



Manual ArchiCrypt Stealth

Dok.-Nr.: ACSAF-HB-0004

Issue date: 25.07.2006

Issue-Nr.: 4.1

The reproduction, distribution and utilization of this document as well as the communication of its contents to others without explicit authorization is prohibited. Offenders will be held liable for the payment of damages. All rights reserved. ArchiCrypt is a registered trademark of Dipl.-Ing. Patric Remus

© 2002-2006 Software Development Dipl.-Ing. Patric Remus

Inhalt

Teil I Introduction	1
1 Welcome	1
Teil II General information	1
1 Important information	1
2 General installation document	2
3 System requirements	2
4 Copyright	2
Teil III Setting up Stealth	3
Teil IV Operation	3
1 Overview	3
2 Stealth Central	5
3 Website blocker	6
4 Cookies	7
5 Plug-ins	8
6 Spyware	10
7 Identity	11
8 Log	11
9 Settings Anonymous servers	12
10 Settings Application behavior	14
Teil V Status-Monitor	18
Teil VI Proxy-Collector	19
1 Overview	19
2 Function overview	20
3 Settings	22
4 Stealth List	23

Teil VII Frequently asked questions (FAQ)	23
Index	25

1 Introduction

1.1 Welcome

Many thanks for choosing ArchiCrypt Stealth!

In the "real" world, it is not normal to hand out your name and address every time you turn around, but, unfortunately, that is normal on the Web. The Internet seems to be completely anonymous; no one sees us and no one hears us when we surf the Web. In reality, however, this anonymity is not what it seems to be. Every website, every page, can clearly identify you based on your so-called [IP address](#). It is possible to record exactly when you visited which site. With the help of "cookies", it is even possible to follow your trail through the Web and create a [profile of your preferences](#). As a result, website administrators can insert advertisements, tailor-made for you -- ads that are not only annoying, but also usually very effective. In other words, we're talking about successful and, for the most part, unnoticed [manipulation](#).

[Hackers](#) discover your IP address and then [specifically attack your computer](#). Based on the information your browser sends the website administrators, your operating system and your browser permit an attack that exactly targets the gaps in your particular system. As a result, you and your system become the target of unwanted advertising in emails, you may provide a starting point for illegal activity or you suddenly face an unstable operating system.

ArchiCrypt Stealth deals with these problems!

ArchiCrypt Stealth is a powerful tool, which allows you to move around unnoticed in the Internet and which gives you complete control over the data your web browser both sends and receives.

Enjoy ArchiCrypt Stealth!

Dipl.-Ing. Patric Remus

The latest ArchiCrypt Stealth developments are always available at www.ArchiCrypt-Shop.com.

2 General information

2.1 Important information

► The anonymity function depends on so-called proxy servers. Unfortunately, we cannot be responsible for their availability and performance, nor for the way they function. We regularly produce lists of servers, which the program can automatically get from our Internet site, if you wish. Nonetheless, it may also be necessary to manually create, or at least supplement, the anonymous server lists.

► By using special scripts, it is possible to detect the real IP address in spite of activating the anonymity function. Using script components in HTML content, it is also possible to set and assess cookies. Self-defined data filters (plug-ins) can help

combat against such scripts in HTML pages.

▶ Your web browser uses various protocols to receive and send data. ArchiCrypt Stealth does its job only when the browser uses so-called HTTP protocols.

▶ Certain content filters can cause the content of various pages to be displayed improperly. In such cases, you need to evaluate, whether Stealth should deal with the site or whether you should place it in the global whitelist. In some seldom cases it could be even necessary to deactivate Stealth.

2.2 General installation document

Be aware that administrator privileges are required for installing the software with Windows 2000 and Windows XP.

- ➔ATTENTION: If you use a [personal firewall](#), you must grant *ACStealth4.exe* (see installation folder) complete access rights.

Before starting the program for the first time, be sure that you are connected to the Internet. The program will then load a current anonymous server list.

See also:
Setting up Stealth

2.3 System requirements

In order to use ArchiCrypt Stealth, your system must meet the following minimum requirements:

- ▶ Pentium processor or comparable CPU
- ▶ 128 MB RAM; 256 MB recommended
- ▶ Hard drive space: approx. 10 MB
- ▶ Windows 2000 or Windows XP
- ▶ Screen resolution: at least 800x600 with a color depth of at least 256 colors
- ▶ Mouse or other Windows-compatible pointer

NOTE:

ArchiCrypt Stealth works together with any browser. Special browser settings are NOT necessary. By default Stealth will use your Standard Browser. You can manually select another browser. (see Settings behavior)

See also:
Setting up Stealth

2.4 Copyright

Copyright

ArchiCrypt Stealth

Copyright © 2002-2006 Dipl.-Ing. Patric Remus
Am Brunneck 6, D-85521 Ottobrunn

All rights reserved.

3 Setting up Stealth

ArchiCrypt Stealth works together with any browser. For example, Internet Explorer, Netscape, Mozilla, Firefox, T-Online Browser, AOL, Opera, etc. Absolutely no settings need to be made. By default Stealth will use your Standard Browser. You can manually select another browser. (see Settings behavior)

➡ **ATTENTION:** If you use a program which functions as a so-called local proxy (127.0.0.1) and is entered in your browser, the data will be sent to that program.

If you use an external proxy, ArchiCrypt Stealth bypasses that setting. The proxy will no longer be called on.

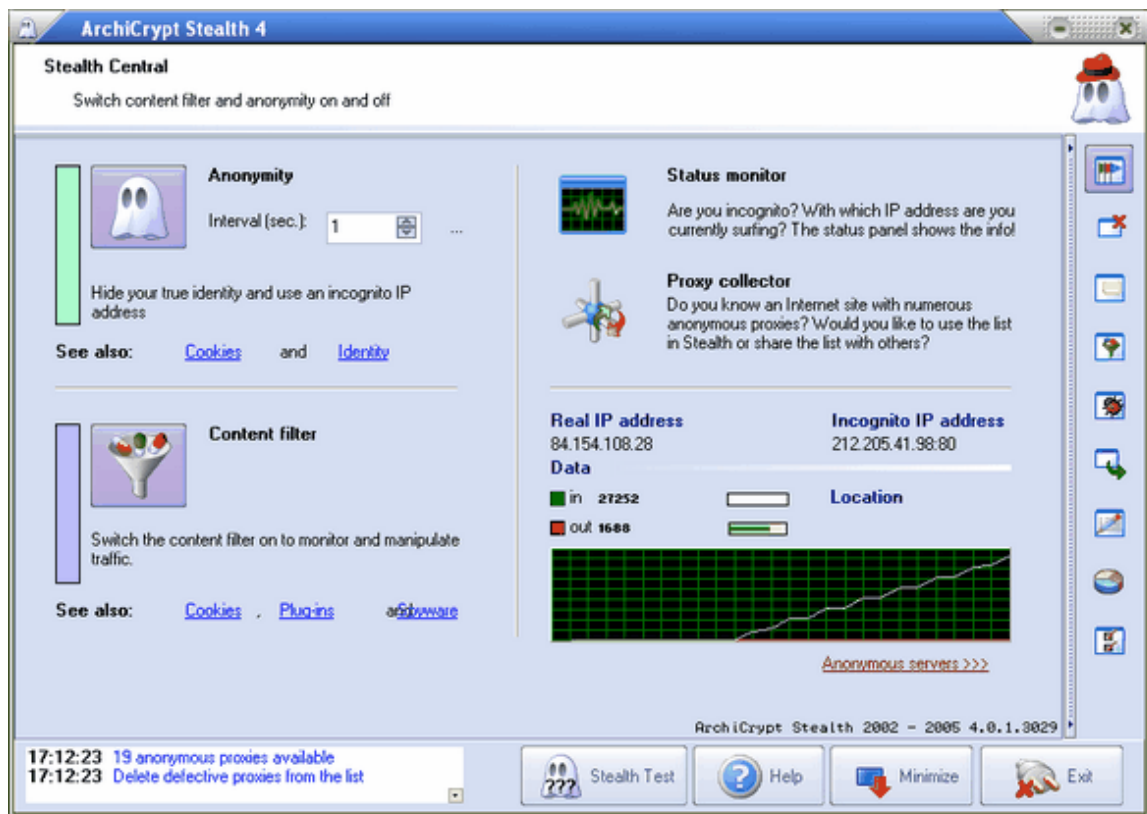
Note:

The anonymity function is dependant on so-called proxy servers. Unfortunately, we cannot be responsible for their availability and performance, nor for the way they function. We regularly produce lists of servers, which the program can automatically get from our Internet site, if you wish. Nonetheless, it may also be necessary to manually create, or at least supplement, the anonymous server lists.

