All-in-one safe communication solution

Handy Multichannel Proxy

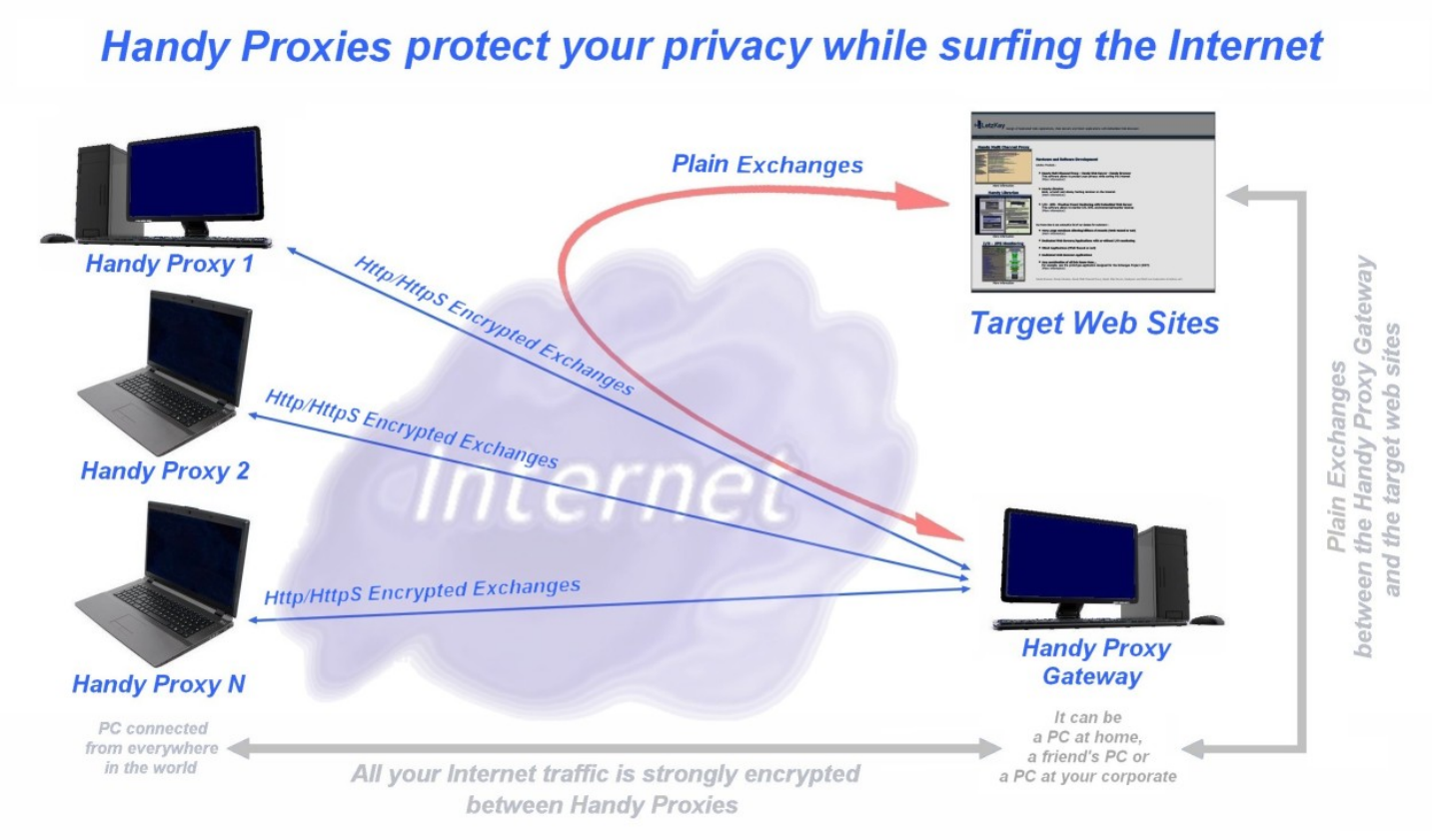
Handy Messaging Server

Handy Web Server

Handy Browser

Manual

Version 1.0



Handy Multichannel Proxy - Handy Messaging Server
Handy Web Server - Handy Browser

Manual **Version 1.0**

1. Introduction to the Handy Proxy Applications

This solution is the ideal protection service for people who have to access the Internet via their PC or Windows tablet from places that could be "hostile". It is also the ideal service if you want to send encrypted e-mail messages without using a third-party service or to provide web services with an access strictly limited to duly authorized persons thanks to integrated encryption functions.

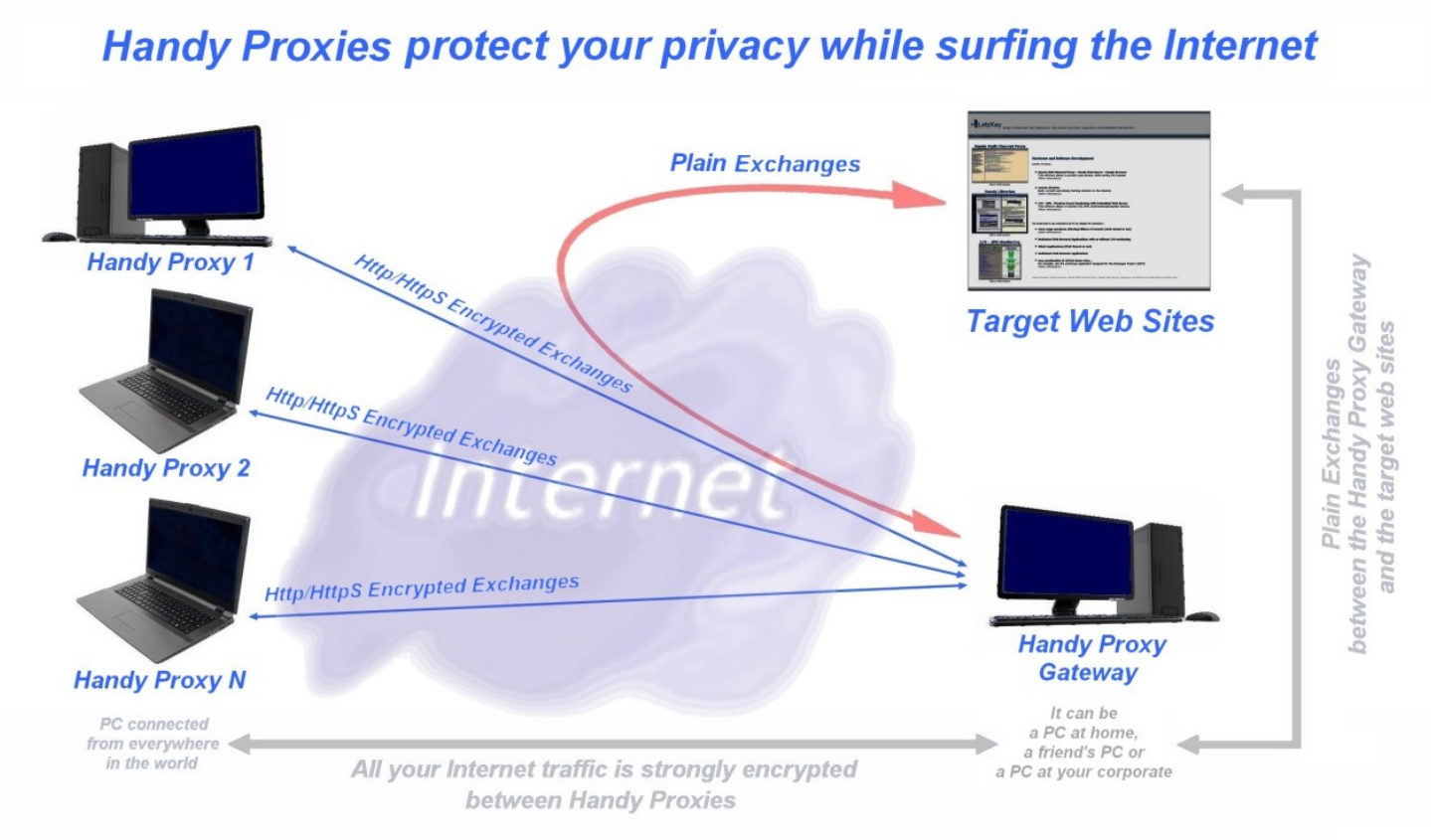
Your privacy is obviously important and whether you are a private user, an IT professional, an Internet provider, a manager or someone having to protect information against piracy, our software will provide the missing link in your configuration.

Thanks to fully encrypted data transfers between 2 Handy Proxies, you will be able :

- to avoid your sensitive and confidential data as your login and password to be tracked or your data to be analysed/sold/stored for a fraudulent use if you connect to the Internet from a WiFi public access point, for example ;

- to avoid your moves to be tracked (when you connect from a place outside your home or office) by the numerous sites that use behaviour data for marketing purposes or by ill-intentioned people ;

- to access the Internet openly only from your home or office, even if you are outside or abroad.



You can install your Handy Proxy configuration on your PC's hard disk or on a USB key. In this case, all your parameter files and all your messages will be stored in the key and nothing will be saved on the host PC. Similarly, the Chrome-based Handy Browser which is provided in standard will save your navigation data (cache file) where you installed it, i.e. on a USB key. This type of installation allows you to use your configuration securely and privately where you want to do it.

This possibility of installing your Handy Proxy on a USB key will allow you, for example, to perform e-banking operations on a PC available in a public, occasional or unusual place without taking the risk of leaving traces of your operations and/or access while securing them via encryption.

Thanks to the Handy Messaging Server integrated into the Handy Proxy and thanks to the Handy Email and Handy Messenger applications, you will be able :

- **to communicate with your addressees in a totally secure way, independently from any Internet provider or chat or e-mail service and even from the Internet itself since your messages will be encrypted : the Internet becomes a simple data carrier (these functions do not use POP3, IMAP or other protocols in order to be completely autonomous from them). The purpose of these applications is to maintain strict confidentiality of your messages, which is imperative namely for companies.**

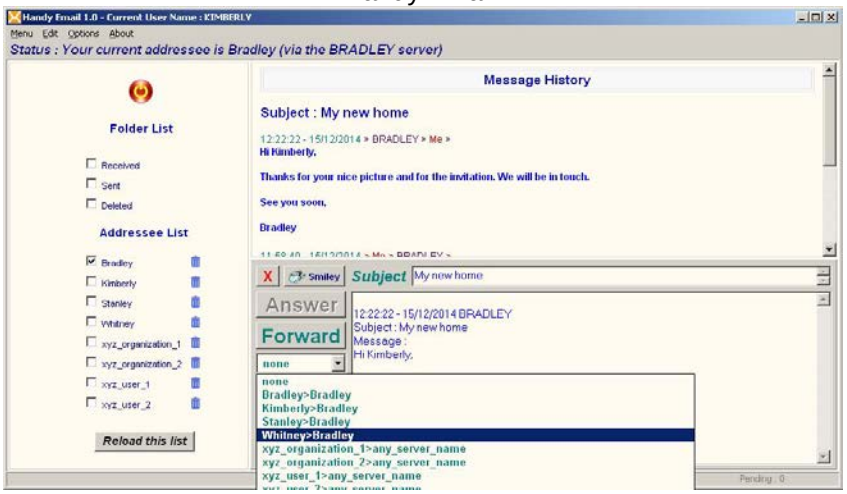
- to easily create your private messaging service for your family, association or company. This service will be available inside your local network and/or via the Internet anywhere in the world (WiFi access,…).

- to send fully encrypted messages and attached files in client-server mode (from computer to computer), allowing complete confidentiality in your private or professional exchanges. A filter checks the kind of attached file, making impossible to send for example files that start automatically. Apart from this, all kinds of files can be sent as attachments (doc, docx, PDF, picture, …).

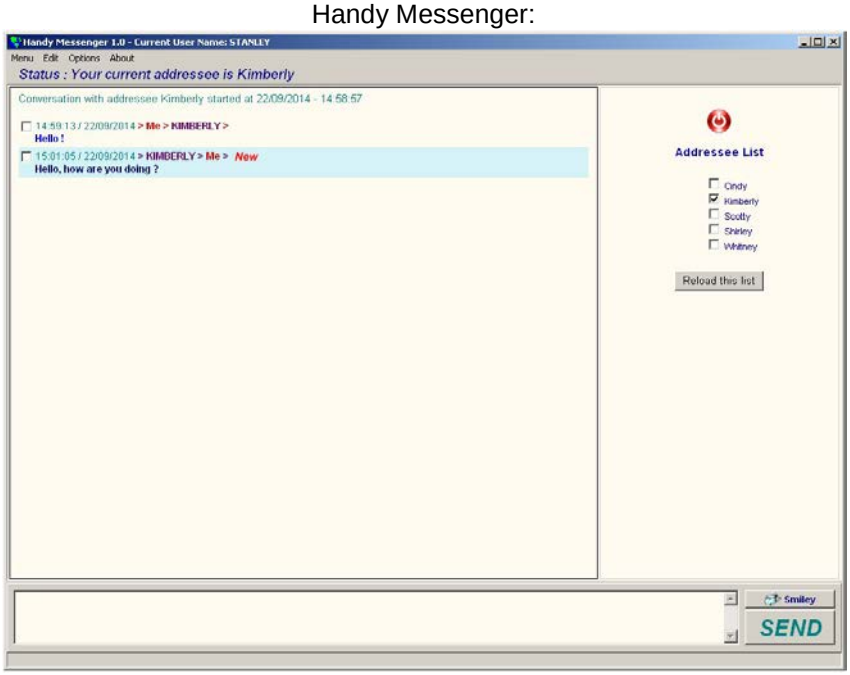
- to use these tools without having to install an SQL database configuration or other complicated modules, since the Handy Messaging Server takes care of everything for you (everything is ready to work after the installation of the package). **This function installs itself automatically and can thus be used by anyone, you will just have to define your addressees to be able to use it immediately after installation.**

Moreover, a safety check is performed automatically when the messages are created. Thanks to this, they cannot spread viruses via encapsulated Javascript micro-programmes or other.

Handy Email:

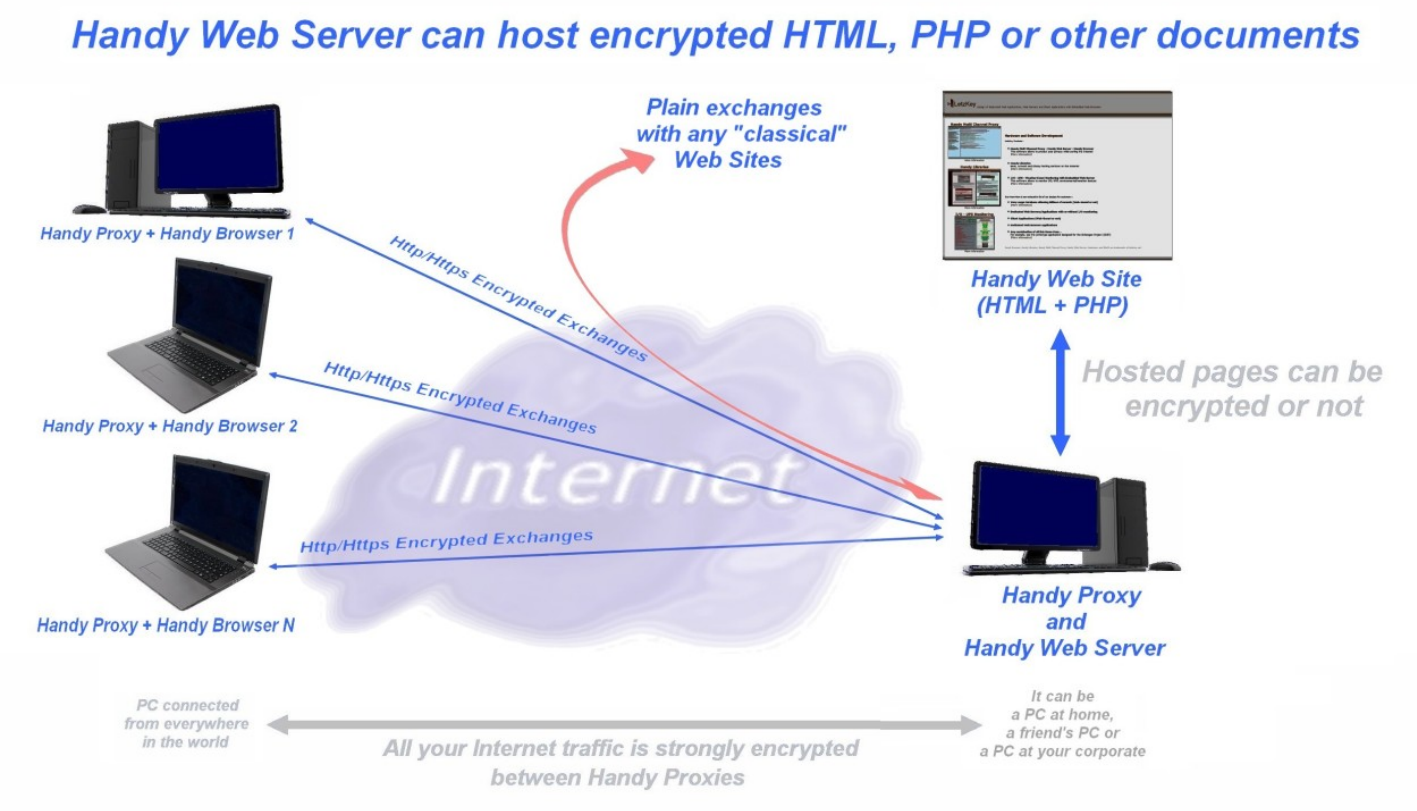


Handy Messenger:

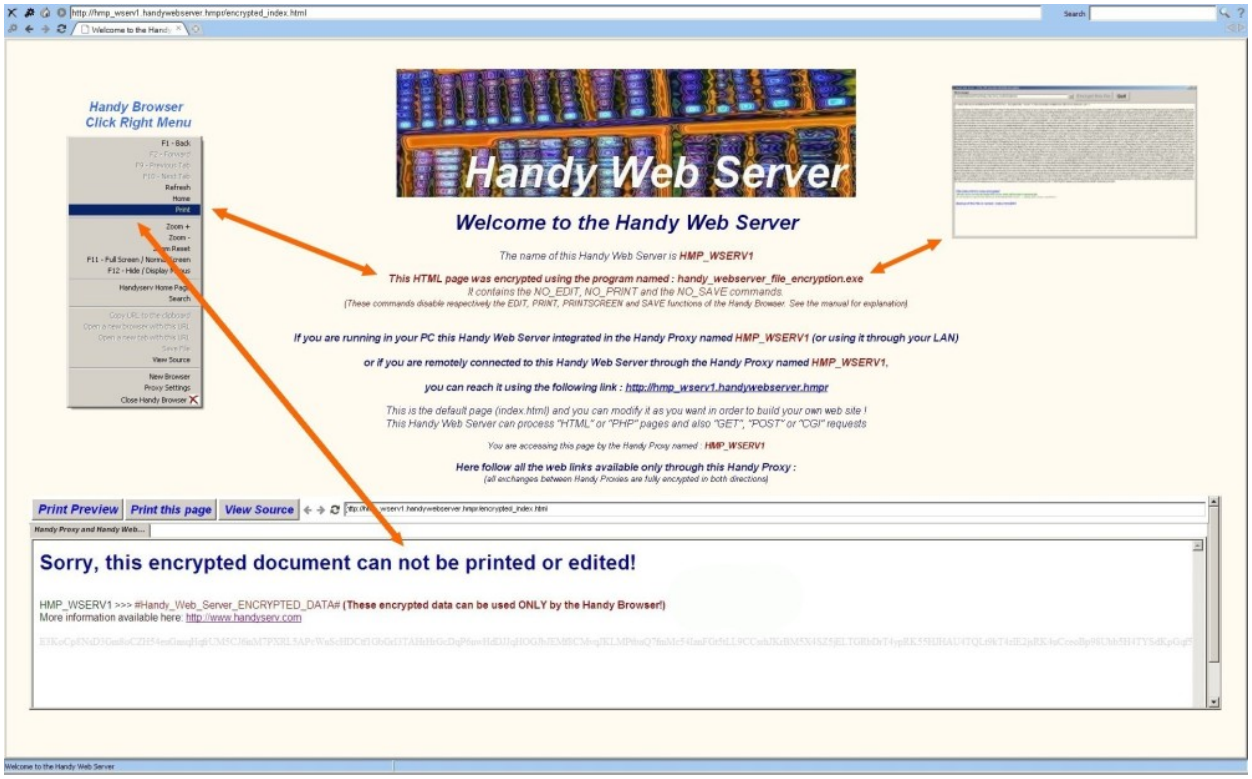


Thanks to the Web Server integrated in the Handy Proxy and the Handy Browser provided by this solution, you will be able :

- to create and host your own web site and decide to make it accessible to some people only or to make it public ;
- to encrypt your HTML, Javascript or PHP pages to protect them against any editing, printing or visualizing ;
- to automatically get a domain name for your web site like this : http://any_name.handywebserver.hmpr ("public" domain name for other Handy Proxy users) or http://any_name.hmpr (private domain name).



Handy Web Server With Encrypted Pages



Handy Browser with Encrypted Pages

Our Internet security solution will also allow you :

- to easily manage the people authorized to access your shared Handy Proxy installed in your home or office ;
- to share between family members, friends or colleagues your software license up to the maximum number of connections allowed by this license ;
- to define up to 10 different connections to other networks, services or other Handy Proxies according to a target web site, a group of web sites or an Internet browser ;
- to define access priorities or to forbid access to web sites you do not want your family or colleagues to visit ;
- to avoid consequently some web sites to reach your browsers or to install malware way before your antivirus detects them ;
- to easily switch to off-line mode while you are away from your desk, and this for all browsers and web pages open in your Windows session.

Our Internet security solution is also dynamical since :

- each Handy Proxy uses its own and unique encryption method and each Handy Proxy can use its own private encryption key (defined and modifiable only by the configuration's owner) ;
- the Handy Proxy encryption method automatically changes every 4 hours, in a way which is transparent to the users.

Moreover :

- all 24 hours, all running Handy Proxies completely recalculate the way they encrypt their data transfers with the other Handy Proxies ;
- the HTTPS/SSL exchanges can be over-encrypted in order to increase your data protection ;
- for 2 Handy Proxies which are interconnected and exchanging encrypted data, Internet is merely used as a data carrier between 2 points defined by their IP addresses. ALL exchanges between these 2 points are then strongly encrypted, whether it be outgoing HTTP or HTTPS requests or incoming data and web pages.

All these functions and encryption methods make unconceivable the possibility to listen to your Internet activity or to have your sensitive data hijacked (as banking data, login, password,...) when you connect to the Internet from an unsecure or simply unknown place.

However, a Handy Proxy can be used in all cases, even at home or at the office, with or without a connection to another Handy Proxy, since the useful web site filtering functions and other functions will still be usable.

Moreover, our solution of integrated web site in the Handy Proxy with or without encryption of hosted pages is ideal to allow you to create your HTML, Javascript and PHP web sites protected out of the "classical" Internet and to gain total control on what is made of them and who is allowed to visit them.

This encryption function of web pages only accessible via a Handy Proxy also allows to protect your intellectual property and/or your investments and/or your data against any person who is not authorized to access them. You can then create "family" or "private corporate" web sites that can be accessed from everywhere in the world as long as you authorized it.

As an additional asset for companies and organisations, we can provide the hosting of your own Handy Proxy users database to make your configuration completely independent from the default one. You would then have a configuration tailored to your needs with all the above-mentioned functionalities. Again, only the persons you have authorized to use your specific environment will be able to access it.

1.1. System requirements

Microsoft Windows 2000, XP, 7, 8
200 MB available hard disk space
256 MB RAM
Microsoft Internet Explorer 6 or newer

1.2. Installation

The Handy Proxy package is available from the Handyserv website (http://www.handyserv.com). You can download and install it very easily as any other software package.

We guarantee that our programs and modules are adware, malware and virus free as long as they are downloaded from within our web site. To help you check this, our web site provides an MD5 checksum allowing to check whether the module to download is ours and was not modified. Moreover, the different programs (.exe) provided in our package are also protected by an MD5 checksum which, in case it is not verified at the launching of one of our programs, will block it and display an error message.

Icons will be created at the installation. We invite you to add the Handy Proxy icon to the Windows startup folder, which will launch the Proxy automatically.

1.3. Quick start & Overview of Handy Proxy powerful functionalities

Here is how to launch Handy Proxy and its other functions for the first time.

1.3.1. How to start as a user

- Download the package from within our web site and follow the usual steps to install it. Launch Handy Proxy.

- When Handy Proxy runs for the first time, it will ask you to introduce the name of your configuration. If the name you choose is free, it will be accepted. Handy Proxy will then be in « Proxy disabled » mode. Click on the button in the upper left corner (« Proxy disabled ») to change this mode into « Proxy enabled ». If your Internet connection is not active, Handy Proxy will inform you of this. Otherwise it will wait for traffic to flow.

- When Handy Proxy is in « Proxy enabled » mode for the first time, it will realize that Windows does not route the Internet traffic through it. Handy Proxy will warn you of this via a message providing you the right parameters to give to Windows, and afterwards it will open the « Internet properties » Windows menu allowing you, via the « Network parameters » item, to flow your Internet traffic via your Handy Proxy. For more information, please refer to the following link :

  Change proxy server settings in Internet Explorer :
  http://windows.microsoft.com/en-us/windows/change-internet-explorer-proxy-server-settings

  Some browsers do not automatically follow Windows proxy settings, as for example Firefox. You will then have to indicate manually to these browsers that they have to use Windows default proxy settings.

- From now on, your Handy Proxy is ready to work and is configured by default. If you want to use Handy Email and Handy Messenger, you now have to configure the messaging server(s) you will connect to as well as your addressees list. The Handy Proxy screen will indicate that you can define your configuration as a messaging server, but before using this function, we invite you to carefully read the next chapter.

1.3.2. How to start if you want your Handy Proxy to be an Internet traffic router and/or a messaging server for other users

After having set up the basic configuration explained above, here are the steps to follow if you want to share your configuration as a secure Internet traffic router and/or as a messaging server (Handy Email and Handy Messenger) :

- First and foremost, you have to define a static IP address inside your network to give a stable address to the configuration. Otherwise this address will change dynamically, preventing your addressees to retrieve your configuration. You will have to use the Windows functions allowing to make your PC's IP address static.

In order to help you to do so, here is a link to a website explaining how to proceed for all existing Windows versions :

Setting a Static IP Address in Windows :
http://portforward.com/networking/staticip.htm

- Now that your PC has a static IP address, you have to make it accessible to those of your addressees who are connected to the Internet and are therefore out of your local network. In order to do this, you have to set up your Internet router so that it reroutes your addressees' traffic to your PC connected to a static IP address in your network. Concerning this setup, we invite you to read chapter 2.1 « Making your Handy Proxy accessible for other users ». This chapter explains step by step, with links to tutorials, how to proceed according to your own router.

- Now that your PC has a static IP address and that it can be accessed from the Internet via your router's NAT functions, it can now be securely accessed by your addressees, either connected to your local network, or via the Internet.

Your configuration is now up and running, either as a user or as a user + server mode. If you wish to fine-tune your configuration and increase its security level, we invite you to read the chapter 9 of this manual which is dedicated to the available configuration files (the default password is 1234 for sensitive files, those can be modified only via the Handy Edit programme that was especially designed for this purpose).

If you modify the basic parameters of your Handy Proxy, we invite you to close the application and start it up again. If you change the filter or user configuration files you do not have to restart your Handy Proxy since the button « Reload URL filter and other files » can be used. Moreover, as a user, you can open a session under different names and thus under different connection configurations to other users.

Please note that each Handy Proxy configuration can become a messaging server. However, we invite you to create only one server inside your family, association or company in order to ease the configurations of the different users to whom you would have to send the messaging definition file. However, it is possible to parameter this file to allow you or your addressees to communicate with several servers (see explanations in chapter 9 of this manual). For example, you could have a Handy Messaging Server inside your company while being connected to one or several other servers of the same kind in other organisations or subsidiaries you want to communicate with in a safe way. The situation is similar for the Handy Web Server function whose access is strictly controlled and that will also allow you to share data in a safe way with people you will have duly authorized to access them.

Attention : if your configuration is used as a secure Internet traffic router and/or as a messaging server, you cannot modify the name of your Handy Proxy since your addressees will use it to connect to your configuration. Indeed, if you modify the server name that was previously included in your addressees' configuration files, they will not retrieve you anymore and your server will be considered as not available ! We therefore invite you to choose a server name once and for all, so that your addressees will not have to modify their configurations files.

1.3.3. What is the purpose of your Handy Proxy's 10 channels and how to use them optimally

Now that you are configured as a user and/or server of your Handy Proxy, let's look further into what you can do thanks to the 10 available channels by means of an example.

Your various Internet browsers can have their traffic wholly or partly routed to one of these 10 channels (or « output channels »).

Each channel can point either to the Internet directly (channel 0 by default) or to another Handy Proxy or another network or even to another service acting as a proxy itself.

Let us take the example of the Tor network. A Handy Proxy cannot directly interface to the Tor network since it must interface in « SOCKS » mode while a Handy Proxy only knows the « http/https » interface. Consequently, in order to reach the Tor network, a third-party interface as the one provided by programmes as Surfing Tunnel or ChrisPC Proxy must be used. Another service which can interface with your Handy Proxy is the UltraSurf programme that gives access to remote proxies. There are of course other existing services, we cannot list them all here.

Here is a concrete example of an advanced use of the powerful Handy Proxy functionalites :

Let us imagine that you want to interface to the three above-mentioned services in addition to connecting to two other Handy Proxies, one of them being on-line in your house and the other one being on-line at your office (we assume that you are outside of these two places using your laptop).

Let us imagine also that you do not want to access Handyserv databases directly for security reasons according to the place where you are (Wi-Fi hotspot for example). Moreover, in this example, you want your Handy Proxy to be a server for other users and you want to pass through a web page of your choice to retrieve your IP public address without using

the service provided by Handyserv by default (please note that your IP public address is mandatory if you want to share your configuration with other users and/or be a messaging server). **This IP address is the one you are allocated by your Internet provider, and by no means the IP address that would appear via a service as Tor or similar,** since this address does not point to your Handy Proxy, thus preventing it from being used by other users who would see it as « absent ».

To reach a solution as the one described in this example, you have to configure your Handy Proxy and set it up adequately. Please refer to chapter 9 of this manual, Master configuration file and other configuration files.

