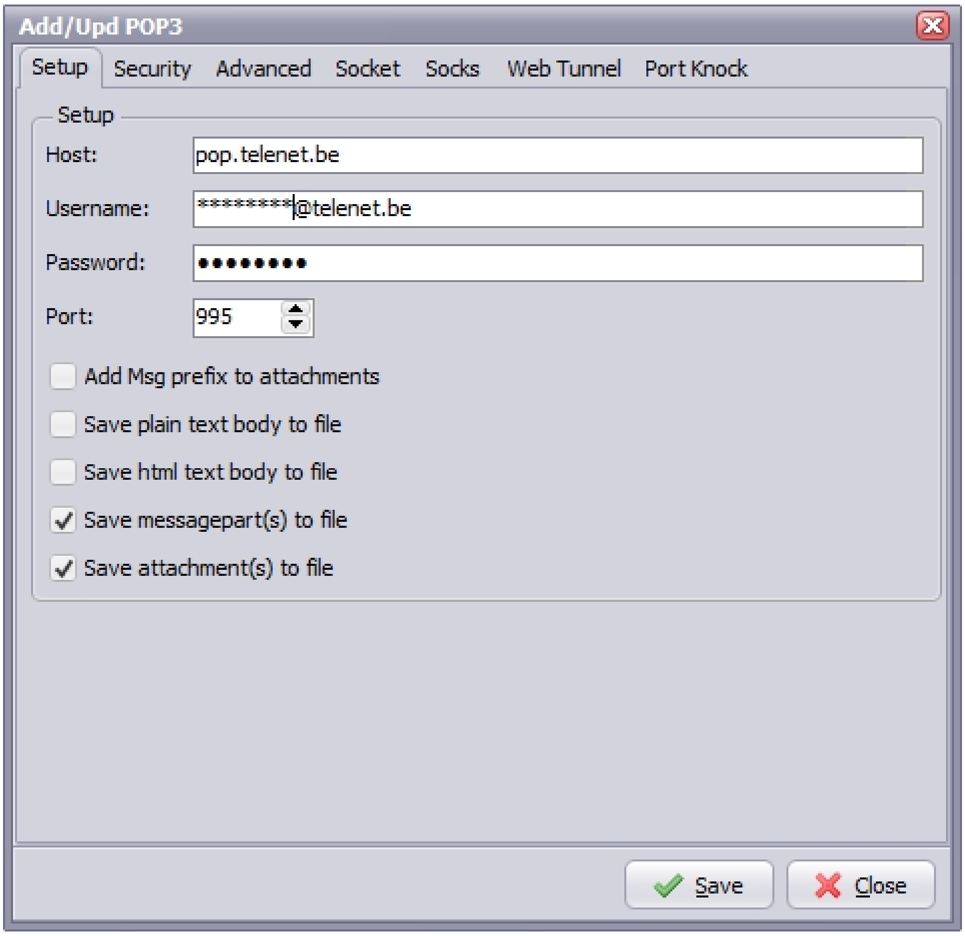
Will search for a removable drives like an USB stick or drive.. When using multiple removable drives you can use the disk size filter option.

POP3 Source

POP3 Source Setup

Add / Update POP3 as Source.

Setup Options



Setup

Host: pop.telenet.be

Username: *********@telenet.be

Password: ●●●●●●●●

Port: 995

□ Add Msg prefix to attachments

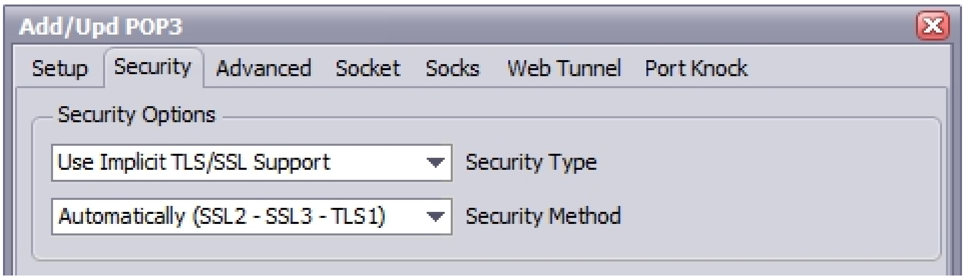
□ Save plain text body to file

□ Save html text body to file

☑ Save messagepart(s) to file

☑ Save attachment(s) to file

Security Options

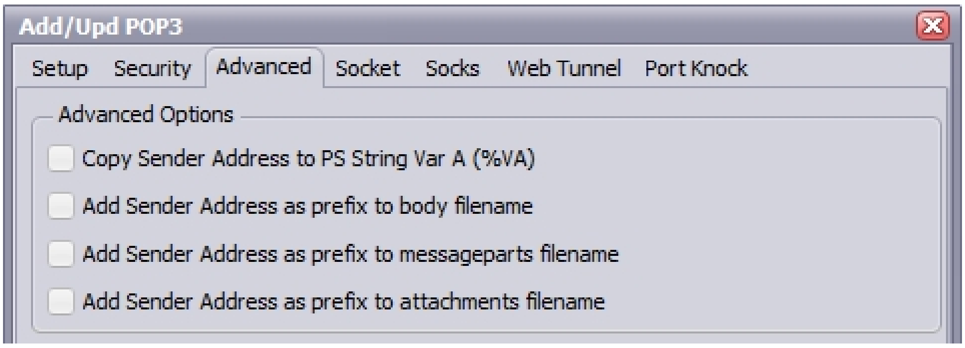


Security Options

Use Implicit TLS/SSL Support — Security Type

Automatically (SSL2 - SSL3 - TLS1) — Security Method

Advanced Options



Advanced Options

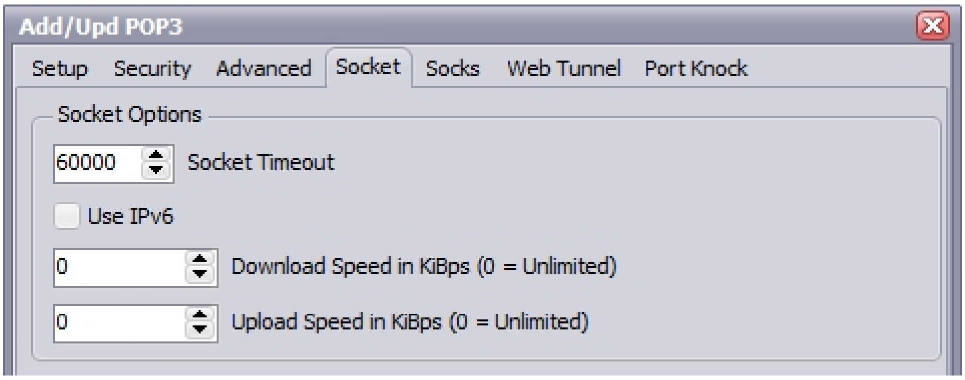
☐ Copy Sender Address to PS String Var A (%VA)

☐ Add Sender Address as prefix to body filename

☐ Add Sender Address as prefix to messageparts filename

☐ Add Sender Address as prefix to attachments filename

Socket



Socket Options

60000 Socket Timeout

☐ Use IPv6

0 Download Speed in KiBps (0 = Unlimited)

0 Upload Speed in KiBps (0 = Unlimited)

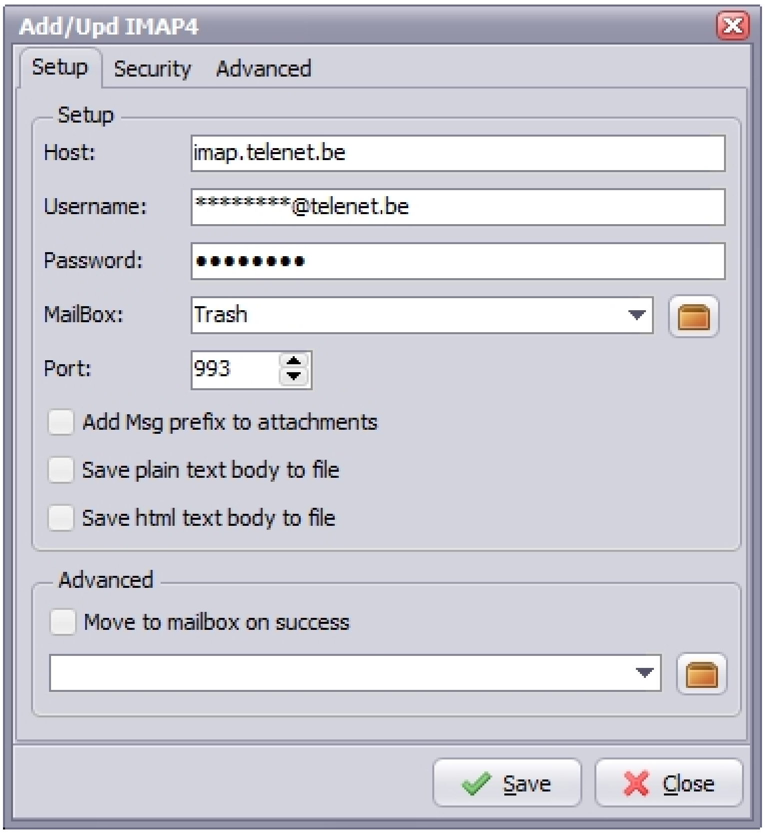
- Socket Timeout: Specifies maximum time of inactivity after which socket operation is canceled and is considered as expired. If you try to connect, read or write something from/to socket and the attempt is unsuccessful for specified number of milliseconds the operation is canceled with timeout error.
- 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 we may receive. The value of 0 (zero) means "no limitation".
- Upload Speed: Use this option to specify the maximum number of KiBps that we may send. The value of 0 (zero) means "no limitation".

IMAP Source

IMAP Source Setup

Add / Update IMAP as Source.

Setup Options



Setup

Host: imap.telenet.be

Username: *********@telenet.be

Password: ••••••••

MailBox: Trash

Port: 993

□ Add Msg prefix to attachments

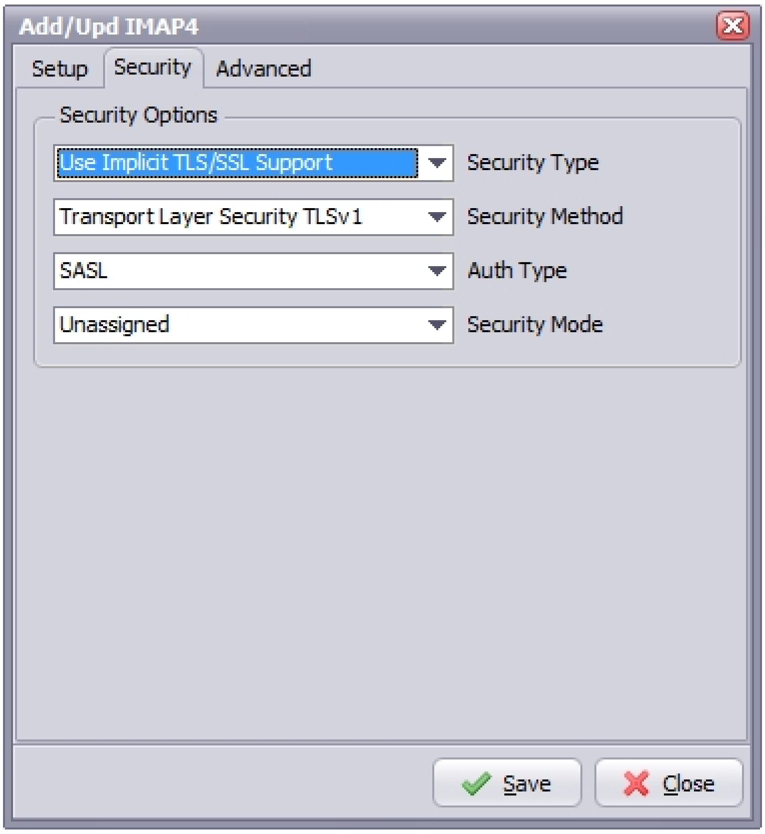
□ Save plain text body to file

□ Save html text body to file

Advanced

□ Move to mailbox on success

Security Options



Security Options

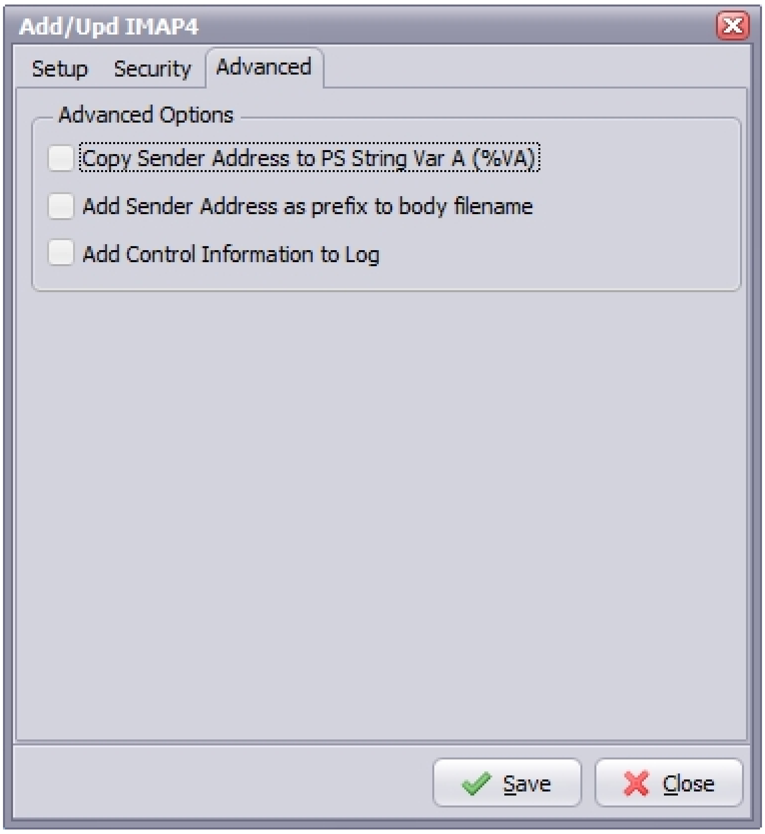
Use Implicit TLS/SSL Support — Security Type

Transport Layer Security TLSv1 — Security Method

SASL — Auth Type

Unassigned — Security Mode

Advanced Options



Advanced Options

□ Copy Sender Address to PS String Var A (%VA)

□ Add Sender Address as prefix to body filename

□ Add Control Information to Log

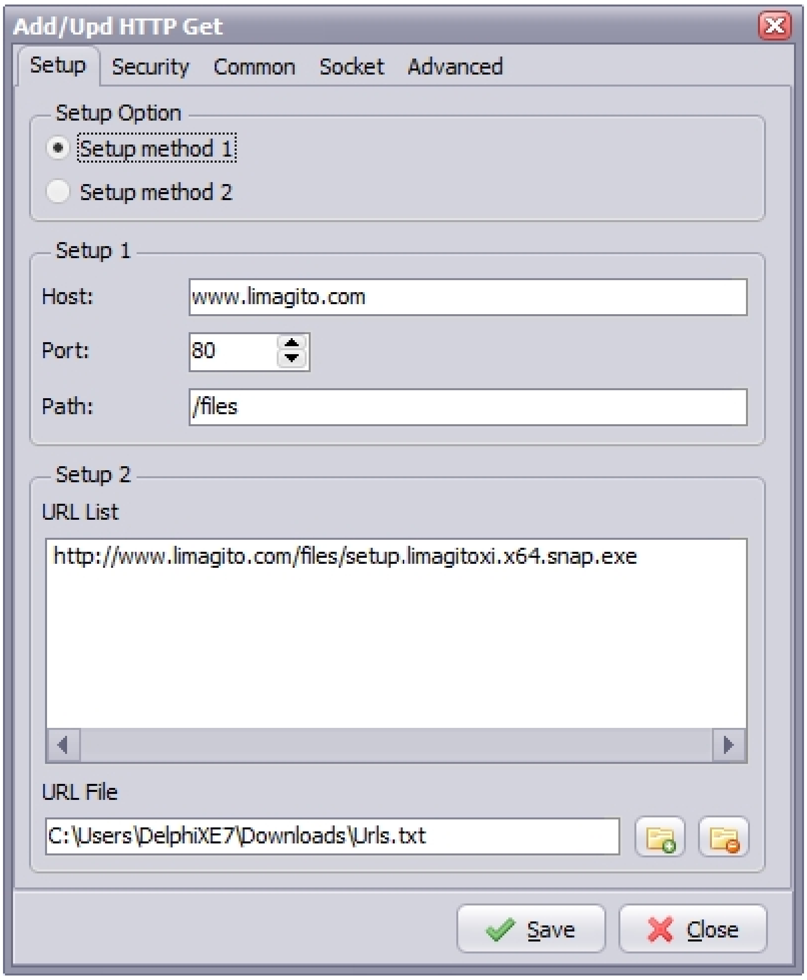
- Add Control Information to log: Add IMAP specific control information to the log.

HTTP Source

HTTP Source Setup

Add / Update HTTP as Source.

Setup Options



Setup Option

● Setup method 1

○ Setup method 2

Setup 1

Host: www.limagito.com

Port: 80

Path: /files

Setup 2

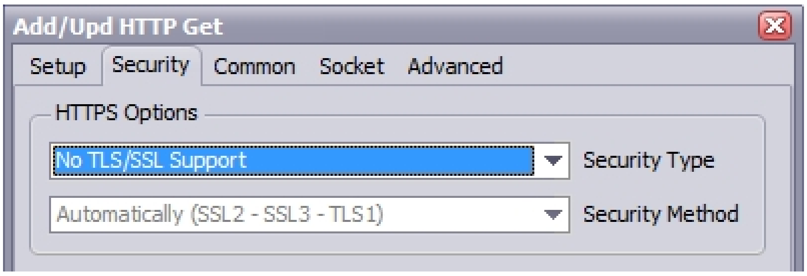
URL List

http://www.limagito.com/files/setup.limagitoxi.x64.snap.exe

URL File

C:\Users\DelphiXE7\Downloads\Urls.txt

Security Options

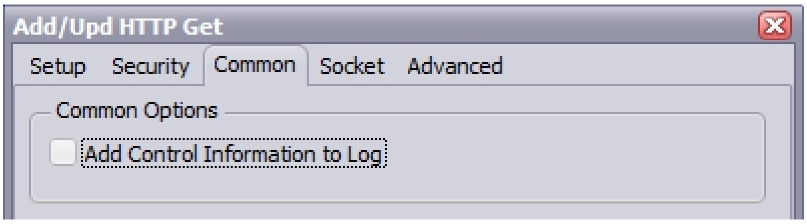


HTTPS Options

No TLS/SSL Support — Security Type

Automatically (SSL2 - SSL3 - TLS1) — Security Method

Common Options

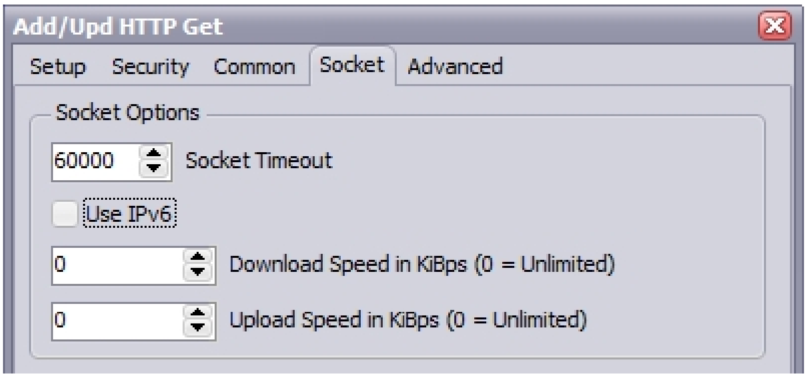


Common Options

□ Add Control Information to Log

- Add Control Information to log: Add HTTP specific control information to the log.

Socket Options



Socket Options

60000 Socket Timeout

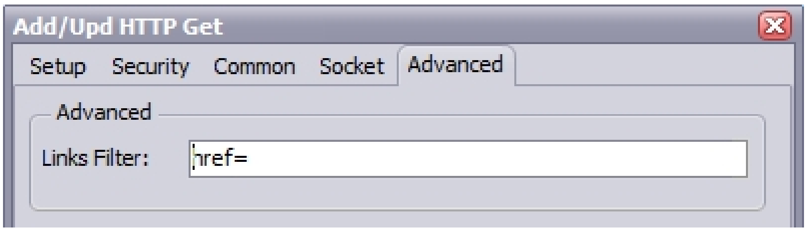
☐ Use IPv6

0 Download Speed in KiBps (0 = Unlimited)

0 Upload Speed in KiBps (0 = Unlimited)

- Socket Timeout: Specifies maximum time of inactivity after which socket operation is canceled and is considered as expired. If you try to connect, read or write something from/to socket and the attempt is unsuccessful for specified number of milliseconds the operation is canceled with timeout error.
- 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 we may receive. The value of 0 (zero) means "no limitation".
- Upload Speed: Use this option to specify the maximum number of KiBps that we may send. The value of 0 (zero) means "no limitation".

Advanced Options



Advanced

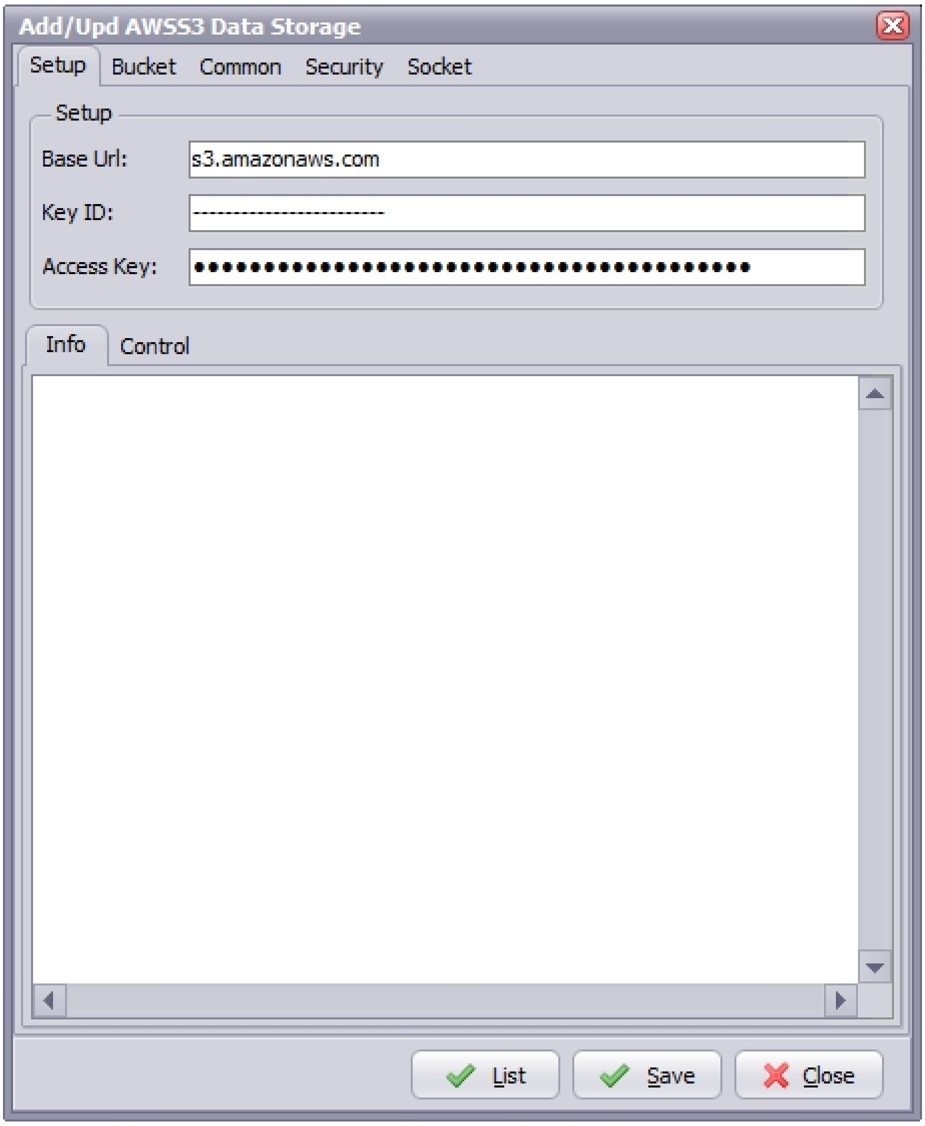
Links Filter: href=

AWSS3 Source

AWSS3 Source Setup

Add / Update AWSS3 as Source. Use this option to connect to S3 or S3-compatible cloud services.

Our AWSS3 option provides functionality to make requests, securely upload and download data using Amazon Simple Storage Service (S3) and compatible services. In S3 storages individual data objects are contained in buckets. Connection is established using the HTTP protocol. By default, secure connection is established. If you don't need a secure connection, please disable the SSL option. To authenticate to S3 storage, you need to provide Access Key and key ID pair.



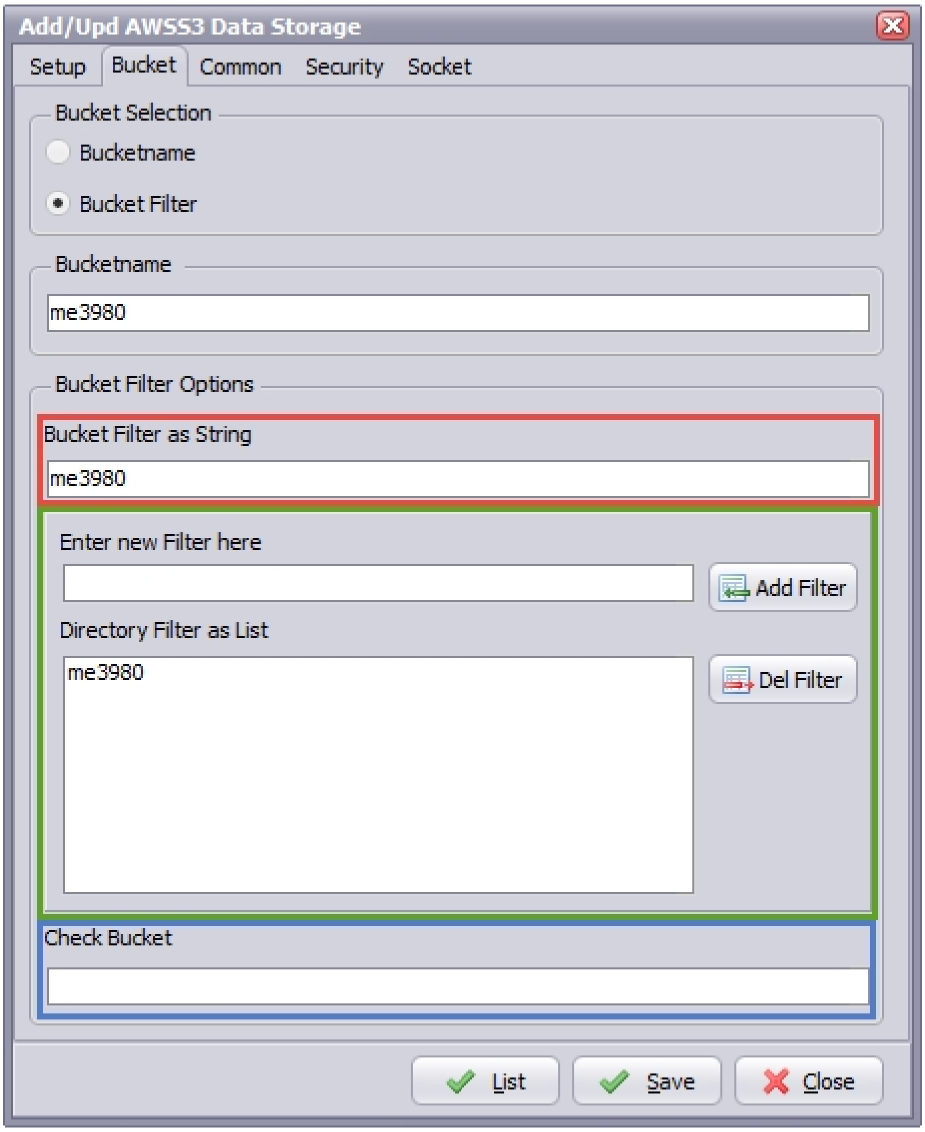
Base Url: s3.amazonaws.com

Key ID: ------------------------

Access Key: ••

- Base Url: Specify the base URL of the S3 service responder.
- Key ID: Use this option to specify the Key ID provided to the user of Amazon data storage. The KeyID and Access Key pair is used to authenticate and communicate with data storage.
- Access Key: Use this option to specify the secret key that was issued by Amazon to the data storage user. The KeyID and Access Key pair is used to authenticate and communicate with data storage.

Bucket Options



Bucket Selection
○ Bucketname
● Bucket Filter

Bucketname: me3980

Bucket Filter Options

Bucket Filter as String: me3980

Enter new Filter here:

Directory Filter as List: me3980

Check Bucket:

- Bucket Selection:
  - Bucketname: Enter the Bucketname you want to download your files from.
  - Bucket Filter: Search for Buckets using a filter.

- Bucket Filter Options:

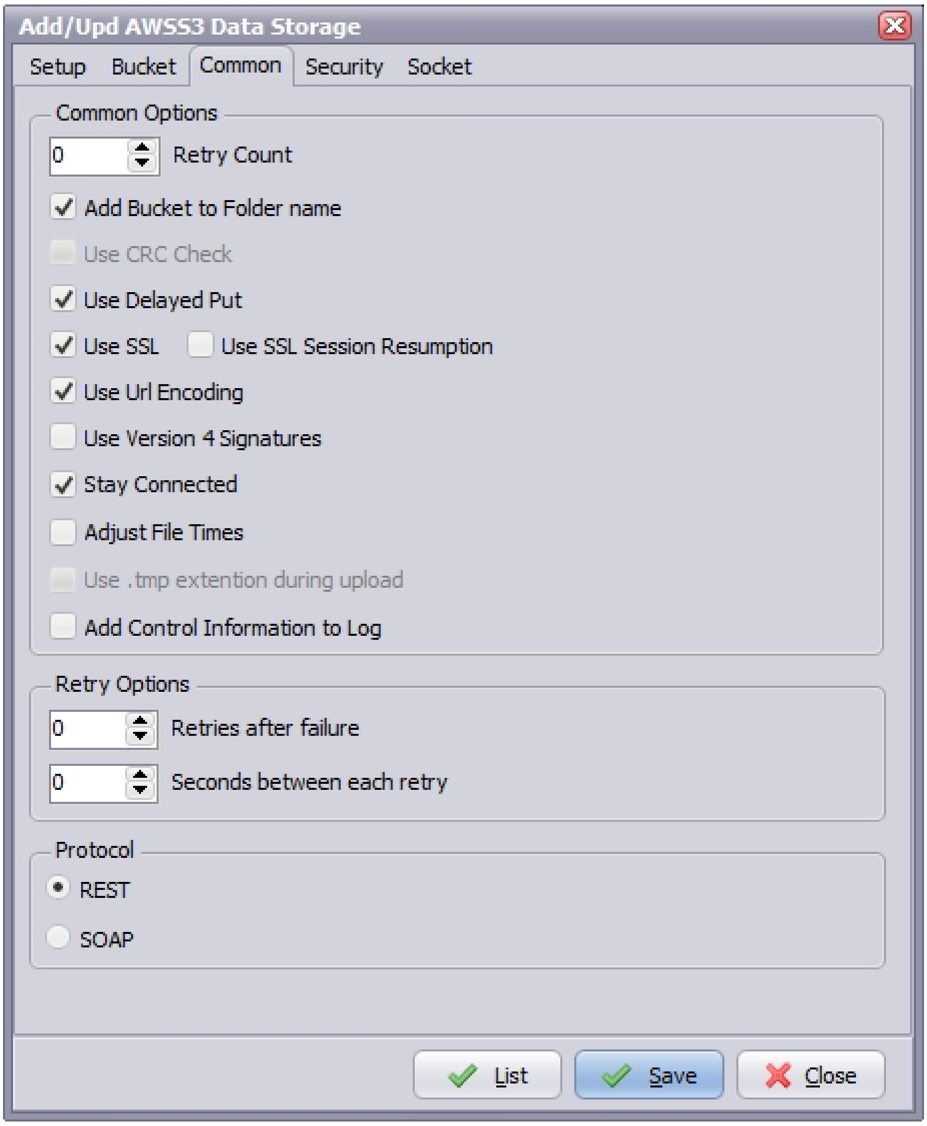
  Bucket filters can be added in two ways:

  1. Adding filters directly (red marked box). Separate each filter with a ';'
  2. Using the Add/Del Filter option. Enter a new filter and click the < Add Filter > button. Filters can also update or delete filters.

  In both cases the result will be visible in the 'Bucket Filter as List' field.

- Check Bucket: Check you filter using this test field.