4 Operation

4.1 Overview

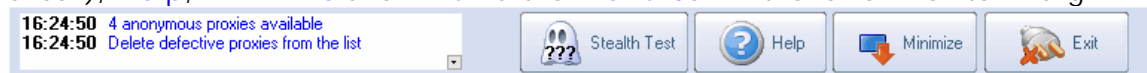
ArchiCrypt Stealth offers two main functions, which can be used independantly of each other. Via its [Anonymity](#) function, ArchiCrypt Stealth not only offers the possibility of surfing the Internet with an incognito IP address, but the software also makes the manipulation of incoming and outgoing data possible with the so-called [Content filter](#). ArchiCrypt Stealth focuses on the so-called HTTP protocol.




The user interface is divided in the following sub-categories:

Stealth Central
 Website blocker
 Cookies
 Plug-ins
 Spyware
 Identity
 Log
 Settings

From any sub-category, you can reach the functions **Stealth Test** (Anonymity check), **Help**, **Minimize** and **Exit** via the **menu bar** in the lower monitor margin.



A status window simultaneously provides comprehensive information about current activity. Information that points to errors is displayed in red. You usually receive an indication of the cause of the error. Click the  button, when you want to take note of the error.

Exit: Ends ArchiCrypt Stealth

Minimize: Minimizes the ArchiCrypt Stealth window and displays it in the system tray (near the clock). You can access various functions by clicking the right mouse button above the ArchiCrypt Stealth symbol and selecting the appropriate entry in

the context menu. Double-clicking the symbol opens the main Stealth window.



Stealth Test: If there is an Internet connection, a page is called up, which attempts to discover your true Internet address. Check whether the given address agrees with your real address. If not, you're surfing anonymously!

➔ **ATTENTION:** *If you test Stealth's functionality and initially run the text without activating the anonymity function, you must first close the browser and possibly delete the browser cache.*

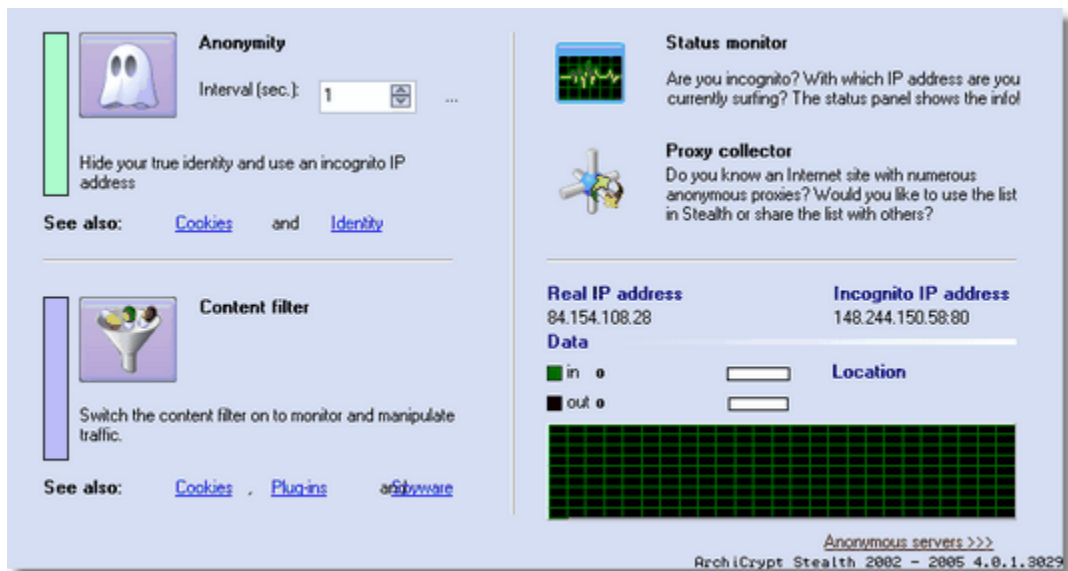
Help: Calls for help relating to the sub-category in use.

4.2 Stealth Central

At **Stealth Central**, you switch the main functions, **Content filter** and **Anonymity**, on or off. At the same time, you can call up the helps, **Status monitor** and **Proxy-Collector** (if present).

Note: Depending on which function you have activated, elements of other pages are either made available or are blocked.

In order to treat incoming cookies, for example, it is necessary to activate the Content filter.



Content filter:

In general, the [Content filter](#) is necessary for filtering and manipulating information. It must be activated in order to manipulate Cookies and to use the highly flexible plug-in system. If you want to filter dialers, Spyware and adware, you must also activate the content filter.



TIP: The content filter also works without activating the anonymity function. In other words, you can always filter your data, even when no currently working proxies are available!

[Anonymity:](#)

The [anonymity](#) function uses one or more computers in the Internet, in order for you to surf incognito. You can manually enter any anonymous server, by clicking the "..." button.

To surf anonymously via one, single server, you must set the [interval](#) for changing the IP address at 0!

➡ **ATTENTION:** *The hotkeys "next IP", "previous IP" and "delete current IP" only work, when you are surfing through one, single anonymous server – that is, the interval is set at 0!*

[Status-Monitor:](#)

Calls up the Statusmonitor.

[Proxy-Collector:](#)

Calls up the Proxy-Collector

Note:

The anonymity function depends on so-called proxy servers. Unfortunately, we cannot be responsible for their availability and performance, nor for the way they function. We regularly produce lists of servers, which the program can automatically get from our Internet site, if you wish. Nonetheless, it may also be necessary to manually create, or at least supplement, the anonymous server lists.

4.3 Website blocker

Requirement: [Anonymity](#) or [Content filter](#) activated!

The [Website blocker](#) prevents access to specified Internet sites. At the same time, this feature is not meant to block guest users. ArchiCrypt Stealth can be started by any user and provides no settings for password protection.

By using the Website blocker you can prevent the pages of designated Internet "players" – those who are known for blending in penetrating ad banners, for example – from being displayed. If a blocked site is encountered, depending on your selection, ArchiCrypt Stealth can display any text (also HTML text) or a standard message. The standard message is less striking.



4.4 Cookies

Requirement:

- ▶ **Outgoing Cookies** -> **Anonymity** or **Content filter** activated!
- ▶ **Incoming Cookies** -> **Content filter** activated!

Cookies are unmistakable sequences of symbols that can accept various bits of information. Cookies are used in many ways and not all uses are potentially harmful.

Many internet "players" integrate their ad banners into multiple pages. When you enter such a site, they first check whether a cookie is already present on your computer. If not, a cookie with an unmistakable series of signals will be placed on your computer, and at the same time the provider notes which page you were on when the cookie was saved. Every page that a provider uses to send an ad banner, can call up this cookie. If he realizes that a cookie is already present, he stores the current page under that cookie – remember, it's unmistakable. After a while, he can create a very comprehensive profile on your preferences and surfing habits.

