Spybot S&D Update and Configuration Server 2.2 *

Safer-Networking Limited
P.O. Box 16
Greystones, Co. Wicklow
Ireland
info@safer-networking.ie
www.safer-networking.ie

November 15, 2011

Contents

List of Figures

1 Overview

This document is a manual intended for administrators who wish to use the **Spybot S&D Update and Configuration Server**. With this software you can easily manage a large number of installations of Spybot S&D in your network using a web-based frontend.
Its main features are:

- Download updates from our server on the Internet to a server on your intranet.
- Store these updates in a central location in your network for easy access for your Spybot S&D-clients.
- Schedule scans with Spybot S&D on the clients.
- Receive emails about the scan results.
- Centrally configure many aspects of all installed Spybot S&D instances in your network.
- Do all this from any host in your network with a web-based and password-protected user interface.

The Spybot S&D Update and Configuration Server consist of two main modules:

Spybot S&D Update and Configuration Server (sbNet) The main application that runs on the server as a service or command line tool. This program downloads the updates for Spybot S&D from the Internet and serves all downloaded updates to the Spybot S&D installations in your network. A web interface can be used for configuring all aspects of the Spybot S&D Update and Configuration Server.

Spybot S&D Client Configurator (SBCC) Program that runs on every client where Spybot S&D is installed. It downloads configuration updates from the server and implements this configuration. This program is available as a service or as a command line version, too. If you don't want to run a separate program for this task, you can also configure your clients via a registry file that is generated by sbNet. See section 2.2 for more details.

1.1 System Requirements

Before installing the Spybot S&D Update and Configuration Server, make sure your system meets or exceeds the following system requirements:

Supported Operating Systems

- Windows 95/98/Me with installed Windows Installer 2.0[1]
- Windows NT 4.0 Workstation with Service Pack 6 or later
- Windows NT 4.0 Server with Service Pack 6 or later
- Windows 2000 Professional
- Windows 2000 Server
- Windows XP Home
- Windows XP Professional
- Windows XP x64 Edition
- Windows Server 2003
- Windows Vista

On older Windows versions that do not include a current version of Internet Explorer by default, make sure Internet Explorer 5.0 or later is installed.

Minimum hardware requirements

- Free disk space: 100 MB
- When using Windows 95/98/Me: 500 MHz processor, 256 MB RAM
- When using Windows NT 4.0: 500 MHz processor, 256 MB RAM
- When using Windows 2000: 500 MHz processor, 256 MB RAM
- When using Windows XP: 1 GHz processor, 512 MB RAM

[1] Can be downloaded from http://www.microsoft.com/downloads/details.aspx?familyid=cebbacd8-c094-4255-b702-de3bb768148f

- When using Windows Server 2003: 1 GHz processor, 512 MB RAM
- When using Windows Vista: 1 GHz processor, 512 MB RAM

1.2 Operation Scenarios

An individual update solution may match one of the two scenarios described below. Detection rules updates for Spybot Search & Destroy are downloaded from the Internet to a local server by the Spybot S&D Update and Configuration Server in both cases.

1.2.1 Use of the integrated HTTP-server

In this case the software also distributes the updates among the clients via its integrated HTTP-server. This configuration is easy to setup and best suited for smaller networks.

1.2.2 Use of an external server

In this scenario sbNet runs on a machine which also runs an external server software for distributing the updates. This software could be a web server like the 'Apache httpd' or the HTTP-Server that is part of Microsoft's 'Internet Information Services'. You can also just use a shared folder your clients can access via an UNC path[2] to distribute the updates. This operation mode is recommended when the integrated HTTP-server of sbNet is not fast enough to serve all the Spybot S&D clients in a larger network.
You may also run the external server on a second host. In order to achieve this setup you may just configure sbNet to save the downloaded update files to a network share from the other host.

[2] for example: `\\server\spybotupdates\`

2 Installation Instructions

2.1 Server Setup

1. If you did not get an installer with included license files, extract the license files, license.key and license.txt, which you received with the confirmation email.

