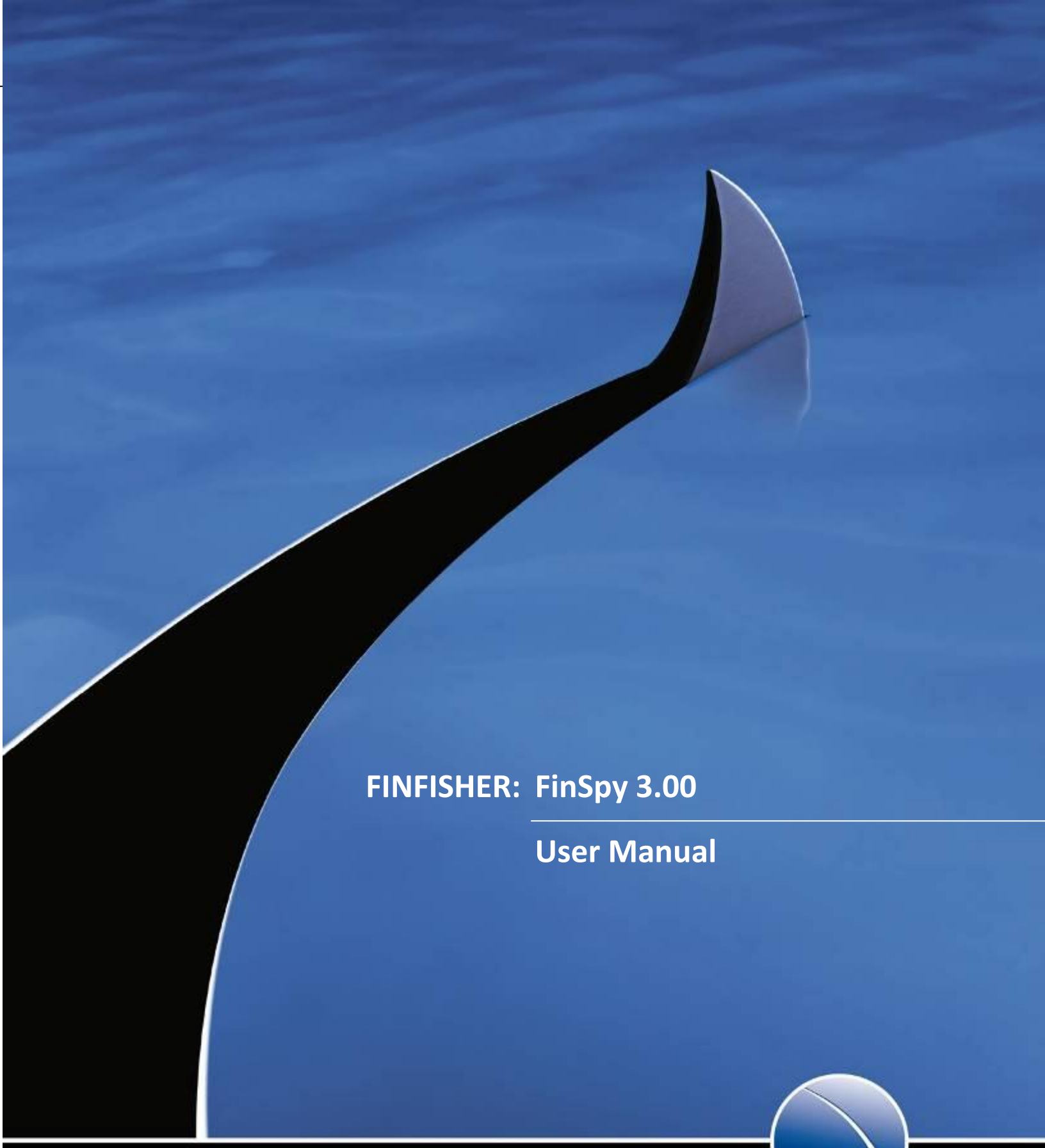


FINFISHER: FinSpy 3.00

User Manual

FINFISHER
IT INTRUSION

WWW.GAMMAGROUP.COM

Date 2011-06-05

Release information

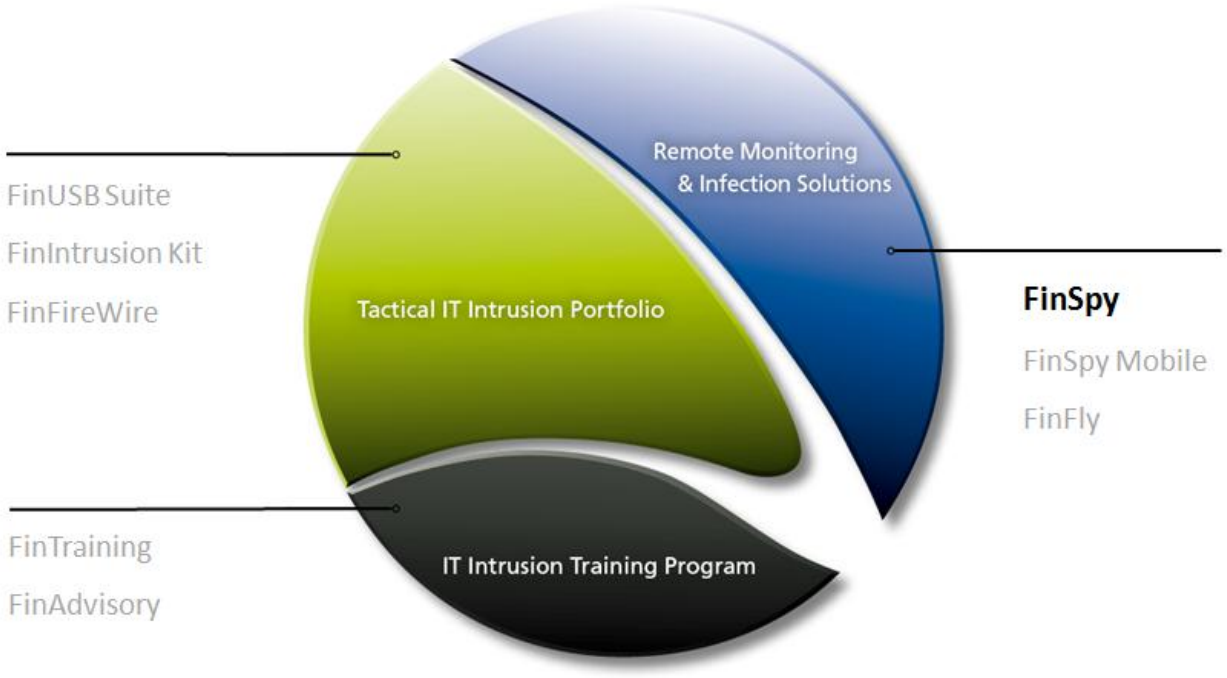
Version	Date	Author	Remarks
1.0	2010-05-13	AH	Initial version
1.1	2010-05-26	HT	Change licensing Add Remote and Offline Master configuration
1.2	2010-05-27	AH	FinSpy Agent: Almost complete Screenshot Replacement FinSpy Master: Change Remote and Offline Master FinSpy Master: Add manual update Misc: Minor changes on different Locations
1.3	2010-07-21	AH	Update to FinSpy 2.40
1.4	2010-08-02	LH	FinSpy Agent: Added section “Target Licensing”.
1.5	2010-08-03	AH	FinSpy Agent: Added section “Visualized Data”.
1.6	2010-10-16	AH	Update to FinSpy 2.50
1.7	2010-10-22	AH	Added Hardware Setup Section
1.8	2011-01-10	AH	Update to FinSpy 2.60
1.9	2011-06-05	AH	Update to FinSpy 3.00

Table of Content

1 OVERVIEW

FinSpy is designed to help Law Enforcement and Intelligence Agencies to remotely monitor computer systems and get full access to:

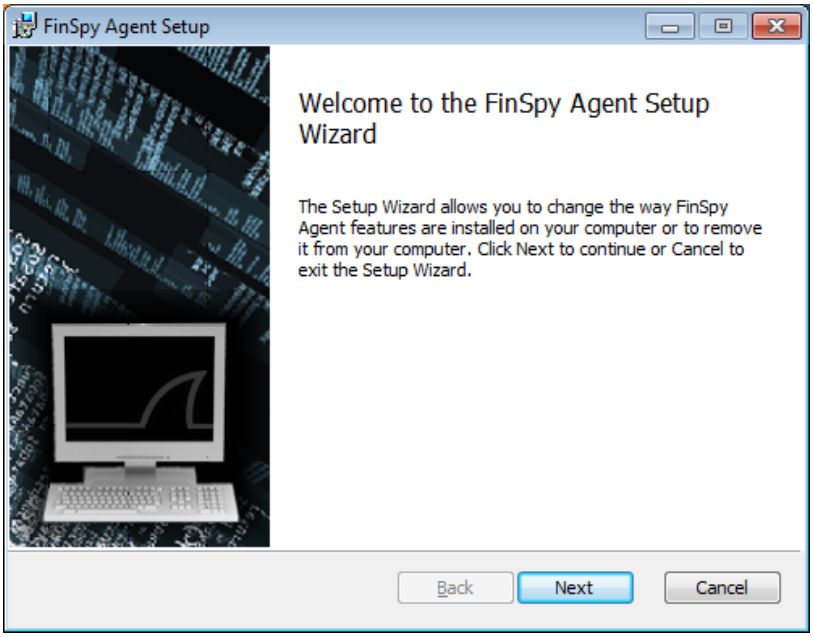
- **Online Communication**: Skype, Messengers, VoIP, E-Mail, Browsing and more
- **Internet Activity:** Discussion Boards, Blogs, File-Sharing and more
- **Stored Data:** Remote access to hard-disk, deleted files, crypto containers and more
- **Surveillance Devices:** Integrated webcams, microphones and more
- **Location:** Trace computer system and monitor locations



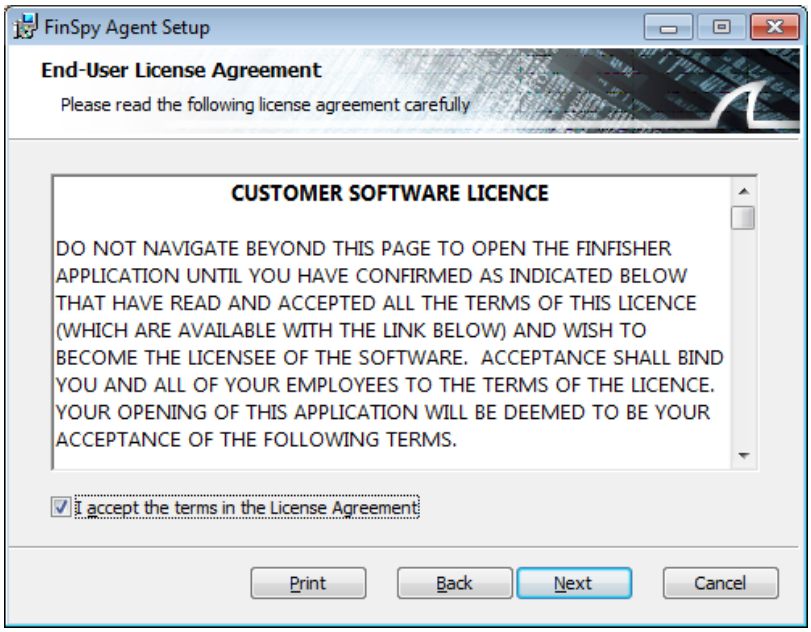
2 FINSPY AGENT

2.1 FinSpy Agent – Installation

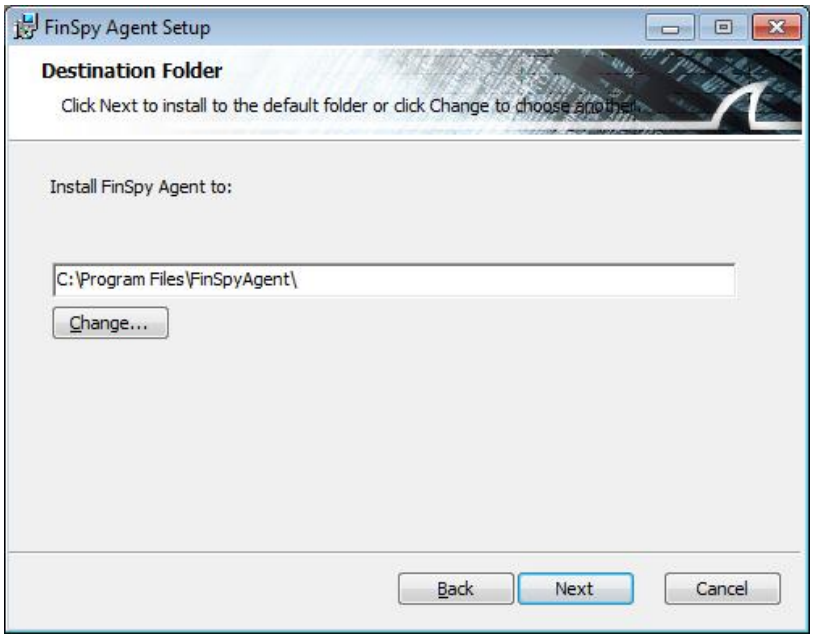
To install FinSpy Agent software, run the setup and follow the steps as shown. Click Install and Finish. No further settings are necessary.

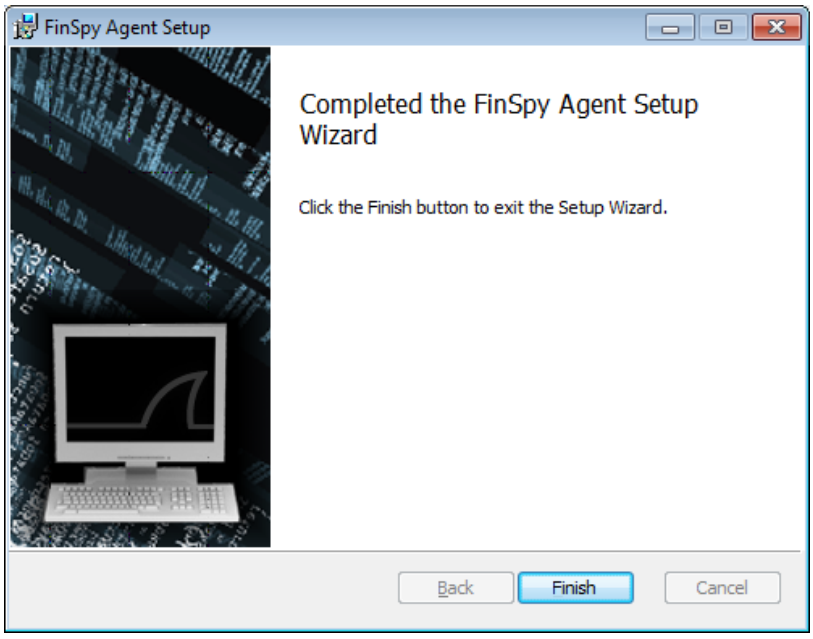


Confirm the license agreement.



Insert the destination folder for the installation.





2.1.1 FinSpy Agent – Additional Software

To operate a computer as a FinSpy Agent the following preparations must be done.

2.1.1.1 Microsoft .NET Framework

The Microsoft .NET Framework is a software framework that can be installed on computers running Microsoft Windows operating systems. It is necessary to have the .NET Framework >= 3.5 SP1 installed to run the FinSpy Agent software.

The framework can be downloaded and installed from:

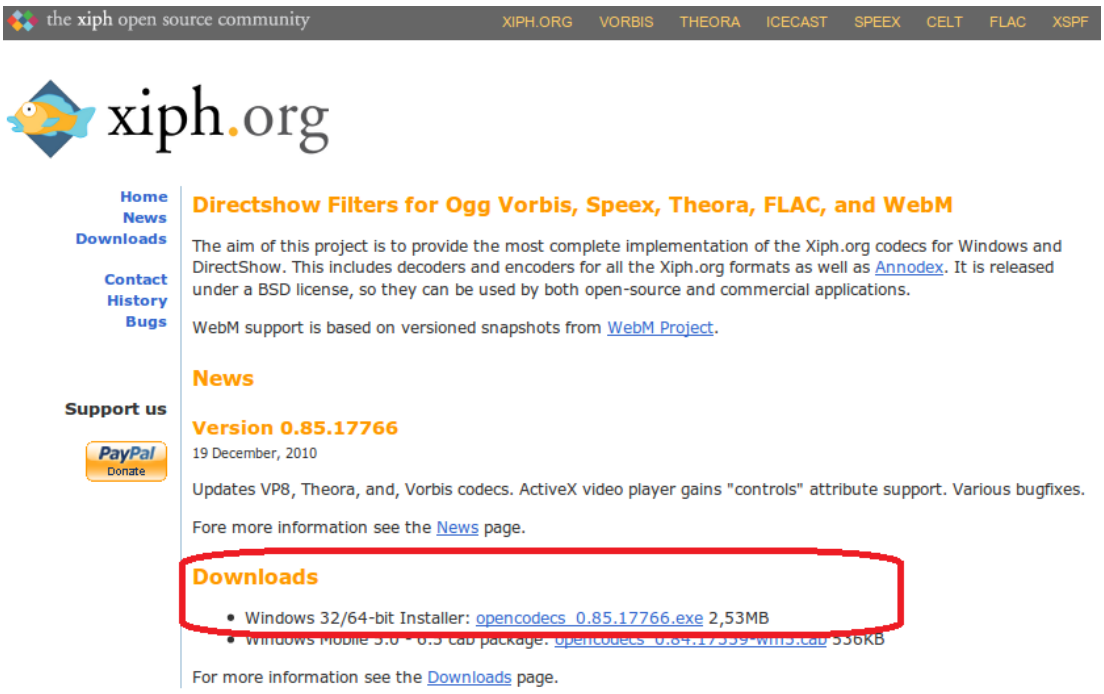
http://msdn.microsoft.com/en-us/netframework/default.aspx

2.1.1.2 OGG Theora Codec

Theora is a free and open video compression format. It must be installed to play Audio and Video.

The codec can be downloaded and installed from:

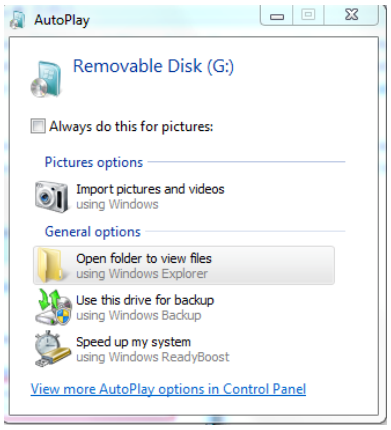
http://www.xiph.org/dshow/



Just follow the instructions of the installation steps. No further changes need to be done. All Audio and Video can now be played within Windows Media Player.

2.1.1.3 Disable AutoPlay

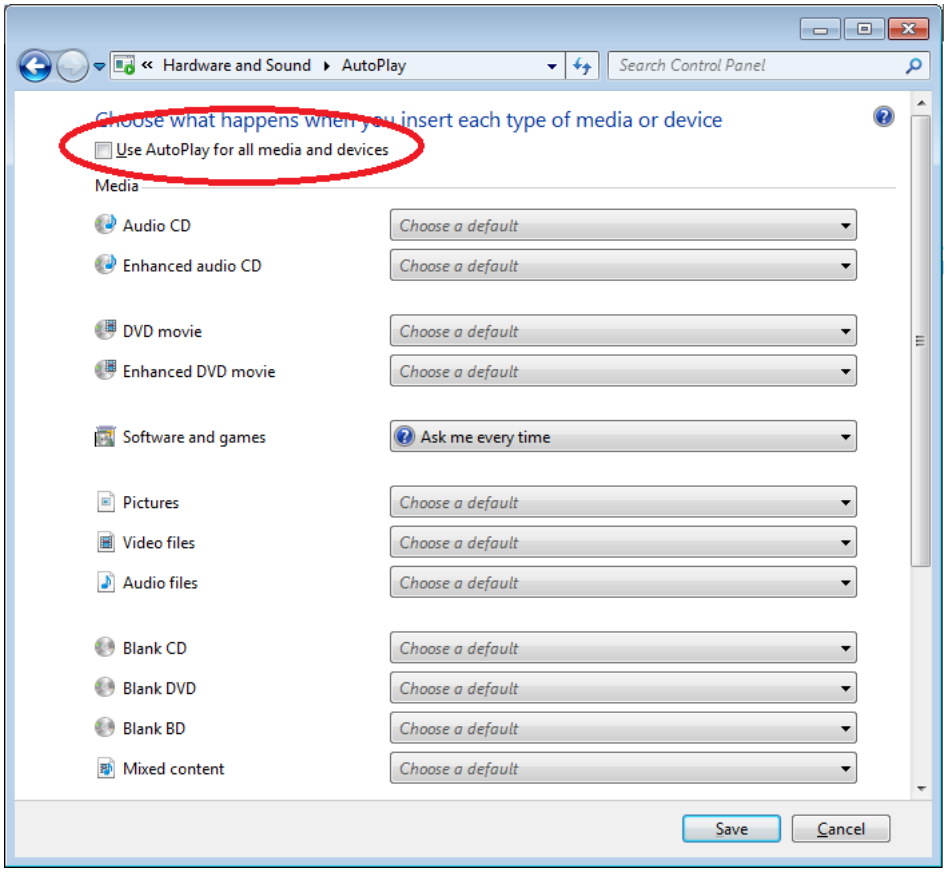
AutoPlay feature enable Windows to pop up the default options when a removable drives like USB flash drive or CD ROM is inserted.



AutoPlay feature is, by default, disabled in Windows 7 due to security reasons. To check if Autorun is disabled on the installation follow the steps.

To disable Autorun:

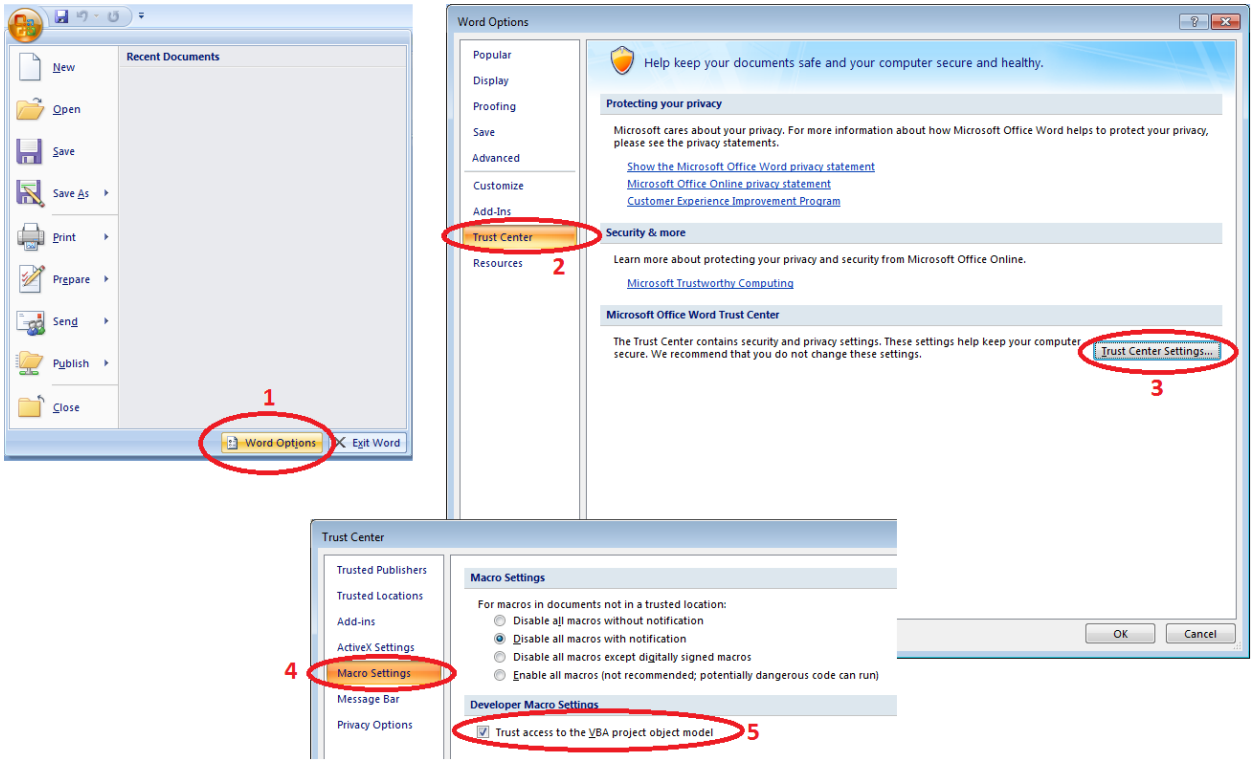
1. Go to **Control Panel\Hardware and Sound\AutoPlay**.
2. Uncheck **Use AutoPlay for all media and devices**
3. Click **Save.**



2.1.1.4 Microsoft Office

To be able to use the FinSpy Agent Office Document infection it is mandatory to change the Trust Center settings within Microsoft Word 2003 or 2007.

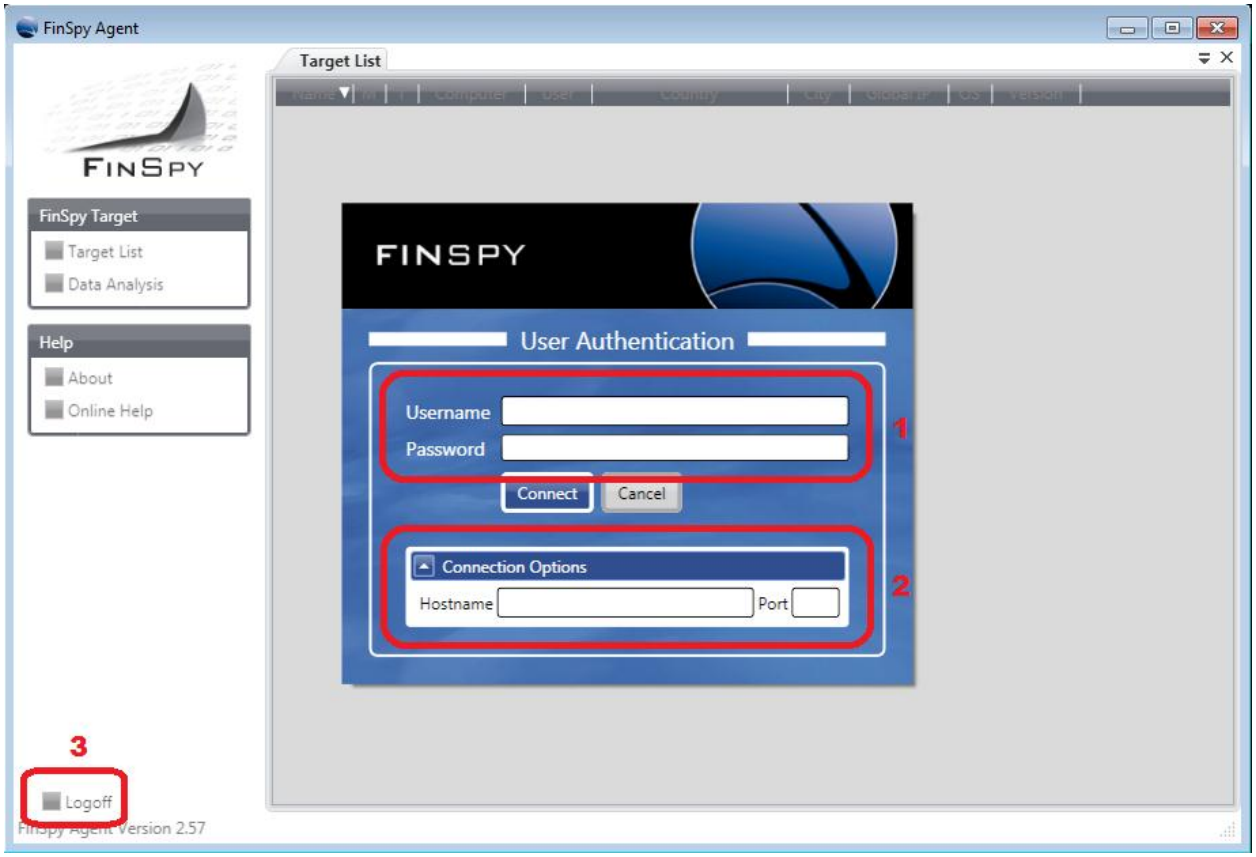
After clicking on the Ribbon of word there is “Word Options” (1) in below corner which will open a new dialog. On the left side is the option “Trust Center” (2) and “Trust Center Settings” (3). Again, a dialog will open. On “Macro settings” (4) and “Trust access to the VBA project object model” (5) must be checked! If not, FinSpy Agent will not be able to infect Microsoft Word (.doc) documents.



2.2 FinSpy Agent – User Manual

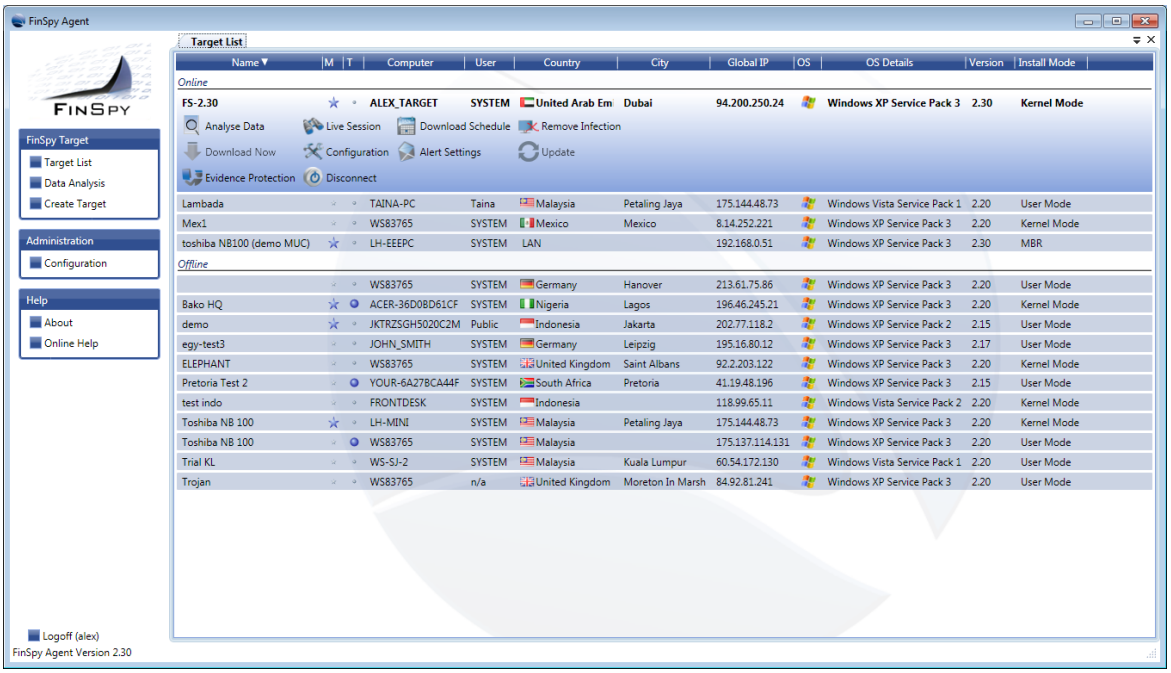
2.2.1 Quick Start and Overview

This chapter describes the handling and layout of FinSpy Agent user interface. To start the FinSpy Agent there will be an icon on the Desktop which needs to be clicked and which will start the main interface.