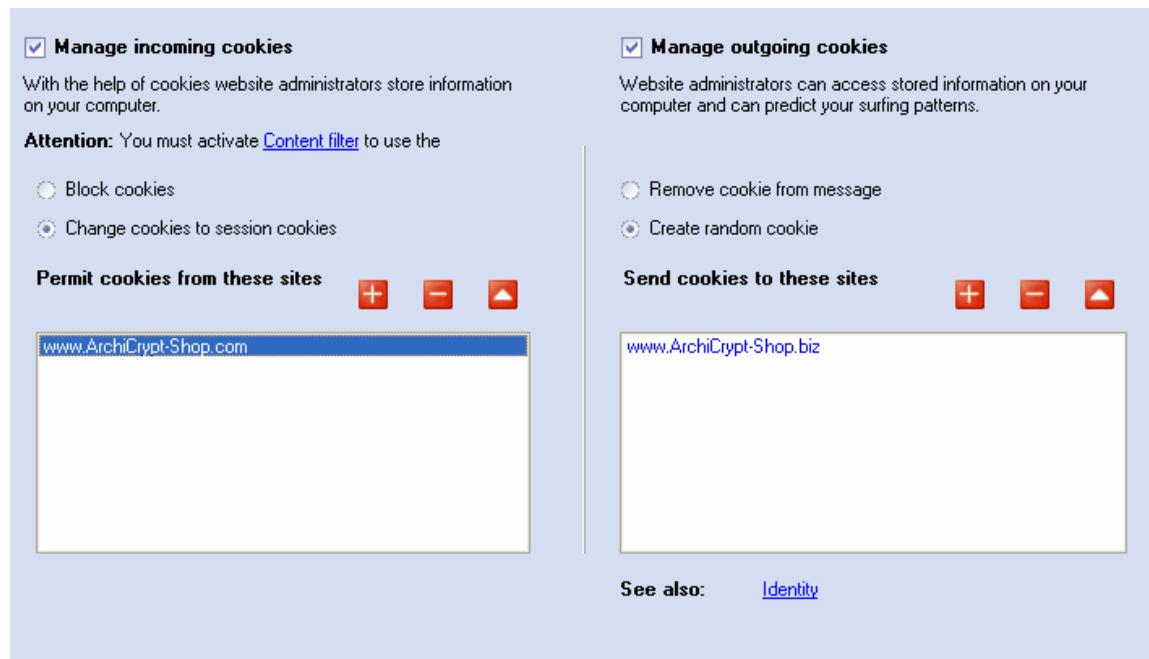
Many users do not know this, however!

Combating and defending against these cookies fall under incoming and outgoing cookies.

Basically, it's enough to deal with **outgoing cookies**, because simply storing the data on your computer doesn't help unless he can access the information. With ArchiCrypt Stealth, he either doesn't get any cookie in return or receives a randomly created cookie for every page you access while surfing. In either case, he is unable to draw any conclusions. The randomly created cookies actually negatively impact his data and his ability to confidently state preferences – they are therefore, in one sense, harmful.

Cookies that have been placed on your computer can also be used locally to

determine which Internet sites you have used. This is certainly not always desirable. Therefore, ArchiCrypt Stealth provides two alternatives.



Blocking Incoming Cookies

The cookies are deleted from the incoming data stream and are, therefore, neither in your computer's memory, nor on the hard drive. There is nothing to access.

Changing Cookies to Session Cookies

The more harmless variation allows Internet sites to place a cookies in your main memory, but denies them a permanent place on your hard drive. This function is helpful, especially for online-shops, for example, since the cookies allow shopping carts to be managed.

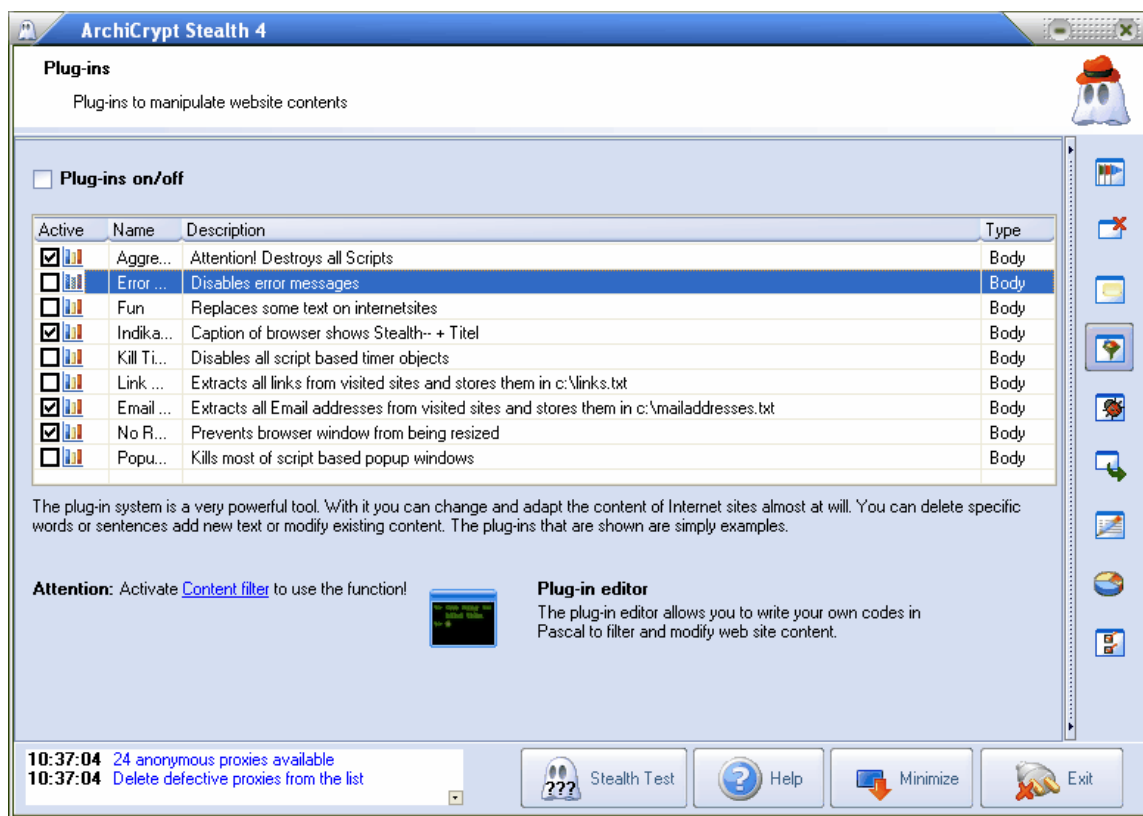
In the lists, [Permit cookies from these sites](#) and [Send cookies to these sites](#) you can enter specific addresses that ArchiCrypt Stealth should ignore. This can be helpful when shopping systems require cookies or your online banking otherwise doesn't work.

With the [+ button](#), you add new addresses to the list; with the [- button](#), you remove marked addresses from the list. The [triangle button](#) permits you revise a marked address.

4.5 Plug-ins

Requirement: [Content filter](#) activated!

The [Plug-ins](#) category provides the most flexible, complete way of manipulating data to meet your requirements.



The so-called plug-ins are shown in a table with the following columns:

Active:

The entry can be switched on and off here. The plug-in will only be used when it is on.

Name:

Name for the plug-in

Description:

Brief description of the plug-in

Type:

There are three types of plug-ins

Body filters the content from web sites

HeaderOUT filters the content of outgoing Headers

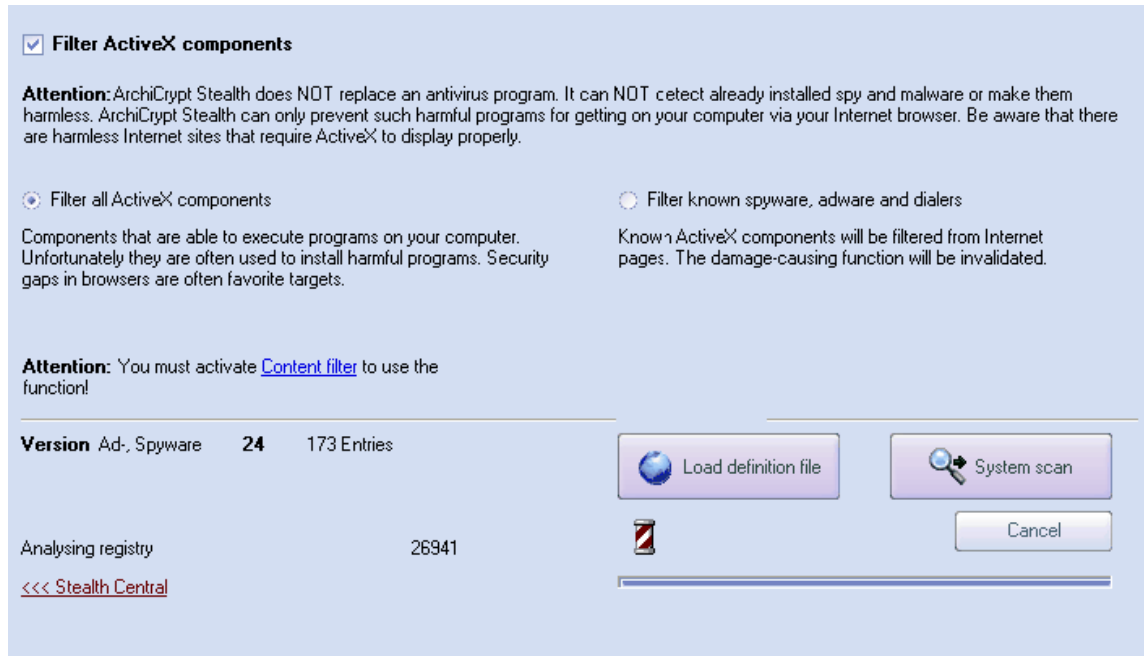
HeaderIN filters the content of incoming Headers

In order to create your own plug-in, you should have a very good knowledge of Delphi/Pascal and possibly personal experience with regular expressions. Use the special plug-in editor to create the plug-ins.