Common Options



Common Options

0 Retry Count

☑ Add Bucket to Folder name

□ Use CRC Check

☑ Use Delayed Put

☑ Use SSL □ Use SSL Session Resumption

☑ Use Url Encoding

□ Use Version 4 Signatures

☑ Stay Connected

□ Adjust File Times

□ Use .tmp extention during upload

□ Add Control Information to Log

Retry Options

0 Retries after failure

0 Seconds between each retry

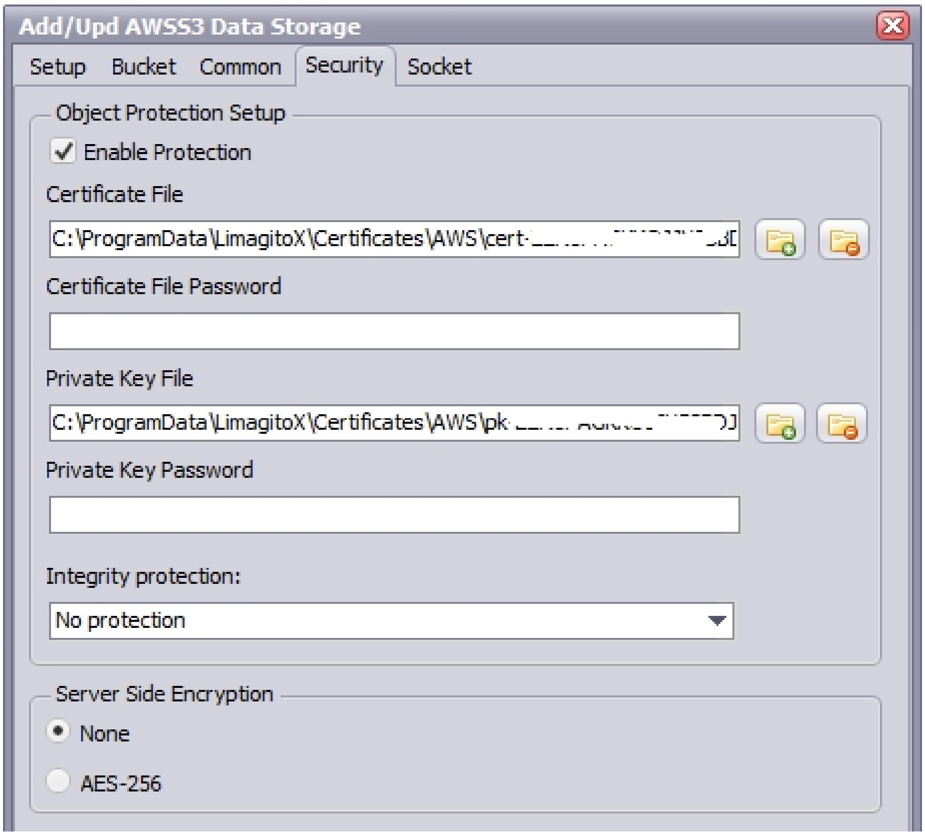
Protocol

● REST

○ SOAP

- Retry Count:
- Add Bucket to Folder name:
- Use Crc Check: Specifies if CRC check should be performed.
- Use Delayed Put: Specifies if PUT requests should be delayed.
- Use SSL: Specifies if secure connection should be established.
- Use SSL Session Resumption: Session reuse is one of the most important mechanism to improve SSL performance.
- Use Url Encoding: Specifies if URL encoding should be used.
- Use Version 4 Signatures:
- Stay Connected: Don't disconnect between scans.
- Adjust File Times: File times will be adjusted after upload/download operation.
- Add Control Information to Log: Add AWSS3 specific control information to the log.
- Retries after failure: Amount of retries after a copy/move failure.
- Seconds between each retry: Seconds that the rule will wait between each retry.
- Protocol: Use this option to specify the protocol which should be used to access the data storage.

Security Options



Object Protection Setup

☑ Enable Protection

Certificate File

C:\ProgramData\LimagitoX\Certificates\AWS\cert-[redacted]

Certificate File Password

Private Key File

C:\ProgramData\LimagitoX\Certificates\AWS\pk-[redacted]

Private Key Password

Integrity protection:

No protection

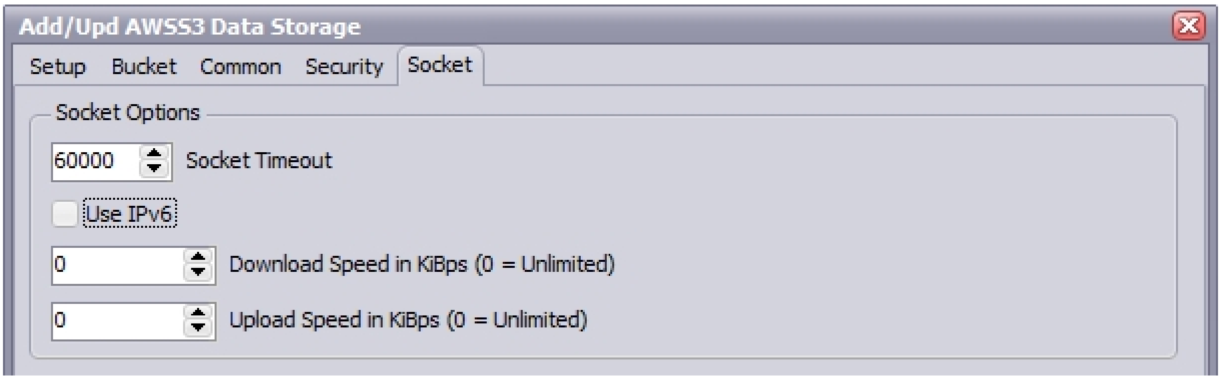
Server Side Encryption

● None

○ AES-256

- Certificate File: This file should contain the certificate (X.509). It recognizes the format automatically. If the format is not recognized, an error is reported. The supported formats are DER, PEM, PFX, SPC.
- Certificate File Password: Password to access the Certificate File.
- Private Key File: This files should contain the certificate's private key (X.509). It will recognizes the format automatically. If the format is not recognized, an error is reported. The supported formats are: DER, PEM, PFX, PVK, NET, PKCS#8.
- Private Key Password: Password to access the Private Key file.
- Integrity Protection:
  - No = no authentication info
  - Basic = basic authentication info should be used if there is no need to access particular blocks of data objects
  - Extended = extended authentication info should be used if there is need to access particular blocks of data objects
- Server Side Encryption: Server-side encryption is about protecting data at rest. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) employs strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.

Socket Options



Socket Options

60000 Socket Timeout

□ Use IPv6

0 Download Speed in KiBps (0 = Unlimited)

0 Upload Speed in KiBps (0 = Unlimited)

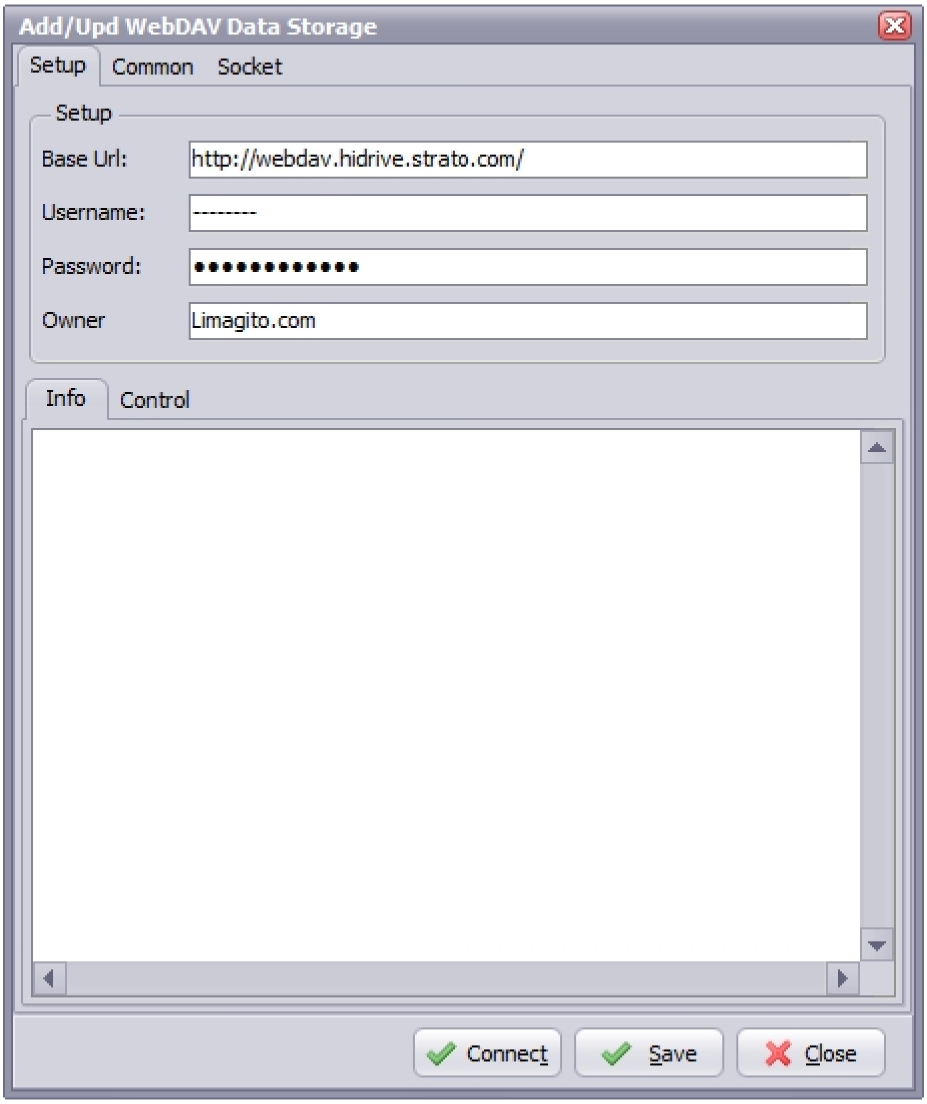
- Socket Timeout: Specifies maximum time of inactivity after which socket operation is canceled and is considered as expired. If you try to connect, read or write something from/to socket and the attempt is unsuccessful for specified number of milliseconds the operation is canceled with timeout error.

- 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 we may receive. The value of 0 (zero) means "no limitation".
- Upload Speed: Use this option to specify the maximum number of KiBps that we may send. The value of 0 (zero) means "no limitation".

WebDAV

WebDAV Source Setup

Add / Update WebDAV as Source.



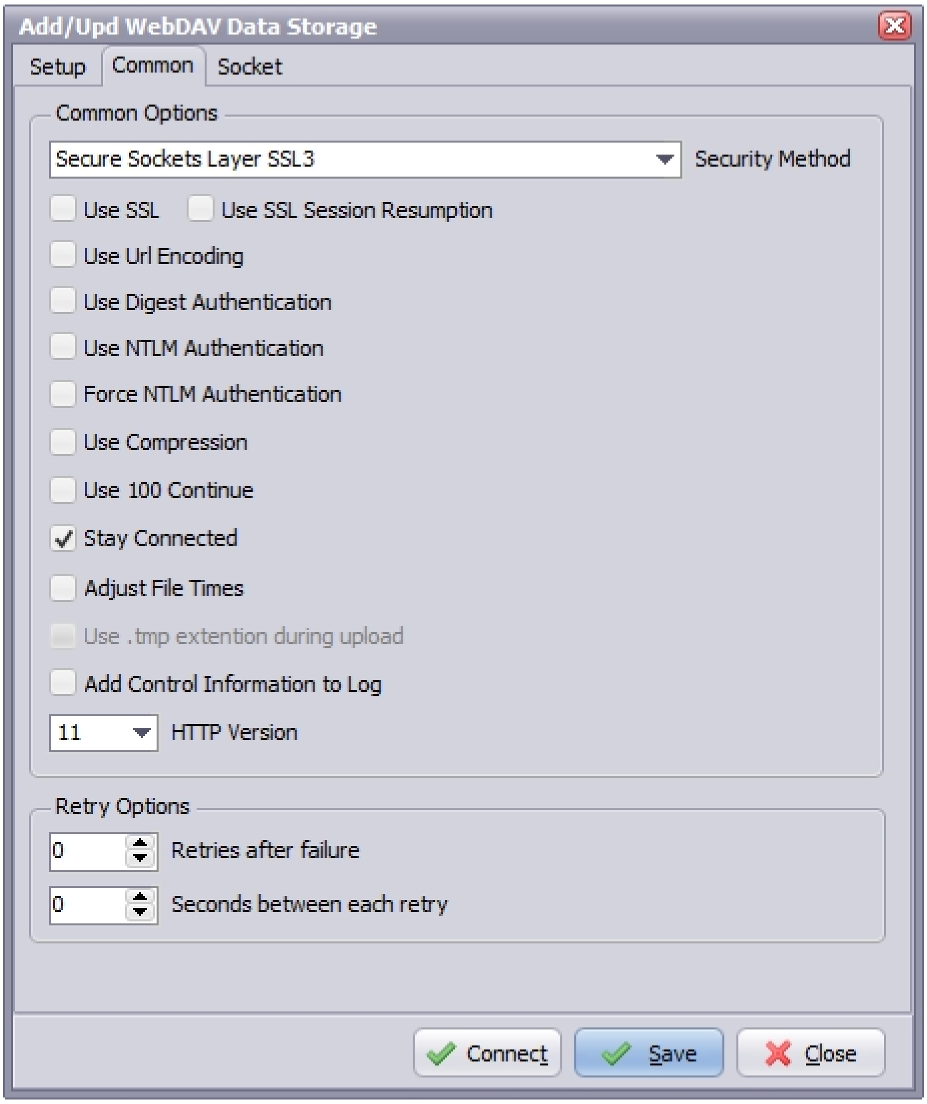
Base Url: http://webdav.hidrive.strato.com/

Username: --------

Password: ●●●●●●●●●●●●

Owner Limagito.com

Security Options



Common Options

Secure Sockets Layer SSL3 — Security Method

□ Use SSL □ Use SSL Session Resumption

□ Use Url Encoding

□ Use Digest Authentication

□ Use NTLM Authentication

□ Force NTLM Authentication

□ Use Compression

□ Use 100 Continue

☑ Stay Connected

□ Adjust File Times

□ Use .tmp extention during upload

□ Add Control Information to Log

11 HTTP Version

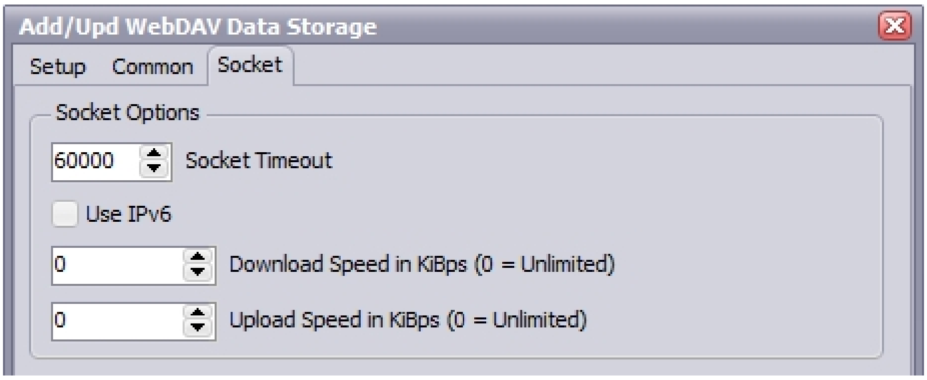
Retry Options

0 Retries after failure

0 Seconds between each retry

- Retries after failure: Amount of retries after a copy/move failure.
- Seconds between each retry: Seconds that the rule will wait between each retry.

Socket Options



Socket Options

60000 Socket Timeout

□ Use IPv6

0 Download Speed in KiBps (0 = Unlimited)

0 Upload Speed in KiBps (0 = Unlimited)

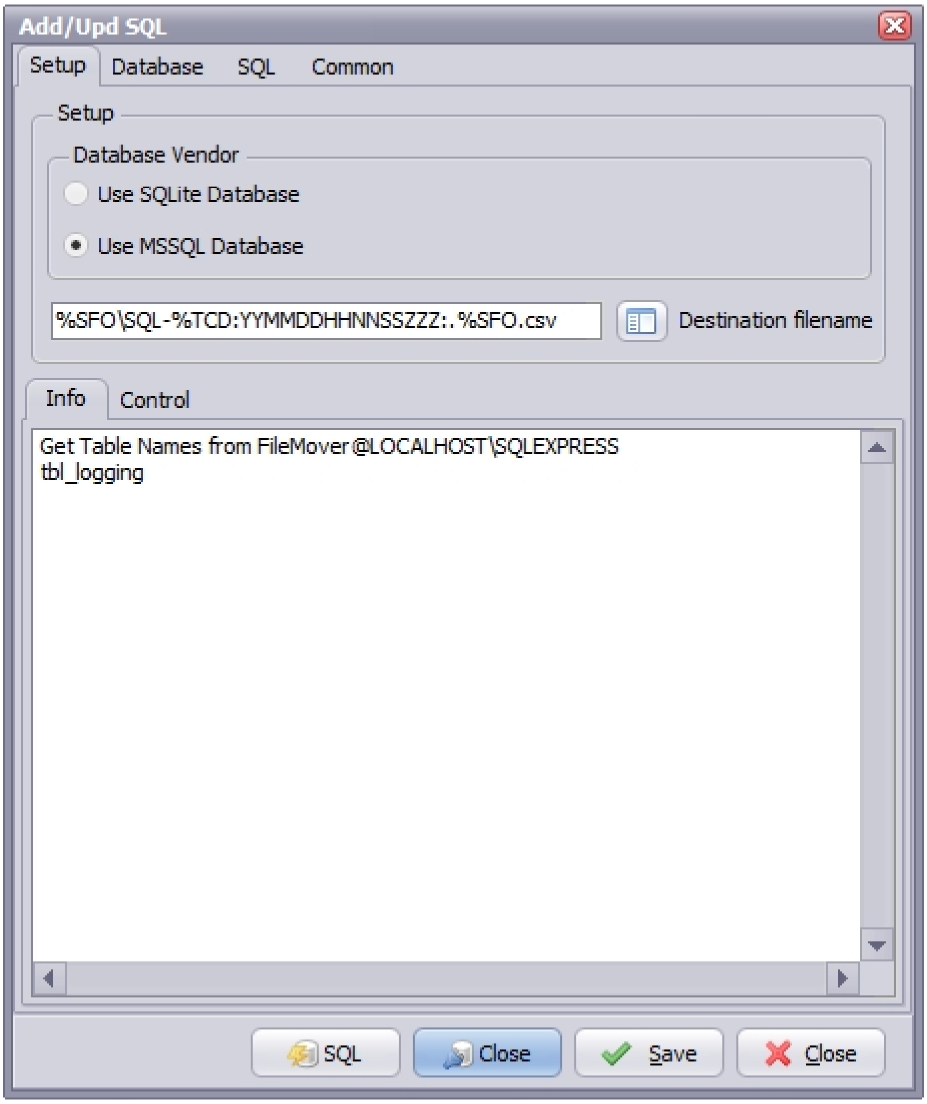
- Socket Timeout: Specifies maximum time of inactivity after which socket operation is canceled and is considered as expired. If you try to connect, read or write something from/to socket and the attempt is unsuccessful for specified number of milliseconds the operation is canceled with timeout error.
- 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 we may receive. The value of 0 (zero) means "no limitation".
- Upload Speed: Use this option to specify the maximum number of KiBps that we may send. The value of 0 (zero) means "no limitation".

SQL Source

SQL Source Setup

Add / Update SQL as Source.

Setup Options



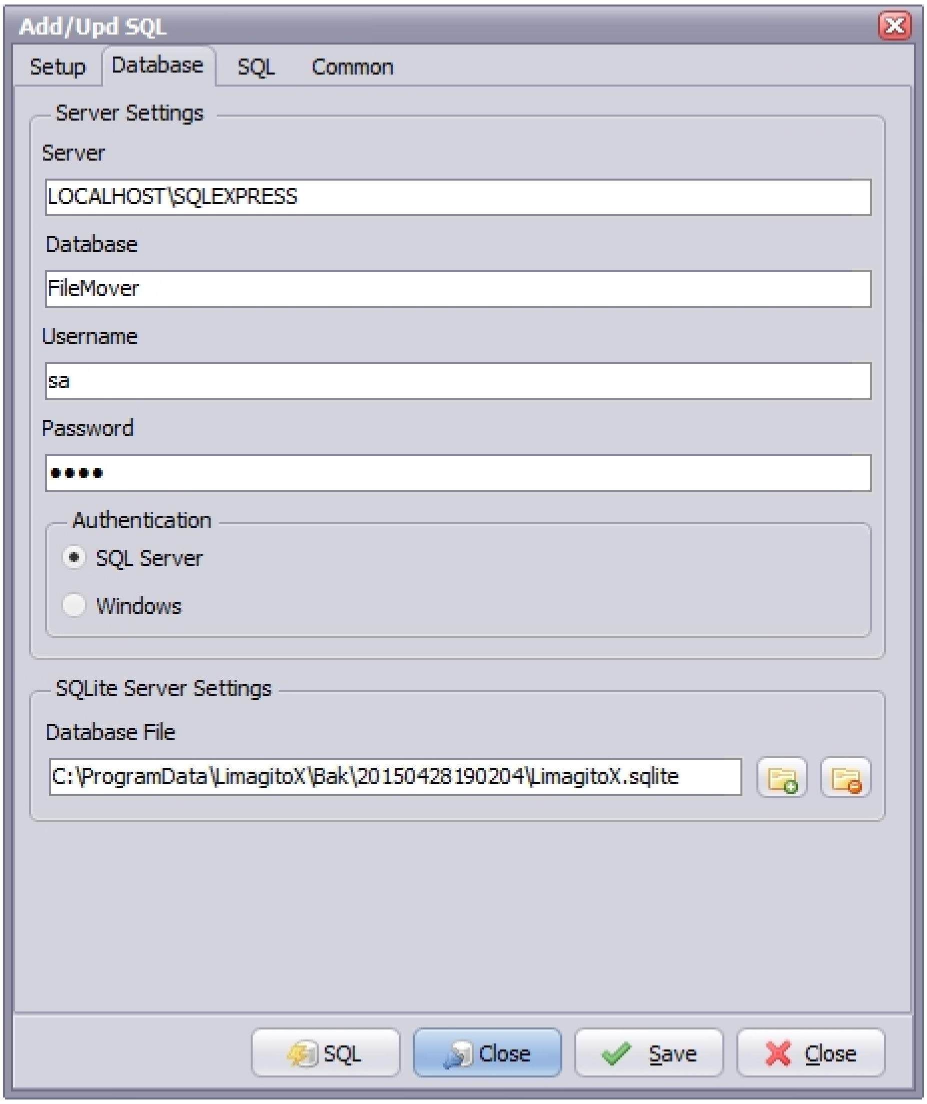
○ Use SQLite Database

● Use MSSQL Database

Destination filename: %SFO\SQL-%TCD:YYMMDDHHNNSSZZZ:.%SFO.csv

```
Get Table Names from FileMover@LOCALHOST\SQLEXPRESS
tbl_logging
```

Database Options



Server Settings

Server: LOCALHOST\SQLEXPRESS

Database: FileMover

Username: sa

Password: ••••

Authentication

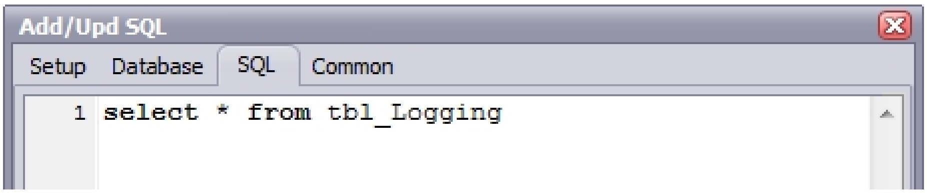
● SQL Server

○ Windows

SQLite Server Settings

Database File: C:\ProgramData\LimagitoX\Bak\20150428190204\LimagitoX.sqlite

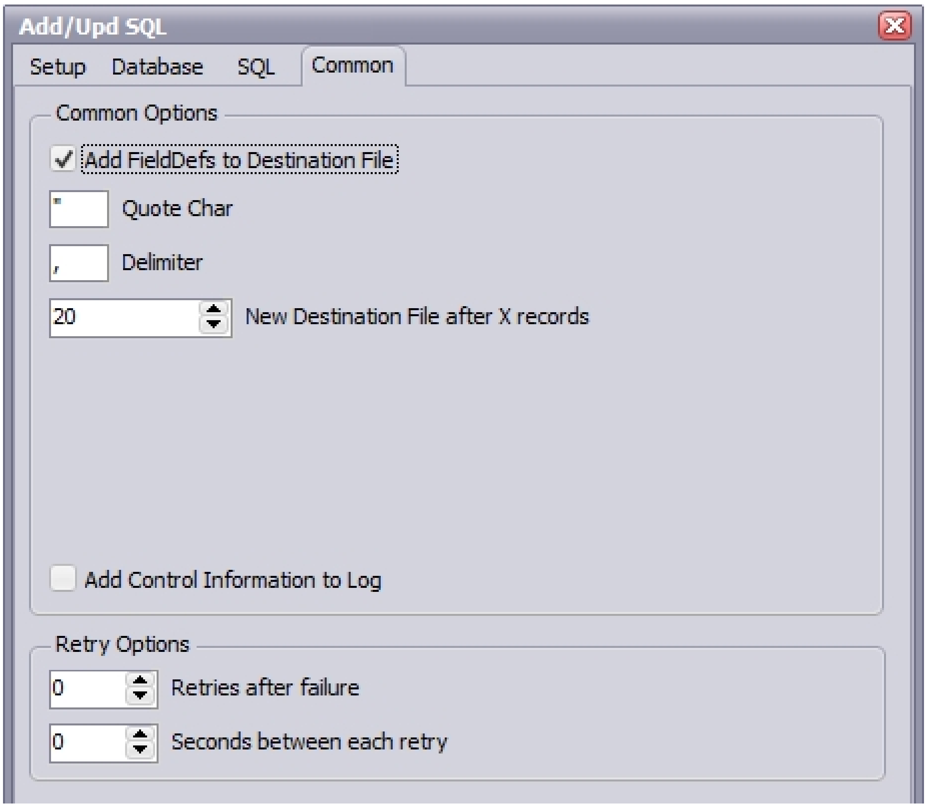
SQL Options



```
select * from tbl_Logging
```

Enter the SQL code you want to execute on the database.

Common Options



Common Options

☑ Add FieldDefs to Destination File

" Quote Char

, Delimiter

20 New Destination File after X records

☐ Add Control Information to Log

Retry Options

0 Retries after failure

0 Seconds between each retry

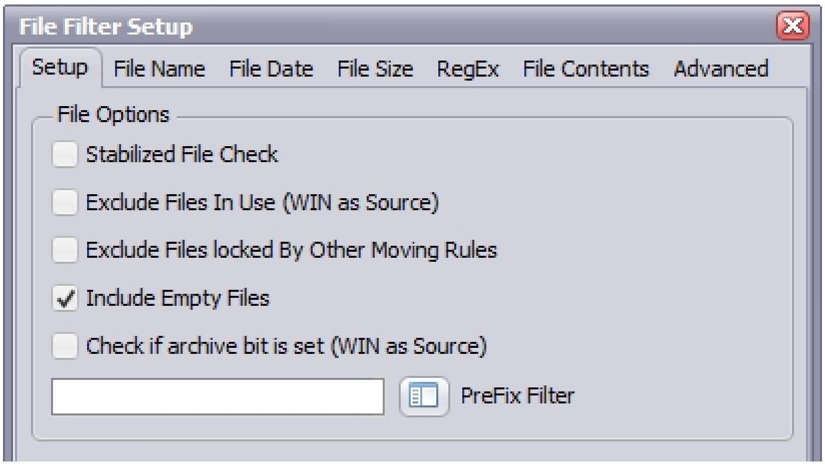
- Retries after failure: Amount of retries after a copy/move failure.
- Seconds between each retry: Seconds that the rule will wait between each retry.

File Filter

File Filter Setup

Add / Update File Filter. For each filter type we have an include and exclude setup available. Exclude priority is higher than include.

Setup Options



File Options

☐ Stabilized File Check

☐ Exclude Files In Use (WIN as Source)

☐ Exclude Files locked By Other Moving Rules

☑ Include Empty Files

☐ Check if archive bit is set (WIN as Source)

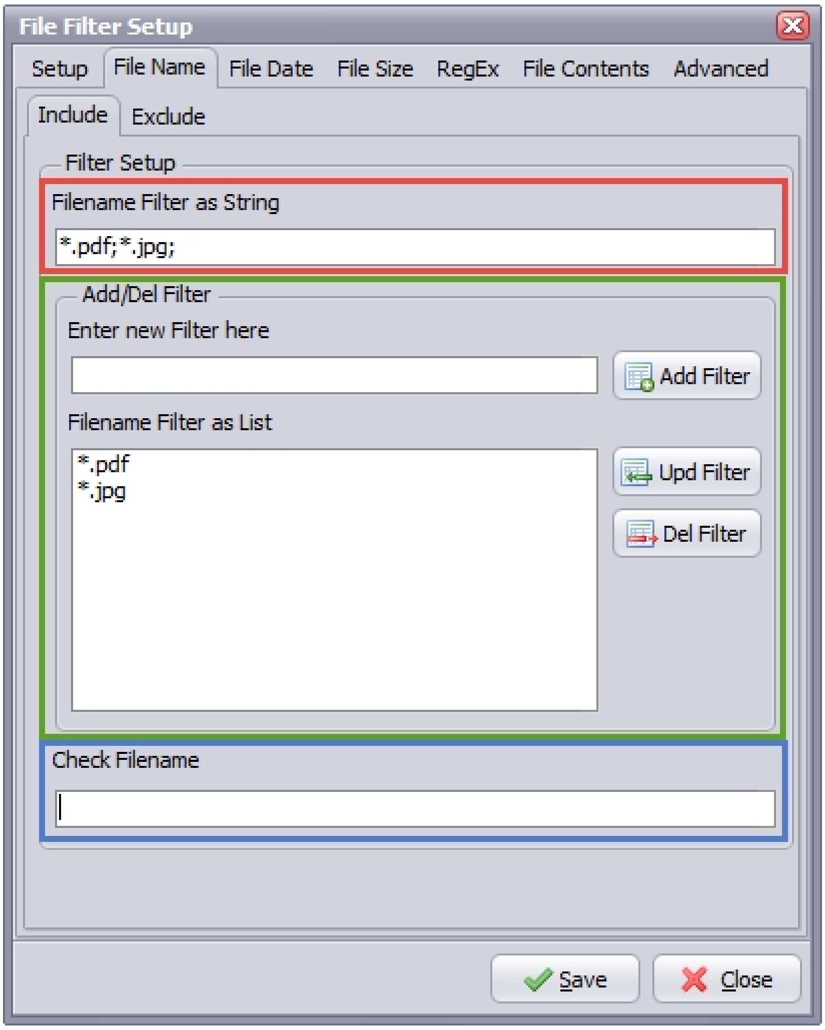
PreFix Filter

- 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.

File Name Options



Filename Filter as String

.pdf;.jpg;

Filename Filter as List

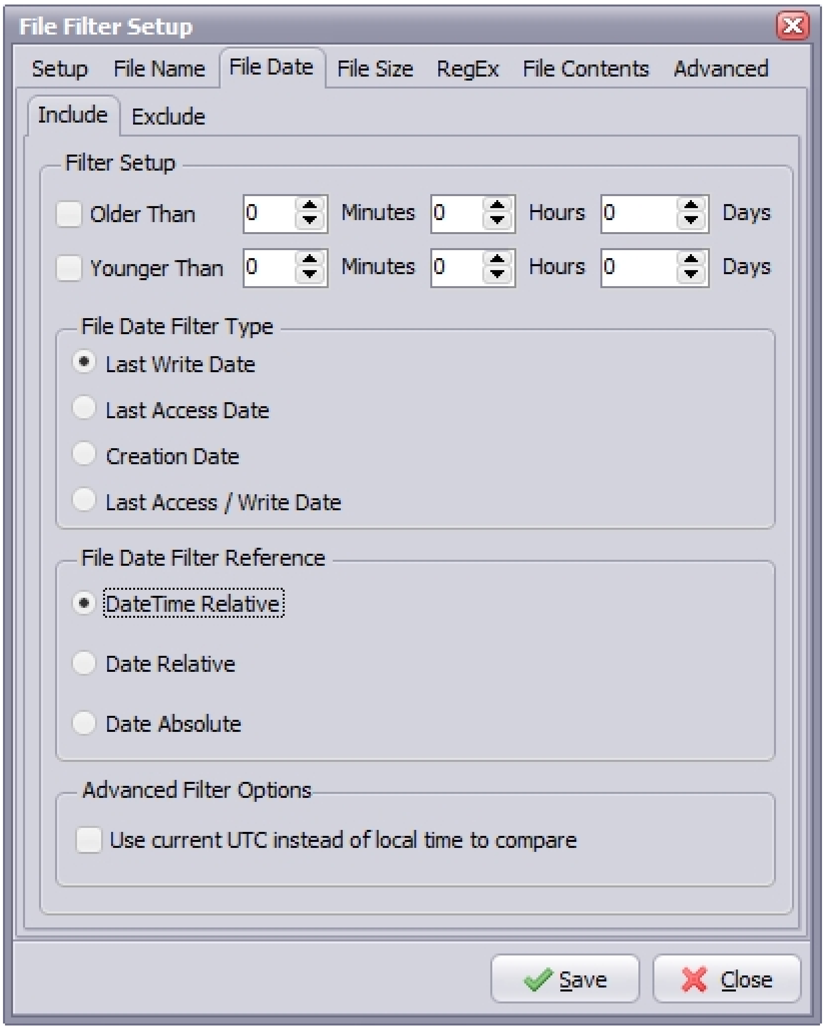
*.pdf
*.jpg

- Filename Include Filter: Scan will only pick up files which filenames are validated by this filter.
- Filename Exclude Filter: Scan will not pick up files which filenames are validated by this filter.
- Add/Del Filter: Filters can be added in two ways:

  3. Adding filters directly (red marked box). Separate each filter with a ';'
  4. Using the Add/Del Filter option. Enter a new filter and click the < Add Filter > button. Filters can also update or delete filters.

  In both cases the result will be visible in the 'Filename Filter as List' field.
- Check Filename: Check you filter using this test field.