1. Username and password
2. Address and port of FinSpy Master to which the FinSpy Agent connects
   This data will be remembered after the first successful login
3. Logoff from the FinSpy Master

After a successful login the main interface will open. It shows the main interface of the FinSpy Agent.



Name	Description
Data Analysis	Monitors and analyzes data of a selected FinSpy Target or all FinSpy Targets.
Create Target	It will open a wizard which guides easily through the creation of a FinSpy Target.
Configuration	Basic Settings for the FinSpy Agent and FinSpy Master can be defined.
Show Logfiles	Gives the possibility of viewing the FinSpy Master system logfiles.
Agent List	Information about FinSpy users, their user rights, logins and current connections.
License Information	Displays information regarding the license.
About	Shows the FinSpy Agent version and software agreement.
Online Help	Connects to online help on the Gamma Group homepage via internet.

2.2.2 Target List

The Target List contains all actions to manage data and FinSpy Infection of a FinSpy Target. All FinSpy Targets are listed in two tables under the following categories:

The following information of infected FinSpy Targets is available:

Name	Description
Name	Name of FinSpy Installer Package (changeable after FinSpy Infection)
M (Data on Master)	New downloaded data available on FinSpy Master
T (Data on Target)	New data available on FinSpy Target (data is ready to download)
UID	FinSpy Target Unique Identifier
Computer	System Name of Target System
User	Username under which the FinSpy Infection operates
Country	Country in which the FinSpy Target is located (detected by public IP)
City	City where the FinSpy Target is located (detected by public IP)
Global IP	Public IP address of the FinSpy Target

Local IP	IP address of the FinSpy Target System
OS	Icon representing the Operating System running on the FinSpy Target machine
OS Details	Operating System including Service Pack which runs on the FinSpy Target machine
Target Time	FinSpy Target local time
Time Zone	FinSpy Target time zone and Daylight Saving Indicator
Alarm	Indicator which shows if an Alert was set
Version	Software Version of the FinSpy Target
Install Mode	This indicates if the FinSpy Target is installed in • MBR (Master Boot Record) • Kernel Mode (as Administrator) • User Mode
License	Shows the License ID of the FinSpy Target

Online: List of FinSpy Targets connected to the internet and FinSpy Master
Offline: List of FinSpy Targets currently not connected to Internet and FinSpy Master
Archived: List of FinSpy Targets not infected anymore

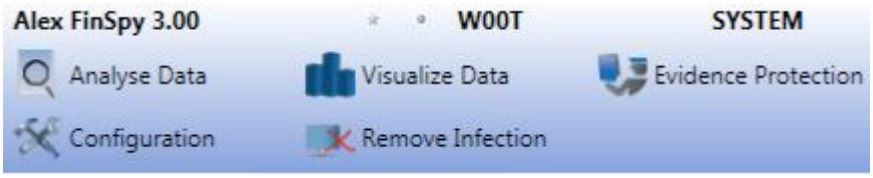
Clicking on a specific target opens all possible actions. Available actions depend on the status of the FinSpy Target (offline/online).
Right-Clicking on any column header allows the user to choose which columns shall be displayed.

2.2.2.1 Target List – Online

The possible actions of an online target are:

Name	Description
Analyse Data	Analyzes data which is already downloaded and available on the FinSpy Master
Visualize Data	Shows the recordings on a visual graph
Evidence Protection	Enables checking of Activity Logging and proofing evidence
Configuration	Management of the FinSpy Target
Live Session	Opens a live session to monitor a FinSpy Target live
Update	Will update the FinSpy Target Core and all the modules.
Remove Infection	Removes the FinSpy Infection from the FinSpy Target
Disconnect	Disconnect from the FinSpy Target

2.2.2.2 Target List – Offline



Possible actions for an infected offline target. An offline target still collects data locally, which can be downloaded any time the FinSpy Target goes online.

Name	Description
Analyse Data	Analyzes data which is already downloaded and available on the FinSpy Master
Visualize Data	Shows the recordings on a visual graph
Evidence Protection	Enables checking of Activity Logging and proofing evidence
Configuration	Management of the FinSpy Target – even offline
Remove Infection	Removes the FinSpy Infection from the FinSpy Target

2.2.2.3 Target List – Archived

Possible actions for a FinSpy target, which is no longer infected. The recorded data is still persistent on the FinSpy Master but the FinSpy target is not infected anymore.

Name	Description
Analyse Data	Analyzes data which is already downloaded and available on the FinSpy Master

Visualize Data	Shows the recordings on a visual graph
Evidence Protection	Enables checking of Activity Logging and proofing evidence
Remove Data	Removes the recorded data from the FinSpy Master

2.2.2.4 Target List – Target Licensing

The number of FinSpy Targets which can be monitored on the system is part of the license information which is imported on the FinSpy Master during the installation.

After infection, the FinSpy Target has no associated license and all its collecting data features are disabled. The FinSpy Master will allocate a license to the newly infected FinSpy Target, if available.

If there is no license available, the FinSpy Agent can still see the FinSpy Target in the Target List and can only work limited with it until an existing infection is removed.

Previously gathered data can still be analyzed.

Once the license is installed on the FinSpy Target all the features become available and the user gains full control over the FinSpy Target.

If all the licenses are used, the new infected FinSpy Targets will be shown as disabled until a new license is available.

To free a license, an existing infection has to be removed from a licensed FinSpy Target. The infection can be removed immediately from an online FinSpy Target or can be scheduled for removal from an offline FinSpy Target. Either way the license will be freed immediately and allocated to an unlicensed target.

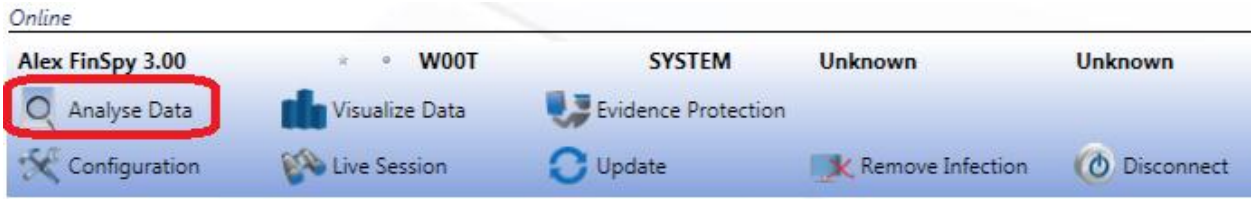
2.2.2.5 Target List – Recorded Data Availability

A star (1) indicates, that there is new “Data on Master” available. This means, new data was downloaded from the FinSpy Target to FinSpy Master.

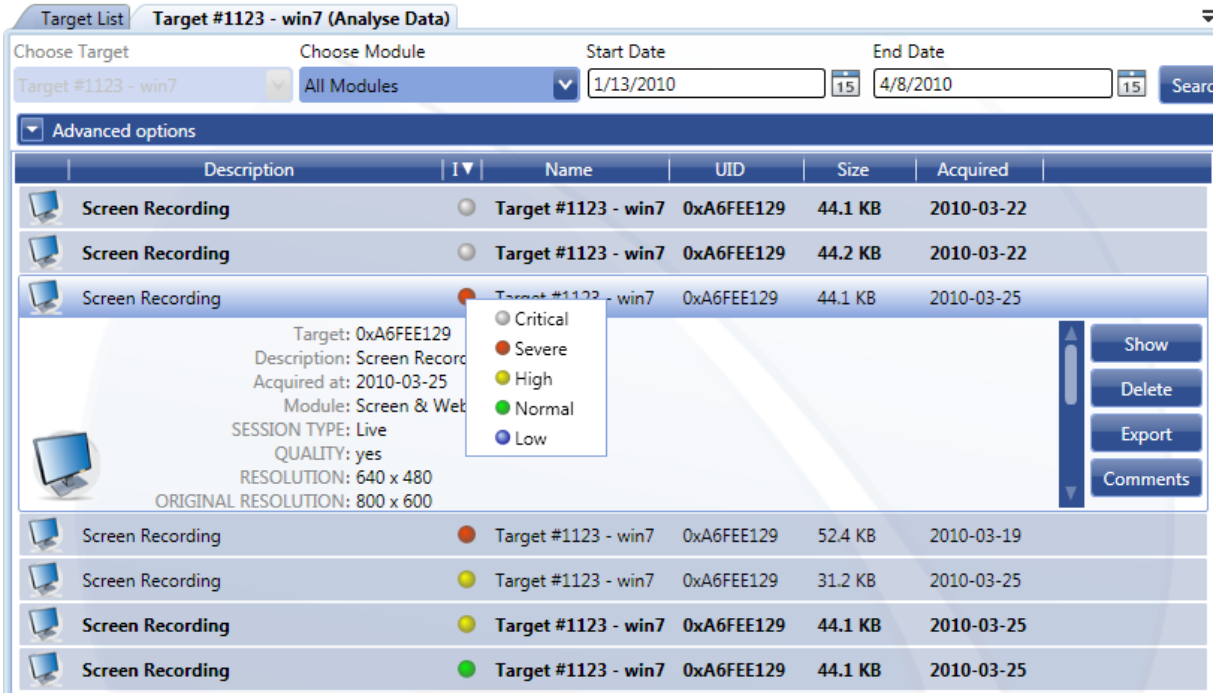
A bullet (2) indicates, there is new “Data on Target” available. This means, there is new recorded data available on the FinSpy Target (e.g. Keylogger recordings, Skype recordings, etc.) which is not transferred to the FinSpy Master, yet.

2.2.3 Analyse Data

Analyse Data gives the possibility of showing all the recorded data which was transferred to the FinSpy Master. The recorded data can be viewed, deleted or exported. “Analyze Data” will show a list of all data recorded of the selected FinSpy Target.

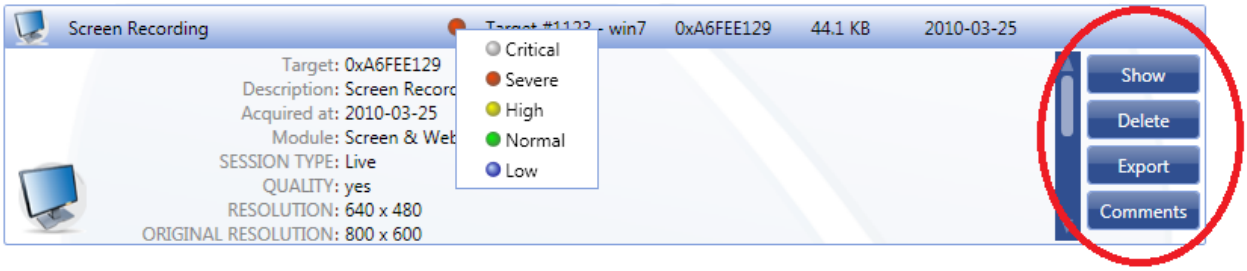


All the data of the selected FinSpy Target is displayed as a list. All new entries in the list are displayed with bold characters. This indicates that the data was not processed yet. Once the data is viewed or exported, the data will not be displayed in bold anymore.



Name	Description
Description	Identifies the module (device/application) of the recorded data set.
I (Importance)	An importance level can be associated to the collected evidence and can be used as ordering criteria. To change the Importance Level, right click in the importance level column of an evidence entry and a popup with all the available importance levels is displayed.
Name	FinSpy Target Name
UID	Unique internal reference to the FinSpy Target
Size	Size of the data set in bytes
Acquired	The date when the data was recorded

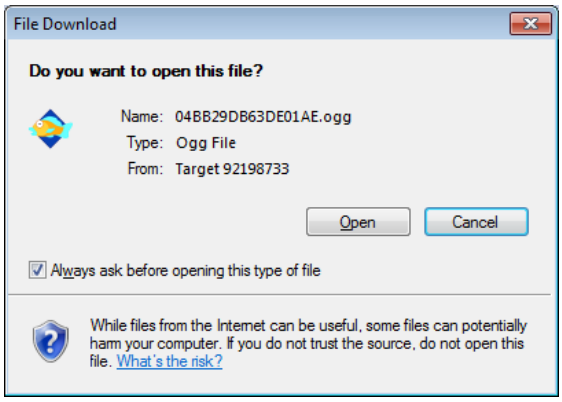
Possible actions for the data entries can be shown and additional information are displayed.



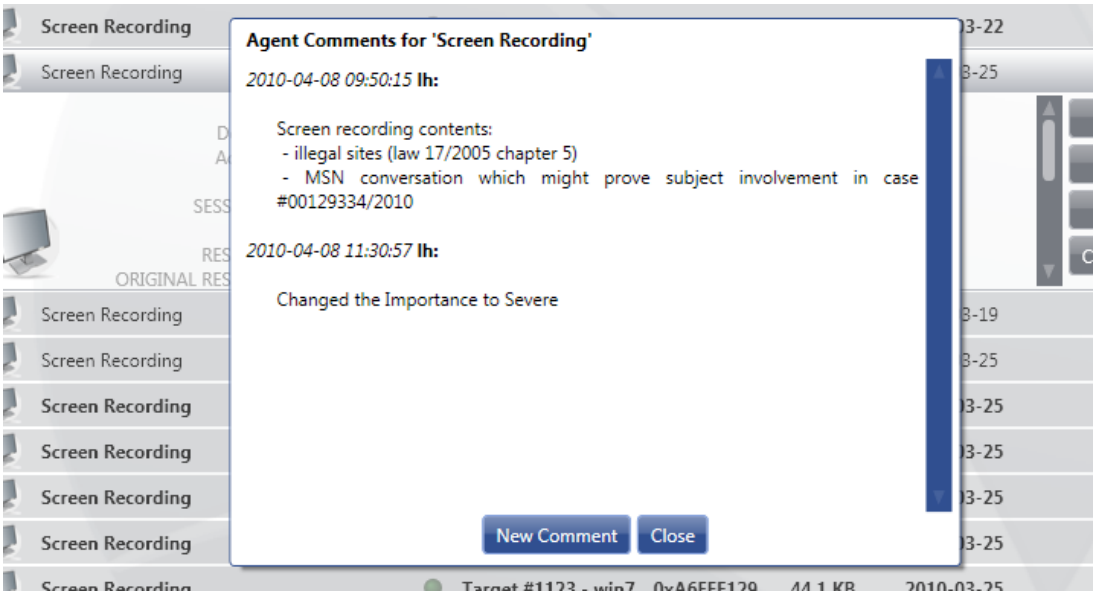
Name	Description
Show	Opens the recorded data. In case of streaming data (video, sound) an external player is opened.
Delete	Deletes the data set from the FinSpy Master.
Export	The data is exported to the FinSpy Agent computer. A folder will open where the data is saved in and the downloaded file selected.

Comments	Opens a window where comments to the data can be stored. Every change of the Importance Level is also logged as a comment.

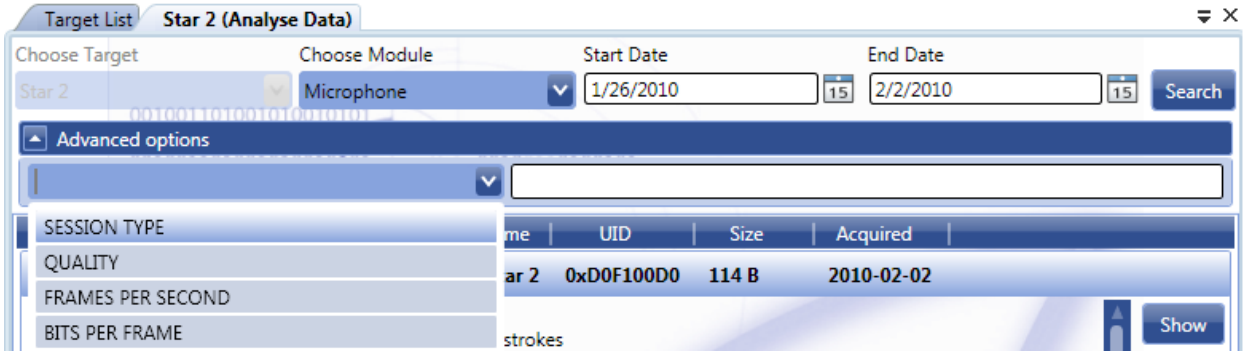
If “Show” is selected a popup may appear which will ask for a confirmation to display the file.



Comments which are once done for a specific data cannot be edited or deleted. The Comments are ordered by time in descending order which means, that the last introduced comment is displayed on top.



There is also the possibility define the search by using filters:

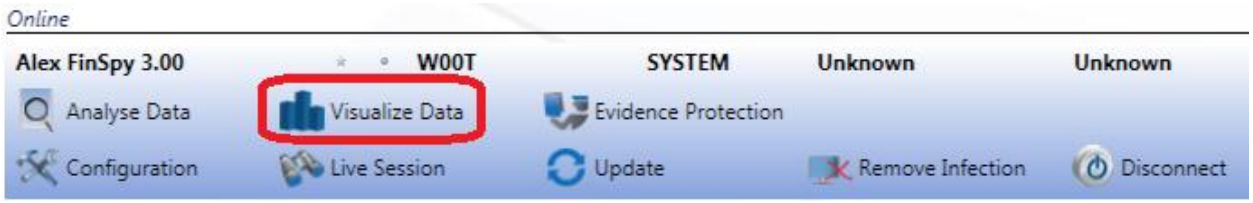


The following filters are available:

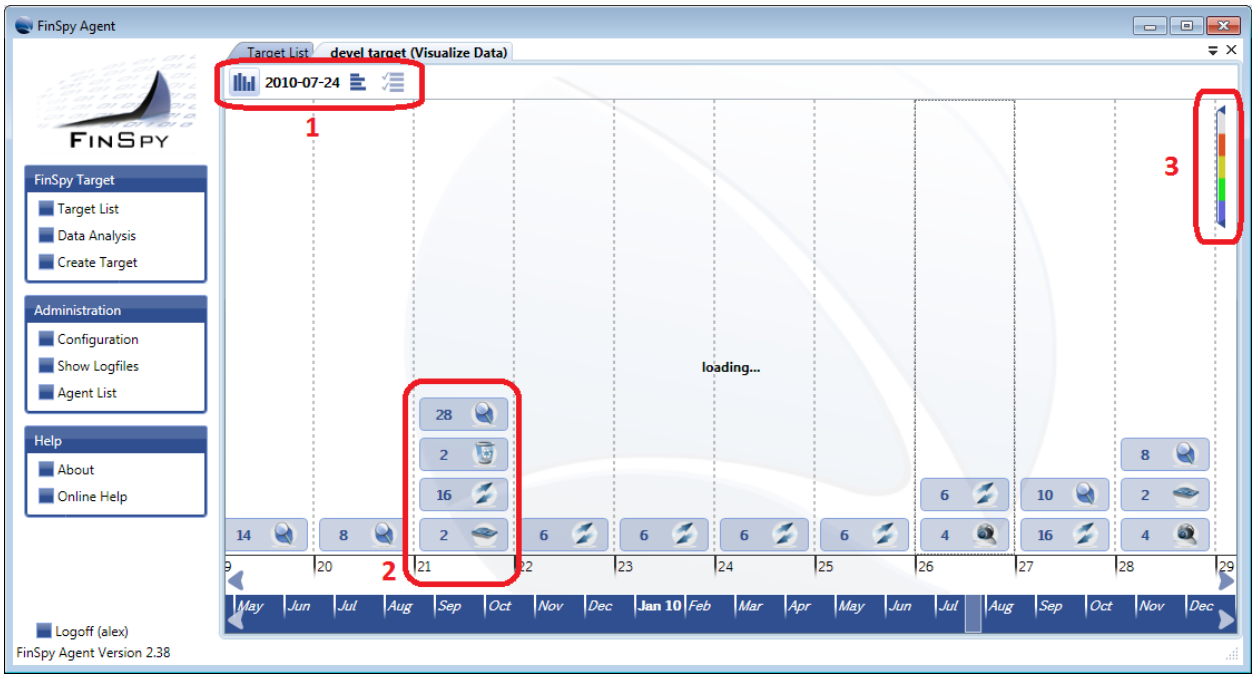
Name	Description
Start – End Date	From which data to which date should be searched
Module	Module by which the data was recorded (e.g. Webcam, Microphone, Keylogger, ...)
Advanced Options	In case a specific module is selected, additional filters can be applied depending on the module(e.g. All targets of a certain time zone)

2.2.4 Visualize Data

Visualize Data enables the FinSpy Agent to display recorded data in a graphical way.



A typical overview will look like the following:

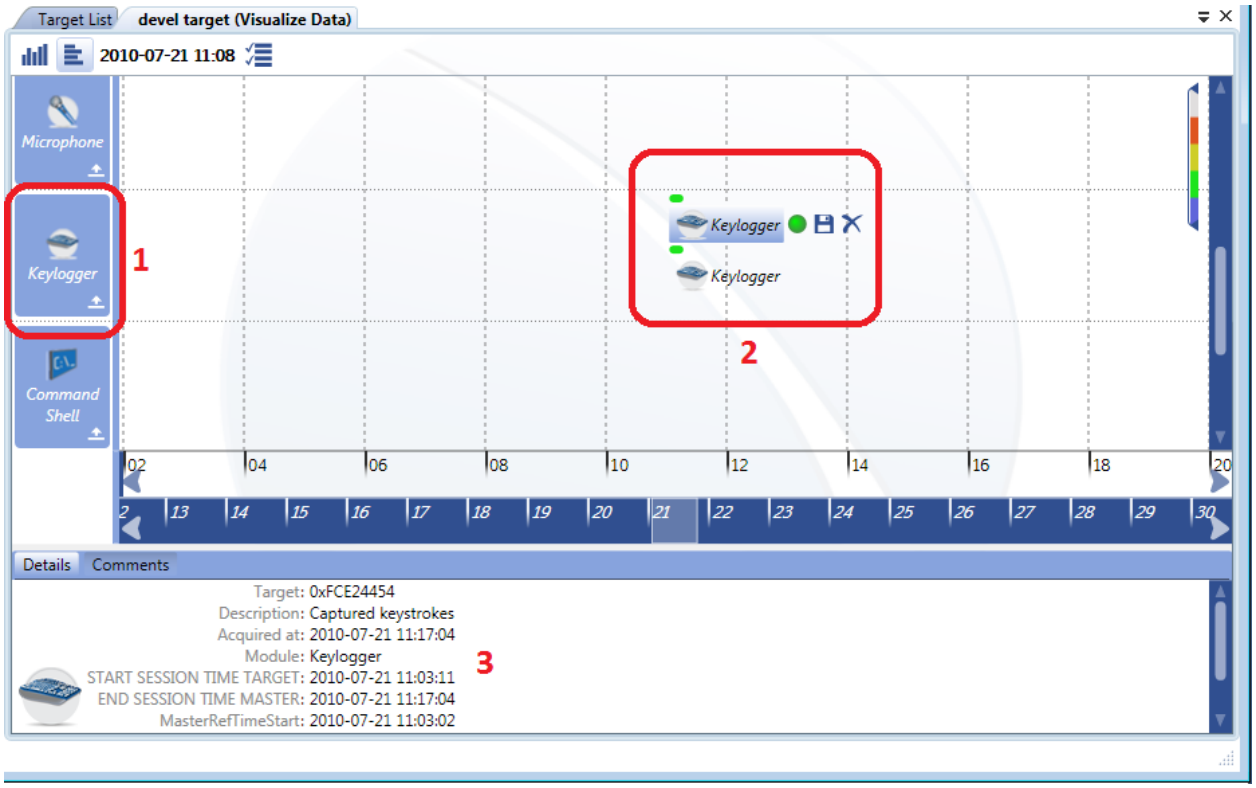


1. The type of visualization. It will give two different graphs. It can be chosen between
   a. Detailed view per day (default)
   b. Detailed view per hour

2. The recorded data on that day. Each data is displayed with the amount of recordings for each module per day.

3. The importance level can be set.

Detailed view per hour:



1. The overview is divided by modules.

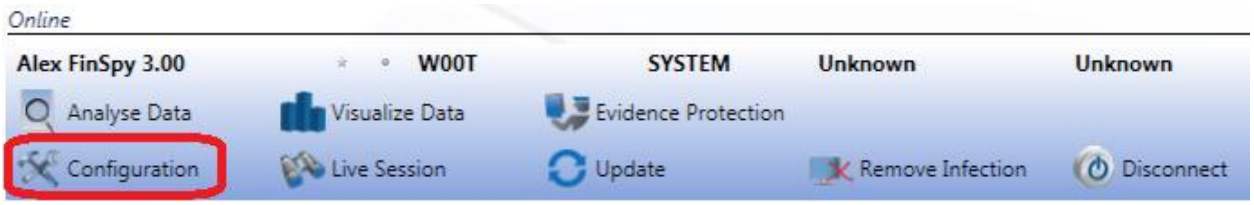
2. Amount of recording per module is shown. Additionally the options “Change Importance”, “Export Record” and “Remove Record” can be selected.

3. Meta-Information for each recording can be viewed if a recording is selected.

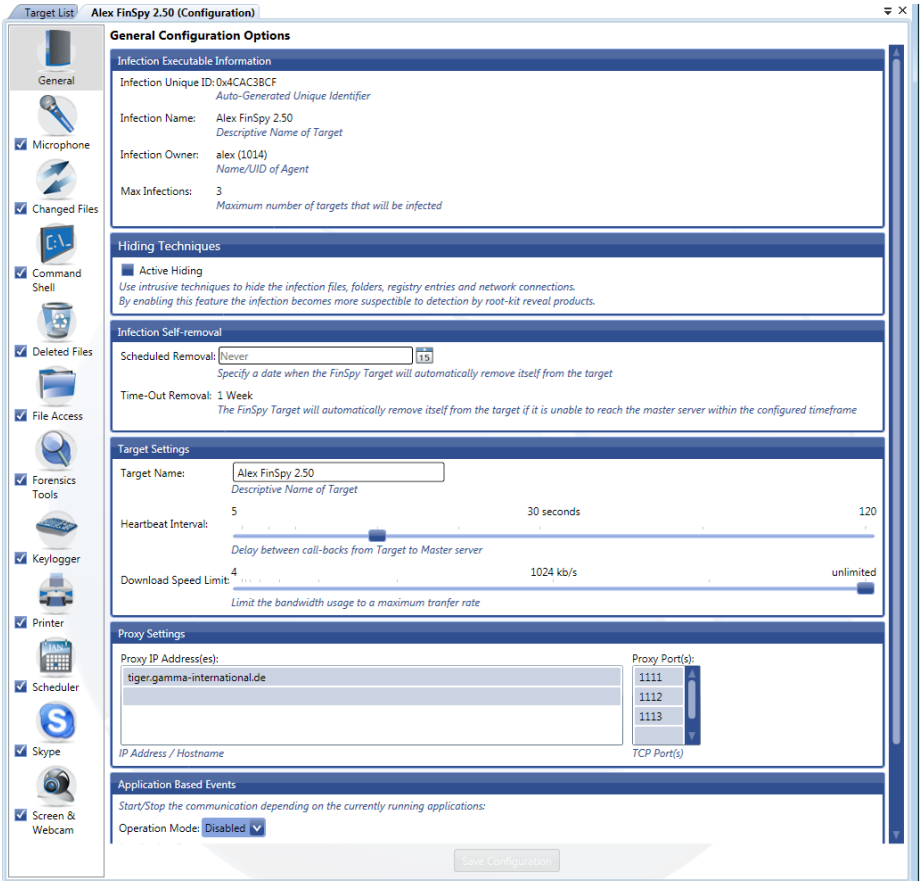
To navigate through date and time the mouse can be used, either via mouse-wheel (up/down) or by dragging the scrollbar.

2.2.5 Configuration

To access the configuration of an infected FinSpy Target, the target needs to be selected and "Configuration" clicked.



A new window opens within the FinSpy Agent. The following image illustrates the layout of the FinSpy target configuration.



This Workspace is divided in two parts. The first part is on the left, which contains the modules and different configuration options and the second is one the right, where module specific configuration options can be set.

Configuration Options:

- General
- Download Schedule
- Alert Settings
- User permissions

The following modules are available:

Module Name	Module Icon	Available on the following OS:
Accesses Files		
Changed Files		
Command Shell		
Deleted Files		
File Access		
Forensics Tools		
Keylogger		
Microphone		

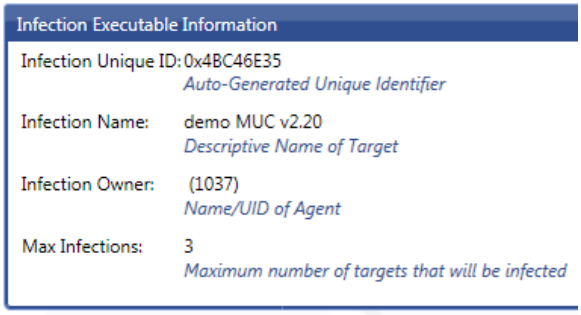
Printer		
Scheduler		
Skype		  
Screen & Webcam	 	 
VoIP		

2.2.5.1 Configuration – General

2.2.5.1.1 Infection Executable Information

This information is not changeable.

- Infection Unique ID: An internal ID of the FinSpy Target Installer
- Infection Name: Given name of the target
- Infection Owner: Internal user ID of the user who generated the FinSpy Target
- Max Infections: Maximum number of FinSpy Targets which can be infected by the device or application



2.2.5.1.2 Hiding Techniques

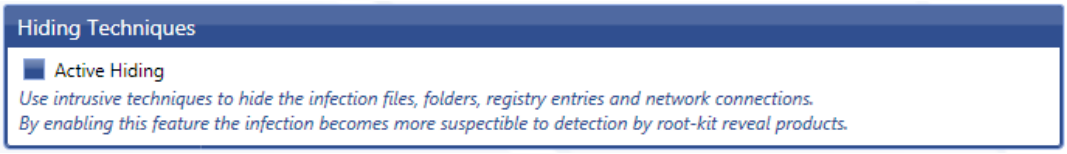
It is possible to activate an advanced hiding method which allows the FinSpy Trojan to be more stealth and extremely hidden.

The following actions are taken if the FinSpy Trojan runs in User-Mode:

- Hides the network connections
- Hides the registry entries
- Hides the Trojan processes

The following actions are taken if the FinSpy Trojan runs in Admin-Mode:

- Hides the network connections
- Hides the Trojan processes

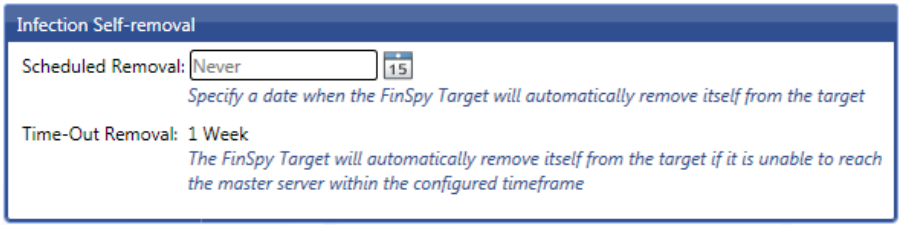


If the Active Hiding is activated it is more likely to be discovered by some root-kit detectors, due to its aggressiveness within the system.