4.6 Spyware

Requirement: [Content filter](#) activated!

The [Spyware](#) page gives you the chance to filter harmful components out of web page content.



Two functions are available:

[Filter all ActiveX components](#) is the safest, but also the most radical. It filters all components from the data that is identified as ActiveX. As a result, even unknown malicious code / programs are blocked; the disadvantage is that even "benign" components do not reach the browser.

[Filter known spyware, adware and dialers](#) uses a definition file, in order to filter only known harmful programs from the data.

With [Load definition file](#) you can load up-to-date definition files for harmful programs from the Internet.

[System scan](#) checks if your computer has been victimized by a known harmful program. If a harmful program is discovered while scanning, the name of the program will be noted. If you then enter the name into a search engine, along with the keyword "Spyware", you will receive information about getting rid of the pest.

➡ **ATTENTION:** *Some anti-spyware programs provide an "immunization." In some cases, this immunization may cause ArchiCrypt Stealth to send a false alarm. Therefore, you should use an anti-spyware tool to be sure that there is no spyware on your system. These programs can usually also remove the harmful components from your system.*

4.7 Identity

Requirement: [Anonymity](#) activated!

Your [identity](#) is primarily determined by your so-called IP address. The anonymity function already takes care of this! Nonetheless, with every site you visit, a lot of information is sent to the website administrator – information you normally cannot influence and may not even know about. If creating your own plug-in is too complicated, you can access the most important functions here.

The functions allow you to specify:

- Browser and operating system
- Accepted languages
- Requesting page (requests origin)
- Who passed the request

The screenshot shows a configuration window with several sections:

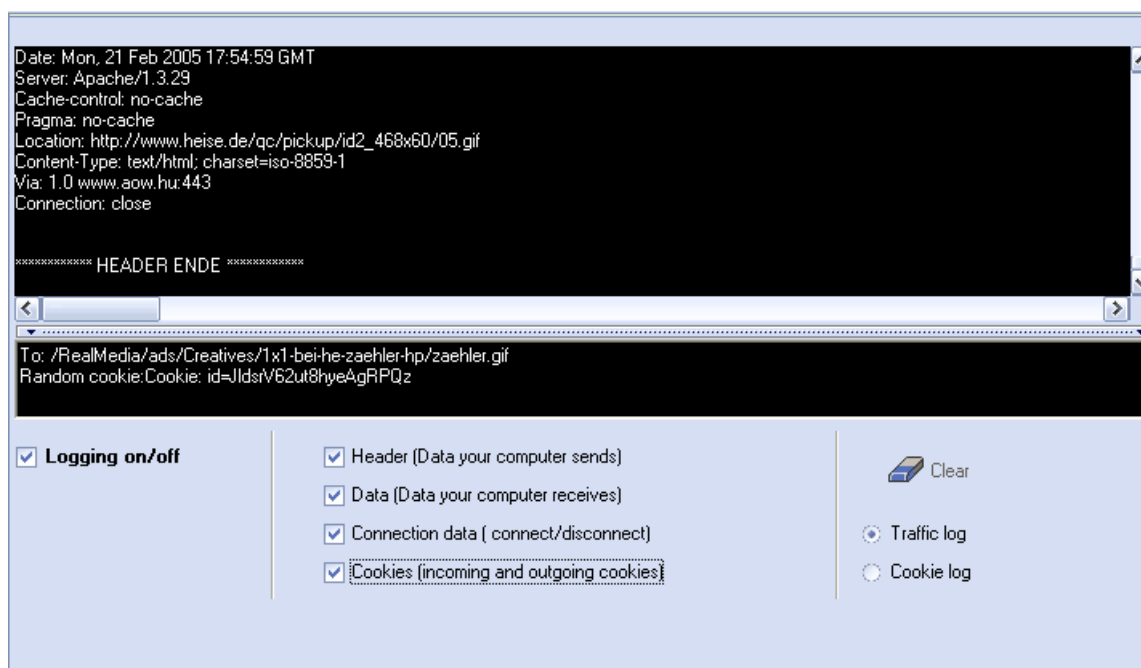
- Browser and operating system:** A checked checkbox. Below it, a globe icon and the text "Which browser do you use?". A dropdown menu shows "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0;". Below this is a note: "(Website administrators can determine which browser and which operating system you are using.)".
- Accepted languages:** An unchecked checkbox. Below it, a speech bubble icon and the text "What language do they speak?". A text input field contains "en". Below this is a note: "(Which languages are accepted? You can draw conclusions about the country of origin. 'en' stands for English 'da, en-gb' for Danish and English.)".
- Conceal origin:** A checked checkbox. To its right is a button labeled "Conceal all outgoing data". Below it, a person icon and the text "Who is requesting the page?". A text input field contains "http://www.google.com". Below this is a note: "(Arbitrary value, fantasy names can betray you however. Enter the Internet sites of as large an Internet directory as possible here.)".
- Generates random client IP:** A checked checkbox. Below it, a cube icon and the text "Creates a random IP address!".
- Where does the request come from?:** A checked checkbox. Below it, a person icon and the text "Where does the request come from?". A text input field contains "yahoo.com, microsoft.com, netscape.com, aol.com". Below this is a note: "(Gives the impression you are simply passing the request on. This keeps anonymous servers from revealing the true identity in this field. Known pages are best here as well.)".

At the bottom left, it says "See also: [Cookies](#) and [Global whitelist](#)".

4.8 Log

The [Log](#) records the selected datatypes.

To activate the log, first choose [Logging on/off](#) and then the data type(s) ([Header](#), [Data](#), [Connection data](#), [Cookies](#)) to log.

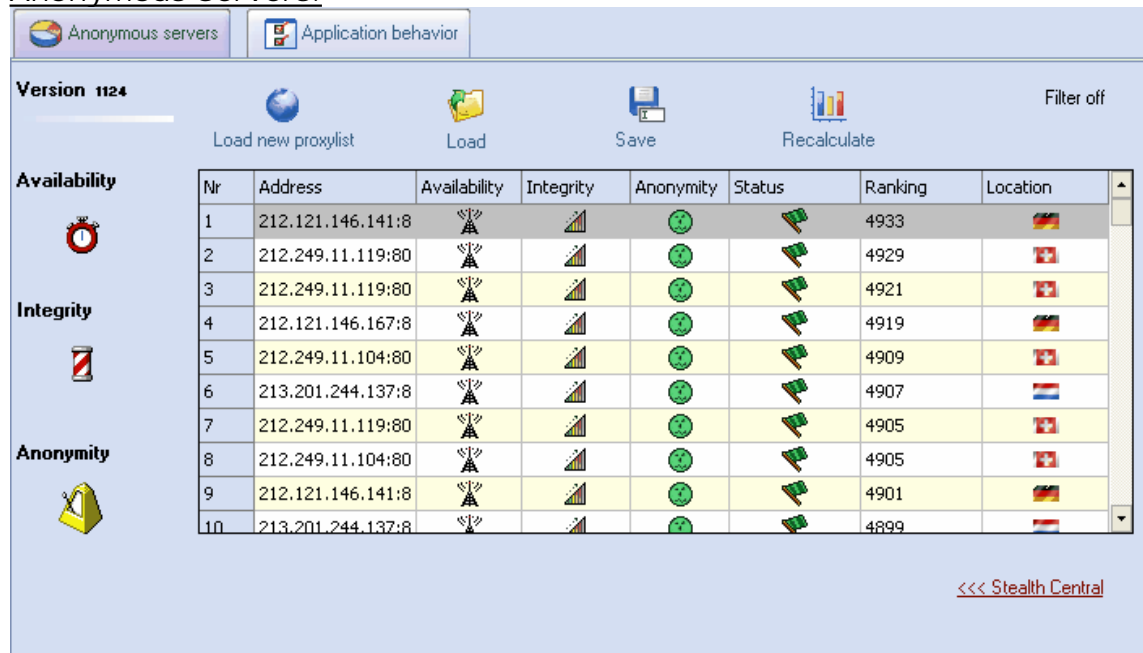


4.9 Settings Anonymous servers

[Anonymous servers](#) and Application behavior

see also: Proxy-Collector

Anonymous Servers:



The [anonymous server list](#) is the heart of the anonymity function.