In our example, when you start your Handy Proxy programme, you get on the screen the following information :

```
*** Your public IP address is :  (found by calling this link : http://)
*** Updated channel list at    : 29/12/2014-13:45:37
*** Fetching the Multichannel HTTP/HTTPS Proxy Configuration and Users Database using the following address and port : 127.0.0.1:6006
This configuration can be shared  - Geolocation results for this Handy Multichannel Proxy : Country=  Country Code=  Continent Code=
*** From server side, your IP address appears as :  - Geolocation : Country=United States; Country Code=US; Continent Code=NA/North America
Checking proxy channel ID 0 (Default_Channel_ID0) ==> Available <Internet>  (29/12/2014-13:45:40)
Checking proxy channel ID 1 (Surfing_Tunnel_Channnel_ID1) ==> Available (Surfing Tunnel Channnel ID1) (29/12/2014-13:45:41)
Checking proxy channel ID 2 (ChrisPC_Proxy_Channel_ID2) ==> Available (ChrisPC Proxy Channel ID2) (29/12/2014-13:45:43)
Checking proxy channel ID 3 (UltraSurf_Channel_ID3) ==> Available (UltraSurf Channel ID3) (29/12/2014-13:45:43)
Checking proxy channel ID 4 (Channel_ID4) ==> Not Used (29/12/2014-13:45:43)
Checking proxy channel ID 5 (Channel_ID5) ==> Not Used (29/12/2014-13:45:43)
Checking proxy channel ID 6 (Channel_ID6) ==> Not Used (29/12/2014-13:45:43)
Checking proxy channel ID 7 (Channel_ID7) ==> Not Used (29/12/2014-13:45:43)
Checking proxy channel ID 8 (Channel_ID8) ==> Available  [Daisy-Chained with:  (29/12/2014-13:45:43)
Checking proxy channel ID 9 (Channel_ID9) ==> Available  [Daisy-Chained with:  (29/12/2014-13:45:43)
*** End of the channel list *******
```

Extract from your Handy Proxy main screen

On this screen, you can see that your Handy Proxy retrieved your IP public address from a web page defined in the « Link_to_fetch_the_Multichannel_Proxy_Public_IP_Address » parameter (« Multichannel_Proxy_Master_Config.def » file, click on the button below, default password : 1234).

You also can see that Handy Proxy was instructed (via the same file) to reach Tor in order to access Handyserv databases by means of the « Fetch_Multichannel_Proxy_Database_Address/Port » parameter in order to make it point to the address and port of the interface programme Surfing Tunnel (to the Tor network), which in this case can be found at address 127.0.0.1 and port 6006.

Using the Surfing Tunnel interface and the Tor network, your Handy Proxy appears under an IP address which is different from its public address. This information is communicated to you under the form of a geolocalisation which indicates that you localisation was retrieved via your public IP address, and under which other IP address you appear to the Handyserv server. Please note that all these exchanges are duly coded and encrypted.

ZqWare's Surfing Tunnel screen

On your Handy Proxy main screen you can see the 10 available channels, where they point to and the result of a connection test. In this example, 5 channels are used. Three of them point to services that are different from a direct access to the Internet (reserved to channel 0), and channels 8 and 9 point to two other Handy Proxies configured to be routers (they are considered as accessible).

According to the chosen configuration, your various Internet browsers can have their traffic routed to one of these 10 channels. But default, channel 0 is selected, which means that your browsers will access the Internet directly unless they are instructed otherwise via the configuration and filter files (see chapter 9 of this manual). You can route all the traffic of a browser to a defined channel, or route only a part of its traffic.

Let us take an example according to which you want to route the Facebook, Google and YouTube traffic, for all browsers, to one of the 10 channels of your Handy Proxy. In order to do that, edit the « Handy_Proxy_Routing_Table.def » file and indicate, according to a syntax you absolutely have to respect (as well as for all other configuration files), the names or name parts of the web sites you want to force the routing, as follows in our example where access to Facebook will pass through channel 0 and traffic to Google will pass through channel 8. Your Handy Proxy applies a scale of priorities ; this one supersedes all others except the interdiction to access a determined web page which applies in the first place.

Proxy_Routing_Table.DEF

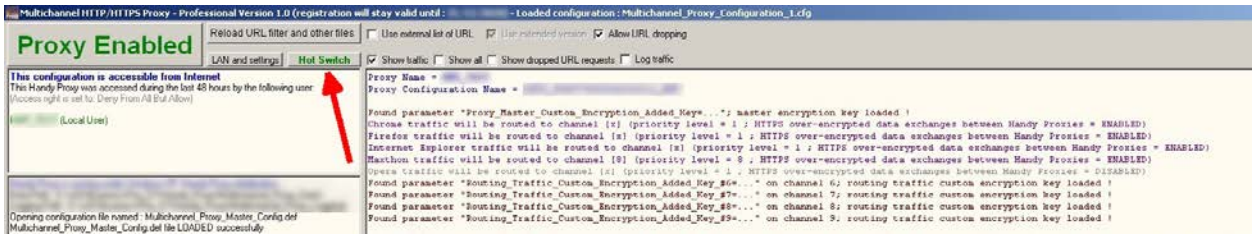
```
1
2  //=============================================================================
3  //
4  // Handy Proxy Routing Table - File name must be : Handy_Proxy_Routing_Table.def
5  // Line starting with // or ! or ( or * are comments
6  //
7  // Handy Proxy (c) Copyright Handyserv - http://www.handyserv.com
8  //
9  //=============================================================================
10
11 //=========================
12 //=== URL Routed to IDO ===
13 //=========================
14
15 //Facebook Forced Rounting
16 #0:facebook.com
17 #0:fbcdn.net
18 #0:akamaihd.net
19
20 //Google Forced Rounting
21 #8:.google.com
22 #0:.googlevideo.com
23
24 //Video Forced Rounting
25 #0:.vimeo.com
26 #0:.vimeocdn.com
27 #0:.youtube.
28 #0:.ytimg.com
```

Why force the routing of a determined web site traffic to a specific channel of your Handy Proxy : some web sites attach importance to your geographical stability, as for example Facebook. If you pass through the Tor network, at some point Facebook will let you know that you access their service inconsistently since your IP address changes regularly (several times an hour). You still can proceed this way, but there is a much more comfortable alternative which is to pass through another Handy Proxy in router mode with a static or much more stable IP address (a dynamic IP address allocated by your Internet provider changes from time to time but lets you appear in the same geographical area and using the same access provider). This way your geolocalisation by these geographically sensible web sites will be stable since the Handy Proxy router can be in your house or at your office which are stable places. Hence, forcing the traffic to some web sites to a determined channel allows to avoid the difficulties generated by an IP address which « travels » from one country to another at the speed of light as the one which is provided by the Tor network. However, this network has an undeniable interest for all web sites which are not protected by geolocalisation. We advise you to route the traffic of all voluminous data (videos, music etc.) directly to the Internet without passing through a network as Tor that can sometimes be very slow, which is not the case if you route this voluminous traffic to another Handy Proxy as long as you connect to it with a fast Internet access.

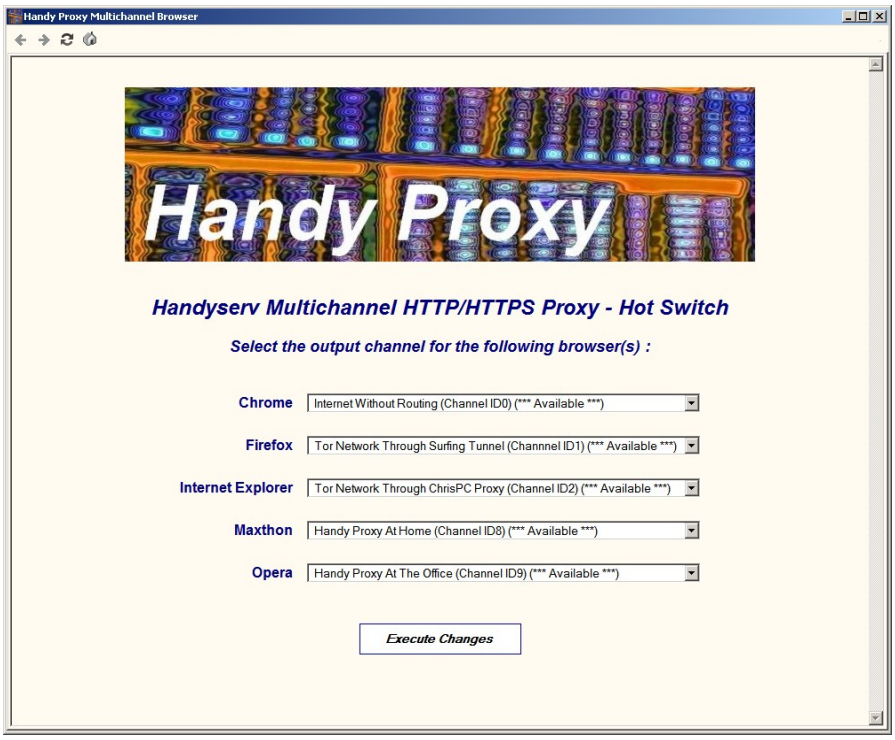
Your Handy Proxy allows you to route your Internet traffic case by case, according to your needs or security and speed criteria and holding into account the criteria used by the web sites you visit.

Your Handy Proxy also includes, to ease your navigation to the different web sites, a « Hot Switch » function allowing your browsers to instantaneously switch from one channel to another.

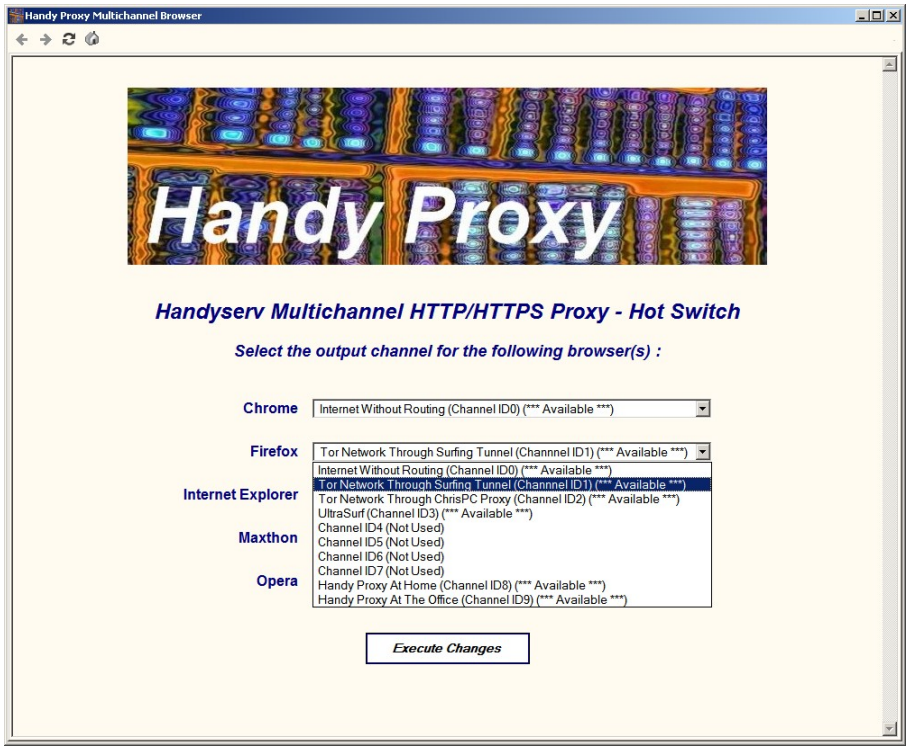
To do this, and after having configured your Handy Proxy as in the example we have chosen that would correspond to your usage, click on the « Hot Switch » button :



You will then get the following screen indicating the connection status of your browers. In this case, we have installed 5 browers under Windows :



When you pull down one of the menus on the right of each browser name, you get the following screen :



In this pull-down menu you see the 10 channels of your Handy Proxy and their connection status. At any time you can choose the output channel for one of your browsers according to your needs. After having selected an output channel for a browser and clicked on the « Execute Changes » button, your Handy Proxy instantaneously reconfigures and all the traffic of the chosen browser will be routed to the new channel, except traffic to web sites whose routing is filtered or forced to another channel as explained above (scale of priorities).

You have now completely configured Handy Proxy and are able to fully exploit the advantages of its different output channels while being, as explained in the preceding subchapters, a user, a router and a messaging server as long as your Handy Proxy can be accessed via your router's NAT setup (as detailed above).

1.3.4. One step further : interconnecting 2 Handy Proxies to reach another network

Now that you know what can be done thanks to the 10 available channels of your Handy Proxy, let us go even further with a more sophisticated configuration.

It must be assumed that you have two Handy Proxies (Proxy A and Proxy B), Proxy A being connected to Proxy B (which is accessible via the NAT setup of the Internet router, see chapter 2.1). By default all their exchanges are encrypted and in this example we have allowed over-encryption of HTTPS and SSL exchanges. We also use, on both sides, private encryption keys (refer to chapter 9 for the parameters associated to these different functions).

In this configuration, we have determined that channel 9 of Proxy A allows to connect to Proxy B. In order to allow one of your browsers of Proxy A (for example Firefox) to reach Proxy B, all of this browser's traffic must be routed to channel 9 of Proxy A (see « Hot Switch » function and associated parameter in chapter 9).

Now concerning Proxy B : if nothing is set up concerning Firefox traffic routing (local traffic and/or traffic coming from Proxy A), all this traffic will flow to channel 0 of Proxy B. However, if on Proxy B a parameter specifies that Firefox traffic must be routed to for example channel 5, in this case all Firefox traffic (local or from Proxy A) (passing through channel 9 of Proxy A in our example) will pass through channel 5 of Proxy B.

Let us imagine now that channel 5 of Proxy B does not point directly to the Internet, but to another IP address and another port. In this case, logically, all Firefox traffic (local and from Proxy A) will pass through these other IP address and port.

Now, figure out that these other IP address and port correspond to the SurfingTunnel programme we mentioned in paragraph 1.3.3. In this case all Firefox traffic (local or from Proxy A) (passing through channel 9 of Proxy A in our example) will flow through channel 5 of Proxy B that will route all the data to the Tor network thanks to the interface provided by the SurfingTunnel programme.

This example illustrates the possibility to reach the Tor network or any other internal or external network via two interconnected Handy Proxies. In other words, Proxy A mustn't necessarily have a direct access to the target network since it will pass through Proxy B to finally reach its target.

In the same example, the target of Proxy B could be a third Handy Proxy (Proxy C) that would allow to reach the Internet in 3 steps. However, adding steps slows the traffic down according to the Internet connection speed of each Handy Proxy (VDSL connections or faster must be privileged). We suggest not to pass through more than 3 steps, otherwise traffic might become very slow. Please note that in our example Proxy C may not be Proxy A, since Proxy A must connect to Proxy B beforehand, and Proxy B itself has to connect to Proxy C afterwords. This one will never be able to connect to Proxy A (such a situation would create a deadlock, and Handy Proxies are protected against deadlocks).

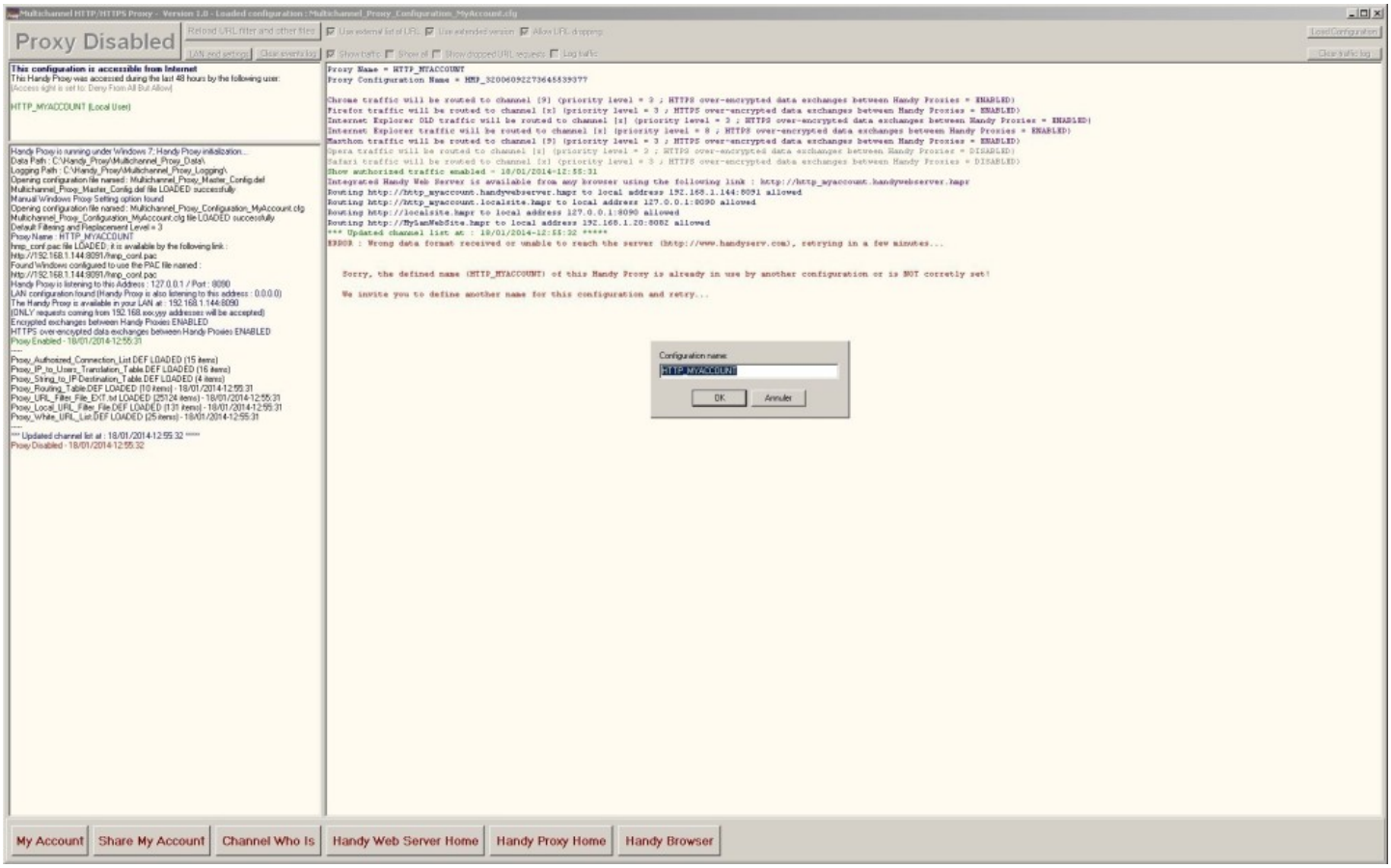
Another very useful example of what could be done with 2 Handy Proxies is to allow to pass through anyplace in the world from a proxy A (via a wifi access) to reach a proxy B (located at home or at your office), Proxy B being for example set up to reach your Intranet via one of the 10 available channels. Again, you could decide that all Firefox traffic, for example, passes through these 2 proxies to finally reach an Apache server that is not public, since in an Intranet. All Handy Proxy access protections are at your disposal to guarantee that only duly authorized persons can reach the final target of your configuration.

Remark : if one of the links in this chain fails, the whole chain could fail or become very slow as in the case of the Tor network where the traffic can momentarily pass through a relatively slow Tor node.

This kind of configuration is available to you as long as you strictly respect the parameters of each of the interconnected Handy Proxies. If your parameters are not consistent you might route the traffic of the chosen browser to another channel and thus « miss » the wished path. In order to make such a sophisticated configuration work, it is important to understand what are the IP addresses and ports used on the Internet.

2. Handy Proxy Usage

After having installed the Handy Proxy software, you get the first screen below :



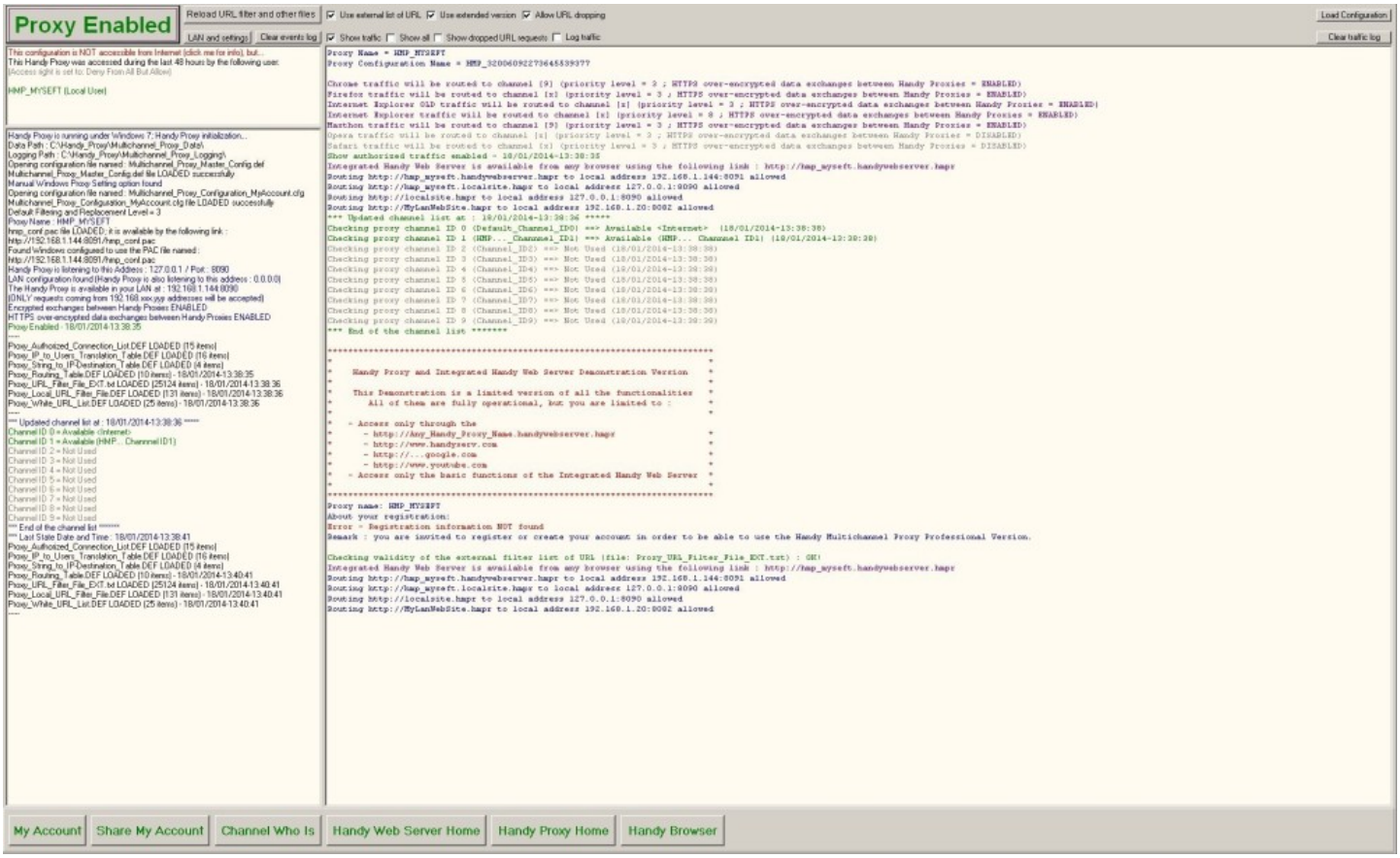
Now you have to choose a name for your Handy Proxy. This name must contain minimum 10 characters, with a maximum of 50.

Concerning the configuration of your Handy Proxy, please refer to the following subchapters of this manual (see chapter 9 « Handy Proxy Configuration Files ») :

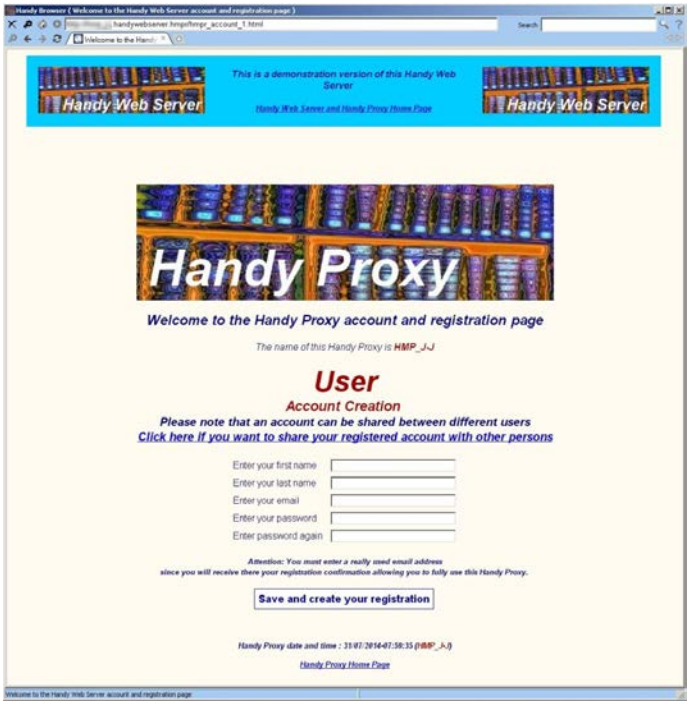
Subchapter 9.1 : Handy Proxy Master Configuration File (Multichannel_Proxy_Master_Config.def)
Subchapter 9.2 : Handy Proxy Configuration File (Default name : Handy_Proxy_Configuration.cfg)

These two configuration files manage all functionalities of your Handy Proxy and of its other modules. There are also different additional configuration files (see chapter 9 « Handy Proxy Configuration Files »).

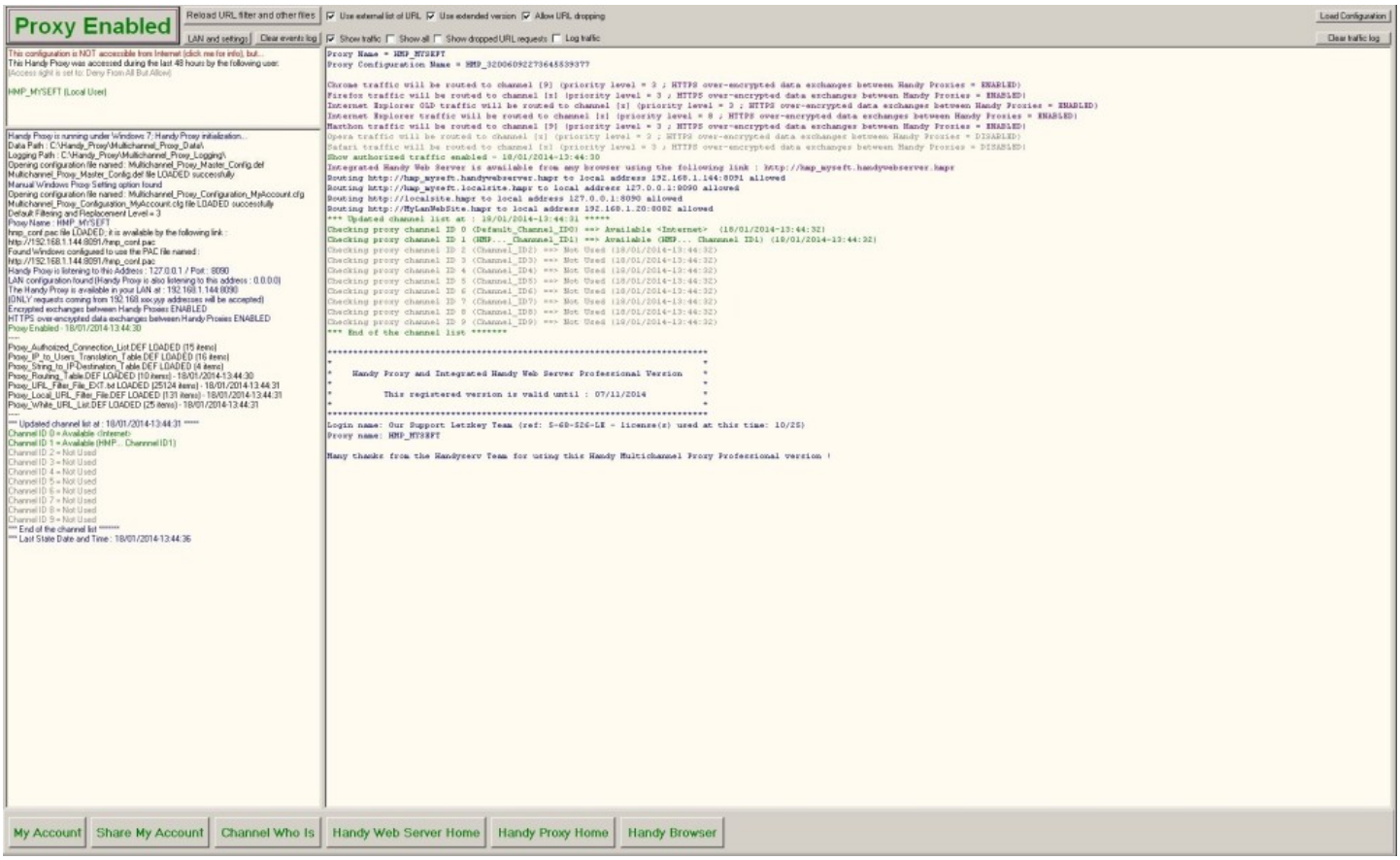
After having chosen a name for your Handy Proxy, you get the following screen telling you that you are allowed to use the Proxy with the selected name. However, at this stage you are (still) in « demonstration » mode. This mode allows you to access specific web sites as Google or Youtube ; all other sites are unaccessible in this demonstration mode. This mode allows you to evaluate the functions of your Handy Proxy and implies no commitment on your part.



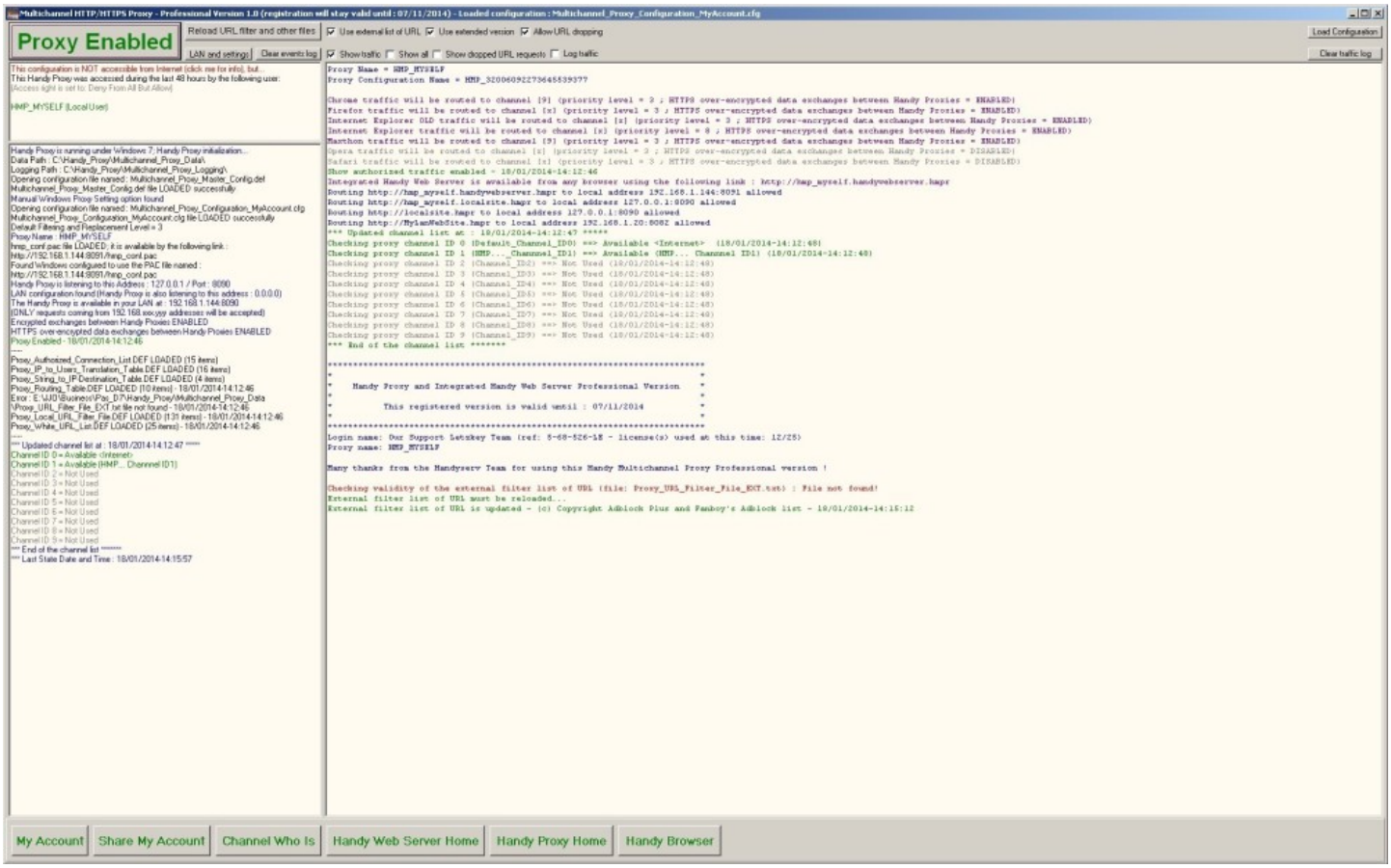
Afterwards, if you wish to use your Handy Proxy without any limitation, click on the « My Account » button on the lower left corner of the screen here above to gain access to the screen below that will allow you to register and get your user's license. This license can be obtained for one single user or several users, according to your needs. After having registered, you will receive a confirmation e-mail. You will then be able to share your license with your family, your friends or colleagues for example. For more information on this, see chapter 3 « Sharing your account ». The only person able to share and modify the license is its owner.