2. Execute the installer 'sbNet-setup.exe'.

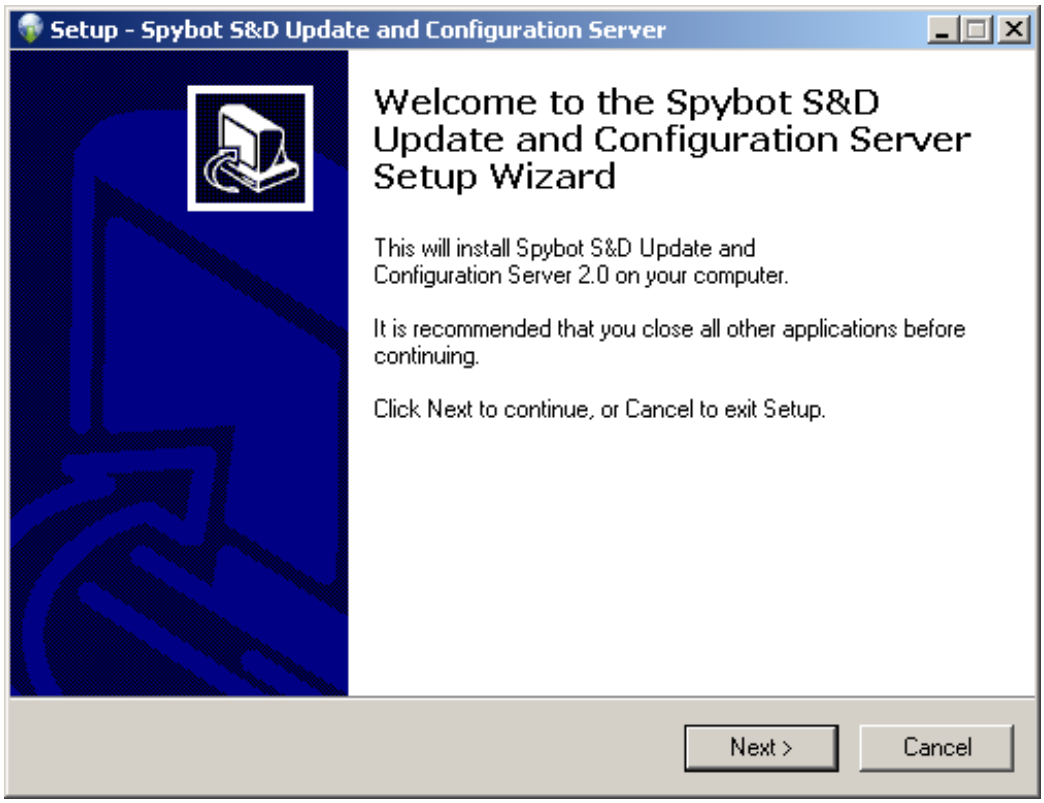


Figure 1: Installation screenshot 1

3. Click on 'Next'.

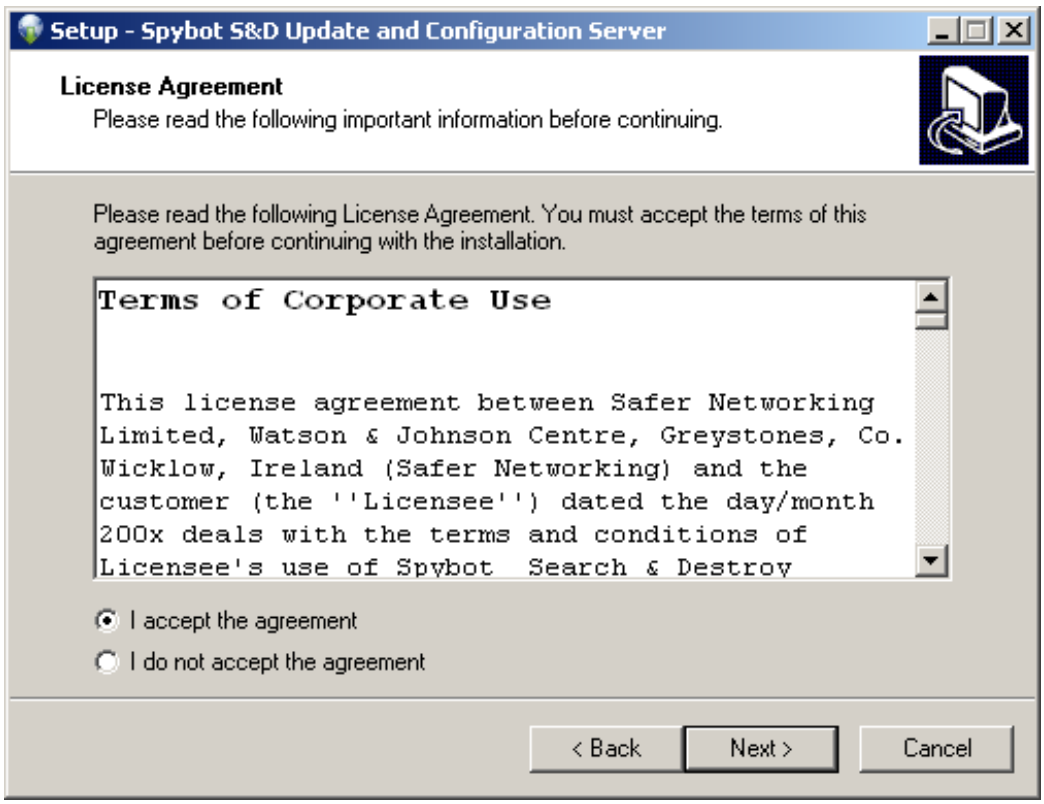


Figure 2: Installation screenshot 2

4. Accept the License Agreement and click on 'Next'.

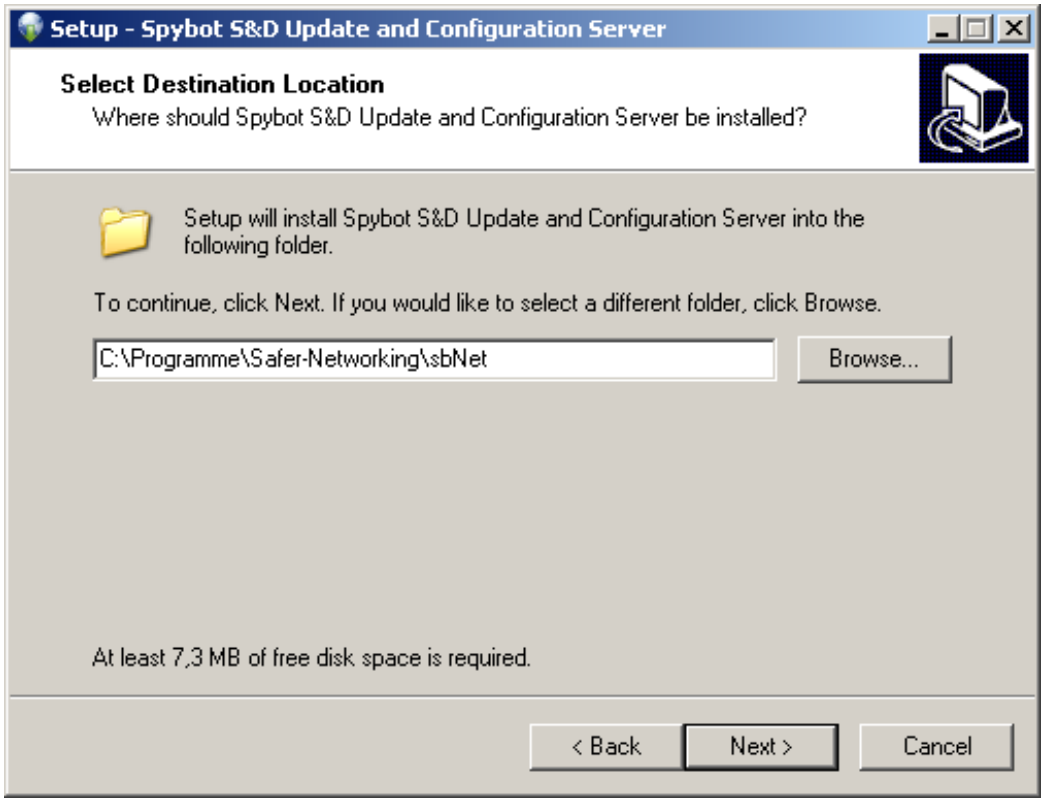


Figure 3: Installation screenshot 3

5. Select the destination location you want to install to.

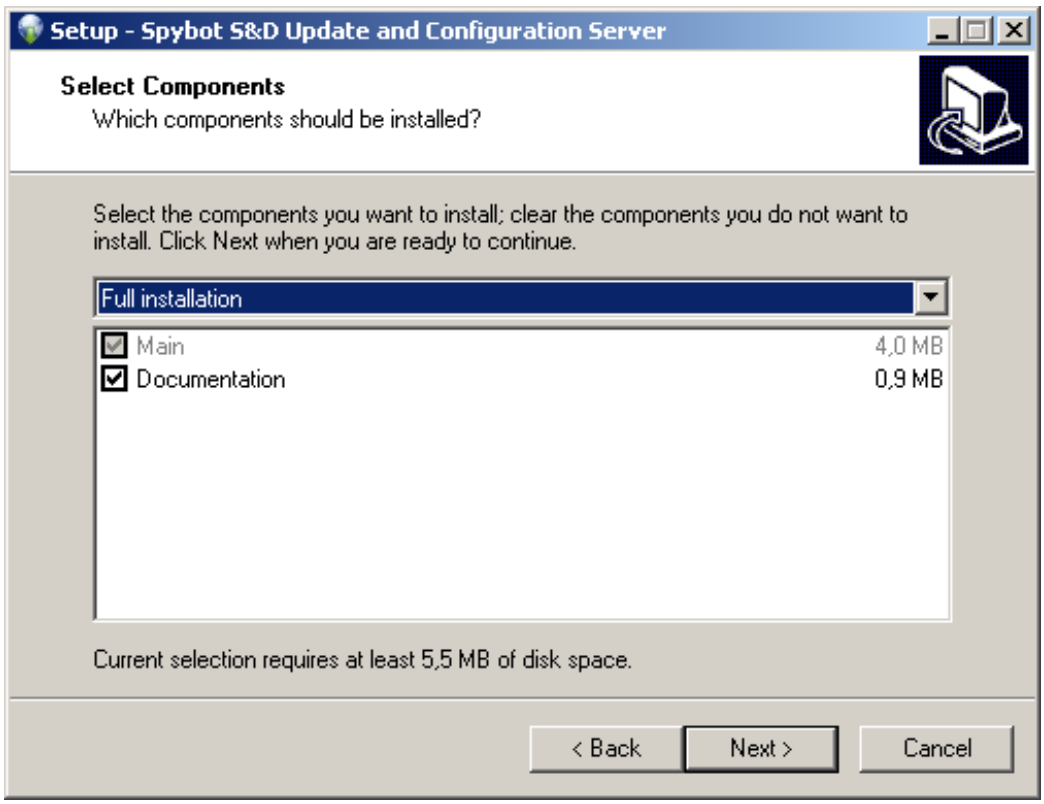


Figure 4: Installation screenshot 4

6. Choose the components you want to install.

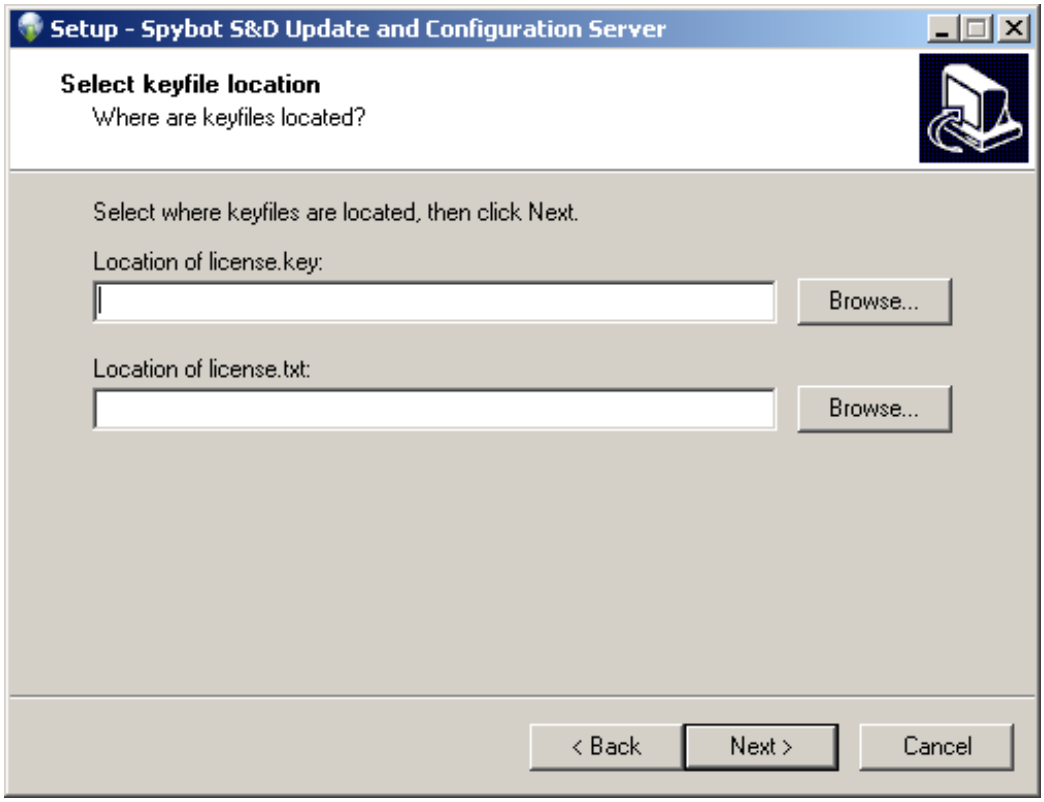


Figure 5: Installation screenshot 5

7. If you did not get an installer with included licensing information, extract the ZIP-Archive with the license and enter the location of the files `license.key` and `license.txt` here. Click on 'Next'. If you got the installer with included licensing information, this page of the installation wizard will not be shown since the correct license files will be installed automatically.

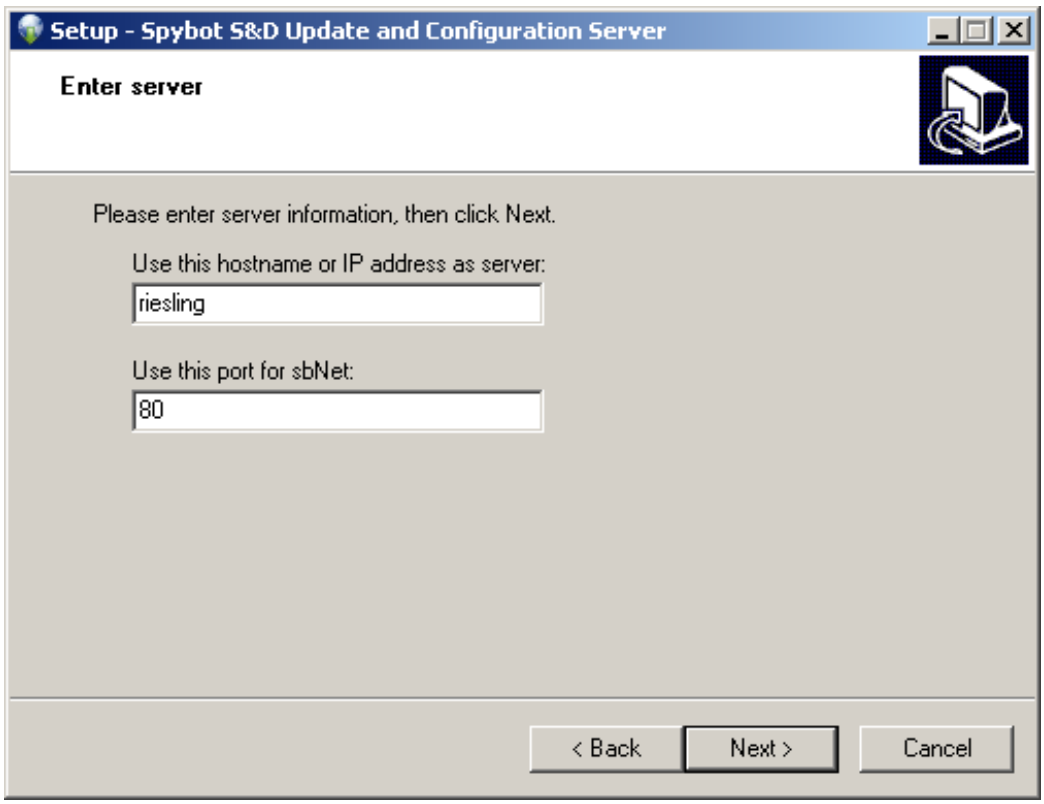


Figure 6: Installation screenshot 6

8. Enter the hostname or IP address of the computer you are installing sbNet on. Enter a port number other than 80, if you need this port for another service on this host, e. g. for a general purpose web server. Click on 'Next'.

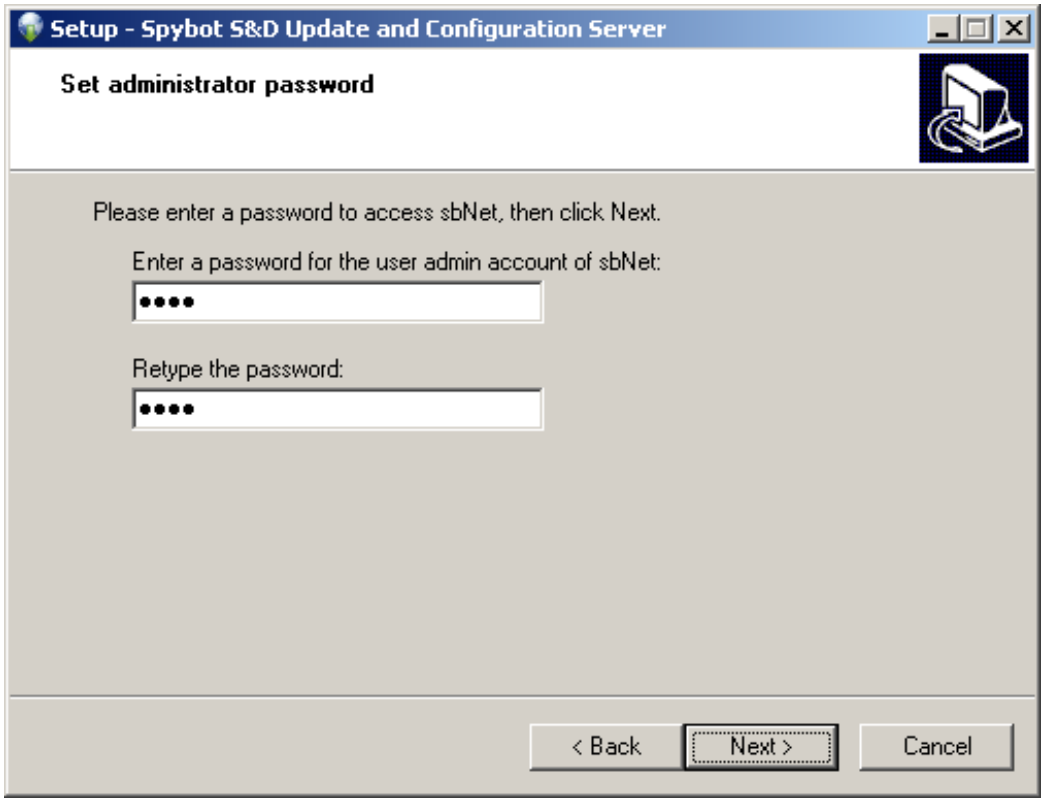


Figure 7: Installation screenshot 7

9. Enter a password for protecting the administrative web interface of sbNet. You need to enter this password and the user name 'admin' when you want to access this interface. Click on 'Next'.

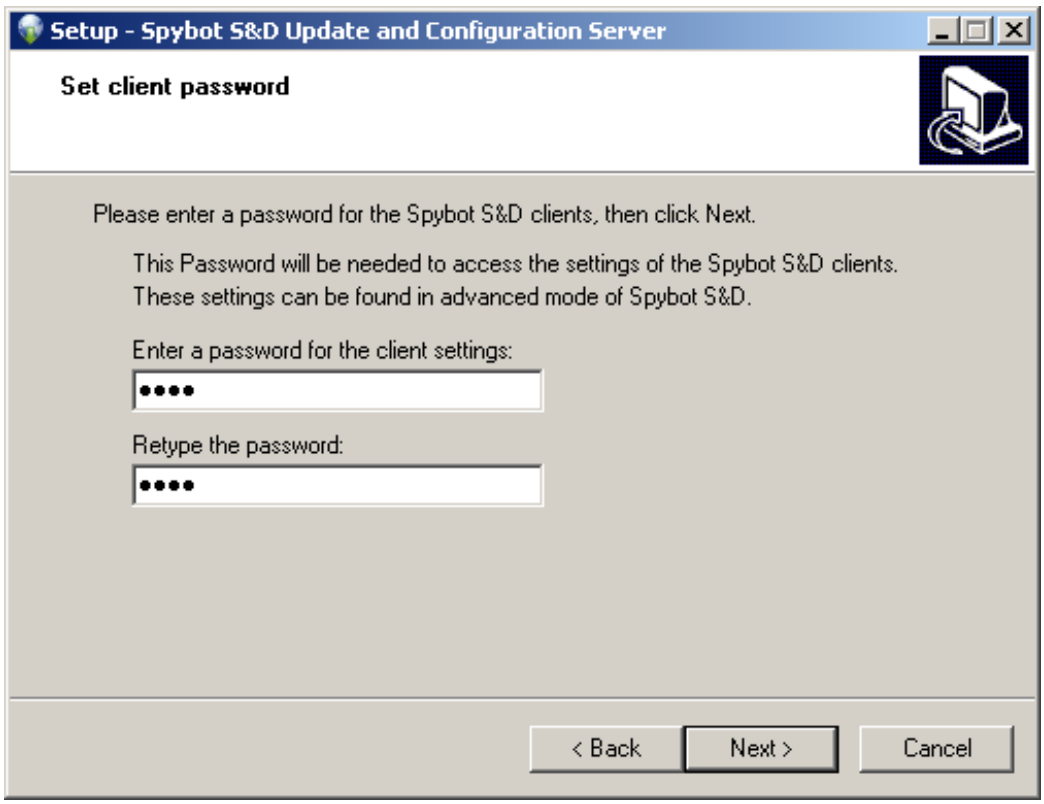


Figure 8: Installation screenshot 8

10. Enter a password for protecting the settings of the Spybot S & D clients in your network. This password will prevent your users from changing the settings by themselves. Click on 'Next'.