2.2.5.1.3 Infection Self-removal

Computers which never go online may become infected by mistake and spread an infected application through an organization. To avoid keeping offline computers infected still recording data, the FinSpy Target can remove itself.

- Scheduled Removal: Date on which the FinSpy Target removes itself from the infected computer
- Time Out Removal: Time after which the FinSpy Target removes itself from the infected computer, if communication with the FinSpy Master fails (even if there is a functional internet connection). This renewal will be disabled once the FinSpy Target contacts the FinSpy Master for the first time.



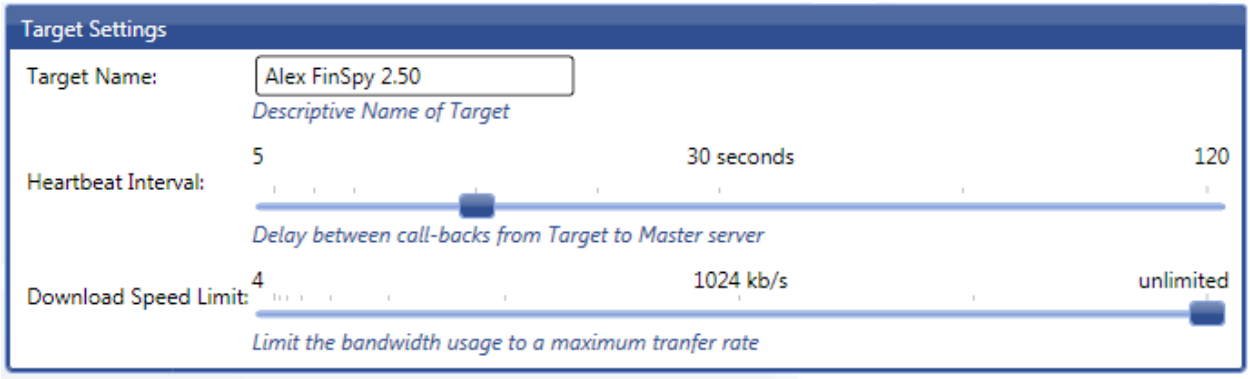
2.2.5.1.4 Target Settings

Behaviour and identification of the FinSpy Target

- Target Name: FinSpy Installer may infect different targets. To separate the FinSpy Targets the previous Target ID of the infected media can be changed

- Heartbeat Interval: The FinSpy target will send “alive” packets in a defined interval to the FinSpy Master. The time of these packets is given in seconds. This is used to update the online/offline status of the FinSpy Target.

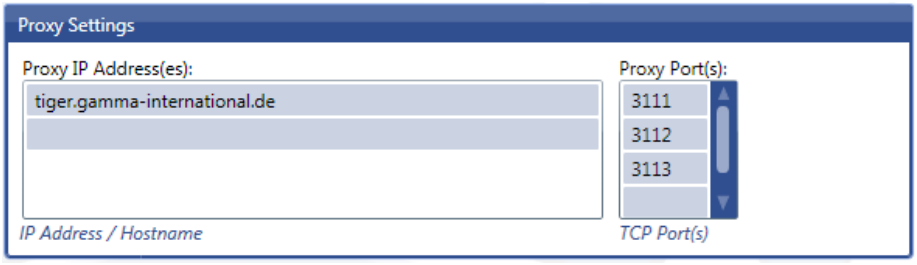
- Download Speed Limit: This option can define the download speed with which the data shall be transferred to the FinSpy Master. This is useful if only a small amount of bandwidth shall be used.



2.2.5.1.5 Relay Settings

The settings of the network configuration between FinSpy Target and FinSpy Master are:

- Relay IP Address: Pre-configured with connected FinSpy Master. This must be the external IP or Hostname address of the FinSpy Master or of the FinSpy Relay. Several IP or hosts can be defined. The infected computer will connect to one of the configured addresses
- Relay Port: Pre-configured with settings retrieved by the FinSpy Master



2.2.5.1.6 Application Based Events

Defines the behavior of the FinSpy Target, if certain applications are running or not running on the FinSpy Target system.

If Operation Mode is set to “Disabled”, the FinSpy Target communication with the FinSpy Master will not be affected by any running application in the system.

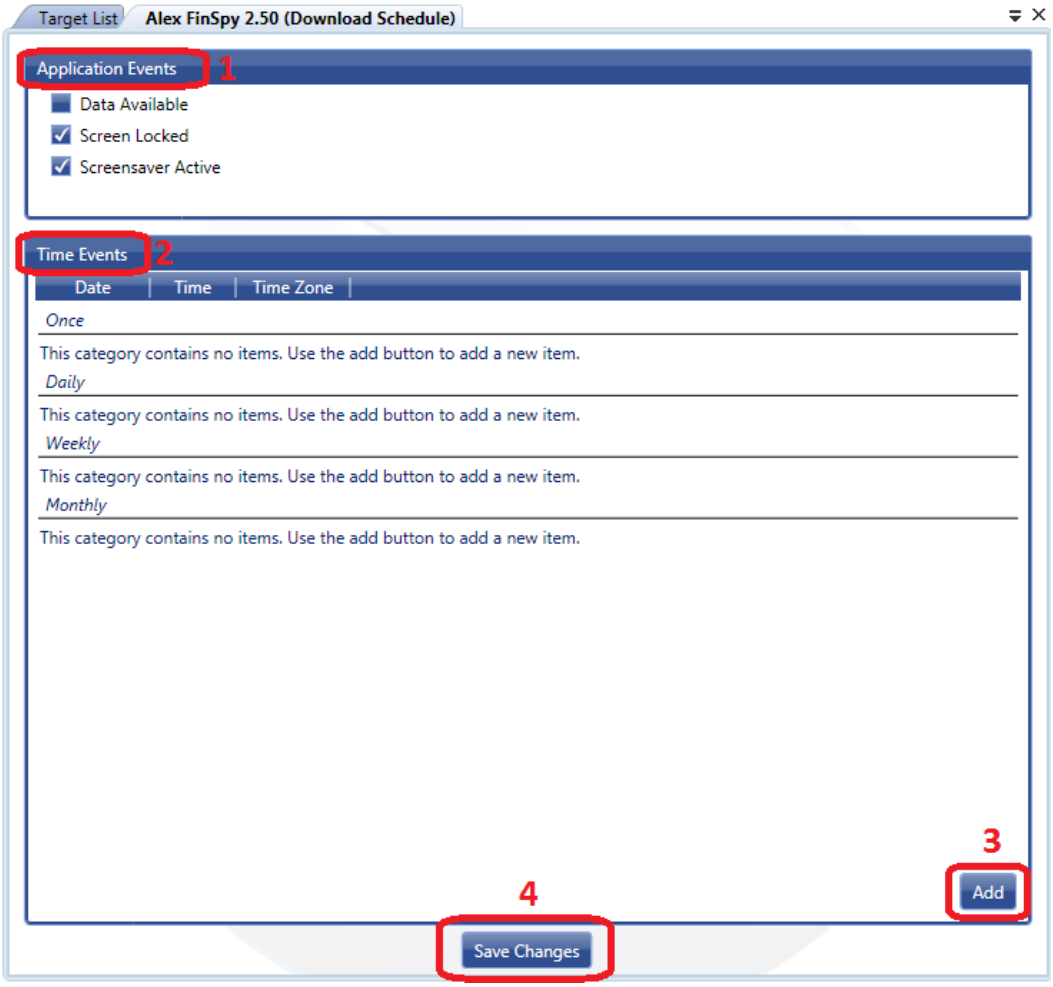
When Operation Mode is set to “Active for Event”, the FinSpy Target will try to connect the FinSpy Master only if the applications listed in the boxes are currently running.

Operation Mode set to “Inactive for Event” suppresses the FinSpy Target communication with the FinSpy Master if one of applications listed in the boxes is currently running.

2.2.5.2 Configuration – Download Schedule

Download schedule will automate downloads of data. Automatic downloads can be initiated by time- and application-based events.

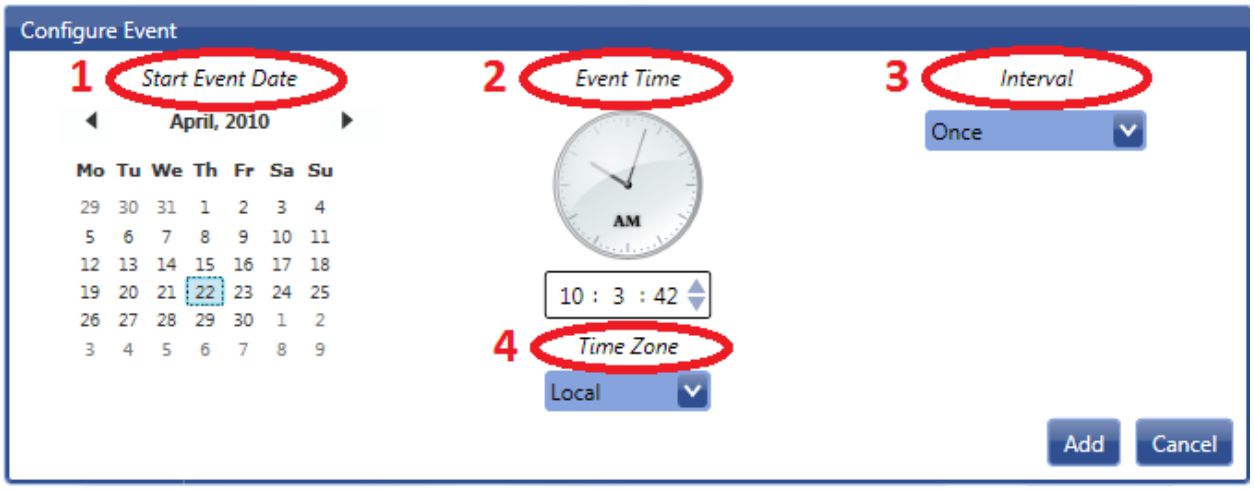
A new tab will open with the separation of “Application Events” (1) and “Time Events” (2). On “Add” (3), new Time Events can be added. “Save Changes” (4) will save all settings for the FinSpy target.



A download of data will be initiated if one of the configured events occurs.

Name	Description
Data Available	As soon as new recorded data is available, the data will be transferred to the FinSpy Master
Screensaver Active	New recorded data will be downloaded to the FinSpy Master if the Screensaver of the target computer is active
Screen Locked	New recorded data will be downloaded to the FinSpy Master if the Computer of the target gets locked

If a new time event is added, a new tab opens in which all parameters of the new time event can be set.

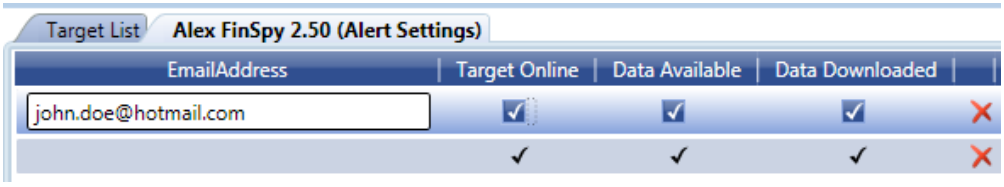


Name	Description
Start Event Date	The first day on which the download starts
Event Time	At which time the download starts
Interval	Interval between the downloads • Once • Daily • Weekly • Monthly
Time Zone	Which time zone should the event refer to • Target • Local • UTC

2.2.5.3 Configuration – Alert Settings

The FinSpy Master can alert via E-Mail if a target status changes. Alert messages are generated by the FinSpy Master. Alerts can be triggered on the following events:

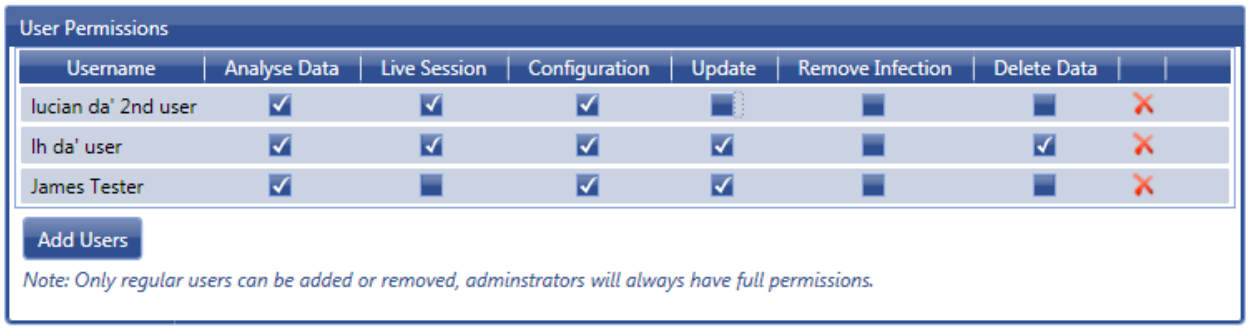
Name	Description
Target Online	An alert will be triggered if a FinSpy Target changes its status from Offline to Online
Data Available	An alert will be triggered if a FinSpy Target has new data recorded which is not transferred to the FinSpy Master yet.
Data Downloaded	An alert will be triggered if the FinSpy Master downloaded new data from the FinSpy Target.



2.2.5.4 Configuration – User Permissions

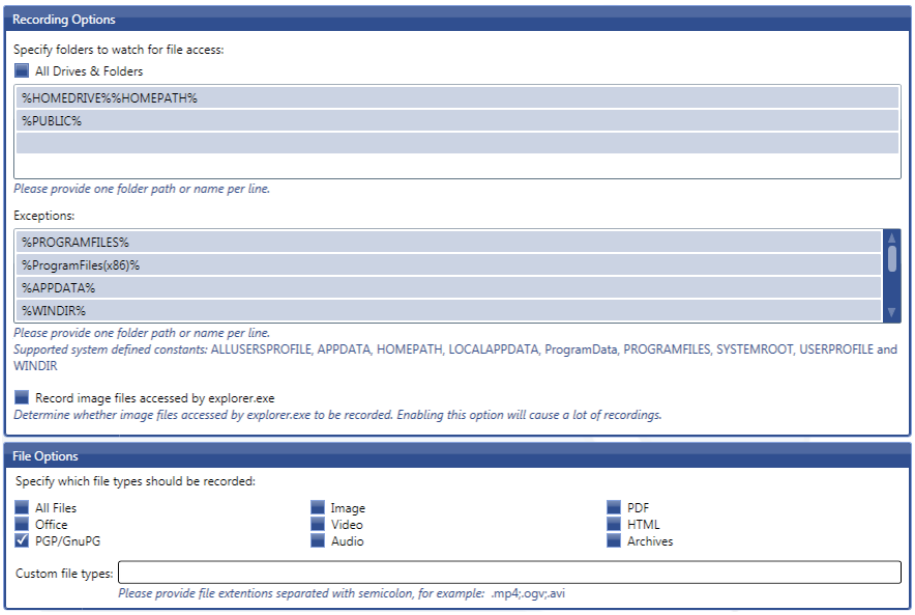
Within this configuration ADMINISTRATOR and SYSTEM ADMINISTRATOR can define rules to allow certain users to fulfil certain actions on the FinSpy Target.

The user management within a target looks like the following:



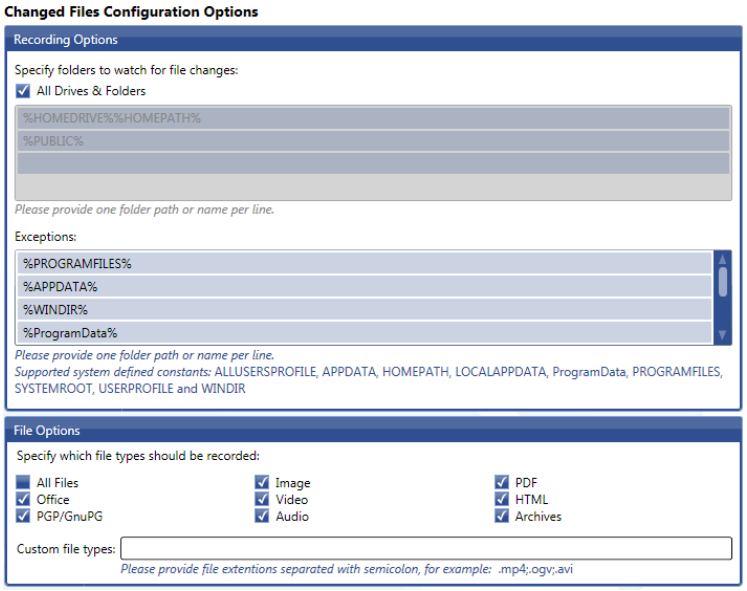
2.2.5.5 Configuration – Accessed Files

The Accessed Files Module records opened files from an infected FinSpy Target. Due to the nature of Operating Systems, a lot of files are opened all the time. Therefore enabling and configuration of this module is important and shall be handled with care. This module might trigger and copy a lot of files to the FinSpy Master.



2.2.5.6 Configuration – Changed Files

The Changed Files Module is in charge of recording the files which were modified while the module is enabled. The FinSpy Agent will provide a configuration for the Changed Files Module where the user can filter the location and file types which have to be monitored by the FinSpy Target module. Additional information such as the event (accessed, newly created, changed) and the time when the event occurred will be provided together with the recorded file.

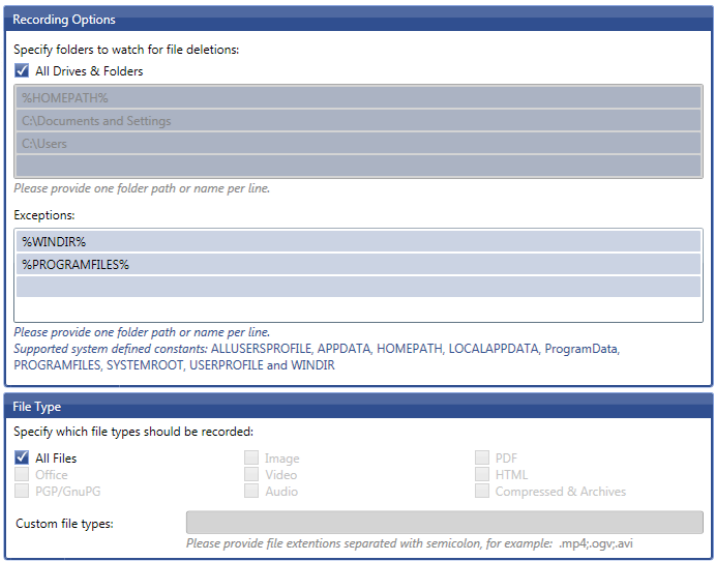


2.2.5.7 Configuration – Command Shell

This module is not configurable but enables the functionality of interacting with the FinSpy Target via a Command Shell.

2.2.5.8 Configuration – Deleted Files

The Deleted Files module enables the FinSpy Target to collect deleted files from the infected system. The Deleted Files module is able to collect all the deleted files, namely: the files which are deleted (moved) to Recycle Bin as well as the files removed using Shift+Delete. The configuration provides the module with filtering capabilities based on location and file type. Additional information such as the time of deletion will be provided together with the recorded data.



2.2.5.9 Configuration – File Access

This module is not configurable but enables the functionality of interacting with the file system of the FinSpy Target.

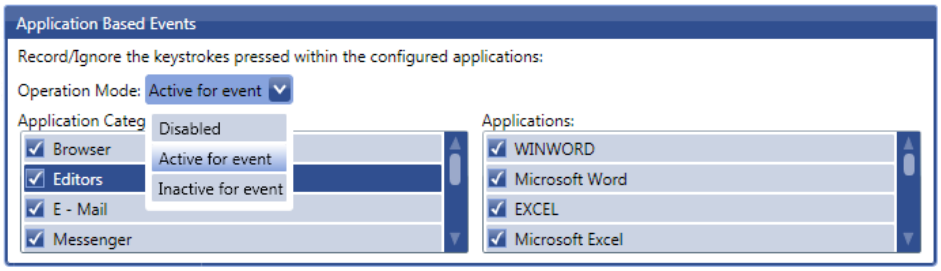
2.2.5.10 Configuration – Forensics Tools

This module is not configurable but enables the functionality of interacting with the file system of the FinSpy Target.

2.2.5.11 Configuration – Keylogger

Application based events can be used to tune the keylogging process. The mechanism used for FinSpy Target communication is adapted for the Keylogger Module to allow/suppress the keylogging for certain applications.

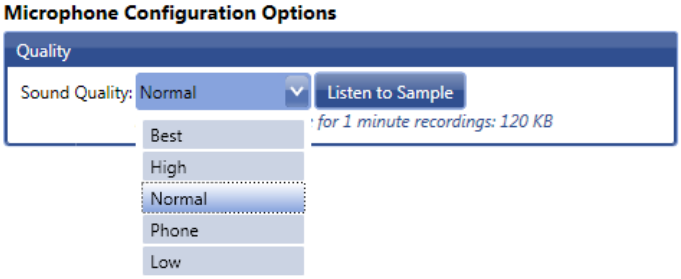
If Operation Mode is set to “Disabled”, the keylogging will not be affected by any running application in the system. When Operation Mode is set to “Active for Event”, the keylogging is only active if the applications listed in the boxes are currently running. Operation Mode set to “Inactive for Event” suppresses the keylogging if one of the applications listed in the boxes is currently running.



2.2.5.12 Configuration – Microphone

In order to define the size of a microphone recording, the quality can be defined. Depending on increasing or decreasing the quality, the amount of data for a recording will change.

Decreasing the quality of recordings can save 80 percent of memory used. The selected sound quality can be tested under “Listen to Sample” as a sample of the selected sound quality is played.

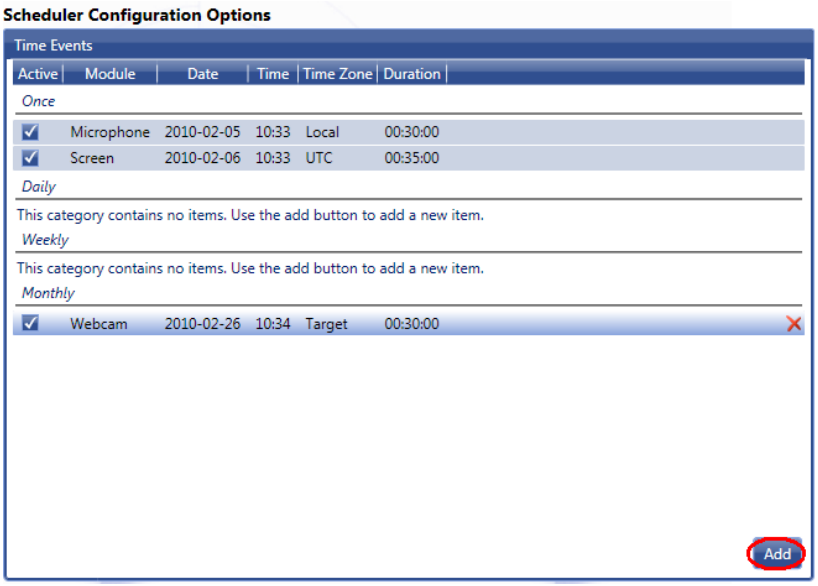


2.2.5.13 Configuration – Printer

This module is not configurable but enables the functionality of capturing all printed on the FinSpy Target system and places a copy as a PDF on the FinSpy Master.

2.2.5.14 Configuration – Scheduler

The Scheduler Module is responsible for time based data recording on the FinSpy Target. Recording can be scheduled at a specific date and time and for a given duration.



To create a new scheduler the “Add“ button is used. This will start up the scheduled event generation wizard.

There are three types of events which can be scheduled:

- Microphone recordings – records the primary installed microphone
- Screen recordings – records screenshots at the configured frequency.
- Webcam recordings – records webcam frames at the configured frequency.

After selecting the desired event type, a new section will appear where the configuration of the selected Event can be defined.

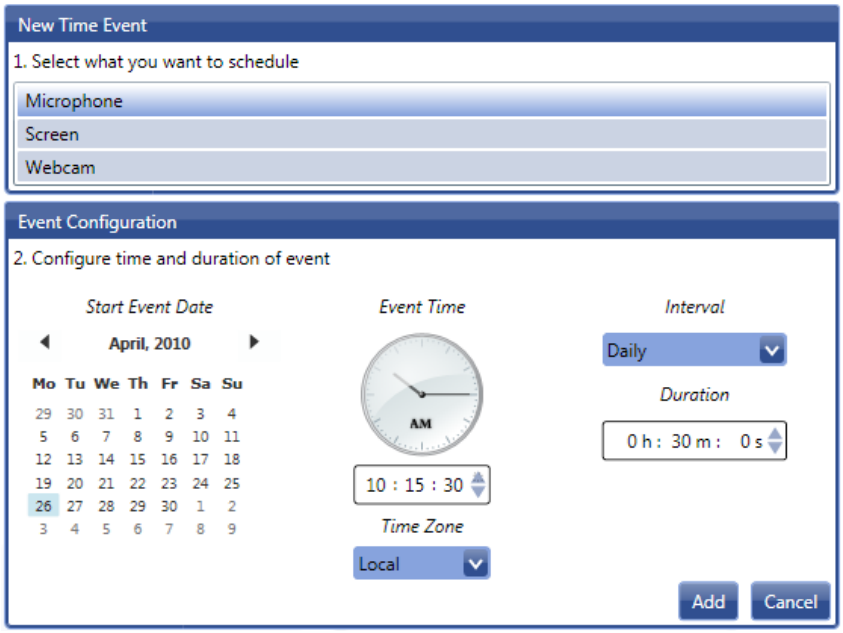
Following Events are available:

- Start Event Date: The day on which the recording should start
- Event Time: The time of the already configured day when the recording should start
- Time Zone: The time zone reference. Available options are:
  - Local: The time refers to the time zone of the FinSpy Master
  - UTC: The time is expressed in Coordinated Universal Time
  - Target: The time refers to the time zone of the target machine
- Interval: Defines the interval of the recording. The available options are:

- Once: The recording is executed only once at the configured date and time
- Daily: The recording is executed every day at the configured time starting with the configured date. There is no end date.
- Weekly: The recording is executed every week on the same week day and time configured.
- Monthly: The recording is executed monthly at the same month day as configured at the same hour as configured. There is no end date. If the recording is scheduled for a day which exists only in certain months (e.g. February 31st) then the recording is executed only in the months which contain day 31.

- Duration: The duration of the recording.

Scheduler Configuration Options



2.2.5.15 Configuration – Skype

There are different possibilities of enabling the Skype Monitoring. The quality of recording and type of communication within Skype is configurable.

Recording Options (1):

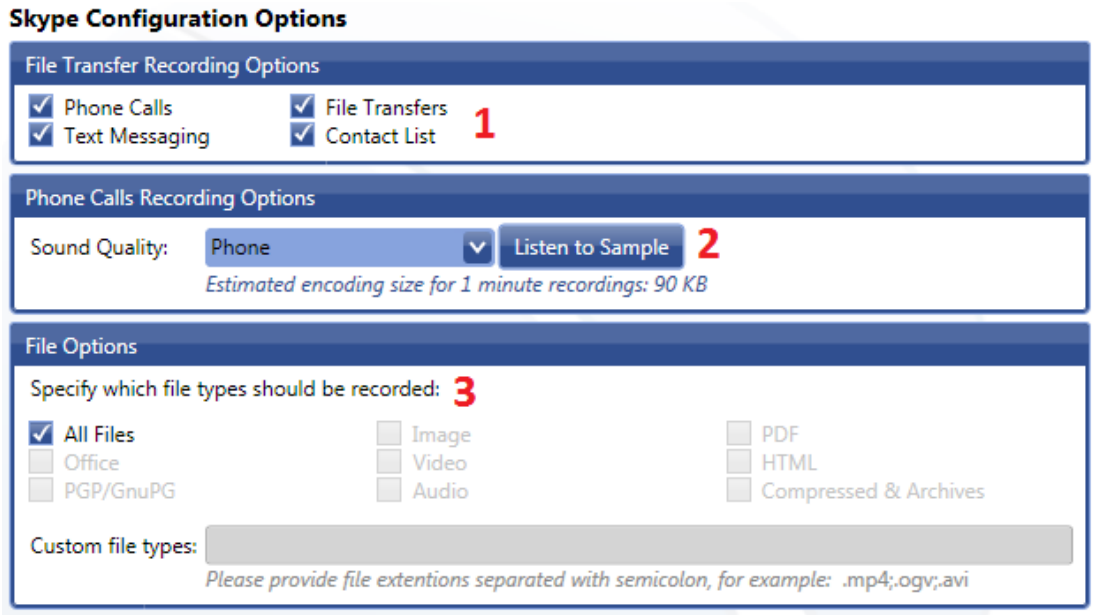
- Phone Calls: All calls between the FinSpy Target and other parties will be recorded.
- Test Messaging: All chats between the FinSpy Target and other parties will be recorded.
- File Transfers: All file transfers between the FinSpy Target and other parties will be recorded.
- Contact List: The contact list of the FinSpy Target will be recorded.

Sound Quality (2):

Decreasing the quality of voice recording may save 80 percent of space. The selected sound quality can be tested under “Listen to Sample”. A sample of the selected sound quality is played.

File Options (3):

To record file transfers via Skype, file recording can be enabled or disabled for specific or all file types. Custom file types can be entered as well.

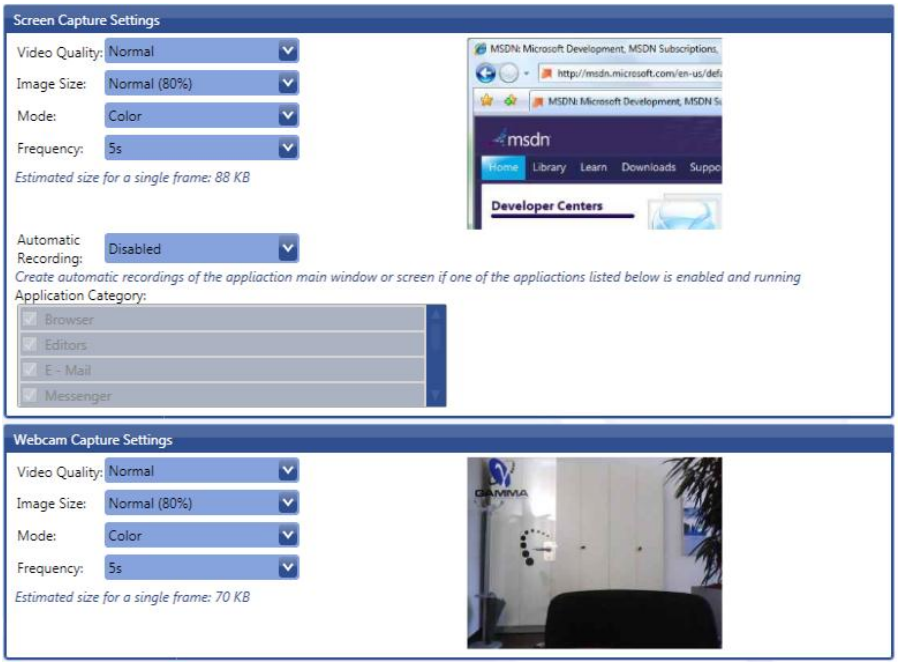


2.2.5.16 Configuration – Screen & Webcam

Recording the Screen of the FinSpy target and the Webcam (if available) is possible with this module.