After having registered and obtained your user's license, you will get the following screen :

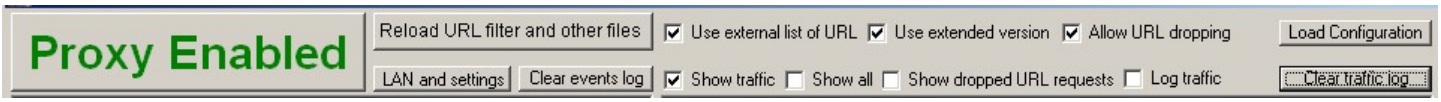


A few seconds after the launching of your Handy Proxy, the software will update itself namely by automatically downloading the default list of links which are filtered by Handy Proxy. Your own filters will be added into this list (for more information, see chapter 9.6 « Handy Proxy Proxy_Local_URL_Filter_File.DEF file »).



Explanation of the different parts of the Handy Proxy screen :

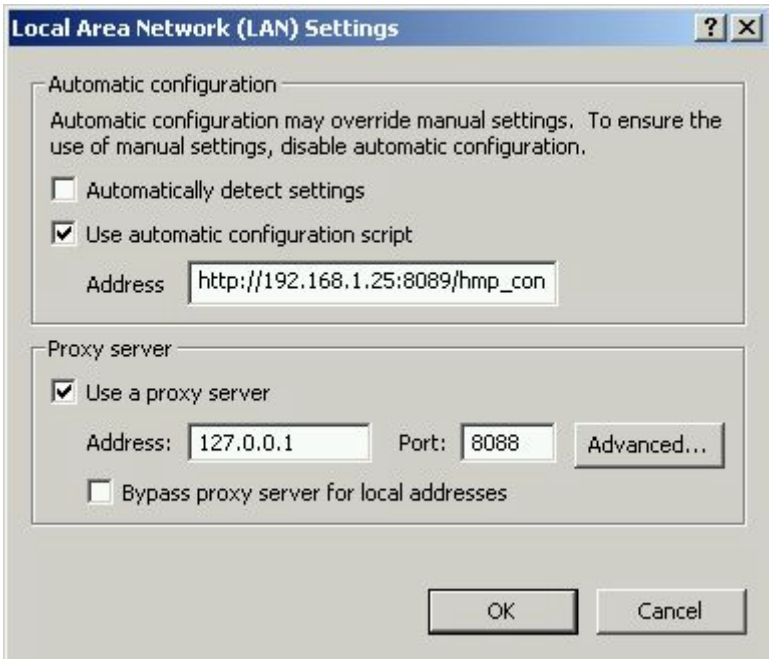
Main options and buttons of your Handy Proxy :



- **« Proxy Enabled » button** : this button allows to authorize or block all the traffic flowing through your Handy Proxy. Thanks to this button, you can block all exchanges between your browser and the web sites that are open into it. It is possible to make the Handy Proxy « transparent » for defined sites. For more information about this, see chapter 9.3 « Handy Proxy hmp_conf.pac file ». You can manage site by site the access/priority authorization that will be granted. For more information about this, see chapter 9.9 « Handy Proxy Proxy_White_URL_List.DEF file ». It is also possible to define, for a given site, the Handy Proxy channel that will « route » the traffic between your browser and the given site. See chapter 9.7 « Handy Proxy Proxy_Routing_Table.DEF file ».

- **« Reload URL filter and other files » button** : this button allows to reload all configuration files mentioned above, except the hmp_conf.pac file which is used by the browsers in real-time.

- **« LAN and settings » button** : this button allows to open the Windows menu (Local Area Network Settings) allowing to define the Internet access via the Handy Proxy for your browser. We advise to use the hmp_conf.pac file which is automatically configured by the Handy Proxy. Select option « Use automatic configuration script » and enter the address as follows, for example : http:\\192.168.1.x:80xx/hmp_conf.pac. This address is indicated in the screen of your Handy Proxy, see area « **hmp_conf.pac file LOADED** ». Please note that the name hmp_conf.pac can NOT be modified and that the port to use is the one of your **Handy Proxy + 1**.



In addition to this or as an alternative, you also can define here manually the address and port of the Handy Proxy used by your browser. Select option « Use a proxy server », and enter in « Address » and « Port » areas the information specified on the screen of your Handy Proxy. See area « **The Handy Proxy is available in your LAN at** …». Please note that your Handy Proxy can setup this area automatically at its launching according to the parameter « Automatic_Windows_Proxy_Setting ». See chapter 9.1 « Handy Proxy Master Configuration file (Multichannel_Proxy_Master_Config.def) ».

Events log of the Handy Proxy :

- **« Clear events log » and « Clear traffic log » buttons** : these buttons allow to clear the respective areas of your Handy Proxy screen.

- **« Use external list of URL » option** : this option allows to ask or not your Handy Proxy to filter the sites or links included in the list which was automatically downloaded. This list is updated all 24 hours.

- **« Use extended version » option** : there are two lists of sites or links to filter, a simplified and an extended one. You can choose the one which is most convenient to you.

- **« Allow URL dropping » option** : this option allows to authorize or not your Handy Proxy to filter the sites defined in the different configuration files previously mentioned.

- **« Show traffic » option** : this option allows to list the exchanges between your browser and web sites. If you do not need it, we advise you to unselect it but in this case you will not be able to click on a listed link to filter or re-authorize it. Explanations about this are provided further in this manual.
  If your Handy Proxy is a « traffic node » for other Handy Proxy users, the display of an event is different : it will not contain the link called by another user in order to preserve his/her privacy. This kind of event will include the following data : who called a link, at what time, and which exchange encryption reference was selected at *T* time between your Handy Proxy and the one of your correspondent who logged in previously. As a reminder, the encryption mode between 2 Handy Proxies changes automatically all 4 hours and completely all 24 hours.

- **« Show all » option** : this option allows to list all exchanges according to their priority.

- **« Show dropped URL requests » option** : this option allows to list the traffic to filtered sites in order to reauthorize them if needed.

- **« Log traffic » option** : this function allows to save on disk all exchanges listed according to the options above. The files are saved into the subdirectory ..\MULTICHANNEL_PROXY_LOGGING. This function has to be used only if absolutely necessary, since disk writing happens each time a link is called by your browser. This includes, for one page, disk writing of the link to the page but also of all elements of the page that must be diplayed. This can lead, for

one single page, to 10 disk writings if a page contains for example 9 pictures. This will obviously slow down your Handy Proxy.

- **« Load configuration » button** : this button allows to reconfigure your Handy Proxy if you require several different usage modes or if you need to connect to other Handy Proxies. Attention : the « master » configuration file is loaded only once at the launching of your Handy Proxy. However, you can reload the configuration subfiles. See paragraph 9.2 « Handy Proxy Configuration file (Default name : Handy_Proxy_Configuration.cfg) ». You can create as many configuration subfiles as you want with extension .cfg and use them at will as long as you strictly comply to the compulsory syntax of this file.

See here below an example of Handy Proxy launching with a given .cfg file :
You can define for example which Handy Proxy channel will be used by a given browser.

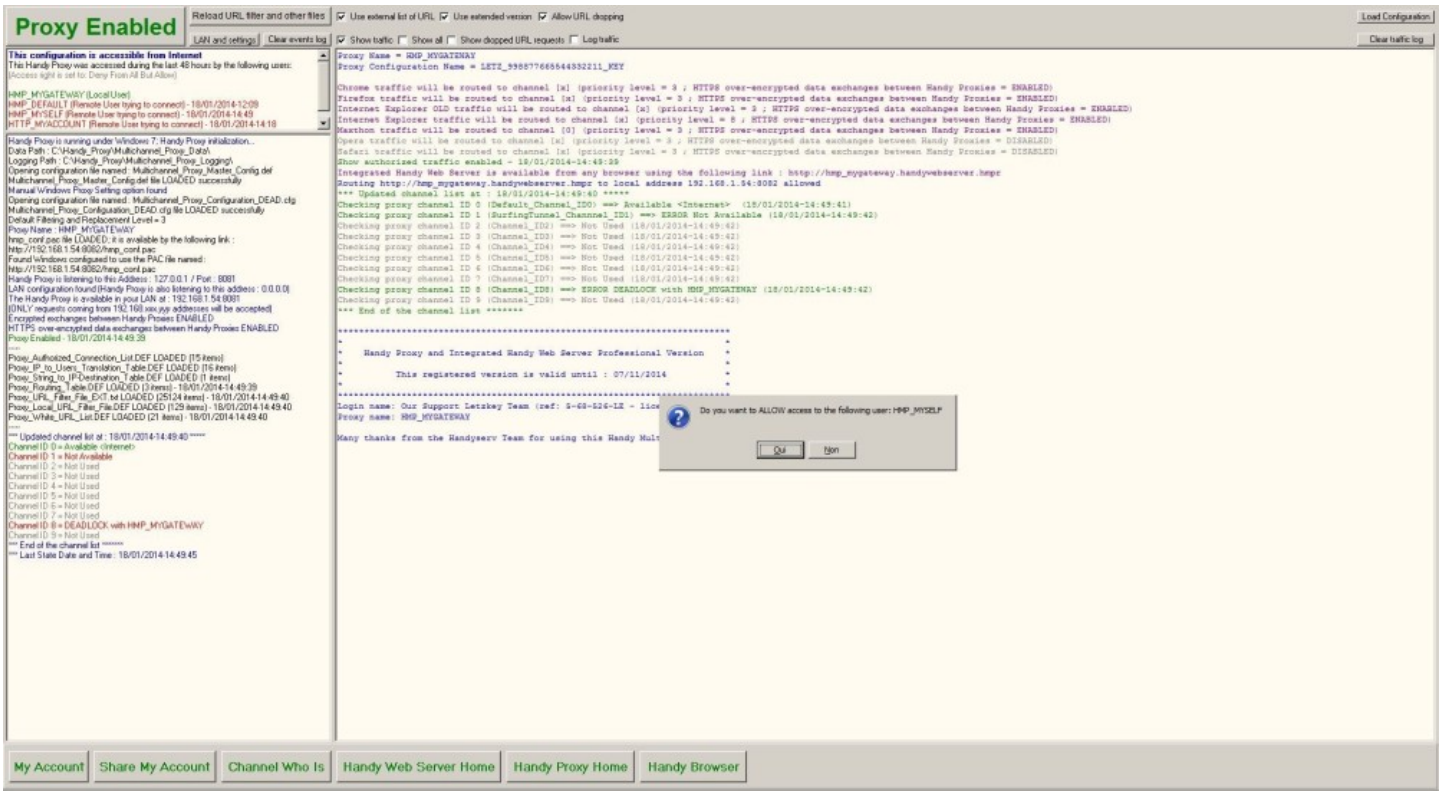
Handy Proxy channels connected to the outside world :

This area indicates « how » and « where to » the 10 channels of your Handy Proxy are connected. By default and automatically, channel 0 is always connected to the Internet via your router. All other channels (from 1 to 9) can be connected to a predefined address and port or to another Handy Proxy user. In those cases, several messages may appear in this area :

- Messages appearing in green indicate that the connection is operational.
- Messages appearing in red always indicate an error : either the chosen destination does not exist or is not available, or you have routed a channel to your own Handy Proxy (« deadlock » case), or the message is « Access denied » which means that the destination exists and is available, but that you cannot access it. You consequently have to ask this destination to autorize you to access its Handy Proxy. See explanations further.

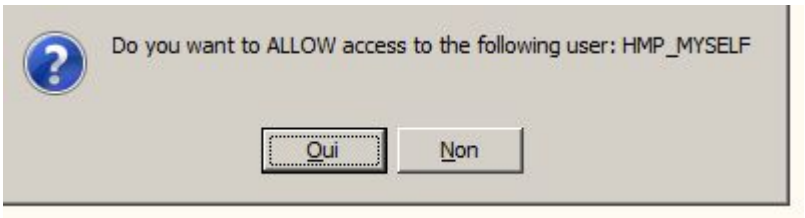
On the following screen, you can notice in the upper left corner that the Handy Proxy is available on the Internet for other users (« This configuration is accessible from Internet ») (see how to proceed further in this manual).

When a user wants to connect to your Handy Proxy which is turned into a router, this user must first be authorized to do so. Here is how to proceed :



First, the user who wishes to connect to your Handy Proxy (which will become a router for this user) appears in the list below. Click on the user in question. In our example, we click on user « HMP_MYSELF » :

When you have clicked on the user you want to authorize, the confirmation screen below appears :



If you confirm, the selected user will be automatically added to the authorized users list as you can see on the following screen. In this list, « Local User » indicates that the Handy Proxy itself is allowed to access the Internet.

To allow a user to use your Handy Proxy as a router between him/her and the Internet, you can, either proceed case by case as explained above, or define a group of users via the following configuration file : Handy Proxy file Proxy_Authorized_Connection_List.DEF (see chapter 9.4). This configuration file includes a function allowing to authorize any user to use your Handy Proxy as a router. Attention, this option must be used with caution. We advise to define users one by one.

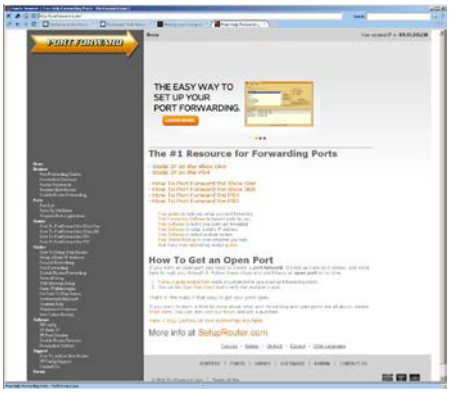
2.1. Making your Handy Proxy accessible for other users

In addition to what was explained previously about allowing remote users to access your Handy Proxy, it must be accessible from the Internet. To achieve this, you have to configure your router and more specifically its NAT function. Each router being different since there are a lot of possible providers, we cannot possibly explain in the present manual how to proceed for each of them. We provide here below links to three sites providing exhaustive explanations. The first one provides an overview with a video tutorial. The second one allows to identify the router you are using and consequently the method to follow in order to modify the NAT table that will have to point to our Handy Proxy (address and port can be retrieved via your Handy Proxy's main screen). The third site is also very useful to allow you to define the NAT table of your router.

This is not very complicated to do, and this method is very widely used.

Please note that none of the users connected to your Handy Proxy will know the address and port of your Handy Proxy or the Internet address which is yours if you are configured in a dynamic IP address (same applies if you are using a static IP address). Concerning this matter, the Handy Proxy includes a function allowing to update your dynamic IP address, thus allowing the connected persons to work in a transparent mode. Remark : when your dynamic IP address is modified by your Internet provider, your Handy Proxy notices it within a very short delay and the update occurs then instantaneously to make the unavailability of your Handy Proxy as short as possible (a few seconds usually).

http://www.nch.com.au/kb/10046.html



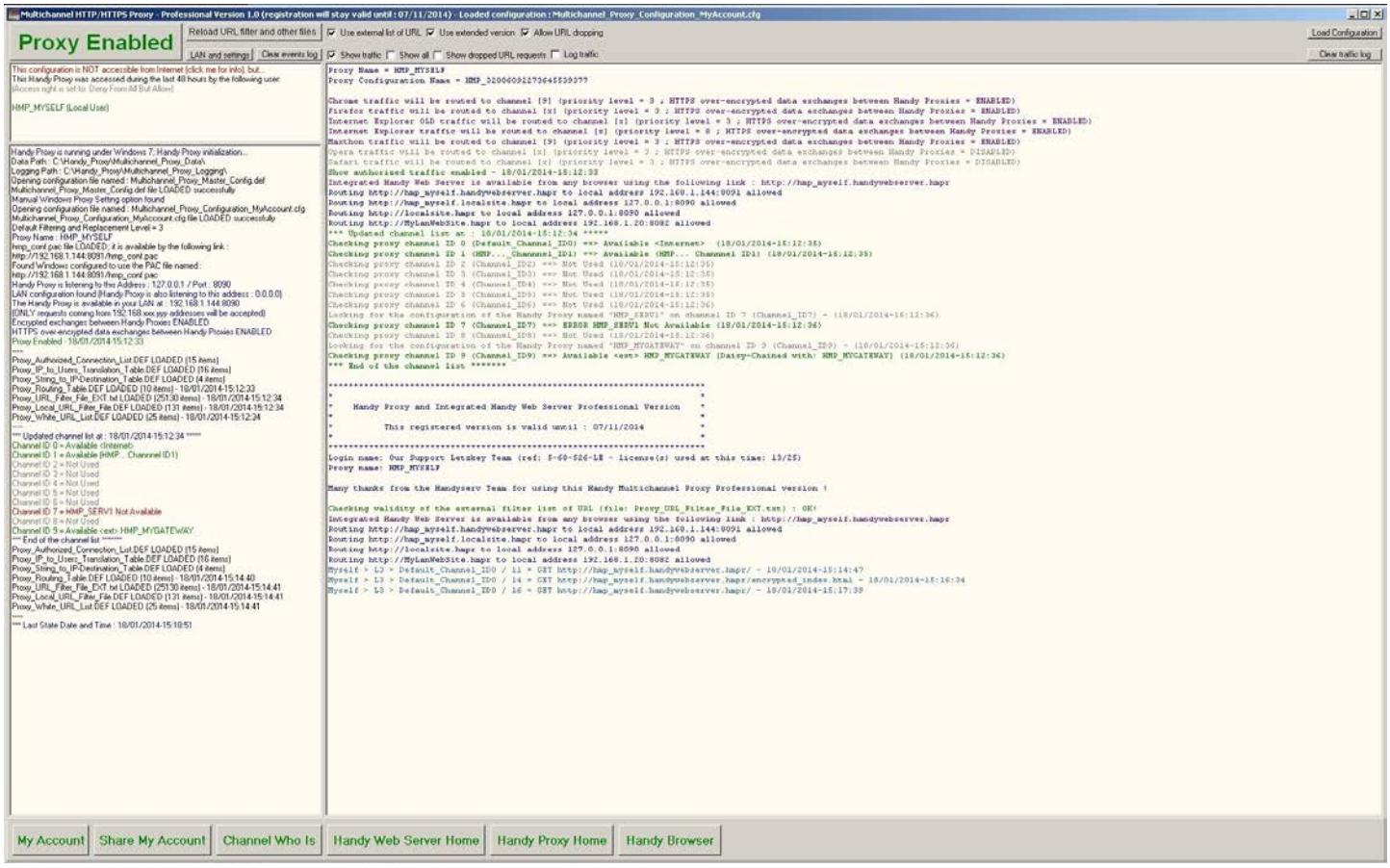
http://portforward.com

http://setuprouter.com

Important remarks concerning some routers : some routers of your LAN to the Internet do not allow a PC in your LAN to send data to an Internet site pointing to your own network. Figure out, for example, that the PC on which you are using your Handy Proxy (name : HMP-1) has got the local address 192.168.1.25 and that you want to use the functionalities of another Handy Proxy in your network that would be configured as a router with address 192.168.1.50 (port 8085, name HMP-2). When setting up HMP-1 so that it can route exchanges with HMP-2, you could, if your router matches the case explained here, not be able to connect from HMP-1 to HMP-2. Of course, this has a meaning in a local area network only if you want to test some functionalities. It is obviously meaningless, in a local area network, to pass through the Internet to access another PC in one's own network. If your router is in the case explained here, it is nevertheless possible to connect from HMP-1 to HMP-2, but you must setup HMP-1 by indicating for the chosen channel the IP address of HMP-2 and not its name (see your Handy Proxy setup). This also applies to the case in which you would like to make the functions of your Handy Web Server and Handy Messaging Server on your HMP-2 available for your own network and for remote users.
In short, internal users of your local area network will have to setup their Handy Proxy to point to the Handy Proxy in router mode and in Web Server/Messaging Server mode via the physical address of this PC in your network, for example 192.168.1.50 (port 8085). On the contrary, remote users of your LAN and Handy Proxy in router mode (and in Web Server/Messaging Server mode) will have to indicate that they want to connect to the name of this Handy Proxy (in this example : HMP-2).
From a practical point of view, for people who should use the services of one of your Handy Proxies in router mode both from within and outside of your local area network, we suggest to create two configuration files that will be used according the usage case (internal or remote).

2.2. How to authorize or not the access to a web link

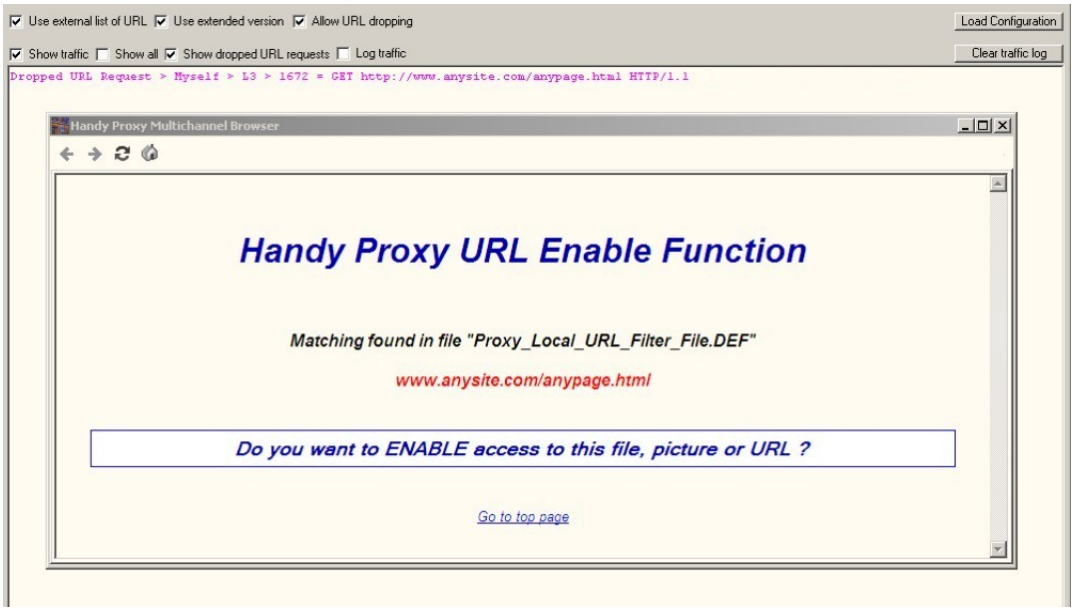
When you use your Handy Proxy, if you check the option « Show traffic », all links to HTML, PHP,… pages are listed. If one of these links does not suit you or is not useful to you, you can make it unaccessible in order to decrease your traffic and thus increase your Internet access performances. In order to do so, just click on the link.



Here is the screen that appears if you click on the link « http://www.anysite.com/anypage.html » as in our example :

In this screen, you can scroll through the list that will allow you to select the blocking level you will apply to the concerned page, link or entire web site. Be very careful while using this function, since it allows to block, for example, all sites ending with a « .com » extension. This can still be meaningful if you want to block all sites of a certain kind or having a given

extension. However, we advise against proceeding this way and recommend to act case by case instead. Generally speaking, it is better to block a given page or even a complete web site.
When a page or a site has become unreachable, it is possible to reauthorize it. To do so, you must first check the option « Show dropped URL requests » in the main menu and ask your browser to open the page or site. Afterwards you have to click on this particular link in the screen of your Handy Proxy. The following screen appears then. You just have to confirm the reauthorization. Please note that you also can use the Proxy_Authorized_Connection_List.DEF file that lists all your filtered links, pages and sites.

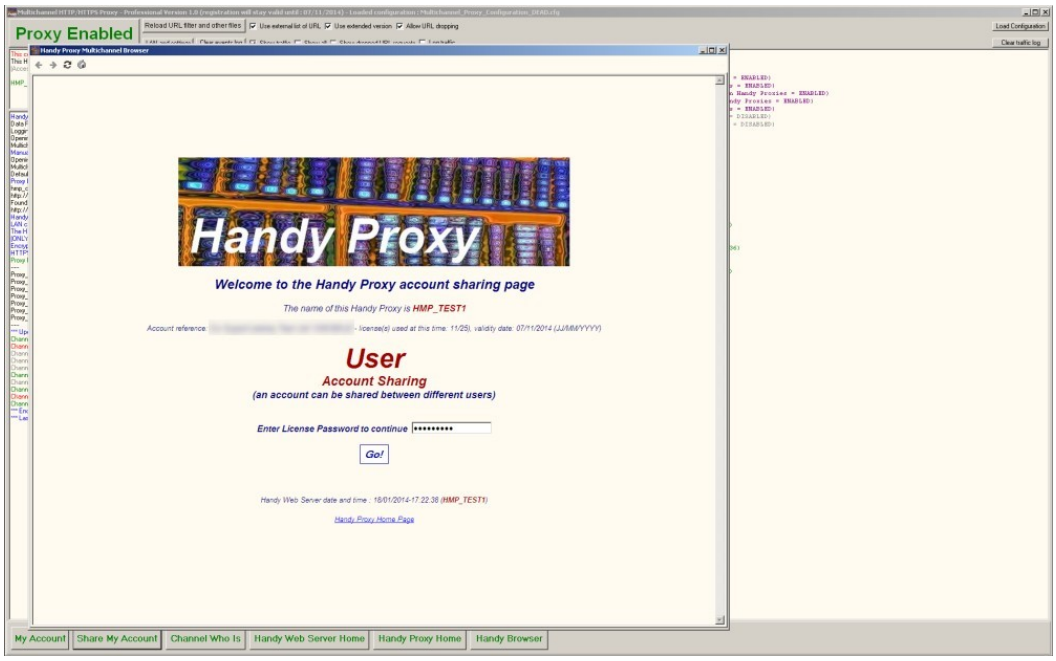


3. Sharing your account

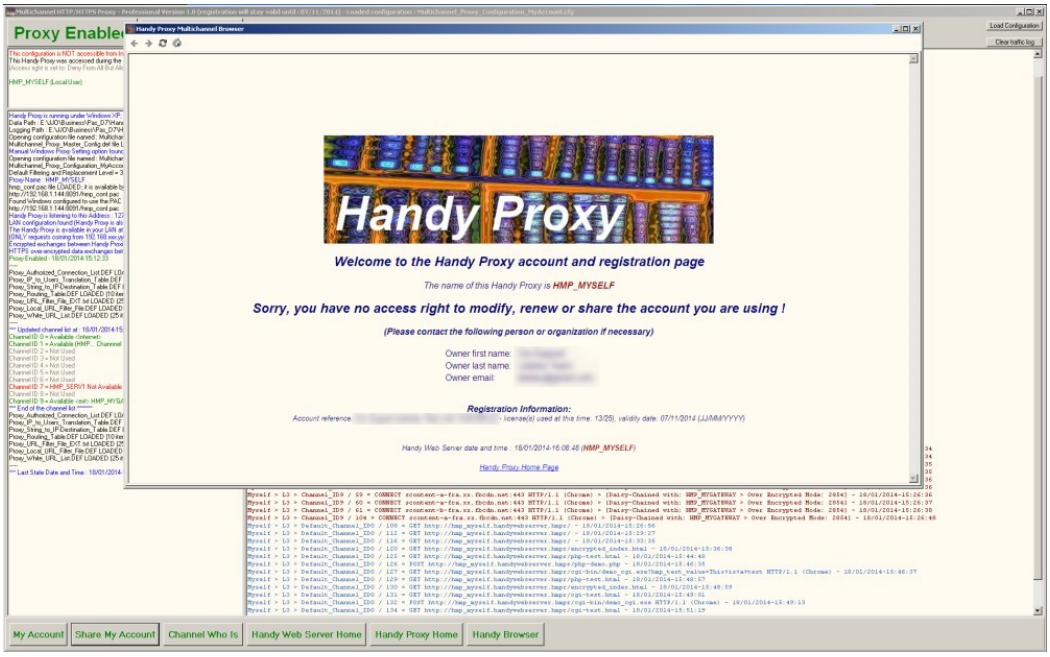
When you are a registered user you can share your license with other persons of your choice according to the type of license you have chosen. Only the owner of the license can share it. The people you authorize to use your license will never be able to share it with others.

At registration time you must carefully define your needs in terms of number of Handy Proxies you will use with your family, your friends or in your company. We advise to provide for a few additional licenses to avoid being limited too rapidly. For example, if your family counts 5 people wishing to use a Handy Proxy, on 5 different PC's, we advise you to use the upper license (for example for 10 users).