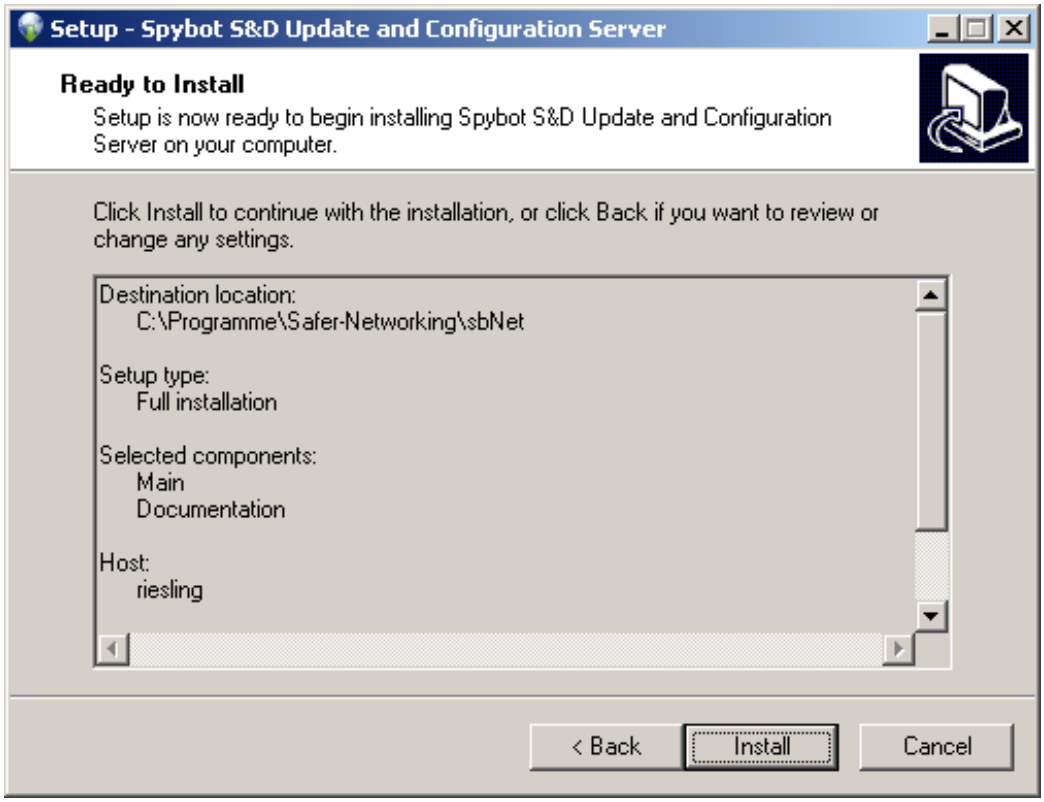


Figure 9: Installation screenshot 9

11. Review the selected installation options and click 'Install' to start the actual installation. You can still cancel the installation by clicking 'Cancel' or change some installation options by going back using the 'Back' button at this point.

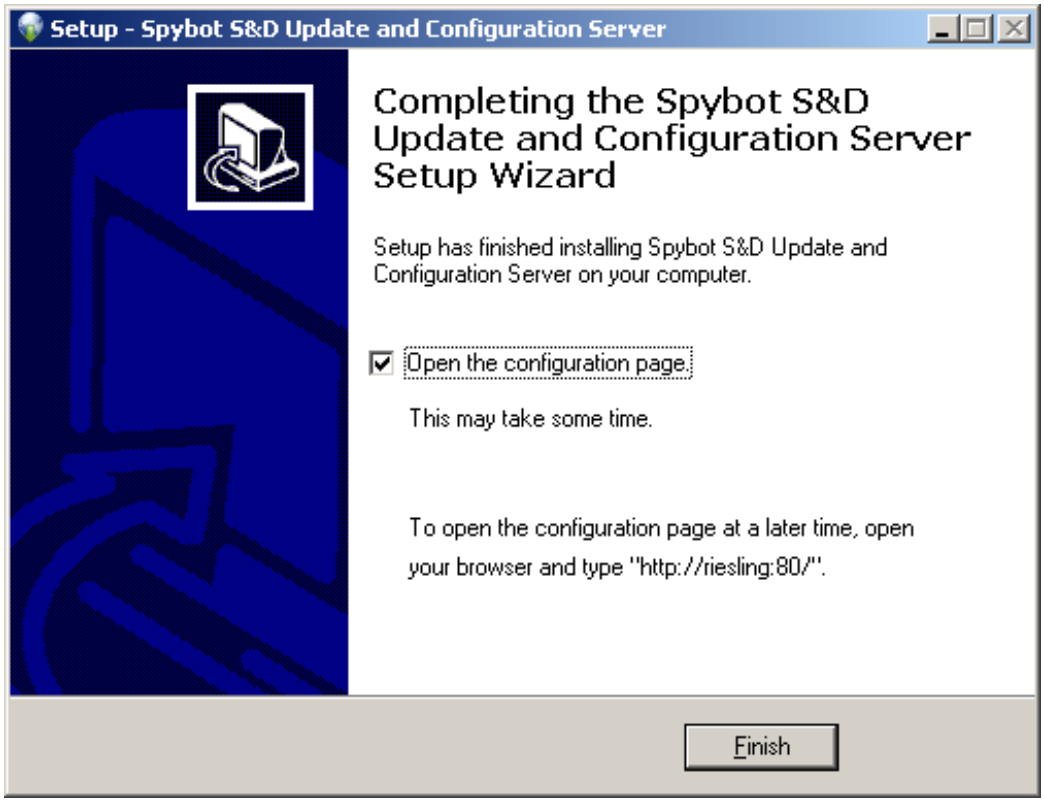


Figure 10: Installation screenshot 10

12. Select 'Open configuration page' and click on 'Finish' in order to start the service 'sbNet' and to display the administrative web interface.

13. When presented with the password prompt of your webbrowser, enter the user name 'admin' and the password you just set during the installation for protecting the administrative web interface of sbNet.

You are now presented with the web interface of sbNet. The next two sections cover how to setup the two operation scenarios mentioned in chapter 1.2.

2.1.1 Setting up a configuration using the integrated HTTP-server

This is the most easy way to setup the Spybot S&D Update and Configuration Server. The result will be the scenario described in section 1.2.1.

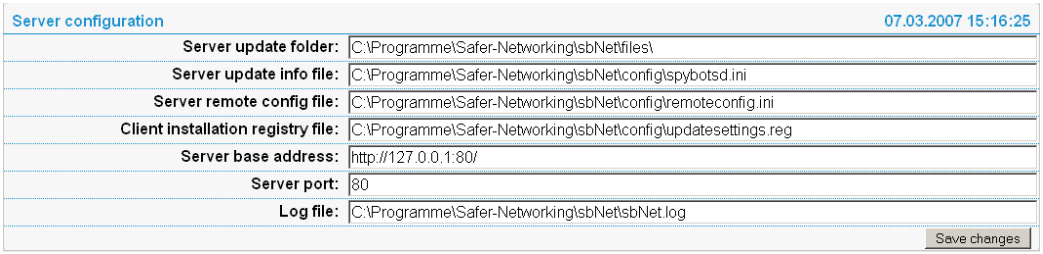


Figure 11: Server configuration page

1. Go to the page 'Server configuration'. You will see a web form like the one shown in figure 11. Enter the base URL the Spybot S&D-clients in your network will use to reach your sbNet installation into the text field 'Server base address'.

   Example: If the host running sbNet has the hostname `spybotserver` and sbNet is listening on port 81, enter `http://spybotserver:81/` into the text field 'Server base address'.

   The port number can be omitted in the text field 'Server base address', if sbNet is listening on the HTTP-standard-port 80.

2. Press the first 'Save changes' button on the page.

3. To activate the configuration, synchronize your sbNet installation with the updates available on the Internet at least once. This will create all files necessary for the clients to download these updates from your intranet host. You can do this either manually using the 'Trigger update synchronization' section on the 'Server configuration' page or by just waiting for the next automatic synchronization.

4. Go to the page 'Client configuration'. You will see a web form like the one shown in figure 12. Update the two text fields 'Update file URI' and 'Config file URI' with the URL chosen above. Leave the file names `spybotsd.ini` and `remoteconfig.ini`intact when doing so. Using the example from above, the URLs will look like following:

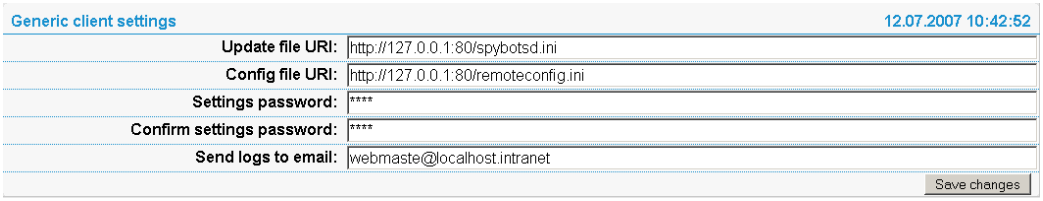


Figure 12: Client URI configuration

- Update file URI: `http://spybotserver:81/spybotsd.ini`
- Config file URI: `http://spybotserver:81/remoteconfig.ini`

5. Press the first 'Save changes' button on the page.

6. Next, configure the clients via one of the three ways described in section 2.2 to make them use your configured Spybot S&D Update and Configuration Server.

2.1.2 Setting up a configuration using an external server

The result will be the scenario described in section 1.2.2. To accomplish this, you need to use an additional server software on the same machine. Either use a web server or a shared folder. In the following we assume that a general purpose web server is listening on port 80 and sbNet is listening on port 81.

1. Create a directory that is accessible from your general purpose web server, e. g. `C:\htdocs\spybot` which is served as `http://spybotserver/spybot/`.

2. Go to the page 'Server configuration'. You will see a web form like the one shown in figure 11. Change the option 'Server update folder' to the folder you just created (`C:\htdocs\spybot\` in the example).

3. Update the settings 'Server update info file' and 'Server remote config file' with the new path, too. In our example the options would read:

   - Server update info file: `C:\htdocs\spybot\spybotsd.ini`
   - Server remote config file: `C:\htdocs\spybot\remoteconfig.ini`

4. Change the option 'Server base address' to the designated URL (`http://spybotserver/spybot/` in our example). Leave the option 'Server port' untouched: this option determines the port of sbNet's *integrated* web server.

5. Press the first 'Save changes' button on the page.

6. Go to the page 'Client configuration'. You will see a web form like the one shown in figure 12. Update the two text fields 'Update file URI' and 'Config file URI' with the URL chosen above. Leave the file names `spybotsd.ini` and `remoteconfig.ini`intact when doing so. Using the example from above, the URLs will look like following:

   - Update file URI: `http://spybotserver/spybot/spybotsd.ini`
   - Config file URI: `http://spybotserver/spybot/remoteconfig.ini`

7. Press the first 'Save changes' button on the page.

8. To activate the configuration, synchronize your Spybot S&D Update and Configuration Server with the updates available on the Internet at least once. This will create all files necessary for the clients to download these updates from your intranet host. You can do this either manually using the 'Trigger update synchronization' section on the 'Server configuration' page or by just waiting for the next automatic synchronization.

9. Next, configure the clients via one of the three ways described in section 2.2 to make them use your configured Spybot S&D Update and Configuration Server.

To use a shared folder instead of a web server to provide the Spybot S&D updates in your intranet, enter the UNC-path of this folder everywhere where we used `http://spybotserver/spybot/` above. So if your server is called `spybotserver` and has a shared folder `spybot` for distributing the updates, the options should read:

- Server base address: `\\spybotserver\spybot\`
- Update file URI: `\\spybotserver\spybot\spybotsd.ini`

- Config file URI: \\spybotserver\spybot\remoteconfig.ini

If you want Spybot S&D Update and Configuration Server to write the downloaded updates and other files to a shared folder on another host, you also have to make sure the process or service has sufficient write permissions for this share. To achieve this for the service, you probably need to change the user sbNet is running under.

2.2 Client Setup

The clients receive their settings from the sbNet server. This can be done by the SBCC or the file `upsatesettings.reg`.
The SBCC and `updatesetting.reg` file are updated during the install process of the sbNet server. Later they will be updated when changed settings for 'Update file URI' and 'Config file URI' are saved.

2.2.1 SBCC

The SBCC retrieves the file `remoteconfig.ini` which contains the command line parameters for the autostart, for the scheduler and parameters for Spybot S&D's settings. All of these settings can be edited in the 'Client configuration' and 'Client settings' pages of sbNet.
There are two versions of the SBCC:

`SBCCSRV.exe` This version will install a service. The service polls the central `remoteconfig.ini` from the server and then deploys the new configuration on the client. The poll interval can be configured in the 'Server configuration', see section 3.3 for details.

`SBCCSCL.exe` This is just a normal executable application. After the first execution, `SBCCSCL.exe` adds entries to the registry so it will run immediately at every system start from then on. With each run it pulls the central `remoteconfig.ini` from the server. Then it deploys the new configuration on the client.

2.2.2 `updatesettings.reg`

The registry file `updatesettings.reg` contains the following Spybot S&D configuration options:

- The 'Update file URI'
- The 'Config file URI'
- The 'Settings password'
- Email address for the client's log files
- The complete 'Client mail settings'

When using sbNet on a Windows 95/98/Me server, only `updatesettings.reg` can be used.

2.2.3 Automated install using SBCC

For the client setup you need a Spybot S&D Corporate Edition installer. During the installation you are asked for the following information:

1. The IP or hostname of the server sbNet is running on.
2. The port number of the sbNet service.

For an installation via command line there are the following additional parameters available:

SBNETIP=[Server] Specifies the server sbNet is running on. Possible values are the IP address or the hostname are of the server.

SBNETPORT=[Port] Specifies the port number the sbNet service is accessible on. This parameter is only needed in case it differs from its default value 80.