File Date Options



Filter Setup

□ Older Than 0 Minutes 0 Hours 0 Days

□ Younger Than 0 Minutes 0 Hours 0 Days

File Date Filter Type

● Last Write Date

○ Last Access Date

○ Creation Date

○ Last Access / Write Date

File Date Filter Reference

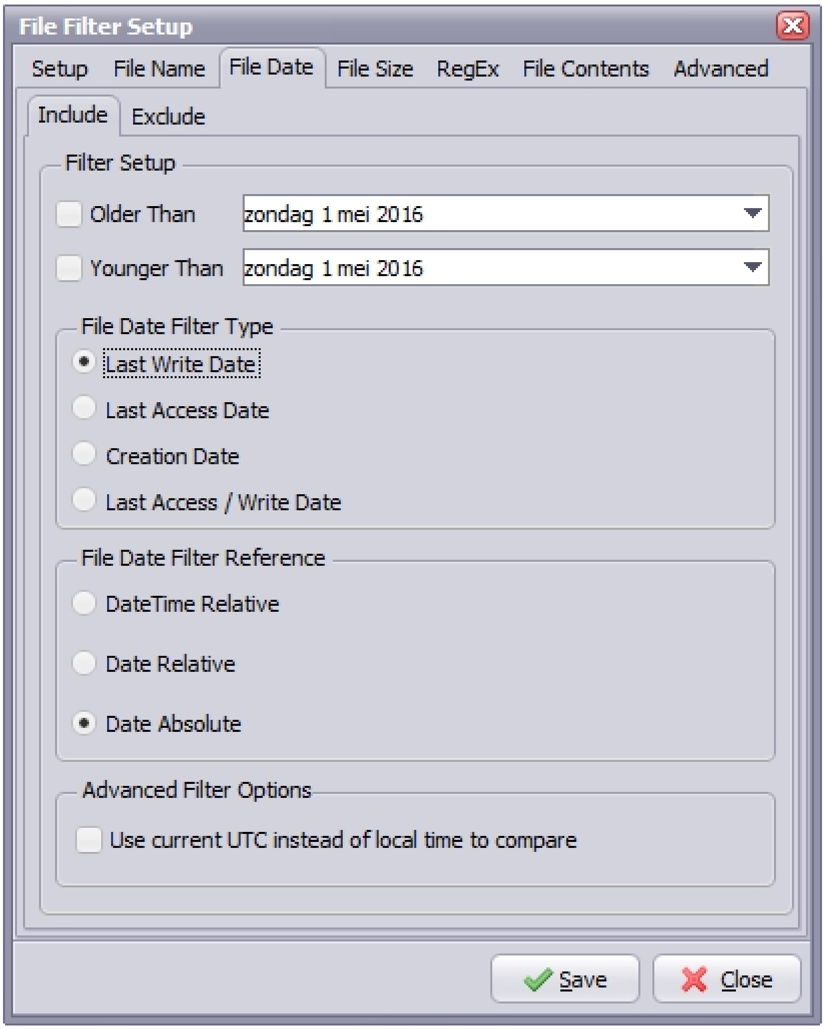
● DateTime Relative

○ Date Relative

○ Date Absolute

Advanced Filter Options

□ Use current UTC instead of local time to compare



Filter Setup

☐ Older Than zondag 1 mei 2016

☐ Younger Than zondag 1 mei 2016

File Date Filter Type

● Last Write Date
○ Last Access Date
○ Creation Date
○ Last Access / Write Date

File Date Filter Reference

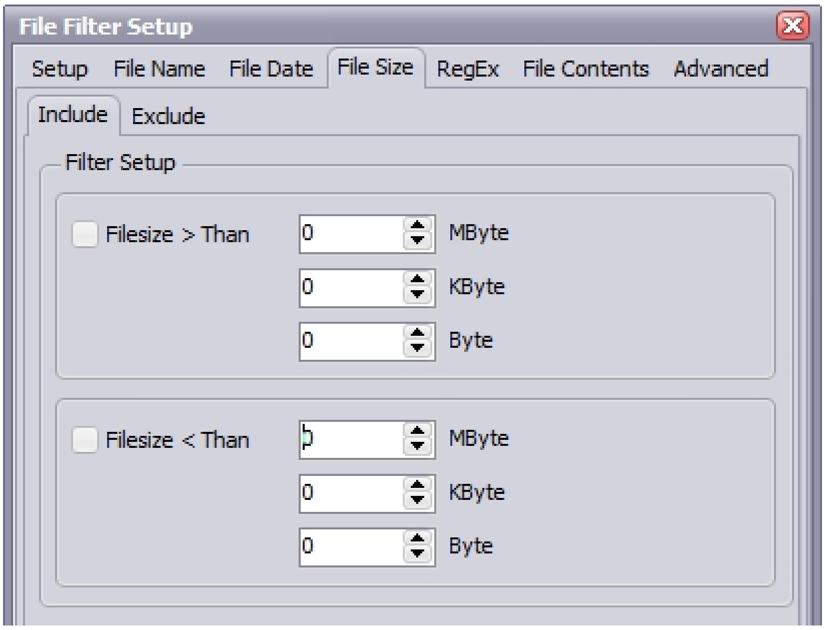
○ DateTime Relative
○ Date Relative
● Date Absolute

Advanced Filter Options

☐ Use current UTC instead of local time to compare

- File Date Include Filter: Scan will only pick up files which file dates are validated by this filter.
- File Date Exclude Filter: Scan will not pick up files which file dates are validated by this filter.

File Size Options



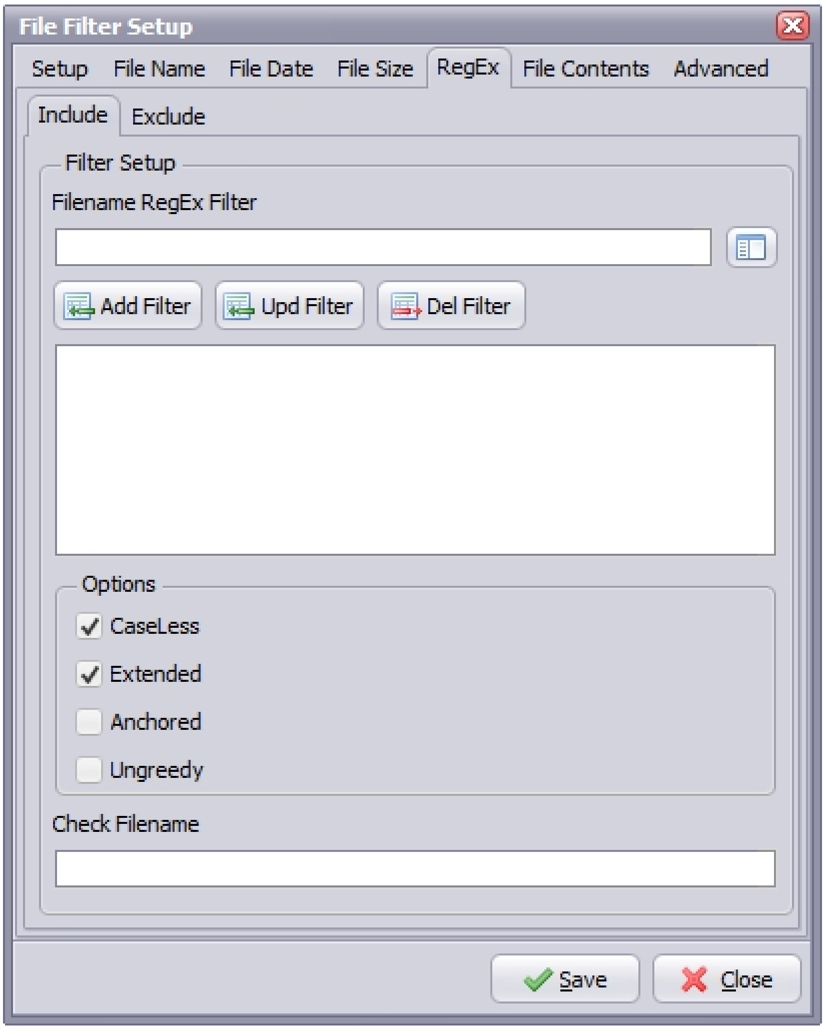
Filter Setup

☐ Filesize > Than 0 MByte
0 KByte
0 Byte

☐ Filesize < Than 0 MByte
0 KByte
0 Byte

- Filesize Include Filter: Scan will only pick up files which file size are validated by this filter.
- Filesize Exclude Filter: Scan will not pick up files which file size are validated by this filter.

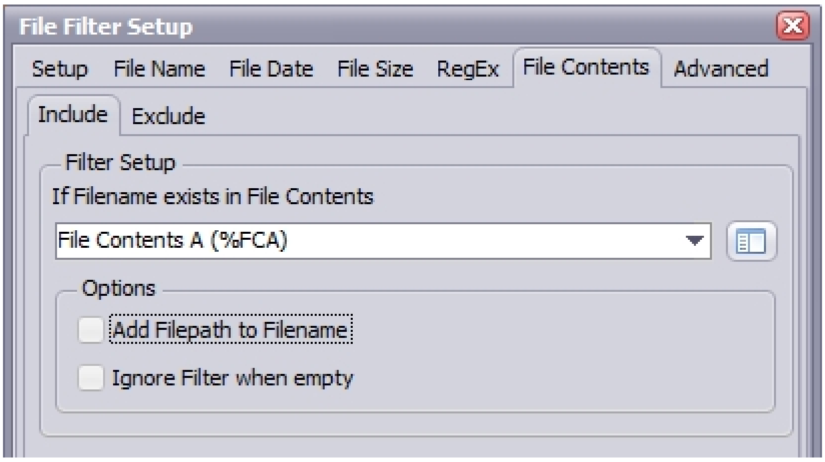
RegEx Options



☑ CaseLess
☑ Extended
□ Anchored
□ Ungreedy

- Filename RegEx Include Filter: Scan will only pick up files using this RegEx filter(s).
- Filename RegEx Exclude Filter: Scan will not pick up files using this RegEx filter(s).

File Contents Options



If Filename exists in File Contents: File Contents A (%FCA)

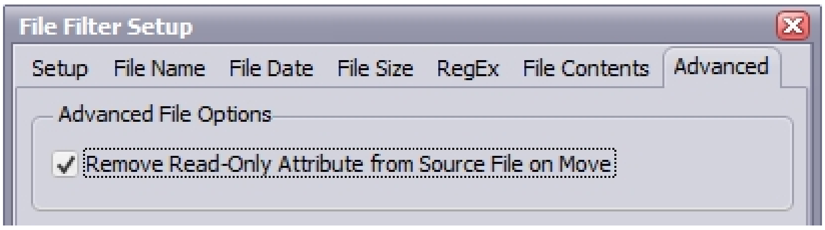
□ Add Filepath to Filename
□ Ignore Filter when empty

- File Contents Include Filter: Scan will only pick up files which exists in the selected File Contents.
- File Contents Exclude Filter: Scan will not pick up files which exists in the selected File Contents.

This filter is used together with the File Contents parameters. Please check the Rule Parameters option.

- Add File Path to Filename: Add source path to filename when checking the selected File Contents.
- Ignore Filter when empty: Filter will be ignored when the selected File Contents is empty.

Advanced Options



Advanced File Options

☑ Remove Read-Only Attribute from Source File on Move

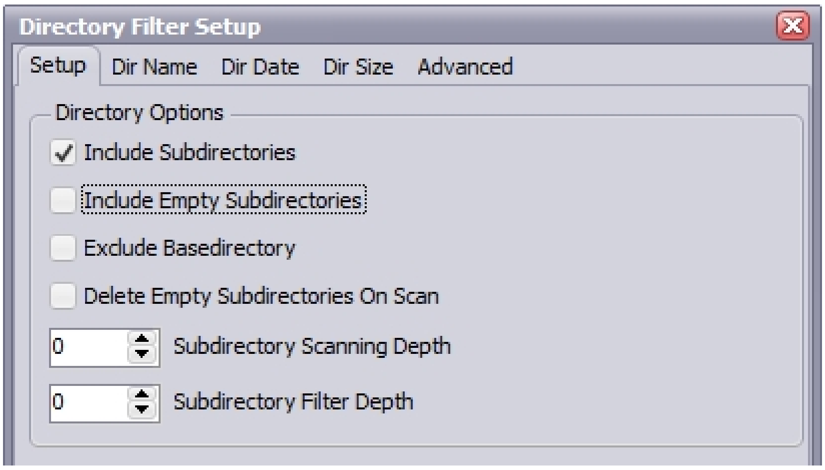
- Remove Read-Only Attribute from Source File on Move: Default setting is to remove the read-only attribute of the source file when the function is set to Move and Source is WIN.

Dir Filter

Directory Filter Setup

Add / Update Directory Filter. For each filter type we have an include and exclude setup available. Exclude priority is higher than include.

Setup Options



Directory Options

☑ Include Subdirectories

□ Include Empty Subdirectories

□ Exclude Basedirectory

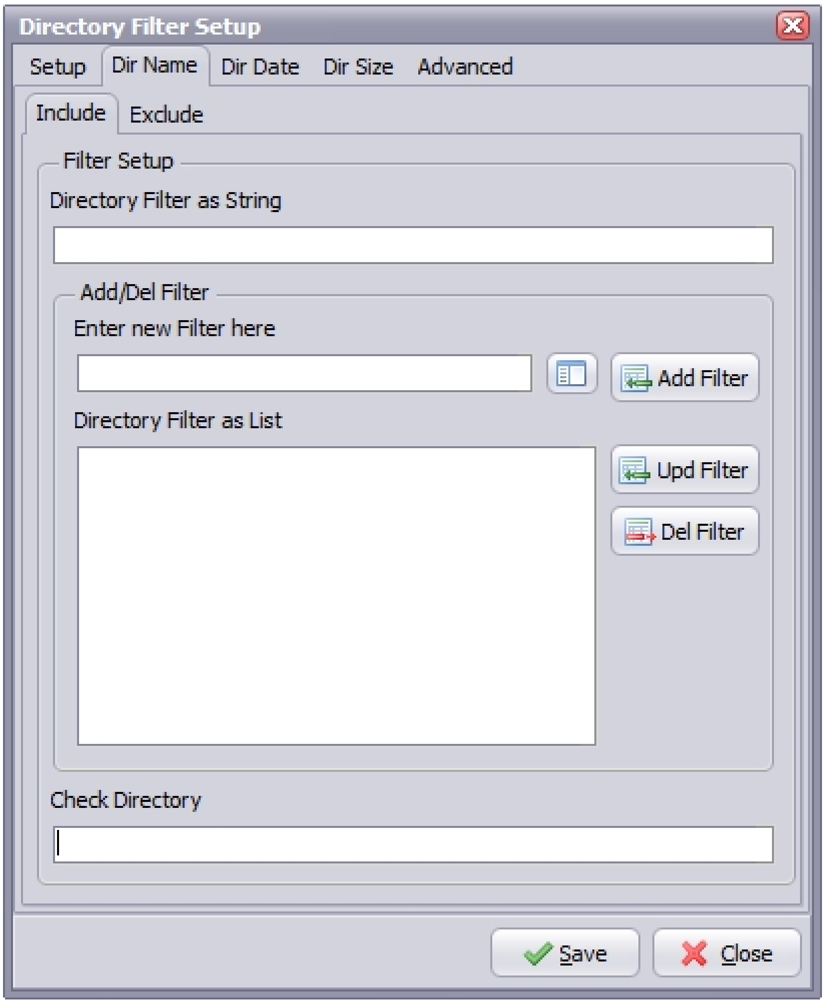
□ Delete Empty Subdirectories On Scan

0 Subdirectory Scanning Depth

0 Subdirectory Filter Depth

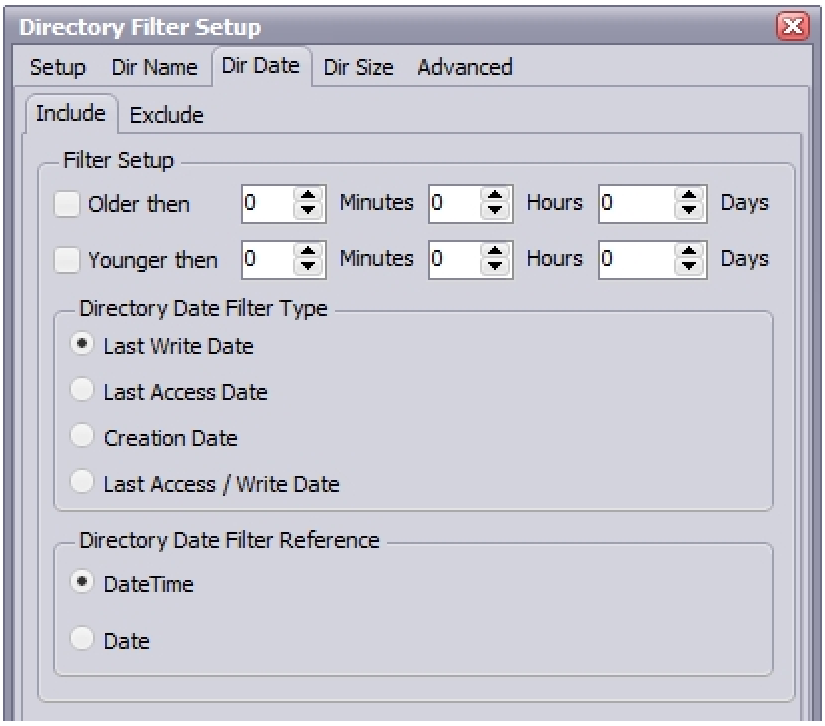
- Include Subdirectories: Include source subdirectories when scanning.
- Include Empty Subdirectories: With empty we mean no files or no files found due to file filter. Enable this option if you want to copy the complete folder structure from source to destination.
- Exclude Basedirectory: Exclude base 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):

Dir Name Options



- Subdirectory Name Include Filter: Rule will scan directories which name are validated by this filter.
- Subdirectory Name Exclude Filter: Rule will not scan directories which name are validated by this filter.

Dir Date Options



□ Older then 0 Minutes 0 Hours 0 Days

□ Younger then 0 Minutes 0 Hours 0 Days

Directory Date Filter Type

● Last Write Date
○ Last Access Date
○ Creation Date
○ Last Access / Write Date

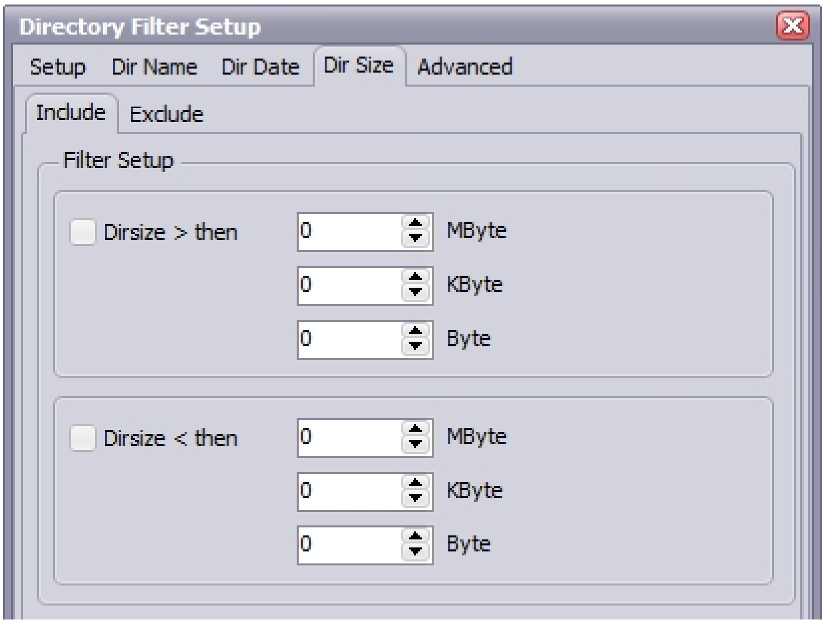
Directory Date Filter Reference

● DateTime
○ Date

- Subdirectory Date Include Filter: Rule will scan directories which date are validated by this filter.

- Subdirectory Date Exclude Filter: Rule will not scan directories which date are validated by this filter.

Dir Size Options

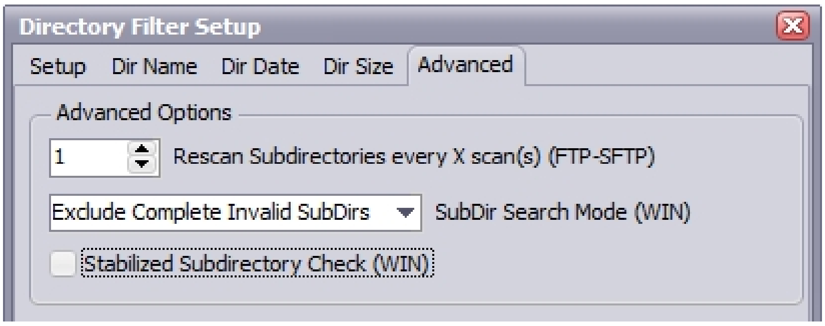


□ Dirsize > then 0 MByte, 0 KByte, 0 Byte

□ Dirsize < then 0 MByte, 0 KByte, 0 Byte

- Subdirectory Size Include Filter: Rule will scan directories which size are validated by this filter.
- Subdirectory Size Exclude Filter: Rule will not scan directories which size are validated by this filter.

Advanced Options



1 Rescan Subdirectories every X scan(s) (FTP-SFTP)

Exclude Complete Invalid SubDirs SubDir Search Mode (WIN)

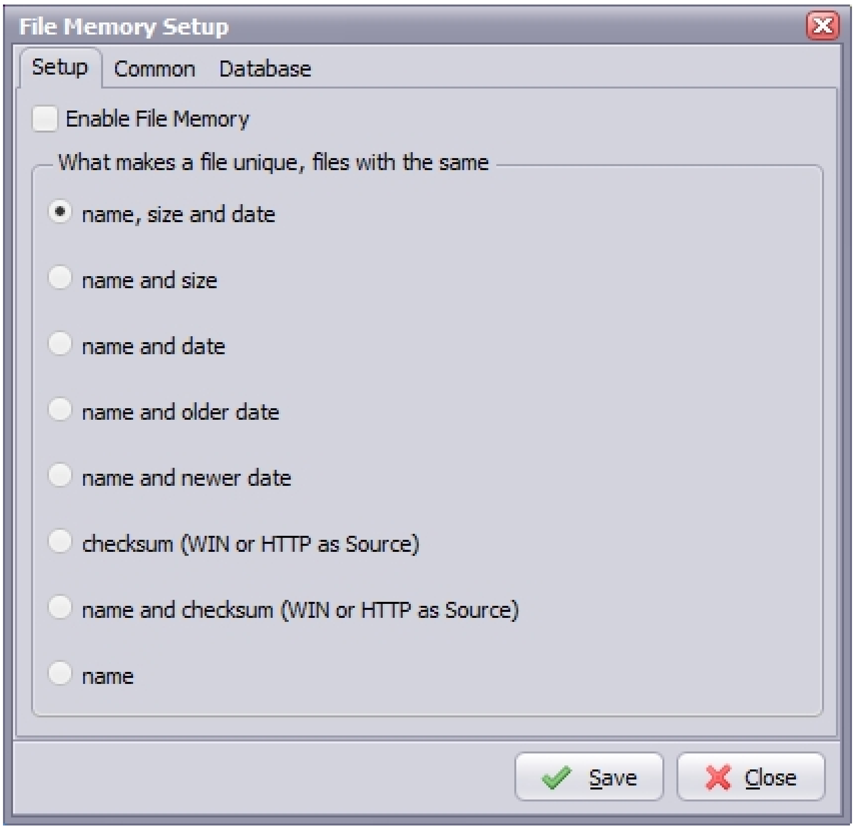
□ Stabilized Subdirectory Check (WIN)

- Rescan Subdirectories every X scan(s) (FTP-SFTP): Rescan Subdirectories every X scan(s)
- SubDir Search Mode (WIN):
    - Exclude Invalid SubDirs: Search in sub-directories. Do not search in an invalid directory, but do search in the sub-directories of an invalid directory.
    - Exclude Complete Invalid SubDirs: Search in sub-directories. Do not search in an invalid directory, and the sub-directories of an invalid directory.
- Stabilized Subdirectory Check (WIN): Scan will wait until the subdirectory is stabilized (not growing). An extra scan is needed to check if the subdirectory is still growing or not. This will double the actual scan time.

Memory

Memory Setup

Setup Options



□ Enable File Memory

What makes a file unique, files with the same

● name, size and date

○ name and size

○ name and date

○ name and older date

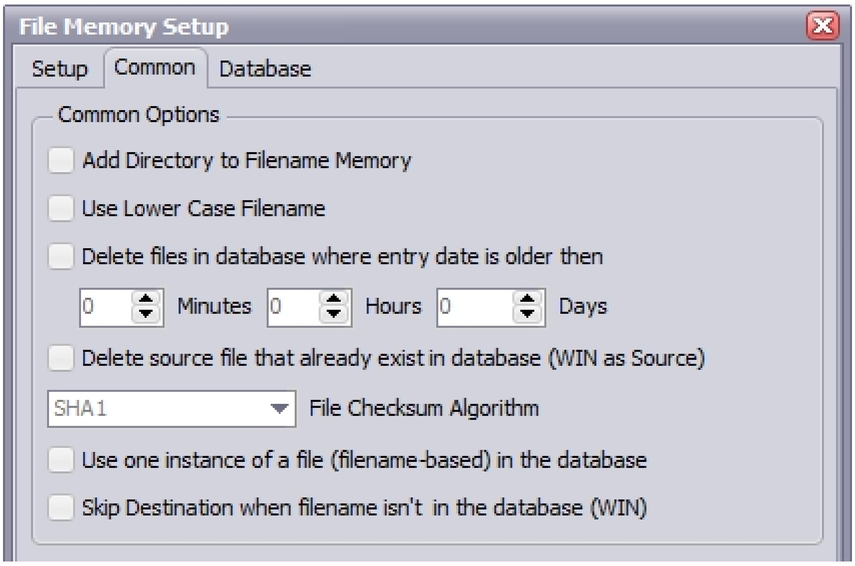
○ name and newer date

○ checksum (WIN or HTTP as Source)

○ name and checksum (WIN or HTTP as Source)

○ name

- 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.



Common Options

□ Add Directory to Filename Memory

□ Use Lower Case Filename

□ Delete files in database where entry date is older then

0 Minutes 0 Hours 0 Days

□ Delete source file that already exist in database (WIN as Source)

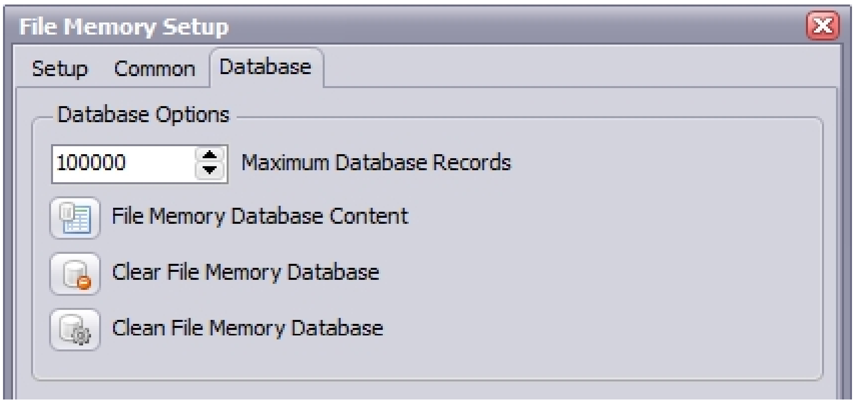
SHA1 File Checksum Algorithm

□ Use one instance of a file (filename-based) in the database

□ Skip Destination when filename isn't in the database (WIN)

- 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 Setup
Setup
Common
Database
Database Options

100000 Maximum Database Records

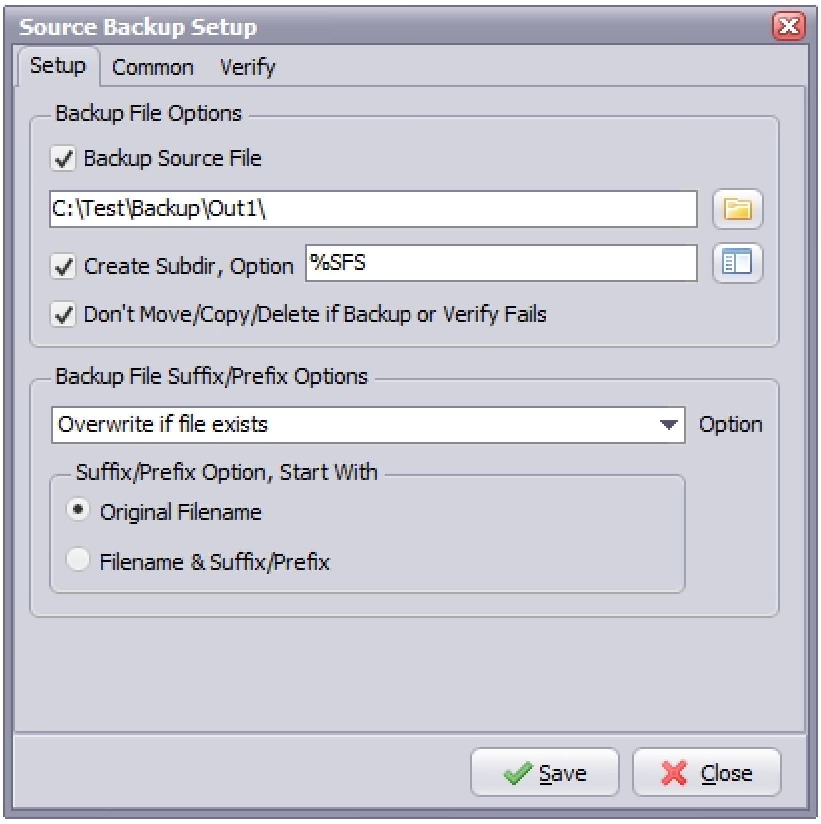
File Memory Database Content
Clear File Memory Database
Clean File Memory Database

- 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.

Backup

Source Backup Setup

Setup Options


Source Backup Setup
Setup
Common
Verify
Backup File Options

☑ Backup Source File

C:\Test\Backup\Out1\

☑ Create Subdir, Option %SFS

☑ Don't Move/Copy/Delete if Backup or Verify Fails

Backup File Suffix/Prefix Options

Option: Overwrite if file exists

Suffix/Prefix Option, Start With

● Original Filename

○ Filename & Suffix/Prefix

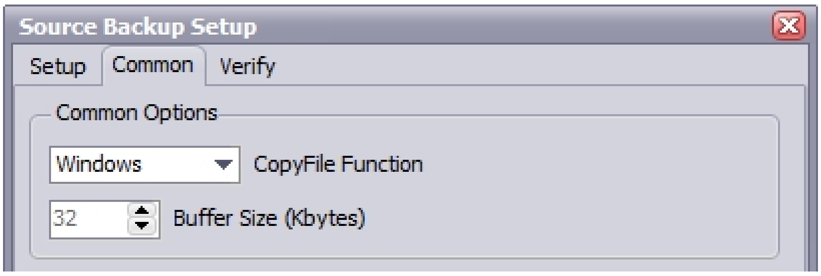
- Backup Source File: Enable this to backup the original source file before doing the actual function.
- Don't Move/Copy/Del if Backup or Verify Fails: No move/copy/delete to destination in case of backup or verify error. The actual function won't be triggered.

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.txt.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.txt").
- Add version number prefix if file exists: Version number prefix will be added if backup file already exists (i.e. "1.filename.txt").
- Add date time sufffix if file exists: Date time suffix will be added if backup 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 backup 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 backup file already exists (i.e. "20131116114801.filename.txt"). Format date time used: "YYYYMMDDHHNNSS".

- Suffix/Prefix Option, Start With
  - Original Filename: First backup will be the original filename when suffix/prefix option in chosen (i.e. "filename.txt").
  - Filename & Suffix/Prefix: First backup will be the original filename & suffix/prefix when suffix/prefix option in chosen (i.e. "filename.txt.1").

Common Options



Common Options

Windows ▼ CopyFile Function

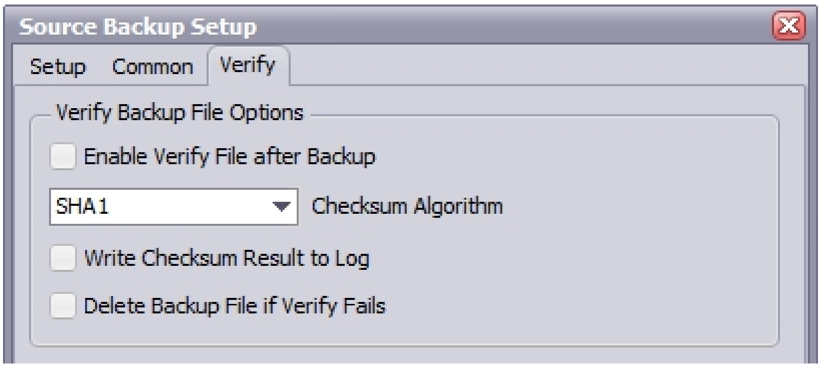
32 Buffer Size (Kbytes)

- 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



Verify Backup File Options

□ Enable Verify File after Backup

SHA1 ▼ Checksum Algorithm

□ Write Checksum Result to Log

□ Delete Backup File if Verify Fails

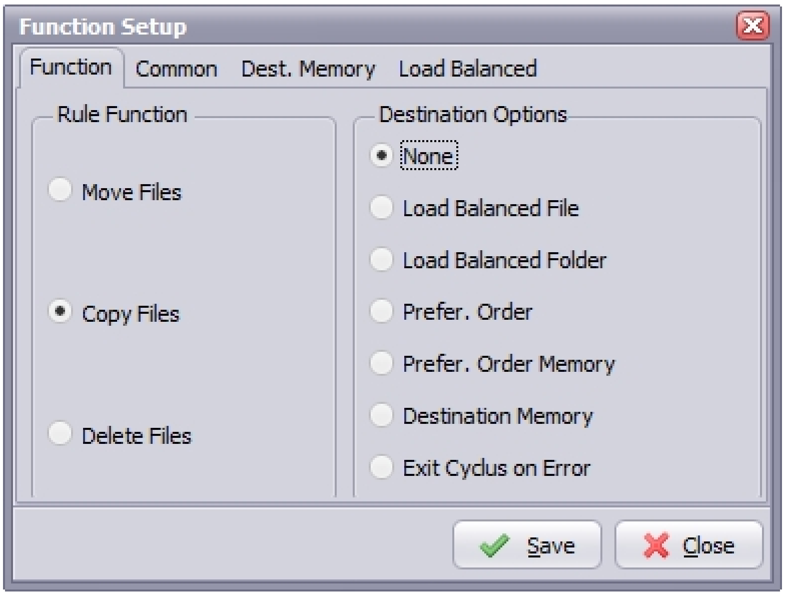
- Enable Verify File after Backup: Compares source and backup files for verified transfer integrity.
- Checksum Algorithm: Checksum Algorithm used for verified WIN transfer integrity (SHA1, MD5, ...).
- Write Checksum Result to Log: The Checksum result will be written to the log file.

- Delete Backup File if Verify Fail: The backup file will be deleted if verification fails.

Function

Function Setup

Function Options



Rule Function

○ Move Files

● Copy Files

○ Delete Files

Destination Options

● None

○ Load Balanced File

○ Load Balanced Folder

○ Prefer. Order

○ Prefer. Order Memory

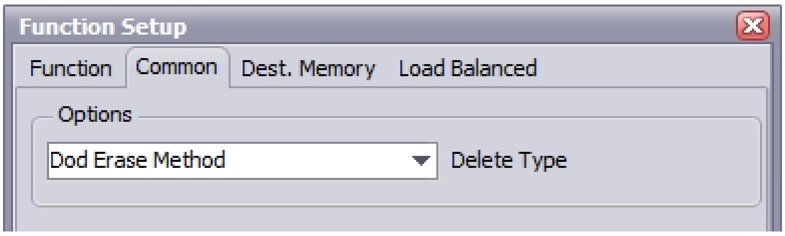
○ Destination Memory

○ Exit Cyclus on Error

Destination Options:

- Load Balanced File: Use load balancing technique with destinations. You need more then 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 then 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 then 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 then 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.
- Exit Cyclus on Error: Break/exit the destination output cyclus on error. This only works with multiple destinations. Output to the next destination will be interrupted when an error occurs.