In order to share your license, click on the « Share My Account » button which is in the bottom menu bar of your Handy Proxy. You will then get the following screen, where you have to enter your password (see the standard parameters in your Handy Proxy's configuration files) :



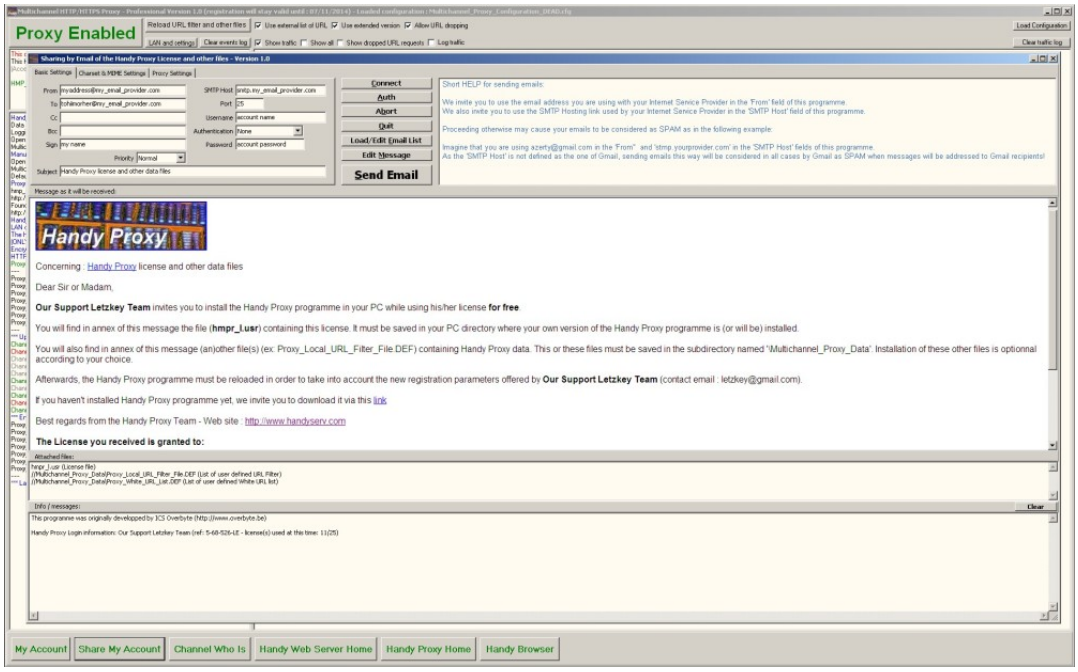
The following screen will appear if you are not the owner of the license you are using :



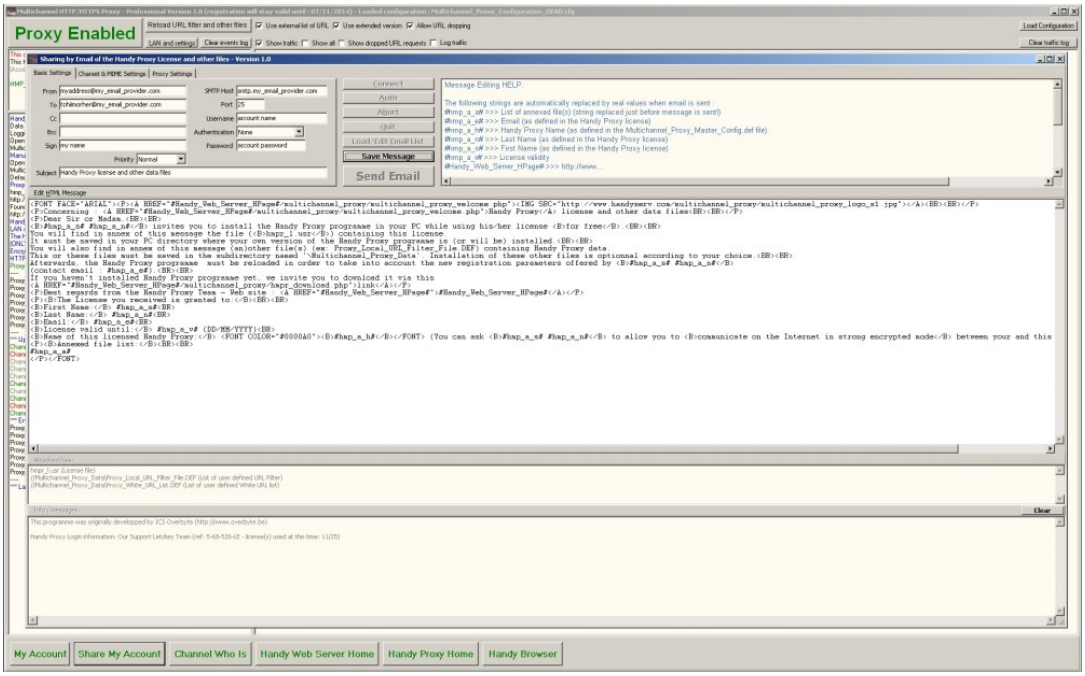
If you are the owner of the license, the screen below will appear. This module is an e-mail generator allowing you to customize the message that will be sent out to the addressees included in the mailing list(s).

This e-mail generator is dedicated to the distribution of the license and of other files of your Handy Proxy. The syntax of the message must include some mandatory information, otherwise the message will be rejected.

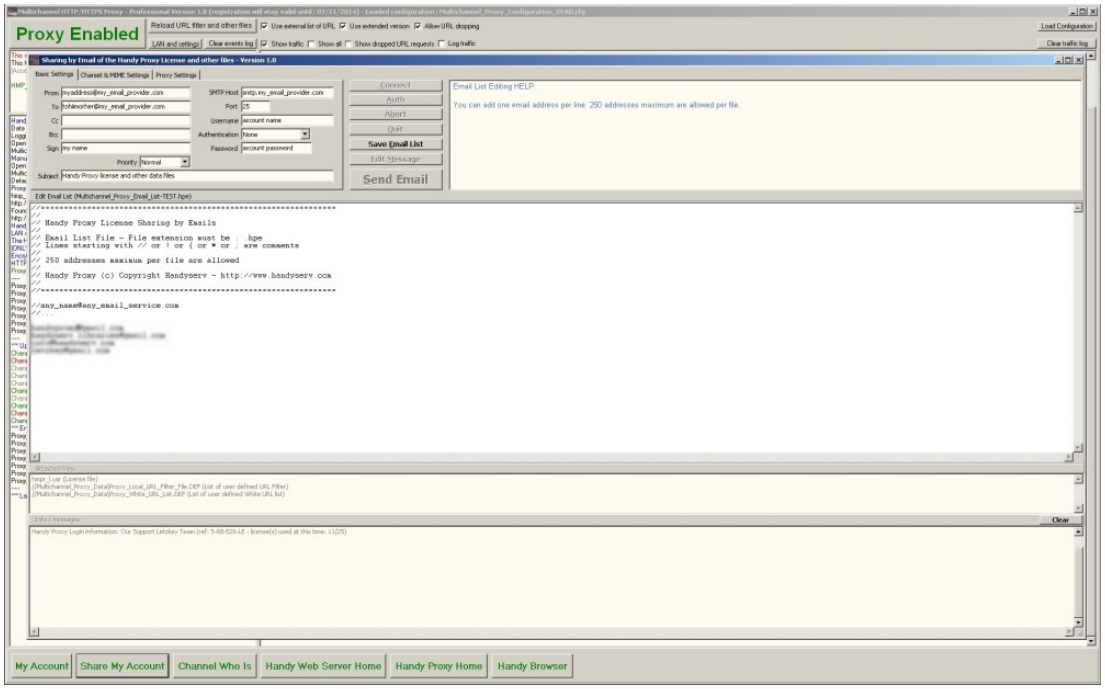
The body of the message may contain some keywords as indicated in the help text included into this module. These keywords will be dynamically replaced by the program according to your Handy Proxy's setup. **You absolutely must strictly comply to the syntax of these keywords, otherwise you will not get the expected result**.



This program features a text editor allowing you to modify the body of the message that will be sent out to the persons of your choice.



In this program you can introduce the e-mail addresses of your correspondents and save them into different files, each one being able to contain up to 250 addresses.



Around the middle of the screen of this module, you can attach other files of your Handy Proxy to the license sent to your correspondents, as for example your file containing the sites and links to filter.

This module uses the services of your Internet provider to send out e-mail. You thus have to setup this module according to your provider, and more specifically the « SMTP Host » area where you must enter the link to the SMTP server of your Internet provider. Please refer to the documentation of your Internet provider to identify this server. You also have to customize the « From » area, otherwise your messages will not be sent out.

The « To » area allows to send one message at a time, without making use of a mailing list.

There are other parameters in the other tabs, but in principle you won't have to modify them, since they are standard.

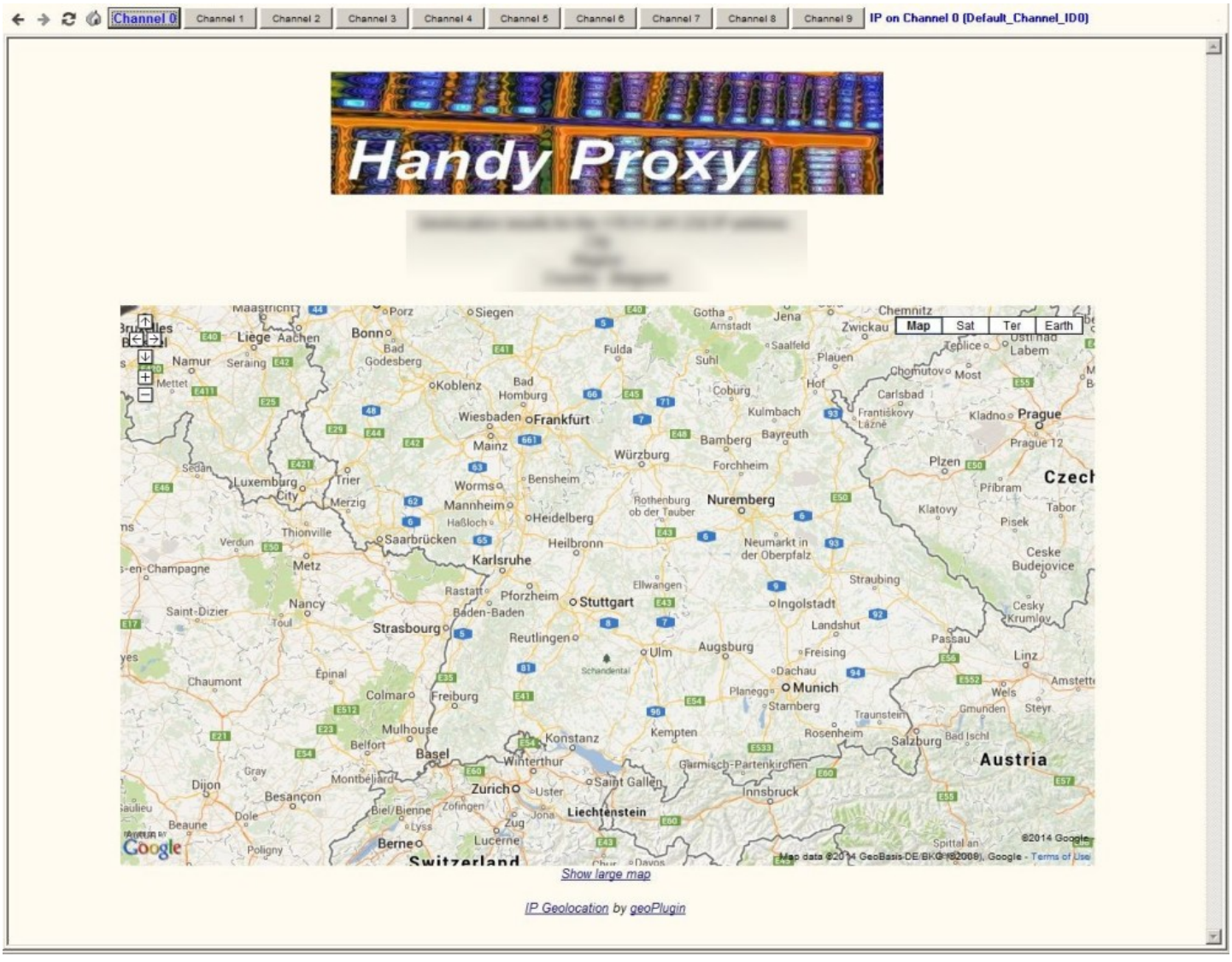
Important remark : it is strictly forbidden to use this module to other ends than distributing the license of your Handy Proxy. Any non-compliant use will lead to immediate termination of your license without any prior notice.

4. Channel Who Is

If you use different channels of your Handy Proxy in order to access another remote Handy Proxy or any other routing node (proxy), it is interesting to know from where you will access the Internet. The « Channel Who Is » function, accessible from the corresponding button, provides this information.

When the screen below appears, choose a channel by clicking on the proper button. Your Handy Proxy will then send a request to know the public IP address corresponding to the selected channel. For example, if channel 9 of your Handy Proxy points to another Handy Proxy located in the United States, the public IP address that will be sent back will be American. On basis of this information, a geolocalization will occur and a Google Map (c) positioned according to the IP address will be displayed. This will allow you to know from where you access the Internet.

As a reminder, all exchanges between 2 Handy Proxies are encrypted, which means that your exchanges from the place you are located will never appear in the clear all the way up to the point where is the other Handy Proxy you correspond with, allowing you to work in an uncrypted mode on the Internet.



5. Handy Integrated Web Server With Encrypted Page

As standard your Handy Proxy includes an additional module which is a complete web server. This server allows to host HTML, Javascript, PHP pages and images (JPG, GIF, PNG).

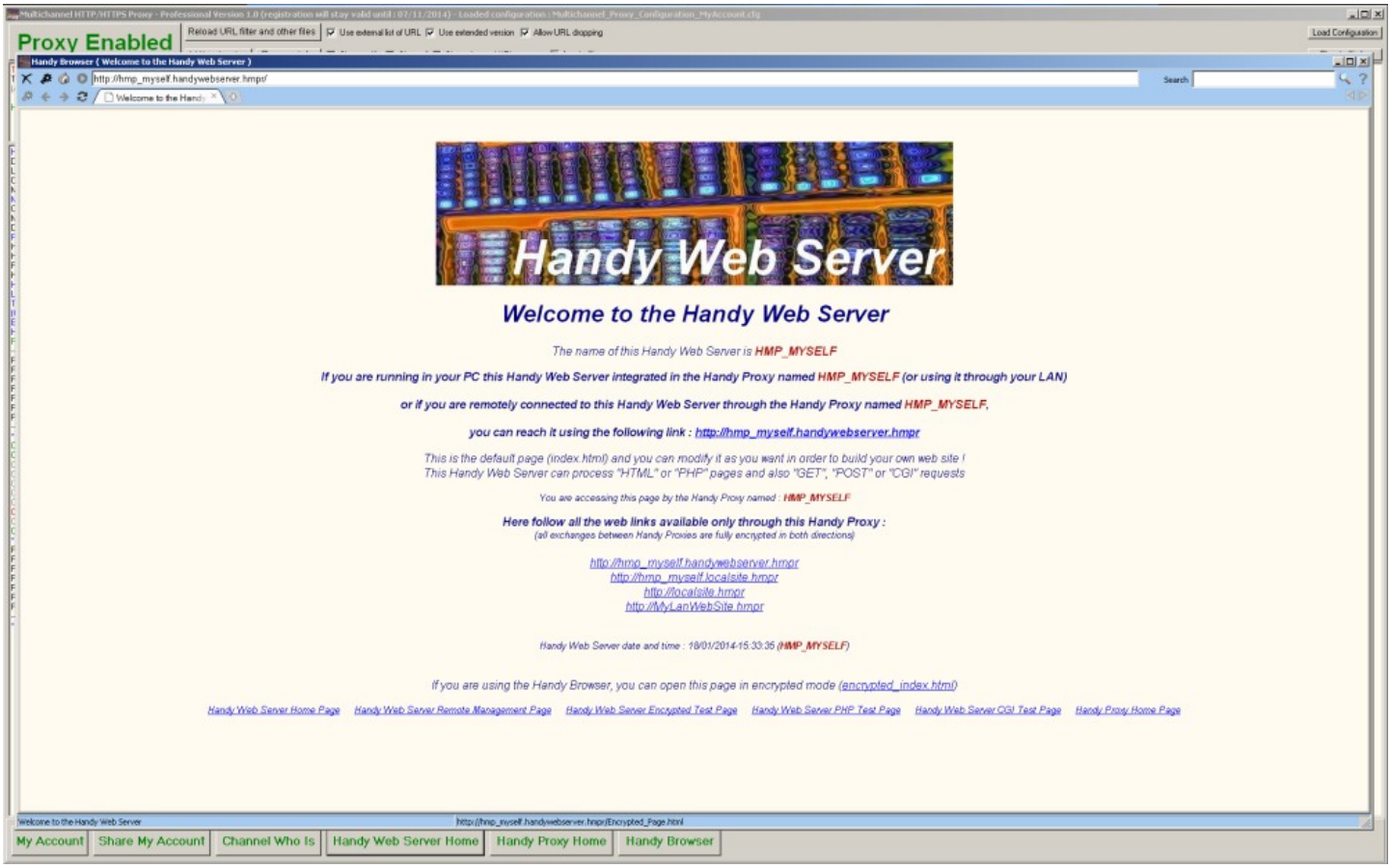
This web server can be reached only via your Handy Proxy, which means that the hosted pages can be accessed only by Handy Proxy users who were authorized to do so. **In other words, you can create totally private web sites.** Moreover, since the data that flow between the Handy Proxies are encrypted, your web pages hosted by your integrated web server will never be crawled and indexed by search engines. The privacy of your data, pages, etc. is perfectly preserved. In addition to this, you also can encrypt your pages as we will see in the next chapter.

Concerning PHP pages, at the installation you are provided with a copy of the original PHP modules (which are in the public domain). However, you do not have to use this installation because it is possible to instruct the web server to use another one. See the « Handy Proxy Master Configuration file (Multichannel_Proxy_Master_Config.def) ».

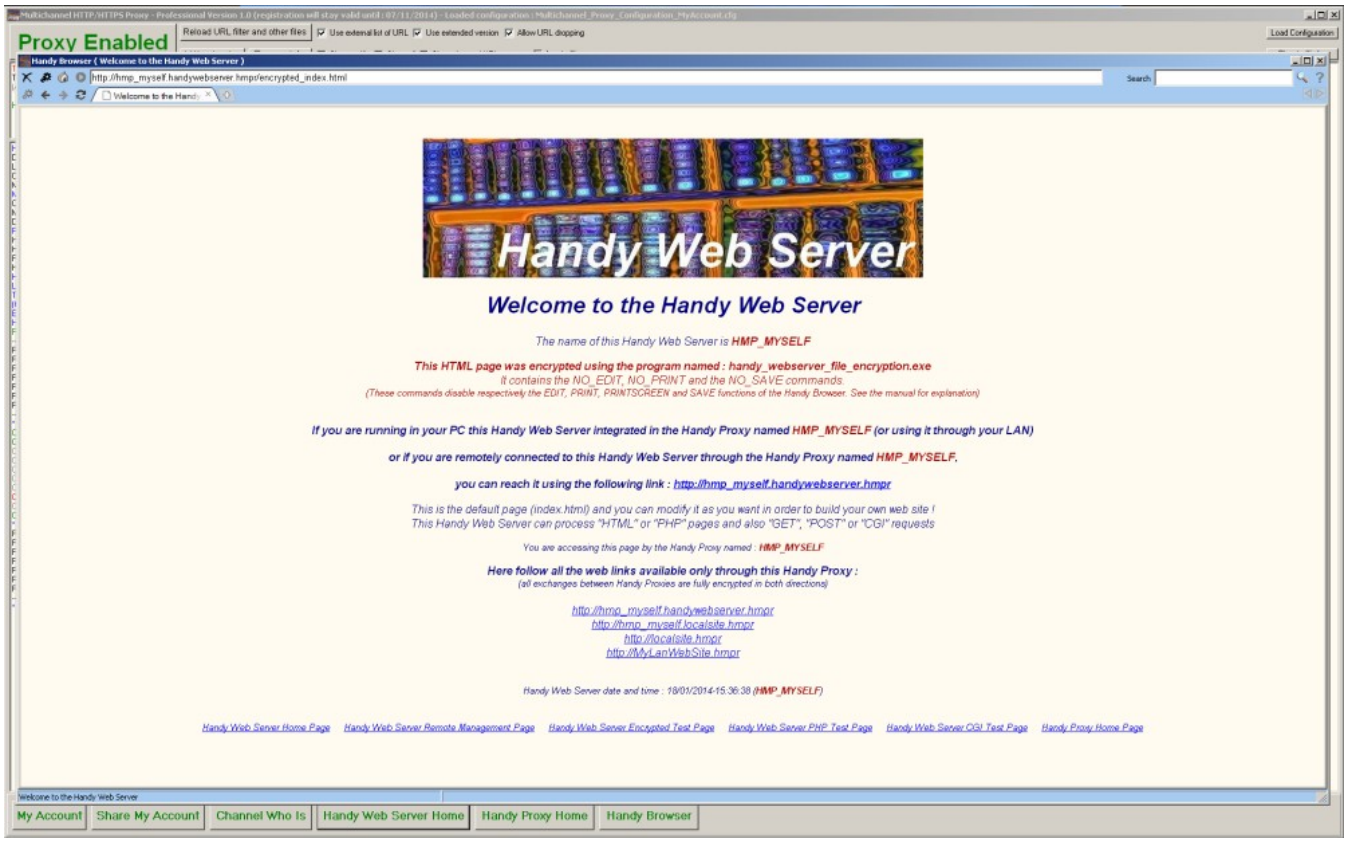
The HTML, Javascript, PHP files (etc.) must be placed into the …\Handy_Web_Server_wwwRoot directory of your Handy Proxy. Attention : PHP INCLUDE files must be placed into a different directory (see further in this manual).

By clicking on the « Handy Proxy Home » button (in the bottom menu bar of your Handy Proxy), you will open your Handy Browser which is described in a specific chapter of this manual.

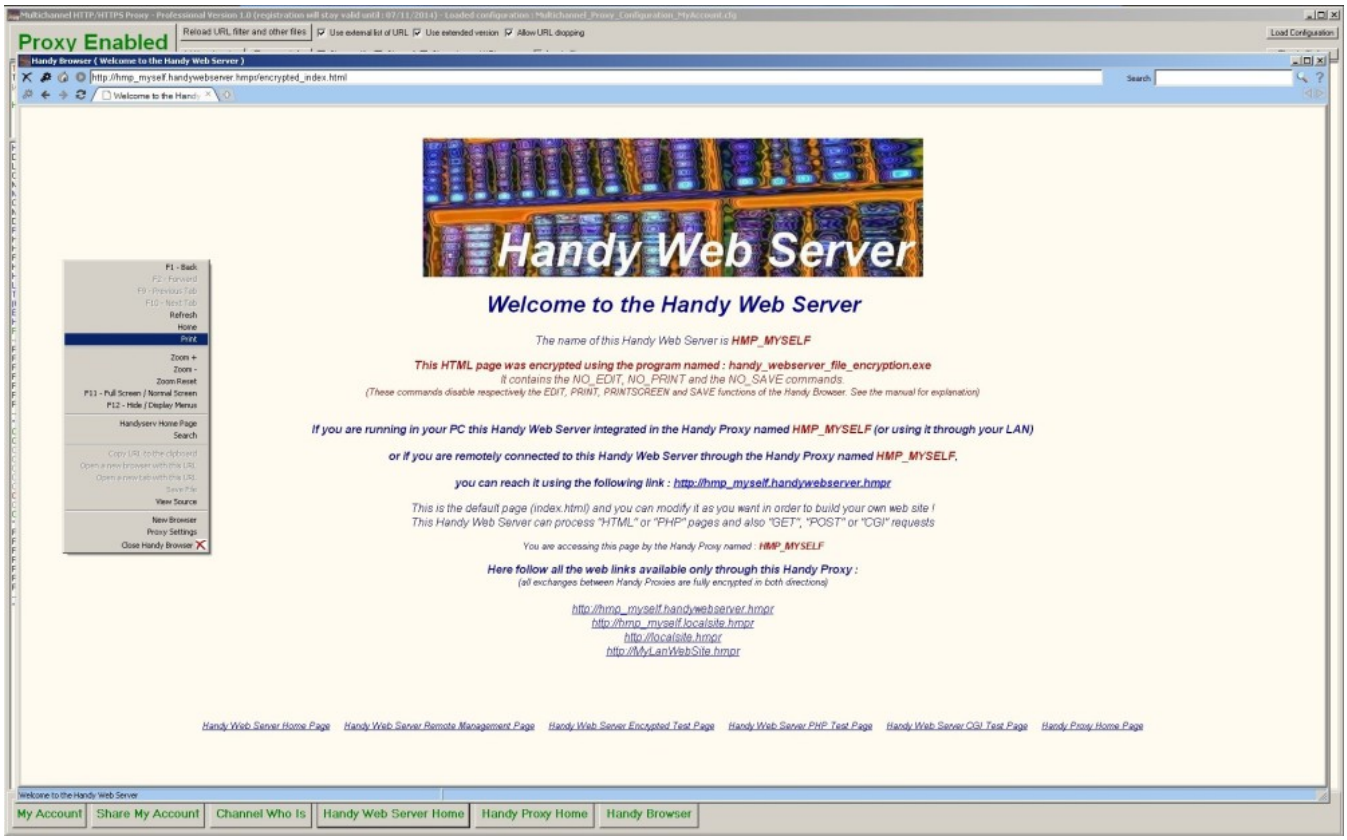
You will get the Handy Web Server default page that was created at the installation. Its name is index.html, but you can modify it according to your needs and the kind of service you want to provide to your correspondents. Clearly, you can create all pages of your choice making use of the HTML and/or PHP language.



The screen below displays the page named « encrypted_index.html ». This page was previously encrypted by the page encryption program provided as a standard feature (and described in a specific chapter of this manual).



Remark : right-clicking on the screen of your Handy Browser gives access to the contextual menu you can see on the left of the screen below. This menu includes standard browsing functions. It can also be accessed from within the main menu which is on the top left of this browser.



You can integrate into your web pages specific commands that will be understood only by the Handy Browser provided in the package. These commands are :

- NO_EDIT : this command prohibits the edition of your pages if they are accessed via your Handy Browser
- NO_PRINT : this command prohibits the printing of your pages if they are accessed via your Handy Browser
- NO_SAVE : this command prohibits the saving of your pages if they are accessed via your Handy Browser

In order to make these commands « inescapable », your pages must be encrypted via the functions provided as standard in this package. Thanks to this, your pages can be viewed only from within a Handy Browser. In the following example, a web page was created including the three commands here above. It was encrypted and is thus accessible only via your Handy Browser.

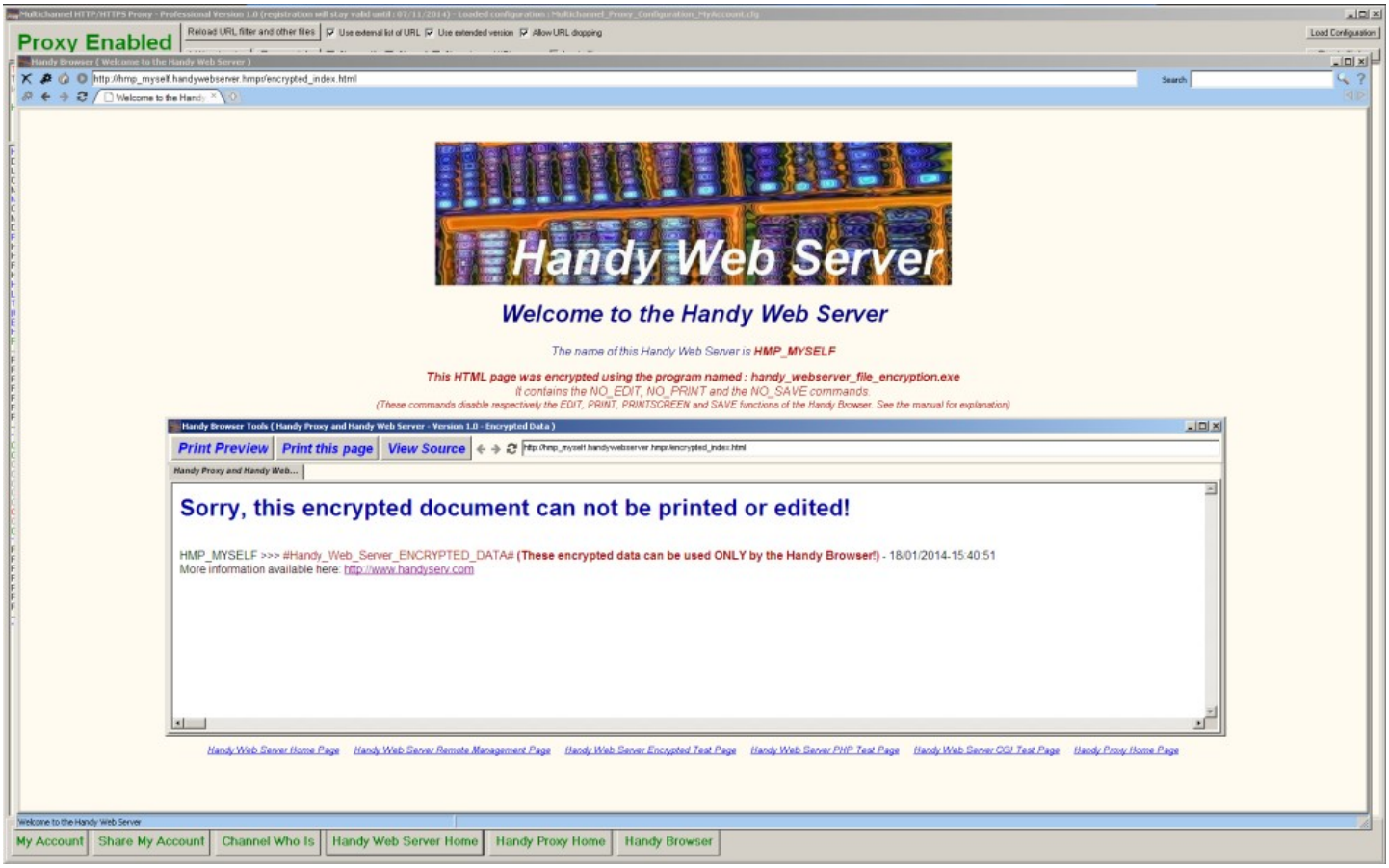
The syntax of these commands is the following :

```
<!-- #Handy_Web_Server_command# -->
```

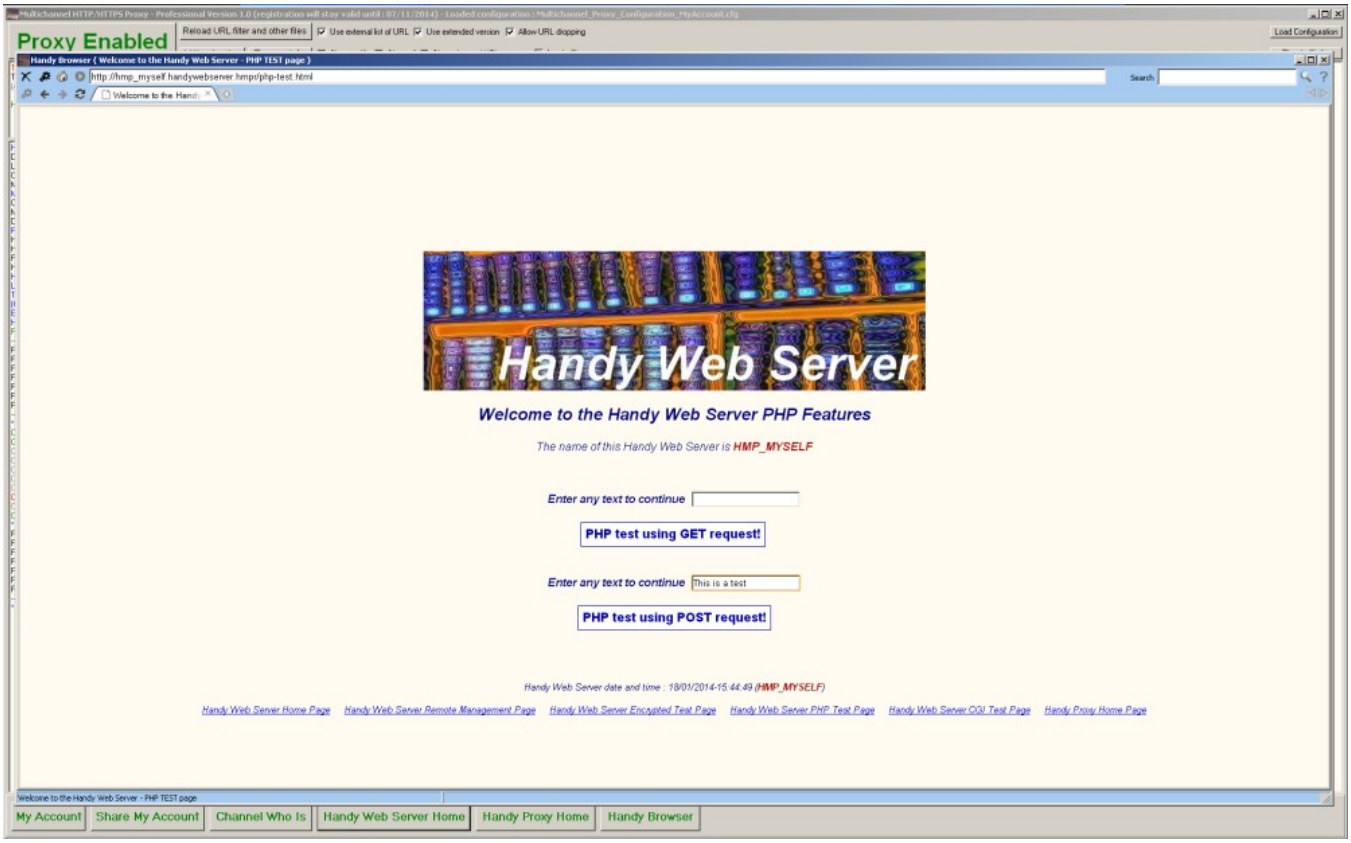
In this syntax which is in fact an HTML comment that your Handy Browser will understand and interpret, « command » must be replaced by NO_EDIT, NO_PRINT or NO_SAVE. The other browsers will not do anything with this command since they will « see » it as a simple comment.