SBCCINSTALLTYPE=[Installtype] Specifys the type of sbcc used on your clients. You can choose between the following values:

- 1: SBCCSRV.exe will be installed.
- 2: SBCCSCL.exe will be executed.

The default value is 1.

Examples:

```
msiexec /i spybotsd163corped.msi SBNETIP=192.168.0.1

msiexec /i spybotsd163corped.msi SBNETIP=192.168.0.1
          SBNETPORT=8080 SBCCINSTALLTYPE=2
```

[2]Except Windows 95/98/Me, since for these Windows versions the SBCC service is not available.

2.2.4 Manual installation using SBCC

Using `SBCCSRV.exe`

1. On the sbNet server, save the URL of the update server in 'Client configuration'.
2. Install Spybot S&D on the clients if this was not already done previously.
3. Copy the file `SBCCSRV.exe` to your clients.
4. Install the service on the client computers with the command line parameter `/install` with the 'Run' menu item in Windows 'Start' menu. E. g.:

   ```
   "C:\Program Files\Spybot - Search & Destroy\SBCCSRV.exe" /install
   ```

5. Start the service entering the command `net start sbcc` into the Windows 'Run' dialog.

Using `SBCCSCL.exe` On the server, save the URL of the update server in 'Client configuration' first. Then execute this file on the client after installing Spybot S&D if you don't want to use the service `SBCC`. Be sure to execute this as an user with administrator rights on the client machine.

Installation using `updatesettings.reg` You may include this registry file at every single system to define individual parameters or generate one file at the admin's PC and install it on all systems via a batch file. An example of an automatic client installation would be a batch like:

```
REM If Spybot S\&D is already installed, do nothing.
IF EXIST %PROGRAMFILES%\Spybot~1\spybotsd.exe EXIT

REM Install Spybot S&D silently
msiexec /i spybotsd163corped.msi /verysilent

REM Merge registry settings so Spybot~S\&D downloads
REM updates from your installation of sbNet.
regedit /s updatesettings.reg
```

For command line options of the Spybot S&D installer see help menu at the client program.
Be sure to execute this as a user with administrator rights on the local machine. Merging the created registry file from the server is necessary to notify the Spybot S&D installations about a change of the settings listed in section 2.2.2.

3 Web Interface

3.1 Status

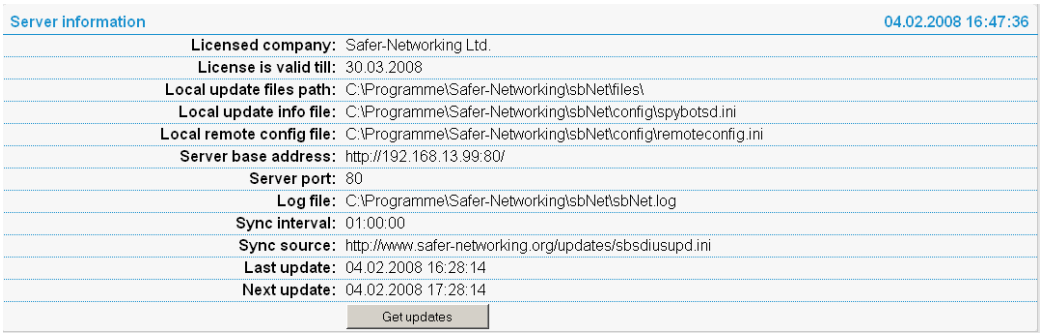


Figure 13: Status screen of sbNet

The status page displays information about the current configuration of sbNet.
Via the 'Get Updates' button you can look manually for new updates at any time.

3.2 Updates

Available updates 07.03.2007 15:14:11

Update	Description	Date	Status
Advanced detection library 1.5.1	!Advanced detection routines update (293 KB)	2007-01-16	
Afrikaans language	Afrikaans (21 KB)	2007-02-14	
Arabian language	Arabic (24 KB)	2007-02-14	
Belarusskiy language	Belarusskiy (26 KB)	2007-02-28	
Brasil (portuguese) help	Brasil (139 KB)	2004-08-20	
Brasil (portuguese) help for TeaTimer	Brasil (32 KB)	2004-08-20	
Brasil (portuguese) language	Brasil (24 KB)	2007-02-14	
Bulgarian language	Bulgarski (28 KB)	2007-02-14	
Catala language	Catalan language file (26 KB)	2007-02-14	
Cesky help for TeaTimer	Cesky (34 KB)	2005-04-27	
Cesky language	Czech language file (25 KB)	2007-02-14	
Cesky license	Czech license file	2004-05-25	
Chinese (simplified) help	Chinese help (263 KB)	2005-06-02	
Chinese (simplified) language	Chinese (23 KB)	2007-02-14	
Chinese (traditional) language	Chinese (25 KB)	2007-02-14	
Dansk language	Danish language file (27 KB)	2007-02-14	
Detection rules (beta)	Updated detections (13 KB)	2007-03-07	
Detection rules: Dialers	!Updated base dialer detections (115 KB)	2006-12-08	
Detection rules: Hijackers	!Updated base hijacker detections (148 KB)	2007-02-07	
Detection rules: Keyloggers	!Updated base keylogger detections (20 KB)	2006-10-27	
Detection rules: Malware	!Updated base malware detections (233 KB)	2007-02-14	
Detection rules: PUPS	!Updated base possibly unpopular software detections (79 KB)	2007-01-19	
Detection rules: Security	!Updated base security exploit detections (8 KB)	2006-12-08	
Detection rules: Spybots	!Updated base spyware & adware detections (108 KB)	2007-02-02	
Detection rules: Trojans	!Updated base trojan horse detections (181 KB)	2007-03-07	
Detection rules: Update	!Most up-to-date detections (389 KB)	2007-03-07	

Figure 14: Updates page

The Updates page displays a list of updates managed by sbNet.

3.3 Server configuration

Here you can define the paths for the download folder, where to store the configuration files and the log file. After the first start the server will create default folders and files in the same folder where you executed sbNet.

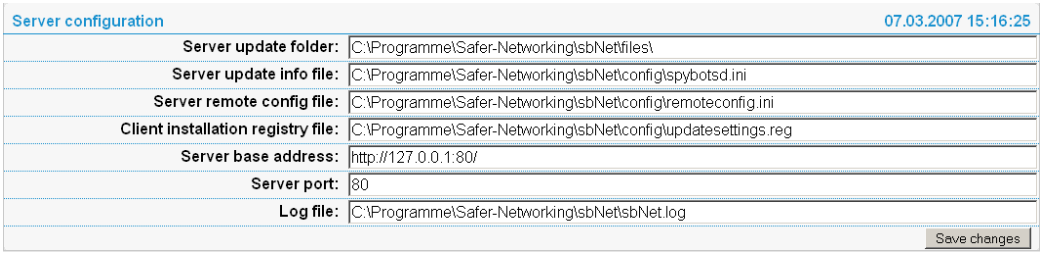


Figure 15: Server configuration page

The following paths can be edited:

1. Server update folder
2. Server update info file
3. Server remote config file
4. Client installation registry file
5. Log file

Furthermore you can define the 'Server base address' and the port on which the server should listen. The default port sbNet uses is 80. If you want to change it, then only use a port which is not used or reserved for other software. Remember to update the 'Update file URI' and the 'Config file URI' when you are using the integrated webserver of sbNet and you change the 'Server base address' or the port.

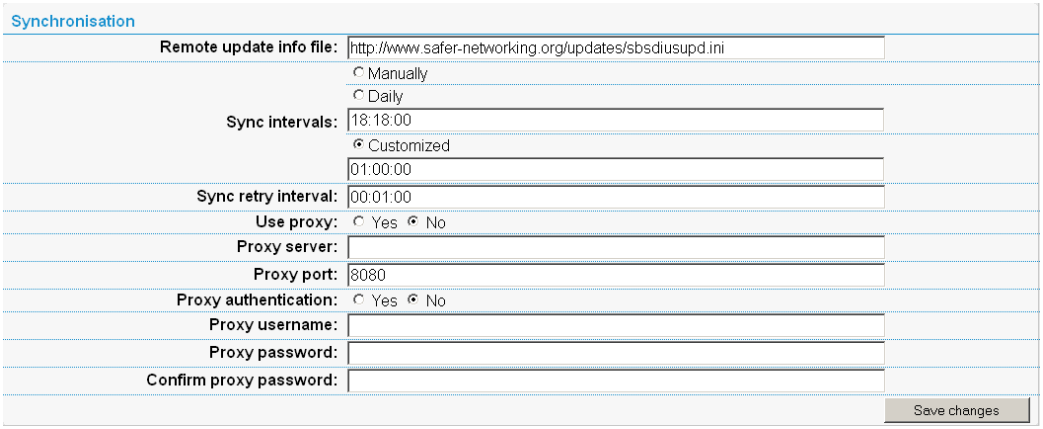


Figure 16: Synchronisation

Remote update info file

Location of the original update info file. Do not change it without a good reason.

Sync interval and Sync retry interval

The interval for the synchronisation with the Safer-Networking Server can be entered here.
Possible options are:

Manually Only look for new updates when the 'Get Updates' button on the Status page is pressed (see section 3.1).

Daily Look for updates once a day at the given time. Enter the time in the 24h format hh:mm:ss.

Customized Valid custom synchronisation intervals are from 01:00:00 (one hour) to 23:59:59 (23 hours, 59 minutes and 59 seconds).

Valid sync retry intervals are from 0:01:00 (one minute) to 23:59:59 (23 hours, 59 minutes and 59 seconds).

Proxy

Following configurations are available if you want to use a proxy for connecting to the Safer-Networking Server:

1. Use proxy
2. Proxy server
3. Proxy port
4. Proxy authentication
5. Proxy username
6. Proxy password
7. Confirm proxy password

Only lower case characters are supported for the username. The @ character is not supported.
Enter the password a second time into the 'Confirm proxy password' text field to avoid typing errors.

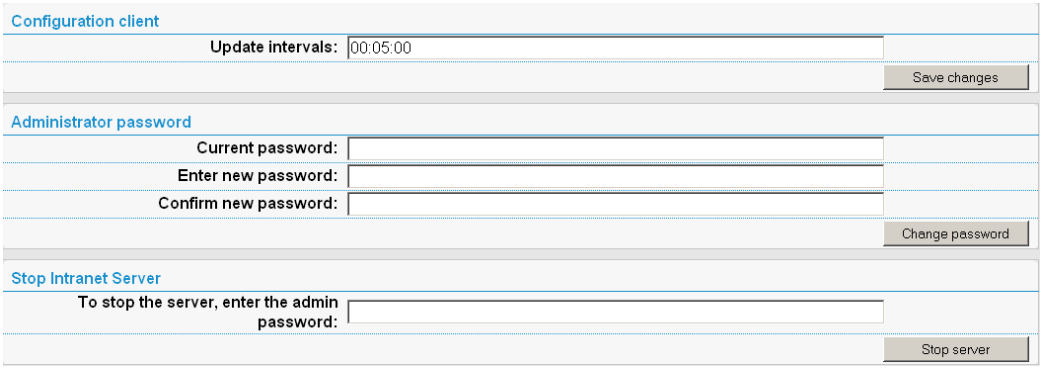


Figure 17: Server configuration page bottom

Update intervals

Configure how often the Spybot Configuration Client (SBCC, see section 2.2) polls sbNet for the configuration file `remoteconfig.ini`. Enter a time in format hh:mm:ss into this textfield.

Administrator password

Enter a new password here if you would like to change the default password. The default username and default password for entering the web interface are:

```
username: admin
password: deichgrab
```

It is recommended to change the default password as soon as possible.

Stop Spybot S&D Update and Configuration Server

To stop the server, enter the admin password and press the 'Stop server' button.

3.4 Client configuration

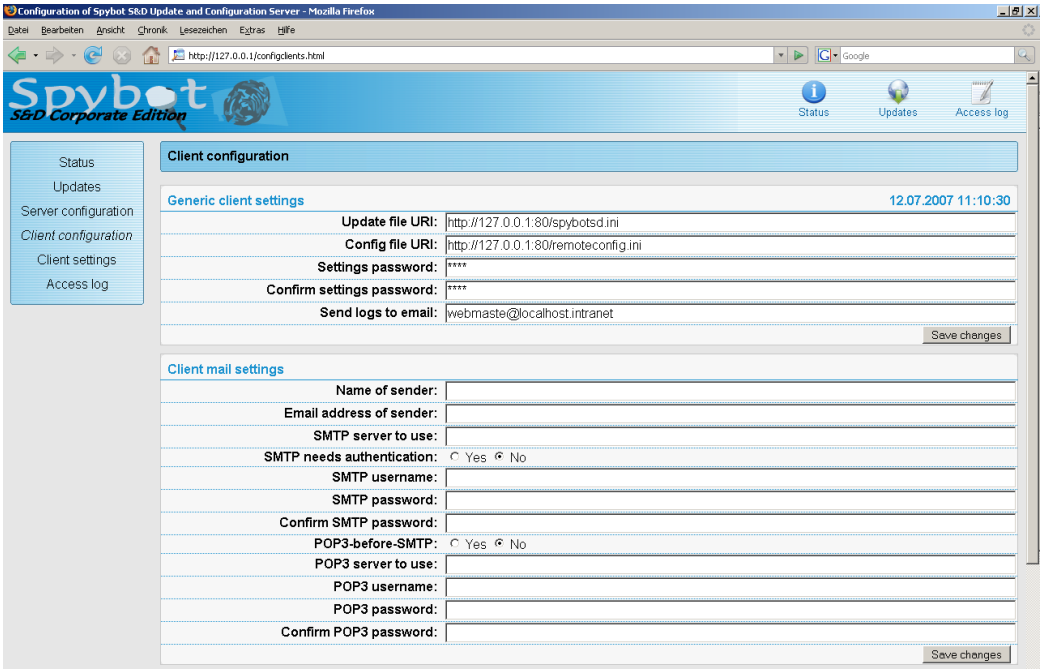


Figure 18: Client configuration page

3.4.1 Generic client settings

This section on the configuration web page offers basic settings that enable the Spybot S&D clients to communicate with sbNet.