Both – Screen & Webcam – have the same settings which can be applied separately.

Name	Description
Video Quality	Best, High, Normal, Low
Image Size	Original (100%), Normal (80%), Half (50%), Quarter (25%) This will result in a percentage resize of the original resolution
Mode	Color, Black & White
Frequency	Interval beginning with 2 seconds and up to 1 hour
Automatic Recording	Application based Screen Recording can additionally be performed. Either the whole screen or just the application window can be recorded if a certain application is running on the FinSpy Target.

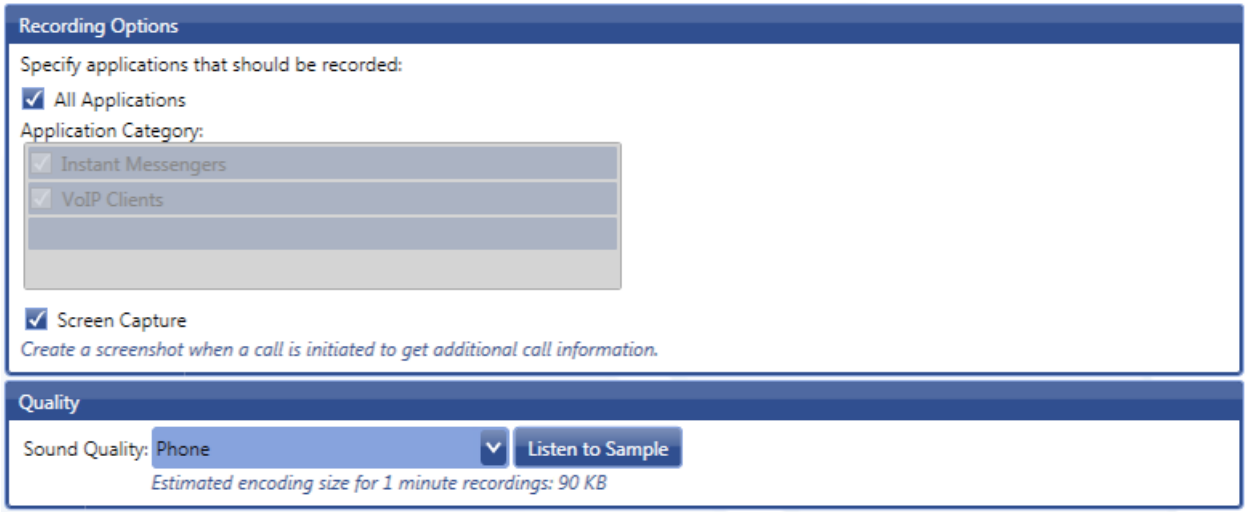


2.2.5.17 Configuration – VoIP

The VoIP module gives the possibility of recording basically all kinds of applications which are used for Voice-over-IP communication such as instant messengers or dedicated VoIP applications.

It will trigger and record the audio channel bidirectional if the Microphone and the Speakers are activated at the same time.

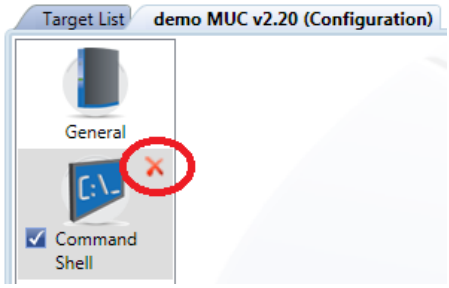
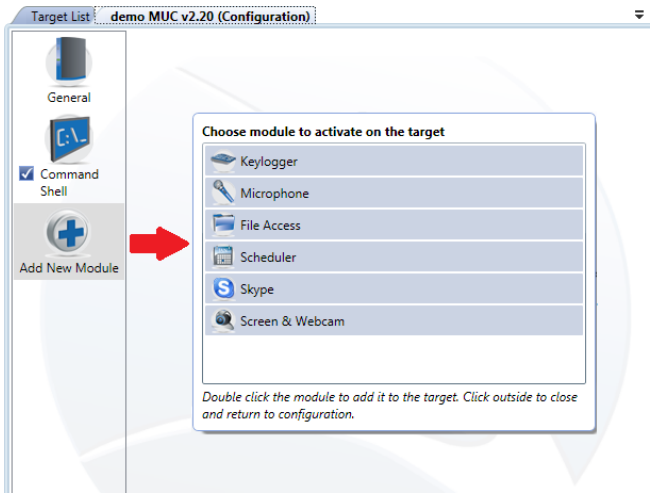
It furthermore captures a snapshot of the screen after a few seconds to see with whom the FinSpy Target is communicating.



2.2.5.18 Configuration – Add & Remove Module

To add & remove modules it is not required to create a new FinSpy Target Package. This can be done easily through the Configuration dialog.

The modules will then immediately be removed from the FinSpy Target or immediately downloaded from the FinSpy Master to the FinSpy Target if added.

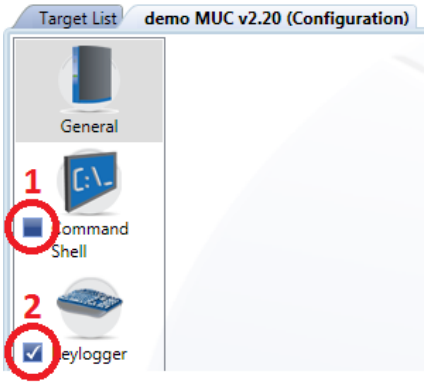
Removing a module	Adding a module
	

2.2.5.19 Configuration – Activate & Deactivate Module

Modules can also be activated and deactivated live on the FinSpy Target.

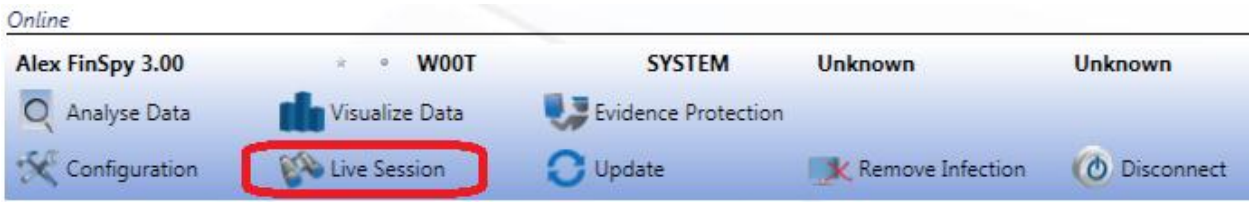
Removing the check from the checkbox (1) will deactivate the module.

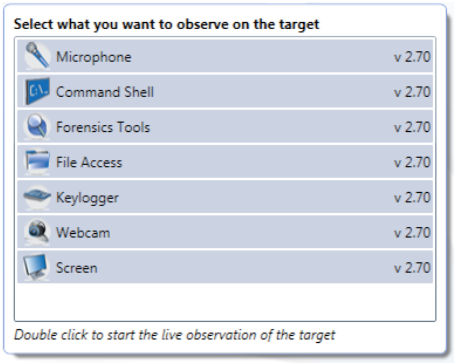
Setting the check in the checkbox (2) will activate the module.



2.2.6 Live Session

Available live access depends on the installed modules on the target. To establish a live session expand a target and select “Live Session“.





The possible modules are obtained and shown in a new dialog. More than one live session per time is possible.

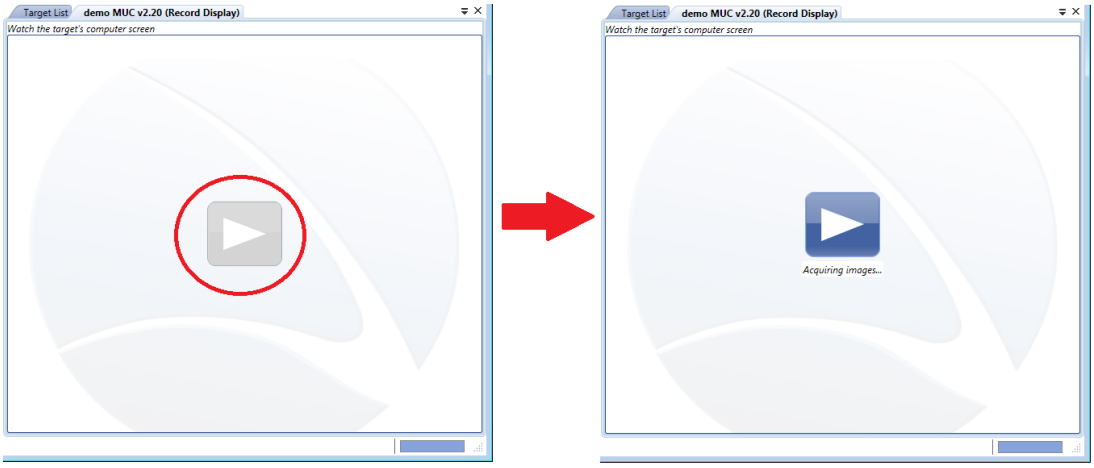
Name	Description
Microphone	Establishes a live session to the Target’s Microphone
Command Shell	Commands can be entered into the Target’s command shell
Forensics Tools	Enables uploading and execution of applications on the target machine.
File Access	Will show a live File Browser of the Target’s computer
Keylogger	Will show a live session of the Target’s keys pressed
Webcam	Establishes a live session to the Target’s Webcam
Screen	Establishes a live session to the Target’s Desktop

Each Live Session is opened in a new tab inside the FinSpy Agent. After closing the live sessions, the connection to the target computer can be ended by clicking "Disconnect" inside the expanded FinSpy Target of tab Target List.

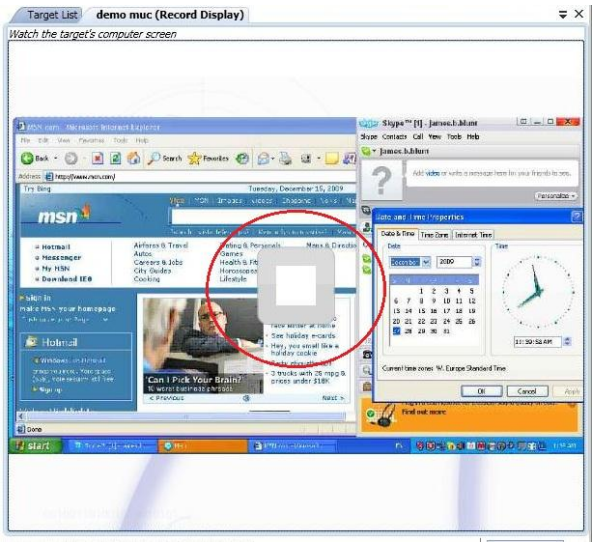
The following chapters describe live access of each module in more detail.

2.2.6.1 Live Session – Microphone / Webcam / Screen

For a live-session of the FinSpy Target's Display, Webcam or Microphone use the "Start" button inside the FinSpy Agent. The quality of the recording depends on the predefined configuration.

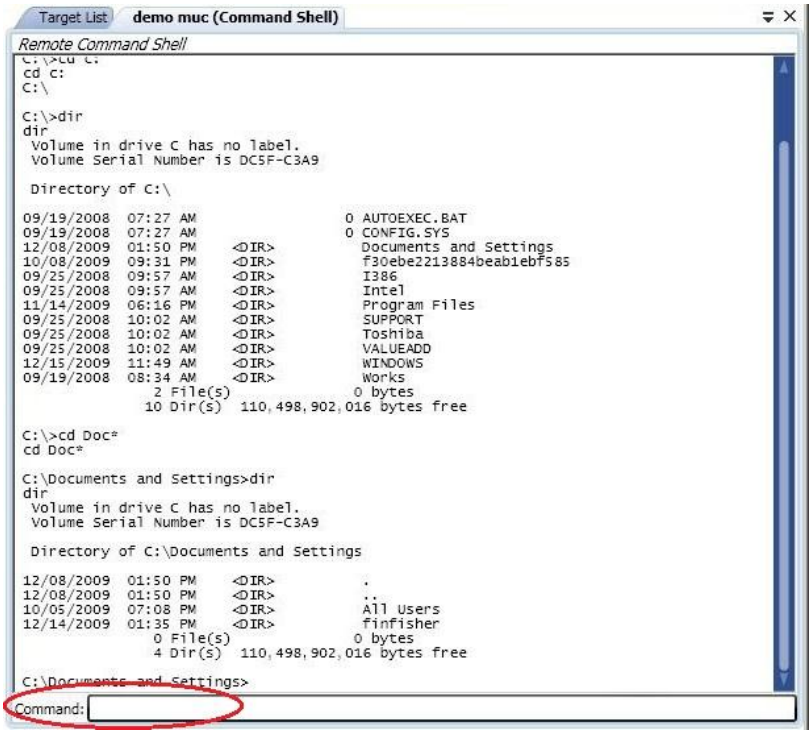


To stop recording live images or microphone, move the mouse over the image and click the "Stop" button.



2.2.6.2 Live Session – Command Shell

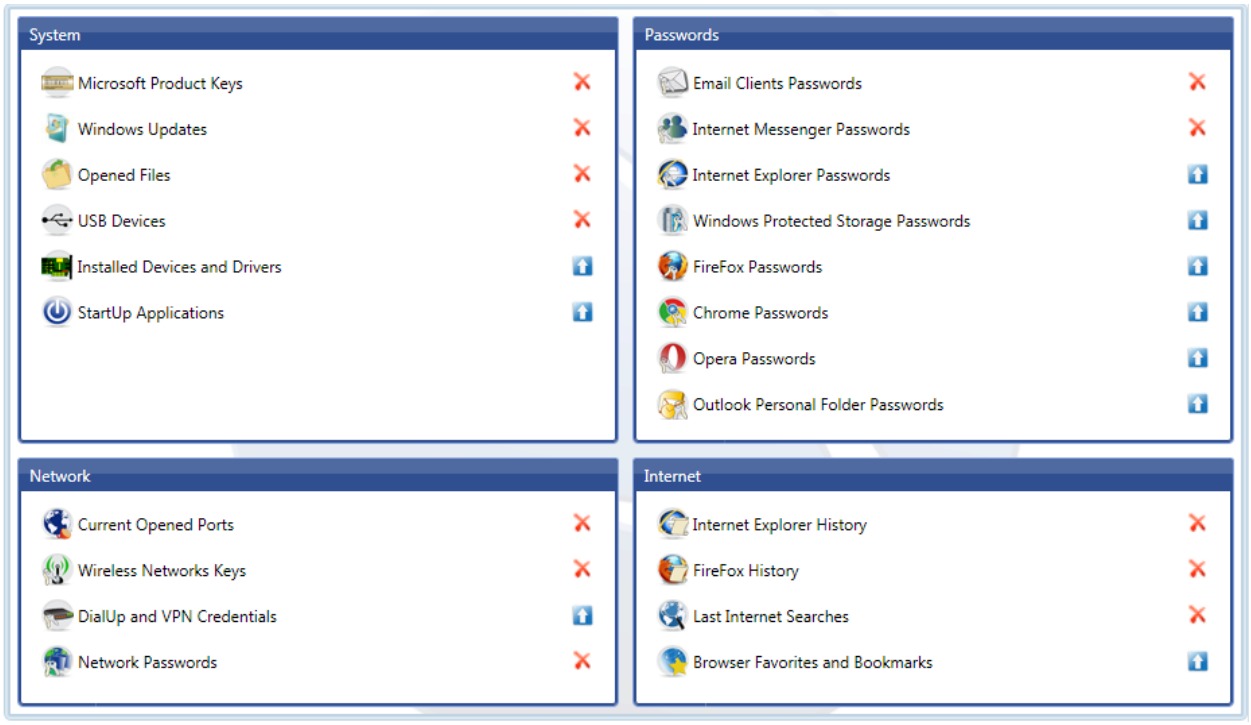
This displays a live command shell session of the Target's computer. The command shell runs with the user rights under which the FinSpy Target is running.



Commands need to be typed into the text box "Command" and executed by clicking "Enter". The command and their outputs are displayed.

2.2.6.3 Live Session – Forensics Tools

The Forensic tools module consists of predefined applications which can be uploaded to a FinSpy Target and then executed.

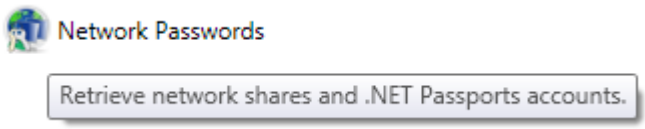


Currently, the following applications exist and are divided into different categories.

Name	Description
System	• Microsoft Product Keys • Windows Updates • Opened Files • USB devices • Installed Devices and Drivers
Network	• Current Opened Ports • Wireless Networks Keys • DialUp and VPN Credentials • Network Passwords
Passwords	• Email Clients Passwords • Internet Messenger Passwords

	• Windows Protected Storage Passwords • Internet Explorer Passwords • Firefox Passwords • Chrome Passwords • Opera Passwords • Outlook Personal Folder Passwords
Internet	• Internet Explorer History • Firefox History • Last Internet Searches • Browser Favourites and Bookmarks • Installed Devices and Drivers

Each item additionally gives a short description about its functionality as soon as the mouse is hovering the item.
For example “Network Passwords” gives the following description:



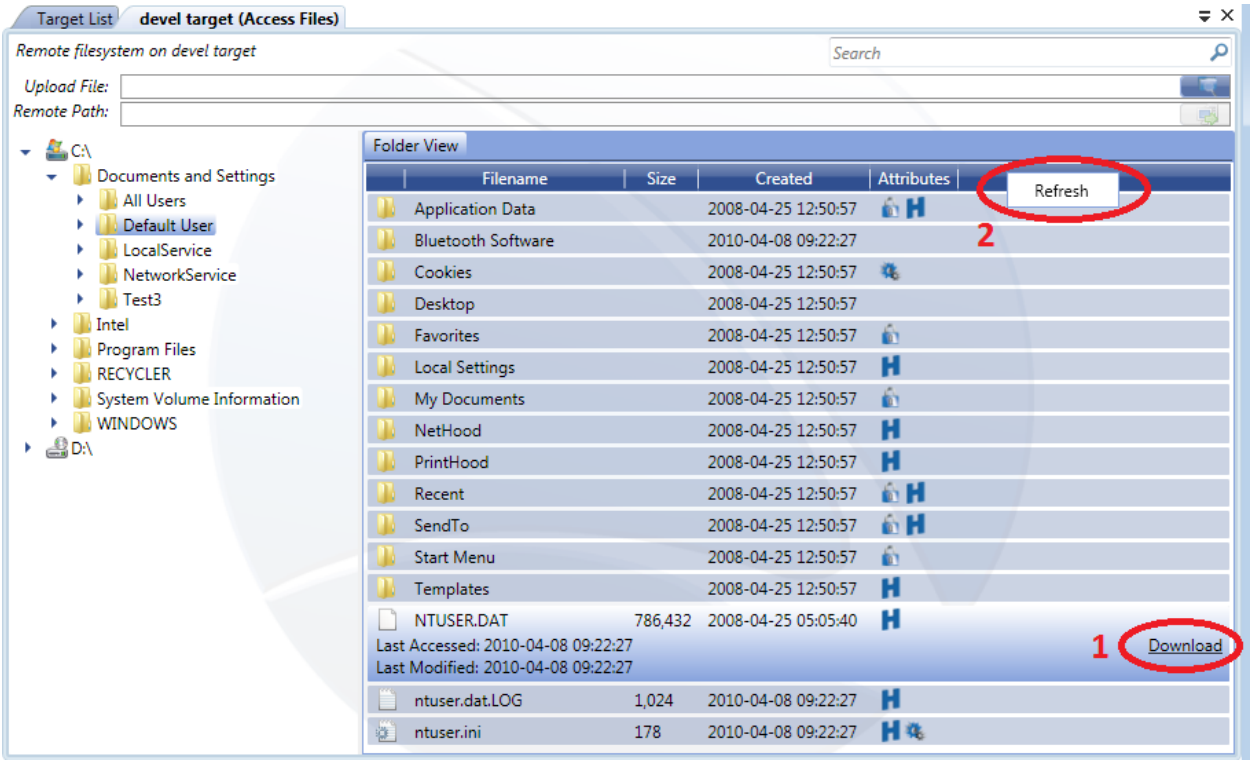
If an application is uploaded to the FinSpy Target it resides on the system until it is deleted. For further executions it will not be necessary to upload it again.
The statuses of the applications are indicated by the following icons:

Name	Description
	This icon indicates that the application is currently **not** uploaded to the FinSpy Target. For execution it needs to be uploaded first.
	The icon indicates that the application is currently uploaded to the FinSpy Target and just needs to be executed. Furthermore it can be removed from the FinSpy Target by clicking this icon.

If any application is executed on the FinSpy Target it will retrieve the results in a CSV file. This can be opened for example with Microsoft Excel.

2.2.6.4 Live Session – File Access

To establish a live session to the targets computer and browse files. Browsing is possible through double clicks on left tree or by double clicks on a folder in the right work pane.

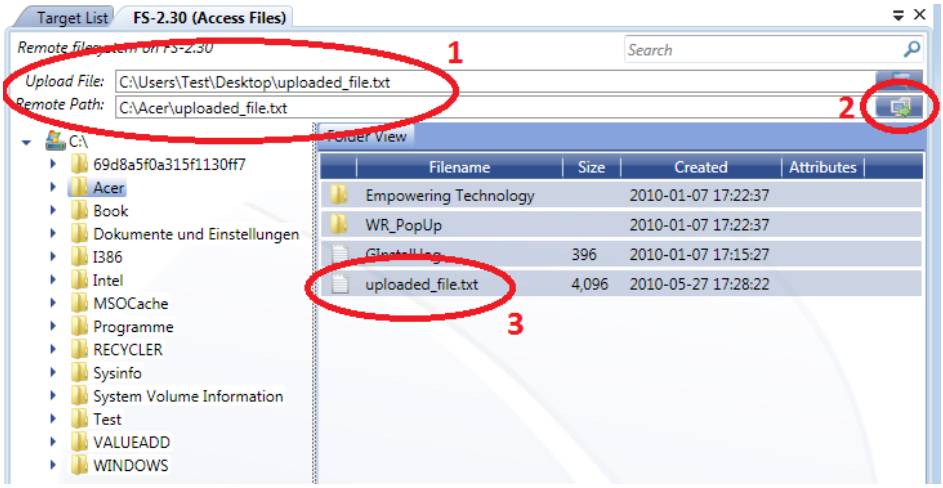


A single click on a file expands it giving more detailed information. To download the file click "Download" (1) on the right. A Progress-Bar at the bottom displays the download progress. The downloaded file can then be viewed through the Analyse data.

Furthermore a refresh of the actual directory can be performed via right-clicking anywhere and “Refresh” (2).

2.2.6.4.1 Live Session – File Access – Upload File

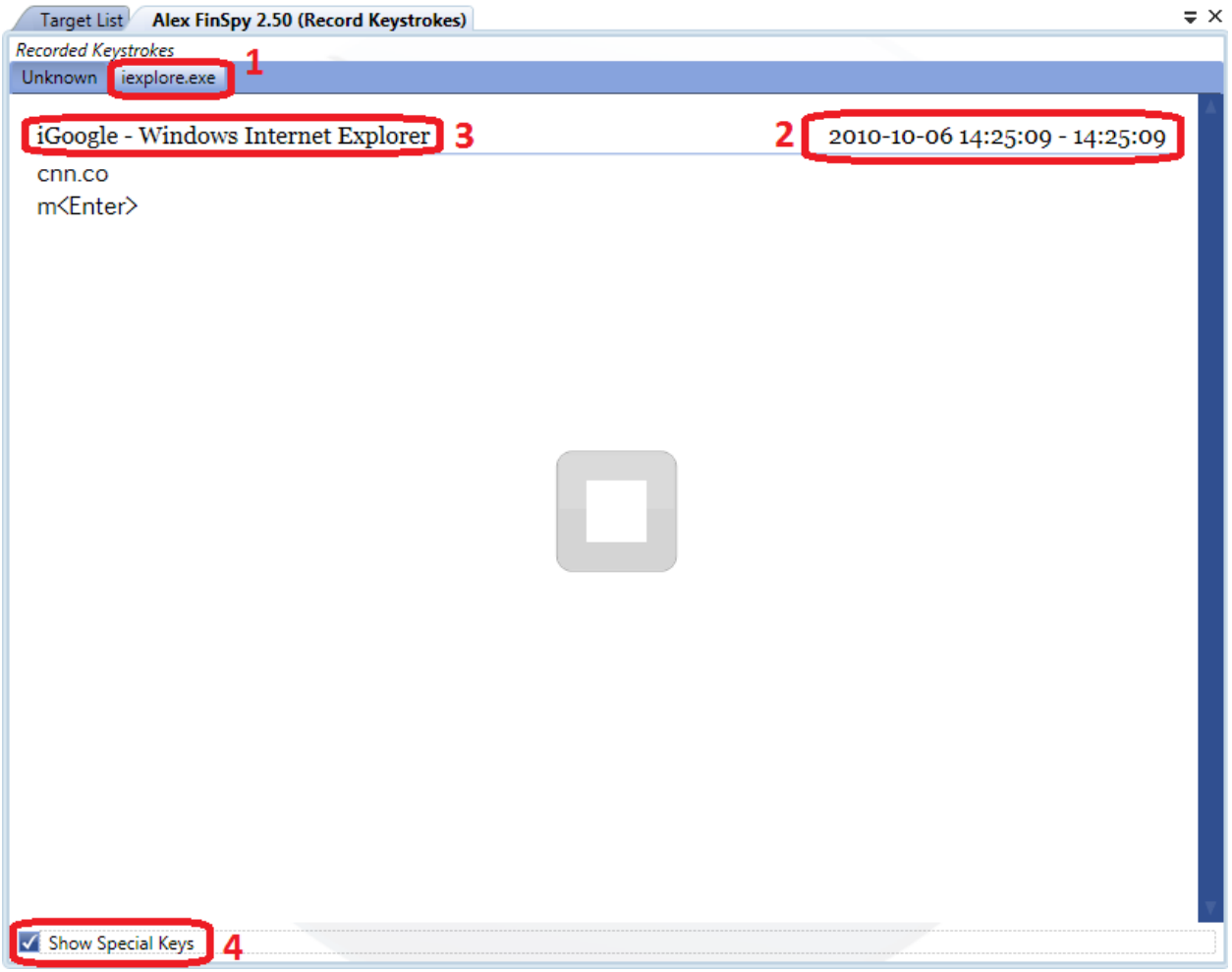
It is possible to upload files to the remote host with the Access File Function.



A file from the local file system needs to be selected and also a remote path defined. This will be by default the current working directory (1). “Click to start file upload” (2) will then put the file on the FinSpy target. This file will now be in the selected remote directory (3).

2.2.6.5 Live Session – Keylogger

To start recording keystrokes, click the “Start” button. Recorded keystrokes are displayed with the following information.



1. The Process Name where the keystrokes are entered
2. Date and time of the keystroke recording
3. The Application Name & Windows Title where the keystrokes were done (e.g. Notepad, Internet Explorer, Firefox)
4. Special chars can be enabled or disabled (e.g. Enter, Backspace, Tab, etc.)

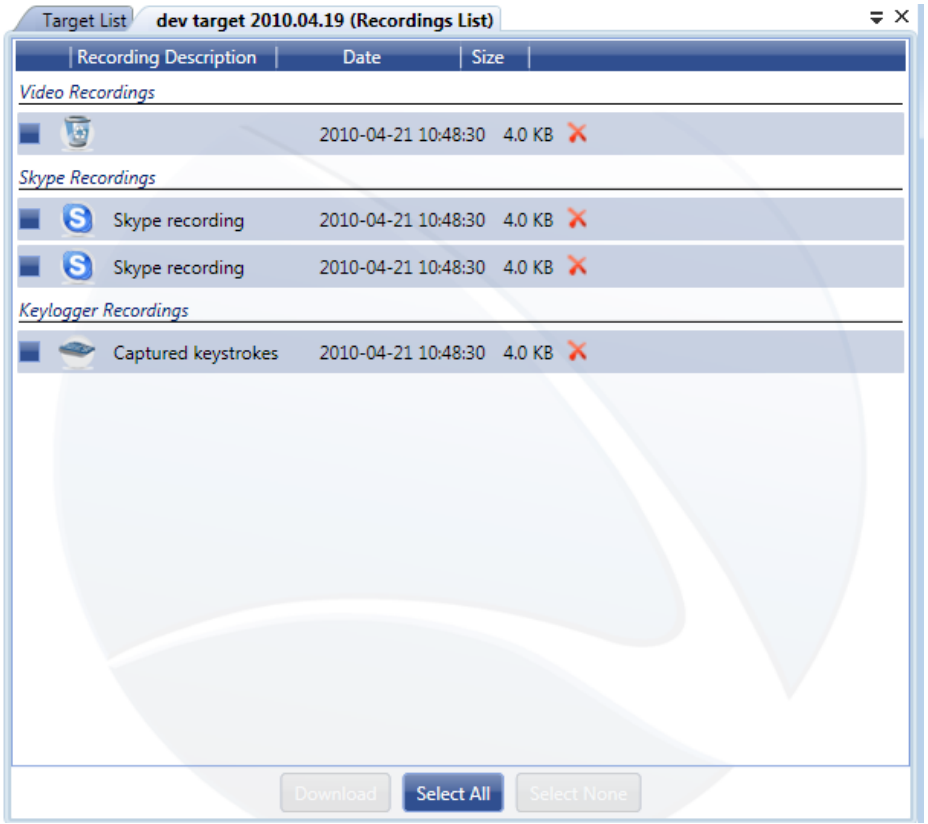
The actual keystrokes can be seen in the main window.

To stop the recording, the “Stop” button needs to be clicked.

2.2.7 Download Now

To perform a manual download of new recorded data to the FinSpy Master expand FinSpy Target in the "Target List" and click on the "Download Now" notification for new available data when the bullet appears.

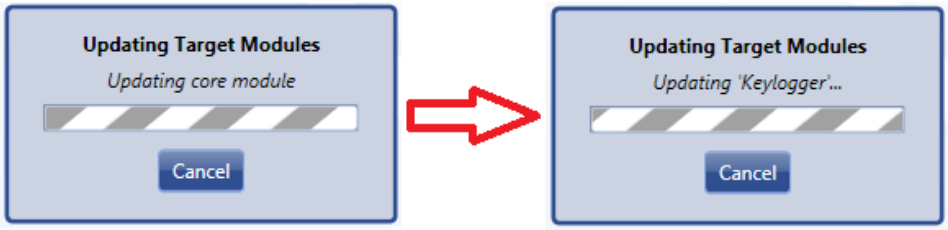
A list with all the possible recordings can be chosen. They are separated in categories to give a better overview.