If you use several of these commands, there must be one line by command in your pages. The syntax of these commands must be strictly respected, including lowercase and uppercase letters. For example :

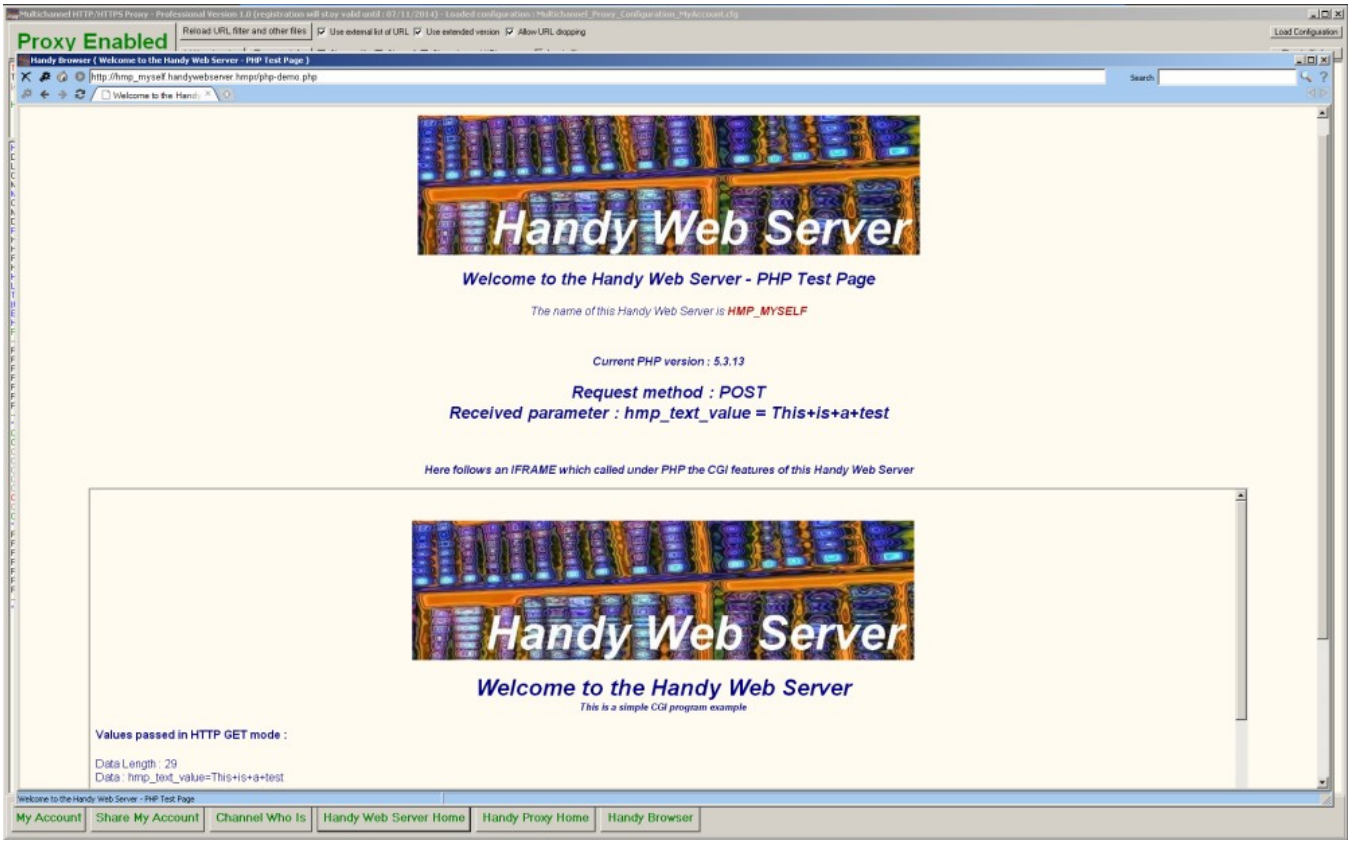
```
<!-- #Handy_Web_Server_NO_PRINT# -->
```



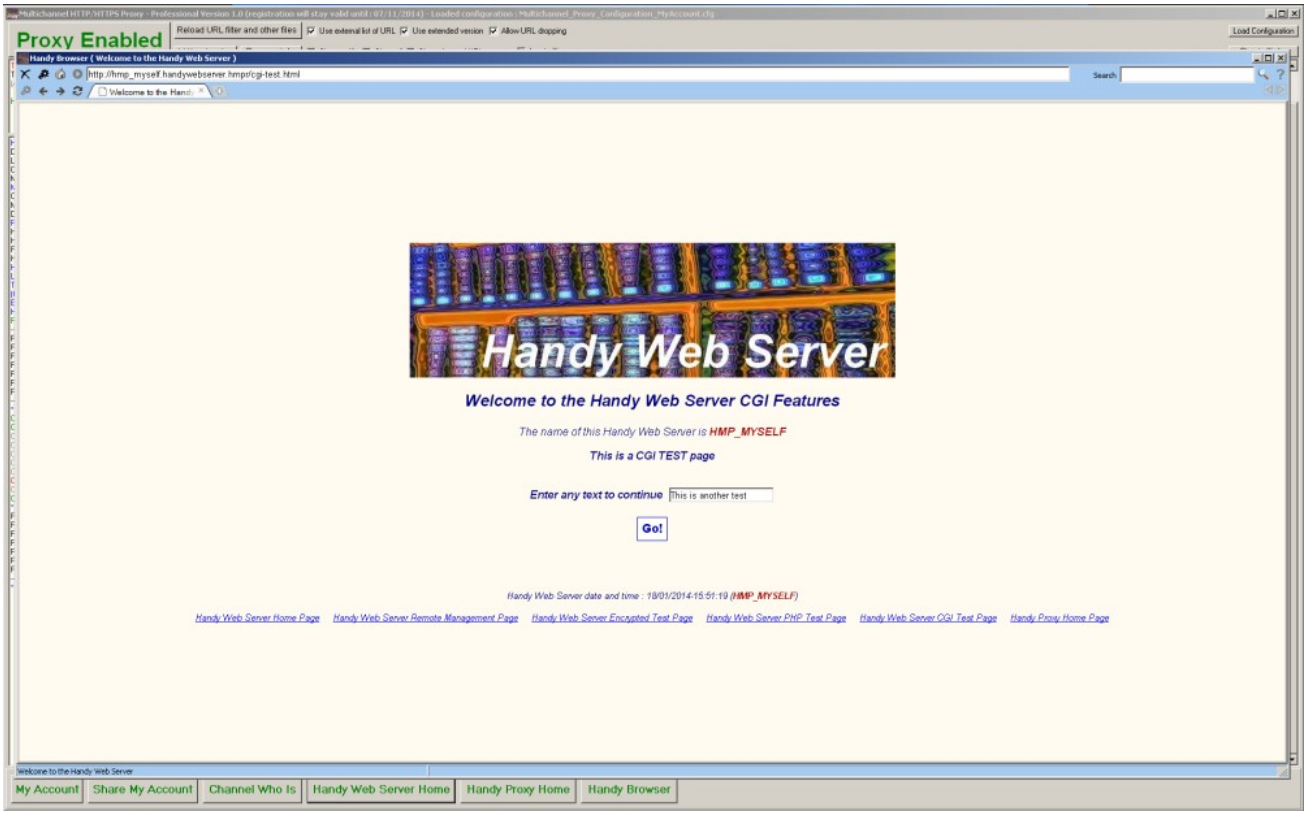
From within the default web page, you can gain access to another page allowing to test your integration of PHP modules from the « php-test.html » page. This page will allow you to call PHP modules via a GET or POST command.



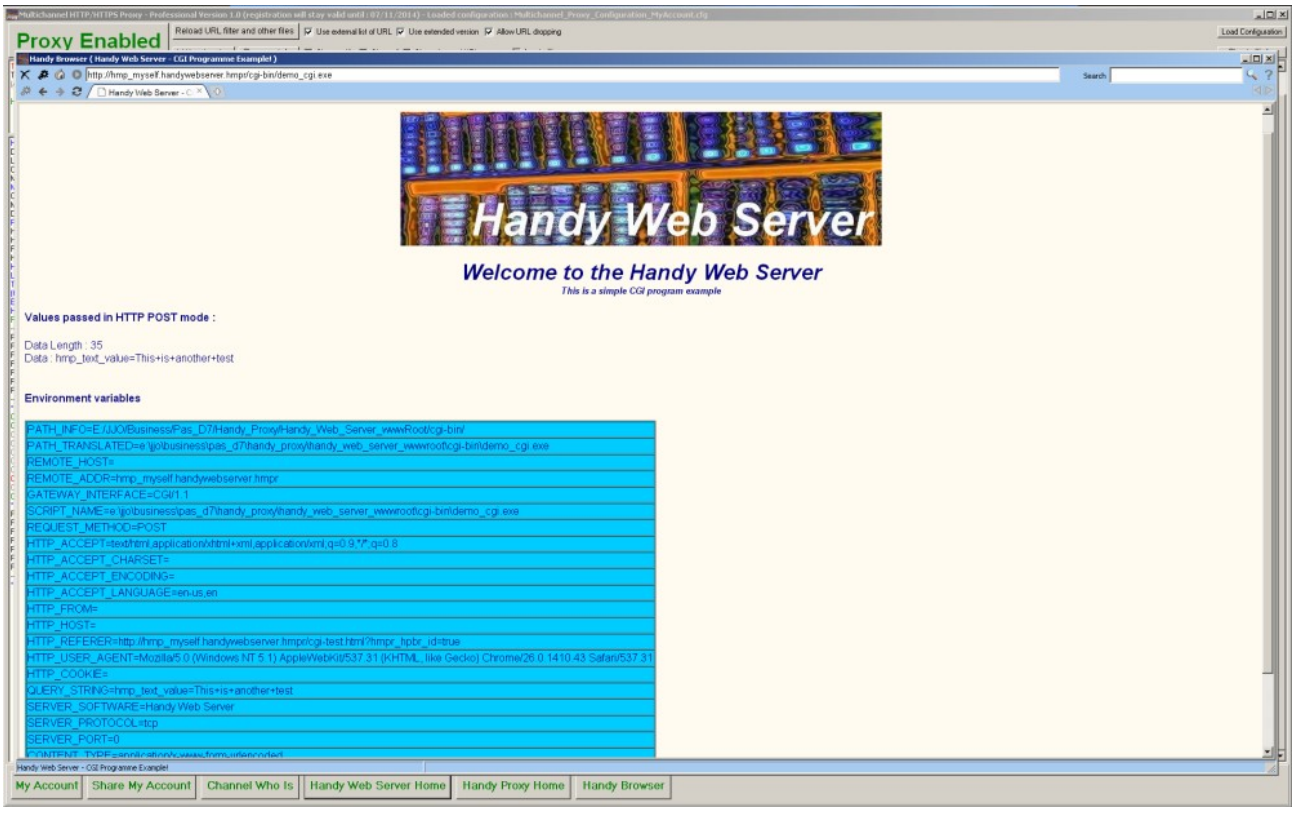
By clicking on the GET or POST button on the previous test page, by calling the « php-demo.php » page, you will get the following result listing the version of the PHP modules that are installed as well as the request result. You can thus create PHP pages of your choice and make them available via your Handy Web Server.



From within the default web page you can access another page that allows to test the CGI functions of your Handy Web Server from the « cgi-test.html » page. This page allows you to call a CGI module made available at the installation in the ..\cgi-bin directory under the name « demo_cgi.exe ».



By clicking on the « Go ! » button on the previous page, by calling the « demo_cgi.exe » module, you will get the following screen listing all the classical CGI parameters. You can thus create your CGI modules and make them available via your Handy Web Server.



Important remarks :

All HTML, Javascript, pictures or PHP files must be placed in the **…\Handy_Web_Server_wwwRoot** directory.
You can create subdirectories in this directory where these files can also be placed.

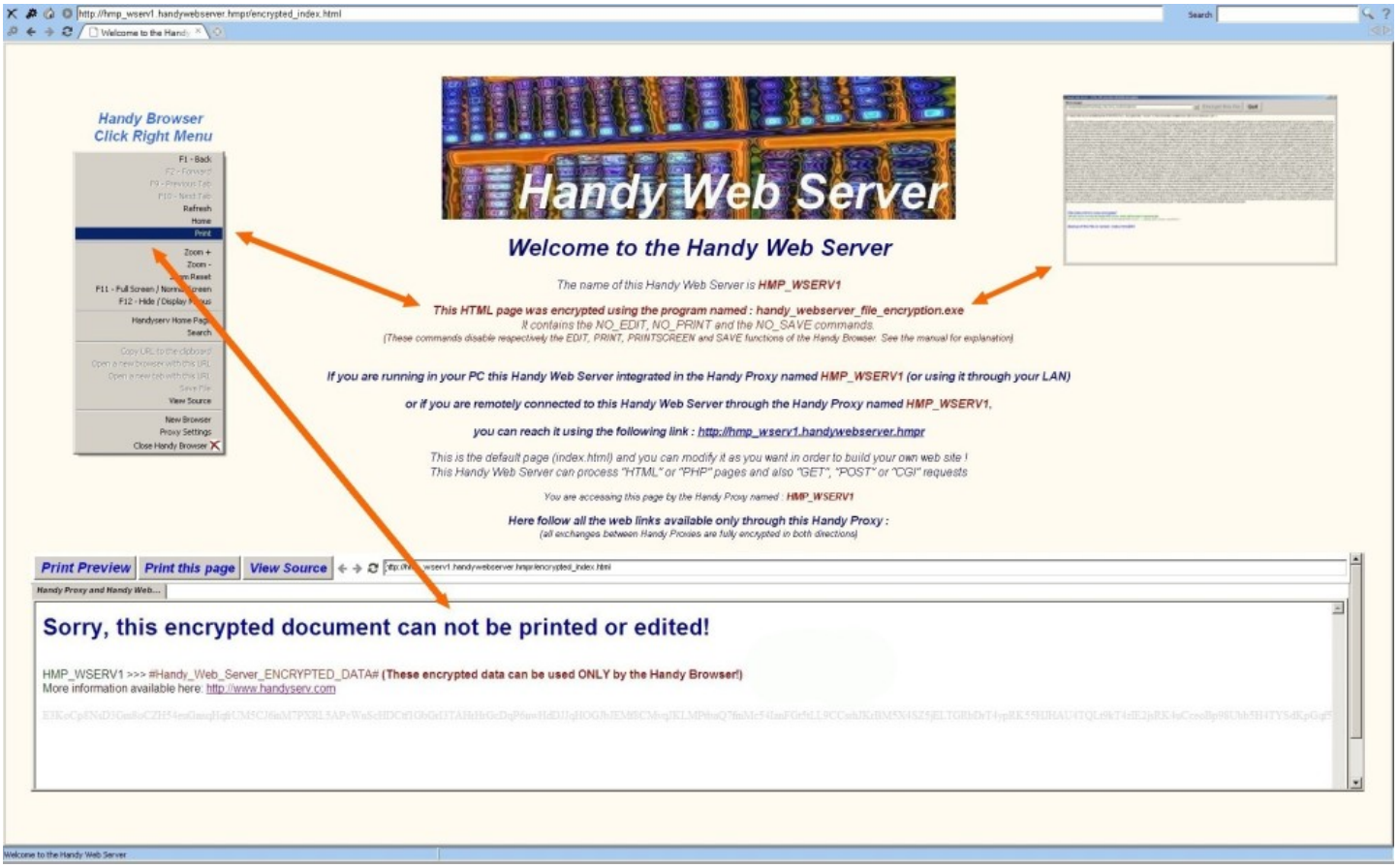
All PHP INCLUDE files must be placed in the **…\Handy_Web_Server_wwwRoot\php_includes** directory.
See paragraph Handy Proxy Master Configuration File (Multichannel_Proxy_Master_Config.def ; parameter name : Path_To_PHP_Apps) and the PHP configuration file (php.ini ; parameter name : include_path).

All CGI files must be placed in the **…\Handy_Web_Server_wwwRoot\cgi-bin** directory.

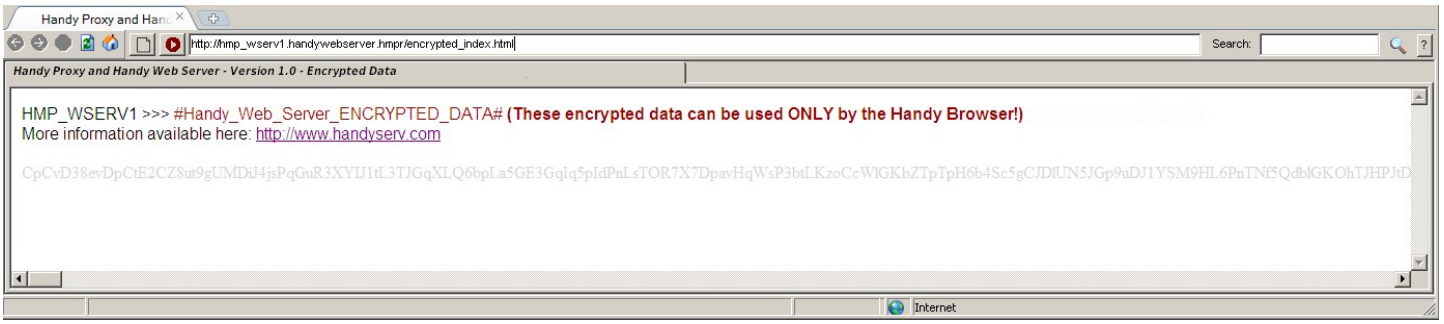
6. Handy Web Server File Encryption

As explained in the previous chapter, you can encrypt your HTML, PHP, etc. pages in order to protect your developments in case you are sharing your pages with other persons using a Handy Proxy.

In the following overview you can see, on the right, the screen of the page encryption program. The pages may include specific commands (see previous chapter) that will be understood by your Handy Browser. By right-clicking on this screen you will open the menu you can see on the left and, if you try to print the page that is displayed, a window will open indicating that this function is not authorized.

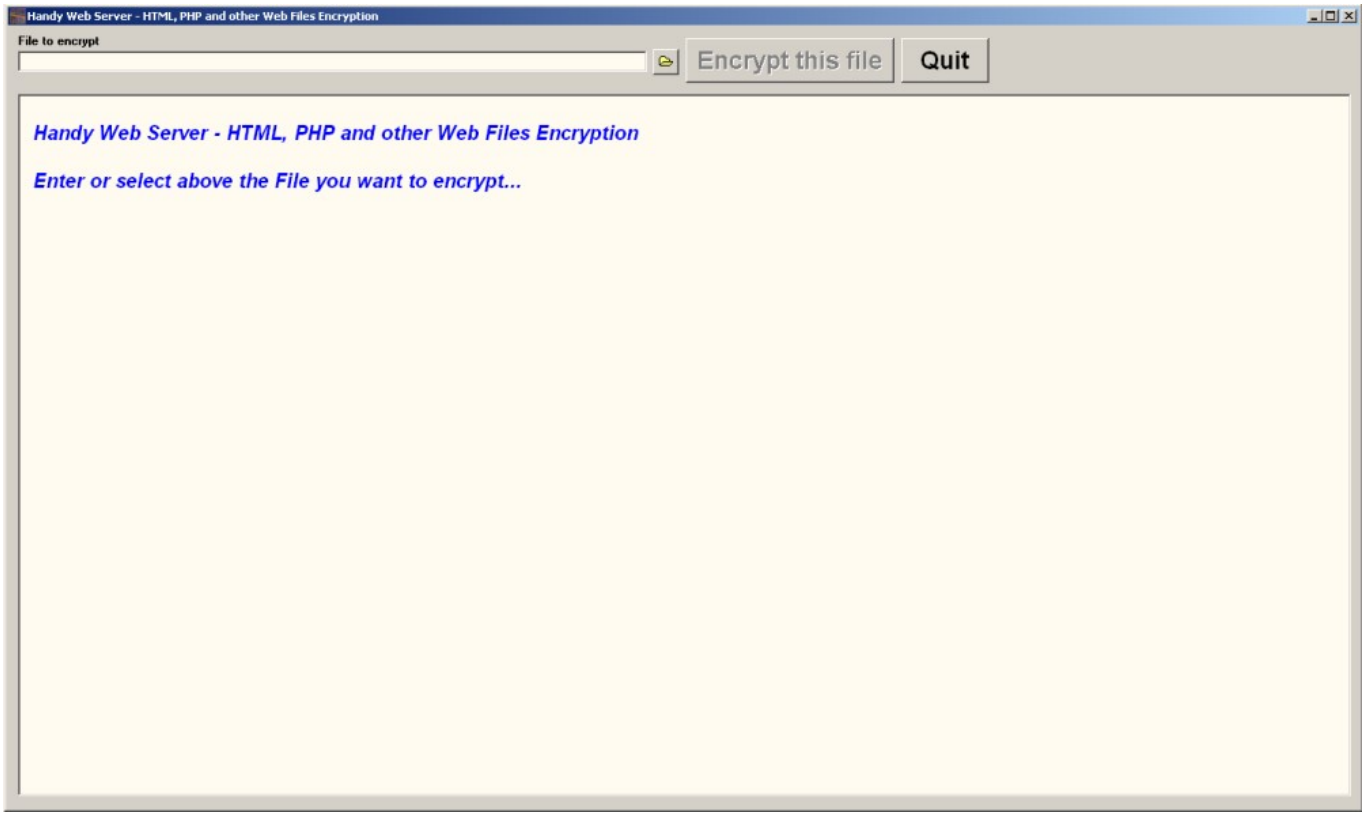


Any other browser that would be used to visit this previously encrypted page will display the following message. Encrypted pages MUST be accessed via your Handy Browser.

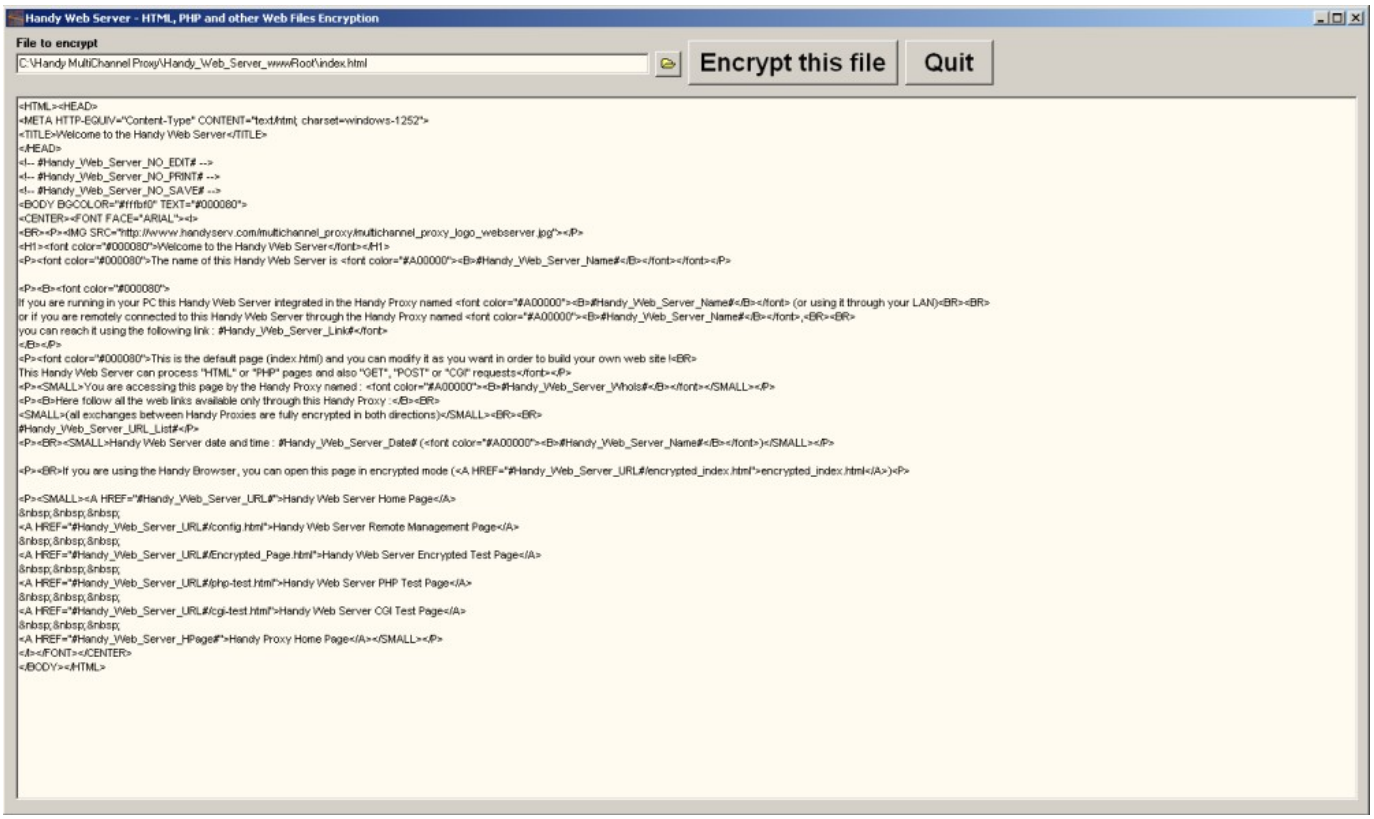


Here is how to encrypt your pages :

Go to your Handy Proxy's directory and launch the « handy_webserver_file_encryption.exe » program. You will get the following screen :



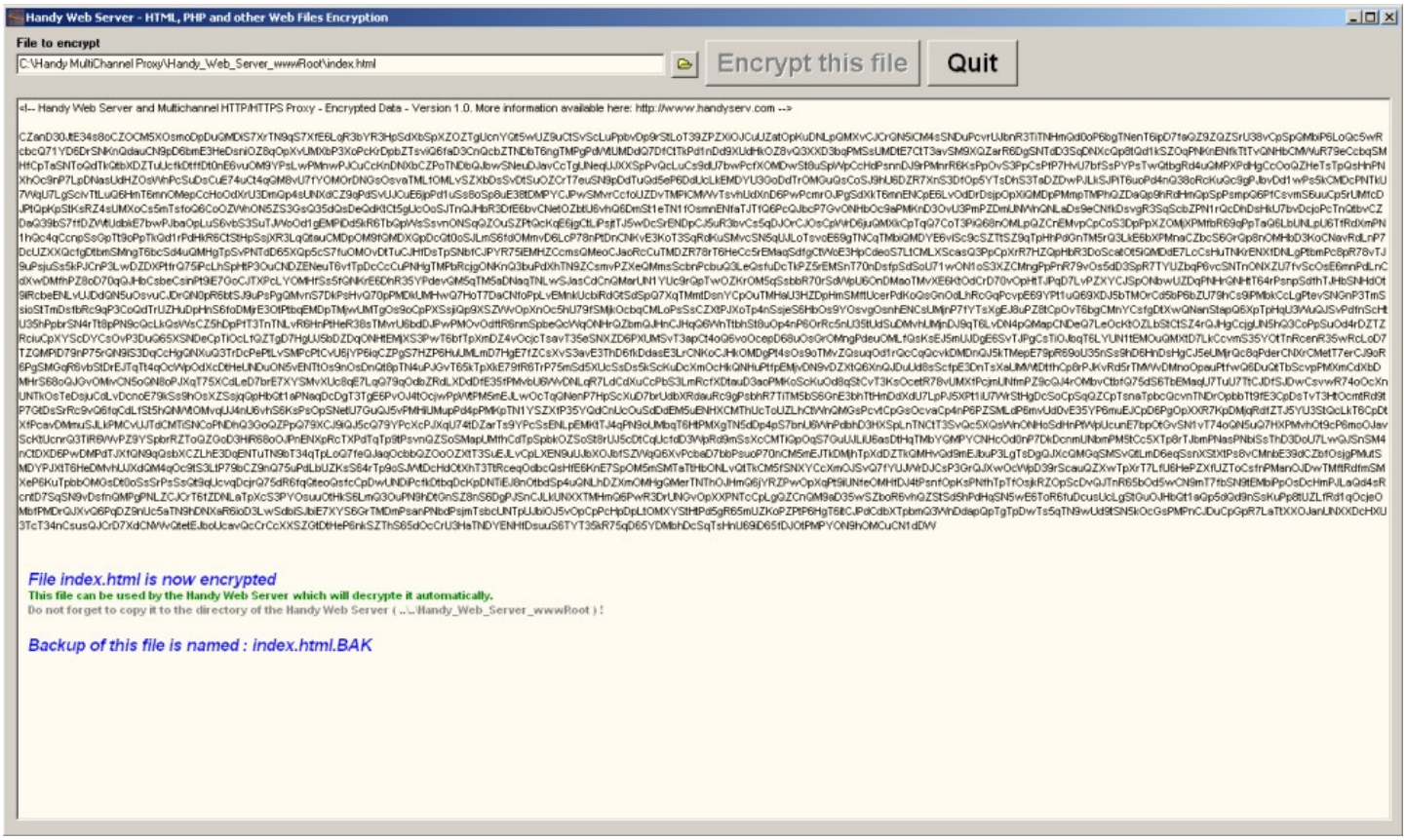
Select, in the directory of your choice, the HTML, Javascript, PHP file of your choice or any other text file you would like to encrypt. The file appears unencrypted on the screen. Click on the « Encrypt this file » button.



The program will then encrypt your file by creating a back-up of the file under its original name followed by a .bak extension. The encrypted file has got the same name than the original file. You must place this file in the **…\Handy_Web_Server_wwwRoot** directory of the web server.

We advise against encrypting files in this directory since you could forget to delete the .bak files. If you delete the .bak files in the web server's directory you might delete the unencrypted source files. Be very cautious while using this encryption program, since the process is irreversible. We do not provide any decryption module, except the fact that your Handy Web Server and your Handy Browser are able to decrypt these pages. If we provided such program your pages would be decryptable by third parties, which would make this function useless.