Update file URI: Enter the URI of the update file (`spybotsd.ini`) served by your sbNet installation. See section 2.1.1 and section 2.1.2 for examples.

Config file URI: Enter the location of the remote configuration file served by your sbNet installation (`remoteconfig.ini`). See section 2.1.1 and section 2.1.2 for examples.

Settings password: Enter a password so that the users on the client PCs cannot change the settings in Spybot S&D. When left blank, the users can change the settings that are received from sbNet.

Confirm settings password: Enter the same password again here to avoid typing errors.

Send logs to email: Enter an email address for receiving copies of the log files from the clients into this text field. Spybot S&D will either use the default installed and configured email client or directly speak to the configured SMTP server, depending on the 'Mailer application' setting on the 'Client settings' page.

These settings are stored in the executables of the Spybot S&D Client Configurator (`SBCCSRV.exe` and `SBCCSCL.exe`) and in the file `updatesettings.reg`. If you change these settings after the initial deployment of the Spybot S&D Client Configurator, you need to deploy it again. Note that you need to uninstall the SBCCSRV service with the parameter `/uninstall` before you can install the updated service again (compare section 2.2.4).

3.4.2 Client mail settings

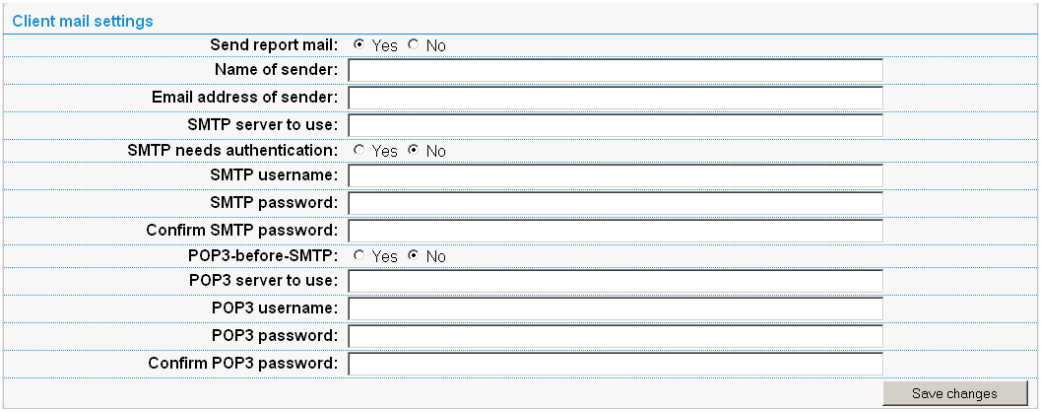


Figure 19: Client mail settings

If the Spybot S&D client should use the SMTP protocol for sending reports, you can define the necessary settings in 'Client mail settings'.

Send report mail: Set to 'Yes' to instruct the Spybot S&D clients to send report emails to the address configured below.

Name of sender: The sender name Spybot S&D should use for the emails.

Email address of sender: The sender address Spybot S&D should use for the emails it sends. Make sure to use an email address the SMTP server allows as a sender. In doubt, consult your mail server administrator.

SMTP server to use: The host name or IP address of your SMTP server.

SMTP needs authentication: Enable if your SMTP server requires an username and password as an authentification for sending mails. Enter these authentification details into the text fields 'SMTP username' and 'SMTP password' below. Enter the password a second time into the 'Confirm SMTP password' text field to avoid typing errors.

POP3 before SMTP: Activate this feature when your mail server requires to successfully perform a POP3 logon before being allowed to send emails via SMTP. Specify the IP address or hostname, the username and the password with the text fields 'POP3 server to use', 'POP3 username' and 'POP3 password'. Enter the password a second time into the 'Confirm POP3 password' text field to avoid typing errors.

3.4.3 Client autostart

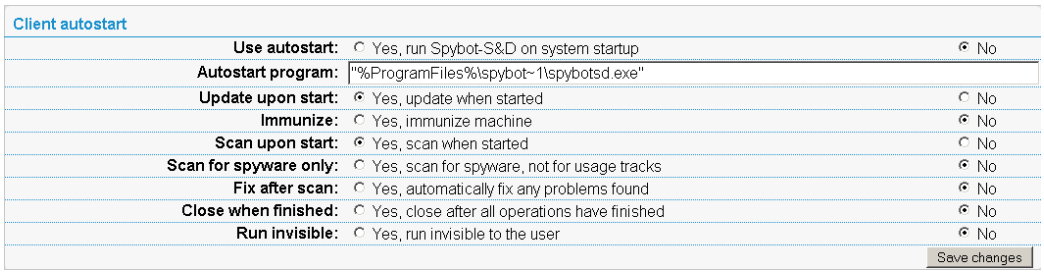


Figure 20: Client autostart

Using the autostart function you can make Spybot S&D run automatically on the client machines when a user logs in doing the tasks activated here. Activate the radio button 'Yes, run Spybot-S&D on system startup' in order to enable this feature.
The following options are available:

Use autostart: Activate starting Spybot S&D on login.

Autostart program: Text field for entering the Spybot S&D's program path.

Update upon start: Download available updates upon program start.

Immunize: Immunize the client machine.

Scan upon start: Scan all selected file sets.

Scan for spyware only: Scan only spyware entries (red entries), ignore all usage tracks.

Fix after scan: Fix all found problems automatically.

Close when finished: Automatically shutdown Spybot S&D when all tasks have been finished.

Run invisible: Do not display Spybot S&D's user interface.

3.4.4 Client scheduler

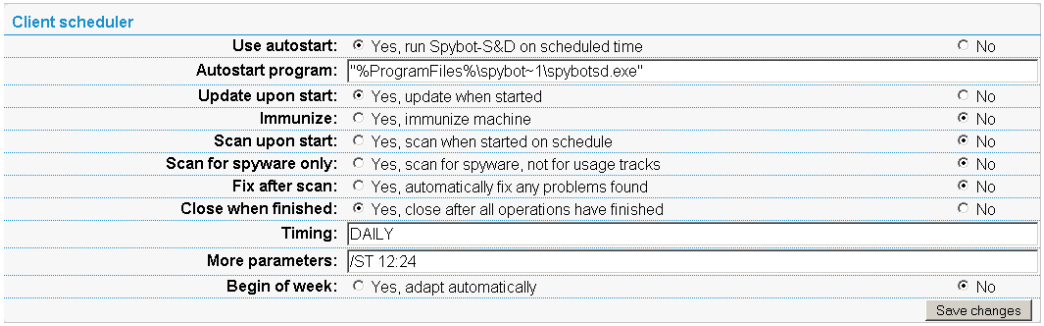


Figure 21: Client scheduler

Using a Microsoft Windows Scheduled Task for Spybot S&D is also possible. The following options are available:

Use autostart: Activate a scheduled task for Spybot S&D.

Autostart program: Text field for entering the Spybot S&D's program path.

Update upon start: Download available updates upon program start.

Immunize: Immunize the client machine.

Scan upon start: Scan all selected file sets.

Scan for spyware only: Scan only spyware entries (red entries), ignore all usage tracks.

Fix after scan: Fix all found problems automatically.

Close when finished: Automatically shutdown Spybot S&D when all tasks have been finished.

Timing: Text field for entering timing schemes. Following types are defined:

- MONTHLY
- WEEKLY
- DAILY

- ONIDLE
- ONLOGON
- ONSTART
- ONCE

More parameters: Text field for entering command parameters for the task. The following parameters can be appended.

/SD Specifies the date the task starts in the format DD/MM/YYYY. The default value is the current date. The /SD parameter is valid with all schedules, and is required for a ONCE schedule.

/ST Specifies the time of day that the task starts in the 24-hour format HH:MM. The default value is the current local time when the command completes. The /ST parameter is valid with DAILY, WEEKLY, MONTHLY, and ONCE schedules. It is required with a ONCE schedule.

/MO Specifies a modifier for how often the task runs within its schedule type. This parameter is valid, but optional, for a DAILY, WEEKLY or MONTHLY schedule. The default value is 1. Note that this modifier has a slight different meaning for the schedule type MONTHLY than for the schedule type DAILY and WEEKLY.

Values for DAILY: 1–365 (a value of 3 means every third day)

Values for WEEKLY: 1–52 (a value of 2 means every second week)

Values for MONTHLY: 1–12 (a value of 5 creates a task for May and October)

Special values: FIRST, SECOND, THIRD, FOURTH, LAST (use these values together with /D to run a task on the first, second, ... week of a month, e.g. on the fourth saturday of a month)

/D Specifies a day of the week or a day of a month. Valid only with a WEEKLY or MONTHLY schedule.

Values for WEEKLY: MON, TUE, WED, THU, FRI, SAT, SUN and * (every day).

Values for MONTHLY: A value of MON–SUN is required when the FIRST, SECOND, THIRD, FOURTH, or LAST modifier for /MO is used. A value of 1–31 is valid only with no modifier or a

modifier of the 1–12 type. The default value is 1 (the first day of the month).

/M Specifies the month or the year, only valid for MONTHLY schedules.

Valid values: JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, DEC and * (every month).

/I Specifies how many minutes the computer should be idle before the task starts. Type a whole number from 1 to 999. This parameter is valid only with an ONIDLE schedule, and then it is required.

Examples for valid tasks:

```
Timing for Scheduler type: ONIDLE
More parameters: /I 10
Start task when computer was idle for ten minutes.

Timing for Scheduler type: DAILY
More parameters: /ST 12:30
Start task at 12:30 every day.

Timing for Scheduler type: DAILY
More parameters: /ST 12:30 /MO 2
Start task at 12:30 on every second day.

Timing for Scheduler type: WEEKLY
More parameters: /ST 12:30 /MO 12 /D WED
Start task every 12th week on Wednesday at 12:30.

Timing for Scheduler type: MONTHLY
More parameters: /D 27 /MO 11 /ST 12:30
Start task once a year on the 27th of November at 12:30.

Timing for Scheduler type: MONTHLY
More parameters: /ST 12:30 /MO 2 /M APR /D FRI
Start task on the second Friday of April at 12:30.
```

Begin of week: Adapt this setting, if Monday is not the first day of the week in your country.

3.5 Client settings

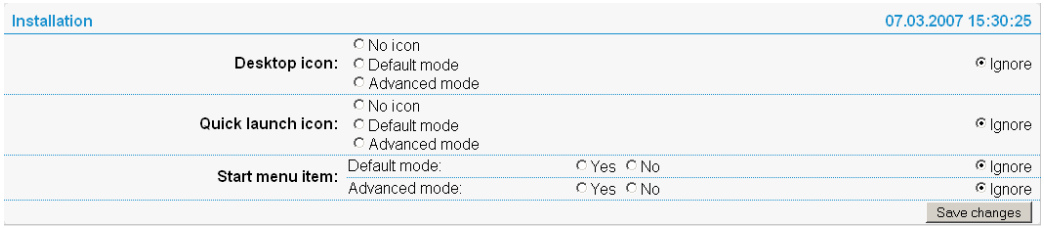


Figure 22: Client settings page

The client settings page offers central options for the Spybot S&D software. Select the 'Ignore' radio button if you don't want to use the specific setting. The following settings can be edited:

Installation

Desktop icon:

- No desktop icon
- Desktop icon for starting in default mode
- Desktop icon for starting in advanced mode

Quick launch icon:

- No quick launch icon
- Quick launch icon for starting in default mode
- Quick launch icon for starting in advanced mode

Start menu item:

- Start menu item for starting in default mode
- Start menu item for starting in advanced mode

Main settings

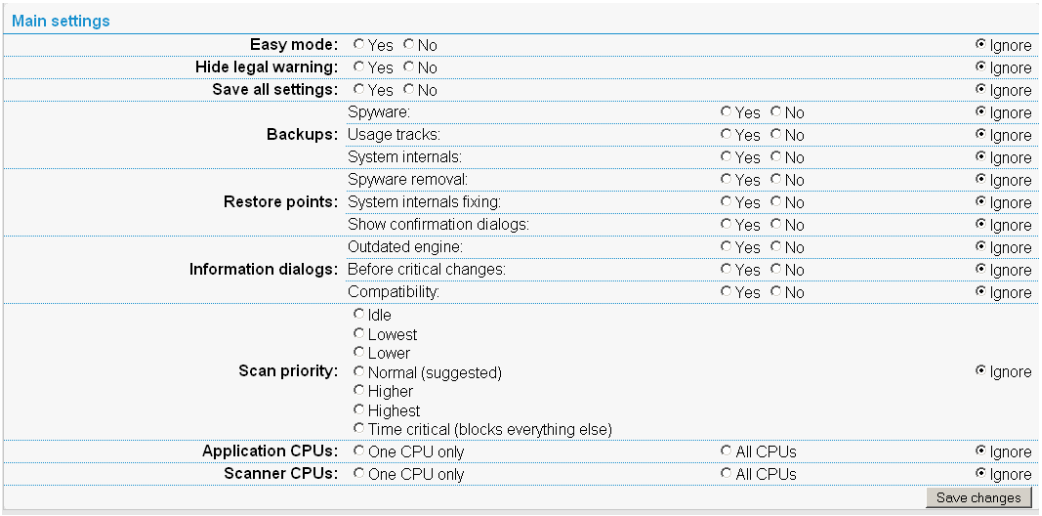


Figure 23: Main settings

Easy mode: Run Spybot S&D in easy mode.