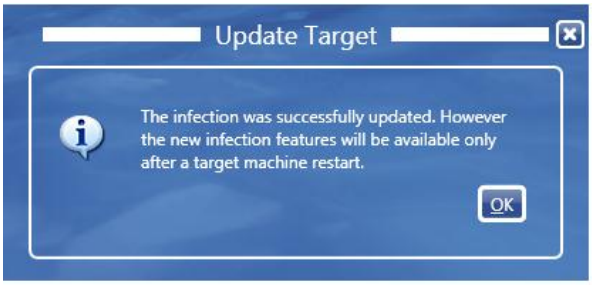
2.2.8 Update Modules

If a new version of FinSpy is released and deployed, it is possible to update a FinSpy Target from an old version to the latest one.

It will start by updating the core module of the FinSpy Target, then update all the installed Modules.



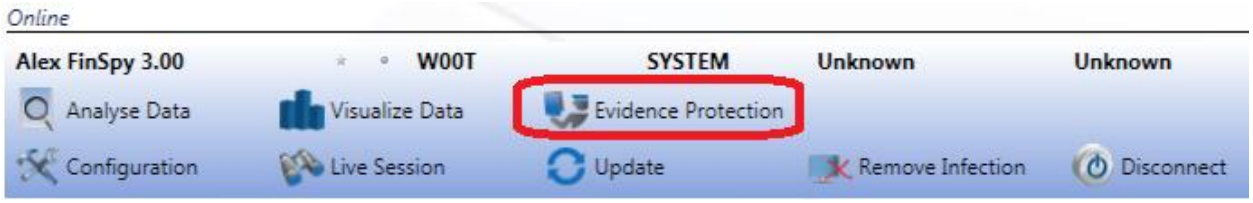
At the end it will pop up a message saying the update process was complete. To activate the new core and the new modules, the FinSpy Target needs to be restarted.



2.2.9 Evidence Protection

This feature helps protecting the collected evidence by using digital signatures and by logging the actions taken to collect the evidence from a FinSpy Target.

To use the Evidence Protection, it can be selected via “Evidence Protection” on each FinSpy Target.



The Evidence Protection Tab contains the following sections:

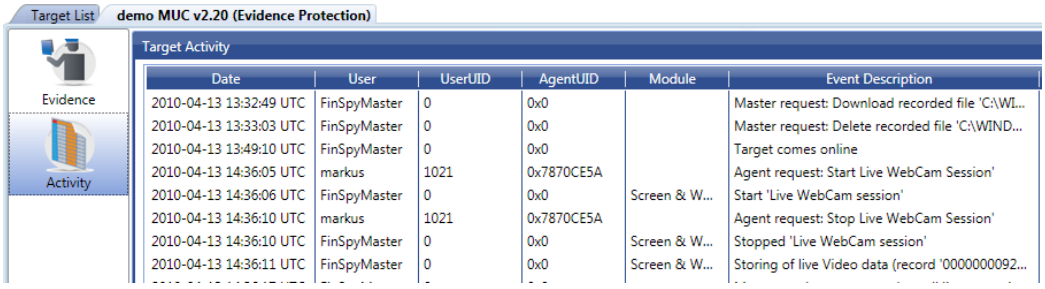
Name	Description
Activity	All the activity which concerns the FinSpy Target is presented since the recording started.
Evidence	All the collected evidence is listed and the user can check if the signature is valid.
History	A history of the FinSpy Target activity can be shown.

2.2.9.1 Evidence Protection – Activity

In the activity logging section all the interactions from FinSpy Master the FinSpy Target are presented as well as all the actions actively taken by a user through the FinSpy Agent software to access the target.

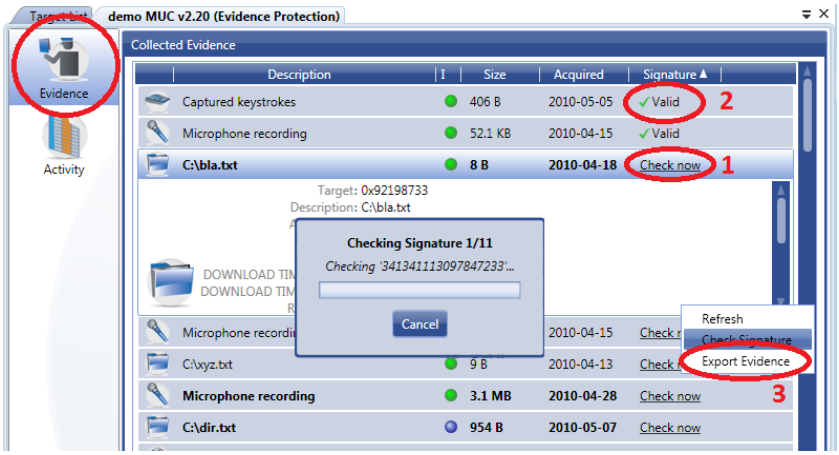
The information recorded for each action is:

Name	Description
Date	Timestamp with the FinSpy Master time represented in UTC.
User	The name of the user which participated in the activity. If the participant was the FinSpy Master, this will be registered accordingly.
UserUID	The Unique Identifier associated with the user.
AgentUID	Unique Identifier associated with the Agent. Since any user can connect from any FinSpy Agent software to the FinSpy Master, this information pinpoints the machine used for the activity.
Module	The Data Collection module the action was associated with. If the action does not concern a data collection module, this column is left blank.
Event Description	Brief description of the event.

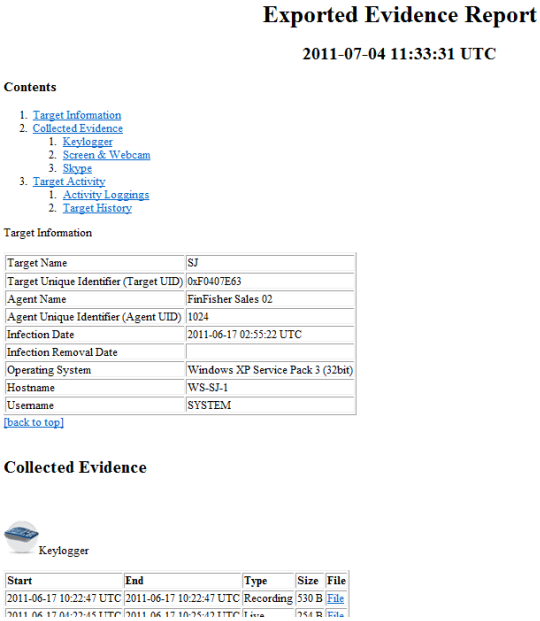


2.2.9.2 Evidence Protection – Evidence

The digital signature can be checked by clicking in the “Check now” (1) field. Upon a signature was verified successfully, the field text will change to “Valid” (2). The signature can be checked for all the collected evidence at a time or by selecting all the entries (Ctrl+A). Exporting of all or certain evidence is possible (3). The folder where the evidence is exported will be opened in a Windows Explorer once the downloaded is finished. A progress dialog will monitor the download of the evidence since this could be a lengthy operation.



The exported evidence is accompanied by a report: **Report.html** which looks similar to the pictures below:



Exported Evidence Report

2011-07-04 11:33:31 UTC

Contents

1. Target Information
2. Collected Evidence
   1. Keylogger
   2. Screen & Webcam
   3. Skype
3. Target Activity
   1. Activity Loggings
   2. Target History

Target Information

Target Name	SJ
Target Unique Identifier (Target UID)	0xF0407E63
Agent Name	FinFisher Sales 02
Agent Unique Identifier (Agent UID)	1024
Infection Date	2011-06-17 02:55:22 UTC
Infection Removal Date	
Operating System	Windows XP Service Pack 3 (32bit)
Hostname	WS-SJ-1
Username	SYSTEM

[back to top]

Collected Evidence

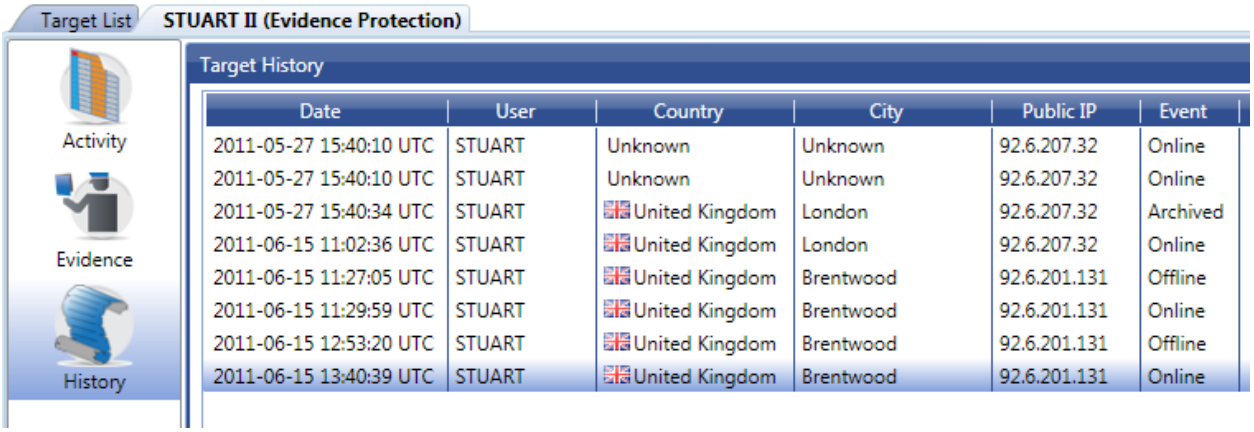
Keylogger

Start	End	Type	Size	File
2011-06-17 10:22:47 UTC	2011-06-17 10:22:47 UTC	Recording	530 B	File

2.2.9.3 Evidence Protection – History

This gives an overview about historical information of a FinSpy Target such as:

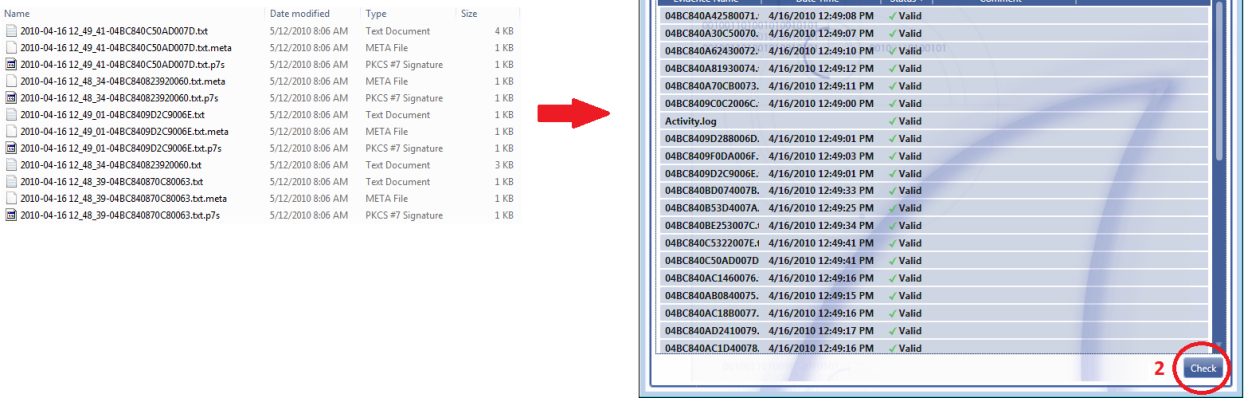
Name	Description
Date	Timestamp with the FinSpy Master time represented in UTC.
User	The Username of the logged in user.
Country	In which country was the Target
City	In which city was the Target
Public IP	Which Public IP the Target connected from.
Event	Brief description of the event.



2.2.9.4 Evidence Signature Verification Tool

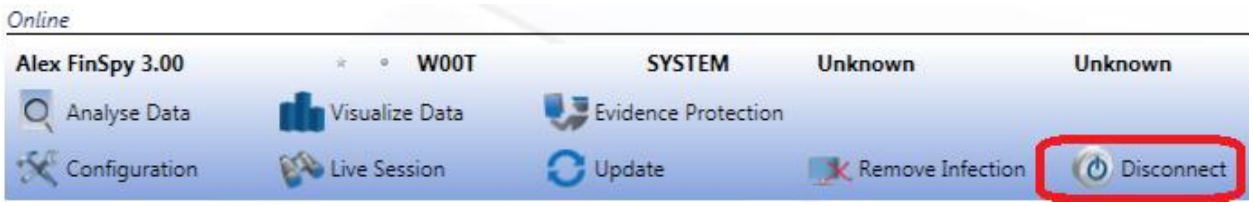
An external tool is also provided to check the digital signature and analyze the exported evidence without the need of a FinSpy Master connection. The Evidence Signature Verification Tool can be run from a standalone PC. It is not necessary to have either the Evidence Data or the Evidence Signature Verification tool running on any FinSpy related computer.

The folder of the exported evidence needs to be selected (1) and afterwards simply checked (2). This will lead to a valid or invalid status.



2.2.10 Disconnect

If a session is established and active to a FinSpy Target, the session can be stopped gracefully through "Disconnect".

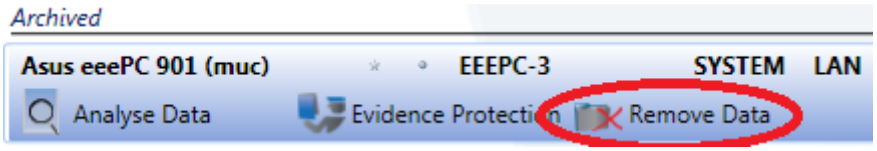


Only one FinSpy Agent can connect to a FinSpy Target at a time. Therefore the "Disconnect" allows another FinSpy Agent to connect to the FinSpy Target.

2.2.11 Remove Data

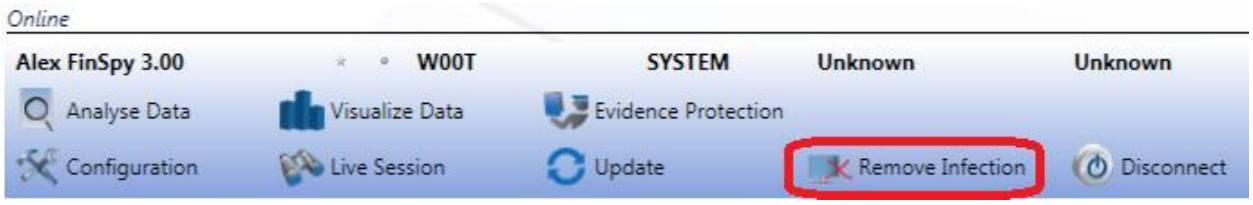
Purging of data removes all data for the selected FinSpy Target from the FinSpy Master database.

To initiate purging of recorded data, expand the respective FinSpy Target in the tab "Target List" and click on "Remove Data".



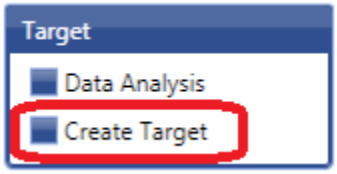
2.2.12 Remove Infection

"Remove Infection" will irrepealably delete the Infection on the FinSpy Target and a further infection is not possible without a restart of the FinSpy Target computer.



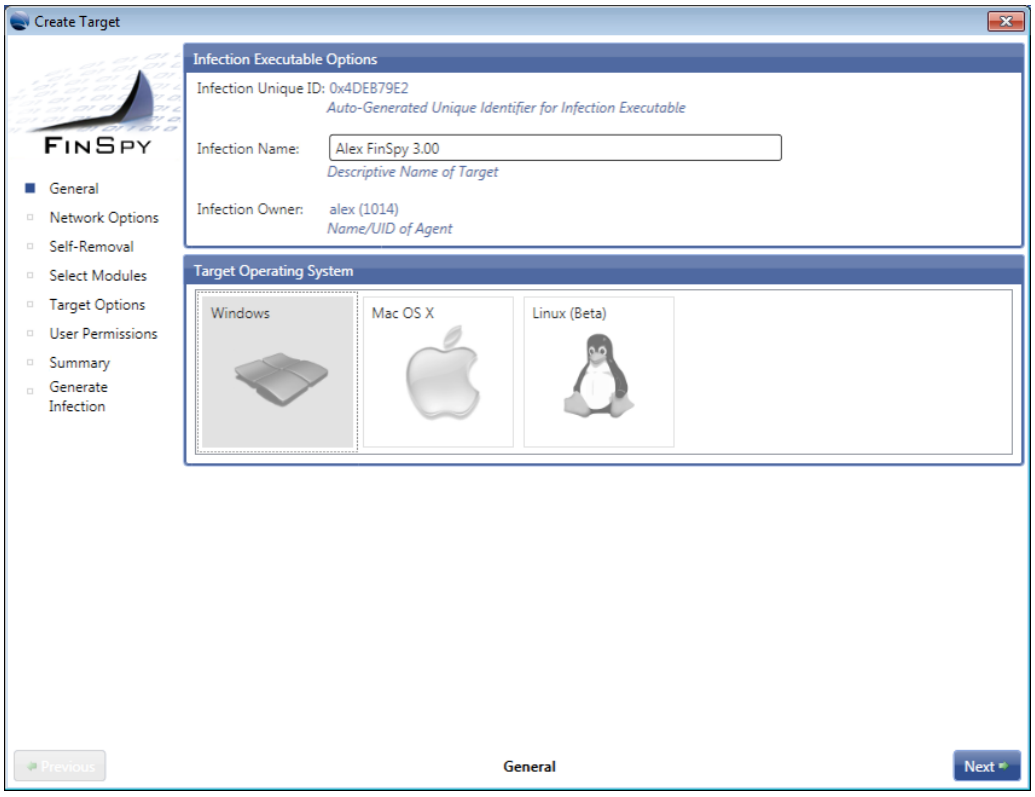
2.2.13 Create Target

A Target is an executable file or Office Document which includes all modules with which a FinSpy Target can be monitored.



Click “Create Target” on the left navigation pane of the FinSpy Agent. This will open the Target Creation Wizard.

Within the wizard, to navigate between the dialogs for configuration, “Next” or “Previous” buttons can be used or clicking on the items on the left navigation pane is possible.

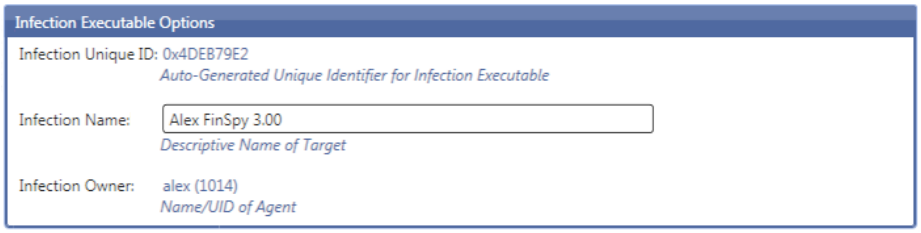


The following dialogs consist of:

Name	Description
General	Name and heartbeat of FinSpy Installer Package.
Network Options	Settings retrieved by the FinSpy Master.
Self-Removal	Criteria when the infection removes itself from the FinSpy Target.
Select Modules	Defining which modules should be integrated with their settings.
Target Options	Advanced configuration of the behaviour of the FinSpy Trojan on the FinSpy Target
User Permissions	Assigning users to the FinSpy Trojan
Summary	Infection Summary
Generate Infection	Media or executable with which a FinSpy Target will be infected.

2.2.13.1 General

General settings configure the behaviour and identification of a FinSpy Installer Package. Some parameters are changeable after infection of a FinSpy Target.



The Operating System of the Target has to be chosen. This will result in a different FinSpy Trojan with different modules.

Currently supported are the following Operating Systems:

Microsoft Windows:

- Microsoft Windows 2000 Clean / SP1 / SP2 / SP3 / SP4
- Microsoft Windows XP Clean / SP1 / SP2 / SP3
- Microsoft Windows Vista Clean / SP1 / SP2 / SP3 (32 Bit & 64 Bit)
- Microsoft Windows 7 Clean / SP1 (32 Bit & 64 Bit)

Apple MacOS:

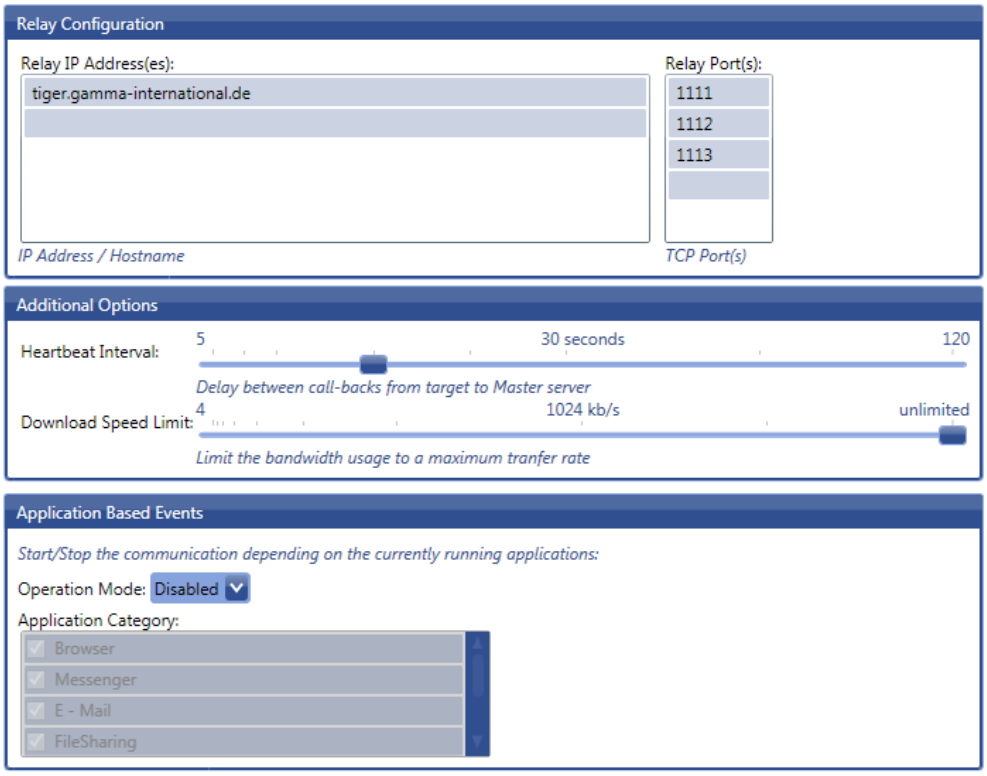
- Mac OS X 10.6.0 – 10.6.8 (Intel)

Linux:

- Ubuntu / Debian
- Fedora / RedHat
- BackTrack
- SuSE

2.2.13.2 Network Configuration

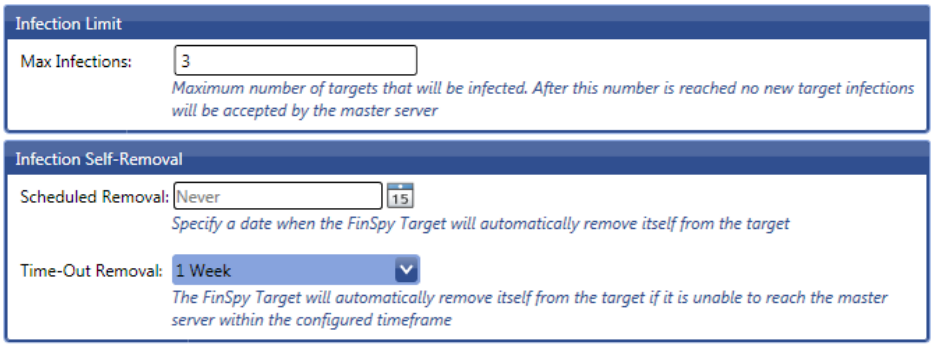
These settings are explained in chapter: Proxy Settings & Application Based Events.



2.2.13.3 Self-Removal

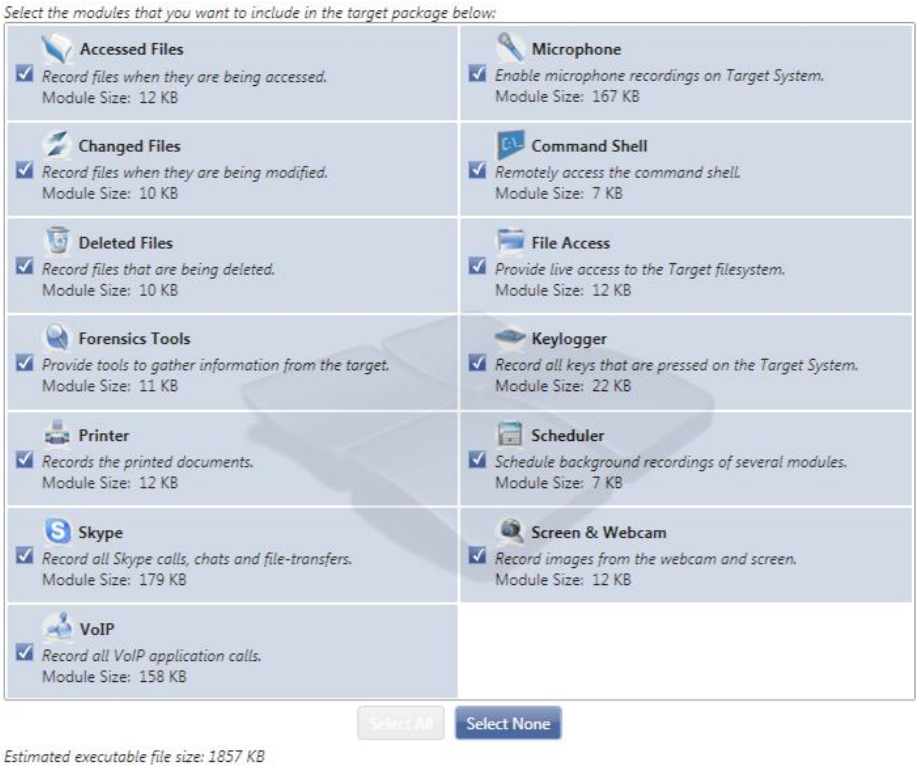
"Infection Limit" specifies the number of FinSpy Targets which can be infected.

"Infection Self-Removal" is explained in chapter: Infection Self-removal.



2.2.13.4 Select Modules

Check the boxes of respective necessary modules.



For detailed description how to configure each Module see the following chapters:

- Configuration – Accessed Files
- Configuration – Microphone
- Configuration – Changed Files
- Configuration – Deleted Files
- Configuration – Keylogger
- Configuration – Scheduler
- Configuration – Skype
- Configuration – Screen & Webcam
- Configuration – VoIP

2.2.13.5 Target Options

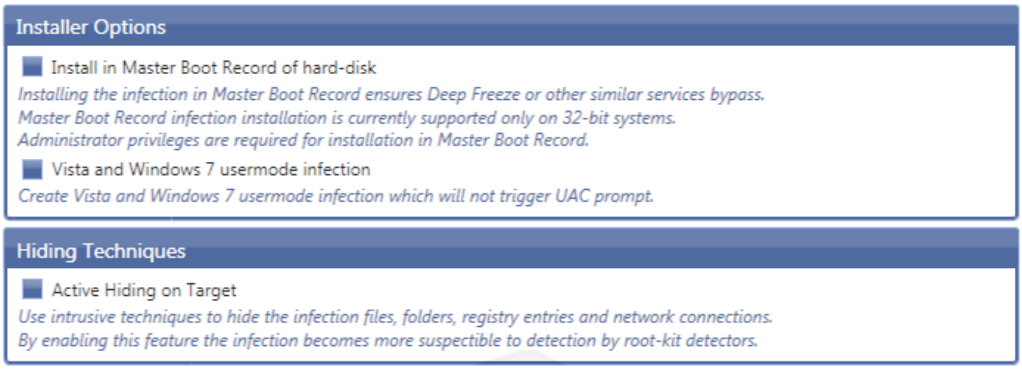
Different Installer options can be defined.

- Install in Master Boot Record of hard-disk

  With this infection, the FinSpy Trojan writes itself to the Master Boot Record of the Target system. This requires Administrative privileges on the Target system. But once installed, this infection makes the Trojan resistant against Software like e.g. Deepfreeze & Norton Ghost.

- Vista and Windows 7 usermode infection

  Using the usermode infection will not result to a so called UAC popup within Windows asking for administrative privileges. A covert method for the installation but also not as powerful as the Trojan will be restricted to the infected user account on the Windows Target.

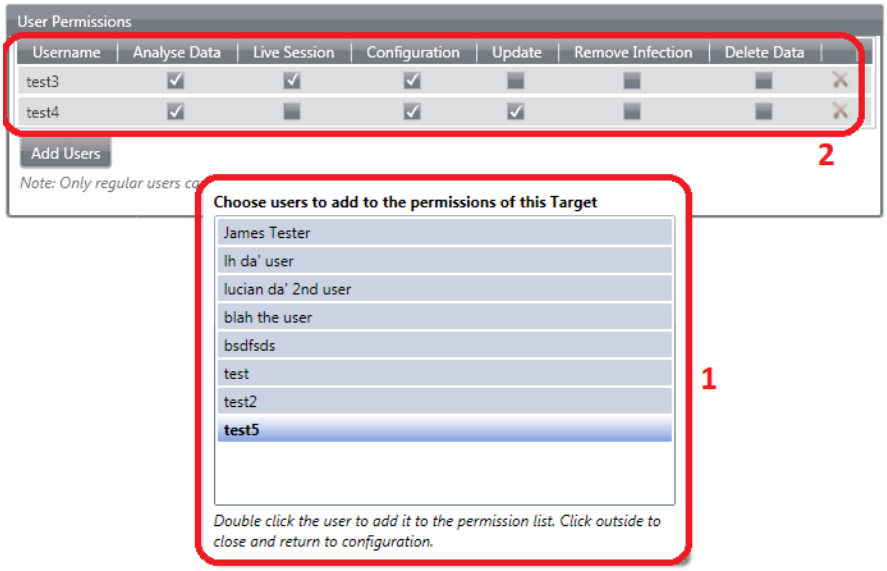


A detailed explanation of Hiding Techniques:

- Hiding Techniques

2.2.13.6 User Permissions

Each creation of a FinSpy Trojan allows assigning users to work with it. Multiple users can be chosen (1). Furthermore it is possible to give special rights to each user like establishing a Live Session or configuring the FinSpy Target (2).