➡ATTENTION: *If ArchiCrypt Stealth is not shut down correctly, the maximum*

number of parallel tests is two (2). You shouldn't enter too high of a value for [maximum concurrent tests](#) (Application behavior - General)! With high-performance systems and a fast Internet connection you can use 20+. Windows XP SP2 limits this value to about 20.

Via the [Load new proxylist](#) button, you can load a current list from the Internet.

see also: Proxy-Collector

With the [Load](#) button, you can load and use a saved list locally.

[Save](#) allows you to save the updated list.

The [filter on / filter off](#) function allows you to filter the chart for servers that reach a specific ranking.

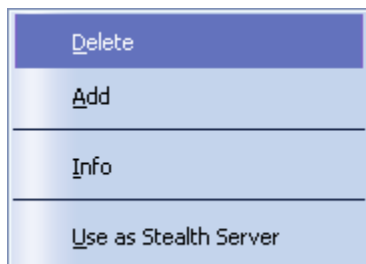
The list provides a [context menu](#) with the functions, [add](#), [delete](#) and [Stealth Server](#).

Call them up by clicking the right mouse button.

With [Add](#) you can manually make an entry to the list, with [Delete](#) you can remove the selected entry from the list.

The [Stealth Server](#) function selects the entry as an anonymous server and switches the interval for changing the IP address to 0.

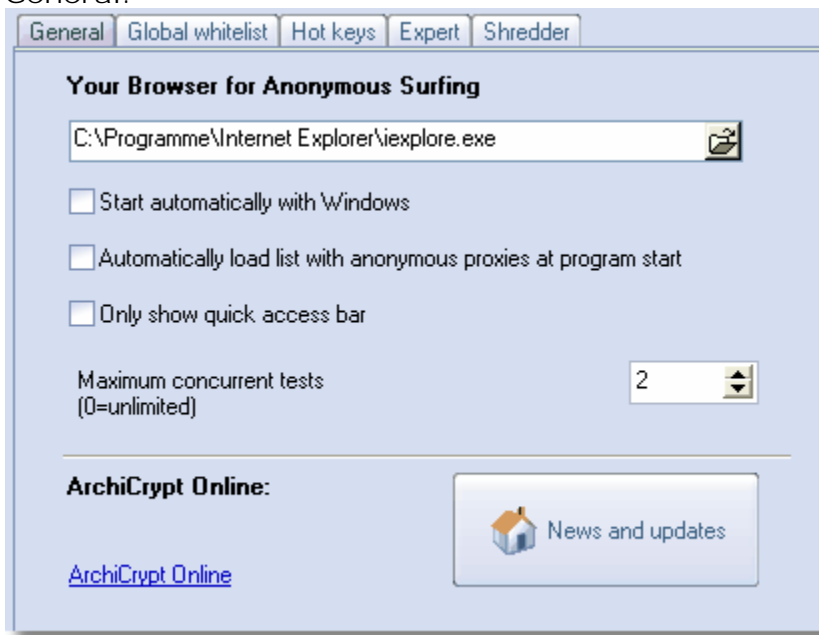
You then continuously surf anonymously via that server in the Internet.



4.10 Settings Application behavior

Application behavior

General:



Selections

Your Browser for Anonymous Surfing

By default, Stealth will use your Standard Browser. You can manually select another Browser!

Start automatically with Windows

ArchiCrypt Stealth starts with Windows.

Automatically load (update) list with anonymous proxies at program start

When starting, ArchiCrypt Stealth automatically loads a list of anonymous servers.

See also. Proxy-Collector

Only show quick access bar

The buttons in the upper margin will be removed. Individual pages of the register (list) are now only available via the quick access bar.

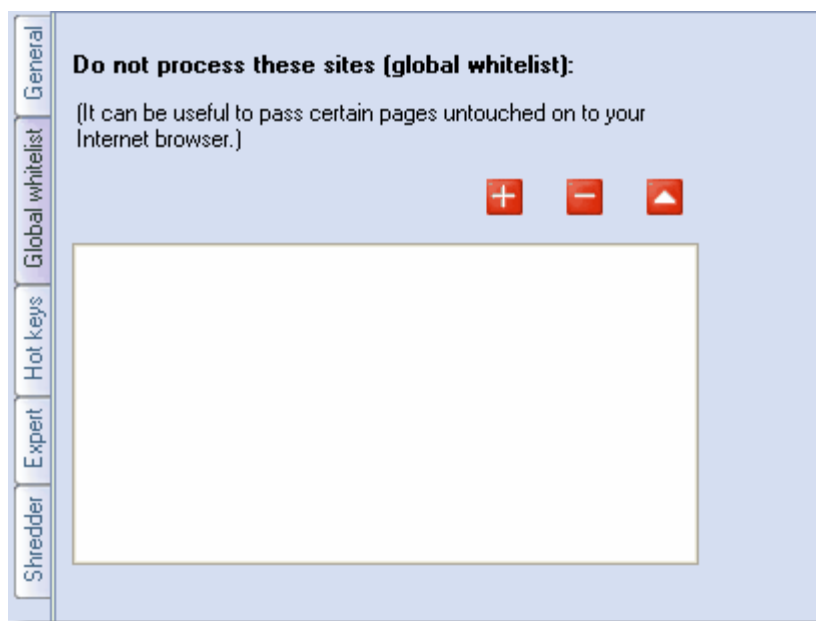
Enable access from Internet Explorer

Creates button on Internet Explorer to call up ArchiCrypt Stealth.

Maximum concurrent tests

Values around 20 are usually possible (please test)

Global Whitelist



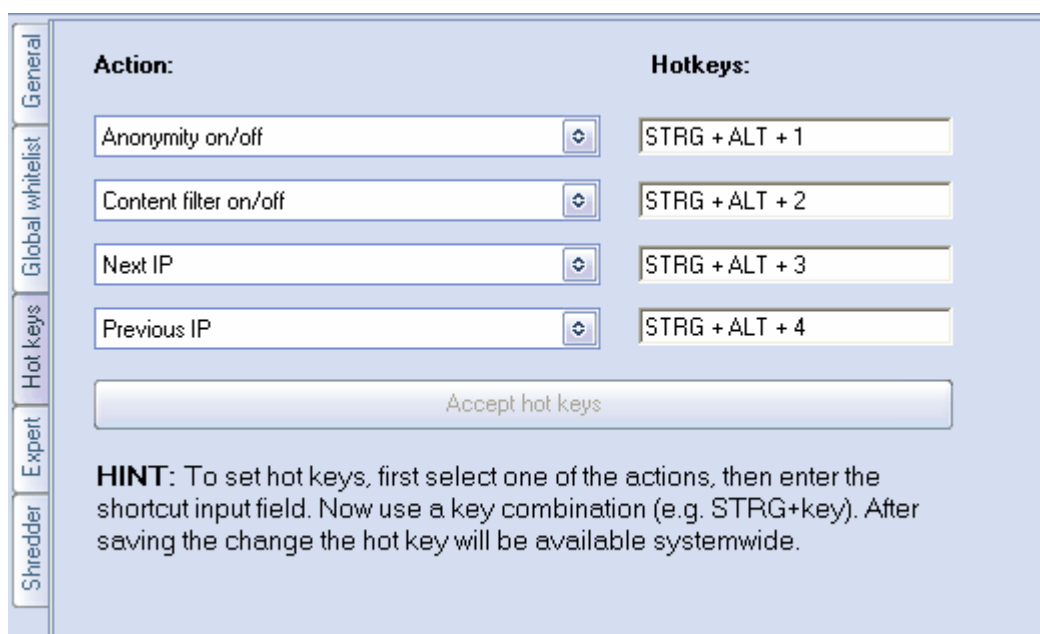
Do not process these sites (global whitelist)

Pages will not be filtered.