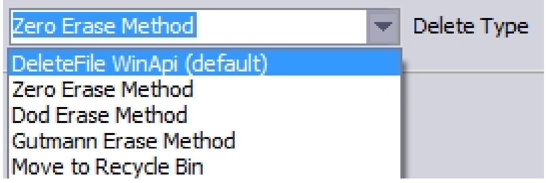
Common Options



Options

Delete Type: Dod Erase Method

- Delete Type: Method that will be used to erase files.

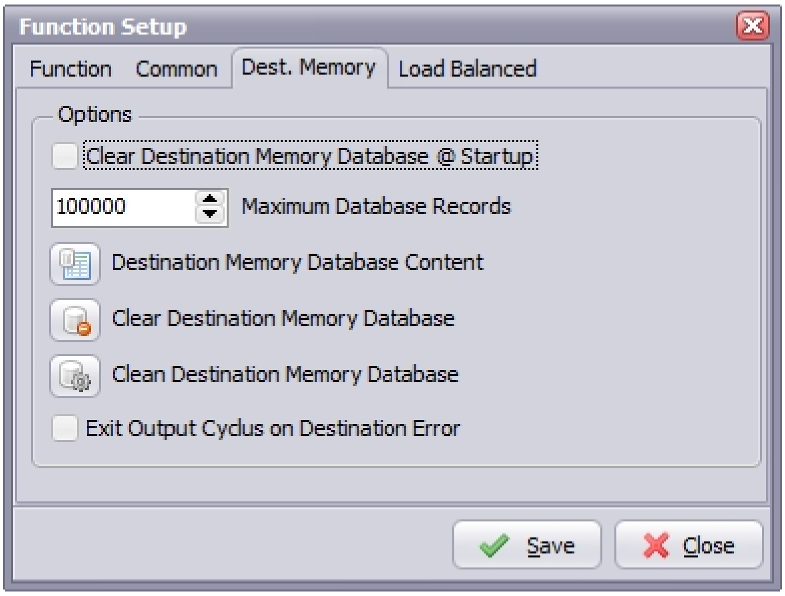


Zero Erase Method ▾ Delete Type

- DeleteFile WinApi (default)
- Zero Erase Method
- Dod Erase Method
- Gutmann Erase Method
- Move to Recycle Bin

https://en.wikipedia.org/wiki/Data_erasure

Destination Memory Options



Options

□ Clear Destination Memory Database @ Startup

100000 Maximum Database Records

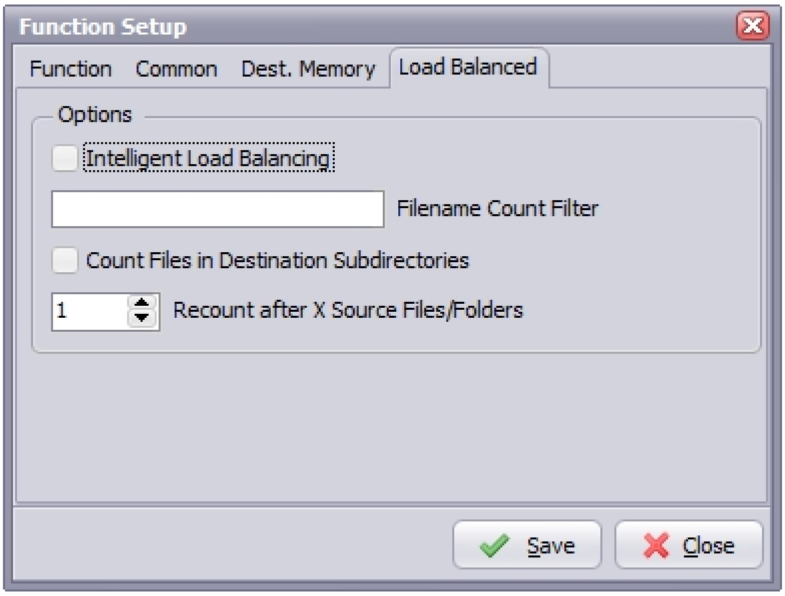
Destination Memory Database Content

Clear Destination Memory Database

Clean Destination Memory Database

□ Exit Output Cyclus on Destination Error

Load Balancing Options



Options

□ Intelligent Load Balancing

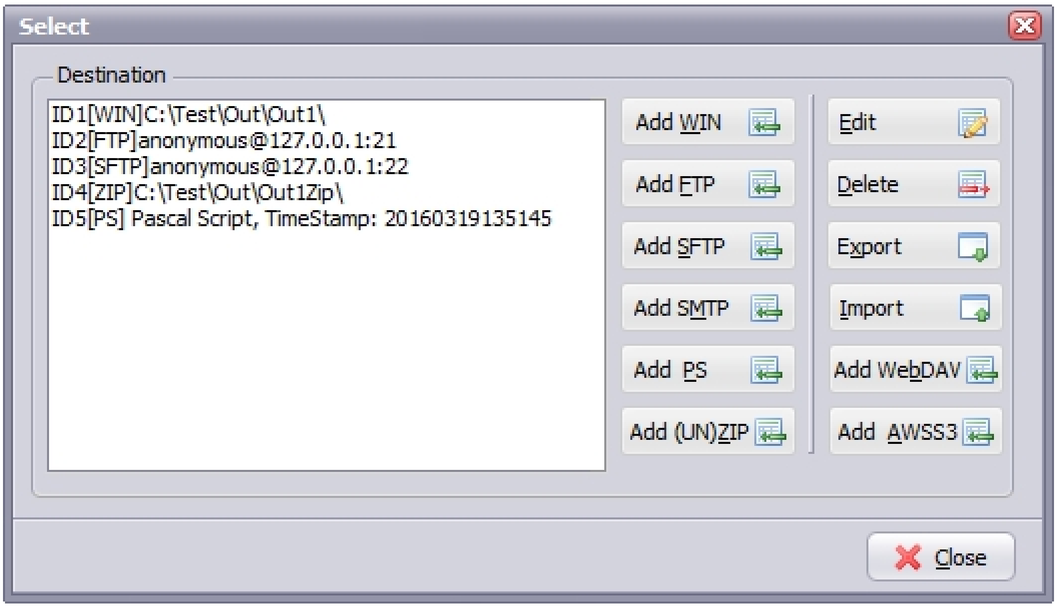
Filename Count Filter

□ Count Files in Destination Subdirectories

1 Recount after X Source Files/Folders

Destination Options

Destination Selection



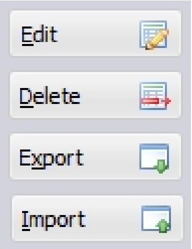
ID1[WIN]C:\Test\Out\Out1\
ID2[FTP]anonymous@127.0.0.1:21
ID3[SFTP]anonymous@127.0.0.1:22
ID4[ZIP]C:\Test\Out\Out1Zip\
ID5[PS] Pascal Script, TimeStamp: 20160319135145

LimagitoX Destination possibilities:

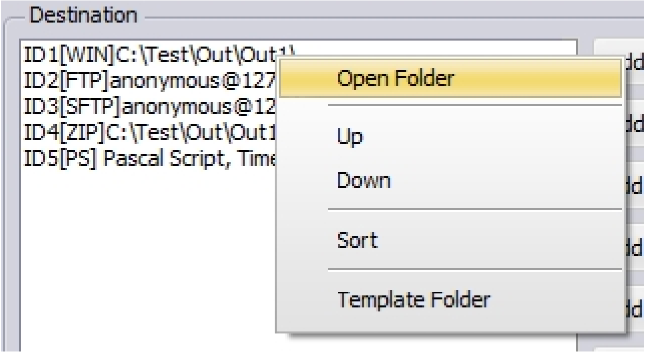
- WIN
- FTP
- SFTP
- SMTP
- PS
- ZIP
- WebDAV
- AWSS3

WebDAV and AWSS3 are part of the +PLUS Option Pack License. Both destinations are available in the Free Lite version so they can be fully evaluated before purchasing.

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

- 

  - Select 'Edit' to open the setup screen of the selected Destination.
  - Select 'Delete' to remove the selected Destination.
  - Select 'Export' to export the setup of the selected Destination (template as ini file).
  - Select 'Import' to import a new destination from an ini template file.

- 

ID1[WIN]C:\Test\Out\Out1\
ID2[FTP]anonymous@127
ID3[SFTP]anonymous@12
ID4[ZIP]C:\Test\Out\Out1
ID5[PS] Pascal Script, Time

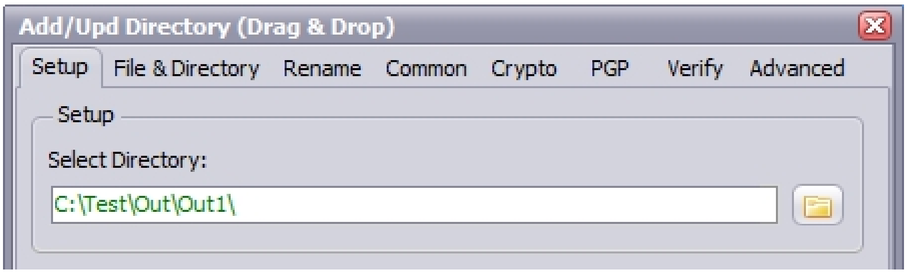
Right click on the selected destination to:

- Open Folder: Open and explore the destination folder (WIN, FTP, SFTP)
- Up/Down: Change entry position in the destination list view
- Sort: Sort the destination list view
- Template Folder: Open and explore the template folder (Export Folder)

WIN Destination

WIN Destination Setup

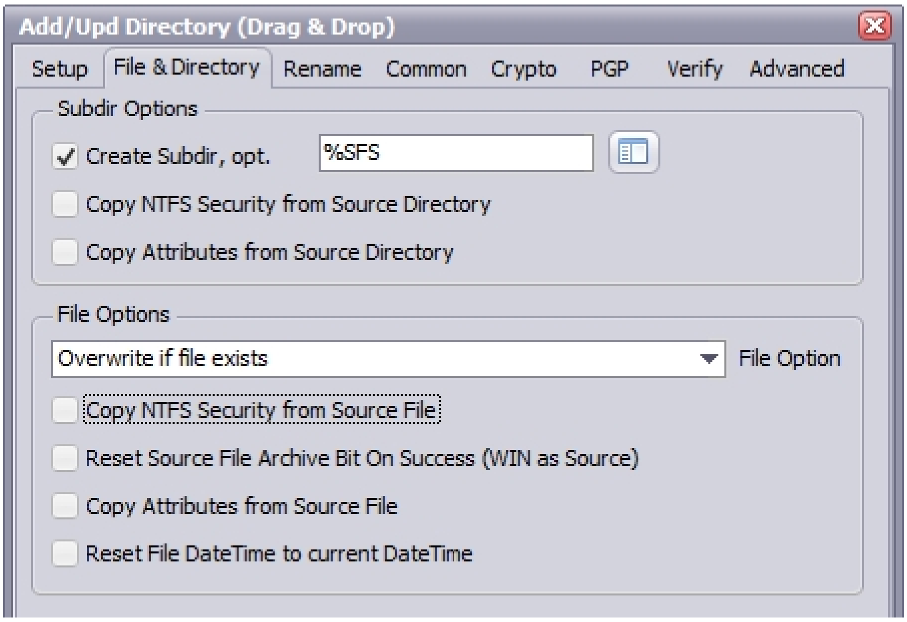
Setup Options



Select Directory: C:\Test\Out\Out1\

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

File & Directory Options



☑ Create Subdir, opt. %SFS

□ Copy NTFS Security from Source Directory

□ Copy Attributes from Source Directory

Overwrite if file exists — File Option

□ Copy NTFS Security from Source File

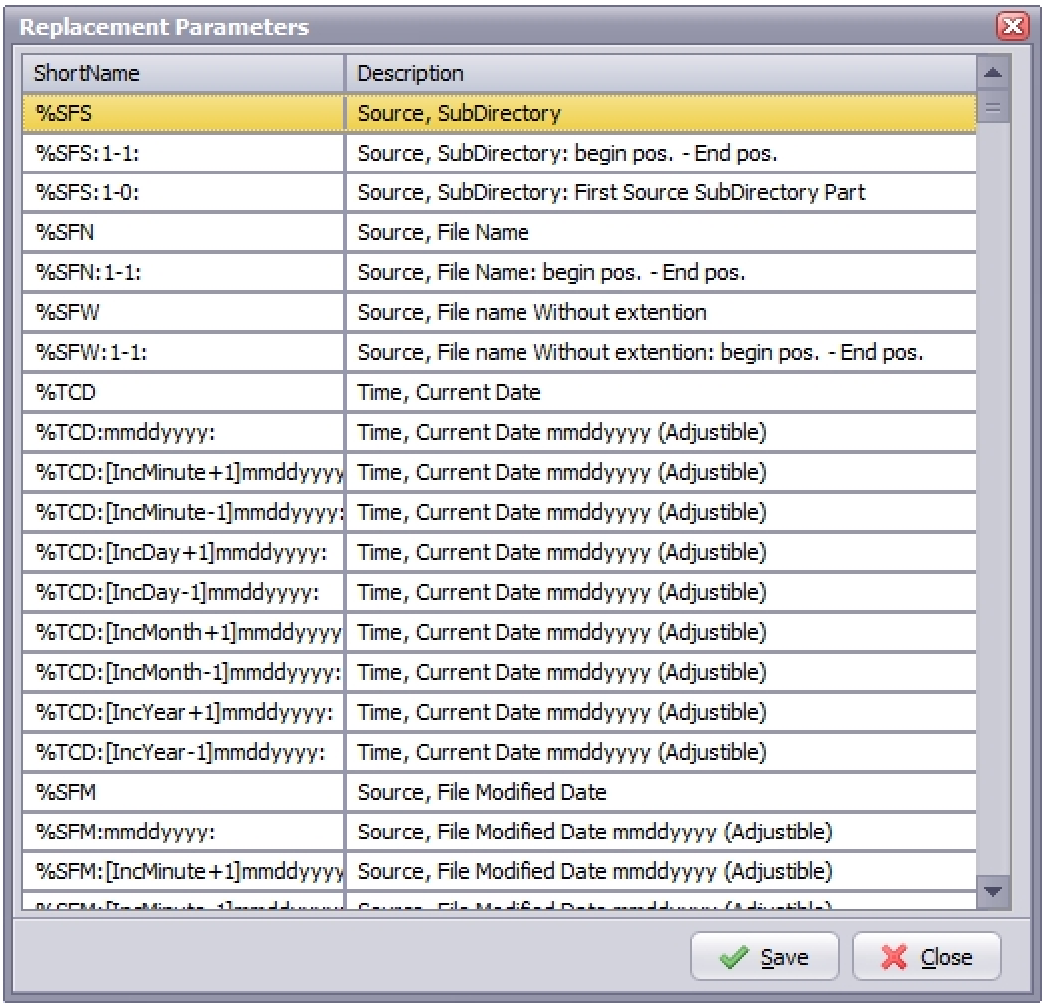
□ Reset Source File Archive Bit On Success (WIN as Source)

□ Copy Attributes from Source File

□ Reset File DateTime to current DateTime

Subdir Options

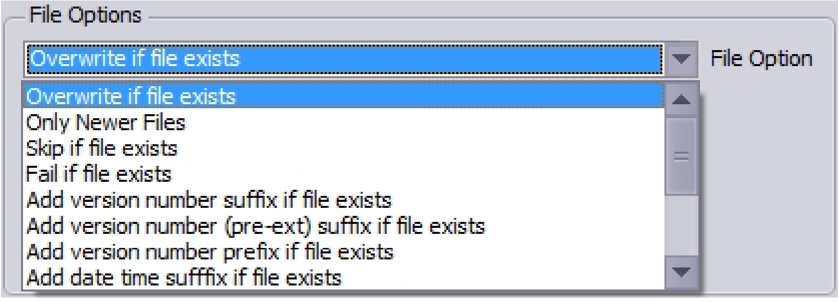
- Create Subdir: Create Subdirectory for the Windows destination.
- Create Subdir, option: Different parameters can be used to create the destination directory.



Replacement Parameters

ShortName	Description
%SFS	Source, SubDirectory
%SFS:1-1:	Source, SubDirectory: begin pos. - End pos.
%SFS:1-0:	Source, SubDirectory: First Source SubDirectory Part
%SFN	Source, File Name
%SFN:1-1:	Source, File Name: begin pos. - End pos.
%SFW	Source, File name Without extention
%SFW:1-1:	Source, File name Without extention: begin pos. - End pos.
%TCD	Time, Current Date
%TCD:mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncMinute+1]mmddyyyy	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncMinute-1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncDay+1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncDay-1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncMonth+1]mmddyyyy	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncMonth-1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncYear+1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncYear-1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%SFM	Source, File Modified Date
%SFM:mmddyyyy:	Source, File Modified Date mmddyyyy (Adjustible)
%SFM:[IncMinute+1]mmddyyyy	Source, File Modified Date mmddyyyy (Adjustible)
%SFM:[IncMinute-1]mmddyyyy	Source, File Modified Date mmddyyyy (Adjustible)

File Options

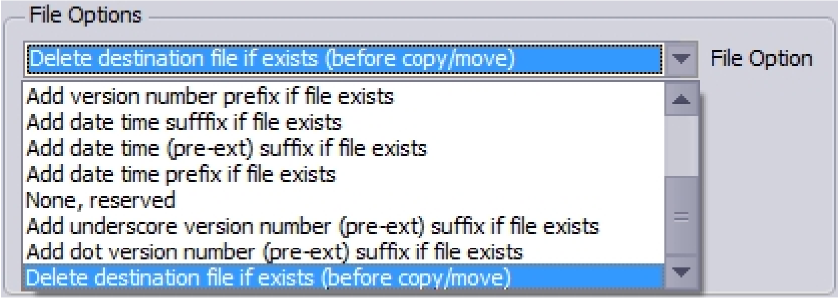


File Options

File Option: Overwrite if file exists

- Overwrite if file exists
- Only Newer Files
- Skip if file exists
- Fail if file exists
- Add version number suffix if file exists
- Add version number (pre-ext) suffix if file exists
- Add version number prefix if file exists
- Add date time sufffix if file exists

- 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 sufffix if file exists: Date time suffix will be added if destination file already exists (i.e. "filename.txt.20131116114801"). Format date time used: "YYYYMMDDHHNNSS".



File Options

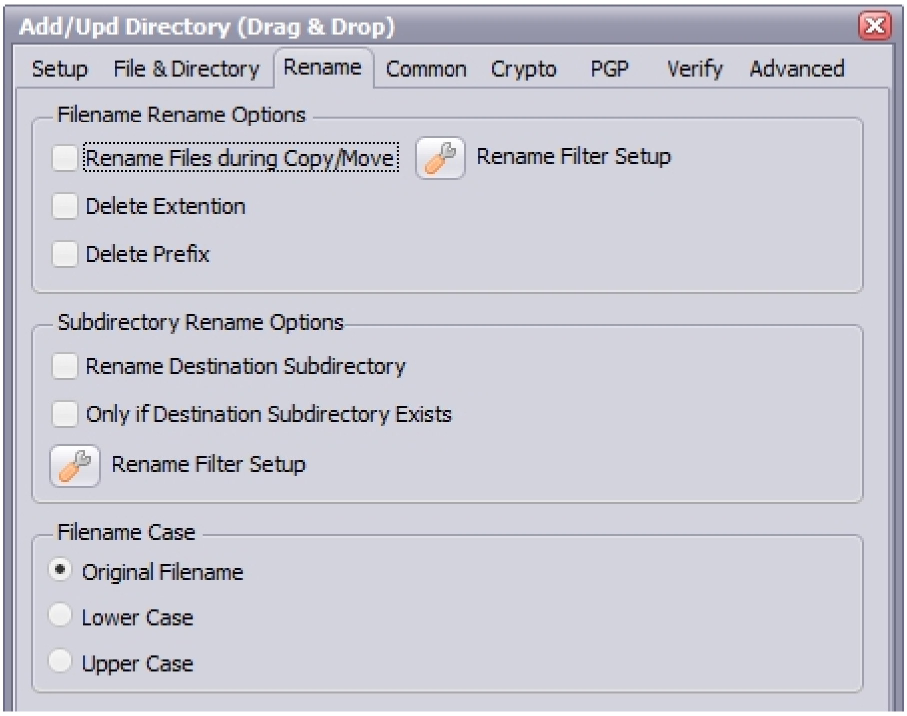
Delete destination file if exists (before copy/move) — File Option

- Add version number prefix if file exists
- Add date time sufffix if file exists
- Add date time (pre-ext) suffix if file exists
- Add date time prefix if file exists
- None, reserved
- Add underscore version number (pre-ext) suffix if file exists
- Add dot version number (pre-ext) suffix if file exists
- Delete destination file if exists (before copy/move)

- 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".
- None, reserved
- Add underscore version number (pre-ext) suffix if file exists:
- Add dot version number (pre-ext) suffix if file exists:
- Delete destination file if exists (before copy/move): Delete the file if it already exists. Before the actual copy/move we'll check if the (source) filename exists in the destination directory and if it exists then we'll delete it first.

- 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 Extention: Delete the extention 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



Add/Upd Directory (Drag & Drop)

Setup | File & Directory | Rename | Common | Crypto | PGP | Verify | Advanced

Filename Rename Options

☐ Rename Files during Copy/Move — Rename Filter Setup

☐ Delete Extention

☐ Delete Prefix

Subdirectory Rename Options

☐ Rename Destination Subdirectory

☐ Only if Destination Subdirectory Exists

Rename Filter Setup

Filename Case

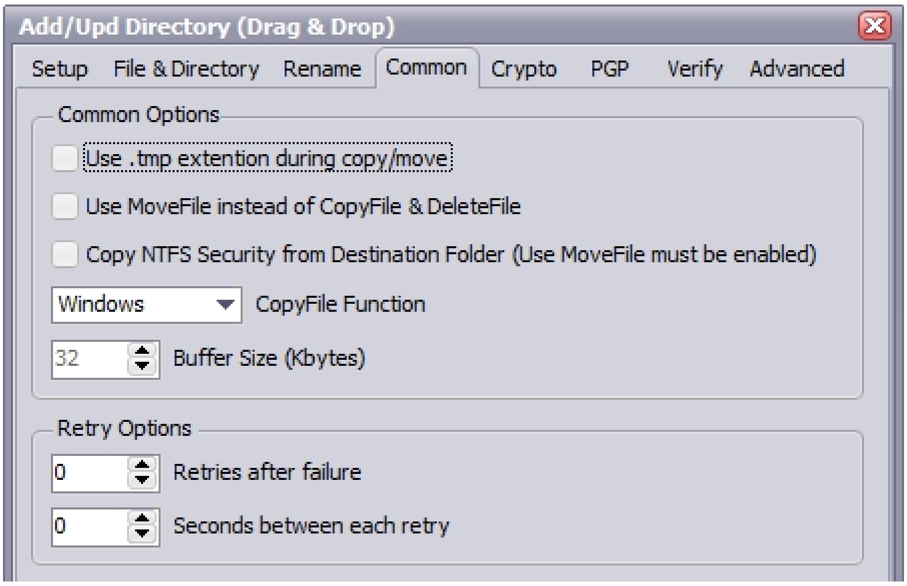
● Original Filename

○ Lower Case

○ Upper Case

- 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 .tmp extention during copy/move

□ Use MoveFile instead of CopyFile & DeleteFile

□ Copy NTFS Security from Destination Folder (Use MoveFile must be enabled)

Windows CopyFile Function

32 Buffer Size (Kbytes)

Retry Options

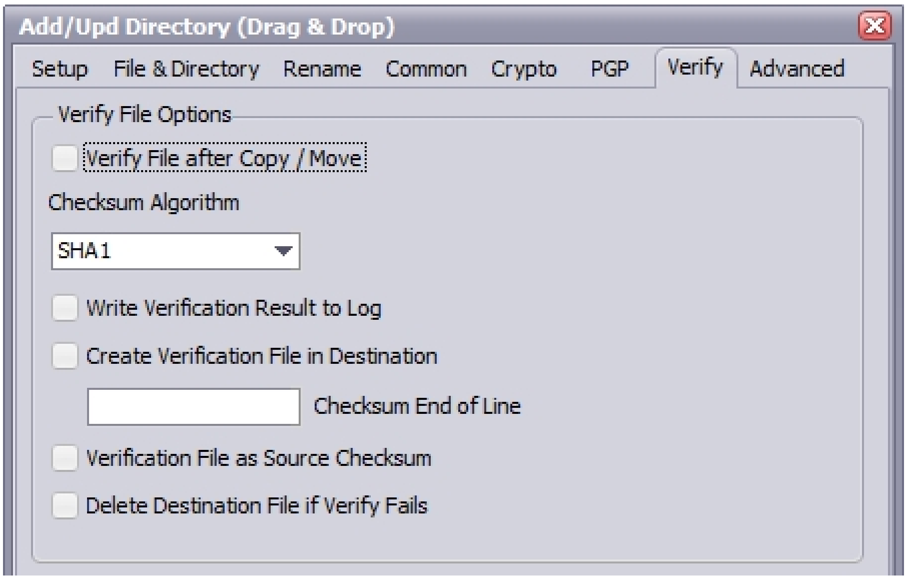
0 Retries after failure

0 Seconds between each retry

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).
- Retries after failure: Amount of retries after a copy/move failure.
- Seconds between each retry: Seconds that the rule will wait between each retry.

Verify Options



Verify File Options

□ Verify File after Copy / Move

Checksum Algorithm

SHA1

□ Write Verification Result to Log

□ Create Verification File in Destination

Checksum End of Line

□ Verification File as Source Checksum

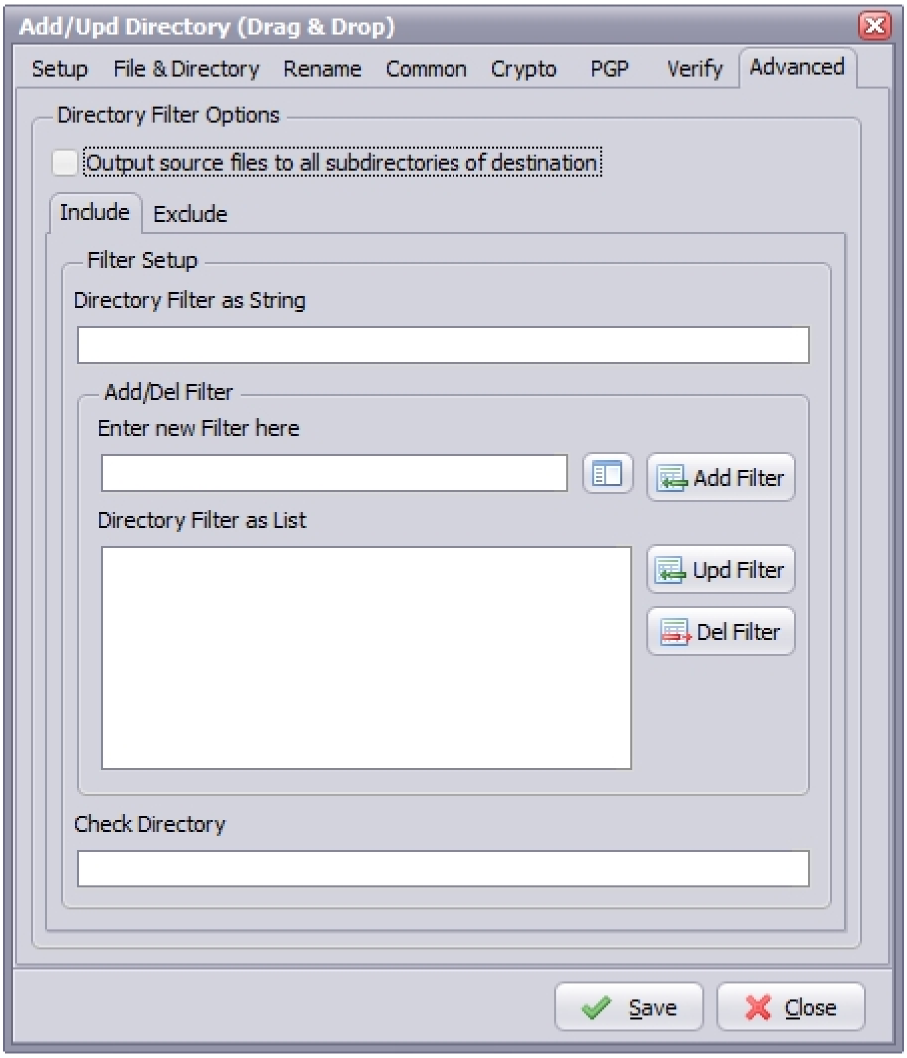
□ Delete Destination File if Verify Fails

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.

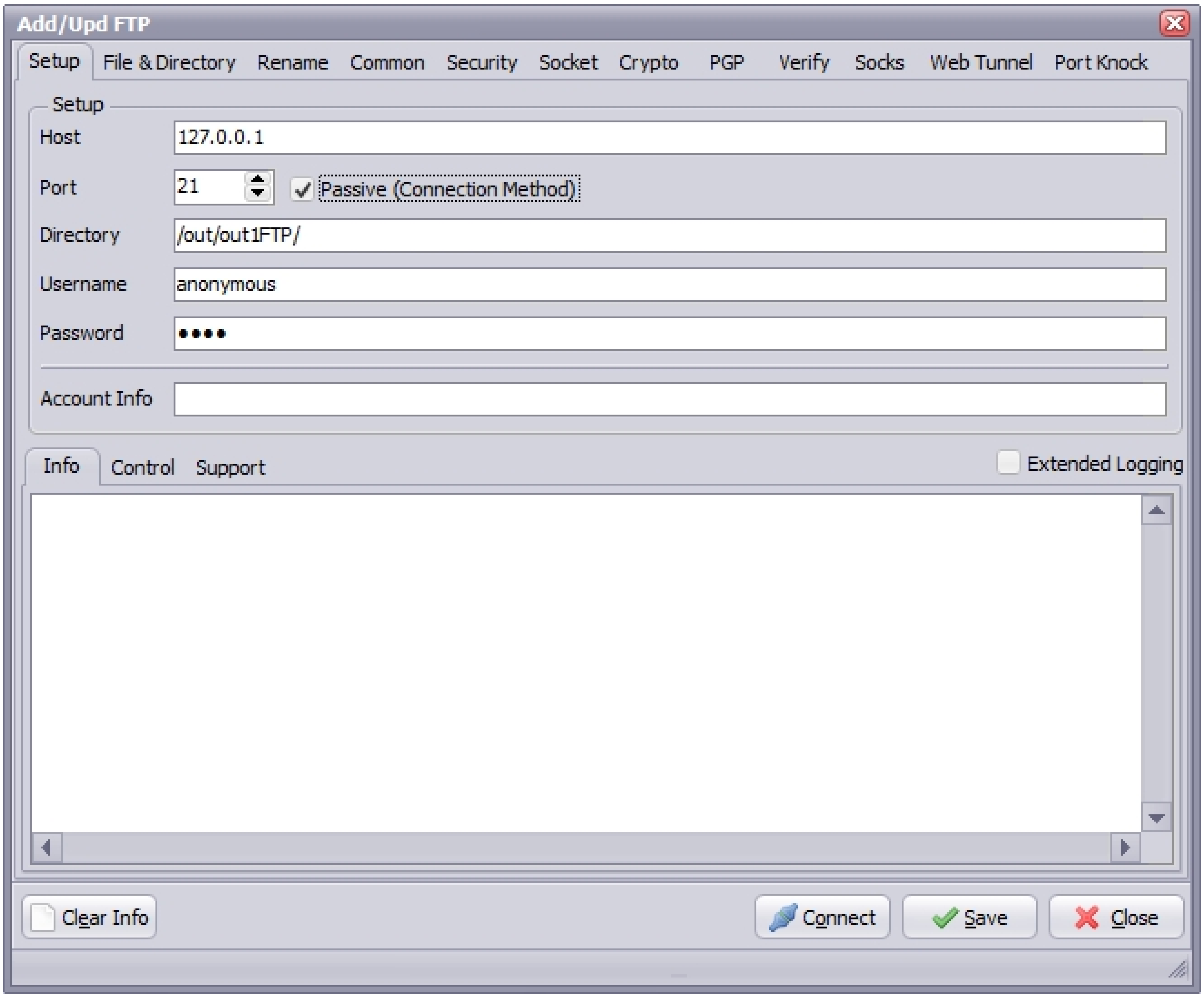
Advanced Options



FTP Destination

FTP Destination Setup

Setup Options



Setup

Host: 127.0.0.1

Port: 21 ☑ Passive (Connection Method)

Directory: /out/out1FTP/

Username: anonymous

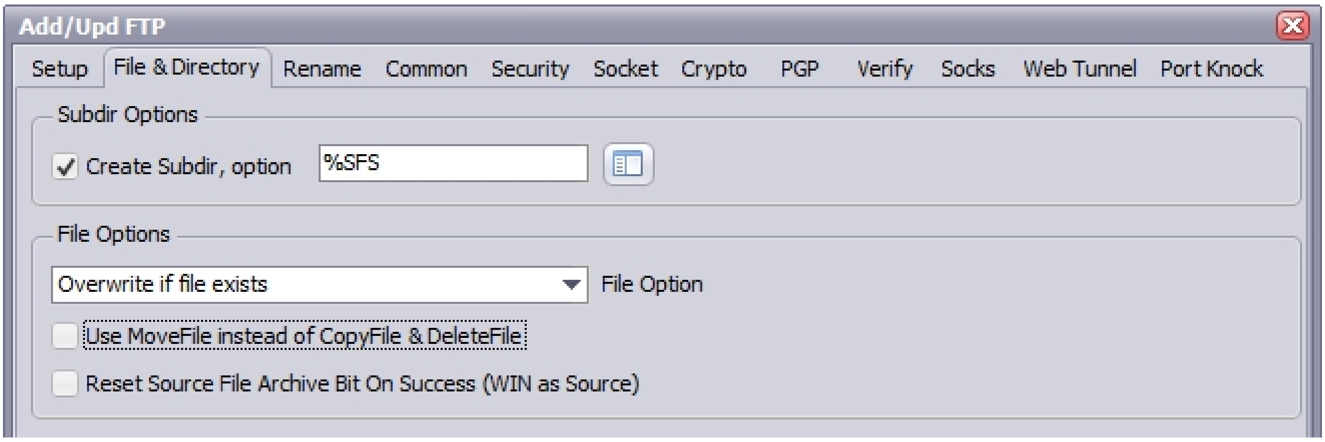
Password: ●●●●

Account Info:

☐ Extended Logging

- 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, option: %SFS

File Options

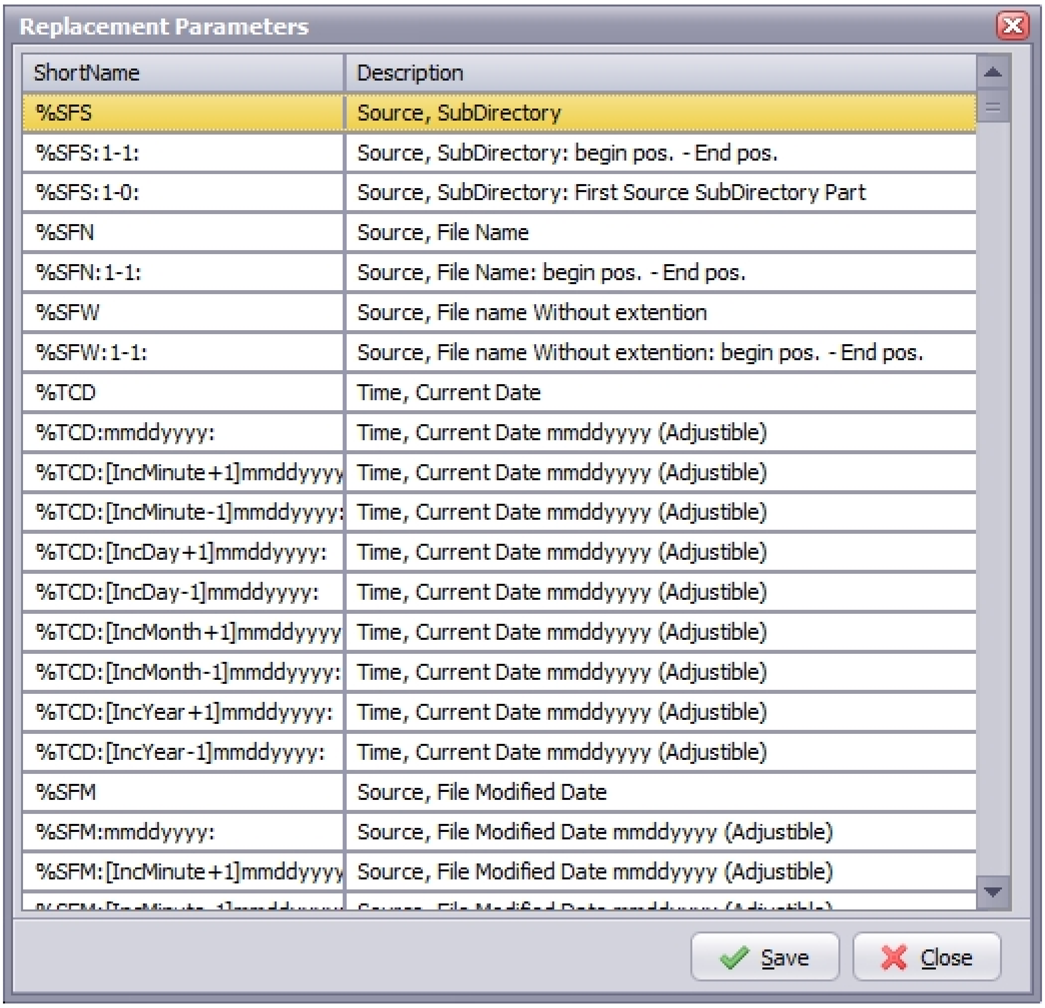
File Option: Overwrite if file exists

☐ Use MoveFile instead of CopyFile & DeleteFile

☐ Reset Source File Archive Bit On Success (WIN as Source)

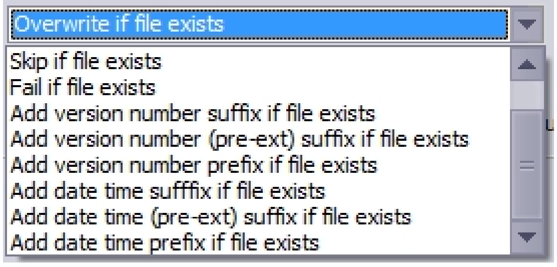
Subdir Options

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



Replacement Parameters

ShortName	Description
%SFS	Source, SubDirectory
%SFS:1-1:	Source, SubDirectory: begin pos. - End pos.
%SFS:1-0:	Source, SubDirectory: First Source SubDirectory Part
%SFN	Source, File Name
%SFN:1-1:	Source, File Name: begin pos. - End pos.
%SFW	Source, File name Without extention
%SFW:1-1:	Source, File name Without extention: begin pos. - End pos.
%TCD	Time, Current Date
%TCD:mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncMinute+1]mmddyyyy	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncMinute-1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncDay+1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncDay-1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncMonth+1]mmddyyyy	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncMonth-1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncYear+1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncYear-1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%SFM	Source, File Modified Date
%SFM:mmddyyyy:	Source, File Modified Date mmddyyyy (Adjustible)
%SFM:[IncMinute+1]mmddyyyy	Source, File Modified Date mmddyyyy (Adjustible)
%SFM:[IncMinute-1]mmddyyyy	Source, File Modified Date mmddyyyy (Adjustible)



Overwrite if file exists

Skip if file exists
Fail if file exists
Add version number suffix if file exists
Add version number (pre-ext) suffix if file exists
Add version number prefix if file exists
Add date time sufffix if file exists
Add date time (pre-ext) suffix if file exists
Add date time prefix if file exists

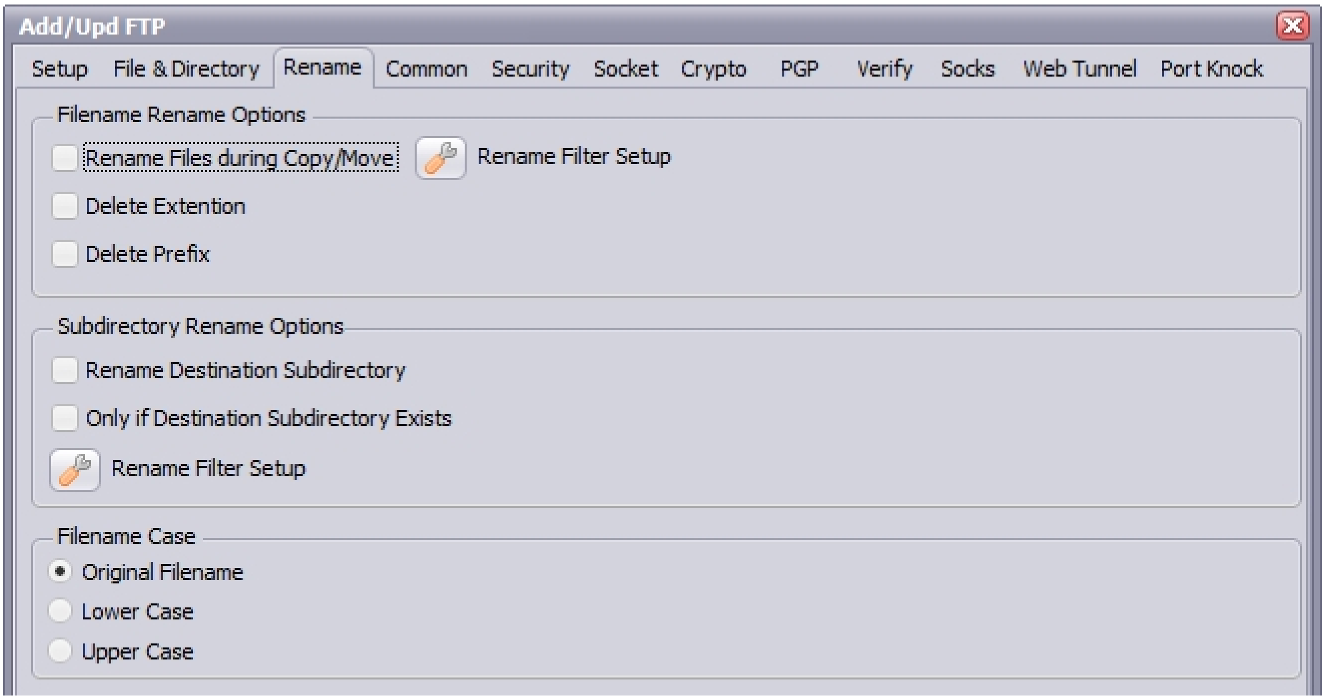
- File Options

  - 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 sufffix 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".

- 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


Add/Upd FTP

Setup | File & Directory | Rename | Common | Security | Socket | Crypto | PGP | Verify | Socks | Web Tunnel | Port Knock

Filename Rename Options

□ Rename Files during Copy/Move   Rename Filter Setup

□ Delete Extention

□ Delete Prefix

Subdirectory Rename Options

□ Rename Destination Subdirectory

□ Only if Destination Subdirectory Exists

Rename Filter Setup

Filename Case

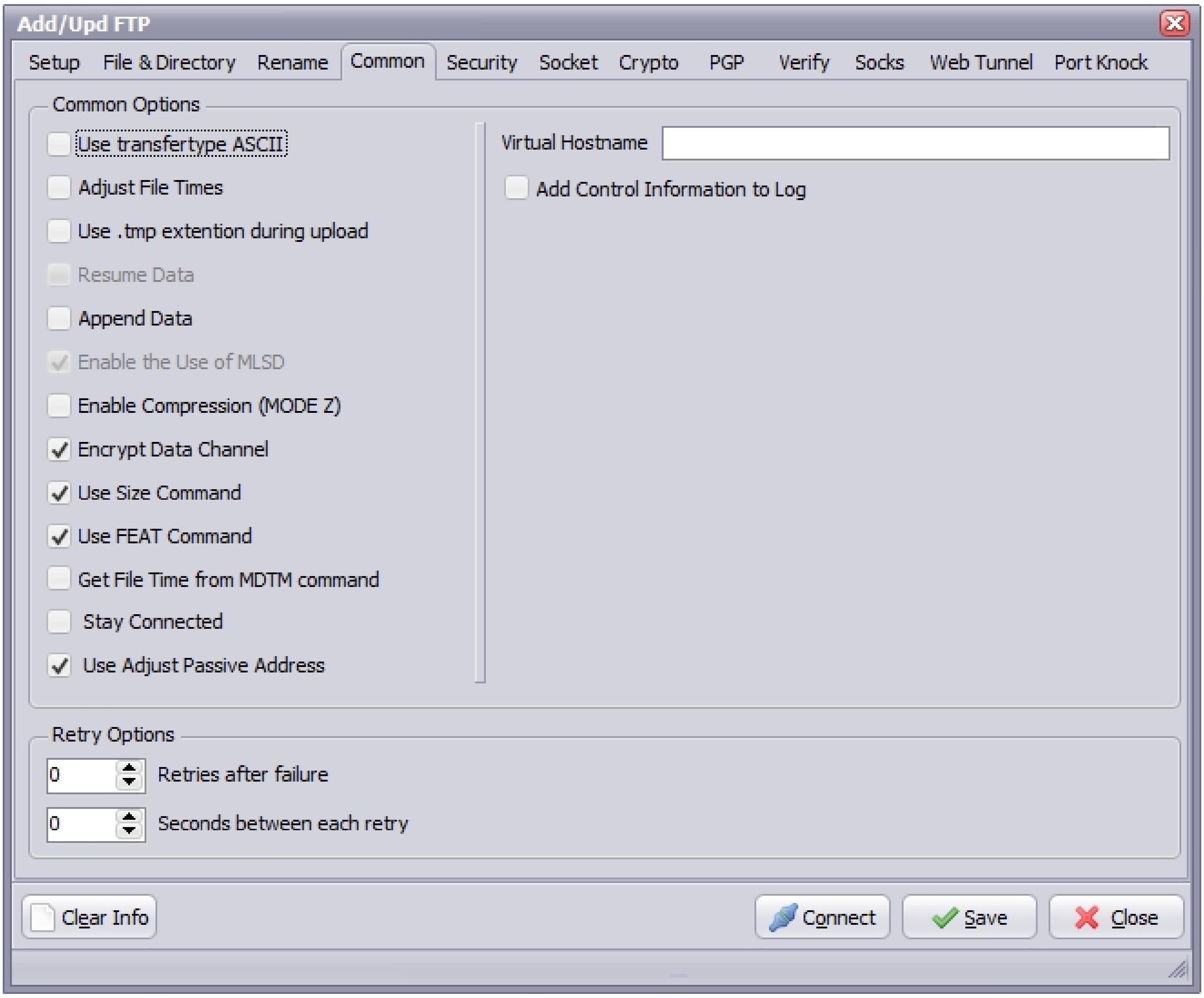
● Original Filename

○ Lower Case

○ Upper Case

- 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/
- 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 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



Add/Upd FTP

Common Options

- ☐ Use transfertype ASCII
- ☐ Adjust File Times
- ☐ Use .tmp extention during upload
- ☐ Resume Data
- ☐ Append Data
- ☑ Enable the Use of MLSD
- ☐ Enable Compression (MODE Z)
- ☑ Encrypt Data Channel
- ☑ Use Size Command
- ☑ Use FEAT Command
- ☐ Get File Time from MDTM command
- ☐ Stay Connected
- ☑ Use Adjust Passive Address

Virtual Hostname:

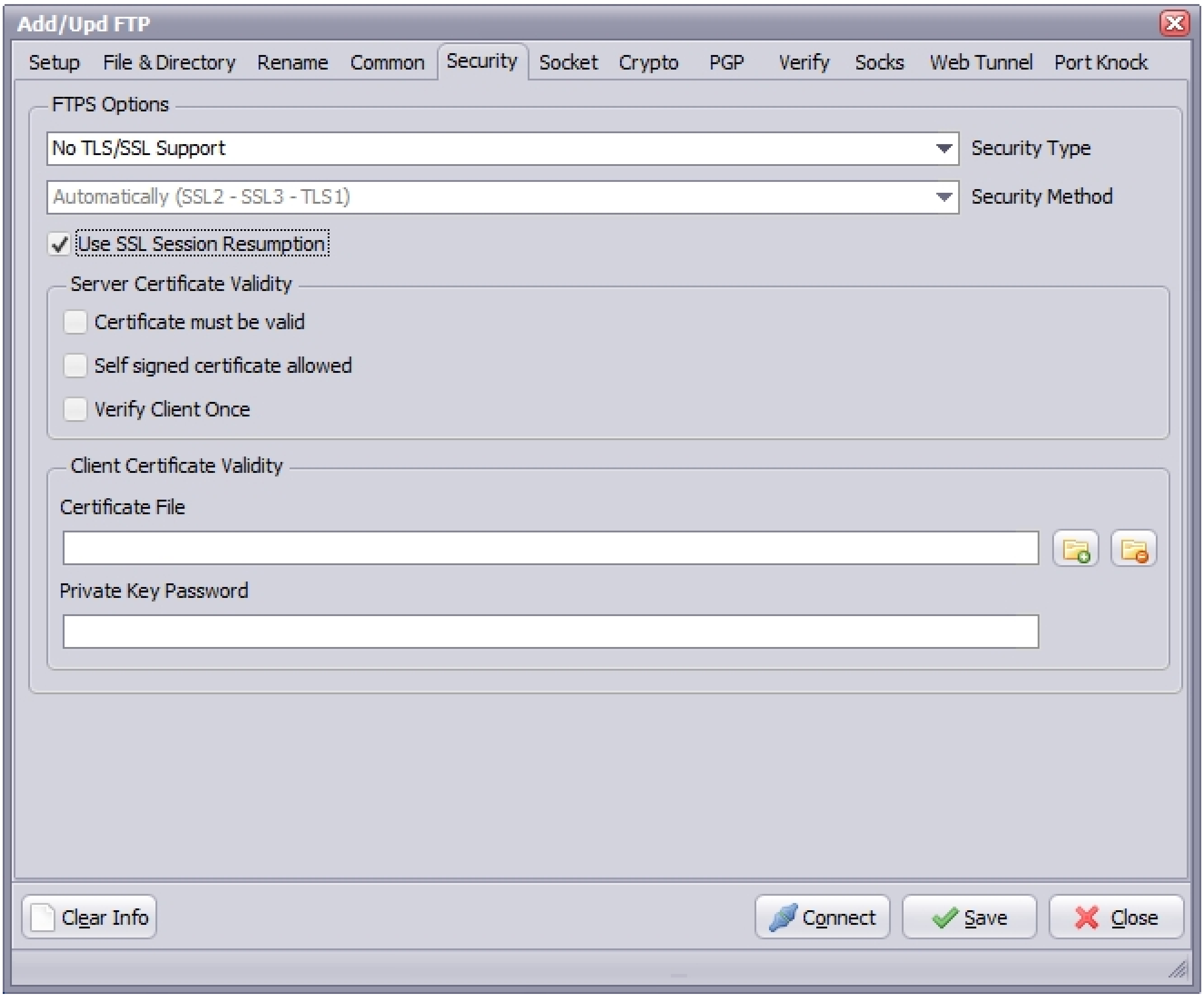
- ☐ Add Control Information to Log

Retry Options

- 0 Retries after failure
- 0 Seconds between each retry

- 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.
- Virtual Hostname: Use this option to allow a server-FTP process to determine to which of possibly many virtual hosts the File Mover wishes to connect.
- Add Control Information to log: Add FTP specific control information to the log.
- Retries after failure: Amount of retries after a copy/move failure.
- Seconds between each retry: Seconds that the rule will wait between each retry.

Security Options



FTPS Options

Security Type: No TLS/SSL Support

Security Method: Automatically (SSL2 - SSL3 - TLS1)

☑ Use SSL Session Resumption

Server Certificate Validity

☐ Certificate must be valid

☐ Self signed certificate allowed

☐ Verify Client Once

Client Certificate Validity

Certificate File

Private Key Password

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.

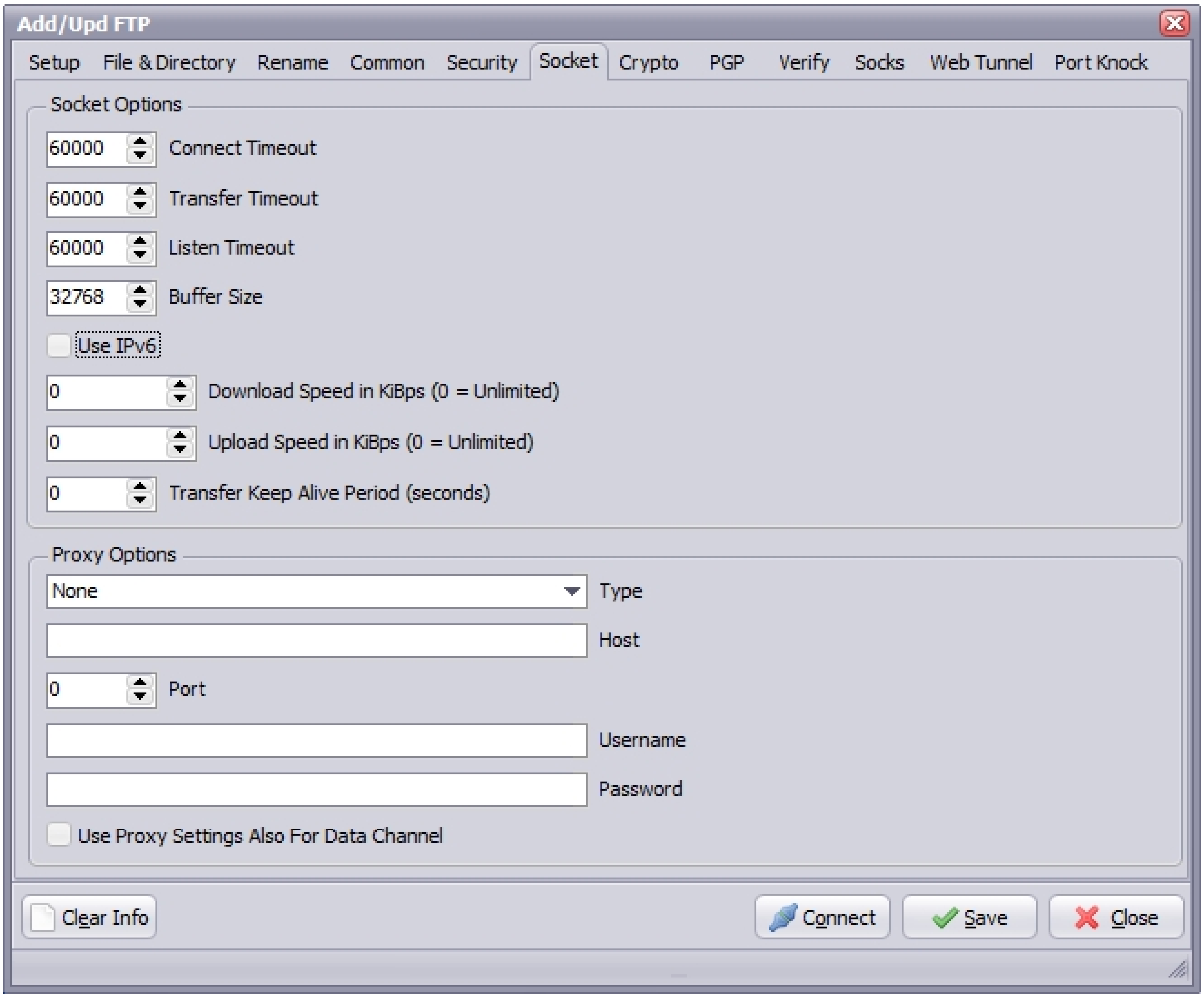
- Self signed certificate allowed: A self signed certificate is allowed.
- Verify client once:

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



Socket Options

60000 Connect Timeout

60000 Transfer Timeout

60000 Listen Timeout

32768 Buffer Size

☐ Use IPv6

0 Download Speed in KiBps (0 = Unlimited)

0 Upload Speed in KiBps (0 = Unlimited)

0 Transfer Keep Alive Period (seconds)

Proxy Options

None Type

Host

0 Port

Username

Password

☐ Use Proxy Settings Also For Data Channel

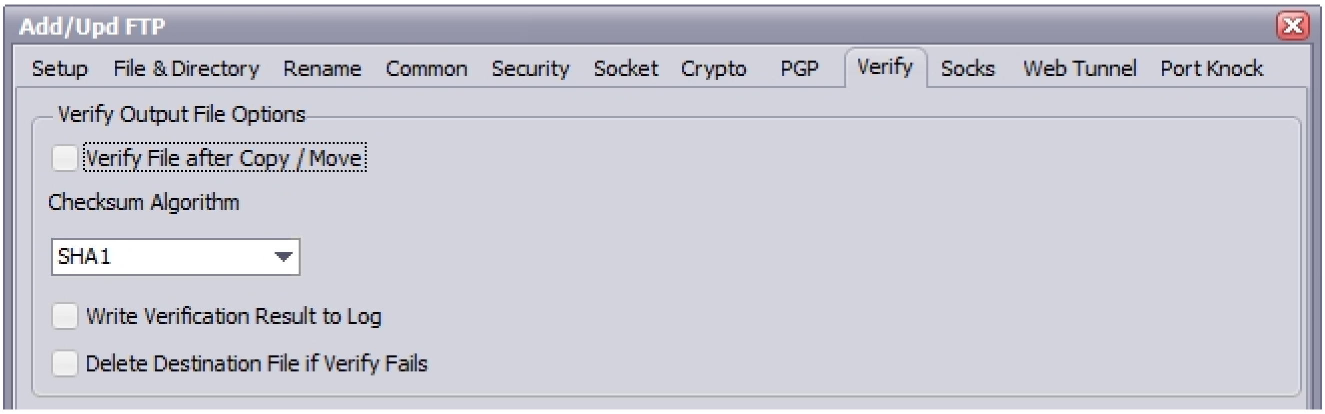
- Connect Timeout: Milliseconds to wait for successful completion of a connection attempt (default 60000). Default value is 60000 ms (1 min).
- Listen Timeout: Use this option to specify maximal time during which the listening socket will be opened in the active mode. If there is no connection request 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.

Proxy Options

- 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.

Verify Options



Verify Output File Options

□ Verify File after Copy / Move

Checksum Algorithm

SHA1

□ Write Verification Result to Log

□ Delete Destination File if Verify Fails

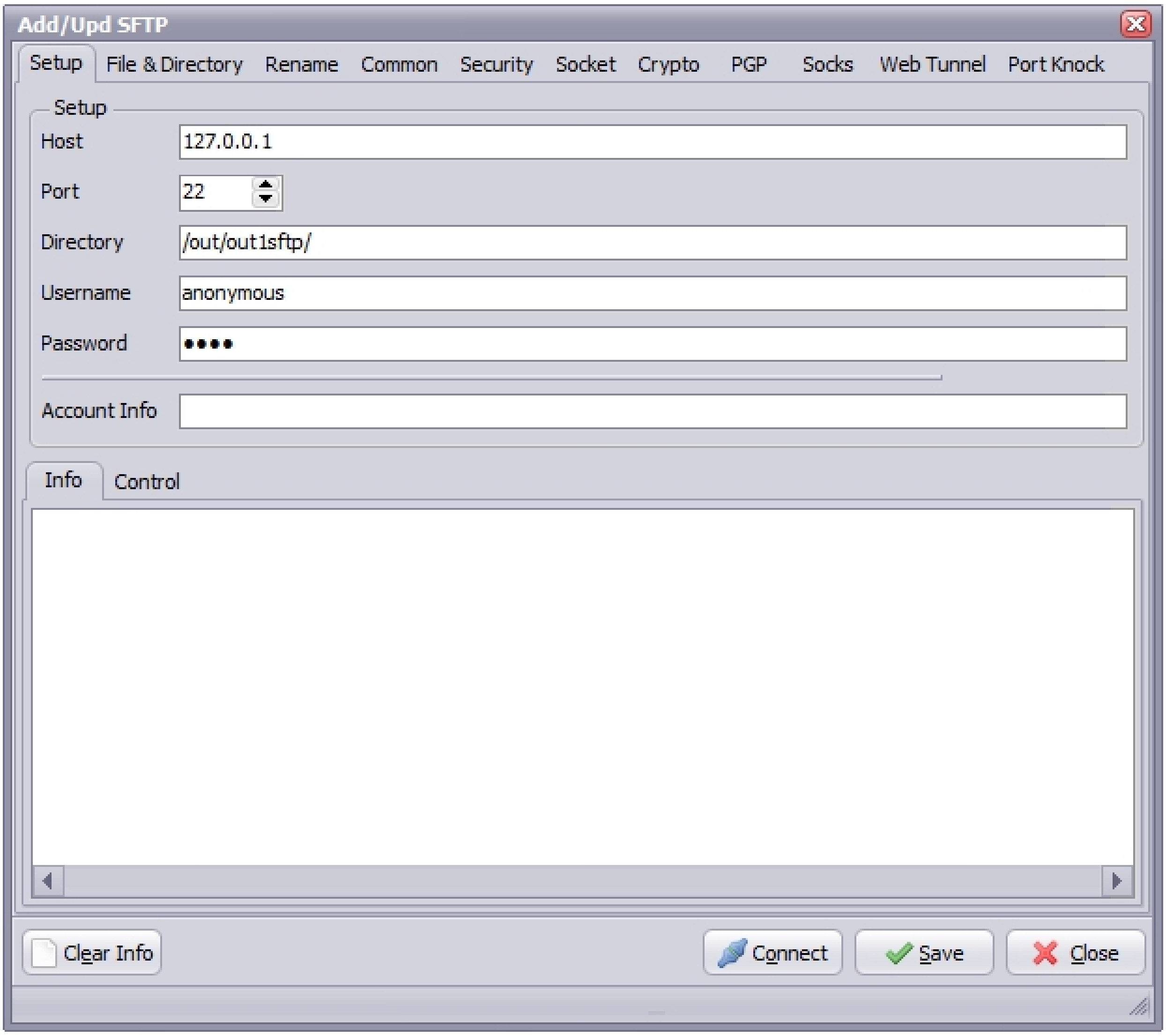
Verify File Options

- 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.

SFTP Destination

SFTP (FTP & FTPS) Destination Setup

Setup Options



Setup

Host: 127.0.0.1

Port: 22

Directory: /out/out1sftp/

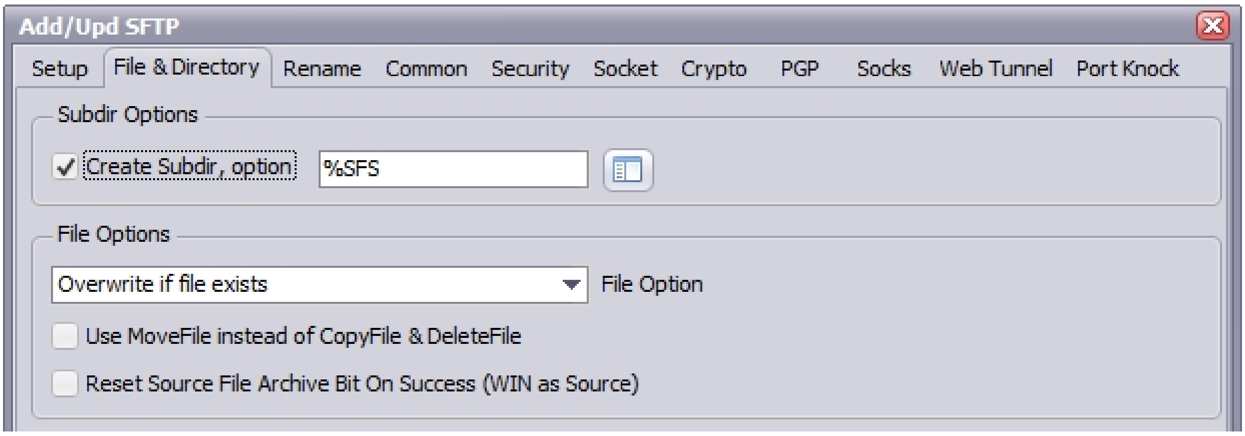
Username: anonymous

Password: ••••

Account Info:

- 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, option: %SFS

File Options

Overwrite if file exists ▾ File Option

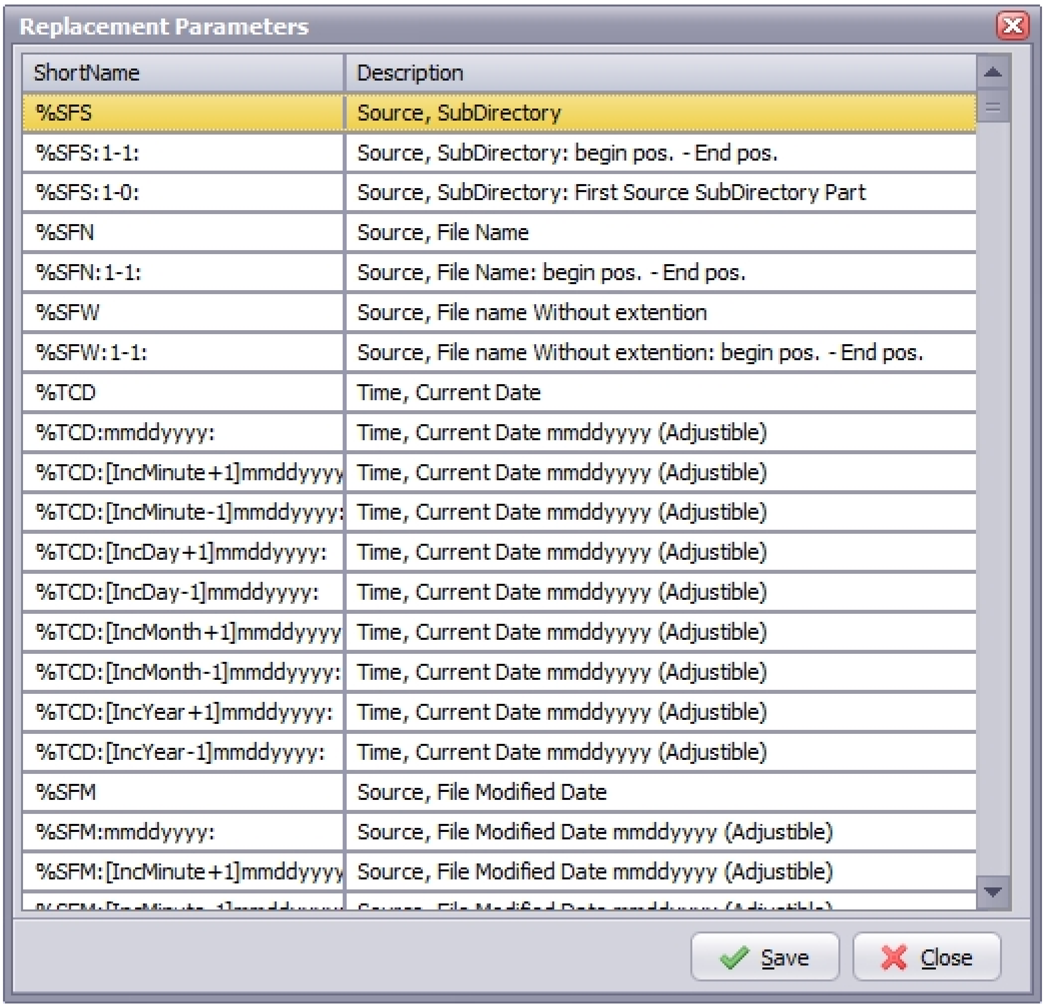
□ Use MoveFile instead of CopyFile & DeleteFile

□ Reset Source File Archive Bit On Success (WIN as Source)

Subdir Options

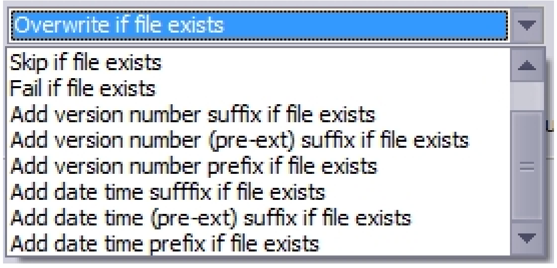
- Create Subdir: Create Subdirectory for the Windows destination.