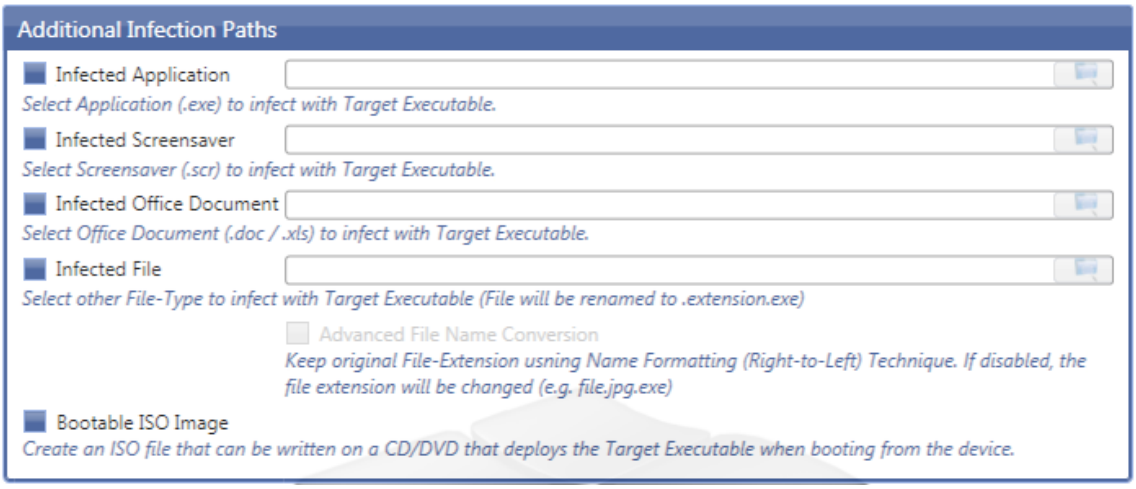


2.2.13.7 Summary

A Summary of the generated infection can be reviewed. Listed is the name of the infection, some configuration settings and also all chosen modules.

2.2.13.8 Generate Infection

On this final dialogue the infection paths can be selected.

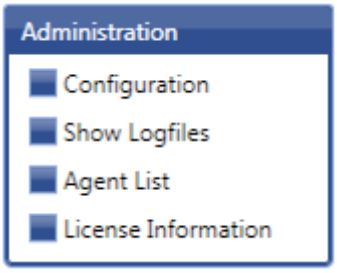


Name	Description
Infected Application	Any executable (*.exe) can be used to merge with the FinSpy Target Executable.
Infected Screensaver	Any screensaver (*.scr) can be used to merge with the FinSpy Target Executable.
Infected Office Document	Any Microsoft Word or Microsoft Excel document can be used to merge with the FinSpy Target Executable. The format must be .doc or .xls and **NOT** .docx or .xlsx!
Infected File	Any file (e.g. .jpg, .avi, .ppt) can be used to merge with the FinSpy Target. The file extension will change to: *filename.extension.exe*
Advanced File Name Conversion	In case “Infected File” was chosen, another technique can be used to be even more covert. The filename makes use of an RTL (right-to-left) technique. The filename will now be: *exe.filename.jpg*
Bootable ISO Image	With this infection technique a bootable CD or DVD will be created with which the Target system will be infected on boot.

Name	Description
Bootable Infection Dongle	Creates an USB Infection which allows infecting the Target System during boot.
Runtime Infection Dongle	Creates an USB Infection Dongle with automatic execution.

2.3 FinSpy Agent – Administration

The Administration on the left pane of the FinSpy Agent gives the possibility to make changes to the FinSpy Master, viewing Log files or displaying who is currently using the system. To view and change these settings, an “Administrator” user must be logged in.



2.3.1 Configuration

Within the “Configuration” settings can all important changes made to the FinSpy Master remotely. If the Master is not reachable for any reason, the changes need to be done manually. See FinSpy Master – Configuration.

Name	Description
User Management 	Users can be added, edited and deleted through the User Management.
Agent Configuration 	Specify where all exported Data will be saved.
Network 	Configuration of the Internal and External Network Interfaces.
Relay Network Configuration 	Configuration of connection details for the FinSpy Targets.

Email Notification 	Configuration of the Email server, user and password for Email notification.
Updates 	Configuration of the FinSpy Master and FinSpy Target Updates.
Evidence Protection 	Configuration of the Evidence Protection certificates, logging activity and functionality.
LEMF Interface 	LEMF database configuration.

2.3.1.1 Configuration – User Management

Inside the User Management, System Administrators and Administrators can perform very granulated User Management. There are three different types of Users:

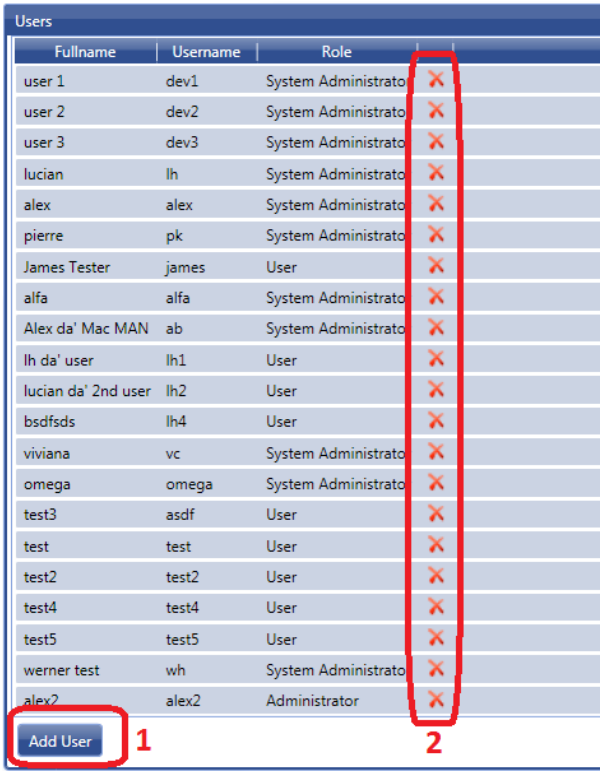
1. System Administrator
2. Administrator
3. User

The following rights are given to each user

Name	Description
System Administrator	• Create / Delete / Modify ALL Users (Including System Administrators) • Configure FinSpy Master (Network, Evidence Protection, Updates, etc) • Full functionality of FinSpy
Administrator	• Full Target Control of all Targets • Target Creation • Assign regular Users to Targets • Install FinSpy Agent updates • All Data Analysis related functionality
Users	• Functionality depends on what was assigned to the user

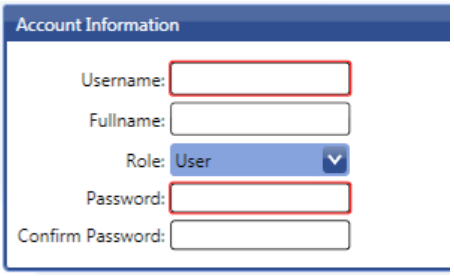
*Note: The upgrade from 2.40 to 2.50 will convert **all** users to System Administrators by default!*

By selecting “User Management” all users on the system will be listed.



It is possible from here to select, add (1) or delete (2) users.

If a user is added, another box below is displayed. A Username and a Password is required!



In the last step, one or multiple targets can be assigned for each user.

2.3.1.2 Configuration – Agent Configuration

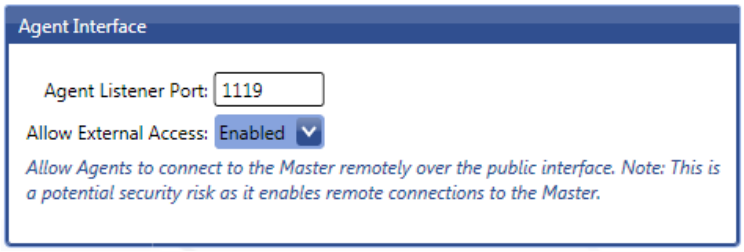
Inside the Agent Configuration the Export folder is defined.

This will include all created FinSpy Targets, exported Evidence and updated FinSpy Agent version installers.

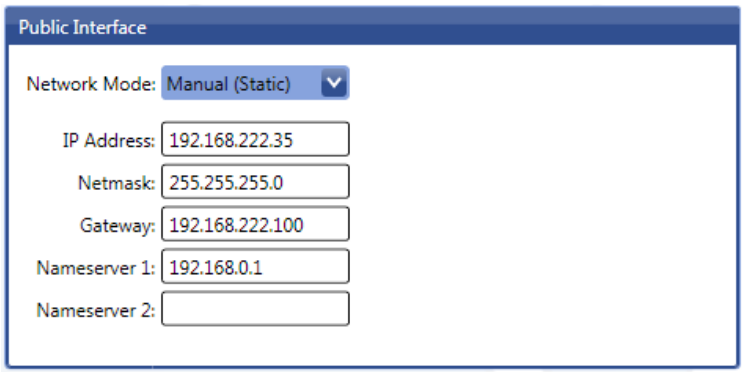
2.3.1.3 Configuration – Network

The network configuration is divided into two parts. One is for the FinSpy Agent and one for the FinSpy Target Connection.

The Agent interface can be configured to also be reachable not only from the internal LAN, but also from the Internet. These settings must be used with caution as it allows connection from outside to the FinSpy Master. If this setting is activated, the FinSpy Agent needs to have the external IP of the FinSpy Master to connect to it, even though it might be in the same LAN.

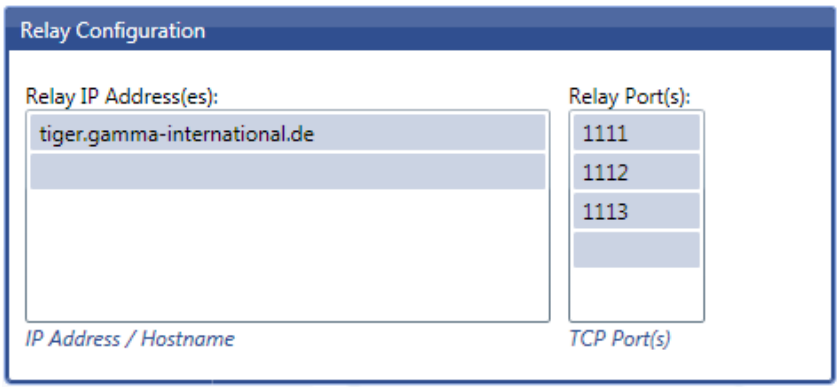


Public interface controls the network settings given by the provider to establish a connection to the internet and being reachable from the internet. This can be either set manually “Manual (Static)” or retrieved via DHCP from a Router connected to the internet.



2.3.1.4 Configuration – Relay Network Configuration

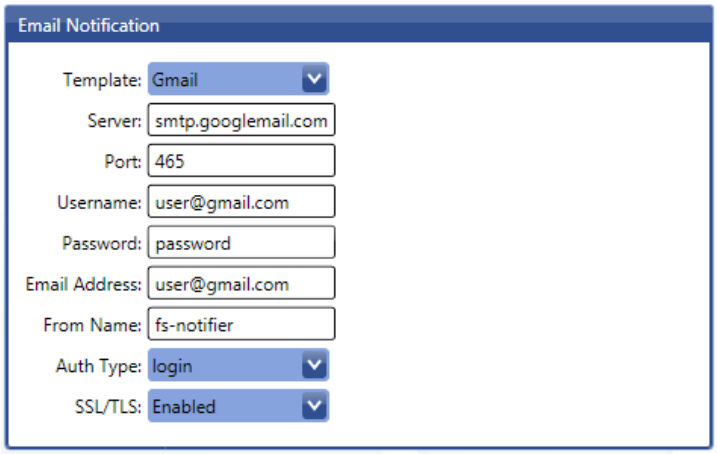
The Relay Network Configuration defines a single relay or multiple relays for the connection of the FinSpy Target to the FinSpy Master or FinSpy Relay. These settings will be retrieved by the FinSpy Agent during creation of a FinSpy Target and set automatically.



2.3.1.5 Configuration – Email Notification

Settings for the Email notification can be set here. They can be differentiated in templates:

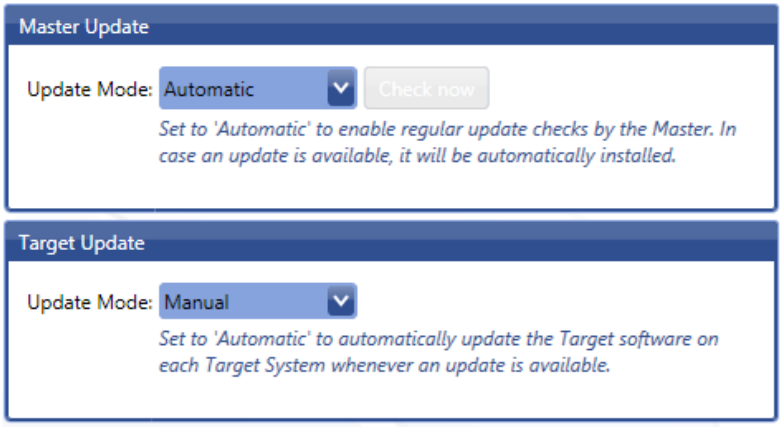
- Local MTA (the FinSpy Master Mail server)
- Predefined Free Mailer
- Custom



Every template needs some minor adjustments like sender Email address, username, password or the From Name.

2.3.1.6 Configuration – Updates

Updates of the FinSpy Master Software and the FinSpy Target Modules can be defined here. Both can be set to “Automatic” or “Manual”. Automatic Updates will be checked in a short interval, which is normally 24 hours, for a newer version on the Update Server provided by Gamma International. With “Manual” an update check will be performed only on user request.

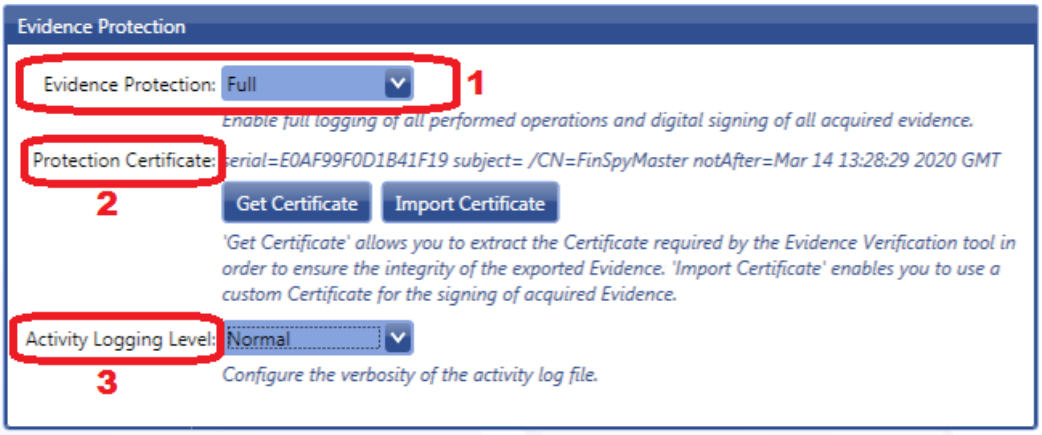


2.3.1.7 Configuration – Evidence Protection

To access this feature on the FinSpy Agent, it must be enabled on the FinSpy Master first. Therefore “Evidence Protection” has to be set to “Full” (1). In the case, that only the Activity on a Target should be logged, this option can also be set to “ActivityLog only”.

Once the feature is activated on the FinSpy Master all the new collected evidence will be digitally signed using a FinSpy Master self generated key. The capability of importing an own key into the FinSpy Master is also given (2).

Furthermore the Logging Level (3) can be defined to: Minimal, Normal, Verbose or completely disabled.

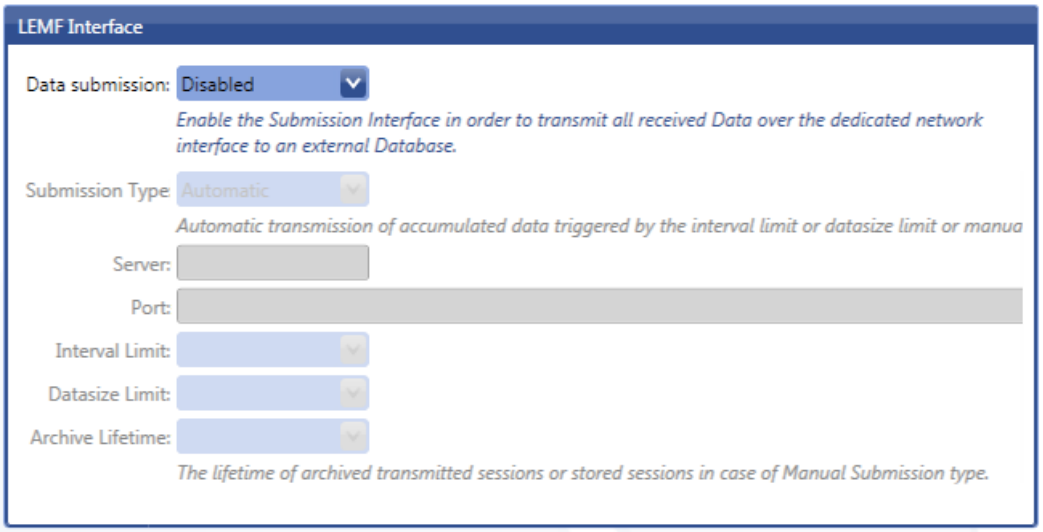


2.3.1.8 Configuration – LEMF Interface

For the integration of an external LEMF Interface this option must be enabled. The FinSpy Master server has a dedicated network interface (eth2) for those interactions.

To specify the external database the following options can be given:

- Server
- Port
- Interval Limit
- Datasize Limit
- Archive Lifetime



2.3.2 Show Logfiles

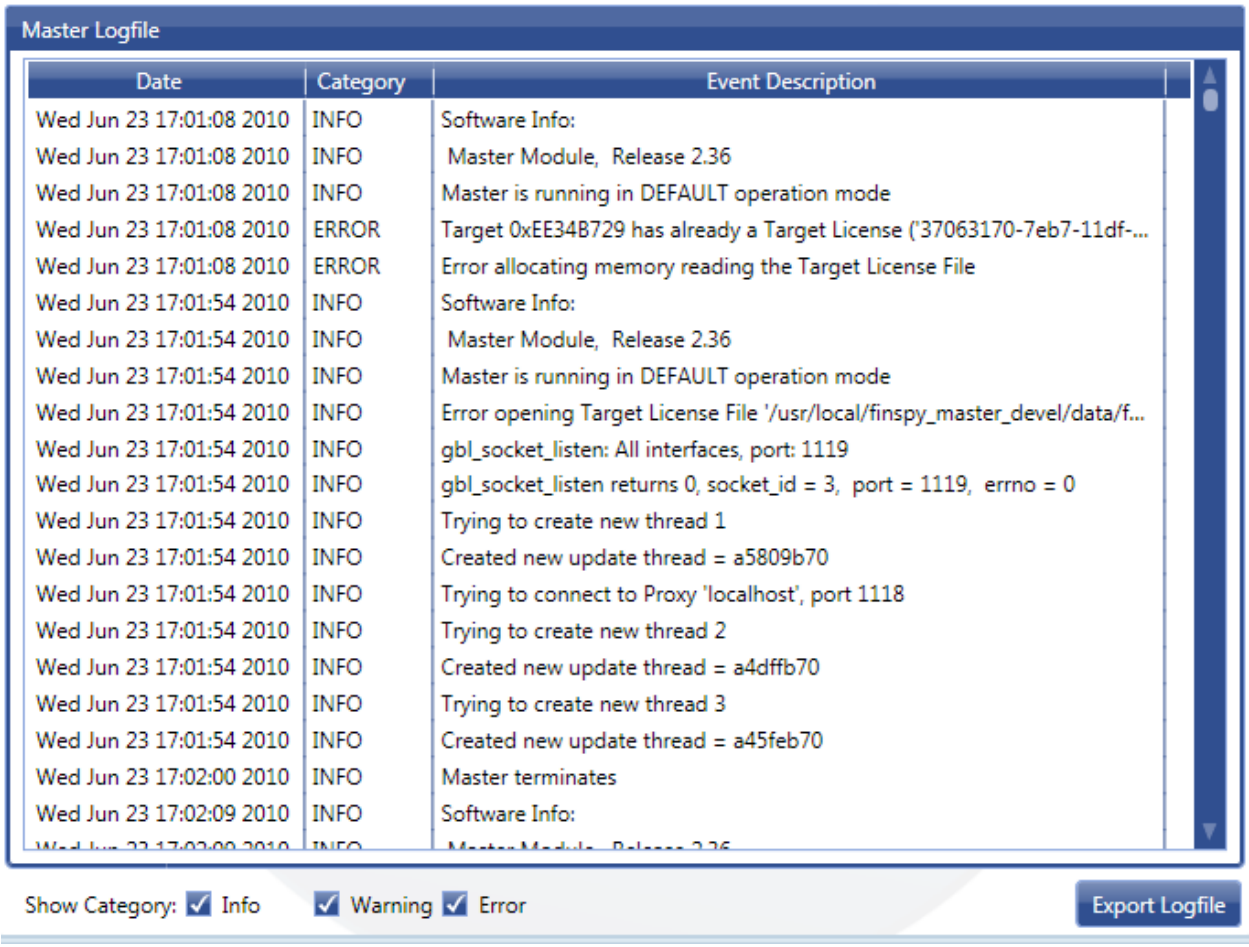
The Logfile viewer lets you monitor the Logs of the FinSpy Master very comfortably.

This Logfile can be divided into three categories:

- Info
- Warning
- Error

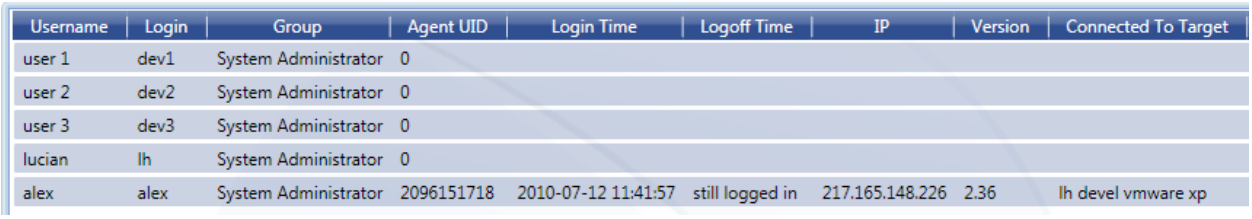
All data will then be shown with its Date, Category and Event Description.

Additionally, all the data can be exported to view the log files offline or with some other editor.



2.3.3 Agent List

If the Administrator of the FinSpy System wants to have an overview about all Agents, the “Agent List” can be used. It will show all necessary information about an Agent like connection information.



Username	Login	Group	Agent UID	Login Time	Logoff Time	IP	Version	Connected To Target
user 1	dev1	System Administrator	0					
user 2	dev2	System Administrator	0					
user 3	dev3	System Administrator	0					
lucian	lh	System Administrator	0					
alex	alex	System Administrator	2096151718	2010-07-12 11:41:57	still logged in	217.165.148.226	2.36	lh devel vmware xp

Name	Description
Username	Description of the User
Login Name	Username which is used to login
Group	Group to which the User belongs
Agent UID	Unique ID of each FinSpy Agent Software
Login Time	Since when is the user logged in
Logoff Time	When the user logged off
IP	From which IP the user logged in
Version	Which client version is the user using
Connected To Target	To which target is the user currently connected

2.3.4 License Information

Licenses can be imported through the FinSpy Agent directly and will be active immediately. Information given for the license:

- Machine UID
- Software UID
- Software Name
- Customer UID
- Valid From
- Valid Until
- Number of Targets
- Number of Agents
- Version Type
- Status

2.3.5 LEMF – Data Management

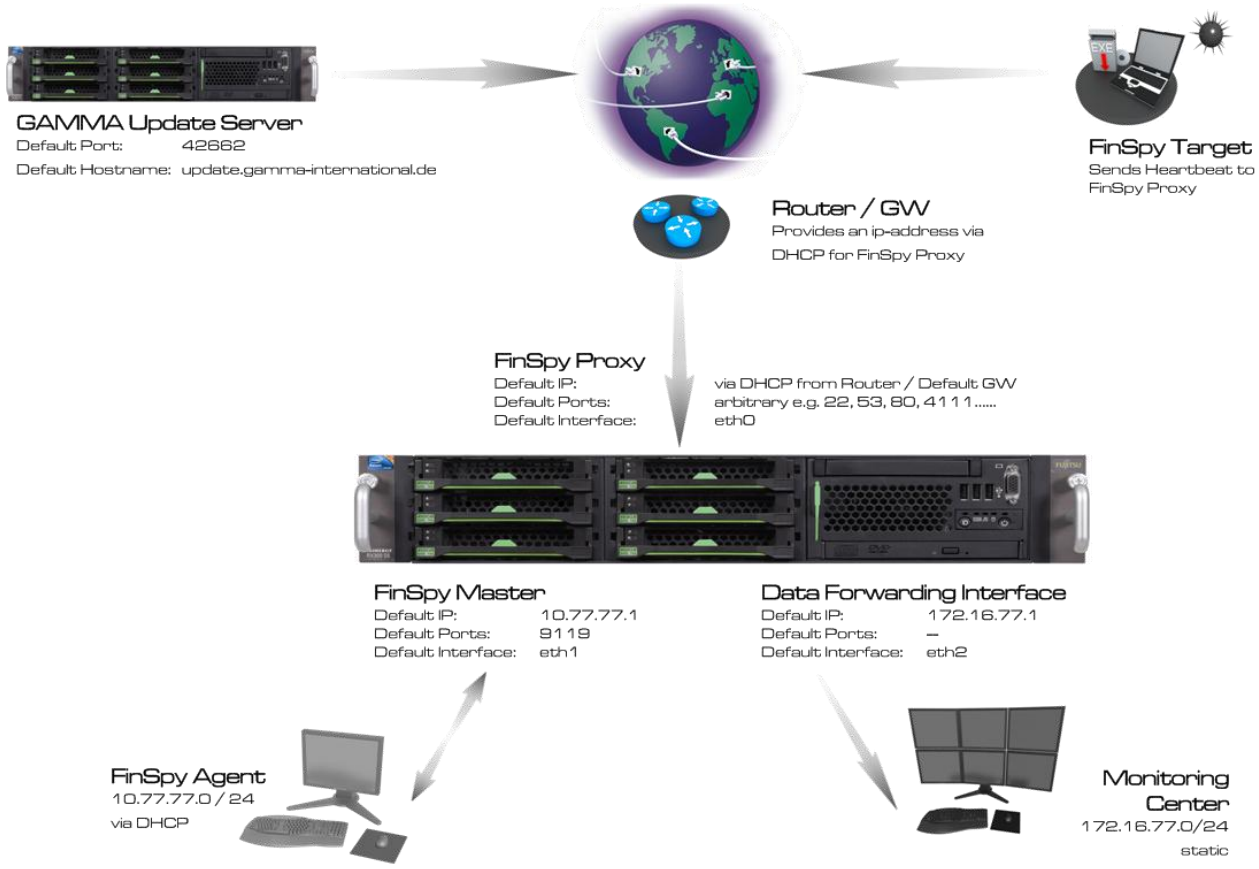
The LEMF - Data Management feature allows the user to take control over the data flow from the FinSpy System to the configured monitoring centre. Data is collected on the FinSpy System into sessions. Once the configured time threshold is reached or the configured data quantity threshold is reached the session is finalized and the data is transmitted to the configured Monitoring Centre. All the transmitted sessions are archived and keep on the FinSpy system for the configured period of time.

Through the LEMF – Data Management the user is able to review all the transmitted sessions and has the capability to resend full sessions or just specific data from a certain session.

FINSPY MASTER

This chapter will cover the installation and configuration of the FinSpy Master. The FinSpy Master is the central data collector and manages the data. The FinSpy Master includes the FinSpy Proxy. The FinSpy Proxy retrieves the data from the FinSpy Target and the FinSpy Relay connections.

The default setup should look like this:



2.4 FinSpy Master – Installation

Except the License, the FinSpy Master software is preinstalled on the FinSpy Master hardware. This means, only the license needs to be generated and installed via a Machine-ID.

This Machine-ID must be sent to your GAMMA sales contact to request the license package which contains the valid license. The following command will generate the Machine-ID:

```
# sudo /usr/local/finspy_master/bin/generate_machine_id -x
```

If you retrieved the license package from the GAMMA support, don't unpack it. Copy the archive to a USB stick or burn it to a CD-ROM.

Mount USB-Stick or CD/DVD on the FinSpy Master:

CD-ROM:

```
# sudo mount /media/cdrom0
```

USB-Stick:

```
# sudo mount /dev/sdb1 /mnt/usb
```

Copy the license archive to /usr/local/finspy_master/data/license

CD-ROM:

```
# cp /media/cdrom0/CERTS-FINSPYV2-Customer_ID-Machine_ID-XX.DAYS.zip \
/usr/local/finspy_master/data/license
```

USB-Stick:

```
# cp /mnt/usb/CERTS CERTS-FINSPYV2-Customer_ID-Machine_ID-XX.DAYS.zip  \
/usr/local/finspy_master/data/license
```

Change the directory and unzip license file.

```
# cd /usr/local/finspy_master/data/license
# unzip  CERTS-FINSPYV2-Customer_ID-Machine_ID-XX.DAYS.zip
```

Remove license zip file

```
# rm CERTS-FINSPYV2-Customer_ID-Machine_ID-XX.DAYS.zip
```

The license is now successfully installed.

2.5 FinSpy Master – Configuration

This chapter will guide through the steps how the FinSpy Master needs to be configured correctly to work.

The main configuration file for the FinSpy Master is the “finspy_master.cfg”.

2.5.1 General

The default template needs to be renamed to activate the changes.

```
# cd /usr/local/finspy_master/data/
# cp finspy_master.cfg_template finspy_master.cfg
```

To edit the file the text editor “nano” can be used.

```
# nano /usr/local/finspy_master/data/finspy_master.cfg
```

Now the following parameters need to be activated and / or edited:

```
FIN_AGENT_NETWORK_INTERFACE = eth1

FIN_PROXY_1 = 127.0.0.1, 9118

# use the Ports as defined in finspy_proxy.cfg as FIN_TARGET_PORTS
FIN_TARGET_PROXY1 = PROXY-IP/HOSTNAME, PROXYPORTS

# could be changed to another mount point e.g. /mnt/data
# The internal HW-RAID shall be used
FIN_REPOSITORY_VOLUME = /mnt/xyz
```

2.5.2 Users Management

In the first step it is necessary to create users which are able to connect to the FinSpy Master.

```
# cd /usr/local/finspy_master/data/
# sudo cp fin_passwd_template .fin_passwd
```

Open the *.fin_passwd* to create, change or delete user accounts.

```
# sudo nano .fin_passwd
```

This will show the template data in the following structure:

userid ; groupid ; login name ; user description ; password ; database permission ; file permission

The following parameters can be changed:

userid ; login name; user description; password

Note: "login name" and "password" have a maximum length of 16 characters where ";" is not allowed as a character.

All other values are reserved for future releases and should not be changed!