Note:

In some seldom special cases, it could be even necessary, to deactivate Stealth!

Hot-keys/shortcuts



You can set ArchiCrypt Stealth so that certain functions are quickly available via hot-keys.

You can choose from the functions:

► **No Action:**

Nothing will be carried out

▶ **Anonymity on/off:**

Anonymisation will be switched on or off

▶ **Content filter on/off:**

The content filter will be switched on or off

➡ **ATTENTION:** *The following hotkeys are only activated when the timeframe for changing the IP address is set to 0!!*

▶ **Next IP:**

The next useable incognito address from the list of anonymous servers will be activated.

▶ **Previous IP:**

The first useable incognito address from the list of anonymous servers which comes before the current incognito address will be activated.

▶ **Delete current IP:**

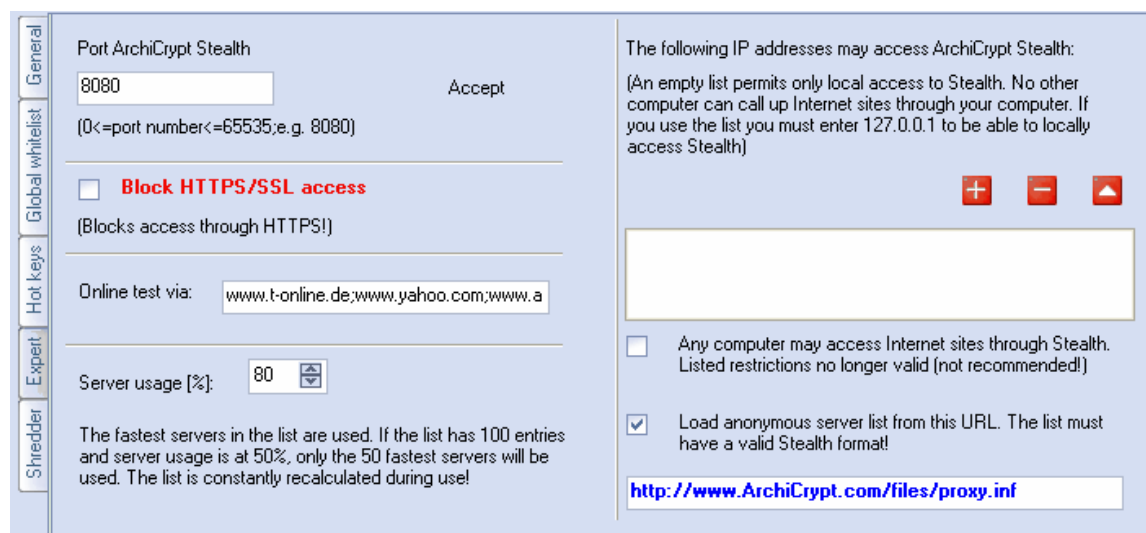
The current incognito address will be deleted from the anonymous server chart.

➡ **ATTENTION:** *The following shortcut and its related functions are only available after installing the full version of ArchiCrypt Shredder version 2 or higher.*

▶ **Shredder:**

Selected Shredder functions will be carried out immediately.

Expert settings



Port ArchiCrypt Stealth

Only change this value if you have problems with the given 8080 value.

Block HTTPS / SSL access

The HTTPS protocol is used when secure data exchange is extremely important.

Major users are online banking, online shopping and, in general, pages where you transmit confidential data. Therefore, for good reasons, ArchiCrypt Stealth allows data with this protocol to be exchanged without impacting it.

Some sites (especially sites that test anonymity) exploit HTTPS access and check your true identity by testing the HTTPS protocol.
By choosing [Block HTTPS/SSL access](#), you can block such attempts.

Online test via

A "ping" will be sent to these sites, to verify that the computer is online. You can enter any page here. Additional pages should be separated by a semi-colon ";"

Server usage

The fastest servers in the list are used. If the list has 100 entries and server usage is at 50%, only the 50 fastest servers will be used. The list is constantly recalculated during use! Performance is best when you set the value at < 70%.

The following IP addresses may access ArchiCrypt Stealth:

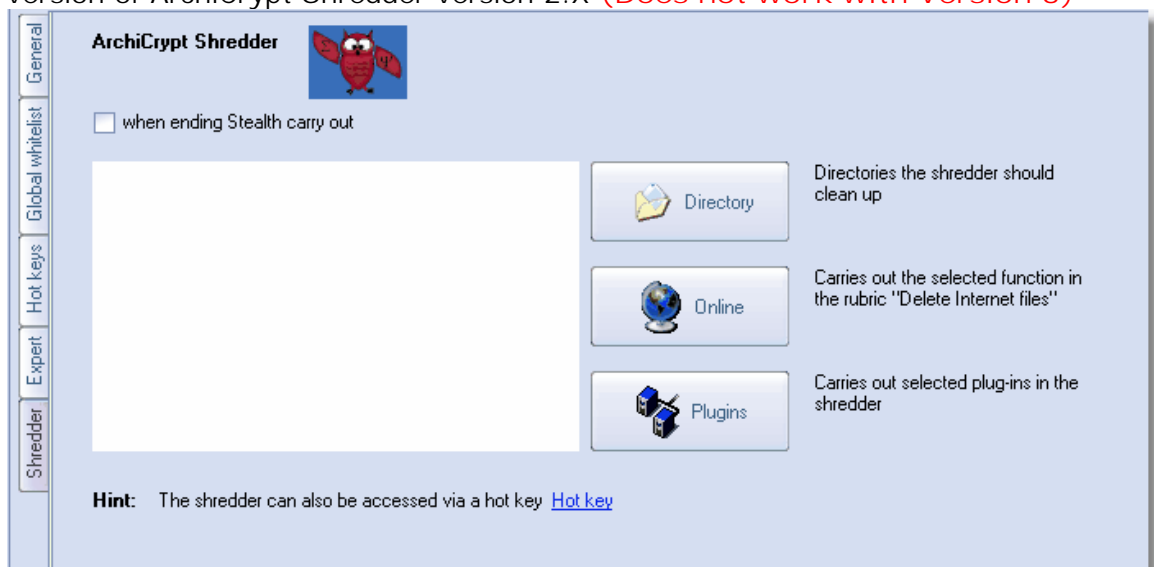
You can set up computers in a network so that they can surf the Internet via Stealth. A description of the set up procedure is in your browser help under the keyword "proxy".

Load anonymous server list from this URL

Load the list of anonymous servers from the Internet address in the entry field. List must be Stealth-conform. Leave blank to use default list from ArchiCrypt site.

Shredder:

➡ **ATTENTION:** The following functions are only available after installing the full version of ArchiCrypt Shredder version 2.X (**Does not work with Version 3**)



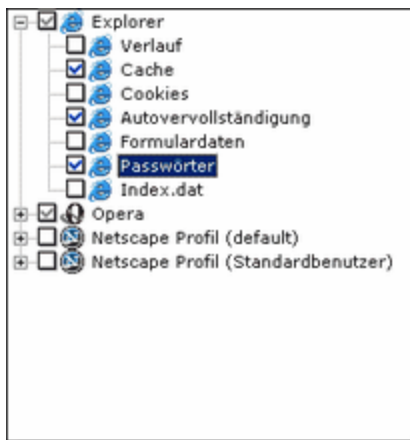
ArchiCrypt Stealth can call up ArchiCrypt Shredder and cause it to delete certain functions. You can select whether the shredding happens automatically when Stealth is shut down, or whether you want it activated by a hotkey (see Hot keys).

Directory:

Select which data should be shredded.

Online:

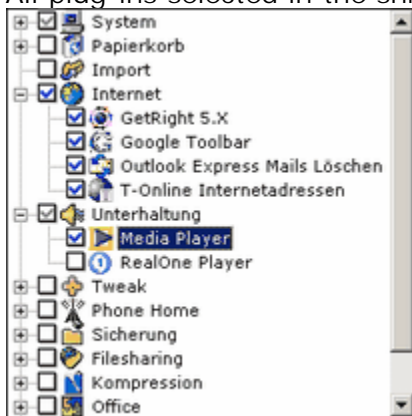
Causes the shredder to carry out the tasks you have selected in category "Online".