Hide legal warning: Do not show legal warning message.

Save all settings: Save settings when closing Spybot S&D.

Backups:

Spyware: Create backups for spyware.

Usage tracks: Create backups for usage tracks.

System internals: Create backups for system internals.

Restore points:

Spyware removal: Create system restore points when removing spyware.

System internals fixing: Create system restore points when fixing system internals.

Show confirmation dialogs: Display confirmation dialogs when creating system restore points.

Information dialogs:

Outdated engine: Display warning for outdated engine.

Before critical changes: Display confirmation dialog for critical changes.

Compatibility: Display compatibility warnings.

Scan priority: Set the Windows process priority for the Spybot S&D scan. Following priorities can be chosen:

- Idle
- Lowest
- Lower
- Normal (suggested)
- Higher
- Highest
- Time critical (blocks everything else)

Application CPUs: Use one CPU only or use all CPUs for the Spybot S&D application.

Scanner CPUs: Use one CPU only or use all CPUs for the scan.

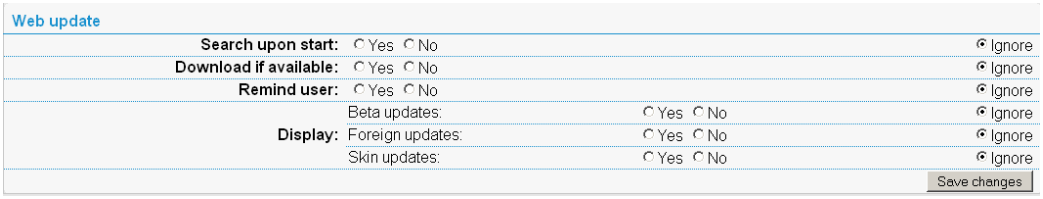


Figure 24: Web update

Web update

Search upon start: Search for updates when running Spybot S&D.

Download if available: Download updates if new updates are available.

Remind user: Remind the user to update Spybot S&D.

Display: Configure which types of updates should be displayed.

Beta updates: Display available beta updates.

Foreign updates: Display foreign language updates.

Skin updates: Display available skin updates.

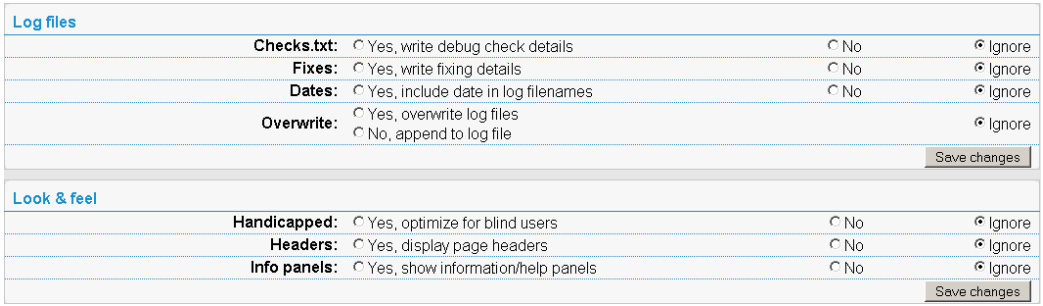


Figure 25: Log files and Look & feel

Log files

Checks.txt: Create log file for detected threats.

Fixes: Create log file for fixed threats.

Dates: Append the date in the log file name.

Overwrite: Overwrite or append to old log files.

Look & feel

Handicapped: Use interface optimized for blind users.

Headers: Display information header.

Info panels: Highlight information panel.

Report settings

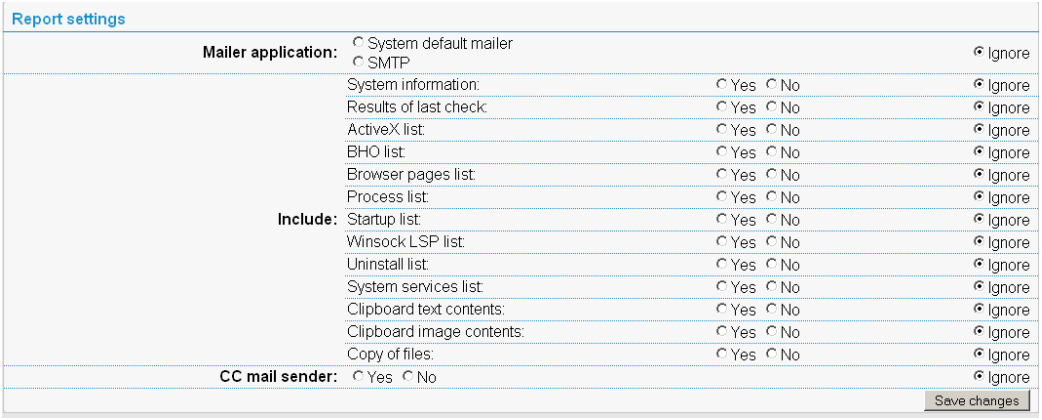


Figure 26: Report Settings

Mailer application: Select 'System default mailer' for using the default email client or select 'SMTP' for using the Simple Mail Transfer Protocol for sending the bug report.

Include: Select the data and files to be sent with your bug report.

System Information: Include system internal information in the bug report.

Results of last check: Include result list in the bug report.

ActiveX list: Include ActiveX list.

BHO list: Include Browser Helper Object list.

Browser pages list: Include default browser pages list.

Process list: Include process list.

Startup list: Include system startups list.

Winsock LSP list: Include Winsock LSP List.

Uninstall list: Include uninstall list.

System Services list: Include services list.

Clipboard text contents: Include clipboard text.

Clipboard image contents: Include clipboard image.

Copy of files: Include spy files.

CC mail sender: Send a carbon copy to the sender of the bug report mail.

Choose 'Yes' for attaching the respective data and 'No' for not doing so, choose 'Ignore' for using the individual client settings.

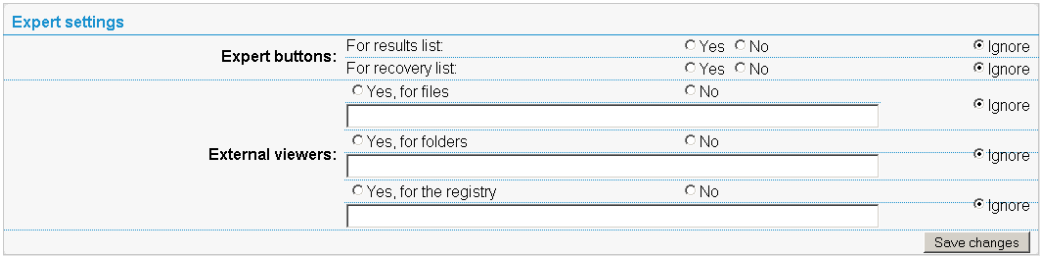


Figure 27: Expert settings

Expert settings

Expert buttons:

For results list: Display advanced result screen buttons.

For recovery list: Display advanced recovery screen buttons.

External viewers:

for files Use external file viewer.

for folders Use external folder viewer.

for the registry Use external registry viewer.

Choose 'Yes' for using the feature, 'No' for deactivating the feature or 'Ignore' for using individual client settings. If you choose 'Yes' for the external viewer then also manually add the path of the external viewer in the provided text field.

3.6 Client log

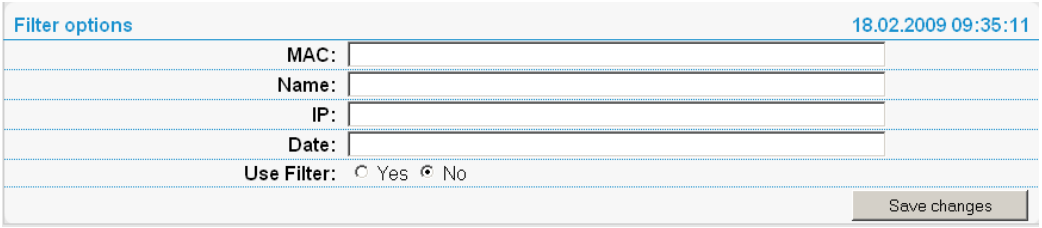


Figure 28: The filter options for the client log

Log of requesting clients — 15 clients

MAC	Name	IP	Date
00-0C-29-B7-75-8F	VMPHILIPP	192.168.13.79	18.02.2009 09:32:58
00-0C-29-A7-51-4F	VM14	192.168.14.14	17.02.2009 17:12:41
00-0C-29-B7-32-8F	VM13	192.168.14.13	17.02.2009 17:10:41
00-0C-29-B7-18-2F	VM12	192.168.14.12	17.02.2009 17:09:41
00-0C-29-B7-19-8F	VM11	192.168.14.11	17.02.2009 16:57:41
00-0C-29-B7-45-8F	VM10	192.168.14.10	17.02.2009 16:54:41
00-0C-29-C7-44-8F	VMP9	192.168.14.9	17.02.2009 16:12:21
00-0C-29-B7-55-2E	VM8	192.168.14.8	17.02.2009 16:14:40
00-0C-29-B7-45-8E	VM7	192.168.14.7	17.02.2009 16:13:12
00-0C-29-B7-15-8F	VM6	192.168.14.6	17.02.2009 16:12:36
00-0C-29-B7-35-8F	VM5	192.168.14.5	17.02.2009 16:02:42
00-0C-29-B7-52-8F	VM4	192.168.14.4	17.02.2009 14:16:38
00-0C-29-B7-23-3F	VM3	192.168.14.3	17.02.2009 14:15:33
00-0C-29-C7-27-8F	VM2	192.168.14.2	17.02.2009 11:14:11
00-0C-29-B7-28-7F	VM1	192.168.14.1	17.02.2009 10:12:43

Figure 29: The Client log

This page shows the client log of sbNet. You may filter the log by different criteria:

MAC: Only show accesses from a certain MAC address (hardware address of the network interface card).

Name: Only show accesses from hosts with the given hostname.

IP: Only show accesses from a certain IP address.

Date: Only show accesses from a certain date. The format is localised and the same as the date displayed in the blue section titles.

You can enable or disable the configured filter options at once with the 'Use Filter' option.

3.7 Access log

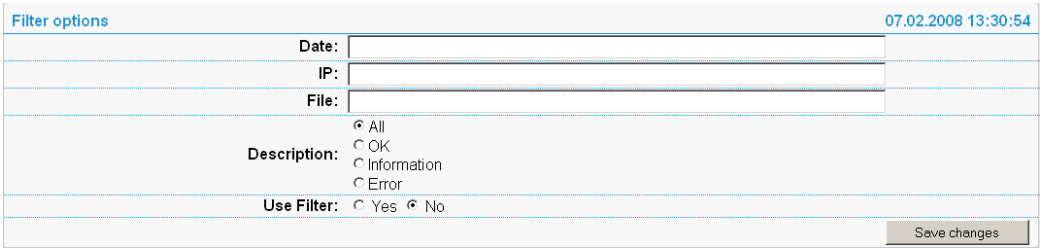
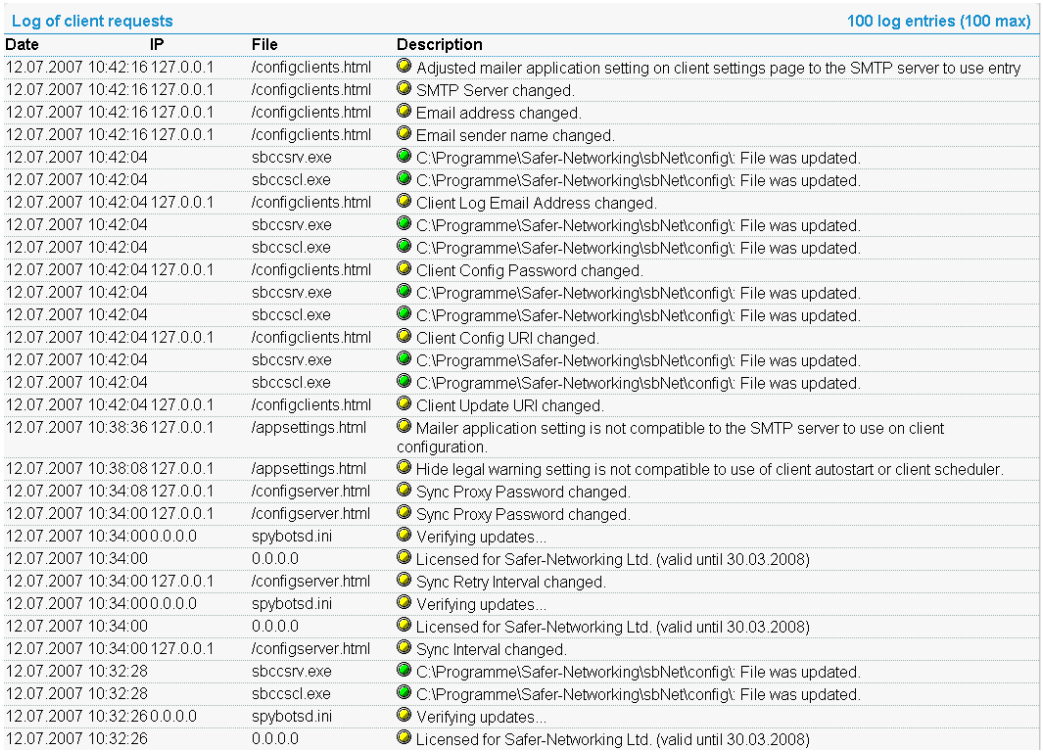