2.5.3 Update – Automatic

The configurations for the Updates are also stored in the “finspy_master.cfg” and should not be changed!

```
FINUM_SERVER           = update.gamma-international.de
FINUM_PORTS            = 42662
FINUM_DESTINATION_PATH = ../updates
```

To force an update request the FinSpy Master needs to be stopped and started which will make the FinSpy Master automatically connect to the GAMMA Update server.

```
# sudo /etc/init.d/finspy_master stop
# sudo /etc/init.d/finspy_master start
```

To check for the currently installed version, you can use the following command:

```
#  cat /usr/local/finspy_master/data/version
```

2.5.4 Update – Manual

To update the FinSpy Master manually the latest version can be obtained via E-Mail from the Gamma support. The two files will be “finspy_master_2-xx.ggi” and “finspy_proxy_2-xx.ggi”. The files must be copied to a USB-Stick or burned to a CD/DVD.

Mount USB-Stick or CD/DVD on the FinSpy Master:

CD-ROM:

```
# sudo mount /media/cdrom0
```

USB-Stick:

```
# sudo mount /dev/sdb1 /mnt/usb
```

Both files must be copied to the /tmp directory

CD-ROM:

```
# cp /media/cdrom0/* /tmp
```

USB-Stick:

```
# cp /mnt/usb/* /tmp
```

Change the directory and execute the files

```
# cd /tmp
# ./finspy_master_2-xx.ggi
# ./finspy_proxy_2-xx.ggi
```

2.5.5 Evidence Protection

By default the “Evidence Protection” feature is disabled. To activate it, the following configuration switch in the “finspy_master.cfg” needs to be changed to “true”.

```
FIN_EVIDENCE_PROTECTION = true
```

To activate the changes, the FinSpy Master needs to be restarted:

```
# sudo /etc/init.d/finspy_master stop
# sudo /etc/init.d/finspy_master start
```

2.5.6 E-Mail Notification

By default, FinSpy Master is using its local MTA (Mail Transfer Agent). No Auth & TLS is used. Following parameters are necessary:

```
# IP-Address of MTA:
FIN_MX_NOTIFY_SERVER = 127.0.0.1

# SMTP Port:
FIN_MX_NOTIFY_PORT = 25

# Authentication Mode:
FIN_MX_NOTIFY_AUTH = plain

# RCPT FROM – User (exim only accept "FinSpy-MP" Domain! case sensitive!):
FIN_MX_NOTIFY_SENDER = fs@FinSpy-MP

# Alias = arbitrary:
FIN_MX_NOTIFY_ALIAS = fs-notifier
```

FinSpy Master can also use a free webmail service (e.g. Gmail) to transport all notification messages. Most of them need pre-authentication & TLS!

```
# Hostname (SMTP Server Gmail):
FIN_MX_NOTIFY_SERVER = smtp.googlemail.com

# SMTP – Port:
FIN_MX_NOTIFY_PORT = 25

# GMAIL Username:
FIN_MX_NOTIFY_USER = user@gmail.com

# GMAIL - Password:
FIN_MX_NOTIFY_PASS = top_secret

# GMAIL required TLS:
FIN_MX_NOTIFY_TLS_ENABLE = yes

# TLS Auth. type = login:
FIN_MX_NOTIFY_AUTH = login

# Sender = GMAIL Username:
FIN_MX_NOTIFY_SENDER = user@gmail.com

# Alias = arbitrary:
FIN_MX_NOTIFY_ALIAS = fs-notifier
```

The FIN_MX_NOTIFY_ALIAS will act as the Sender Name.

To activate the changes, the FinSpy Master needs to be restarted:

```
# sudo /etc/init.d/finspy_master stop
# sudo /etc/init.d/finspy_master start
```

2.6 FinSpy Master – Proxy Configuration

The FinSpy Proxy needs a minimal setup as almost everything is already preconfigured. The FinSpy Proxy needs to know on which ports it will listen.

The main configuration file for the FinSpy Master is the “finspy_proxy.cfg”.

The default template needs to be renamed to activate the changes.

```
# cd /usr/local/finspy_proxy/data/
# cp finspy_proxy.cfg_template finspy_proxy.cfg
```

To edit the file the text editor “nano” can be used.

```
# nano /usr/local/finspy_proxy/data/finspy_proxy.cfg
```

Now the following parameters need to be activated and / or edited:

```
FIN_MASTER_NETWORK_INTERFACE = lo
FIN_TARGET_NETWORK_INTERFACE = eth0
FIN_TARGET_PORTS = 22,53,80,443,4111
```

To activate the changes, the FinSpy Master needs to be restarted:

```
# sudo /etc/init.d/finspy_proxy stop
# sudo /etc/init.d/finspy_start start
```

2.7 FinSpy Master – Remote and Offline Master Configuration

It is possible to setup a Remote Mode and Offline Mode. They basically split the FinSpy Master functionalities in two FinSpy Masters with complementary limited functionalities.

The Offline Master has the recorded files in the database and the FinSpy Agent can process data while the Remote Master is contacted by the targets and stores the received, encrypted recordings. The recorded files have to be imported with the Agent to the Offline Master. This gives a higher security to the Offline Master if remote attacks are conducted.

2.7.1 Remote Master Configuration

To setup the Remote Master the following parameter must be added into the “finspy_master.cfg” file.

Set Remote Master Mode:

```
FIN_MASTER_MODE = REMOTE
```

Copy required certificates and the fin_target_licenses.txt from Offline Master to USB Stick

```
# sudo mount /dev/sdXX /mnt/usb
# sudo cp /usr/local/finspy_master/data/certs/trojan-commu* /mnt/usb
# sudo cp /usr/local/finspy_master/data/fin_target_licenses.txt /mnt/usb
# sudo umount /mnt/usb
```

Copy required certificates and the fin_target_licenses.txt from USB Stick to Remote Master

```
# sudo mount /dev/sdXX /mnt/usb
# sudo mv /mnt/usb/trojan-commu* /usr/local/finspy_master/data/certs/
# sudo mv /mnt/usb/fin_target_licenses.txt /usr/local/finspy_master/data/
# sudo umount /mnt/usb
```

To activate the changes, the FinSpy Remote Master needs to be restarted:

```
# sudo /etc/init.d/finspy_proxy stop
# sudo /etc/init.d/finspy_master stop

# sudo /etc/init.d/finspy_proxy start
# sudo /etc/init.d/finspy_master start
```

2.7.2 Offline Master Configuration

To setup the Offline Master the following parameter must be added into the “finspy_master.cfg” file.

Set Offline Master Mode:

```
FIN_MASTER_MODE = OFFLINE
```

Assume FIN_TARGET_PROXY_1 values from Remote Master

```
FIN_TARGET_PROXY_1   = (same values as Remote Master)
```

To activate the changes, the FinSpy Offline Master needs to be restarted:

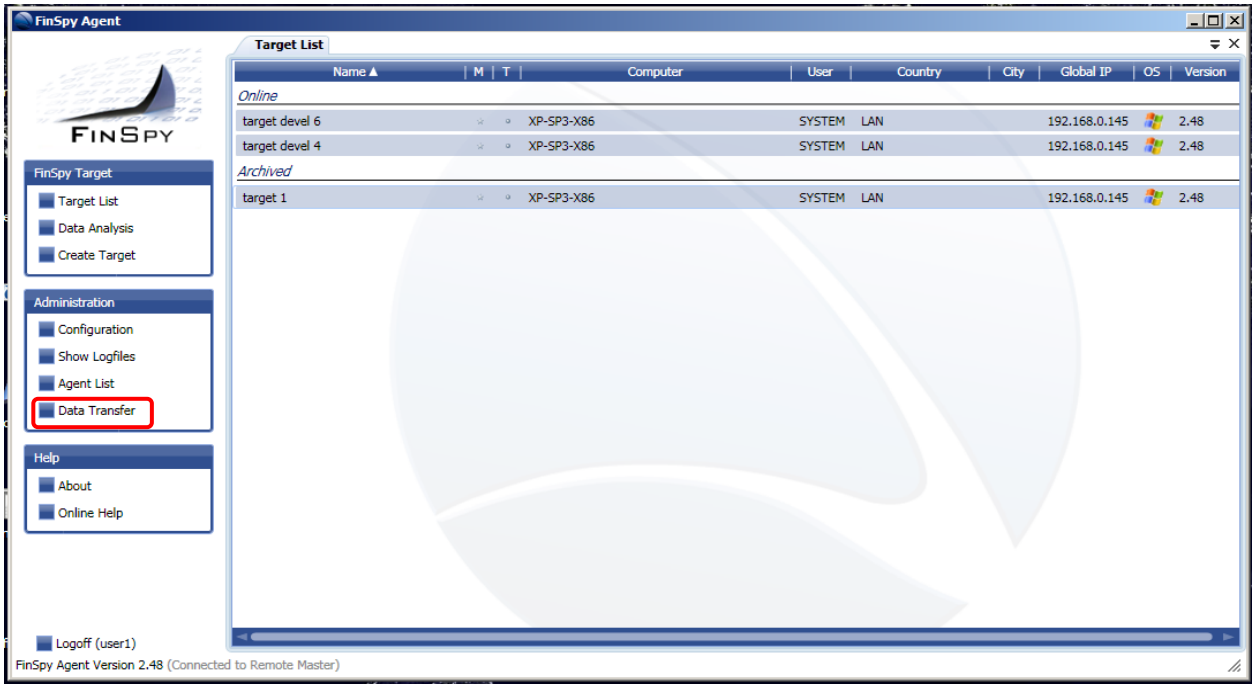
```
# sudo /etc/init.d/finspy_master stop
# sudo /etc/init.d/finspy_master start
```

2.7.3 Data Transfer

It is necessary to transfer data from the Remote Master to the Offline Master and then it needs to be imported into the database.

2.7.3.1 Export Data from Remote Master

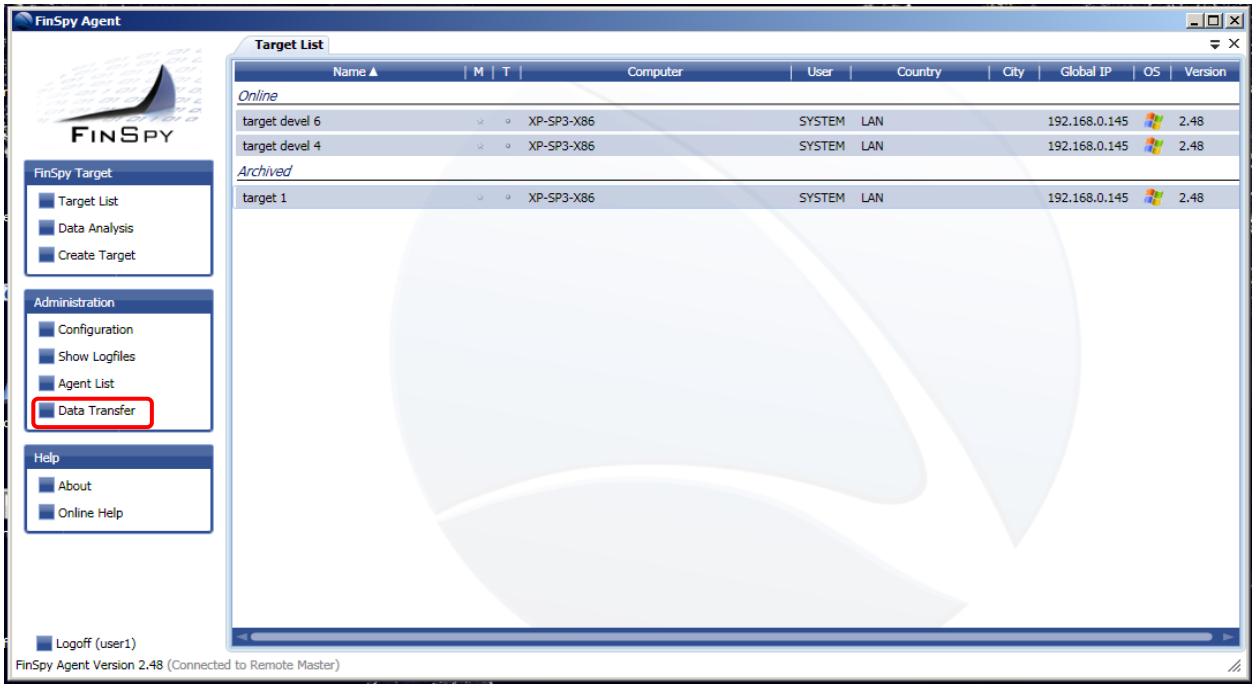
- Connect Agent to the Remote Master
- Please select Data Transfer



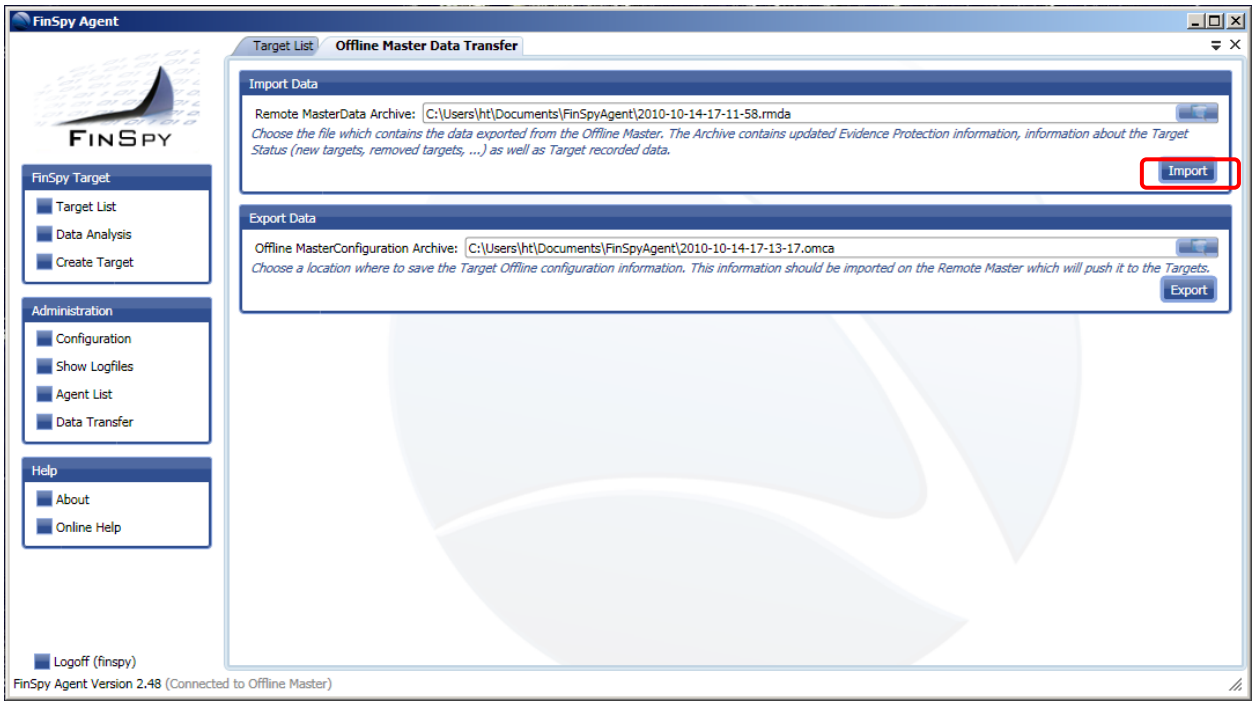
- Select Export

2.7.3.2 Import Data to the Offline Master

- Connect Agent to the Offline Master
- Select Data Transfer



- Select Import



2.8 FinSpy Master – Monitoring

There is a monitoring daemon installed on the system which checks and if necessary restarts applications like FinSpy Master and FinSpy Proxy.

The software being used is “monit”. Monit automatically checks if the defined services are running.

FinSpy Master and FinSpy Proxy need to be configured first.

In the following “*finspy_xxx*” is mentioned which stands for both commands:

- finspy_master
- finspy_proxy

Configure “monit” daemon to monitor *finspy_xxx*:

```
# sudo monit monitor finspy_xxx
# sudo /etc/init.d/monit restart
```

Check if *finspy_xxx* is running:

```
# sudo monit summary
```

The following results may appear.

Successful:

Process ‘finspy_proxy’ running

Failed:

Process ‘finspy_proxy’ not monitored

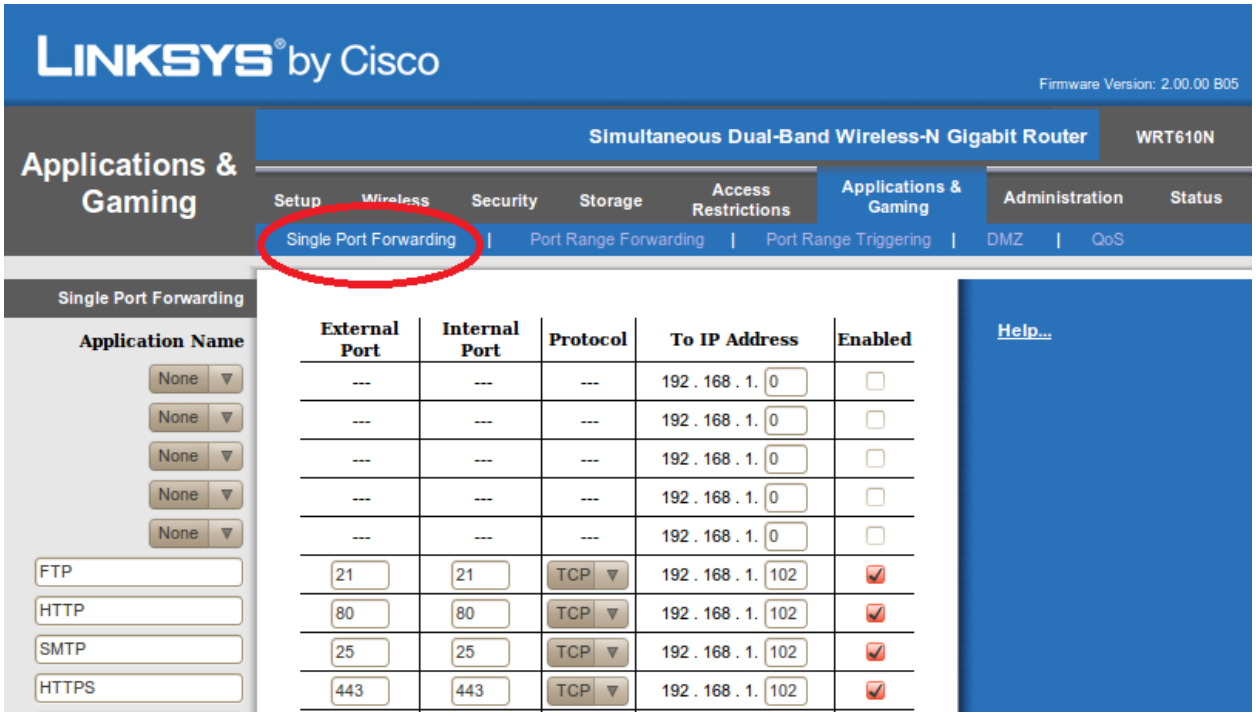
Process ‘finspy_proxy’ Does not exist

2.9 FinSpy Master – Port forwarding

It is necessary that the FinSpy Master is able to retrieve packets from the internet through a Router or Firewall. Normally, Router or Firewalls will block TCP packets which come from outside. That means that some ports on the Router or Firewall must be forwarded to the internal network. This is a so called Port Forwarding.

Every Router or Firewall handles this differently. Please check the corresponding manual on how to do this.

In the following example a Linksys Router was chosen. In this case our FinSpy Master has the IP "192.168.1.102" and should retrieve packets on the Ports 21, 25, 80 and 443.



2.10 FinSpy Master – Dynamic DNS

If the FinSpy Master doesn't have the chance of retrieving a public static IP address, a dynamic DNS can be used. A dynamic DNS service allows users to have a subdomain that points to a computer with regularly-changing IP addresses.

On the FinSpy Master this can be realized with a small application called "ddclient". "ddclient" is used to update dynamic DNS entries for accounts on Dynamic DNS Network Services' free DNS service. Various free DNS services can be used like DynDNS.com

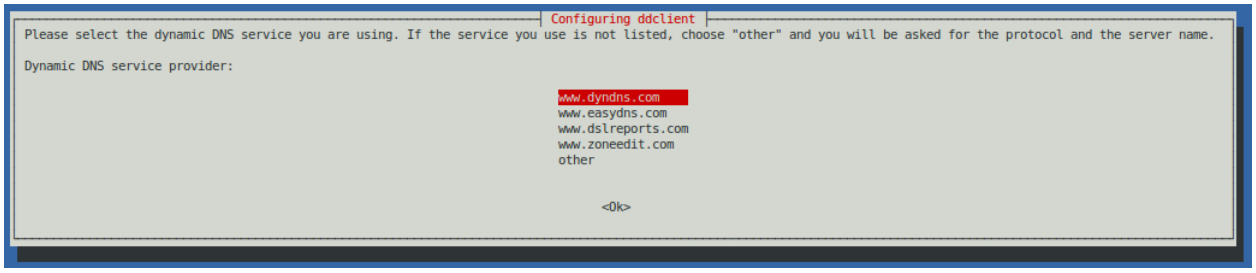
To use "ddclient" a registration is required on the page.

To install ddclient:

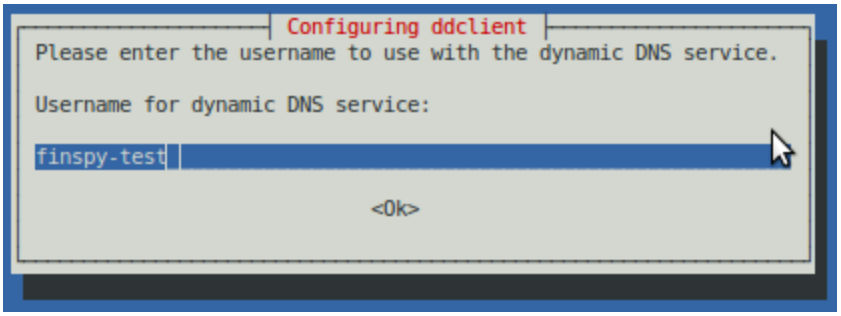
```
# sudo aptitude install ddclient
```

It will ask several questions during the installation.

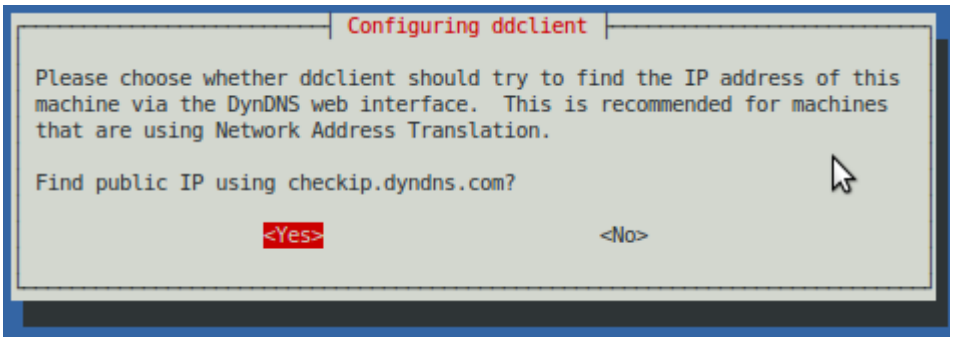
Which service shall be used:



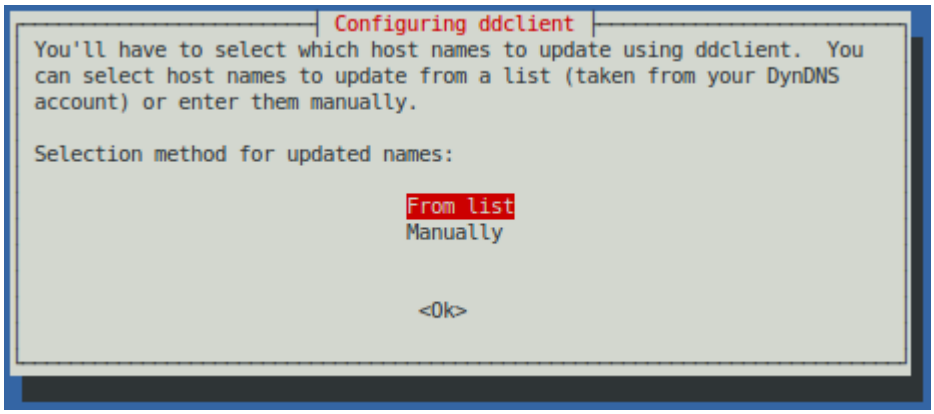
Username which is registered on the service:



Auto retrieval of the IP address:



Updating host:



After the installation, everything should run fine now with the host **finspy-test.dyndns.com**.

If some configuration needs to be changed, the configuration file is located at "/etc/ddclient.conf" and should look like this:

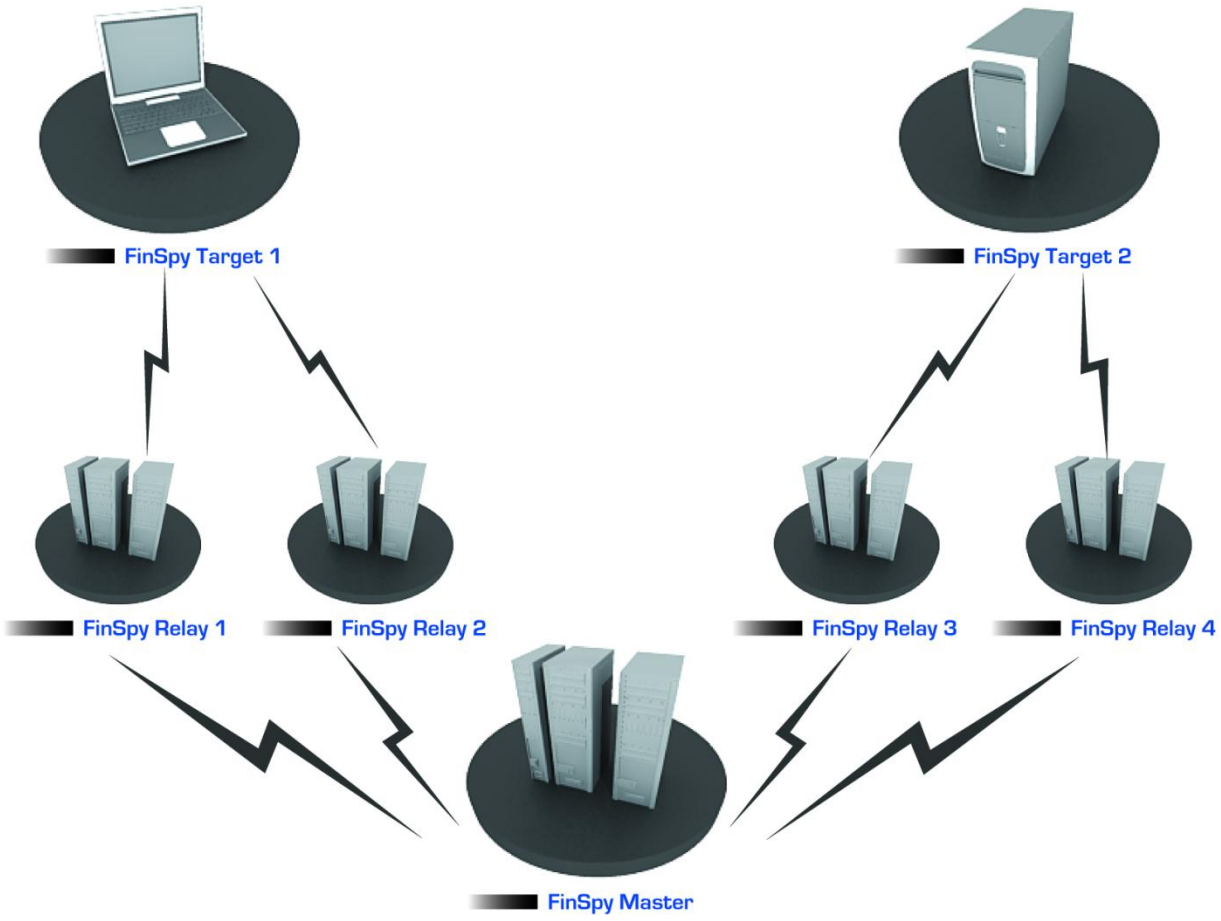
```
protocol=dyndns2
use=web, web=checkip.dyndns.com, web-skip='IP Address'
server=members.dyndns.org
login=finspy-test
password='dfUc!45XfP'
```

Username and Password can easily be edited.

3 FINSPY RELAY

The FinSpy Relay will handle and relay all connections from the FinSpy Target to the FinSpy Master. The FinSpy Relay acts as a proxy between those two endpoints. This will help by not having a direct connection from the FinSpy Target to the FinSpy Master. Instead, the FinSpy Relay can reside in any place in the world.

The FinSpy Relay is a small program which can be installed on most Windows and Linux Operating Systems.



3.1 FinSpy Relay – Configuration Options

The FinSpy Relay runs according to the settings from the "relay.cfg" file which can be found in the following directories.