Screenshot Shredder

Plug-ins:

All plug-ins selected in the shredder will be carried out.



Screenshot Shredder

5 Status-Monitor

The status monitor is responsible for constantly informing you on the status of the ArchiCrypt Stealth functions.

The colored bars near the anonymisation and content filter symbols indicate whether each function is on or off.

RED means: Function deactivated, not available!

GREEN/BLUE means: Function activated and available!



Status-Monitor with activated Content filter

Throughput shows whether your browser is sending or receiving data.



Status monitor with activated anonymisation and content filter.

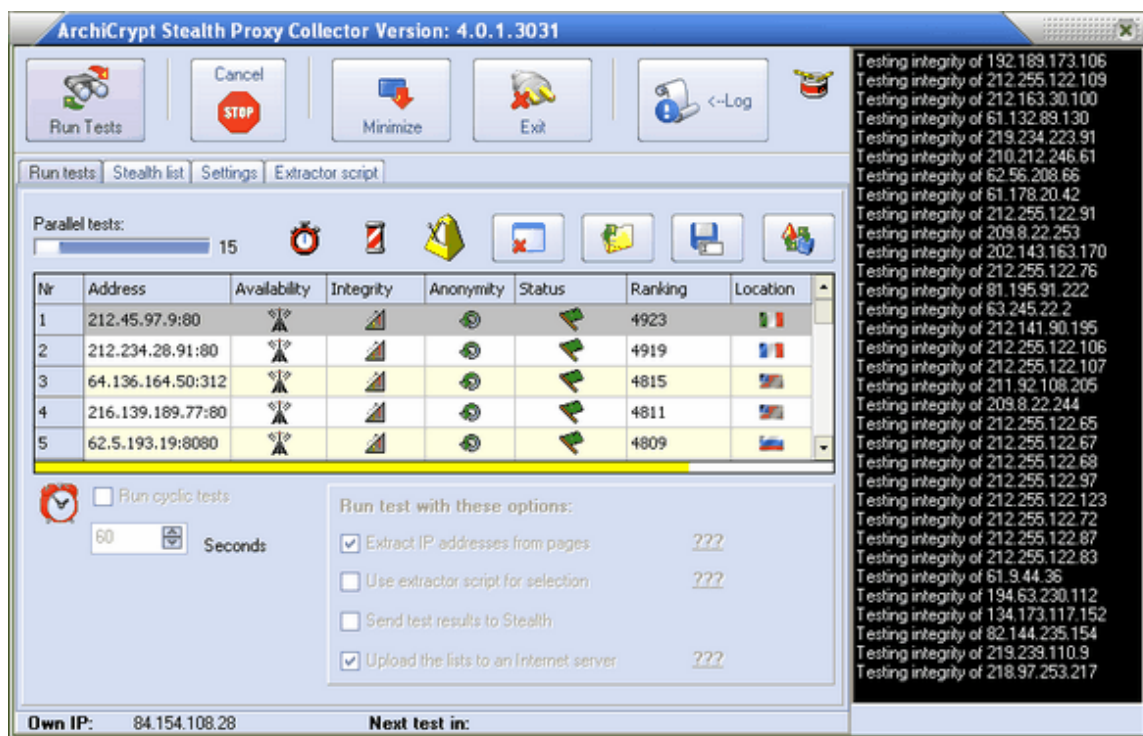
When the anonymity function is activated, the Incognito IP shows which IP address you are surfing with in the Internet. Location displays where the computer is, whose IP address you are currently surfing with in the Internet.

6 Proxy-Collector

6.1 Overview

➡ **ATTENTION:** *The Proxy Collector is an additional tool, which is not absolutely necessary for operating ArchiCrypt Stealth. Proxy Collector is not part of Stealth, but must be purchased separately!*

The Proxy Collector is responsible for collecting the so-called anonymising proxies, testing their functioning, properly preparing them for Stealth and, if necessary, passing them directly on to ArchiCrypt Stealth or uploading them via FTP and making them available for use by a larger circle of Stealth users.

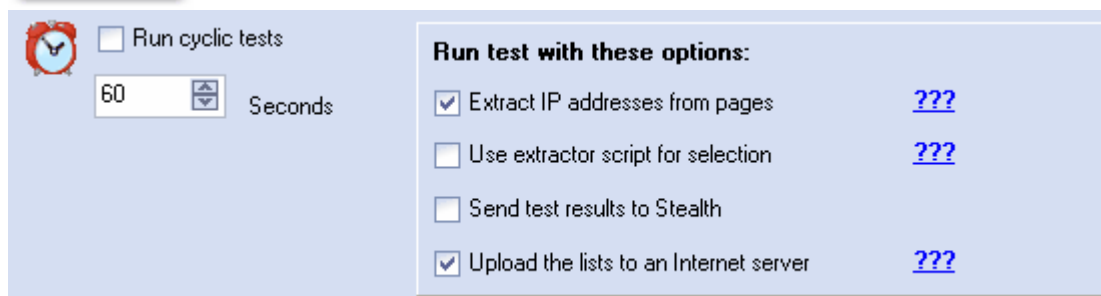


see also Functions

6.2 Function overview

Testing the main function Run Tests is started with the [Run Tests](#) button.

Test settings are entered under [Run test with these options:](#)



► If [no option is selected](#), the list ArchiCrypt Stealth is currently using, will be tested.

► [Extract IP addresses from pages](#) There are numerous Internet sites, which provide lists of anonymous servers. At the same time, the lists contain very many sub-par servers or servers that are not anonymous. In addition, anonymous servers

are often only briefly available. ArchiCrypt Proxy Collector can automatically visit specified sites and extract server information from them. Pinpoint the sites, from which Proxy Collector should extract data under Settings-"Address Sites".

➔ **ATTENTION:** *The IP addresses must be available in the IP address format: Port (e.g. 212.34.0.3:8080 or 80.79.6.12:6312)*

After the IP addresses have been collected, the servers will be tested to see whether they actually produce anonymity.

▶ **Use extractor script for selection**

If you know the program language Delphi well, you can write your own routines to extract the information from Internet sites.

▶ **Send test results to Stealth**

If ArchiCrypt Stealth is activated, you can transfer the newly found and tested lists to Stealth during operation. Stealth will begin to use these new lists immediately. This method is ideal if you want to constantly supply Stealth with "fresh" lists.

▶ **Upload the lists to an Internet server**

You can cause Stealth to place the tested lists on an Internet server via FTP Upload. The list is then further available for you and other insiders. (See also Stealth Liste)

Run cyclic tests

Set an interval for Stealth to test a list. All the tasks that were specified under [Run test with these options](#) will be repeatedly carried out.



Tip: You can continue to surf anonymously with ArchiCrypt Stealth, while Proxy Collector constantly creates lists with up-to-date proxies in the background.

Anonymous Server List

The chart offers several additional functions.

Parallel tests:

Nr	Address	Availability	Integrity	Anonymity	Status	Ranking	Location
1	212.45.97.9:80					4923	
2	212.234.28.91:80					4919	
3	162.38.132.8:80					4902	
4	212.234.28.89:80					4899	
5	195.137.237.197:8					4888	



Deletes the complete chart



Loads a proxy list (must have valid Stealth format)



Saves the current list in a valid Stealth format



Sends the list in its current form to Stealth. Stealth accepts the untested list.

6.3 Settings

General

Maximum number of parallel tests

20+ (please test)

Automatically increase the list version when creating

Automatically increases the version number of the list

Test priority

The higher the test priority, the harder your system will have to work.

Online test via

A "ping" will be sent to these sites, to verify that the computer is online. You can enter any page here. Additional pages should be separated by a semi-colon ";"

Address sites

List of sites to inspect. A prefixed ";" prevents the site from being inspected.

Please, give each address its own line.



TIP: You can also leave the field blank. ArchiCrypt Stealth Proxy Collector then accesses an internal list that contains IP addresses which are usually in the desired format.

FTP

The settings are necessary when you want to automatically place anonymous proxies, which have been tested and contain a valid Stealth format, on a server in

the Internet.