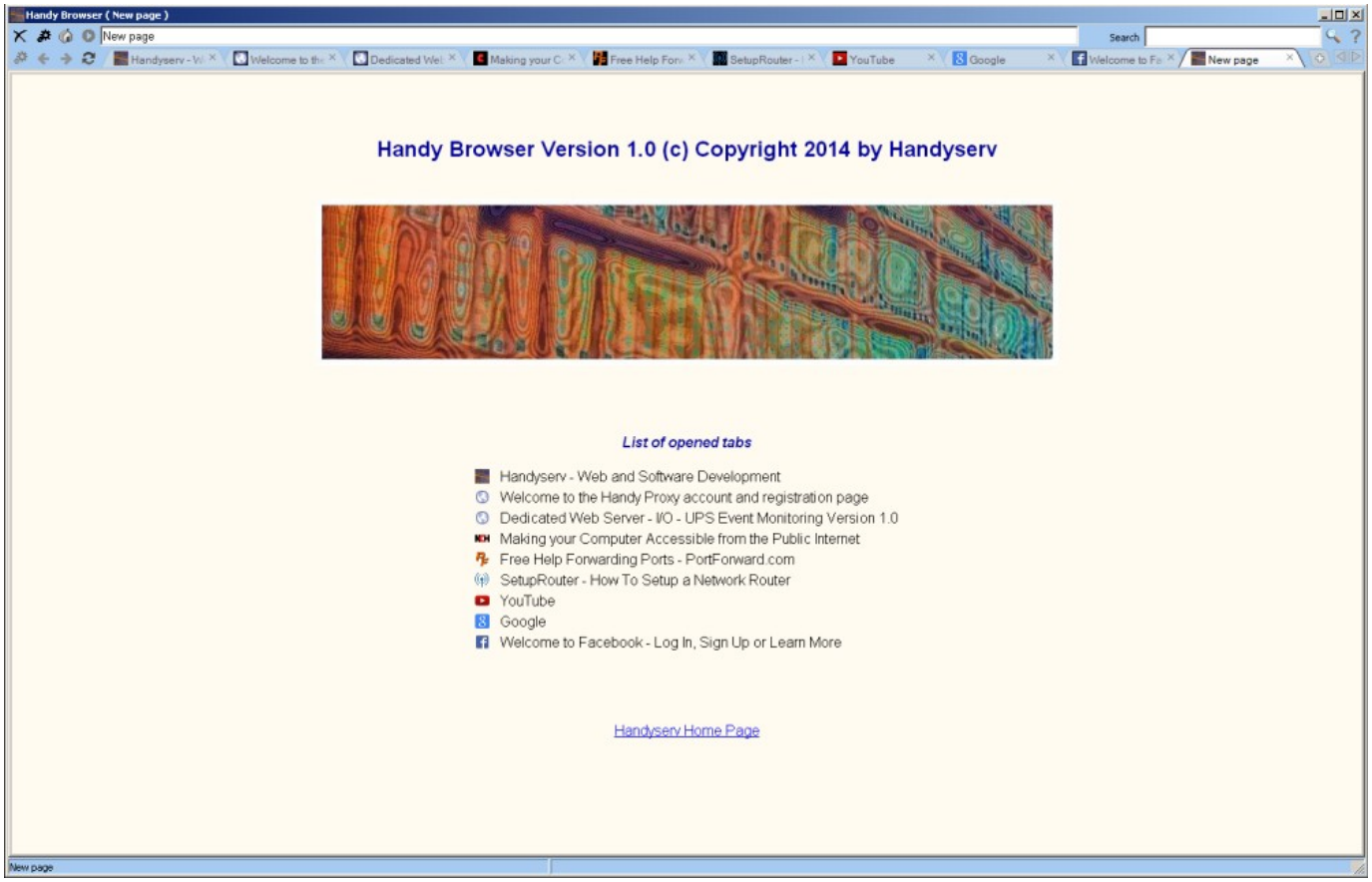
To avoid any loss of data, we invite you to create your web pages into an « X » directory, to copy them afterwards into a « Y » directory to encrypt them thanks to this program, and to finally copy them into your Handy Web Server's directory.



7. Handy Browser

Your package includes a browser named Handy Browser. Handy Browser is a browser as many others ; it is based on the Chromium (c) technology and is thus compatible with today's Internet technologies. You can use it to visit Facebook, Youtube, etc. However, the current version of this browser does not allow to install add-ons as Java or other tools as customized navigation menus, etc.

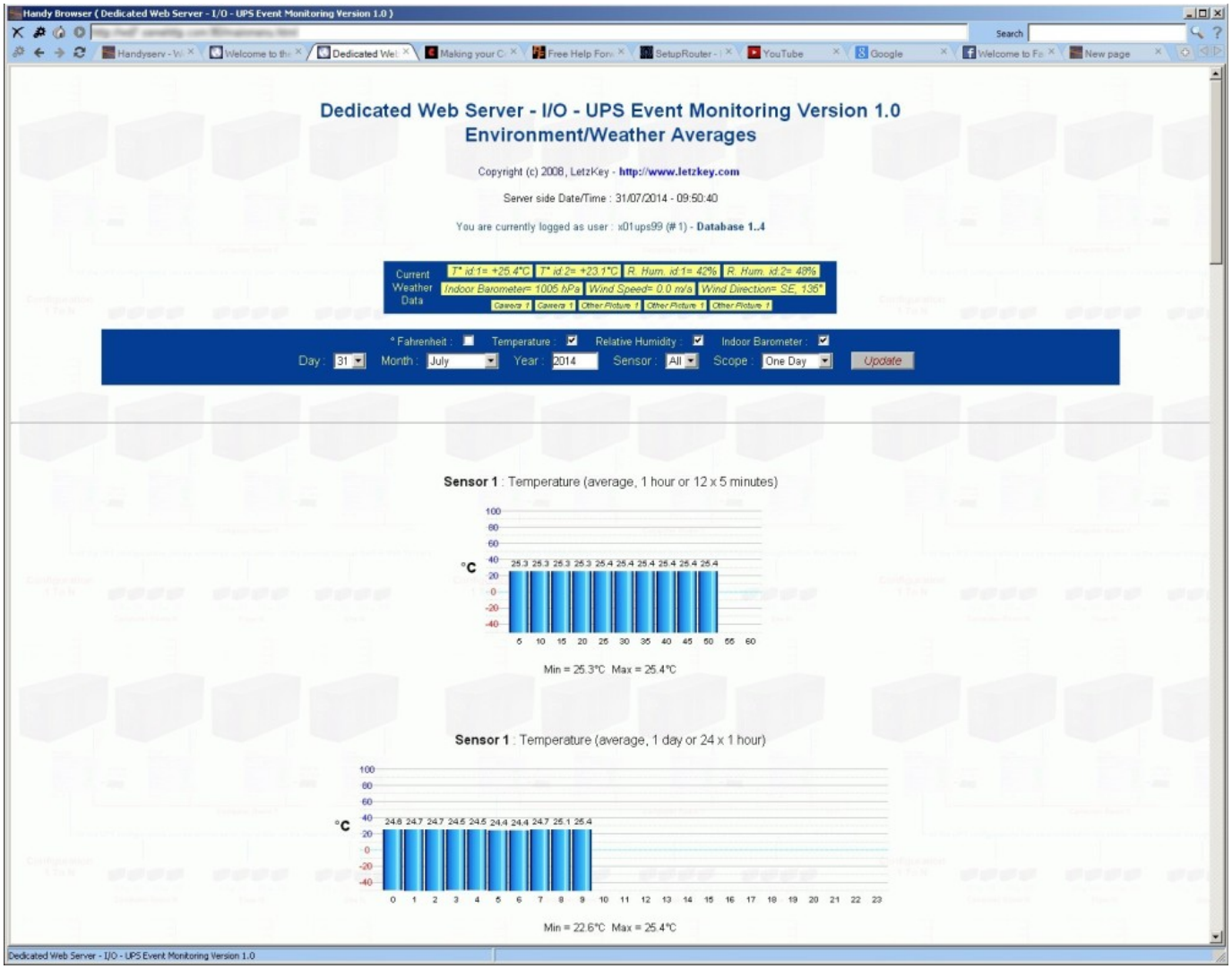
Handy Browser is not, consequently, a « full-feature » browser, but it is able to display the pages encrypted by the « handy_webserver_file_encryption.exe » programme (provided in the package) and made available via your Handy Web Server. For more information about this, please refer to the previous chapter.



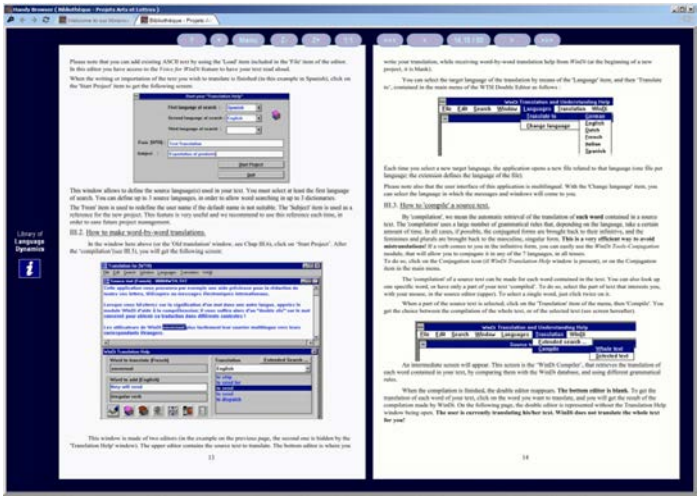
Handy Browser offers, in addition to the multi-tabs function, classical navigation features as well as « full screen » options that are described further in this manual.

Here below you can see an example of the call of a web service available via the address and link rerouting that we will see further in this manual. This web site is not public and was completely encrypted by a Handy Proxy.

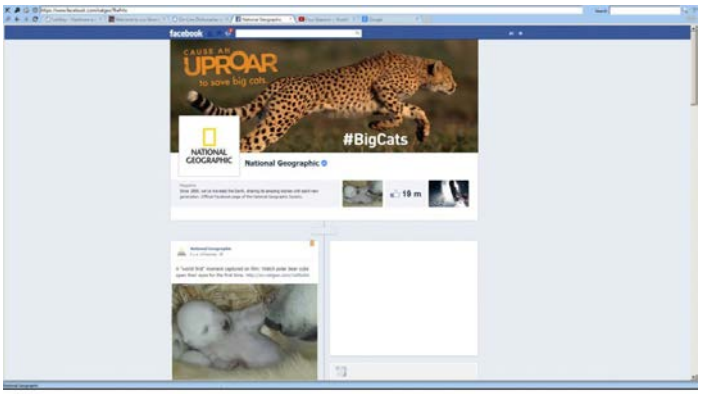
As you can see, your Handy Browser allows multi-tabs. You can see that one of the tabs is open on Youtube, another on Google and a third one on Facebook.



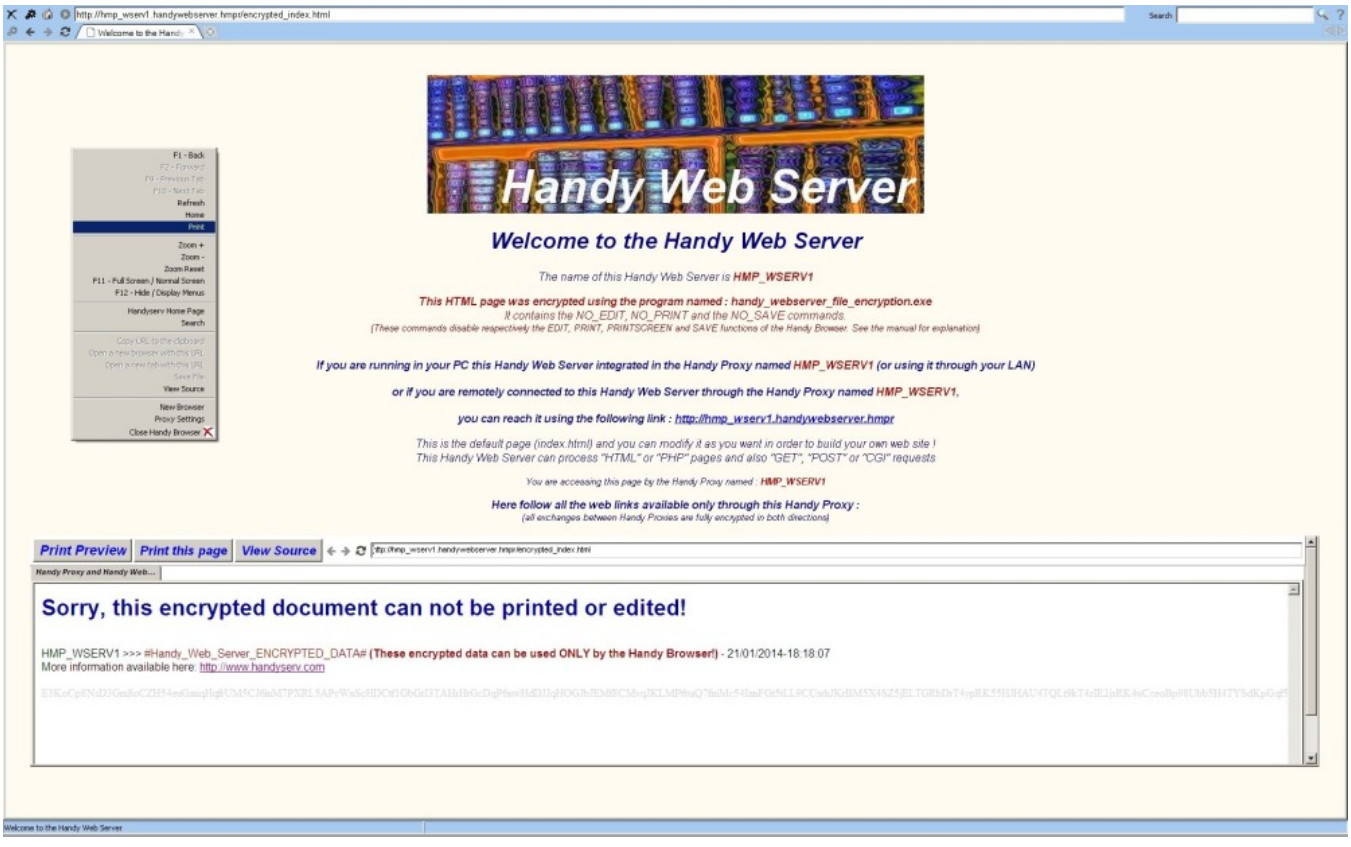
Here are examples of use with public web sites :



The two examples below show pages open by your Handy Browser on Youtube and Facebook :



Here is an example of use of your Handy Browser with an encrypted page containing specific commands (for more information about this, please refer to the previous chapters) :



7.1. The different screen modes of the Handy Browser

Your Handy Browser offers 4 « full screen » display modes. You can either call them via the main menu of this browser, or by right-clicking. In this case you will get the following menu with functions F11 and F12, which means that these 2 functions are also available via your keyboard.

The 4 modes are (as illustrated by the screens below) :

- Full display of menus, tabs and Windows title bar ;
- Partial display of menus, tabs and Windows title bar ;
- Partial display of menus and tabs ;
- Display of the web page only (contrarily to other browsers, this mode allows you to keep access to the Windows task bar).

8. Handy Communication

8.1. Introduction

Your Handy Proxy includes two additional applications allowing to communicate with persons using this same tool. These two programmes are named Handy Email and Handy Messenger.

As explained previously, all exchanges between Handy Proxies are safe and encrypted. The same applies for these two programmes that also exchange data in a safe and encrypted way by sending them through your Handy Proxy.

These two applications operate solely in « computer to computer » mode (client-server) without using any storage Internet website, which guarantees full confidentiality of exchanges between your addressees and yourself. **The principle is to create a messaging server via a Handy Proxy. This server is a PC dedicated to this function inside a family, an association or a company. It should ideally be available 24 hours, 7 days a week,** but it can also be used for other applications since your Handy Proxy is a Windows task as another, non exclusive. If you expect a high volume of data exchange between this server and your addressees, we advise you to fully dedicate a PC to that function. It will then be a true server since its machine time will be entirely available to the Handy Proxy and its server functions. The Windows version of this PC can be Windows 2000, XP, 7 or 8, which means that any PC, even older, can be used.

We repeat that if a messaging server you are trying to connect to is not available (not on-line or switched off), you will not be able to send messages to your addressees via this server. It is therefore crucial that this or these machines are available via the Internet at the time you want to send your messages. Please refer to chapter 2.1 explaining how to proceed. In spite of this, it is still possible to communicate with servers that are available only from time to time ; your messages will then be processed only when these servers are accessible. This situation can make the exchange delays randomly long, since you and your addressees would have to connect at the times of server availability.

How do these applications work ?

If your addressee is connected in your LAN, exchanges will happen locally without using the Internet. In the case of a remote addressee, these two programmes will use Internet as a data carrier, in client-server mode as previously explained and in a totally safe way since all data will flow via the Handy Proxies (the one of the server and the one of your addressee).

To achieve this, these programmes will first try to connect to the server(s) locally (inside of your LAN) and if this attempt does not succeed, they will automatically launch a remote communication attempt by using the Internet as a data carrier and still in a client-server mode via the Handy Proxies.

All the message exchanges are based solely on the « http » protocol, which means that no other communication protocol is used and no specific communication port is open on your side or on your addressees' side. Again, this method guarantees the safety of exchanges since it does not require to open a port that could be accessed otherwise than via your Handy Proxy that includes the indispensable access protections as explained in the preceding chapters.

Since these two programmes connect from computer to computer in client-server mode, the possible connexion problems between your configuration (server and/or client) and your addresses' configuration must be managed. In order to solve this kind of problem that will unavoidably happen since the Handy Proxies of the target servers might be off-line at a given time, your Handy Proxy contains, in addition to its other functions, a messaging server that allows to safely deliver your pending messages. It must be clear that the messages that remain pending because the target servers are not on-line *stay on your side*, waiting to be delivered. If one or several messages to one or several addressees is not immediately sent out, the messaging server included in your Handy Proxy will attempt, for 8 days (priority mode), to reach the target server(s) to deliver the pending message(s) as soon as possible. Afterwards (non-priority mode), when the target servers are on-line again, your messaging server will immediately deliver the messages which are still pending and which are dated of more than 8 days.

Consequently, the best way to use these two applications is to let the Handy Proxies that are used as messaging servers work as often as possible so that they can send your pending messages to your addressees. This will also allow you to receive the messages that were sent to you as soon as possible.

The defined servers will be contacted in two different ways :

- **Slow mode** : this mode is the one by default when the Handy Email and Handy Messenger applications are not active. When a message is received, your Handy Proxy starts the concerned application (in the event it is not active yet) and the fast mode is engaged. The slow mode (« slow polling ») corresponds to a 10-minute cycle.
- **Fast mode** : this mode allows to fetch and send your messages to the defined servers in a fast way. The fast mode (« fast polling ») corresponds to a 1-minute cycle for Handy Email and to a 30-second cycle for Handy Messenger. This mode gets back to slow after 15 minutes.

The state of your messaging servers is displayed on the Handy Proxy screen according to the slow or fast mode. You can cancel this visualization via a parameter (see chapter 9, file Multichannel_Proxy_Master_Config.def).

In order to send an instant message or an e-mail to an addressee, you have to know both the name of his/her Handy Proxy and the name of the server he/she is connecting to, i.e. the name of the Handy Proxy used as a messaging server. These two informations must be entered manually into the file defining the addressees and the target servers (see next paragraph).

The method according to which you have to add manually the names of the Handy Proxies of your addressees to be able to write them is classical and similar to other services. Thanks to our method, you will communicate only with the persons included into the addressees' list and nobody else will be able to send you messages. This allows to stay exclusively inside a circle of well-determined addressees without ever receiving spam or unsollicited e-mail from unknown persons (ultimate anti-spam solution). However, the Handy Proxy team found it interesting to give addressees who are not included in your list the possibility to write you in a way that their messages reach you and stand by, in a transparent way. This will work only if this person knows the name of your Handy Proxy. This allows to start exchanges in one direction ; you are then free to add the person(s) in question into your addressees list if you wish to. The applications will tell you whether such kind of messages are on hold. You will not have to include their senders into your list to read them, since an overview function allows to read the messages without opening them. You can remove a message you do not like without opening it, and its sender will not appear anymore. If on the contrary you are willing to correspond with the sender, one click of the mouse allows to include him/her into the addressees list and you will be able to reply to the message, forward it to other addressees, etc.

8.2. Configuration of Handy Email and Handy Messenger : first steps

First and foremost, and before being able to send an instant message or an e-mail, you have to create your addressees list as well as the list of the messaging servers you will connect to. The principle is exactly the same as when you send an e-mail via your usual applications, since you add to your addressees list the name of your addressee followed by a server name, both items being separated by the @ character, as for example « john@emailserver.com ». In our case, the only difference is the syntax : you will use the « > » character instead of « @ ». For example, as we will see below : « Kimberly>Bradley » translates by : « Kimberly » can be reached via the server named « Bradley ». This is identical to the way your usual messaging solution works. The syntax difference, via the « > » character, allows to clearly differentiate one application from another in order to avoid the integration of classical e-mail adddresses in the Handy applications and vice versa.

The addressees list can solely be accessed via the Editor we have included in this package, since this file is encrypted. You can also protect the access of this file by a password. You could afterwards provide this file to family members, friends or colleagues ; they will not be able to modify it since they will not know your password. For more information about this, please refer to the configuration files of your Handy Proxy and more specifically the file « Multichannel_Proxy_Master_Config.def » which is encrypted and password-protected (password by default : 1234).

Your addressees list follows a syntax that must be strictly respected, otherwise, either it will be rejected (by the applications that make use of it) with an error message indicating which problems were encountered, or you will not be able to send messages to an addressee because for example his/her server is ill-defined (or non existing).

Important remark : the applications systematically check whether the defined servers exist and whether they are present into the Handyserv databases as recognized users. The same verification applies to the addressees. In case of syntax error, server or addressee duplication, the applications will send no message unless those errors are corrected in order to make sure that your messages reach the right addressees on the right servers. It is your responsibility to create existing and consistent servers and addresses.

At the launching of your installation, you must first give your Handy Proxy a name of your choice that you will be able afterwards (and only afterwards) to define as a messaging server. If you try to reach a server which is not defined yet, the applications will notice that there is an anomaly and they will not start ; they will display an error message instead. This PC will have to be accessible via the Internet if it is not connected to your local network. Please refer to chapter 2.1 of this manual which explains how to proceed and how to share your Handy Proxy and its messaging server functions.

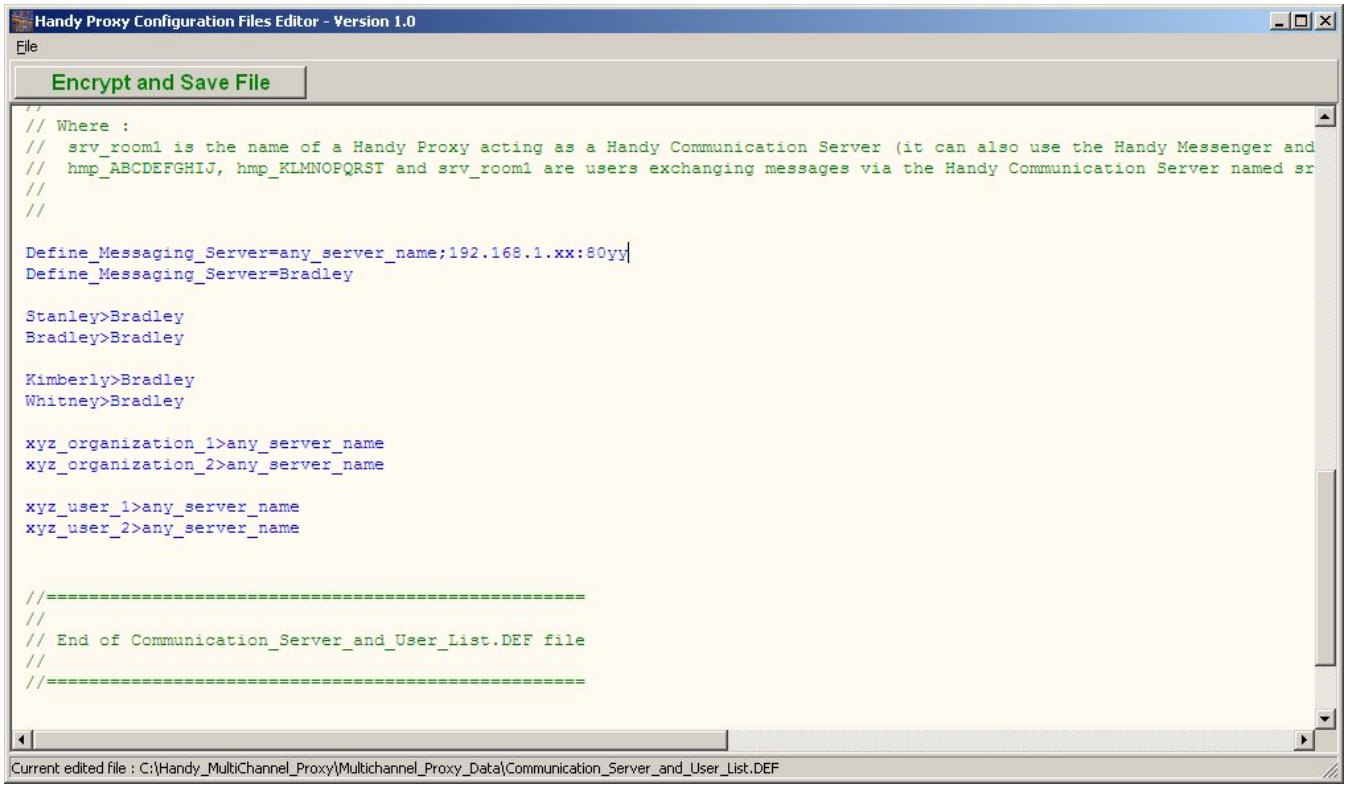
ATTENTION : if your configuration is also used as a messaging server, you cannot modify the name of your Handy Proxy since your addressees will use your machine as a server. If this name changes, they will not be able to retrieve you.

Now, let us take an example of definition via the Handy Proxy configuration file editor.

In this file, you must **first and foremost** define the server(s) you and your addressees will connect to. Any server that would have been defined after the addressees list will not be held into account, and an error message will automatically

appear to tell you that a definition is missing. After having defined the messaging servers, you will be able to include your addressees list, as in the following example.

Here is the screen of this editor open on the addressees list. This file can be reached via the « Edit » menu, « Edit Addressee List » item available in the Handy Messenger and Handy Email applications :



The definition of your messaging servers, either local or remote, must respect the following syntax :

Define_Messaging_Server=[server name];[local IP address in your network]:[port]

The « IP address » and « port » parameters are optional, and are to use only if you have to reach your server from within your local network and possibly from the Internet via a laptop for example, if you are outside your local network.

Define_Messaging_Server=any_server_name;192.168.1.xx:80yy

This means that the server « any_server_name » will be accessible from the Internet via its address « IP:port » in your local network. Please refer also to chapter 2.1 of this manual.

If you never gain access to the local network of the server you want to connect to, define it as follows :

Define_Messaging_Server=Bradley

In the example above, « Bradley » is the name of a Handy Proxy used as a server and having to be defined as previously explained.

Remark : every server definition you will add will make it necessary to connect to it in order to check whether messages were sent to you or in order to send your messages. This can take some time. We therefore advise you to limit the

number of servers you will connect to. A number of 10 up to 15 servers seems reasonable. We advise you to gather your addressees on the same server, or to distribute them over a low number of servers.

After having defined the server(s) (and only after), you will list your addressees as follows :

Any_user>any_server_name

More specifically, and as in the example shown above :

Kimberly>Bradley

This address translates by : « Kimberly » can be reached via the server named « Bradley ».

After having defined your addressees and servers configuration file, you will be able to check this configuration as follows :

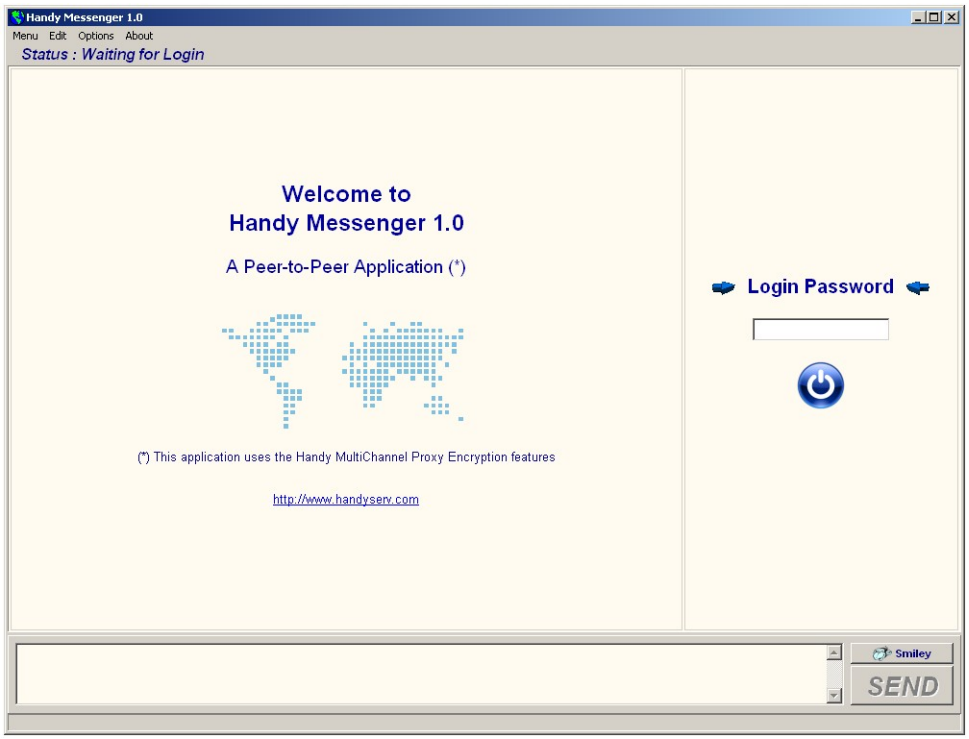
In the menu bar of Handy Messenger and Handy Email, the « About » item and the « List of my remote Handy Messaging Servers » option will give you the status of your connections with the different servers you are connected to. There are several possible cases : either a server is in your local network, or it is accessible only from the Internet. If a server is not accessible, this will be clearly indicated and you will be able to see if you are connected to this server via your network or from the Internet.
This list updates regularly but not in real time. If the status of a server changes, a certain delay is necessary before this option lets you know about it. The reconnection, if necessary, happens automatically and always after a delay of a few minutes.

It is imperative that the PCs that are messaging servers via the Handy Proxy remain switched on ! Otherwise they obviously will not be available and you will not be able to send messages to these servers. However, you will be able to create messages that will remain pending until the connection to the server(s) in question can be re-established.