Figure 30: The filter options for the access log



Log of client requests — 100 log entries (100 max)

Date	IP	File	Description
12.07.2007 10:42:16	127.0.0.1	/configclients.html	Adjusted mailer application setting on client settings page to the SMTP server to use entry
12.07.2007 10:42:16	127.0.0.1	/configclients.html	SMTP Server changed.
12.07.2007 10:42:16	127.0.0.1	/configclients.html	Email address changed.
12.07.2007 10:42:16	127.0.0.1	/configclients.html	Email sender name changed.
12.07.2007 10:42:04		sbccsrv.exe	C:\Programme\Safer-Networking\sbNet\config\ File was updated.
12.07.2007 10:42:04		sbccscl.exe	C:\Programme\Safer-Networking\sbNet\config\ File was updated.
12.07.2007 10:42:04	127.0.0.1	/configclients.html	Client Log Email Address changed.
12.07.2007 10:42:04		sbccsrv.exe	C:\Programme\Safer-Networking\sbNet\config\ File was updated.
12.07.2007 10:42:04		sbccscl.exe	C:\Programme\Safer-Networking\sbNet\config\ File was updated.
12.07.2007 10:42:04	127.0.0.1	/configclients.html	Client Config Password changed.
12.07.2007 10:42:04		sbccsrv.exe	C:\Programme\Safer-Networking\sbNet\config\ File was updated.
12.07.2007 10:42:04		sbccscl.exe	C:\Programme\Safer-Networking\sbNet\config\ File was updated.
12.07.2007 10:42:04	127.0.0.1	/configclients.html	Client Config URI changed.
12.07.2007 10:42:04		sbccsrv.exe	C:\Programme\Safer-Networking\sbNet\config\ File was updated.
12.07.2007 10:42:04		sbccscl.exe	C:\Programme\Safer-Networking\sbNet\config\ File was updated.
12.07.2007 10:42:04	127.0.0.1	/configclients.html	Client Update URI changed.
12.07.2007 10:38:36	127.0.0.1	/appsettings.html	Mailer application setting is not compatible to the SMTP server to use on client configuration.
12.07.2007 10:38:08	127.0.0.1	/appsettings.html	Hide legal warning setting is not compatible to use of client autostart or client scheduler.
12.07.2007 10:34:08	127.0.0.1	/configserver.html	Sync Proxy Password changed.
12.07.2007 10:34:00	127.0.0.1	/configserver.html	Sync Proxy Password changed.
12.07.2007 10:34:00	0.0.0.0	spybotsd.ini	Verifying updates...
12.07.2007 10:34:00		0.0.0.0	Licensed for Safer-Networking Ltd. (valid until 30.03.2008)
12.07.2007 10:34:00	127.0.0.1	/configserver.html	Sync Retry Interval changed.
12.07.2007 10:34:00	0.0.0.0	spybotsd.ini	Verifying updates...
12.07.2007 10:34:00		0.0.0.0	Licensed for Safer-Networking Ltd. (valid until 30.03.2008)
12.07.2007 10:34:00	127.0.0.1	/configserver.html	Sync Interval changed.
12.07.2007 10:32:28		sbccsrv.exe	C:\Programme\Safer-Networking\sbNet\config\ File was updated.
12.07.2007 10:32:28		sbccscl.exe	C:\Programme\Safer-Networking\sbNet\config\ File was updated.
12.07.2007 10:32:26	0.0.0.0	spybotsd.ini	Verifying updates...
12.07.2007 10:32:26		0.0.0.0	Licensed for Safer-Networking Ltd. (valid until 30.03.2008)

Figure 31: The Access log

This page shows the access log of sbNet. You may filter the log by different criteria:

Date: Only show accesses from a certain date. The format is localised and the same as the date displayed in the blue section titles.

IP: Only show accesses from a certain IP address.

File: Only show accesses to a certain file. You have to specify the exact name of the file.

Description: Configure which kind of logged information is shown: All log lines, only successful accesses ('OK'), only informational lines or only error messages.

You can enable or disable the configured filter options at once with the 'Use Filter' option.

4 Troubleshooting and Support

4.1 Troubleshooting

After installation the web interface shows a critical license error

Make sure the program direcotry of sbNet contains the files `license.txt` and `license.key` and then restart sbNet. The license files are contained in the archive `license.zip` we sent you by email or directly in the installer of sbNet. If you have not received your license files yet, contact sales@safer-networking.ie.

The sbNet server can not be reached by the clients

Check the firewall settings of the computer sbNet is running on. Also make sure the port sbNet is listening on (port 80 by default) is not used by another network service like a general purpose web server.

Scheduled scans are not executed on Windows 95/98/Me/NT 4 clients

Make sure Microsoft Windows' 'Scheduling Agent' is installed and running. It is included e.g. in Microsoft Internet Explorer 5.0 and later. When installing Internet Explorer, don't chose 'Minimal Installation' and make sure you are including the 'Offline Browsing Pack'. If `mstask.exe` is not running after system startup on Windows 95/98/Me, add a link to it into the Autostart folder. On Windows NT 4 make sure the the 'Task Scheduler' service is running.

Problems reconfiguring paths in the 'Server configuration' section

When reconfiguring the paths in the 'Server configartion' section, you first have to create the according directories. Only after this, go to this section in the web interface and change the paths. If the directories do not exists before changing these options, your changes will not be saved.

Even when using sbNet, my users can still change Spbot S&D's configuration

You can deny users access to Spybot S&D's configuration by defining the 'Settings password'. See section 3.4.1. After this the user is prompted for this password before he can change Spybot S&D's configuration.

Problems getting log emails from the Spybot S&D clients

Make sure you entered the correct settings for your mail server in the 'Client mail settings' on the 'Client configuration' page. Furthermore when you plan to run Spybot S&D as a scheduled task, you need to configure it to use the SMTP protocol directly instead of the installed 'System default mailer'. You can do this via the option 'Mailer application' on the 'Client settings' page of sbNet.

Problems storing updates downloaded by sbNet on a different computer

If you want sbNet to save the downloaded updates on a network share of another computer, you have to make sure the sbNet service is run with sufficient access rights. You can change the username the service runs with in the Properties dialog of the service as shown on screenshot 4.1.

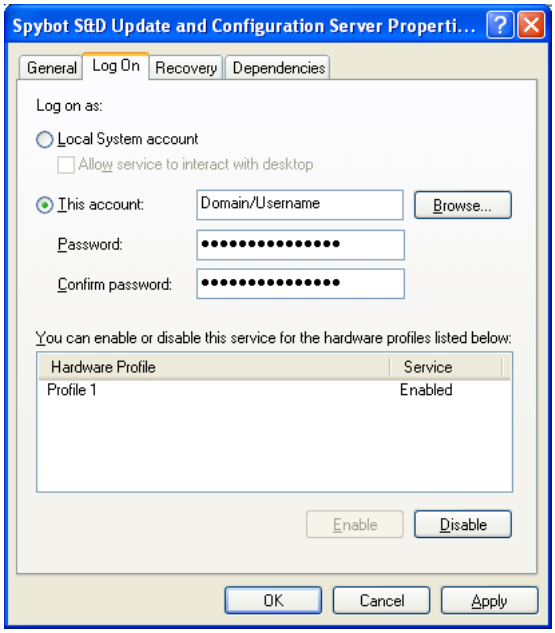


Figure 32: Service Properties dialog

4.2 Contact

Safer-Networking offers different contact channels on the website.

Bug report For reporting a bug you found in Spybot S&D Update and Configuration Server, use:
`http://www.safer-networking.ie/en/contact/bugs.html`

Software information For general support for our software use:
`http://www.safer-networking.ie/en/contact/software.html`

Order For ordering the Spybot S&D Update and Configuration Server use:
`http://www.safer-networking.ie/en/contact/order.html`

Demo-Version For requesting a demo of Spybot S&D Update and Configuration Server use:
`http://www.safer-networking.ie/en/contact/demo.html`

5 Reference

5.1 Parameters for Spybot S&D

Here is a list of command line parameters supported by the Spybot S&D main executable (`SpybotSD.exe`):

/taskbarhide Runs Spybot S&D completely hidden (no window, no taskbar icon), so make absolutely sure you only use it in combination with /autoclose (otherwise it would remain in memory sitting idle). Useful only in combination with /autocheck, /autoupdate or /autoimmunize, as it cannot be controlled when completely invisible.

/minimized Starts the window minimized.

/uninstall Uninstalls Spybot S&D. This command line parameter is very outdated — `unins00.exe` should be used instead!

/blinduses Starts with support for blind users (special menus).

/autoupdate Does an update after starting the program.

/autocheck Starts scanning immediately.

/autofix Fixes problems after scan.

/autoclose Closes program after it has scanned or updated.

/autoimmunize Runs the immunization at program start.

/onlyspyware Fixes only spyware (red) entries with /autofix, leaving all usage tracks as they are.

/easymode Starts with easier interface for newbies.

6 Terms of Corporate Use

This License Agreement (hereinafter "Agreement") between Safer-Networking Ltd. of Mill Road, Greystones, Co. Wicklow, Ireland (hereinafter "Safer-Networking Ltd.") and the Customer (hereinafter "Licensee") sets out the terms and conditions of Licensee's use of Spybot - Search & Destroy software programs, i. e. Spybot Search & Destroy Small Business Edition, Spybot Search & Destroy Corporate Edition, Spybot Search & Destroy Service Edition, Spybot Search & Destroy Corporate Service Edition and, including any additional components, e. g. the minimal Operating System (Windows 7 PE) as the case may be, updates, upgrades, modifications, revisions, copies, documentation and design data set out in the Schedule (the "Software").

§1. GRANT OF LICENSE.

1.1 The Software is copyright, trade secret and confidential property of Safer-Networking Ltd. or its Licensors who maintain exclusive title to all Software and retain all rights not expressly granted by this Agreement. Insofar as Software is supplied to Licensee (either in tangible or non tangible form) and subject to (i) the payment of the License Fees set out in the relevant Price List and (ii) depending on the Software obtained by Licensee, Safer-Networking Ltd. grants to Licensee a non-exclusive, non-transferable and non-sublicensable right for the agreed License Term to use the Software under the following conditions. The right to use includes the right to install, load and run the Software.

a) Spybot Search & Destroy Corporate Edition ("CE Software")

CE Software consists of client software and server software. Licensee shall be entitled to use the server software for internal business purposes on any number of servers within his own network. The number of clients, i. e. devices, on which the client software is used, may not exceed the number of licences obtained by Licensee. For the purposes of this Agreement, a virtual device is considered the same as a physical device.
CE Software may be distributed by means of a bootable Service CD that also contains a minimal Operating System (Windows 7). For the minimal Operating System (Windows 7) separate license terms apply (see Sec. 1.1e))

b) Spybot Search & Destroy Small Business Edition (SBE Software)

Licensee shall be entitled to use SBE Software for Licensee's internal business purposes. The number of clients, i. e. devices, on which the SBE Software is used, may not exceed the number of licences obtained by Licensee. For the purposes of this Agreement, a virtual device is considered the same as a physical device.
SBE Software may be distributed by means of a bootable Service CD that also contains a minimal Operating System (Windows 7). For such minimal Operating System (Windows 7) separate license terms do apply (see Sec. 1.1e))

c) Spybot Search & Destroy Service Edition (SE Software)

Licensee shall be entitled to use SE Software to scan and clean infected computers belonging to third parties.
SE Software is distributed by means of a bootable Service CD. SE Software may accessed from the Service CD or any other device that is accessible from the computers of the third party. The Service CD contains a minimal Operating System (Windows 7) for which separate license terms apply (see Sec. 1.1e)) and SBE Software. By way of derogation from Sec. 1.1b) this SBE Software may be only used for support cases.

d) Spybot Search & Destroy Corporate Service Edition (CSE Software)

The Corporate Service Edition is licensed for the use by the Licensees support staff while while servicing computers that are owned by Licensee. The support staff are permitted to install the software on a non system external device such as an external harddisk or flash drive if necessary for the purpose of servicing the Licensees computers or they may use the software from the Service-CD. If the software is run from an external device at Licensee's site or other location the Software may not be installed or copied to the computer being serviced. Therefore, the real time services of Spybot-Search & Destroy will not be available.
CSE Software is distributed by means of a bootable Service CD. The Service CD contains a minimal Operating System (Windows 7) for which separate

license terms do apply (see Sec. 1.1e)) and SBE Software. By way of derogation from Sec. 1.1b) SBE Software may be only used for support cases.

e) Limited Operating System (Windows 7)

The Service CD may contain Windows software licensed from Microsoft Corporation and/or MS Affiliate(s) ("minimal Operating System"). It is expressly stated, that the minimal Operating System is not sold to Licensee and is provided "as is". The minimal Operating System may only be used as a boot, diagnostic, disaster recovery, setup, restoration, emergency service, installation, test and/or configuration utility program. The use of the minimal Operating System as a general purpose operating system or as a substitute for a fully functional version of any operating system product is strictly prohibited. All rights not expressly granted are reserved.

§2. LIMITED WARRANTY.

2.1 Safer-Networking has endeavoured to ensure that the Software does not contain any backdoors or content to intentionally harm the Licensee. Nothing herein shall be construed as a warranty by Safer-Networking Ltd. that the Software licensed herein corresponds with any representations or descriptions howsoever published nor that the Software is fit for the purpose intended by the Licensee, the Licensee's servants or agents nor that the Software is merchantable. Any such warranties and any warranties purported to be implied by Irish law into this agreement shall not be implied and are hereby excluded. Their exclusion has been drawn specifically to the attention of the Licensee who acknowledges this by contracting these terms.