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



Replacement Parameters

ShortName	Description
%SFS	Source, SubDirectory
%SFS:1-1:	Source, SubDirectory: begin pos. - End pos.
%SFS:1-0:	Source, SubDirectory: First Source SubDirectory Part
%SFN	Source, File Name
%SFN:1-1:	Source, File Name: begin pos. - End pos.
%SFW	Source, File name Without extention
%SFW:1-1:	Source, File name Without extention: begin pos. - End pos.
%TCD	Time, Current Date
%TCD:mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncMinute+1]mmddyyyy	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncMinute-1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncDay+1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncDay-1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncMonth+1]mmddyyyy	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncMonth-1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncYear+1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncYear-1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%SFM	Source, File Modified Date
%SFM:mmddyyyy:	Source, File Modified Date mmddyyyy (Adjustible)
%SFM:[IncMinute+1]mmddyyyy	Source, File Modified Date mmddyyyy (Adjustible)
%SFM:[IncMinute-1]mmddyyyy	Source, File Modified Date mmddyyyy (Adjustible)

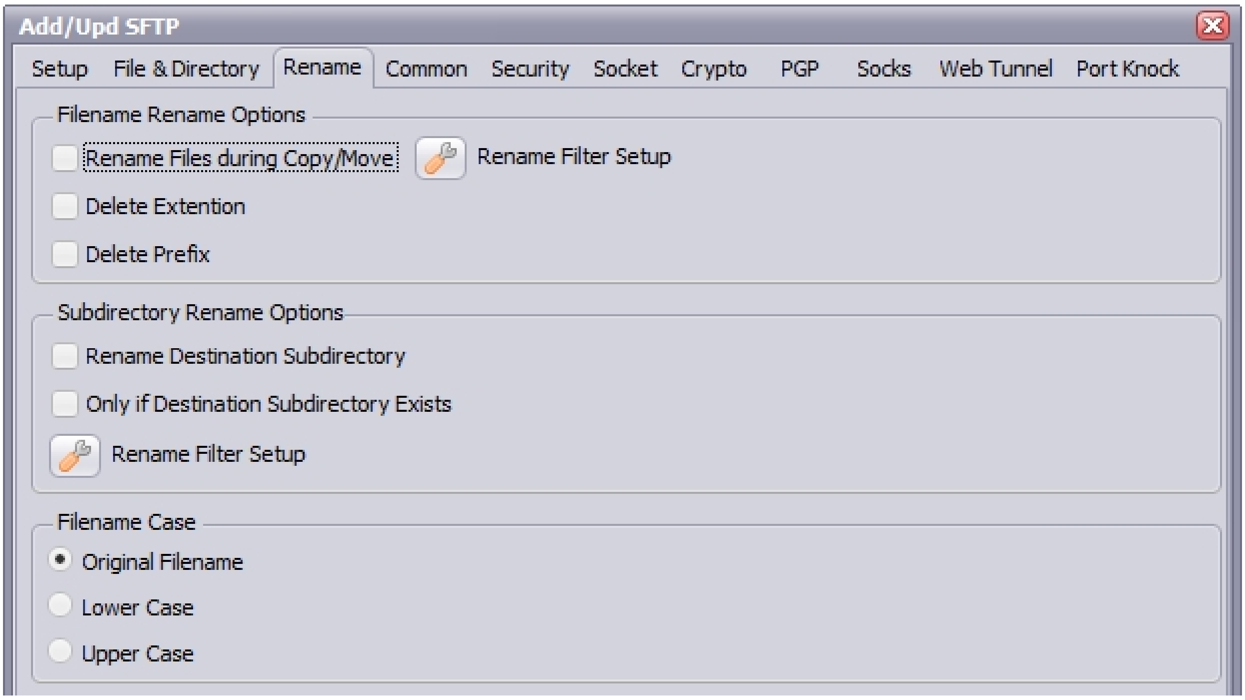
-  File Options

Overwrite if file exists
Skip if file exists
Fail if file exists
Add version number suffix if file exists
Add version number (pre-ext) suffix if file exists
Add version number prefix if file exists
Add date time sufffix if file exists
Add date time (pre-ext) suffix if file exists
Add date time prefix if file exists

  - 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 sufffix 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".

- 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



Filename Rename Options

□ Rename Files during Copy/Move

□ Delete Extention

□ Delete Prefix

Subdirectory Rename Options

□ Rename Destination Subdirectory

□ Only if Destination Subdirectory Exists

Filename Case

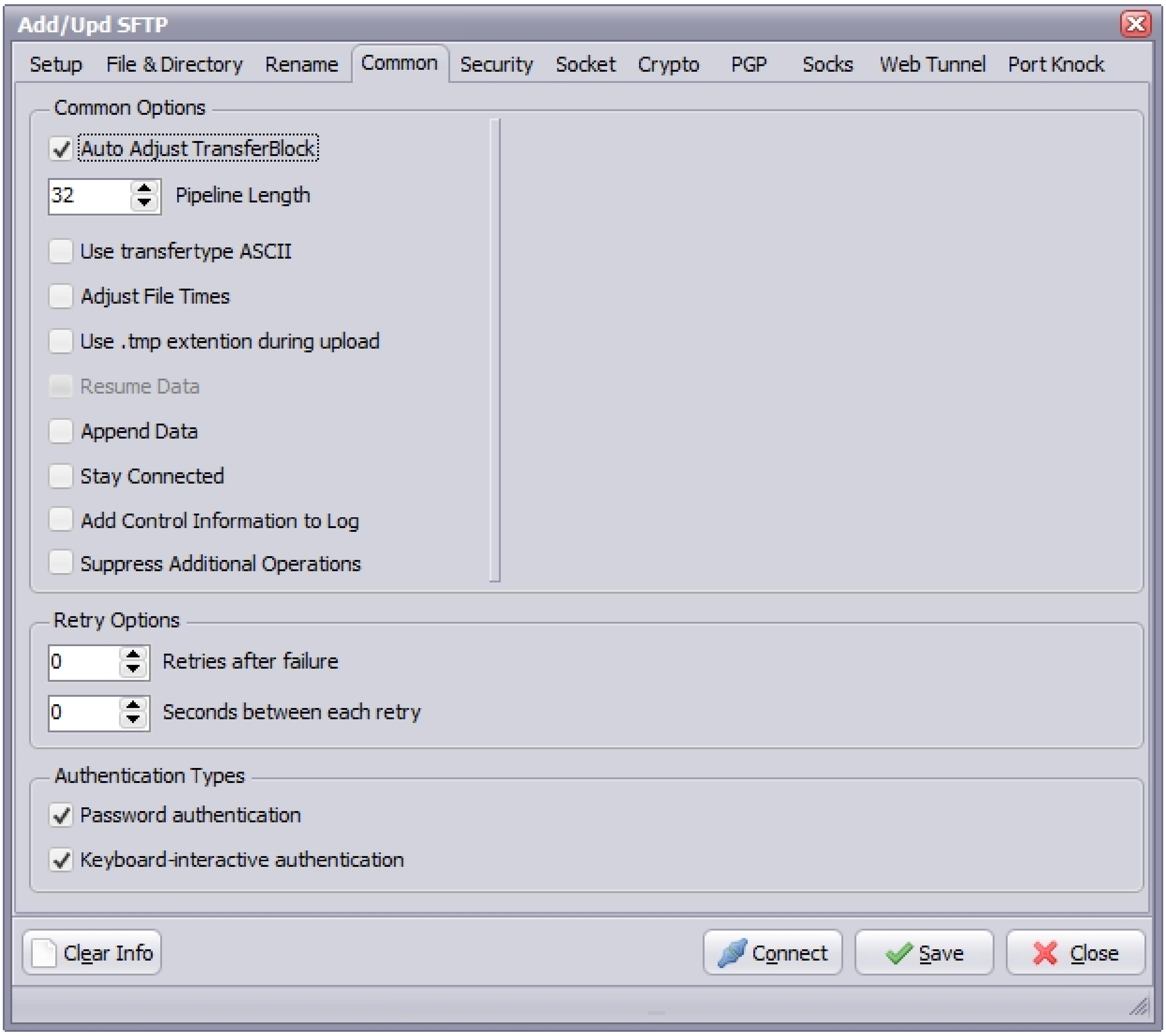
● Original Filename

○ Lower Case

○ Upper Case

- 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/
- 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 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

32 Pipeline Length

□ Use transfertype ASCII

□ Adjust File Times

□ Use .tmp extention during upload

□ Resume Data

□ Append Data

□ Stay Connected

□ Add Control Information to Log

□ Suppress Additional Operations

Retry Options

0 Retries after failure

0 Seconds between each retry

Authentication Types

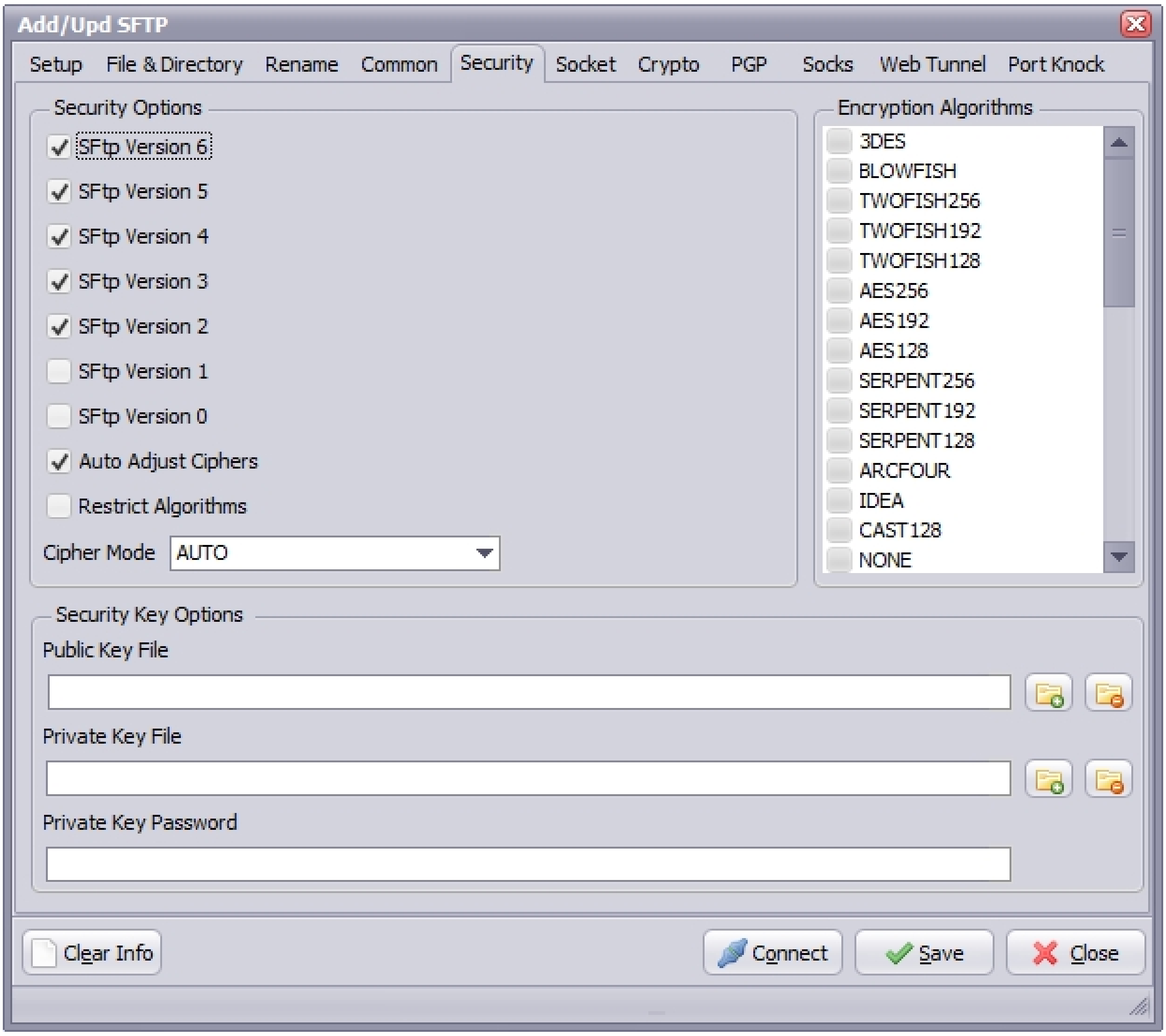
☑ Password authentication

☑ Keyboard-interactive authentication

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.
- Add Control Information to log: Add SFTP specific control information to the log.
- Suppress Additional Operations: Enable Suppress Additional Operations option to work around buggy SFTP servers.
- Retries after failure: Amount of retries after a copy/move failure.
- Seconds between each retry: Seconds that the rule will wait between each retry.
- Authentication Types: Specify which authentication types SSH client should try to use during the negotiation process.

Security Options



Security Options

- ☑ SFtp Version 6
- ☑ SFtp Version 5
- ☑ SFtp Version 4
- ☑ SFtp Version 3
- ☑ SFtp Version 2
- □ SFtp Version 1
- □ SFtp Version 0
- ☑ Auto Adjust Ciphers
- □ Restrict Algorithms

Cipher Mode: AUTO

Encryption Algorithms

- □ 3DES
- □ BLOWFISH
- □ TWOFISH256
- □ TWOFISH192
- □ TWOFISH128
- □ AES256
- □ AES192
- □ AES128
- □ SERPENT256
- □ SERPENT192
- □ SERPENT128
- □ ARCFOUR
- □ IDEA
- □ CAST128
- □ NONE

Security Key Options

Public Key File:

Private Key File:

Private Key Password:

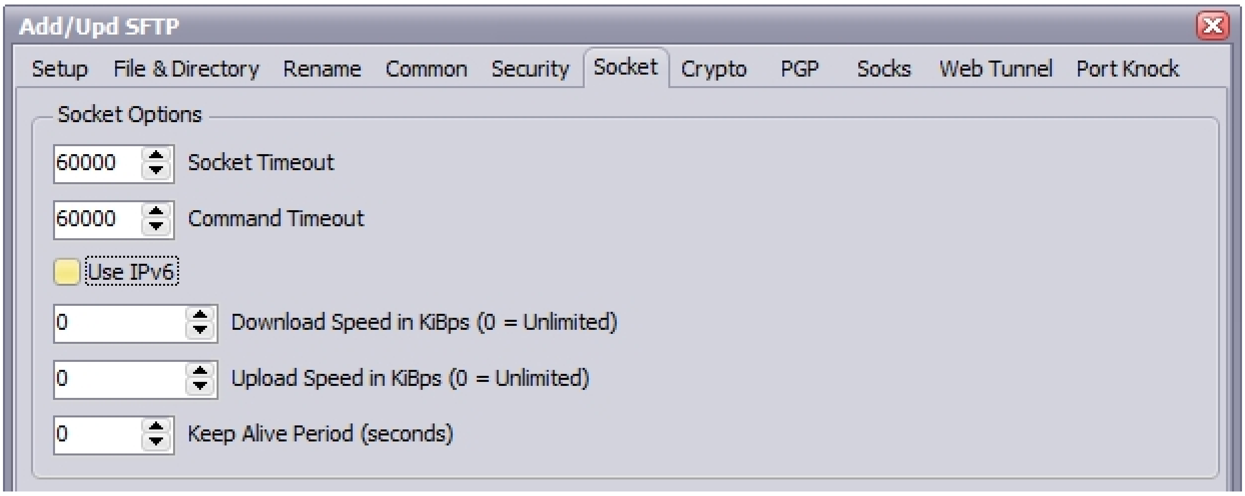
Security Options

- 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



60000 Socket Timeout

60000 Command Timeout

□ Use IPv6

0 Download Speed in KiBps (0 = Unlimited)

0 Upload Speed in KiBps (0 = Unlimited)

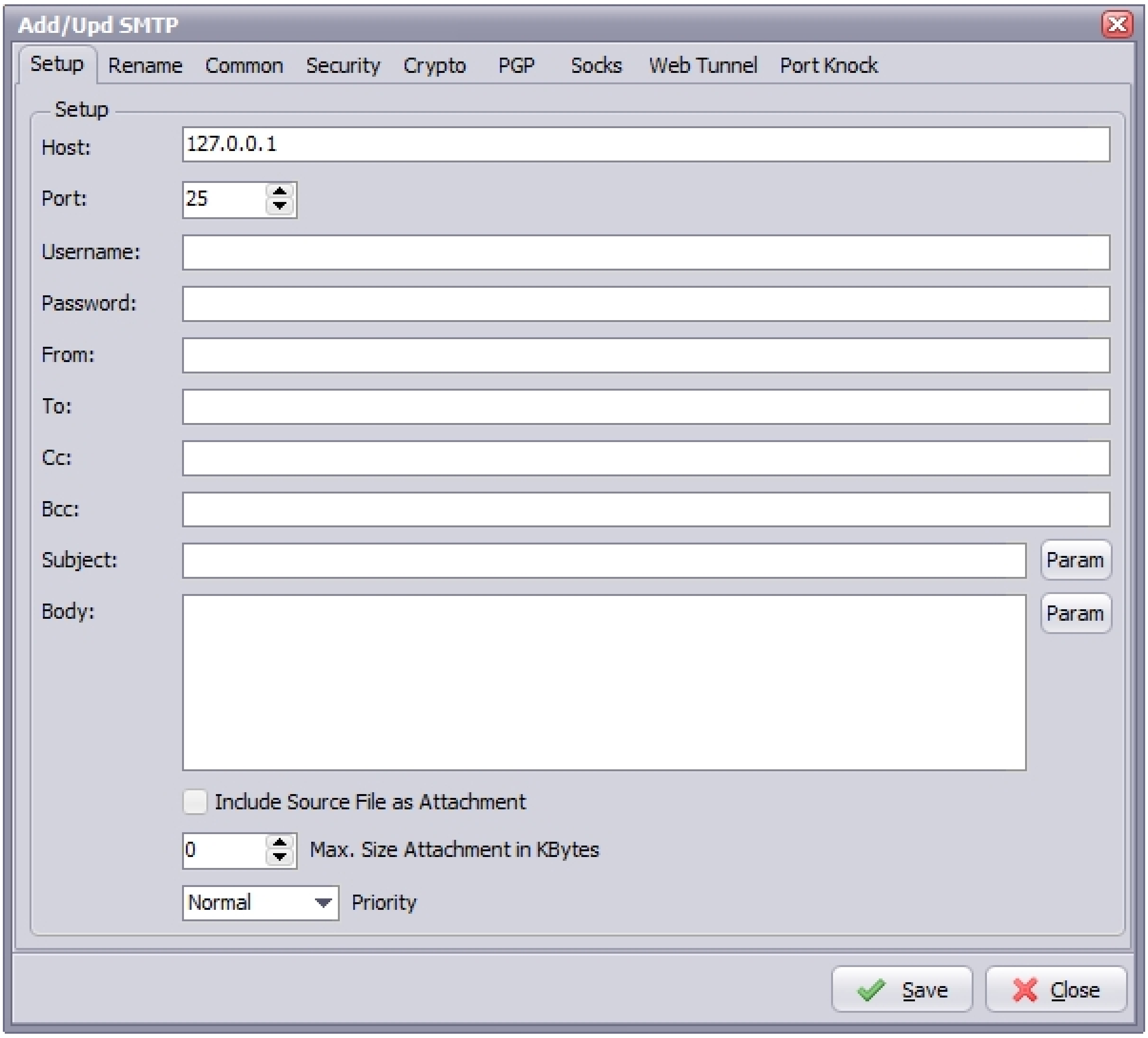
0 Keep Alive Period (seconds)

- Socket Timeout: Specifies maximum time of inactivity after which socket operation is canceled and is considered as expired. If you try to connect, read or write something from/to socket and the attempt is unsuccessful for specified number of milliseconds the operation is canceled with timeout error.
- Command Timeout: Use this option to specify the timeout (in milliseconds) for execution of SSH commands on the server.
- 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).

SMTP Destination

SMTP Destination Setup

Setup Options



Setup

Host: 127.0.0.1

Port: 25

Username:

Password:

From:

To:

Cc:

Bcc:

Subject:

Body:

□ Include Source File as Attachment

0 Max. Size Attachment in KBytes

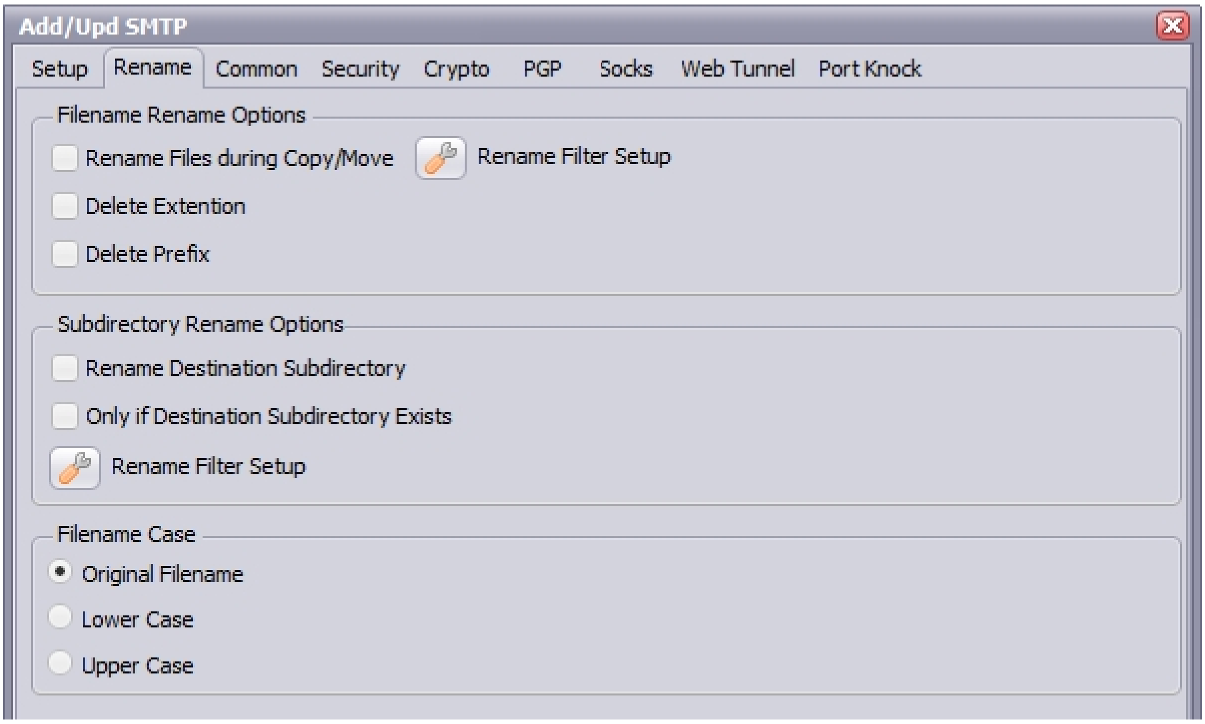
Normal Priority

- 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



Add/Upd SMTP

Filename Rename Options

□ Rename Files during Copy/Move

Rename Filter Setup

□ Delete Extention

□ Delete Prefix

Subdirectory Rename Options

□ Rename Destination Subdirectory

□ Only if Destination Subdirectory Exists

Rename Filter Setup

Filename Case

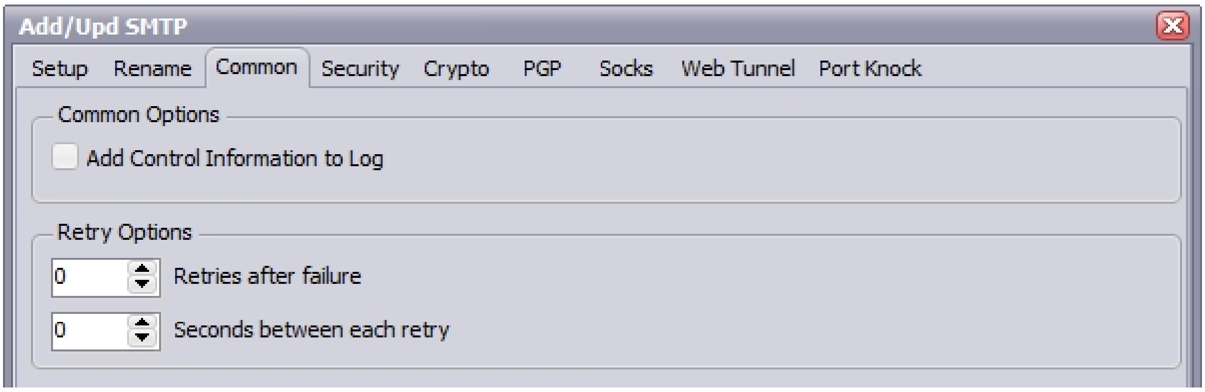
● Original Filename

○ Lower Case

○ Upper Case

- 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



Add/Upd SMTP

Common Options

□ Add Control Information to Log

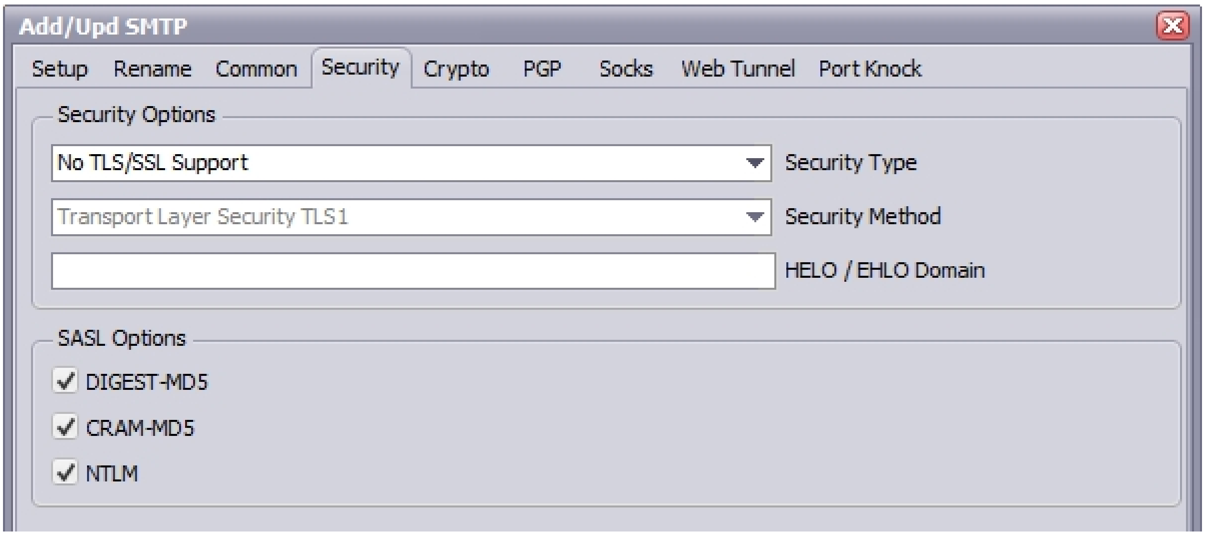
Retry Options

0 Retries after failure

0 Seconds between each retry

- Add Control Information to log: Add SMTP specific control information to the log.
- Retries after failure: Amount of retries after a copy/move failure.
- Seconds between each retry: Seconds that the rule will wait between each retry.

Security Options



Security Options

No TLS/SSL Support — Security Type

Transport Layer Security TLS1 — Security Method

HELO / EHLO Domain

SASL Options

☑ DIGEST-MD5

☑ CRAM-MD5

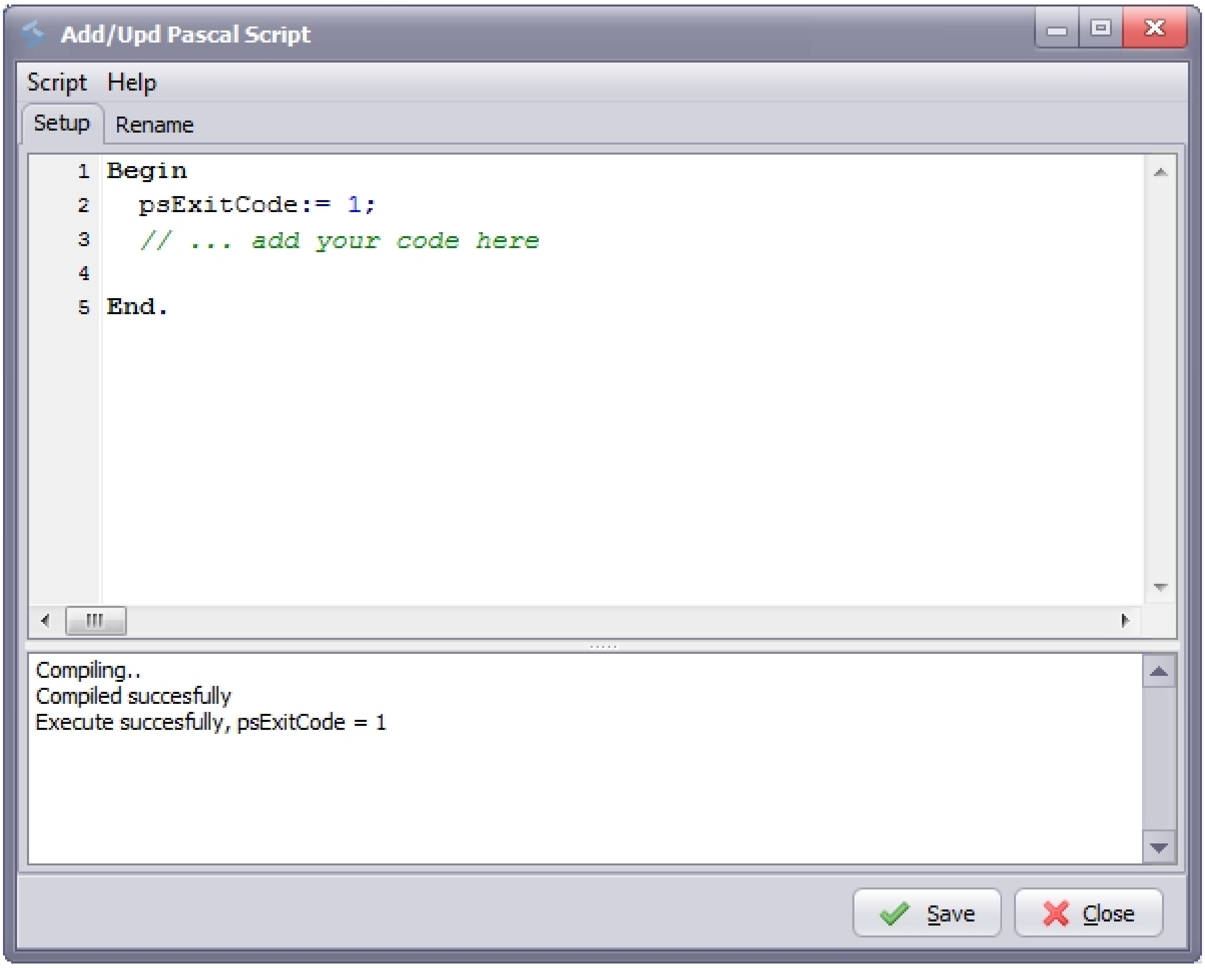
☑ NTLM

- 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.
- SASL Options: Use this option to enable or disable specific SASL authorization mechanism

PS Destination

Pascal Script Destination Setup

Setup Options

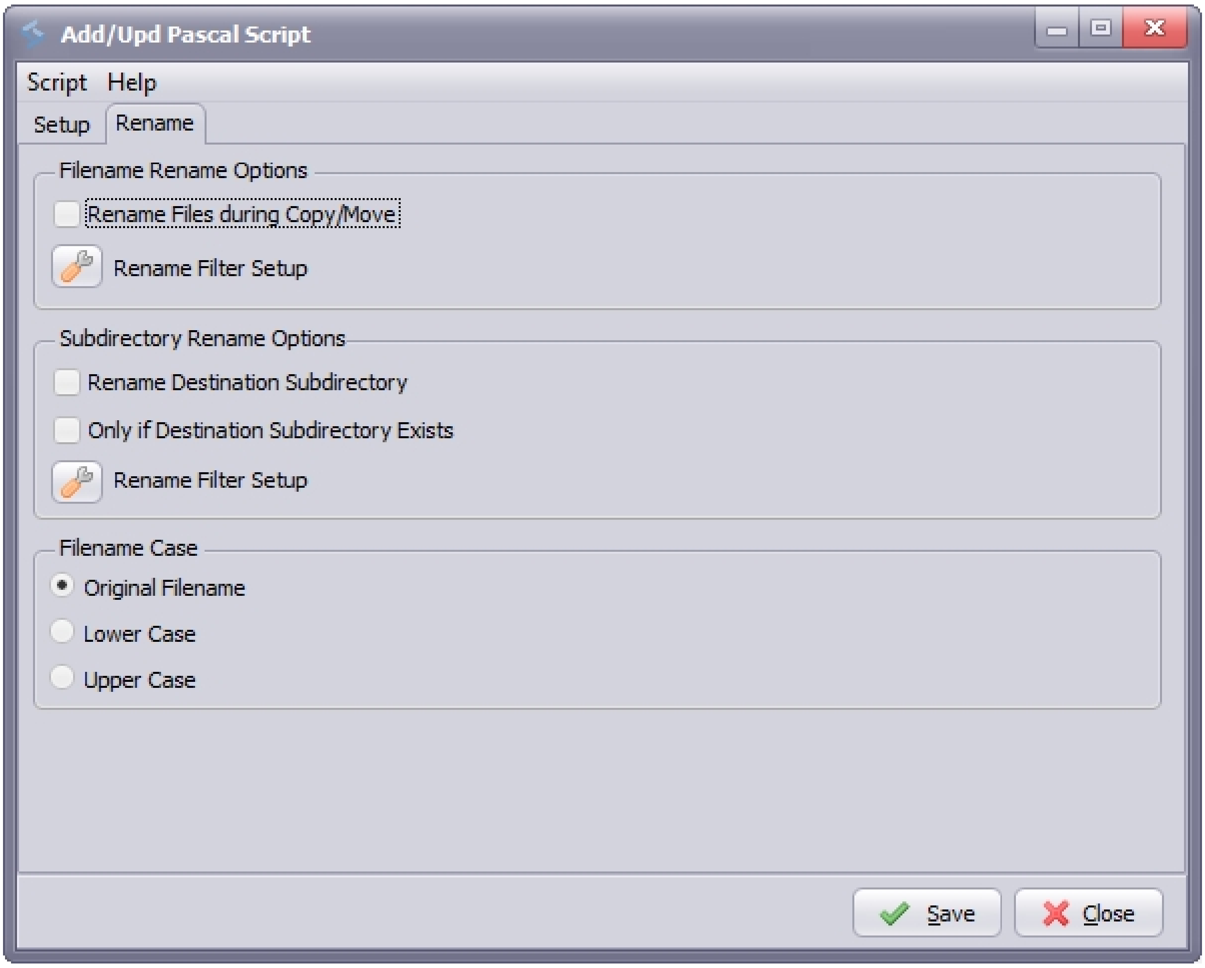


```
Begin
  psExitCode:= 1;
  // ... add your code here

End.
```

```
Compiling..
Compiled succesfully
Execute succesfully, psExitCode = 1
```