Windows: In the same directory of the binaries where FinSpy Relay was installed

Linux: */usr/local/ffrelay/data/*

The "relay.cfg" file contains the following settings:

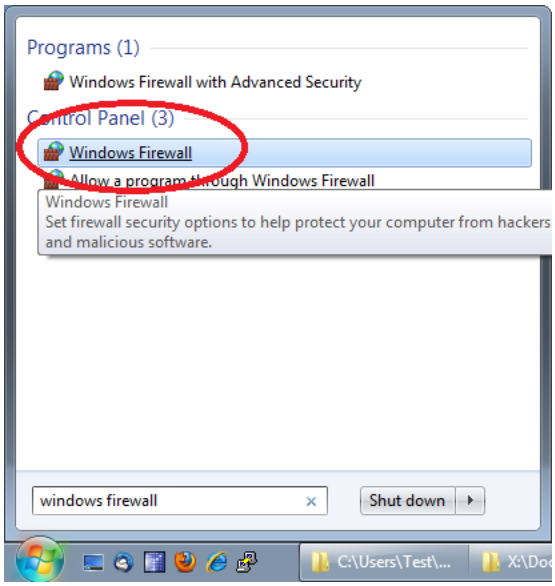
Name	Description
CFG_TARGET_PORTS	Contains the ports where the FinSpy Relay "listens" for incoming FinSpy Target connections, e.g.: CFG_TARGET_PORTS = 1111, 1112, 1113
CFG_NEXT_HOP_1	Contains the Hostname and ports where the Relay should connect to (next FinSpy Relay or FinSpy Master/Proxy), e.g.: CFG_NEXT_HOP_1 = 192.168.0.49, 1111
CFG_SOCKET_TIMEOUT	Contains the socket read/write timeout in seconds, e.g.: CFG_SOCKET_TIMEOUT = 10

The default template of the "relay.cfg" which comes with the FinSpy Relay:

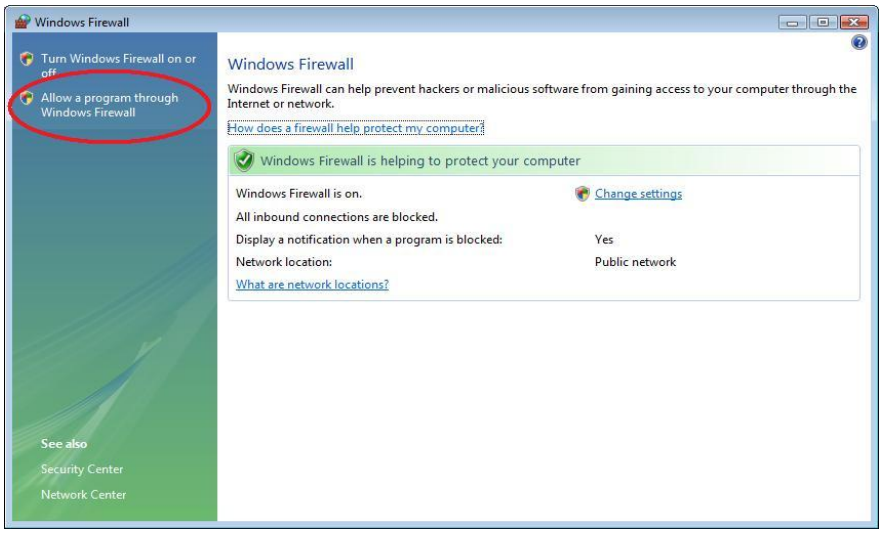
```
# Configuration file for the Relay Module
# list of ports for incoming (target-side) connections:
CFG_TARGET_PORTS    = 2000
# Next hops to connect (relays, proxy)
CFG_NEXT_HOP_1          = hostname, 2050
# socket read/write-timeout (in seconds)
CFG_SOCKET_TIMEOUT = 10
```

3.2 FinSpy Relay – Windows

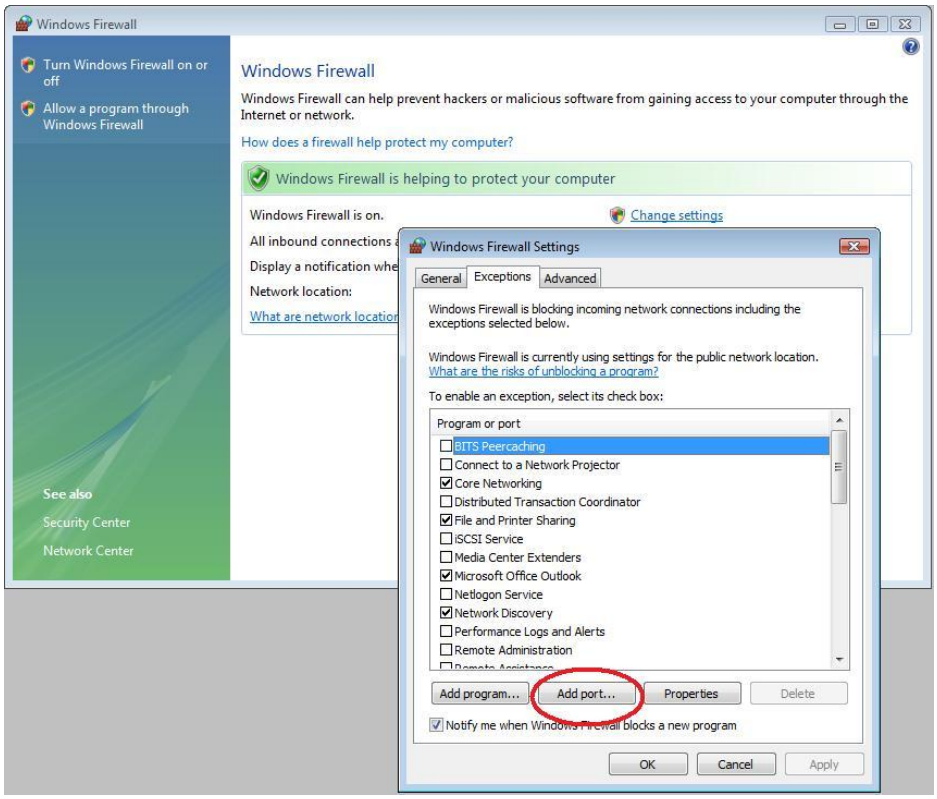
3.2.1 Prerequisites

Name	Description
Windows Firewall	To operate a Windows Computer as a FinSpy Relay, the following preparation must be made. The Windows Firewall should be instructed to let the FinSpy Relay accept and forward data. The Windows Firewall is enabled by default on every Windows Computer. 

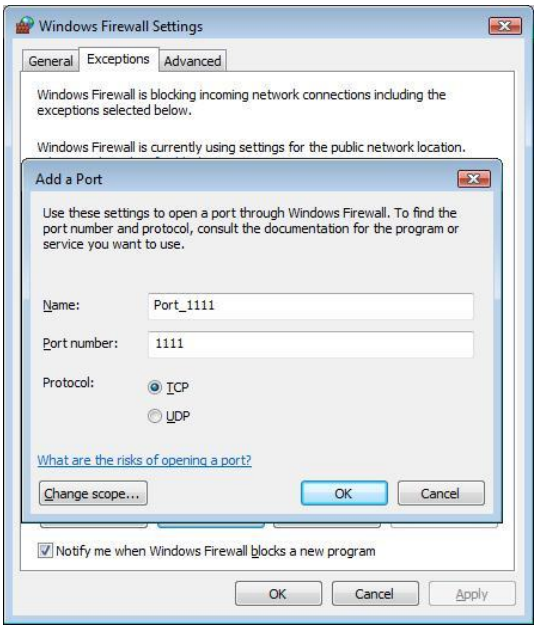
Click “Allow a program through Windows Firewall”.



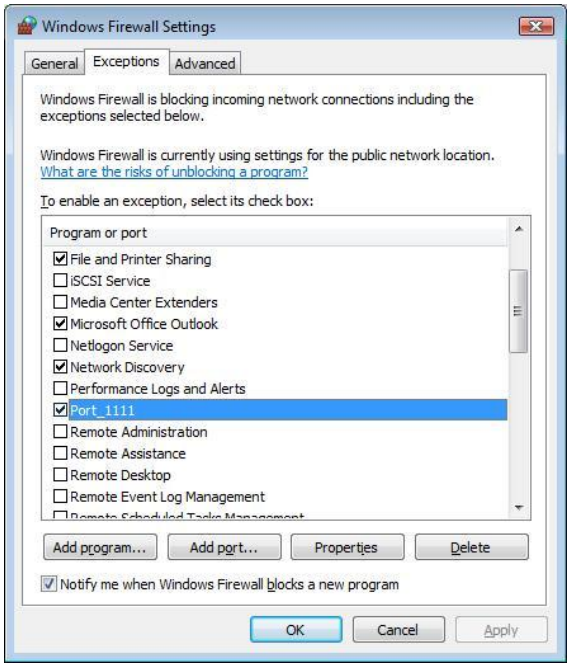
At the “Exceptions” Tab, click “Add Port” in order to add the ports the FinSpy Relay will be working with.



Enter one of the ports where the FinSpy Relay “listens” for the Targets or a port used by the FinSpy Relay to send out data.



Now the ports must be selected in the exception list to activate them.



Redo the steps in order to add all the ports used by the FinSpy Relay for incoming and outgoing ports.

3.2.2 Installation

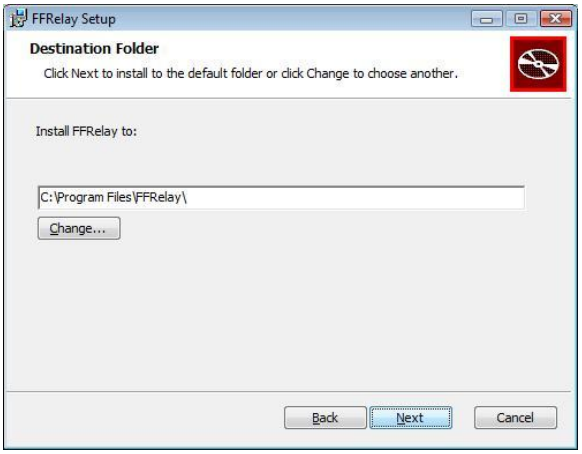
To install the FinSpy Relay in Windows the Installer needs to be executed.

The filename is: *RelayInstaller_2.xx.x.msi*

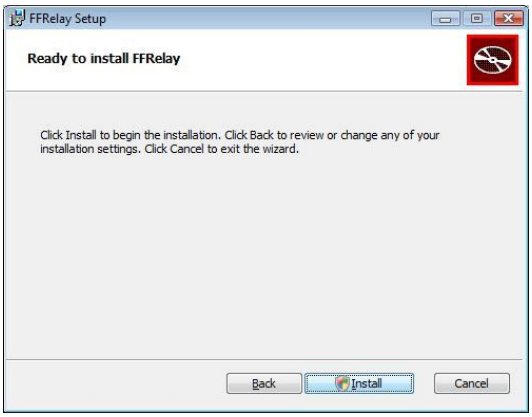
This will start the installation.

At the License Agreement “I accept the terms in the License Agreement” must be selected.

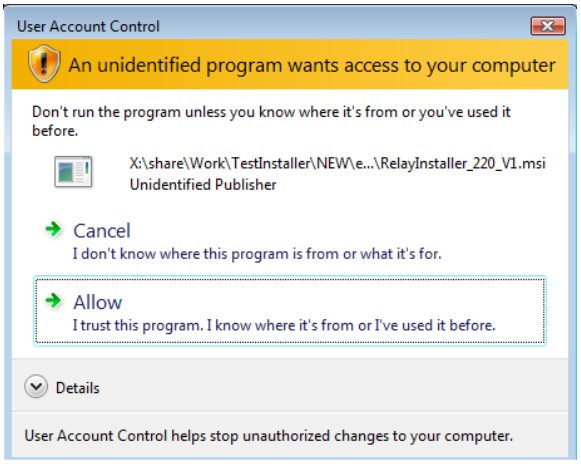
Now the directory where the FinSpy Relay will be installed can be chosen:



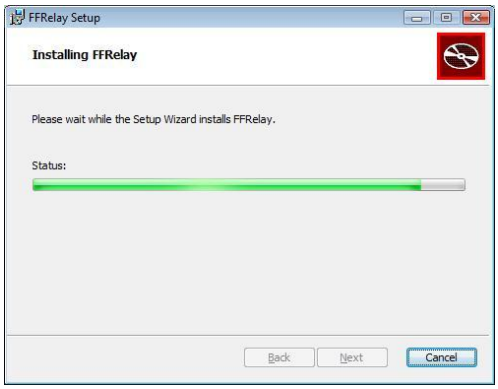
After choosing the directory, click OK and the following dialog will be shown:



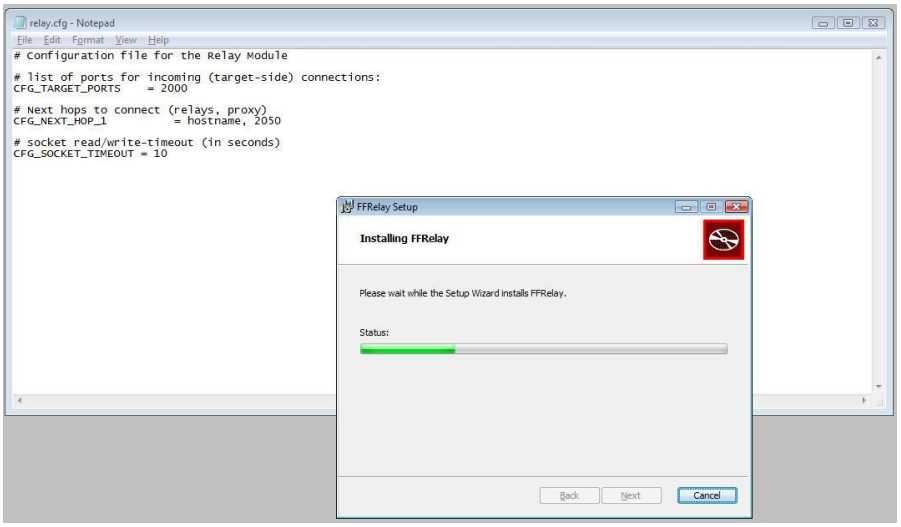
Once the “Install” button is clicked, on Windows Vista and Windows 7, the UAC (user account control) popup will be shown and this needs to be allowed!



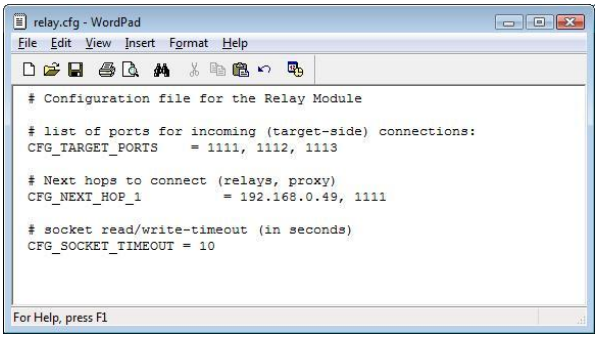
Once “Allow” is clicked, the installation starts:



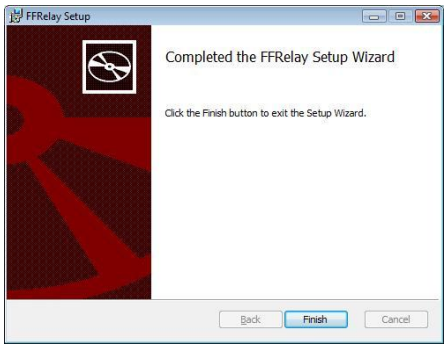
During the installation, the installer will open Notepad with the relay.cfg file where the relay settings should be done:



Note: sometimes the relay.cfg file is opened behind the installer.



After editing the relay.cfg it needs to be saved and closed. The installer continues until the FinSpy Relay is installed.



The “relay.cfg” needs to be changed according to FinSpy Relay – Configuration Options.

3.2.3 Monitoring

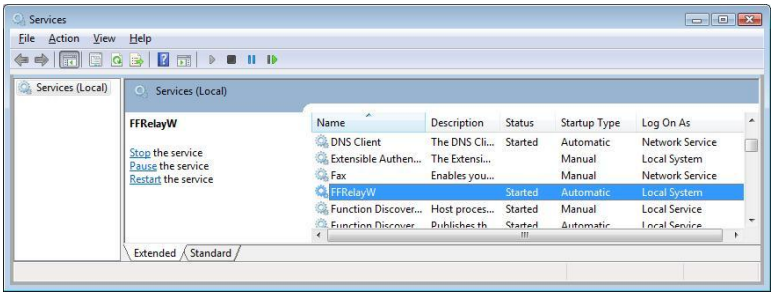
Along with FinSpy Relay comes also a FinSpy Relay Monitoring, which takes care of starting/stopping the Relay. If the FinSpy Relay crashes then the FinSpy Relay Monitoring will restart it. The FinSpy Relay Monitoring is a Windows-Service. If the FinSpy Relay Monitoring service is stopped, the service will then also stop the FinSpy Relay. If the FinSpy Relay Monitoring is started it will start the Relay.

The FinSpy Relay Monitoring binary and service name is: *FFRelayW*(.exe)

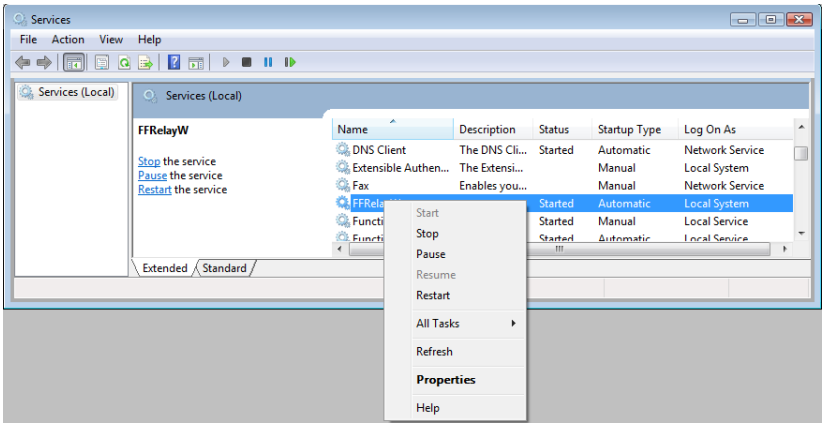
The FinSpy Relay binary name is: *FFRelay*(.exe)

To control the FinSpy Relay Monitoring open the Services window:

Control Panel\Administrative Tools\Services

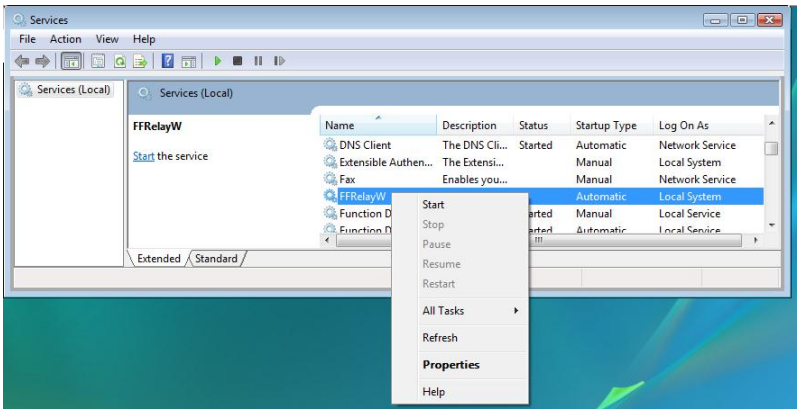


Right-click on the Service and chose whatever action is needed (e.g. “Stop”):



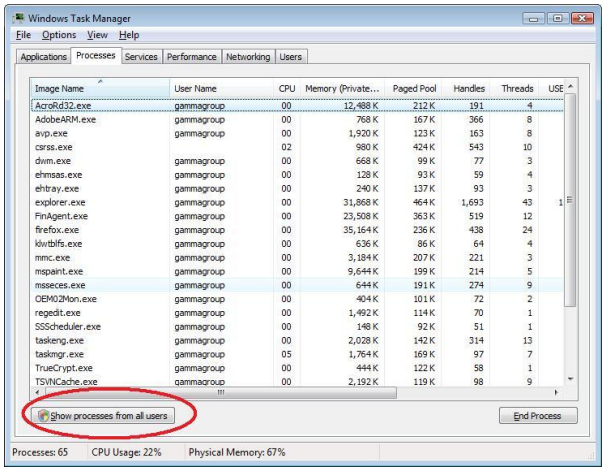
If the FinSpy Relay Monitoring service is stopped, the Relay is also stopped.

To start the FinSpy Relay Monitoring the *FFRelayW* service needs to be right-clicked and “Start” chosen:



To check if *FFRelayW* and *FFRelay* are running, the Task-Manager needs to be opened and the "Processes" Tab must be active:

The *FFRelayW* process is running in the SYSTEM context as it is a service and because the *FFRelay* is started by the service it runs also in the SYSTEM context, meaning none of them run as the current user. In order to see all the processes running on a machine click "Show processes from all users":



Now all the processes running on the machine will be shown, including the *FFRelayW* and *FFRelay*.

3.3 FinSpy Relay – Linux

3.3.1 Prerequisites

The software runs “out-of-the box” under normal circumstances.

Name	Description
Hardware	• minimal 256 MB RAM • recommended 512 MB RAM
Linux Distributions	• Ubuntu / Debian
Software	“monit” should be installed. http://mmonit.com/monit/ Further information can be obtained from the FinSpy Master section.

3.3.2 Installation

To install the FinSpy Relay in Linux the Installer needs to be executed with “root” privileges.

The filename is: *ffrelay.ubuntu.2.xx.ggi*

```
root@localhost:~$ ./ffrelay.ubuntu.2.xx.ggi
 FInstaller 1.0
----------------------
Extracting Installation Files...
installer
ffrelay.ggi.tar

Launching Installer...

CDIR
/home/xaitax
TMPDIR
/tmp/selfextract.fYCZZ4
Stopping FFRelay
monit: generated unique Monit id xxx and stored to '/root/.monit.id'
monit: service 'ffrelay' -- doesn't exist
Extracting Software Files...
./
./usr/
./usr/local/
./usr/local/ffrelay/
./usr/local/ffrelay/lib/
./usr/local/ffrelay/bin/
./usr/local/ffrelay/bin/ffrelay
./usr/local/ffrelay/updates/
./usr/local/ffrelay/data/
./usr/local/ffrelay/data/relay.cfg_template
./usr/local/ffrelay/data/version
./etc/
./etc/monit.d/
./etc/monit.d/ffrelay
./etc/init.d/
./etc/init.d/ffrelay

Running Post-Installation Steps...
Starting FFRelay
monit: service 'ffrelay' -- doesn't exist

FFRelay Installer done.
```

The only thing which needs to be done after installation is to rename the configuration file so that it is accepted by the FinSpy Relay.

```
# cd /usr/local/ffrelay/data/
# cp relay.cfg_template relay.cfg
```

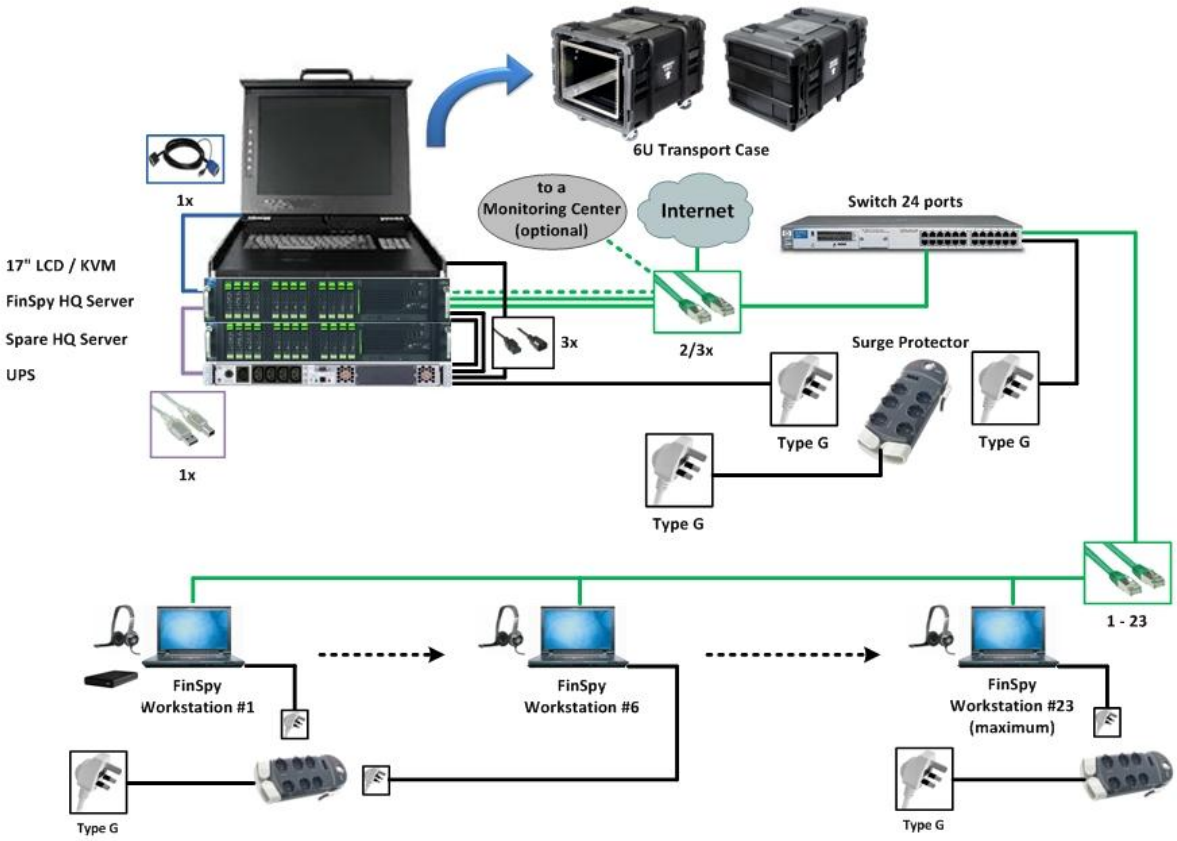
The “relay.cfg” needs to be changed according to FinSpy Relay – Configuration Options.

4 FINSPY HARDWARE SETUP

It is necessary to know how the FinSpy Setup needs to be configured in detail. The following chapter will give an inside view into the FinSpy periphery.

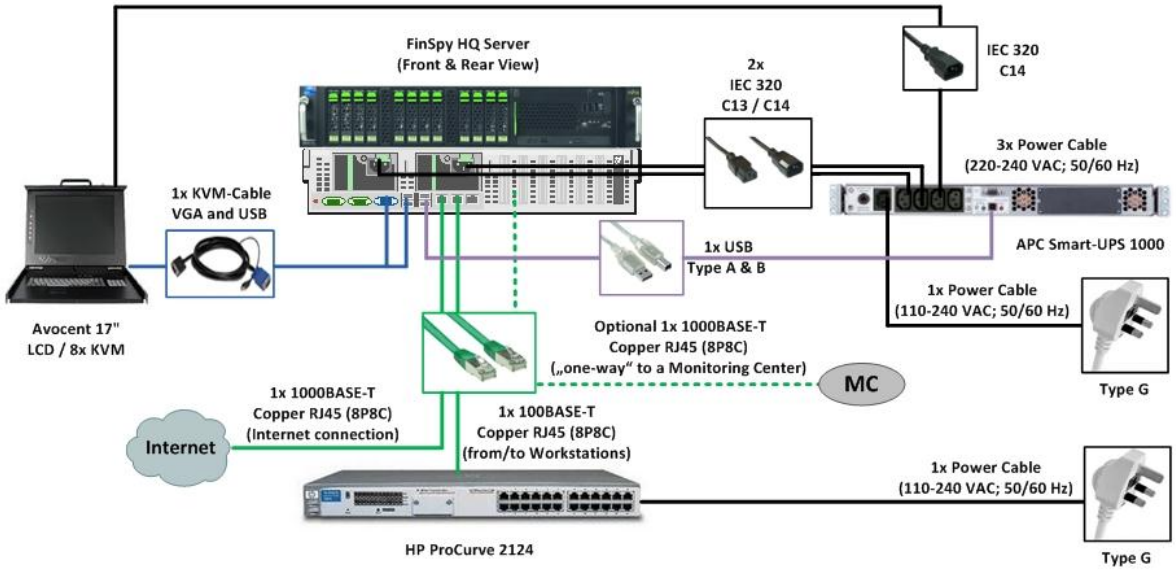
4.1 FinSpy Total Setup

The following diagram gives a detailed view into the FinSpy Hardware setup.



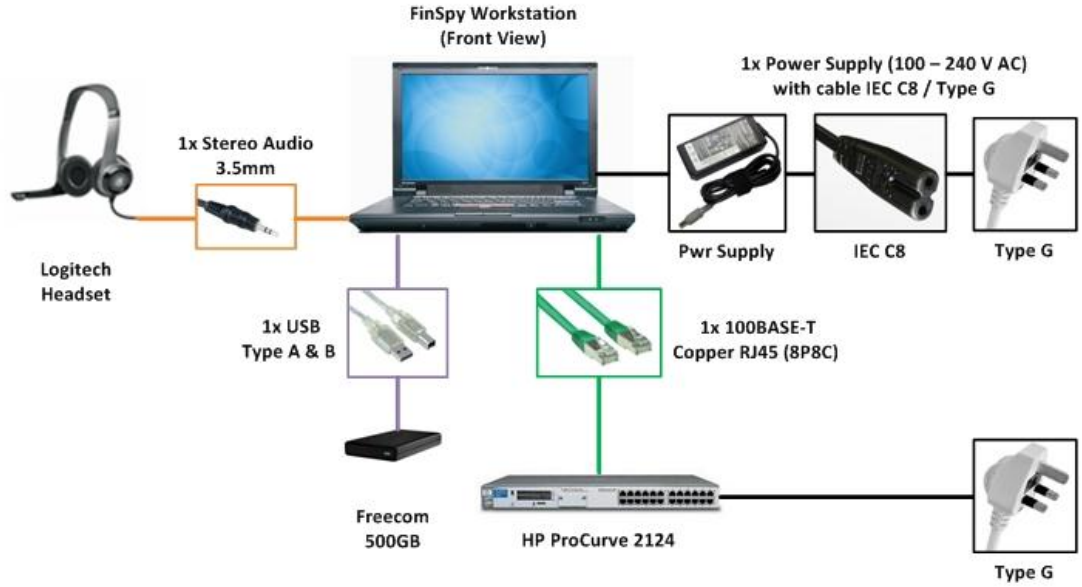
4.2 FinSpy Master Setup

The following diagram gives a detailed view into the FinSpy Master Hardware setup.



4.3 FinSpy Agent Setup

The following diagram gives a detailed view into the FinSpy Agent Hardware setup.



5 SUPPORT

All customers have access to an after-sales website that gives the customers the following capabilities:

- Download product information (Latest user manuals, specifications, training slides)
- Access change-log and roadmap for products
- Report bugs and submit feature requests
- Inspect frequently asked questions (FAQ)

The after-sales website can be found at

- https://www.gamma-international.de
    - Username:
    - Password:

FINFISHER
IT INTRUSION

Home | Products | Support | Knowledge Base | Contact Us | www.GammaGroup.com

My Account [Log Out]

FINFISHER: GOVERNMENTAL IT INTRUSION
AND REMOTE MONITORING SOLUTIONS

FinSpy
- Generic Information
- Roadmap
- ChangeLog
- FAQs
- User Manual
- Training Slides

Home » Products » FinSpy

FinSpy is a field-proven Remote Monitoring Solution that enables Governments to face nowadays challenges of **monitoring Mobile and Security-Aware Targets** that regularly **change location**, use **encrypted and anonymous communication** channels and **reside in foreign countries**. Traditional Lawful Interception solutions **face new challenges** that can only be **solved using active systems** like FinSpy:

QUICK INFORMATION	
Usage:	Strategic Operations Tactical Operations
Capabilities:	Remote Computer Monitoring
Content:	Hard- and Software

- Data not transmitted over any network
- Encrypted Communication
- Targets in foreign countries

FinSpy has been **proven successful** in operations around the world **since many years** and valuable intelligence has been acquired about Target Individuals and Organizations.
When FinSpy is installed on a computer system or mobile phone it can be **remotely controlled and accessed** as soon as it is connected to the internet/network, **no matter where in the world** the Target System is based.

Usage Example 1: Intelligence Agency
FinSpy was installed on several computer systems inside Internet Café's in critical areas in order to monitor them for suspicious activity, especially **Skype communication** to foreign individuals. Using the Webcam, pictures of the Targets were done while they were using the system.

Usage Example 2: Organized Crime
FinSpy was **covertly deployed on the mobile phones** of several members of an Organized Crime Group. Using the **GPS tracking** data and **silent calls**, essential information could be gathered from **every meeting that was done** by this group.

Download Catalog: FinSpy-Catalog.pdf (352 KB)
Download Specifications: FinSpy-2.20-Specifications.pdf (2.38 MB)
Download Video: FinSpy-Video.wmv (4.68 MB)

Site Map

GAMMA INTERNATIONAL
United Kingdom

Tel: +44 - 1264 - 332 411
Fax: +44 - 1264 - 332 422

info@gammagroup.com

WWW.GAMMAGROUP.COM