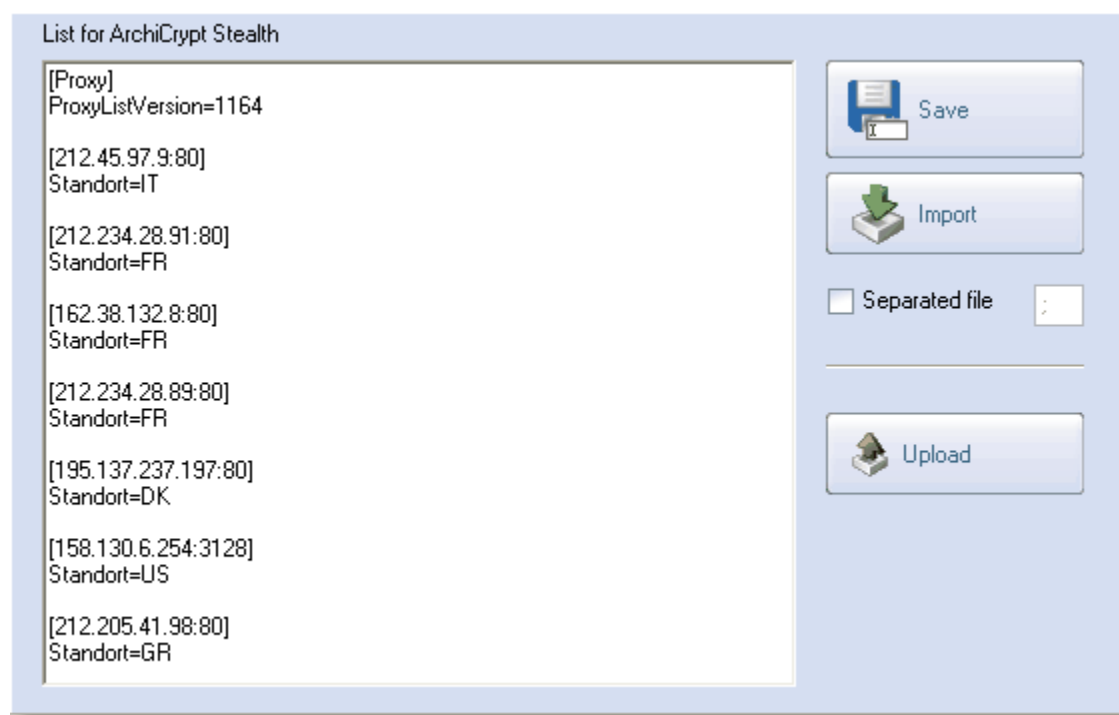
➔ Important: *Always start the path with a "/" and omit the path when you enter the file name.*

You can check the correctness of your settings with the function [Test](#).

You can place specific [minimum requirements](#) on the number and performance of the anonymous servers. This function is very helpful when you want to automatically place the list on your server via FTP upload. You avoid having poor or empty lists appear on your server.

6.4 Stealth List

ArchiCrypt Proxy Collector can not only create lists that conform to Stealth, but in some cases also convert existing lists to a valid format ([Import](#)). The list must contain IP addresses with the format IP address:port (e.g. 212.34.0.3:8080 or 80.79.6.12:6312) and are separated by specific separators. The new file can be stored under [Save](#). With [Upload](#) you send the list, exactly as pictured on the left, to your server. Any settings for minimum number and number of best servers will be ignored! (see Settings).



7 Frequently asked questions (FAQ)

Following you will find several important tips for correcting possible problems.

➔ Important: *Almost all of the errors that appear in our support program, point back to an*

incorrectly functioning [firewall](#), which prevents Stealth from accessing the Internet. Therefore, be absolutely sure that any firewall you may be using gives Stealth the necessary communication rights. If you use a [personal firewall](#), you must grant ACStealth4.exe (installation folder) and TestProxies.exe (for Proxy-Collector) complete access rights.

In order to determine whether the error lies here, you should completely switch off your firewall for a short time. Sometimes it was even necessary to uninstall the firewall. Sometimes it will suffice to delete all Stealth specific rules.

If the error no longer appears, the problem lies with the firewall configuration – that needs to be adapted / reconfigured.

From time to time, the source of the problem is also found in a hardware firewall. Be aware that Stealth requires the "ping" protocol (ICMP), in order to determine your online status. So please enable the Ping(ICMP) protocol.

Content filter does not function

Slow / no page reproduction with anonymity function

IP address in spite of anonymity

Browser no longer displays pages

Program XY does not work, if anonymization is activated

[Content filter](#)

Delete browser cache (temporary Internet files)

[Slow / no page reproduction with anonymity function](#)

ArchiCrypt Stealth uses so-called anonymous proxies. We choose these proxies very carefully and update the list regularly. But because we have no influence over the computers and their administrators, it can happen that the proxies are suddenly shut off or the proxy content itself is blocked. As a result, pages are reproduced very slowly or, in some cases, no connection to the page is created at all.

If a proxy causes errors, simply delete the appropriate entry from the list of anonymous proxies.

- Mark the entry
- Click the right mouse button
- Choose "delete entry" from the menu

[IP address in spite of anonymity](#)

Switch off active contents (ActiveX) and scripting in your Internet browser. Be sure to block HTTPS/SSL access.

(see Settings in manual)

[Browser no longer displays pages](#)

Re-start Stealth and then exit Stealth again. Possibly switch the anonymity function off, if no high-performance proxies are available.

[Program XY does not work, if anonymization is activated](#)

Please register this application in [Settings application behavior - Global whitelist - "Do not touch traffic of these applications"](#).

Index

- A -

- Accepted languages 11
- Address sites 22
- adminstrator 2
- adminstrator privileges 2
- anonymisierende Proxies 19
- anonymising proxies 19
- Anonymity 3, 5
- Anonymity check 3
- Anonymity on/off 14
- Anonymous servers 12
- anonymously via one single server 5
- Automatically increase the list version when creating 22
- Automatically load (update) list with anonymous proxies at program start 14

- B -

- Beim Testen 20
- Block HTTPS / SSL access 14
- Blocking Incoming Cookies 7
- Body filters 8
- Browser and operating system 11

- C -

- Changing Cookies to Session Cookies 7
- Connection data 11
- Content filter 3, 5
- Content filter on/off 14
- context menu 12
- Cookies 11

- D -

- Dauertest durchführen 20
- Delete current IP 14
- Directory 14
- Do not process theses sites 14

- E -

- Enable access from Internet Explorer 14
- Exit 3
- Expert settings 14

- F -

- Filter all ActiveX components 10
- Filter known spyware adware and dialers 10
- filter on / filter off 12
- filtering and manipulating information 5
- FTP 22
- FTP upload 22

- G -

- Global Whitelist 14

- H -

- Hauptfunktion Testen 20
- Header 11
- HeaderIN filters 8
- HeaderOUT filters 8
- Help 3
- Hot-keys 14

- I -

- Identity 11
- IP-Adressen aus Seite extrahieren 20

- L -

- Liste anonymer Server 20
- Load 12
- Load anonymous server list from this URL 14
- Load definition file 10
- Load new proxylist 12
- local proxy 3
- Log 11
- Logging on/off 11

- M -

manipulate Cookies 5
manipulating 8
Maximum concurrent tests 14
Maximum number of parallel tests 22
menu bar 3
Minimize 3
minimum requirements 22

- N -

Next IP 14
No Action 14

- O -

Online 14
Online test via 14, 22
Only show quick access bar 14

- P -

Permit cookies from these sites 7
Personal Firewall 2
plug-in editor 8
Plug-ins 8
Port ArchiCrypt Stealth 14
Previous IP 14
Proxy Collector 19
Proxy-Collector 19

- R -

Requesting page 11

- S -

Save 12
Send cookies to these sites 7
Server usage 14
Setting up Stealth 3
shortcuts 14
Shredder 14
Spyware 10
Standard Browser 14

Start automatically with Windows 14
Status monitor 5
Status-Monitor 18
Stealth Central 5
Stealth Server 12
Stealth Test 3
System scan 10

- T -

Test priority 22
Testergebnis an Stealth senden 20
The following IP addresses may access ArchiCrypt
Stealth: 14

- U -

Upload der Liste auf einen Internetserver 20

- W -

Website blocker 6
Who passed the request 11

Endnotes 2... (after index)

Back Cover