Rename Options

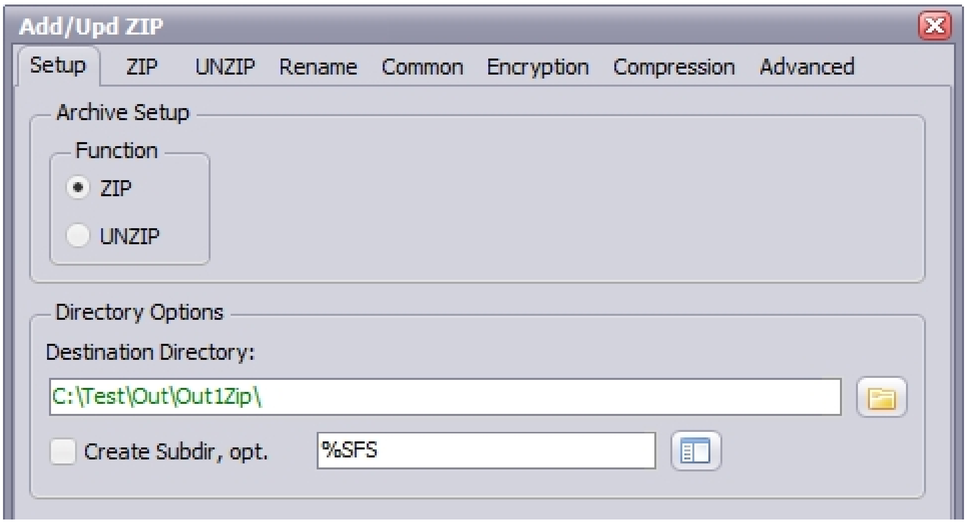


- Rename Files during Copy/Move: Use regular expressions to rename the destination filename. A very good site with information about regular expressions is http://www.regular-expressions.info/
- Rename Destination Subdirectory: Use regular expressions to rename the destination subdirectory.
- Only if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

ZIP Destination

ZIP/UNZIP Destination Setup

Setup Options

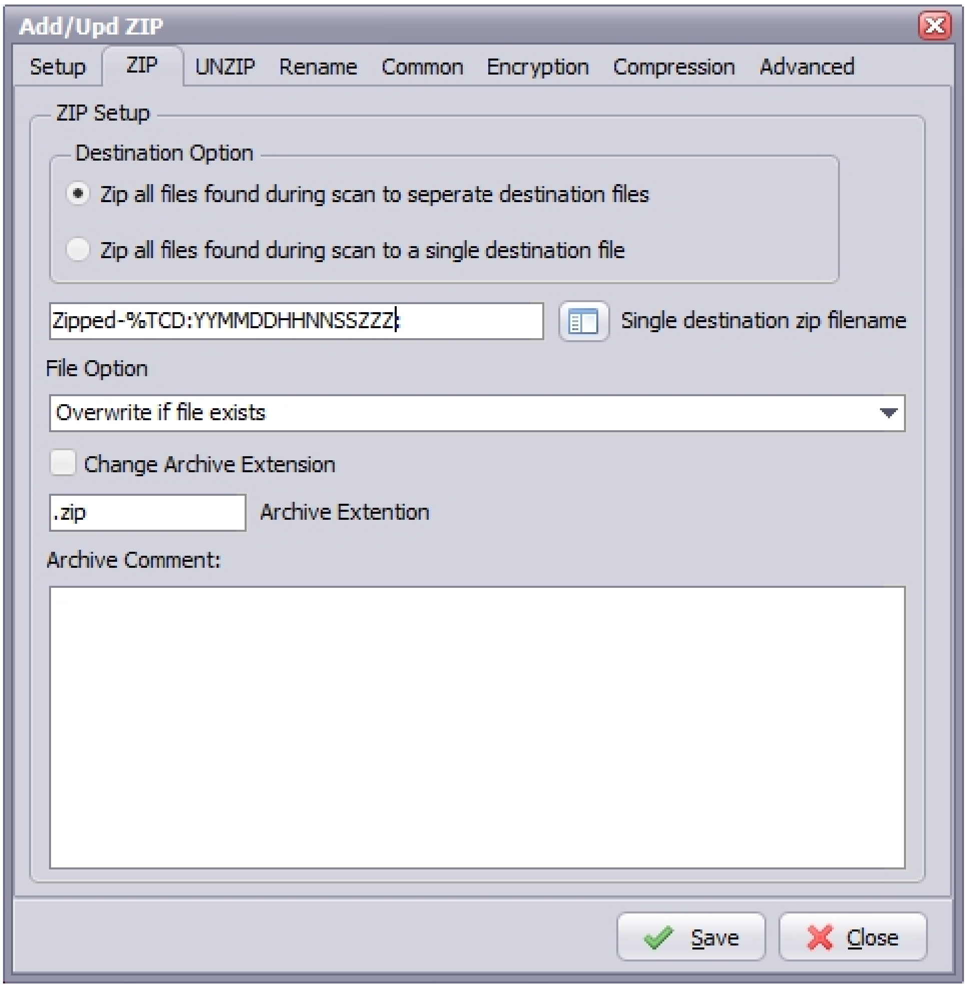

Add/Upd ZIP
Setup ZIP UNZIP Rename Common Encryption Compression Advanced
Archive Setup
Function
● ZIP
○ UNZIP
Directory Options

Destination Directory: C:\Test\Out\Out1Zip\

□ Create Subdir, opt. %SFS

- 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



ZIP Setup

Destination Option

● Zip all files found during scan to seperate destination files

○ Zip all files found during scan to a single destination file

Single destination zip filename: Zipped-%TCD:YYMMDDHHNNSSZZZ

File Option: Overwrite if file exists

□ Change Archive Extension

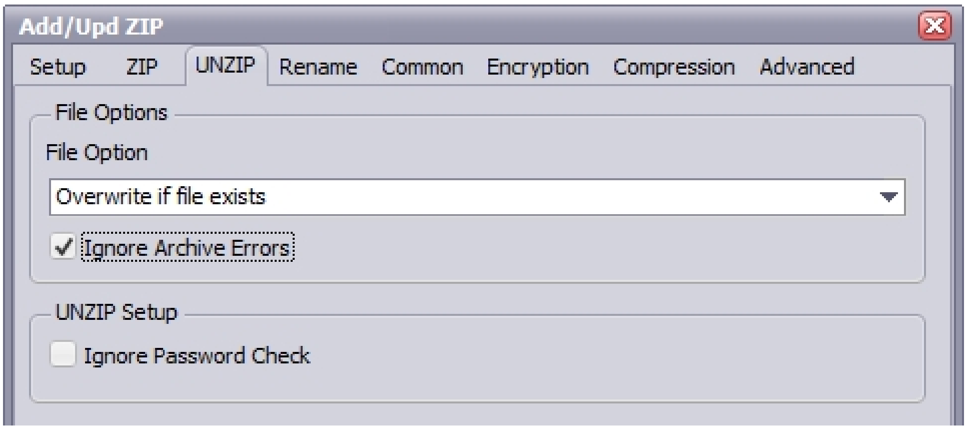
Archive Extention: .zip

Archive Comment:

- 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 sufffix 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 Extention: Change the extention 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%SFN).

- %SFP = Source File Path
- %SFN = Source File Name

UNZIP Options



File Options

File Option: Overwrite if file exists

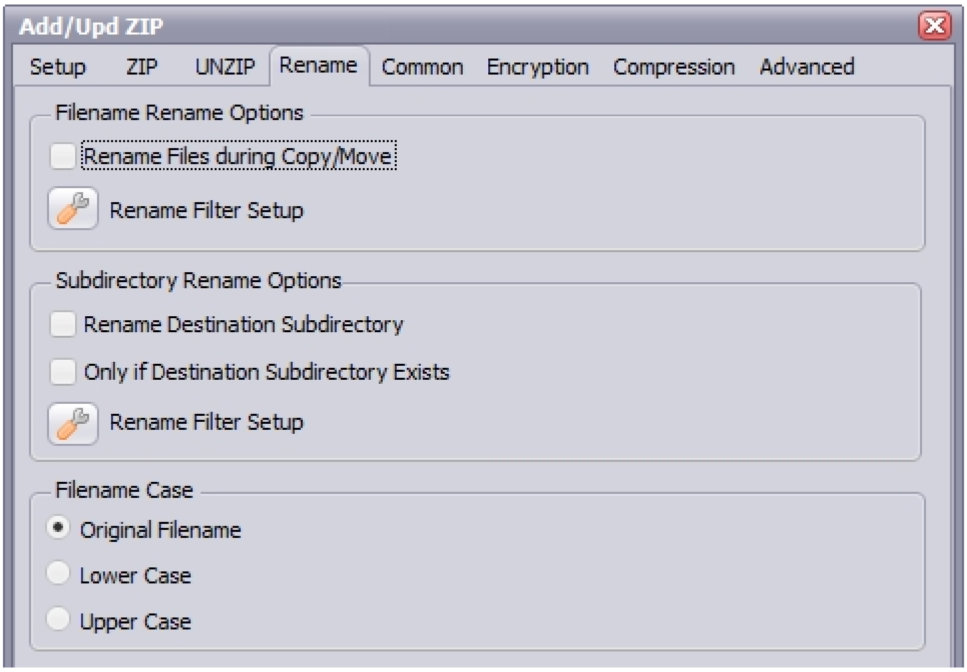
☑ Ignore Archive Errors

UNZIP Setup

☐ Ignore Password Check

- 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



Filename Rename Options

☐ Rename Files during Copy/Move

Subdirectory Rename Options

☐ Rename Destination Subdirectory

☐ Only if Destination Subdirectory Exists

Filename Case

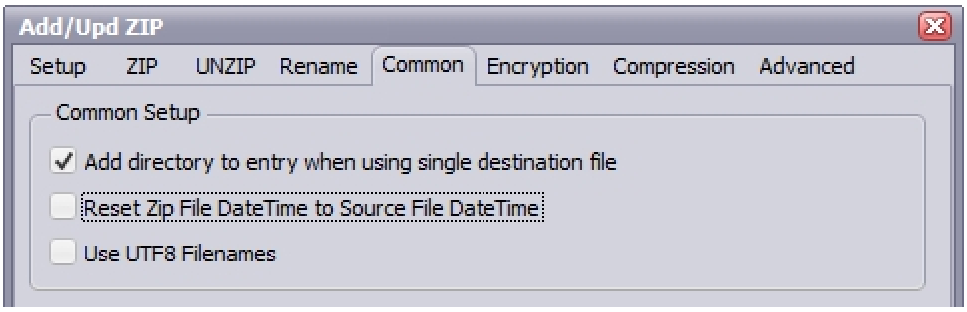
● Original Filename

○ Lower Case

○ Upper Case

- 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.

Common Options



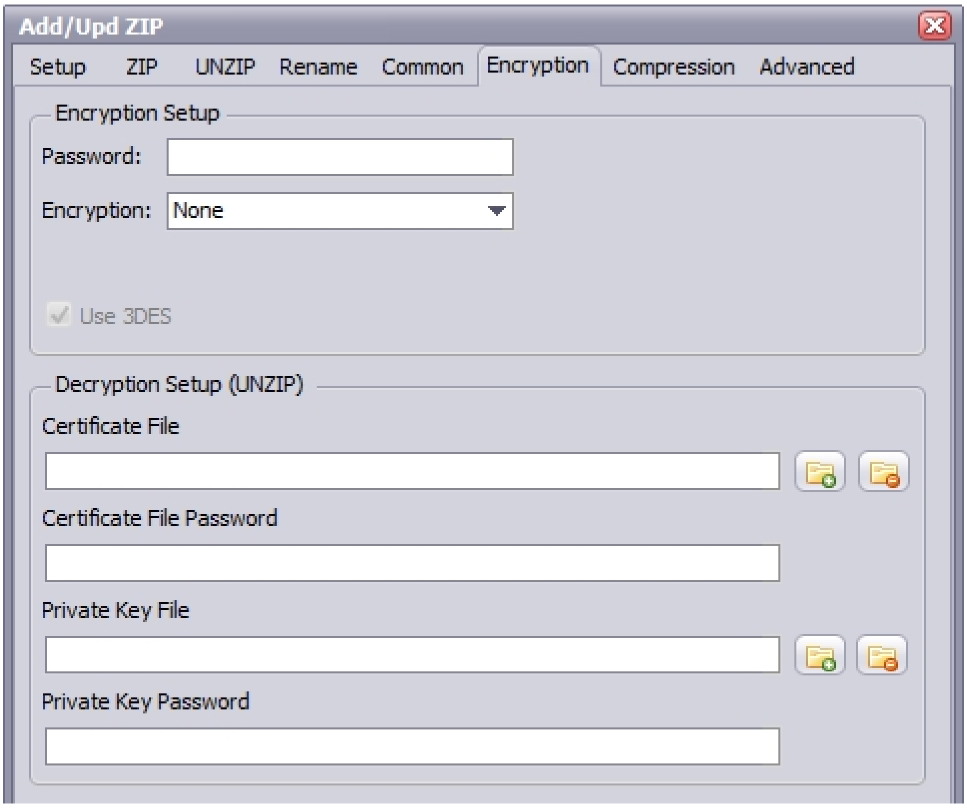
Common Setup

☑ Add directory to entry when using single destination file

□ Reset Zip File DateTime to Source File DateTime

□ Use UTF8 Filenames

Encryption Options



Encryption Setup

Password:

Encryption: None

☑ Use 3DES

Decryption Setup (UNZIP)

Certificate File

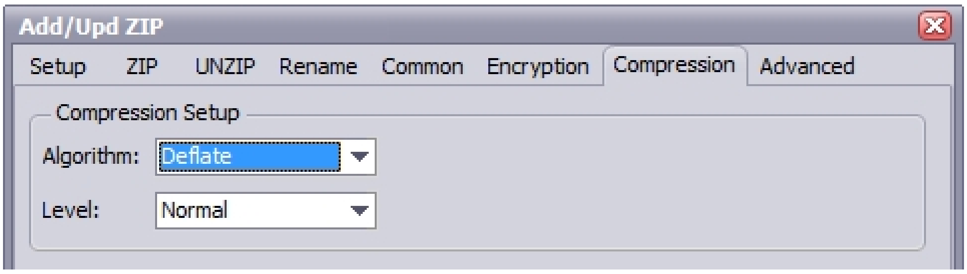
Certificate File Password

Private Key File

Private Key Password

- 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



Compression Setup

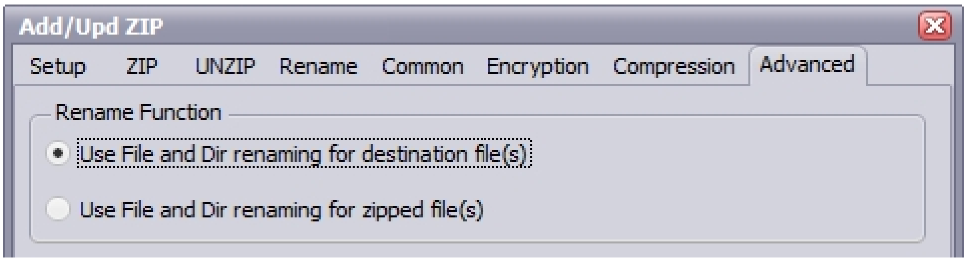
Algorithm: Deflate

Level: Normal

- 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.

Advanced Options



Rename Function

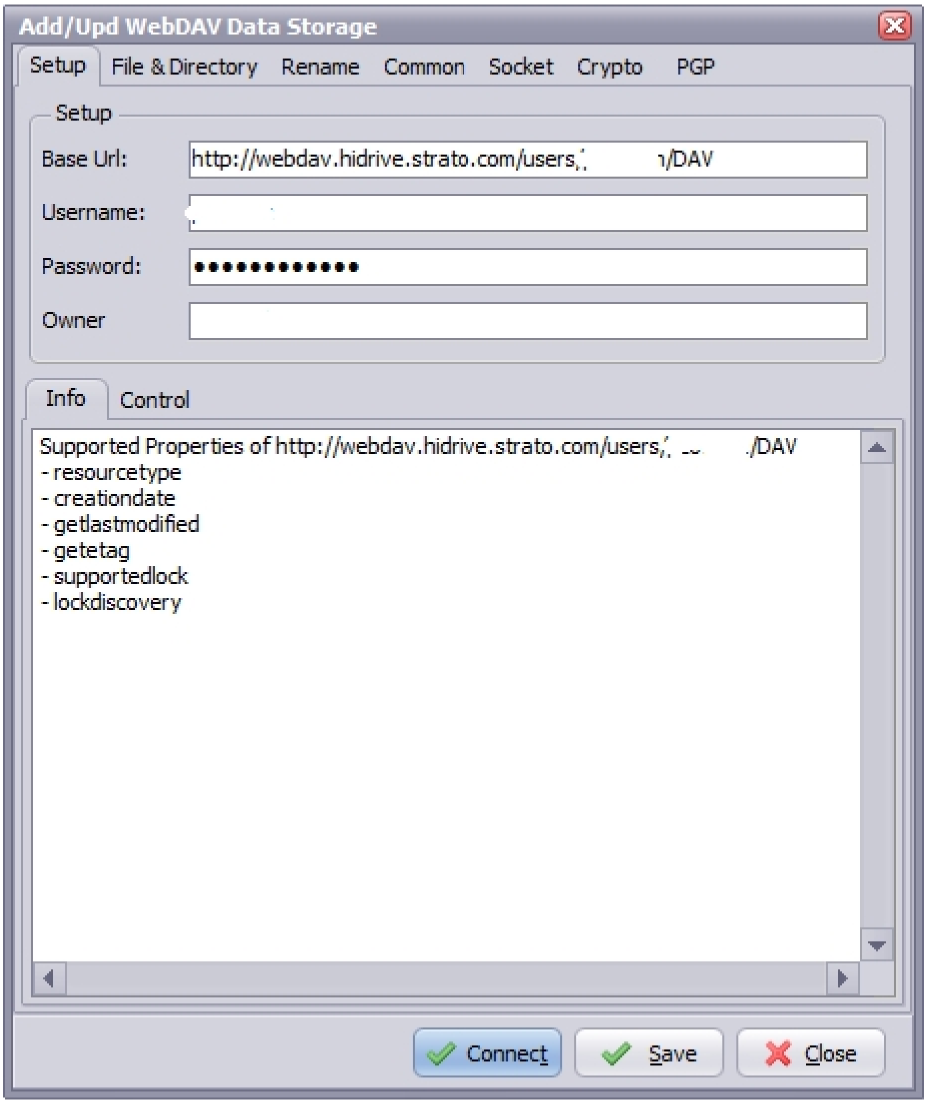
● Use File and Dir renaming for destination file(s)

○ Use File and Dir renaming for zipped file(s)

WebDAV

WebDAV Destination Setup

Add / Update WebDAV as Destination.



Setup

Base Url: http://webdav.hidrive.strato.com/users,', 1/DAV

Username:

Password: •••••••••••••

Owner

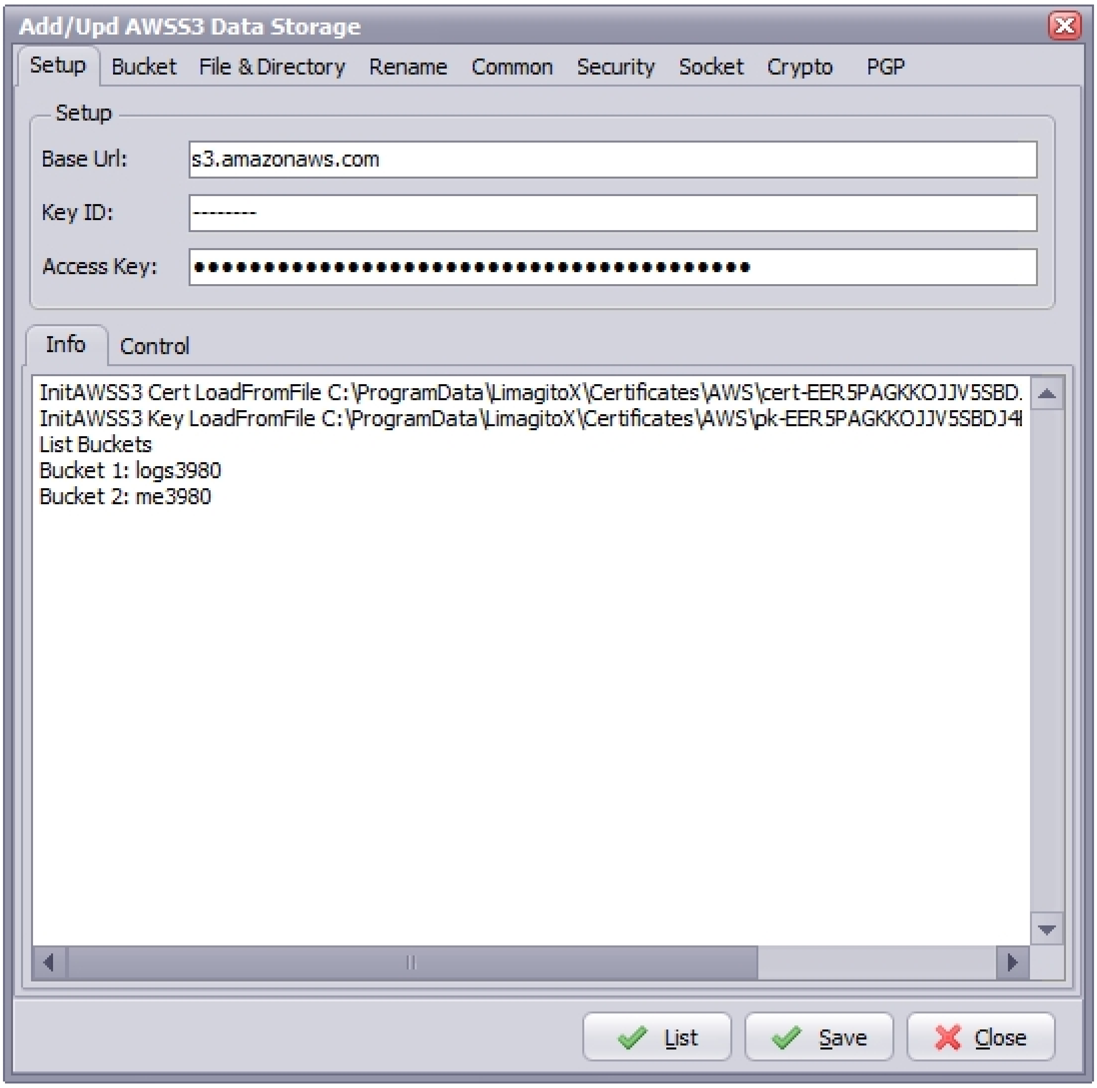
```
Supported Properties of http://webdav.hidrive.strato.com/users,', -- ./DAV
- resourcetype
- creationdate
- getlastmodified
- getetag
- supportedlock
- lockdiscovery
```

AWSS3

AWSS3 Destination Setup

Add / Update AWSS3 as Destination. Use this option to connect to S3 or S3-compatible cloud services.

Our AWSS3 option provides functionality to make requests, securely upload and download data using Amazon Simple Storage Service (S3) and compatible services. In S3 storages individual data objects are contained in buckets. Connection is established using the HTTP protocol. By default, secure connection is established. If you don't need a secure connection, please disable the SSL option. To authenticate to S3 storage, you need to provide Access Key and key ID pair.



Base Url: s3.amazonaws.com

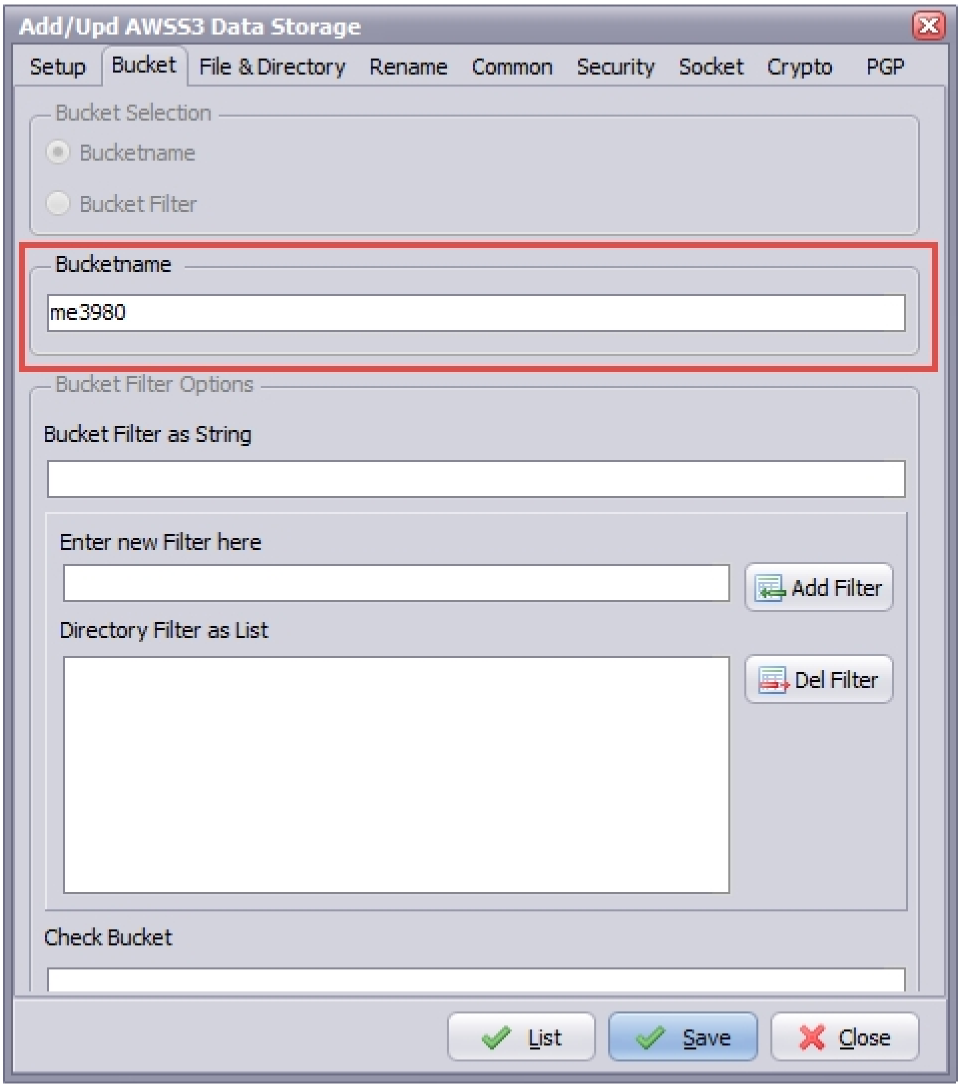
Key ID: --------

Access Key: ●●

```
InitAWSS3 Cert LoadFromFile C:\ProgramData\LimagitoX\Certificates\AWS\cert-EER5PAGKKOJJV5SBD.
InitAWSS3 Key LoadFromFile C:\ProgramData\LimagitoX\Certificates\AWS\pk-EER5PAGKKOJJV5SBDJ4
List Buckets
Bucket 1: logs3980
Bucket 2: me3980
```

- Base Url: Specify the base URL of the S3 service responder.
- Key ID: Use this option to specify the Key ID provided to the user of Amazon data storage. The KeyID and Access Key pair is used to authenticate and communicate with data storage.
- Access Key: Use this option to specify the secret key that was issued by Amazon to the data storage user. The KeyID and Access Key pair is used to authenticate and communicate with data storage.

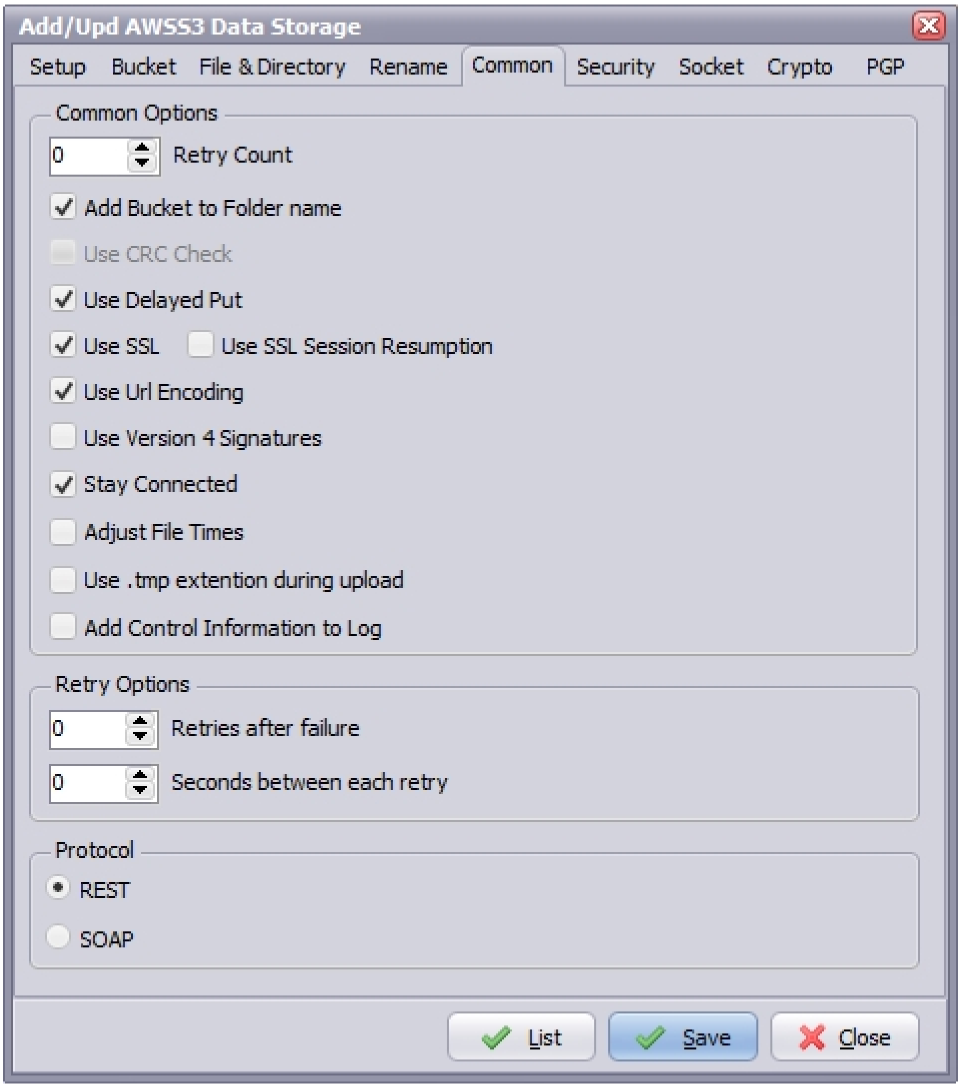
Bucket Options



Bucketname: me3980

- Bucketname: Enter the Bucketname you want to upload your files to.

Common Options



Common Options

0 Retry Count

☑ Add Bucket to Folder name

□ Use CRC Check

☑ Use Delayed Put

☑ Use SSL □ Use SSL Session Resumption

☑ Use Url Encoding

□ Use Version 4 Signatures

☑ Stay Connected

□ Adjust File Times

□ Use .tmp extention during upload

□ Add Control Information to Log

Retry Options

0 Retries after failure

0 Seconds between each retry

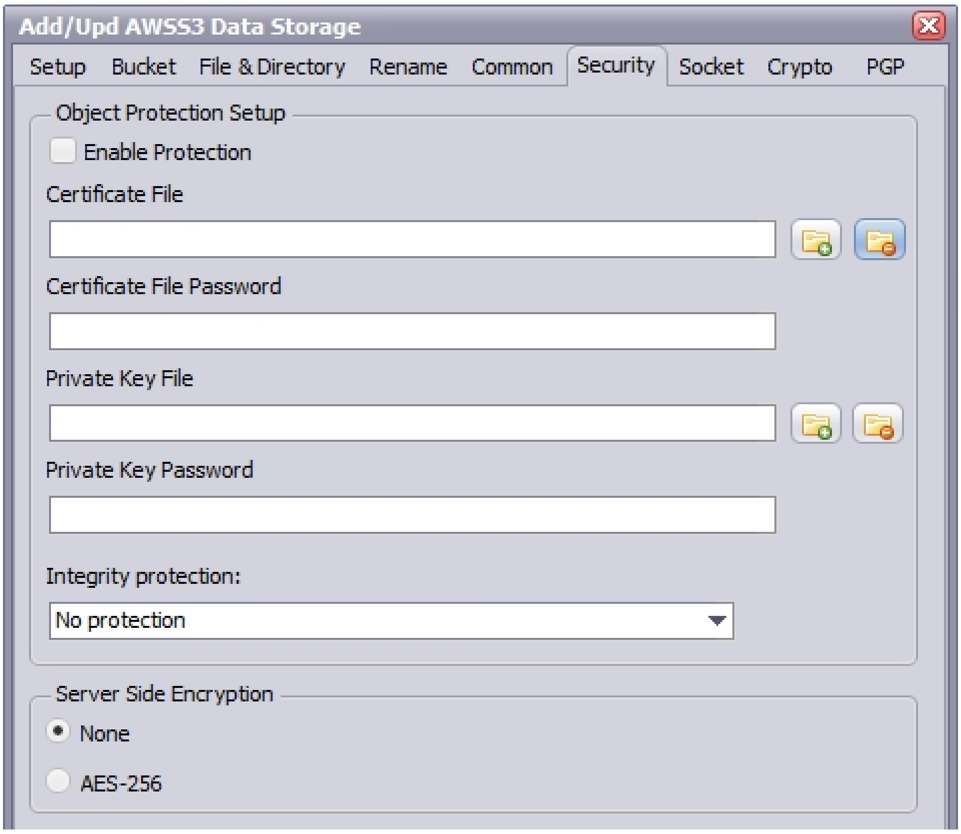
Protocol

● REST

○ SOAP

- Retry Count: Amount of AWSS3 retries after a failure.
- Add Bucket to Folder name:
- Use Crc Check: Specifies if CRC check should be performed.
- Use Delayed Put: Specifies if PUT requests should be delayed.
- Use SSL: Specifies if secure connection should be established.
- Use SSL Session Resumption: Session reuse is one of the most important mechanism to improve SSL performance.
- Use Url Encoding: Specifies if URL encoding should be used.
- Use Version 4 Signatures:
- Stay Connected: Don't disconnect between scans.
- Adjust File Times: File times will be adjusted after upload/download operation.
- Use .tmp extention during upload: Use a temporary extension during upload.
- Add Control Information to Log: Add AWSS3 specific control information to the log.
- Retries after failure: Amount of retries after a copy/move failure.
- Seconds between each retry: Seconds that the rule will wait between each retry.
- Protocol: Use this option to specify the protocol which should be used to access the data storage.