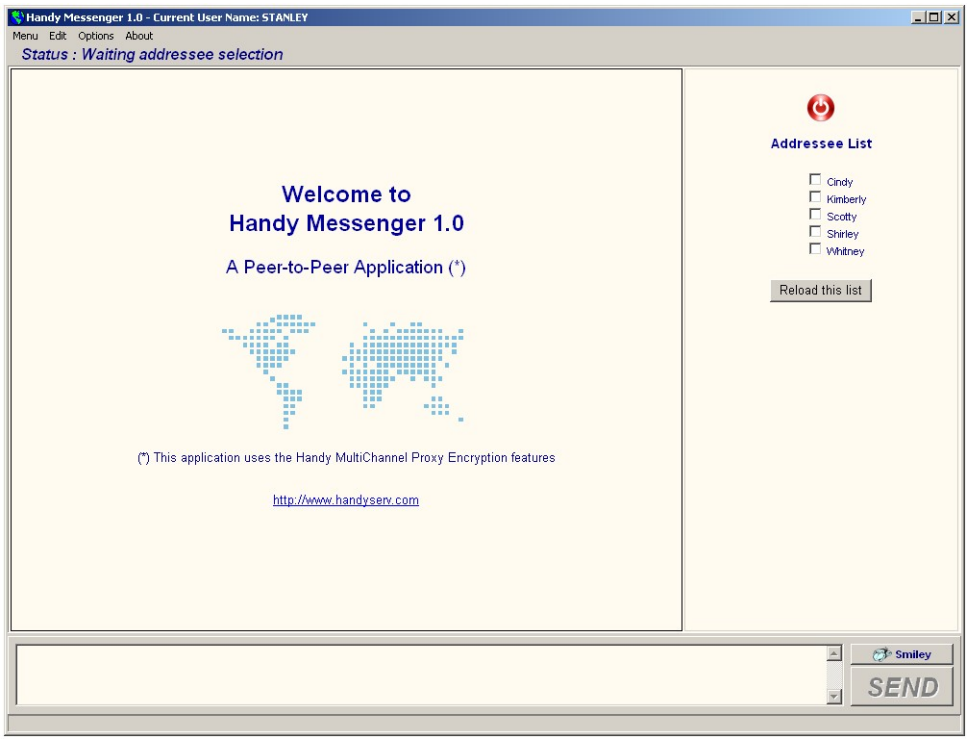
8.3. Handy Messenger

As explained in the introduction of this chapter, we remind you that this message exchange programme is completely secure and will only work between Handy Proxy users. It is therefore a condition that your Handy Proxy is running on your PC, otherwise Handy Messenger will not work since it will not have access to its safe and encrypted communication channel.

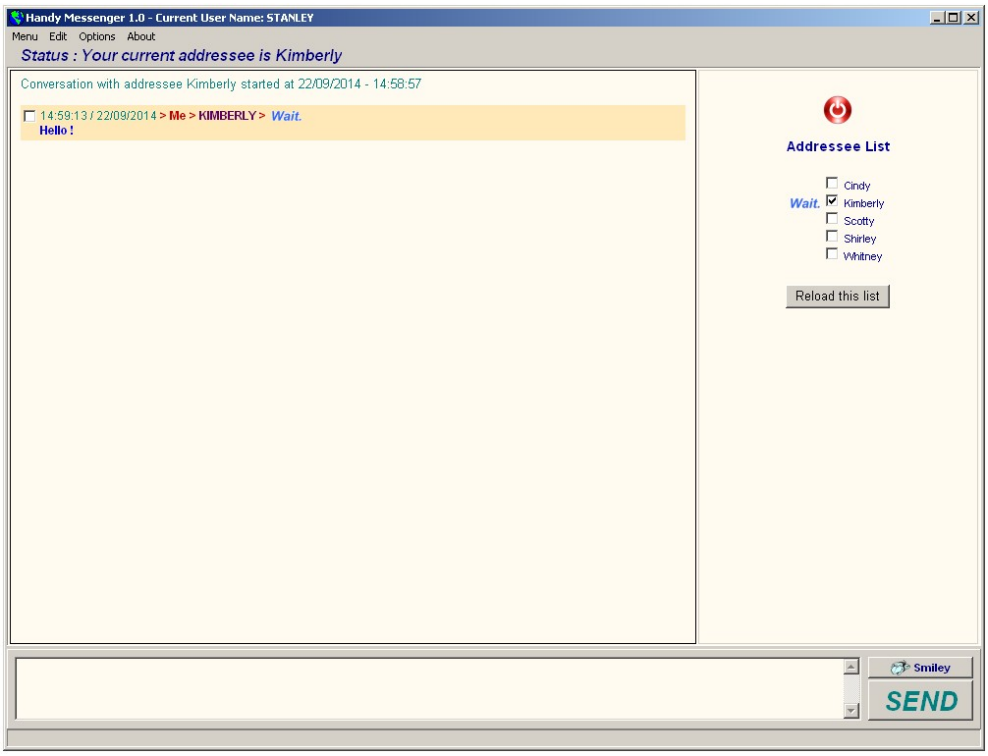
Here is the home screen that suggests you to login with your password (see configuration files to know more about this) :



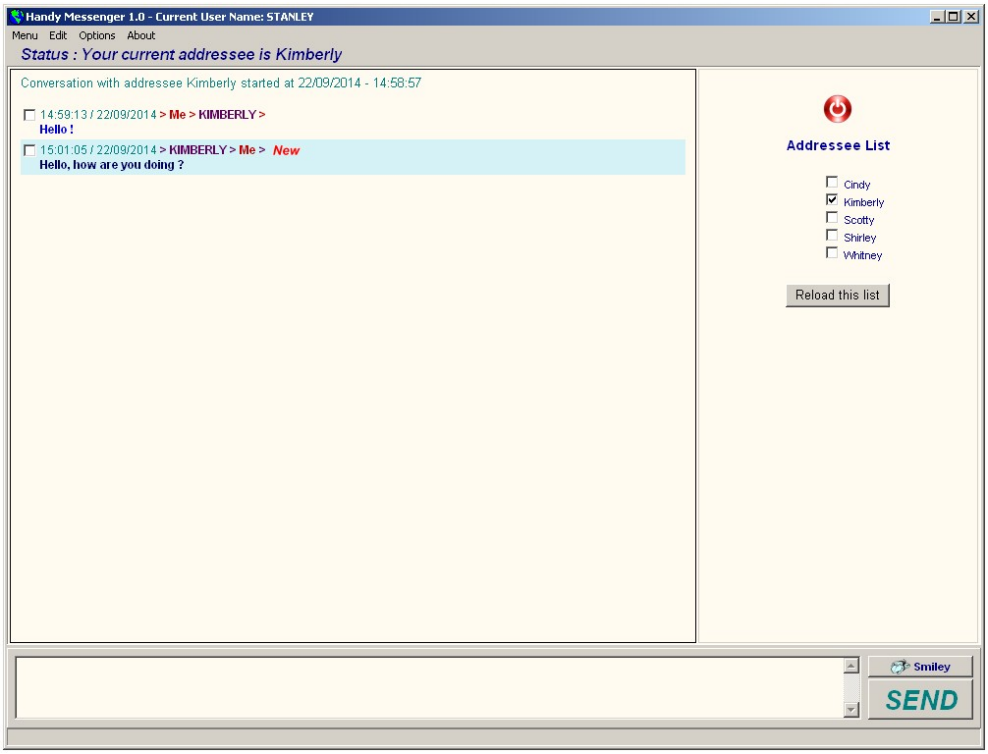
Once you are logged in, your addressee list appears :



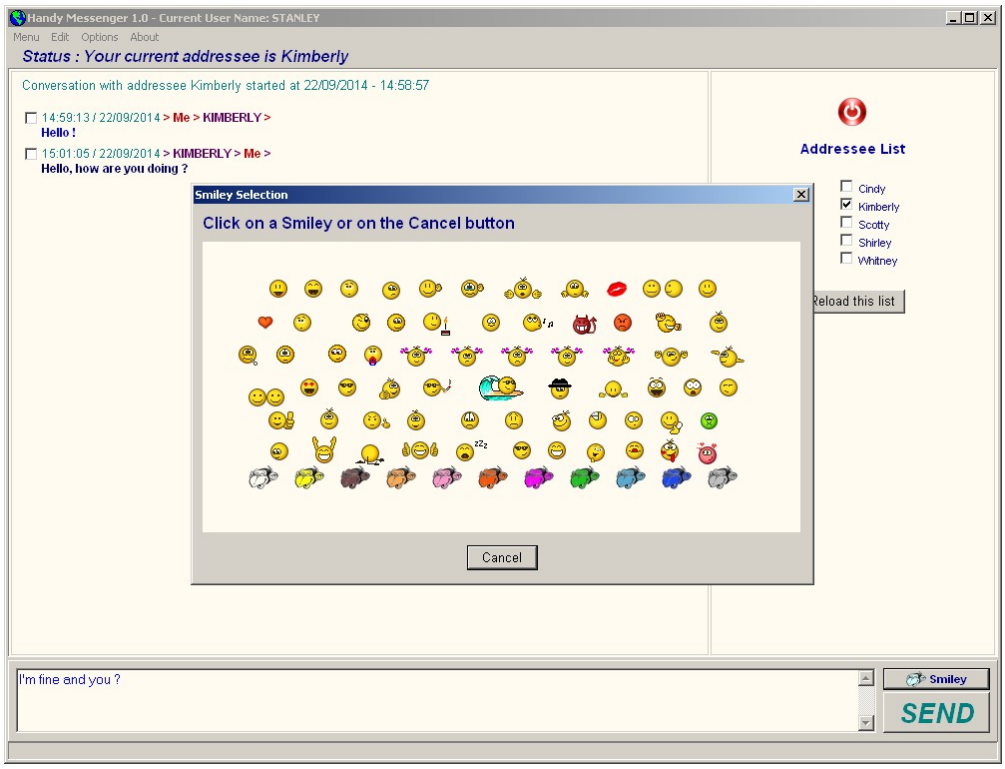
After having selected (checked) an addressee, you can start exchanging messages with him/her ; write your message in the lower part of the screen and click on the « Send » button to send it out, after which your message appears in the upper part of the screen and is immediately sent out to your addressee (as long as his/her Handy Proxy is on-line). If this is not the case, as we will explain further on, your message(s) will be « pending », i.e. waiting to be sent later. A series of blinking indicators allow you to follow the status of your messages. On the screen below, the indicator is « Wait. », which means « Waiting to be read » by your addressee to whom the message was already delivered. Moreover, new messages that have not been read yet appear against a light orange background.



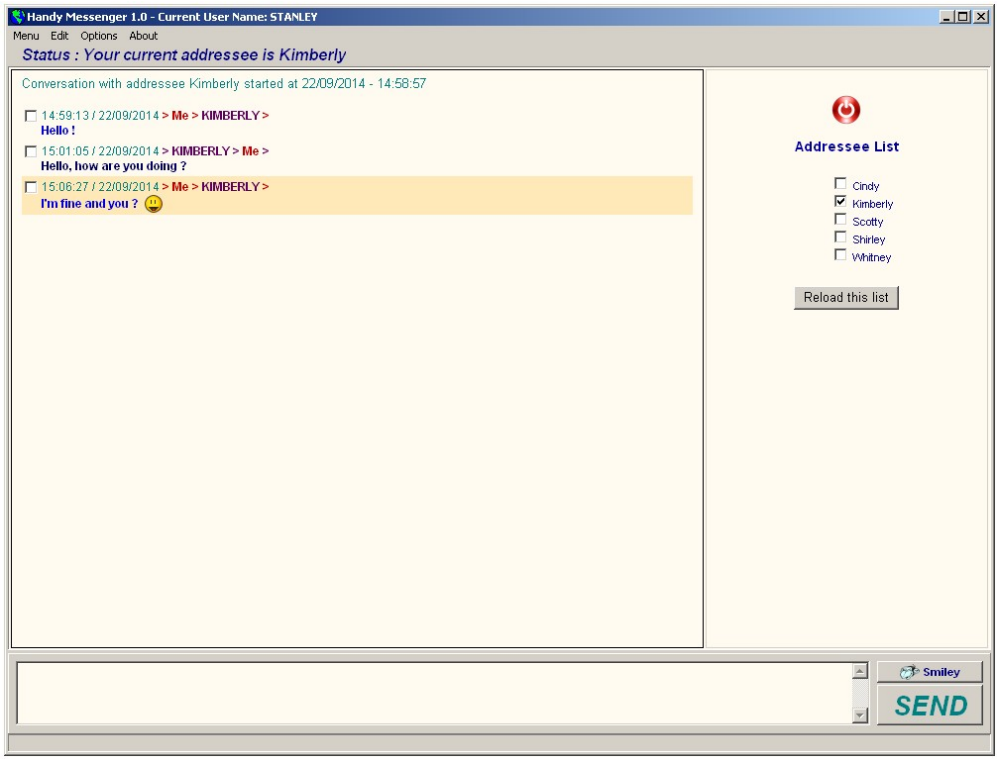
On the following screen the addressee had read the message since its state is not « Waiting to be read » anymore. The addressee has replied, and his/her message, with the status « New », is appearing against a blue background. On the addressee side, his/her message will have the status « Waiting to be read » until you see the screen below.



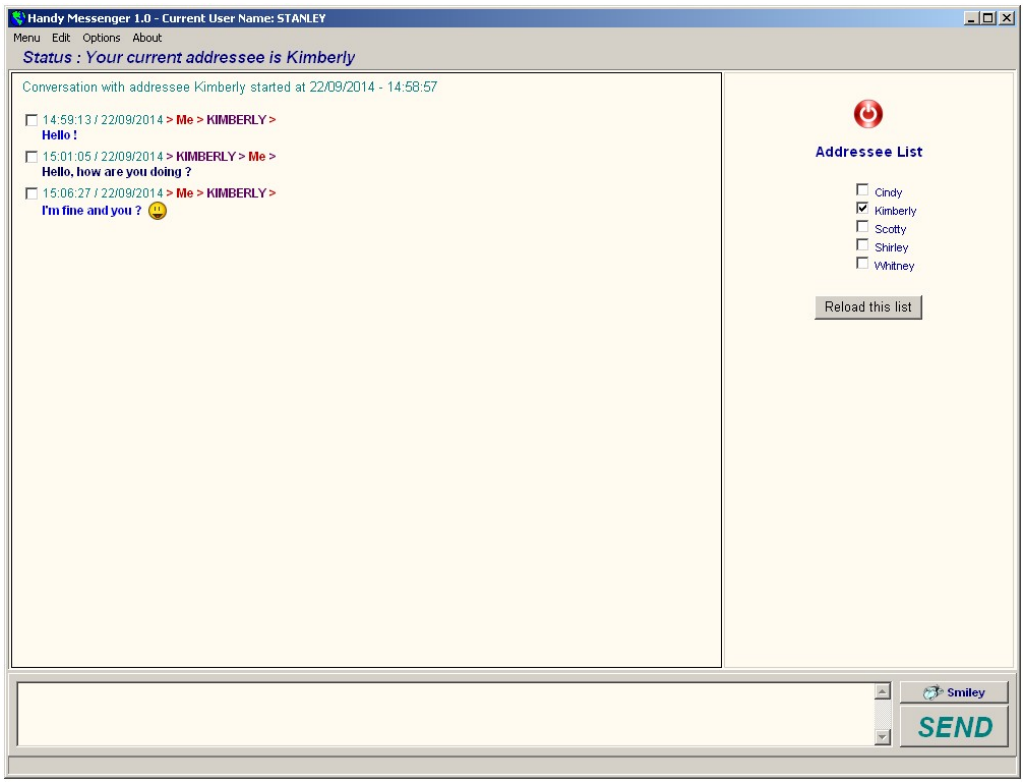
We have made available a range of smileys to enhance your messages. Click on the « Smiley » button in the lower right corner of the screen to gain access to the following screen allowing you to select the smiley(s) of your choice.



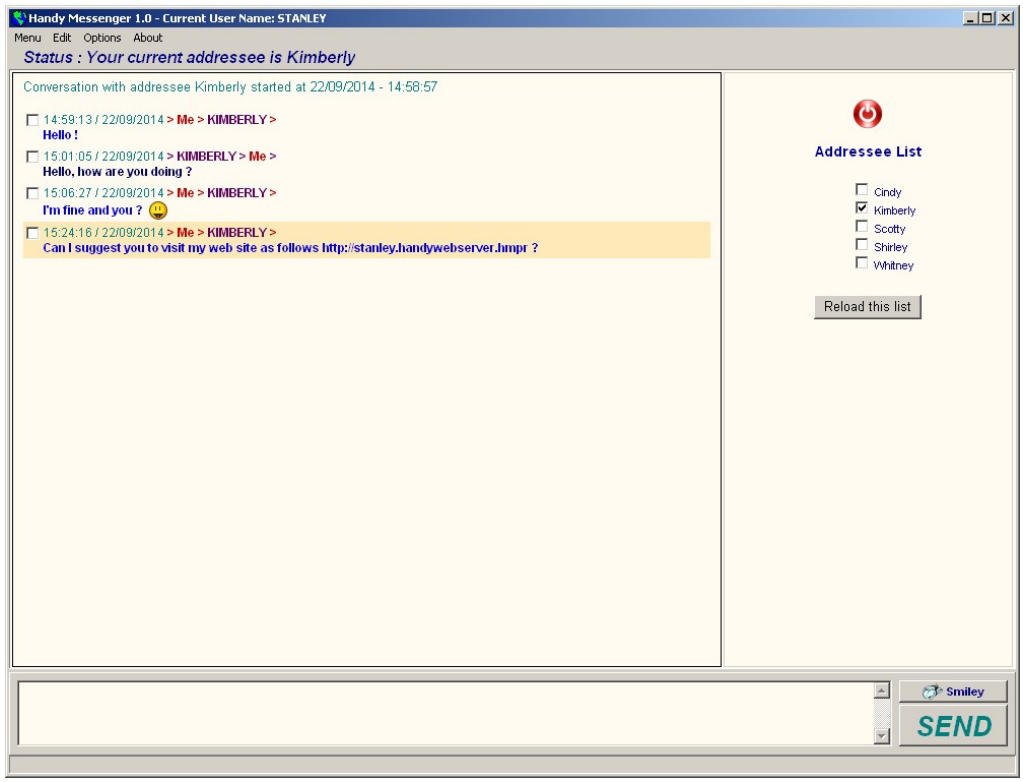
Here, once again, your message has immediately been sent out to your addressee :



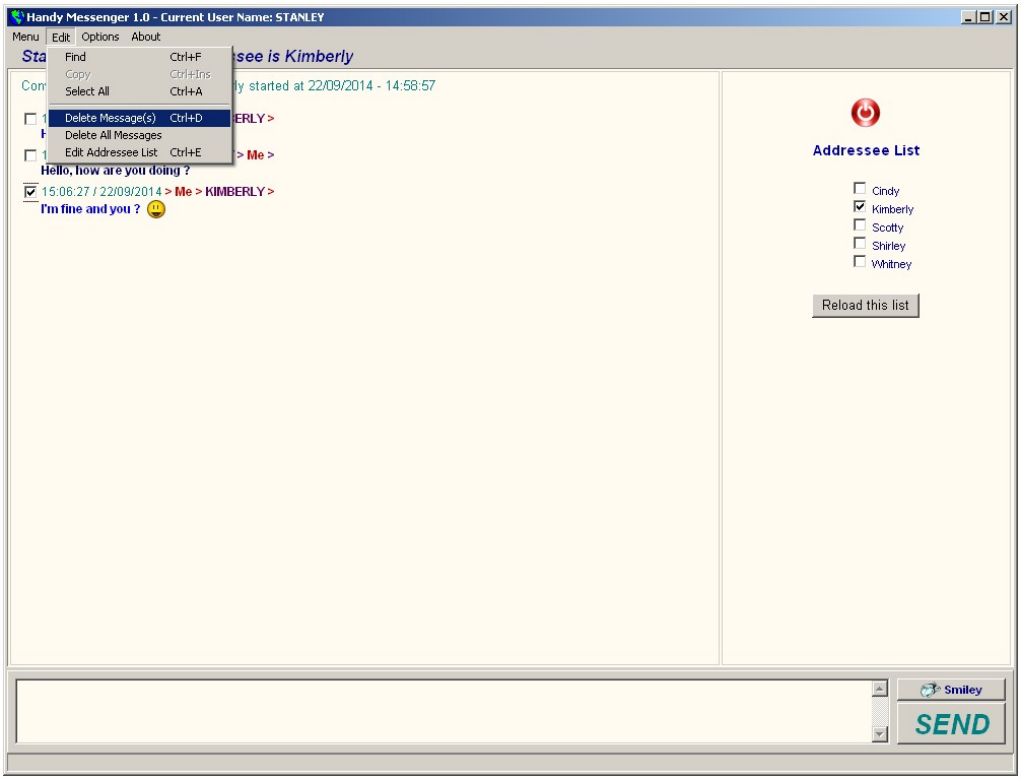
The following screen indicates that all your messages were sent out to, and read by, your addressee :



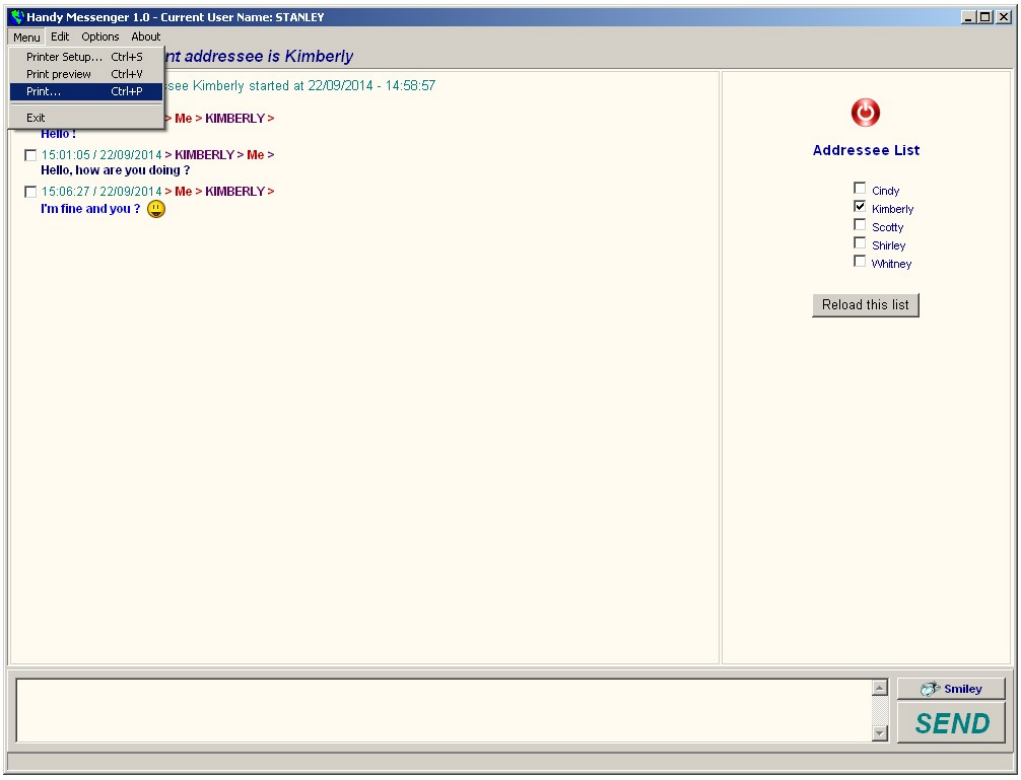
You can send links to web pages or sites. If you click them, your Handy Browser will open on the page that was called. On the bottom of the screen you can see the link when you move your mouse over it, to show you that it is identical to what is indicated.



At any time, you can delete a whole conversation or one or several messages being part of it. Check the message(s) you want to remove, click on the “Edit” menu and use the “Delete Message(s)” function, which can also be called via the Ctrl+D keys. Attention, contrarily to the “Delete All Messages” function, removing individual messages does not call any confirmation submenu and this action cannot be undone.

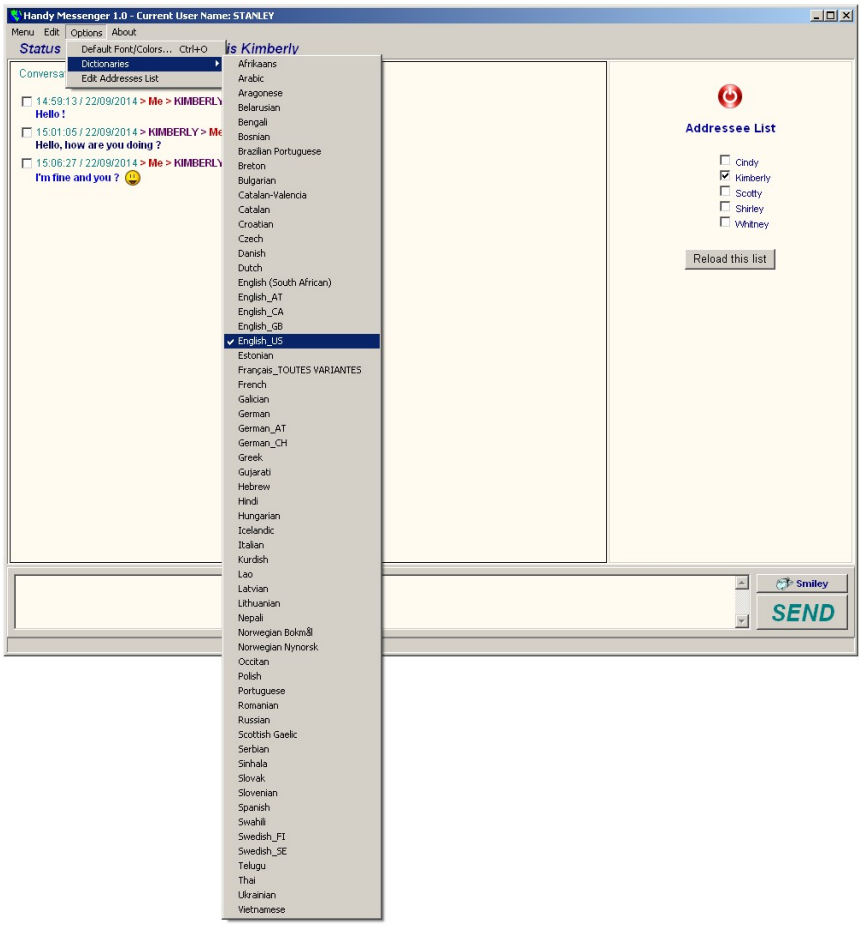


You can print the whole conversation if you want, as on the screen below :

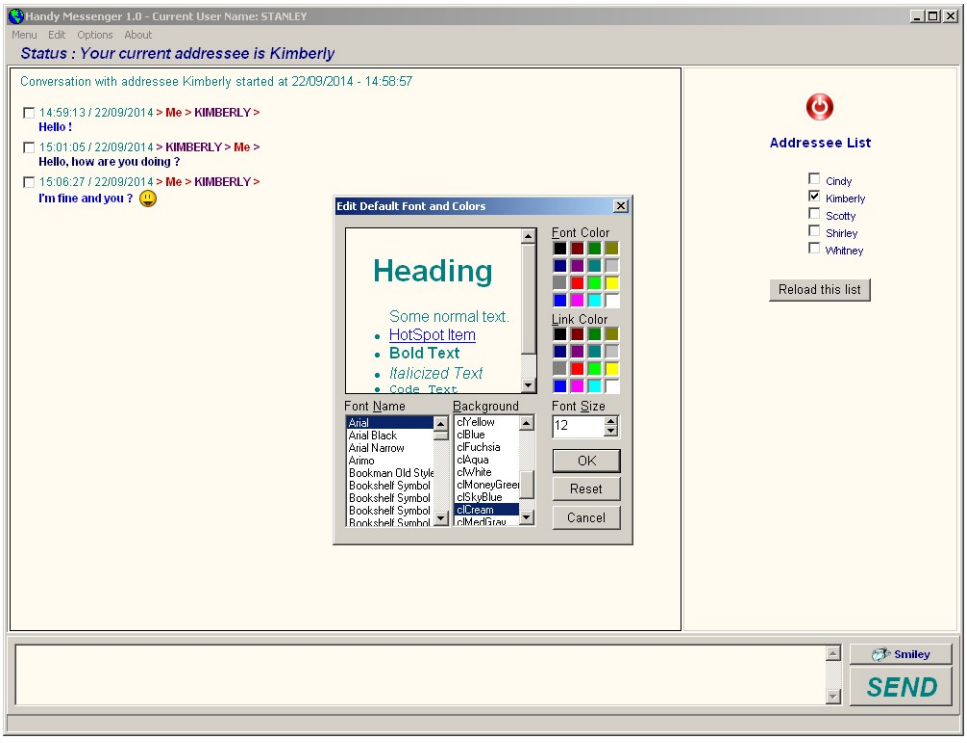


While drawing up your messages, you can gain access to several spelling dictionaries that you can select. If a word appears in red when you are writing a message, right-click it to get suggestions if available.

In the same “Options” menu, the “Edit Addressees List” function allows you to modify your addressees list via the editor that was especially designed for that purpose, since this file is encrypted and its access is password-protected. Please refer to the configuration files chapter to learn how to proceed.



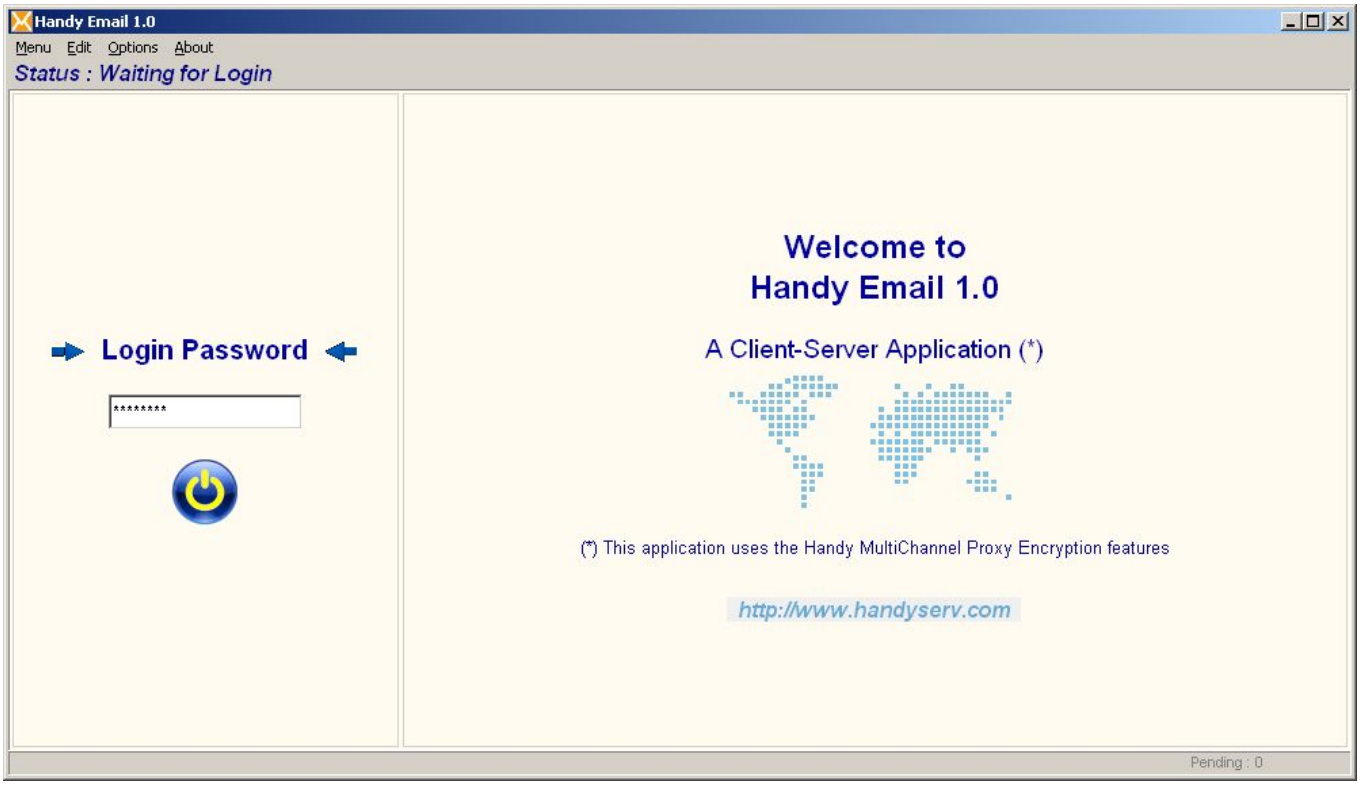
You also can choose the font you wish, its size and color, as well as the background color of the screens.