2.2 The warranties set forth in this Section 2 are exclusive. Neither Safer-Networking Ltd. nor its Licensors make any other warranties, express, implied, or statutory, with respect to Software or other material provided under this Agreement. Licensee especially acknowledges that no statement or representation of Safer-Networking Ltd. shall be considered as a guarantee regarding the fitness of the Software for any particular purpose, unless such statement has been expressly confirmed to the Licensee by Safer-Networking Ltd. in writing.

§3. DOCUMENTATION AND UPDATES.

Safer-Networking Ltd. provides the necessary user documentation of the Software. This may also be provided electronically, e. g. by provision over the Internet. Safer-Networking has no contractual obligation to provide regular updates and the provision of updates does not constitute any such contractual obligation of Safer-Networking Ltd.

§4. RESTRICTIONS.

4.1 Safer-Networking Ltd. does not authorize all or any portion of the Software to be "issued to the Public", "put into circulation", or subject to a "first sale" as the copyright laws may use those (or similar) terms. Licensee is not allowed to distribute, sublicense, lease, rent, loan or otherwise transfer the Software to a third party.
4.2 All Software will be supplied and may be used in object code form only. Except as otherwise permitted for purposes of interoperability as specified by applicable and mandatory local law, Licensee shall not reverse-assemble, reverse-compile, reverse-engineer or in any way derive from Software any source code or decrypt the database.
4.3 Licensee shall not remove alphanumeric identification characters, trademarks and copyright notices.
4.4 Licensee may copy Software only as reasonably necessary to support the authorized use and may make necessary backup copies. Each copy must include all notices and legends embedded in Software and affixed to its medium and container as received from Safer-Networking Ltd. All copies shall remain the property of Safer-Networking Ltd. or its Licensors. Licensee shall maintain a record of the number and primary location of all copies of Software, including copies merged with other software, and shall make those records available to Safer-Networking Ltd. upon request.
4.5 Licensee shall not make Software available in any form to any person other than employees and contractors, excluding Safer-Networking Ltd.'s competitors, whose job performance requires access. Licensee shall take appropriate action to protect the confidentiality of Software and ensure that any person permitted access to Software does not disclose it or use it except as permitted by this Agreement.
4.5 The provisions of this Section 4 shall survive the termination or expiration of this Agreement.

§5. FEES.

5.1 The License Fees shall be payable in advance in Euros (USD if Licensee is located in the USA or Canada) for the amounts and the period indicated in the Price List and shall be payable as set out in the Price List. Safer-Networking Ltd. shall issue invoices for the License prior to the date of commencement of the relevant periods.
5.2 In the case of the extension of the Agreement as set out in Sec. 10.1 of this Agreement, the relevant version of the Price List at the time of the extension shall apply.
5.3 If the use of the Software at any time exceeds the maximum number of licenses granted to Licensee under this Agreement Licensee shall pay to Safer-Networking Ltd. the applicable additional License Fee so arising at the rates in the Price List. The number of Software licenses granted shall be deemed to be adjusted accordingly on payment by the Licensee of the applicable additional License Fee.
5.4 The License Fees and other charges from Safer-Networking Ltd. are due when invoiced and payable within 14 calendar days of the receipt of invoice by the Licensee. In case of a delay in payment, Safer-Networking Ltd. is entitled to charge interest on arrears at 8%-points (eight percentage points) above the then-current European Central Bank Lending rate.
5.5 The License Fee and all other charges are exclusive of VAT and all other Taxation, which shall, if applicable, be chargeable to the Licensee.
5.6 It is specifically agreed that Safer-Networking Ltd. may, at its sole discretion, treat a failure by the Licensee to pay amounts due within the time allowed under this Section 5 as a suspension made at the Licensee's request of any Maintenance and Technical Support that may be agreed by the parties separately.

§6. INSTALLATION AND SUPPORT.

6.1 Licensee is responsible for installation and use of the software. Support issues of the Licensee will be handled solely by Safer-Networking Ltd. and not by any of its Licensors. Available support consists of email support that has priority over freeware users. Phone support information will be published on www.safer-networking.ie.
6.2 THE MINIMAL OPERATING SYSTEM CONTAINS A TIME-OUT FEATURE THAT WILL AUTOMATICALLY REBOOT THE DEVICE AF-

TER SEVENTY-TWO HOURS OF CONTINUOUS USE. THIS TIME-OUT FEATURE WILL RESET EACH TIME THE COMPONENT IS RE-LAUNCHED.

§7. SPECIFICATION OF THE SOFTWARE.

The Software is designed to scan for software that poses a threat to the privacy of the user of a computer ("Malware"). While the Software endeavours to detect known Malware, not all Malware will be detected. Spybot Search & Destroy software runs on Windows computers running 2000, XP, 2003 Server, Vista, 2008 Server or Windows 7 only.

§8. LIMITATION OF REMEDIES AND DAMAGES.

In no event will Safer-Networking Ltd., its Licensors or their affiliates be liable for any indirect, incidental special or consequential damages or for any lost profits, lost savings, lost revenues or lost data arising from or relating to the Software or this agreement, even if Safer-Networking Ltd., its Licensors or their affiliates have been advised of the possibility of such damages. In no event will Safer-Networking Ltd., its Licensors or their affiliates liability or damages to Licensee or any other person ever exceed the amount paid by Licensee to use the software, regardless of the form of the claim. The software is not fault-tolerant. It is not designed for use in High Risk Activities, where the failure of this Software could lead directly to death, personal injury or severe physical or property damage. Neither Safer-Networking Ltd. nor its Licensors or their affiliates shall be liable for any damages resulting from or in connection with the use of software in any application where the failure or inaccuracy of the software might result in death or personal injury.
IN NO CASE SHALL Safer-Networking Ltd. ITS LICENSORS' OR THEIR AFFILIATES' LIABILITY EXCEED THE PURCHASE PRICE PAID FOR THE SOFTWARE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.
The Software may contain third party device drivers. Such device drivers are provided solely for your convenience. It is your responsibility to confirm whether such device drivers are applicable to your environment. The device drivers are provided by Safer-Networking Ltd. "AS IS" WITHOUT ANY TECHNICAL SUPPORT OR WARRANTY OF ANY KIND, INCLUDING BUT NOT LIMITED TO FITNESS FOR A PARTICULAR PURPOSE.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT AND UNDER NO LEGAL THEORY SHALL SAFER-NETWORKING LTD., ITS SUPPLIERS OR THEIR AFFILIATES BE LIABLE FOR ANY DIRECT, CONSEQUENTIAL, SPECIAL, INCIDENTAL, PUNITIVE OR INDIRECT DAMAGES OF ANY KIND ARISING OUT OF OR RELATED TO THE THIRD PARTY DEVICE DRIVER.

§9. INFRINGEMENT.

9.1 Safer-Networking Ltd. will defend or settle, at its option and expense, any action brought against Licensee alleging that Software infringes a patent or copyright in the United States, Canada, Japan, or member state of the European Patent Office. Safer-Networking Ltd. will pay any costs and damages finally awarded against Licensee that are attributable to the infringement action. Licensee understands and agrees that as conditions to Safer-Networking Ltd.'s obligations under this section Licensee must: (a) notify Safer-Networking Ltd. promptly in writing of the action; (b) provide Safer-Networking Ltd. all reasonable information and assistance to defend or settle the action; and (c) grant Safer-Networking Ltd. sole authority and control of the defense or settlement of the action.
9.2 If an infringement claim is made, Safer-Networking Ltd. may, at its option and expense: (a) replace or modify Software so that it becomes non-infringing; (b) procure for Licensee the right to continue using Software; or (c) require the return of Software and refund to Licensee any License Fee paid, less a reasonable allowance for use.
9.3 Safer-Networking Ltd. has no liability to Licensee if infringement is based upon: (a) the combination of Software with any product not furnished by Safer-Networking Ltd.; (b) the modification of Software other than by Safer-Networking Ltd.; (c) the use of other than a current unaltered release of Software; (d) the use of Software as part of an infringing process; (e) a product that Licensee make, use or sell; (f) any Beta Code contained in Software; (g) any Software provided by Safer-Networking Ltd.'s Licensors who do not provide such indemnification to Safer-Networking Ltd.'s customers; or (h) infringement by Licensee that is deemed willful. In the case of (h) Licensee shall reimburse Safer-Networking Ltd. for its attorney fees and other costs related to the action upon a final judgment.
9.4 THIS SECTION 9 STATES THE ENTIRE LIABILITY OF SAFER-NETWORKING LTD. AND ITS LICENSORS AND LICENSEE'S SOLE

AND EXCLUSIVE REMEDY WITH RESPECT TO ANY ALLEGED PATENT OR COPYRIGHT INFRINGEMENT OR TRADE SECRET MISAPPROPRIATION BY ANY SOFTWARE LICENSED UNDER THIS AGREEMENT.

§10. TERM.

10.1 The initial Term of this Agreement is twelve (12) months. The Agreement shall automatically be extended for additional twelve (12) months each unless terminated by giving notice 2 (two) calendar months prior at the end of the relevant Term by registered letter.
10.2 The right of one of the Parties to terminate the Agreement early for cause by means of registered letter shall remain unaffected. Prior of such termination for cause and, especially, prior to termination due to a material breach of contract, the respective party shall notify the other party that has committed the alleged breach demanding the other party to remedy the breach within 30 (thirty) days the breach was reported. Termination for cause shall be reported by means of a registered letter and, whenever possible, no later than the cancelation period of thirty (30) days, however, at a cancelation period minimum of 10 (ten) days.
10.3 Reasons for Safer-Networking Ltd. to be entitled to terminate this Agreement for cause shall include, in particular, when Licensee makes use of the Software without authorization of Safer-Networking Ltd. If Safer-Networking Ltd. is entitled to terminate this Agreement for cause it may demand immediate payment of liquidated damages which shall be established as half of the fee amount up to the time of the end of the relevant Term as set forth in Sec. 10.1 of this Agreement. Liquidated damages may be determined as a higher or lesser amount, if Safer-Networking Ltd. proves higher or Licensee proves lower losses or damage.
10.4 Upon any termination or expiration, Licensee agree to cease all use of Software and return it to Safer-Networking Ltd. or certify deletion and destruction of Software, including all copies, to Safer-Networking Ltd.'s reasonable satisfaction.

§11. EXPORT.

Software may be subject from time to time to regulation by local laws and European Union export regulations, which prohibit export or diversion of

certain products, information about the products, and direct products of the products to certain countries and certain persons. The minimal Operating System is subject to U.S. export restrictions. Licensee agrees that Licensee will not export any Software or direct product of Software in any manner without first obtaining all necessary approval from appropriate local and European Union government agencies.

§12. RESTRICTED RIGHTS NOTICE.

If Licensee is acquiring any material on behalf of any unit or agency of the U.S. government ("Government"), Licensee shall notify Safer-Networking Ltd. in writing prior to delivery of such material and shall obtain the Government's agreement that the Licensed Program is "commercial computer software" and/or "commercial computer software documentation" pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable, and any use, modification, reproduction, release performance, display, or disclosure shall be prohibited except as expressly permitted by this Agreement, which terms shall govern.

§13. AUDIT RIGHTS.

With reasonable prior notice, Safer-Networking Ltd. or its Licensor shall have the right to audit during Licensee's normal business hours all records and accounts as may contain information regarding Licensee's compliance with the terms of this Agreement. Safer-Networking Ltd. or its Licensor shall keep in confidence all information gained as a result of any audit. Safer-Networking Ltd. shall only use or disclose such information as necessary to enforce its rights under this Agreement.

§14. GOVERNING LAW AND JURISDICTION.

This Agreement shall be governed by and construed under the laws of Ireland. All disputes arising out of or in relation to this Agreement shall be submitted to the exclusive jurisdiction of Dublin, Ireland. This section shall not restrict Safer-Networking Ltd.'s right to bring an action against Licensee in the jurisdiction where Licensee's place of business is located.

§15. SEVERABILITY.

If any provision of this Agreement is determined by a court to be or becomes invalid, unenforceable or illegal, such provision shall be (i) modified to be made valid, enforceable and legal in such a manner as to best effectuate the intent of the parties at the inception of this Agreement; or (ii) be deemed eliminated where such modification is not practicable; and (iii) the remainder of this Agreement shall remain in effect in accordance with its terms as modified by such modification or deletion.

§16. MISCELLANEOUS.

This Agreement sets forth the entire understanding and agreement of the parties regarding the subject matter hereof, and supersedes all prior agreements or representations, oral or written regarding such subject matter. This Agreement may not be modified or amended except in writing signed by a duly authorized representative of the party against whom enforcement is sought.

§17. LICENSEE CONSENT.

Licensee herby consents to the following features of the Software. Application offline privacy. Even though Spybot-S&D scans Licensee's system, it will not search specifically for any personally identifiable information. Everything that is not detected as a possible threat will be ignored. Possible threats will be shown and, if log options are switched on, written to a log file that may reside on an intranet server depending on the installation.

§18. PRIVACY.

Even though Spybot Search & Destroy scans a system, it will not search specifically for any personally identifiable information. Everything that is not detected as a possible threat or usage track will be ignored. Possible threats and usage tracks will be shown and, if log options are switched on, written to a local log file. For further information please visit http://www.safer-networking.ie.
Windows is a registered trademark of Microsoft Corporation.

Spybot and Spybot - Search & Destroy are Trademarks of Patrick Kolla-ten Venne
This agreement is accepted by installing the software.

Index