Security Options



Add/Upd AWSS3 Data Storage

Object Protection Setup

□ Enable Protection

Certificate File

Certificate File Password

Private Key File

Private Key Password

Integrity protection: No protection

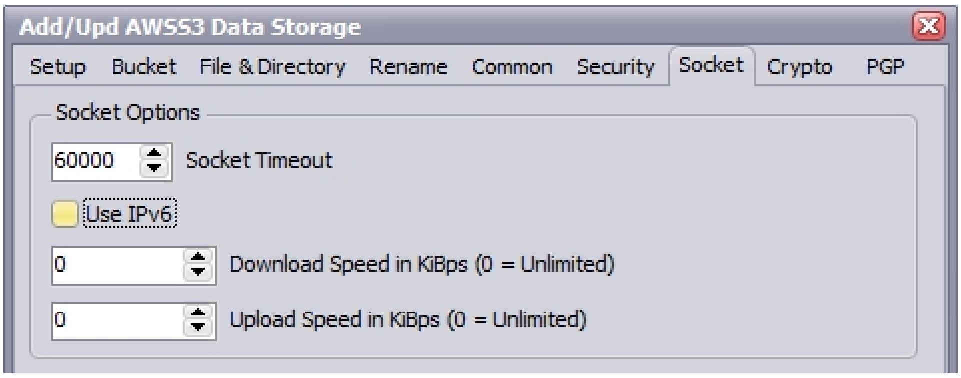
Server Side Encryption

● None

○ AES-256

- Certificate File: This file should contain the certificate (X.509). It recognizes the format automatically. If the format is not recognized, an error is reported. The supported formats are DER, PEM, PFX, SPC.
- Certificate File Password: Password to access the Certificate File.
- Private Key File: This files should contain the certificate's private key (X.509). It will recognizes the format automatically. If the format is not recognized, an error is reported. The supported formats are: DER, PEM, PFX, PVK, NET, PKCS#8.
- Private Key Password: Password to access the Private Key file.
- Integrity Protection:
  - No = no authentication info
  - Basic = basic authentication info should be used if there is no need to access particular blocks of data objects
  - Extended = extended authentication info should be used if there is need to access particular blocks of data objects
- Server Side Encryption: Server-side encryption is about protecting data at rest. Server-side encryption with Amazon S3-managed encryption keys (SSE-S3) employs strong multi-factor encryption. Amazon S3 encrypts each object with a unique key. As an additional safeguard, it encrypts the key itself with a master key that it regularly rotates. Amazon S3 server-side encryption uses one of the strongest block ciphers available, 256-bit Advanced Encryption Standard (AES-256), to encrypt your data.

Socket Options



Add/Upd AWSS3 Data Storage

Socket Options

60000 Socket Timeout

□ Use IPv6

0 Download Speed in KiBps (0 = Unlimited)

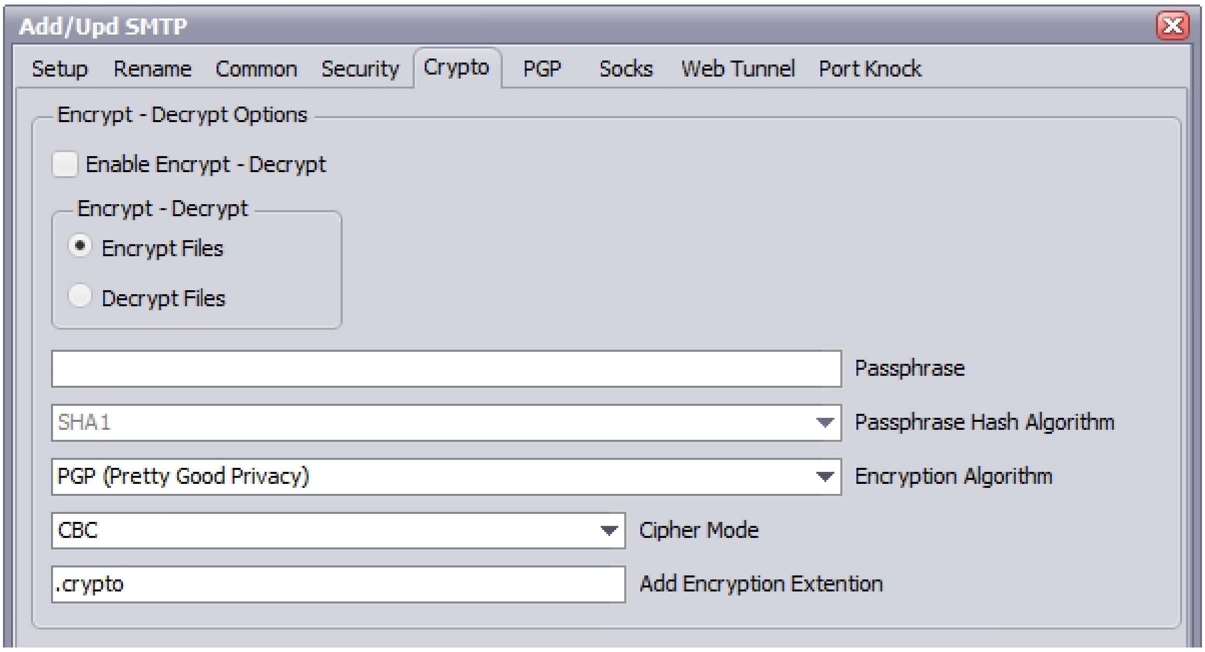
0 Upload Speed in KiBps (0 = Unlimited)

- Socket Timeout: Specifies maximum time of inactivity after which socket operation is canceled and is considered as expired. If you try to connect, read or write something from/to socket and the attempt is unsuccessful for specified number of milliseconds the operation is canceled with timeout error.

- 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 we may receive. The value of 0 (zero) means "no limitation".
- Upload Speed: Use this option to specify the maximum number of KiBps that we may send. The value of 0 (zero) means "no limitation".

Crypto Option

Crypto Destination Option



Encrypt - Decrypt Options

□ Enable Encrypt - Decrypt

Encrypt - Decrypt

● Encrypt Files

○ Decrypt Files

Passphrase:

Passphrase Hash Algorithm: SHA1

Encryption Algorithm: PGP (Pretty Good Privacy)

Cipher Mode: CBC

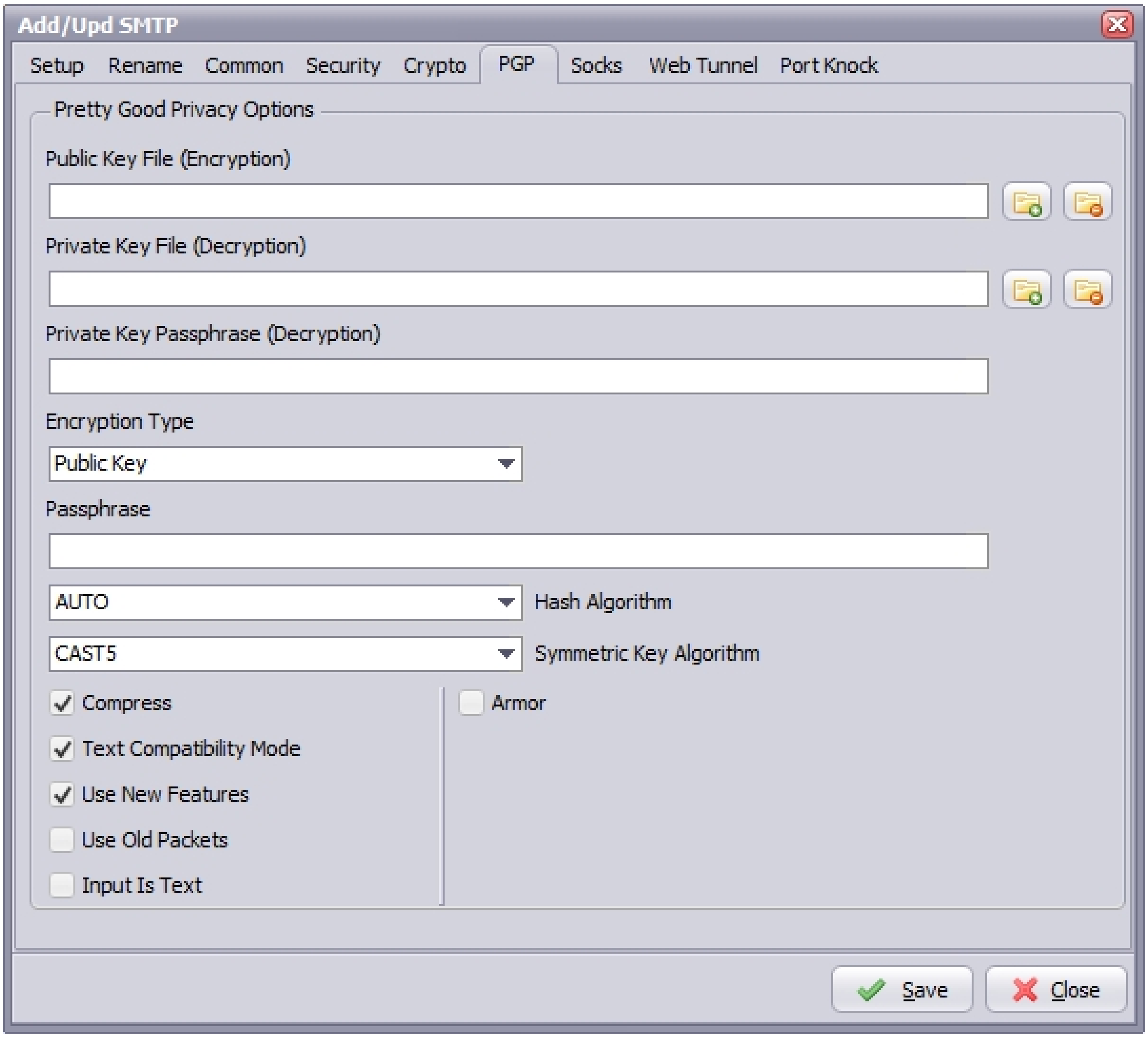
Add Encryption Extention: .crypto

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.

PGP Option

PGP Destination Option



Pretty Good Privacy Options

Public Key File (Encryption)

Private Key File (Decryption)

Private Key Passphrase (Decryption)

Encryption Type: Public Key

Passphrase

Hash Algorithm: AUTO

Symmetric Key Algorithm: CAST5

☑ Compress

☑ Text Compatibility Mode

☑ Use New Features

☐ Use Old Packets

☐ Input Is Text

☐ Armor

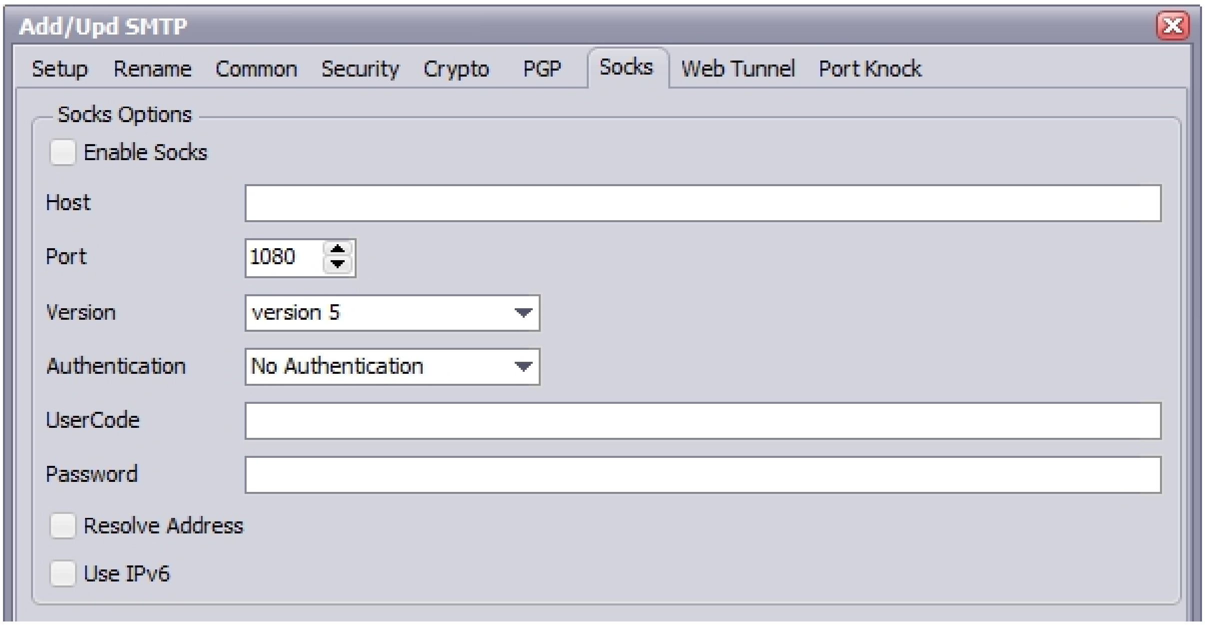
To enable PGP you need to set the Encryption Algorithm to PGP (check the Crypto Tab).

- 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 optiony 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 andSign 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 Option

Socks Destination Option



Socks Options

□ Enable Socks

Host	
Port	1080
Version	version 5
Authentication	No Authentication
UserCode	
Password	

□ Resolve Address

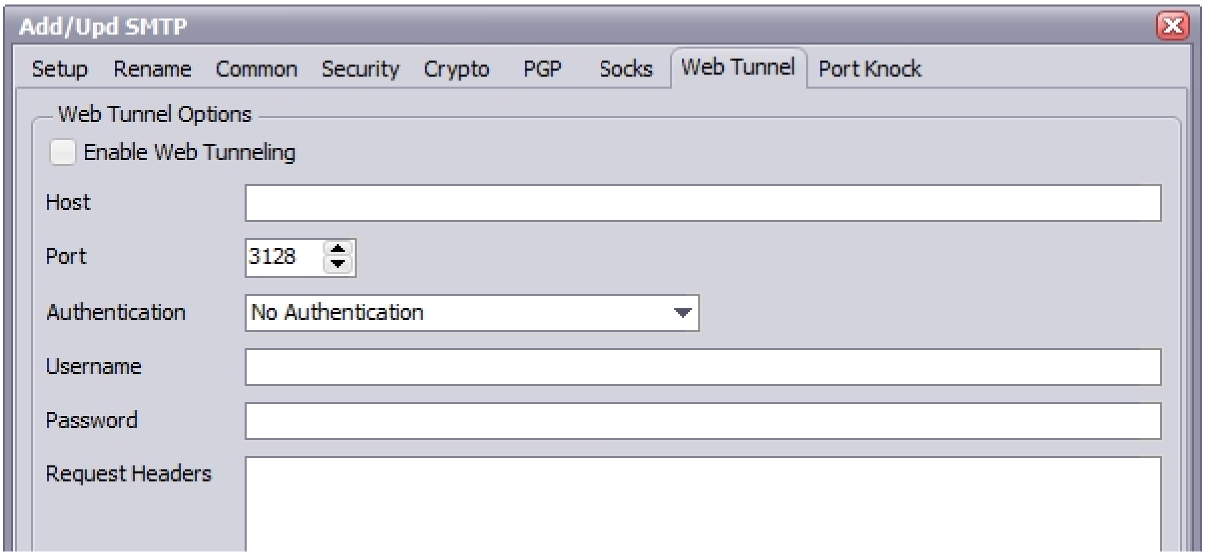
□ Use IPv6

- 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.

Web Tunnel

Web Tunnel Destination Option

"WebTunneling (HTTPS Proxy) is a feature provided by some HTTP proxy servers. This feature is described in RFC 2817 as an HTTP's CONNECT verb (command). Using this command the server opens a transparent communication to remote host."



Web Tunnel Options

□ Enable Web Tunneling

Host

Port 3128

Authentication No Authentication

Username

Password

Request Headers

- Enable Web Tunneling: Enable this option if web tunneling (HTTP proxy) should be used.
- Host: Specifies the address of the HTTP Proxy server.
- Port: Specifies a port on HTTP proxy server to connect to. Default value is 3128.
- Authentication: This option specifies the method of authentication to use with HTTP Proxy server.
- Username: Specifies the username (user id) to be used to authenticate to the HTTP proxy server.
- Password: Specifies the password to be used to authenticate to the HTTP proxy server.
- Request Headers: Use this option to customize Web Tunnel HTTP request headers.

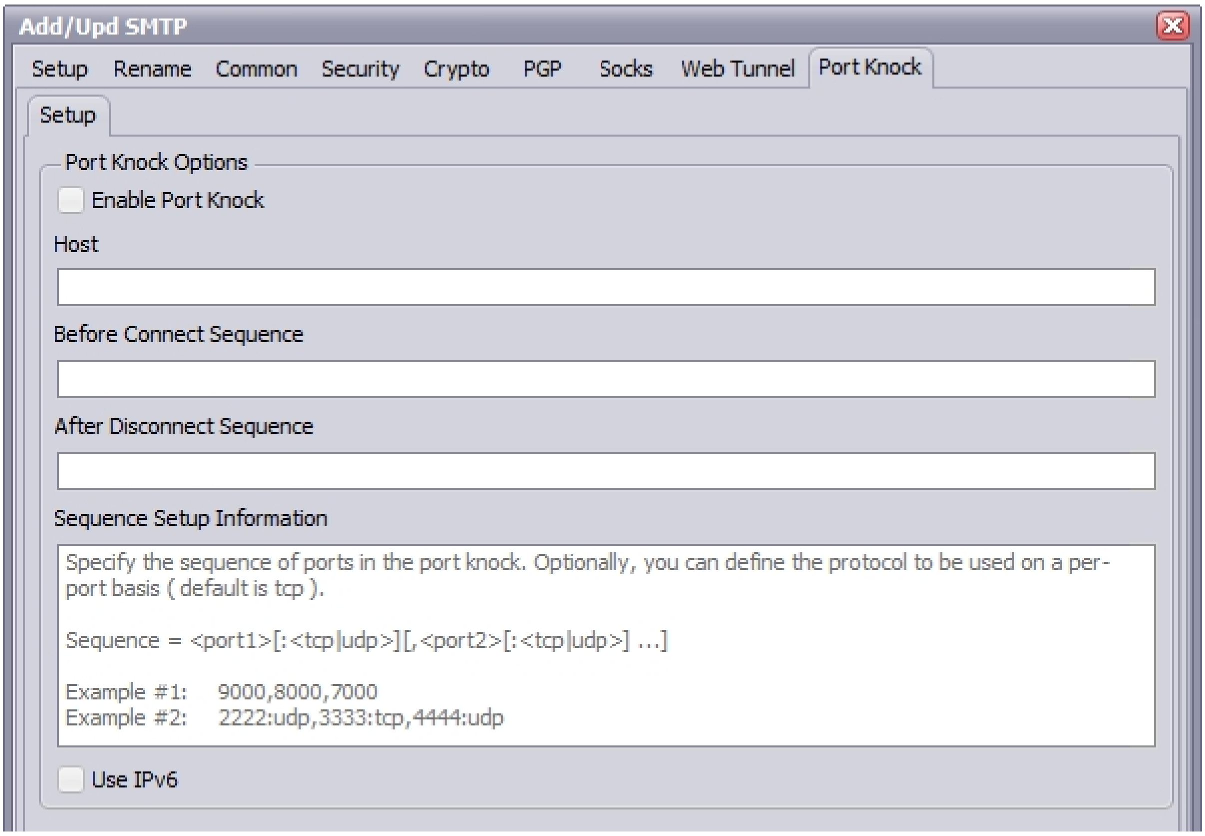
Port Knock

Port Knock Destination Option

"Port knocking is a method of externally opening ports on a firewall by generating a connection attempt on a set of prespecified closed ports. Once a correct sequence of connection attempts is received, the firewall rules are dynamically modified to allow the host which sent the connection attempts to connect over specific port(s). The primary purpose of port knocking is to prevent an attacker from scanning a system for potentially exploitable services by doing a port scan because unless the attacker sends the correct knock sequence, the protected ports will appear closed."

More information about Port Knocking can be found here:

- http://www.portknocking.org/
- http://en.wikipedia.org/wiki/Port_knocking
- http://linux.die.net/man/1/knockd
- http://blog.chipx86.com/2011/02/10/i-invented-port-knocking/



□ Enable Port Knock

Host

Before Connect Sequence

After Disconnect Sequence

Sequence Setup Information

Specify the sequence of ports in the port knock. Optionally, you can define the protocol to be used on a per-port basis (default is tcp).

Sequence = <port1>[:<tcp|udp>][,<port2>[:<tcp|udp>] ...]

```
Example #1:    9000,8000,7000
Example #2:    2222:udp,3333:tcp,4444:udp
```

□ Use IPv6

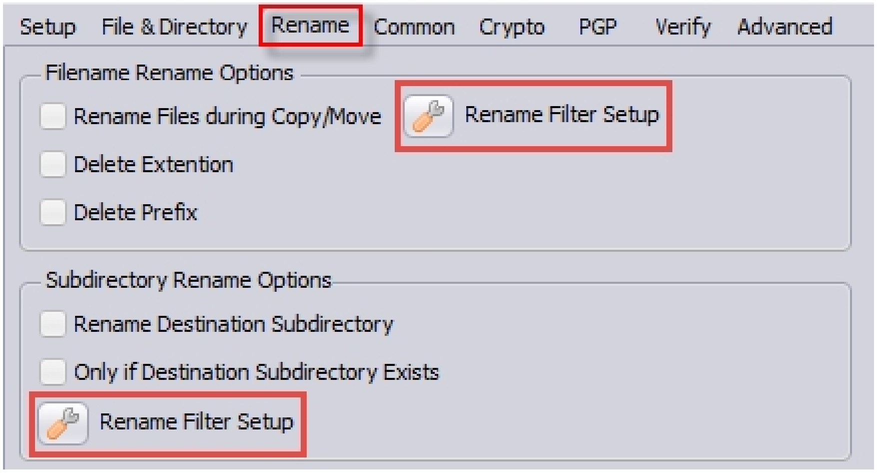
- Enable Port Knock: Enable/Disable Port Knocking option
- Host: With Port Knocking enabled, a sequence of port-hits will go to this address by sending TCP (or UDP) packets.
- Before Connect Sequence: Specify the sequence of ports in the port knock. Optionally, you can define the protocol to be used on a per-port basis (default is tcp).
- After Disconnect Sequence: Specify the sequence of ports in the port knock. Optionally, you can define the protocol to be used on a per-port basis (default is tcp).
- Use IPv6: This option defines whether IP protocol version 6 should be used.

Renaming

Rename Destination Option

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.



Filename Rename Options

☐ Rename Files during Copy/Move

Rename Filter Setup

☐ Delete Extention

☐ Delete Prefix

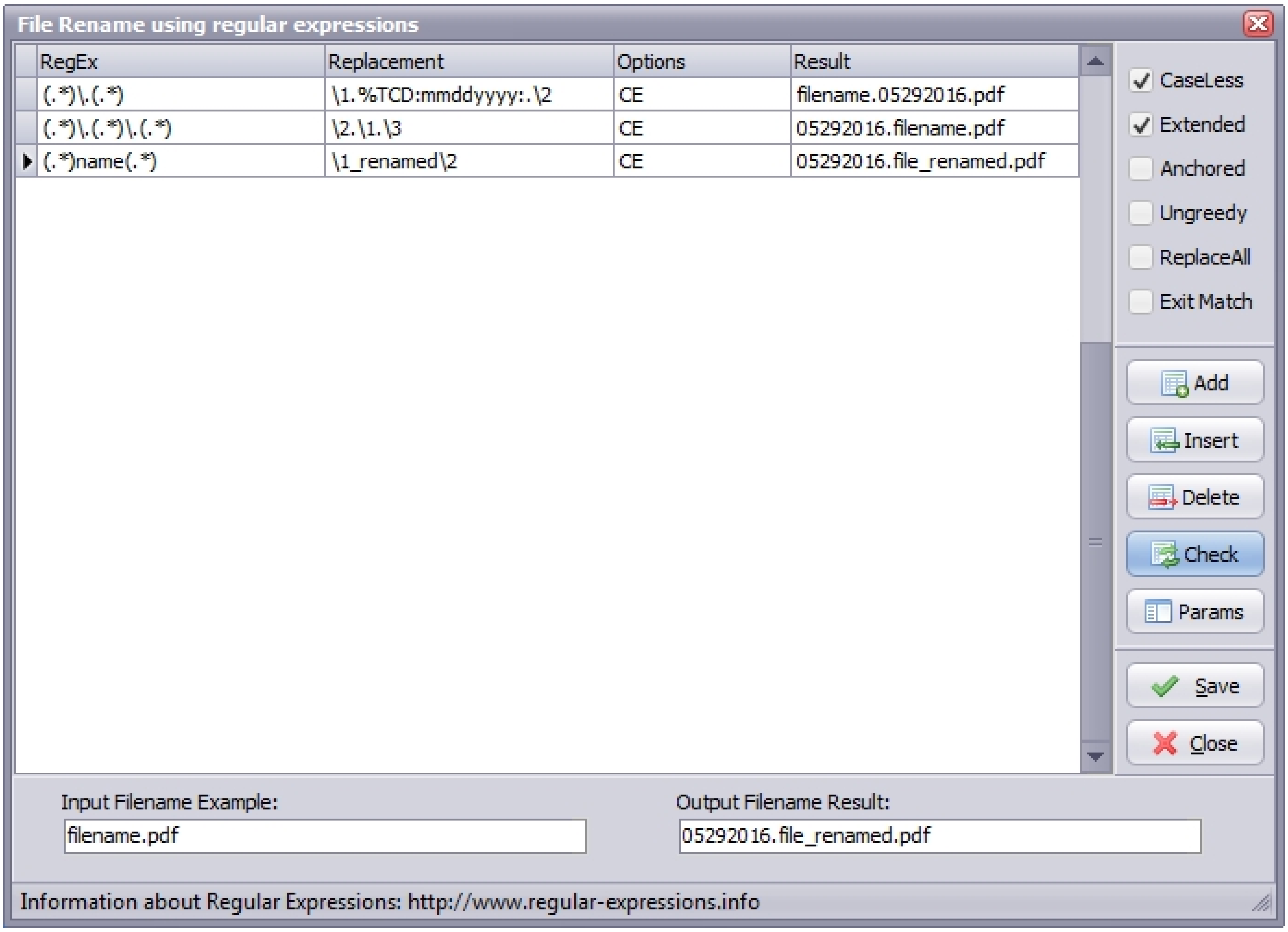
Subdirectory Rename Options

☐ Rename Destination Subdirectory

☐ Only if Destination Subdirectory Exists

Rename Filter Setup

Rename Filter Setup Options



File Rename using regular expressions

	RegEx	Replacement	Options	Result
	(.*)\.(.*)	\1.%TCD:mmddyyyy:.\2	CE	filename.05292016.pdf
	(.*)\.(.*)\.(.*)	\2.\1.\3	CE	05292016.filename.pdf
▶	(.*)name(.*)	\1_renamed\2	CE	05292016.file_renamed.pdf

☑ CaseLess

☑ Extended

☐ Anchored

☐ Ungreedy

☐ ReplaceAll

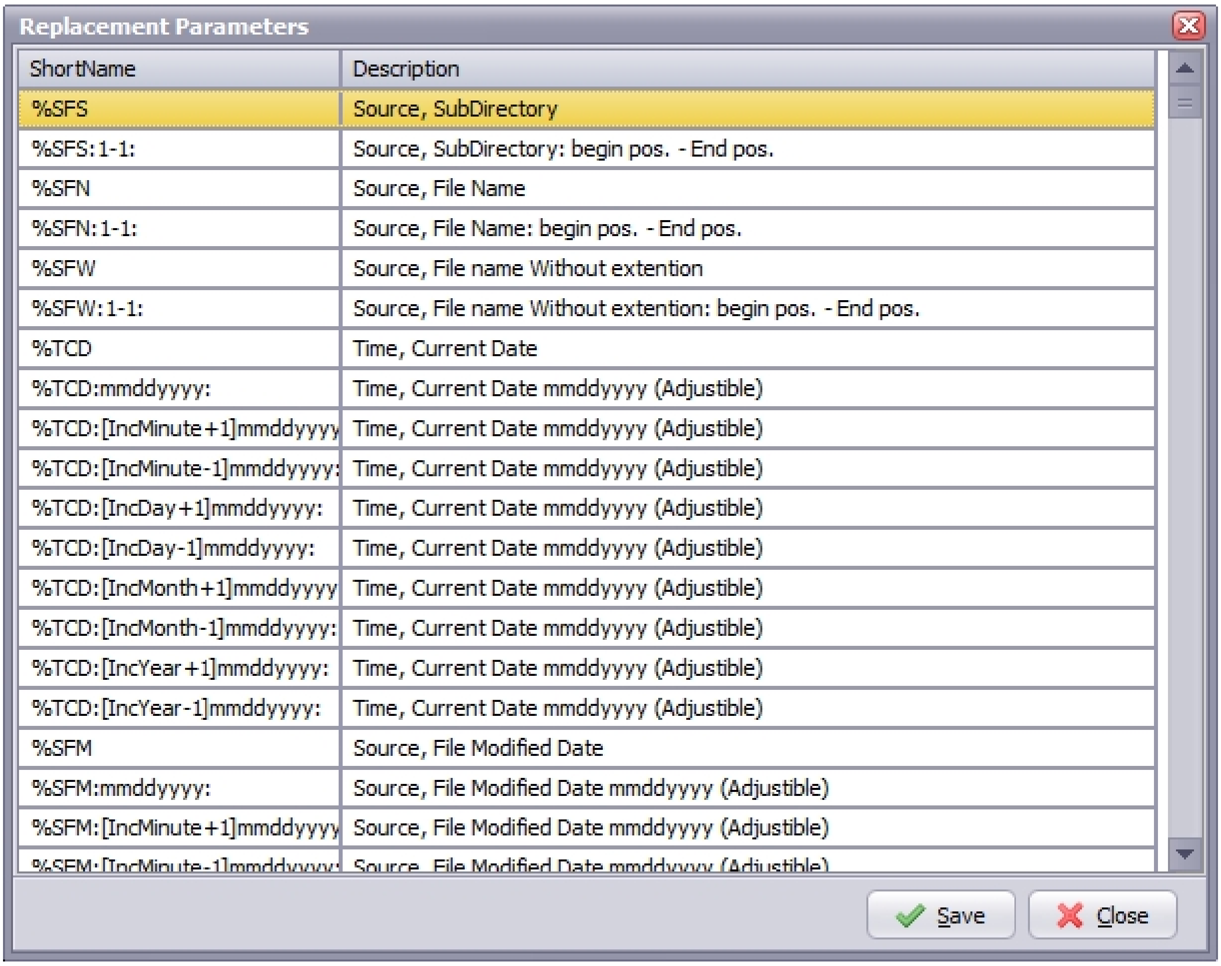
☐ Exit Match

Input Filename Example: filename.pdf

Output Filename Result: 05292016.file_renamed.pdf

Information about Regular Expressions: http://www.regular-expressions.info

- 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.



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 extention
%SFW:1-1:	Source, File name Without extention: begin pos. - End pos.
%TCD	Time, Current Date
%TCD:mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncMinute+1]mmddyyyy	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncMinute-1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncDay+1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncDay-1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncMonth+1]mmddyyyy	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncMonth-1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncYear+1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%TCD:[IncYear-1]mmddyyyy:	Time, Current Date mmddyyyy (Adjustible)
%SFM	Source, File Modified Date
%SFM:mmddyyyy:	Source, File Modified Date mmddyyyy (Adjustible)
%SFM:[IncMinute+1]mmddyyyy	Source, File Modified Date mmddyyyy (Adjustible)
%SFM:[IncMinute-1]mmddyyyy:	Source, File Modified Date mmddyyyy (Adjustible)

- 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.

FAQ

SFTP

SFTP connection to the server is not established. WTF?

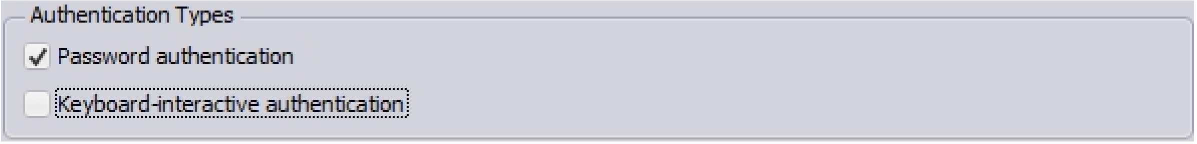
You execute a rule which uses SFTP and … nothing. Connection is not established.

SSH family of protocols is complex and various SFTP servers interpret the specifications differently. This leads to the problem, when to connect and interoperate with some server you need to select the right combination of SSH protocol settings.

1. SFTP protocol has it's own versions (LimagitoX supports SFTP versions 2 to 6). The server and LimagitoX must have the overlapping set of enabled versions. If the server is configured to support only SFTP 3 and LimagitoX has only versions 4 to 6 enabled, then you don't get a connection. You need to check and adjust Versions property of LimagitoX. Moreover, some servers work correctly only when just one version (SFTP 3) is enabled. I.e. you might need to enable just SFTP 3 in LimagitoX in order to successfully work with such server.

2. If the server closes connection without reporting any error, this usually means that you are connecting to the buggy server, which doesn't interpret the LimagitoX client request correctly. What does this mean? LimagitoX sends the list of known algorithms to the server. The server must ignore the unknown entries in the list of algorithms. However many servers crash or close connection when they come across the name of the algorithm, that they don't understand. In particular, all 3.x versions of OpenSSH do this. In this case you need to turn off all algorithms besides the very old and well-known (listed below). LimagitoX tries to detect the old servers automatically and disable the newer algorithms. This is controlled by the 'Auto Adjust Ciphers' option (default enabled). In most cases this solves the problem. If it does not, disable the 'Auto Adjust Ciphers' option and enable the 'Restrict Algorithms' option. This will turn off all algorithms besides the very old and well-known (forced).

3. In some cases users had to disable the Keyboard-interactive authentication in order to get their connection working.



Authentication Types

☑ Password authentication

□ Keyboard-interactive authentication