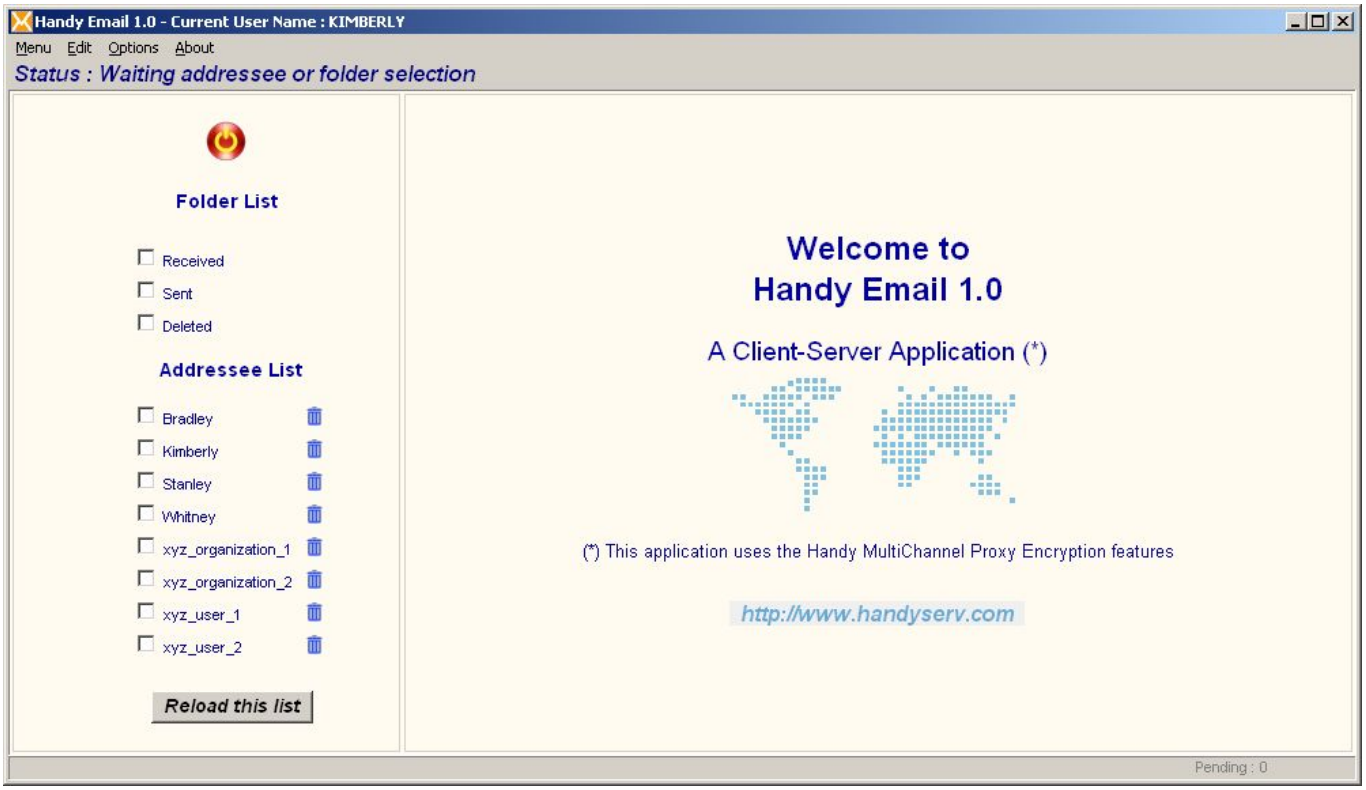
8.4. Handy Email

As explained in the introduction of this chapter, we remind you that this message exchange programme is completely secure and will only work between Handy Proxy users. It is therefore a condition that your Handy Proxy is running on your PC, otherwise Handy Email will not work since it will not have access to its safe and encrypted communication channel.

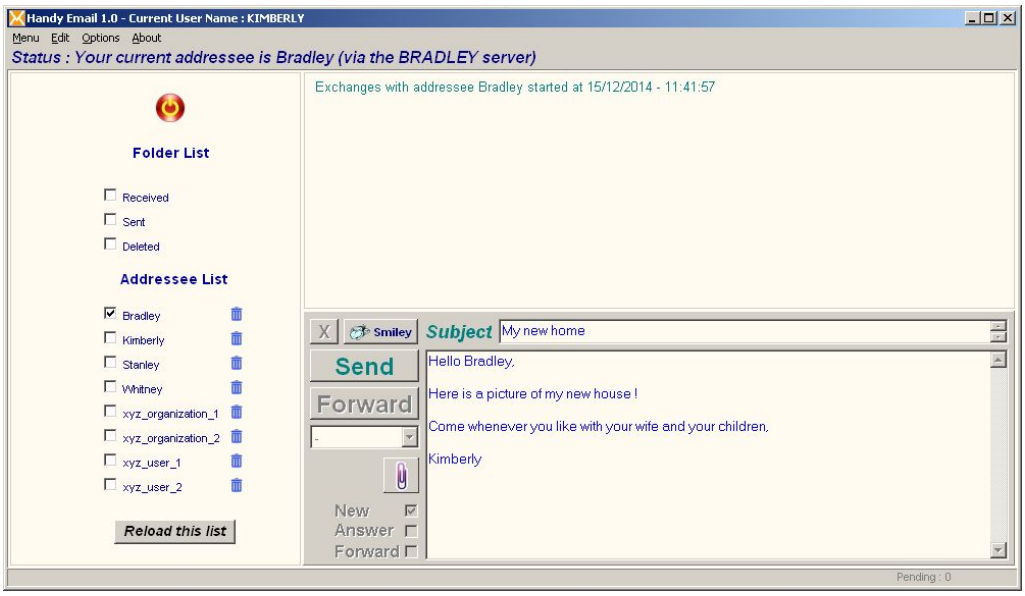
Here is the home screen that suggests you to login with your password (see configuration files to know more about this) :



Once you are logged in, your addressee list and your folder list appear :

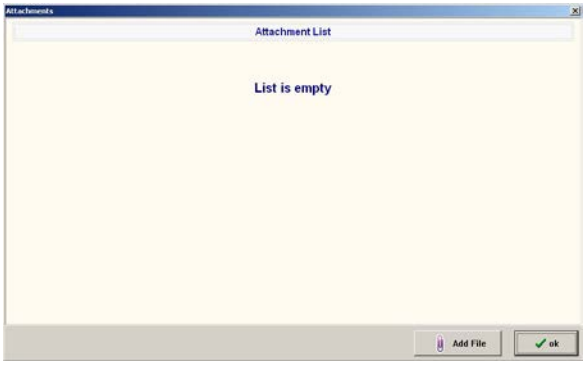


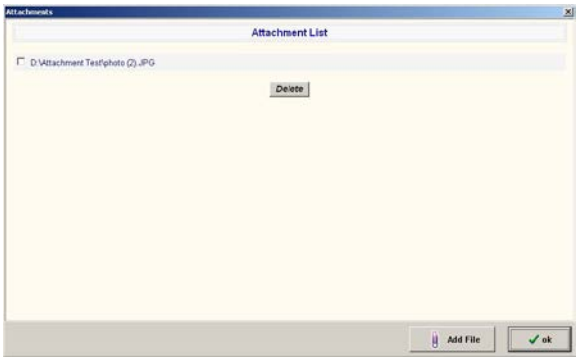
After having selected (checked) an addressee, you can start exchanging messages with him/her ; write your message in the lower part of the screen and click on the « Send » button to send it out, after which your message appears in the upper part of the screen and is immediately sent out to your addressee as long as his/her Handy Proxy is on-line. If this is not the case, as we will explain further on, your message(s) will be « pending », i.e. waiting to be sent later.

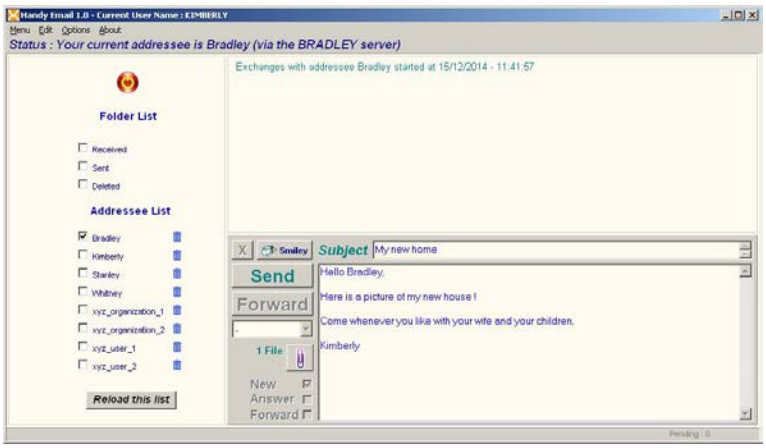


You can attach one or several files to your message (images or other, all formats are supported). If you click on the “paperclip” icon, here are the screens you will get. Click on the “Add File” button and select the file(s) you want to send. At any time you can modify the attachment list by deleting (“Delete” button) a file or adding (“Add file” button) a file to the list. Confirm your selection (“OK” button”). The number of attached files appears next to the “Paperclip” icon.

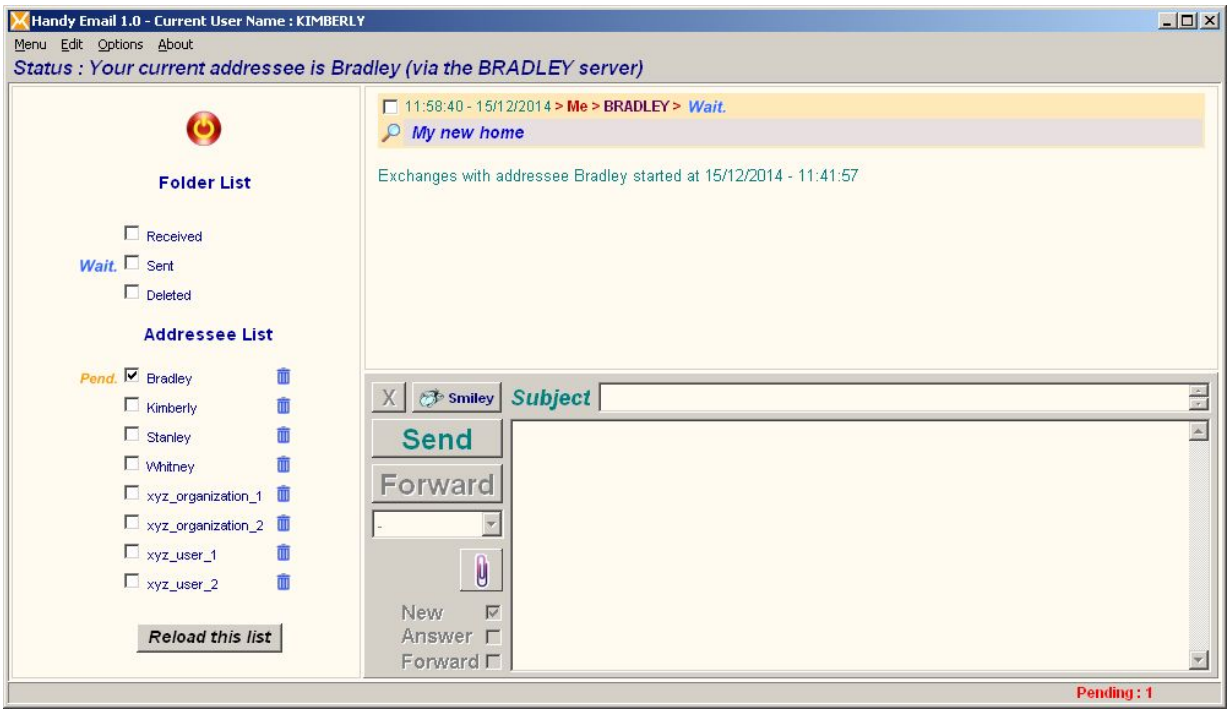
As well as the messages themselves, your original files attached to these messages will be copied in a temporary directory of your Handy Proxy and encrypted before being sent out to your addressee(s), so that these files will never circulate in an understandable format between you and your addressee(s). The name and format of the original file will appear to your addressees only when they want to view the image (if an image was sent) or save the file on their hard disk.



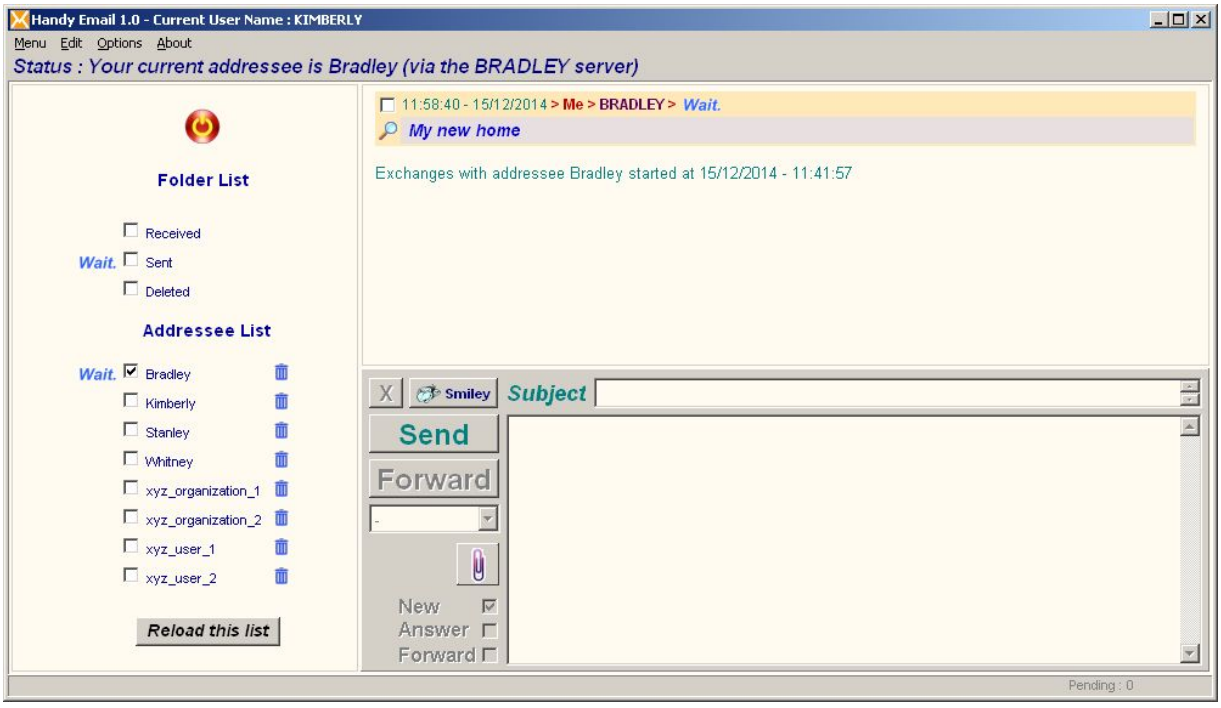




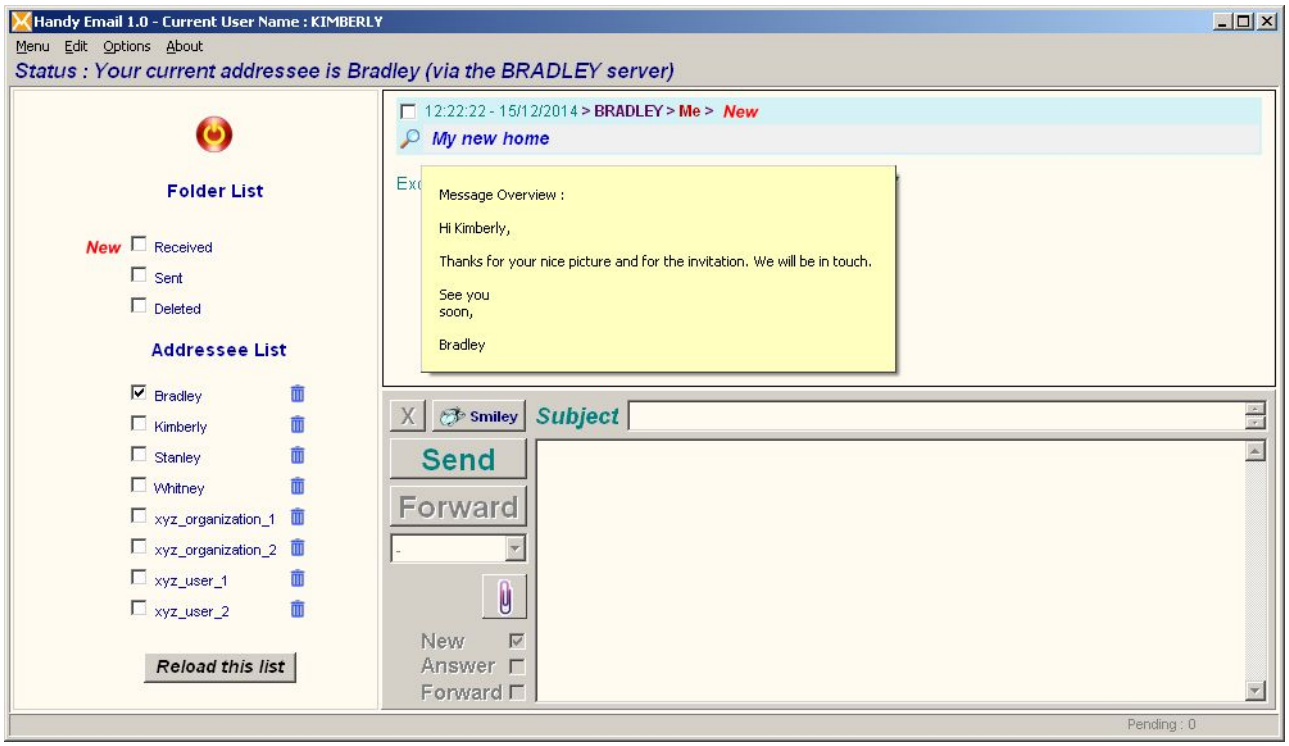
When you click on the “Send” button, first of all the attached files are sent out to your addressee’s server. Your message is on hold until all attachments were delivered. These attachments and this message are on your side, and they will so remain until the delivery of the entire message is achieved. To follow the status of your messages, you can refer to the indicator located on the lower right corner of the screen below. If this indicator is different from “0”, one or several messages are still on your side, unsent. This means, and this point is important, that the Handyserv applications shouldn’t be closed as long as these messages were not delivered ; otherwise, they won’t be sent before you start your Handyserv applications again.



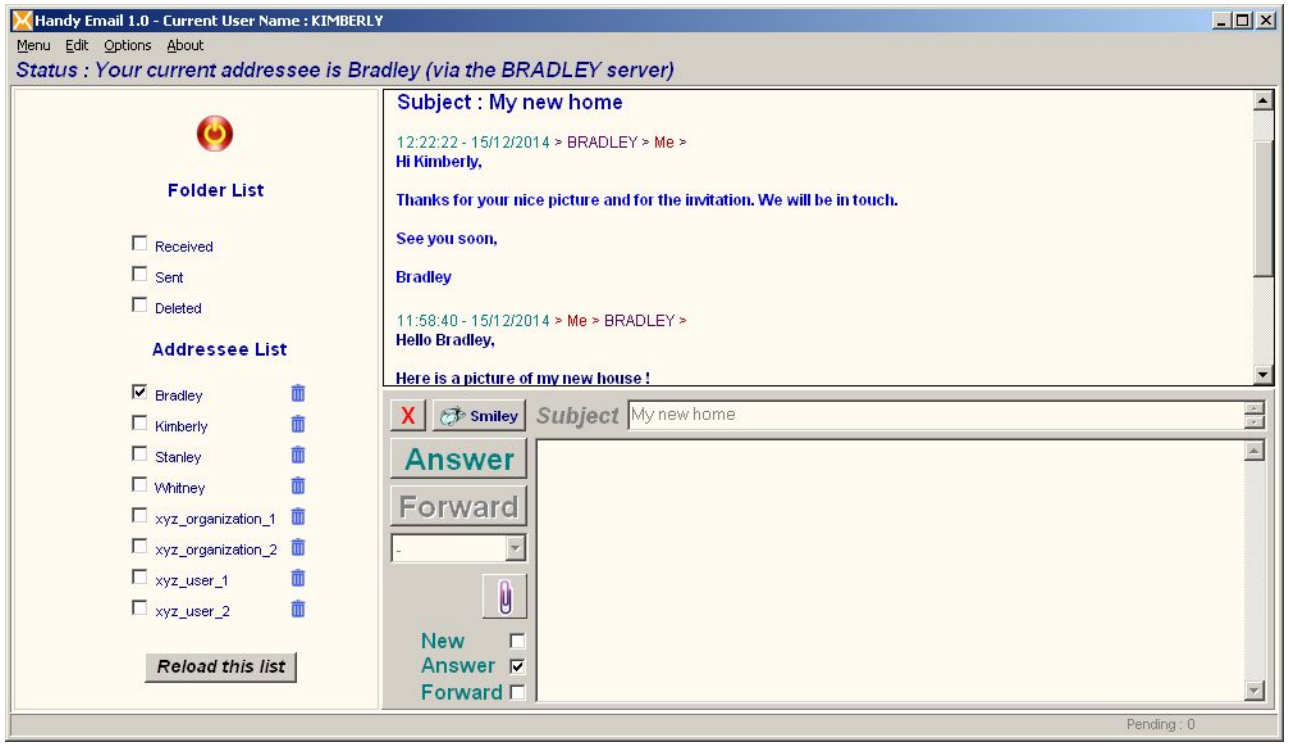
The following screen indicates that your message was delivered, along with its attachments, to your addressee’s server : the “Pending” indicator, on the lower right corner of the screen, equals “0” and appears in grey.



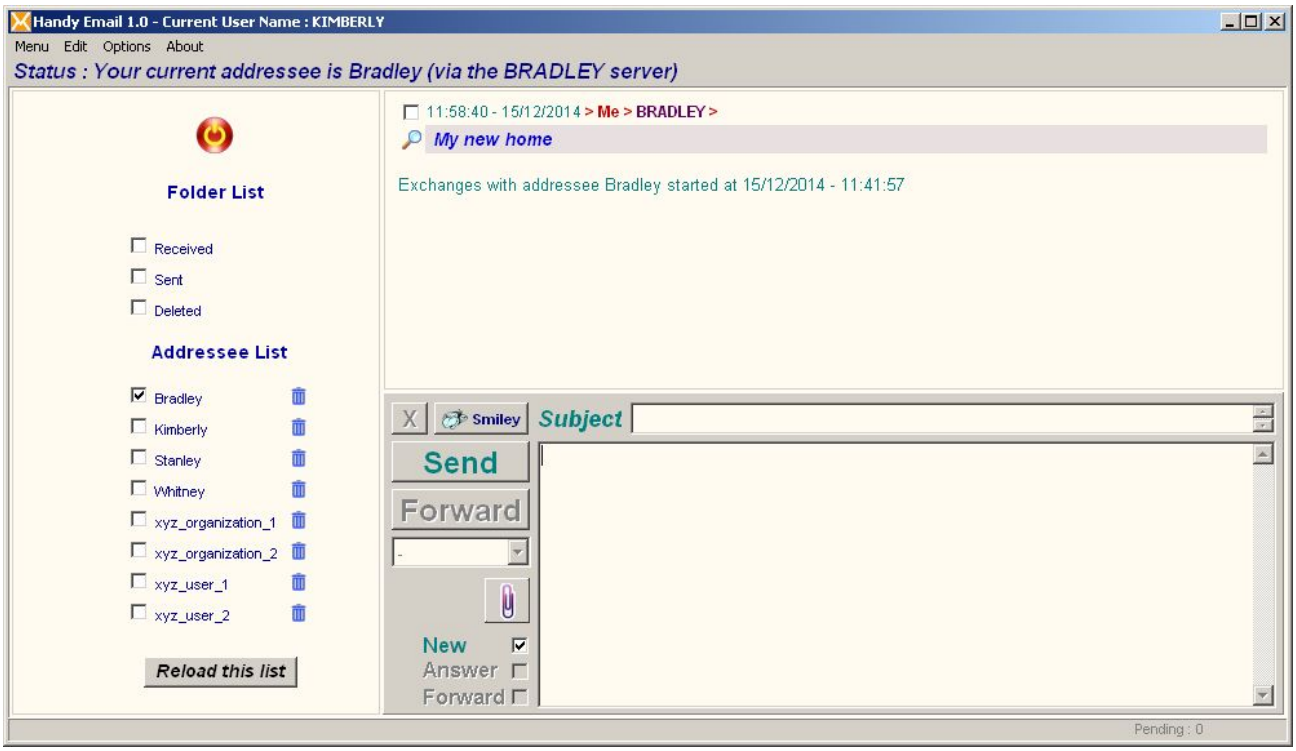
Now, let us see what is happening on the side of your addressee. He/she got a message from you. The blinking indicator “New” appears next to the “Received” folder. Your addressee can view this message by moving his/her mouse over the magnifying glass icon which is next to the message subject, in the message list.



The message opens when its addressee clicks on its subject. An acknowledgement of receipt is then sent out to its sender.

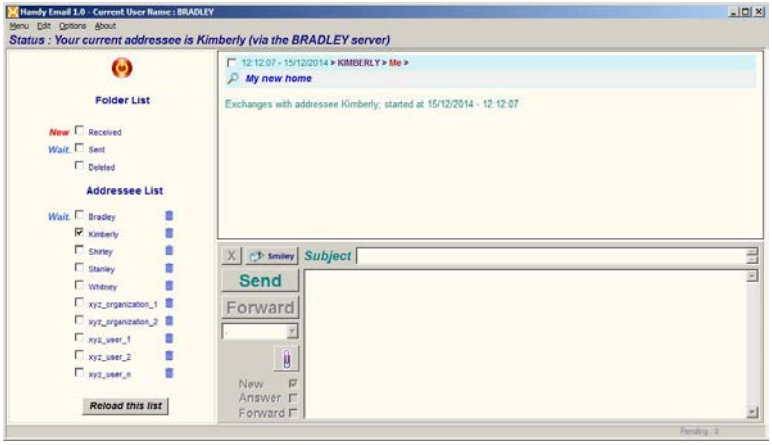


When your addressee has read your message, its “Waiting” status on your side disappears.

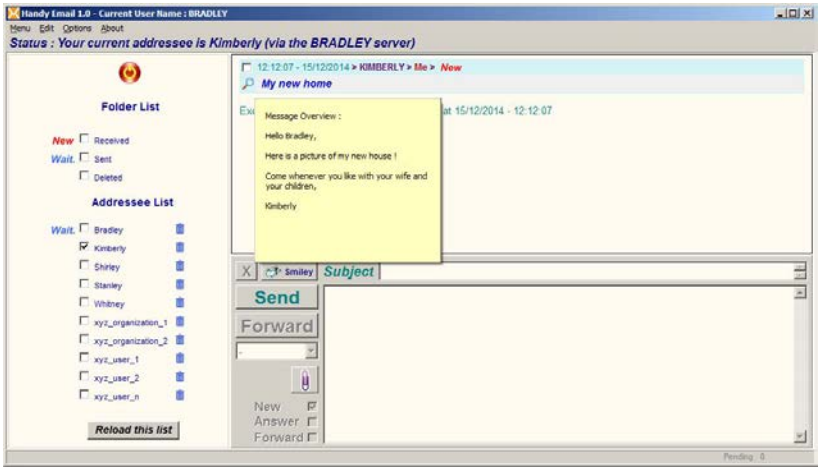


Let us go back to your addressee who received your message and an attached file. When he/she clicks on the “image” or “file” button contained in the body of the message, he/she gets the following screen allowing him/her to view the image (if the file is an image) and/or to save the file on his/her hard disk. At this moment, the file encrypted on your side will be decrypted, and its original name will be shown to your addressee.

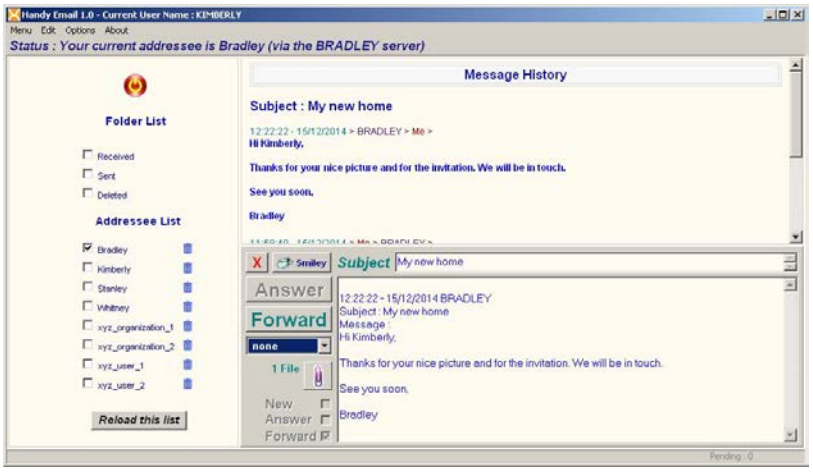
If your addressee want to reply and draws up a message that he/she sends out, here is what you will get, i.e. a new message waiting to be read by you :



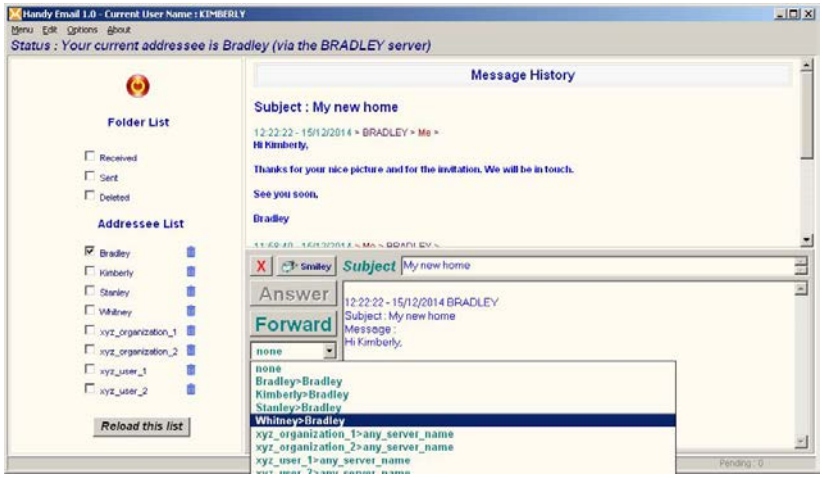
As explained above, you can view the contents of this reply by moving the mouse over the magnifying glass icon :



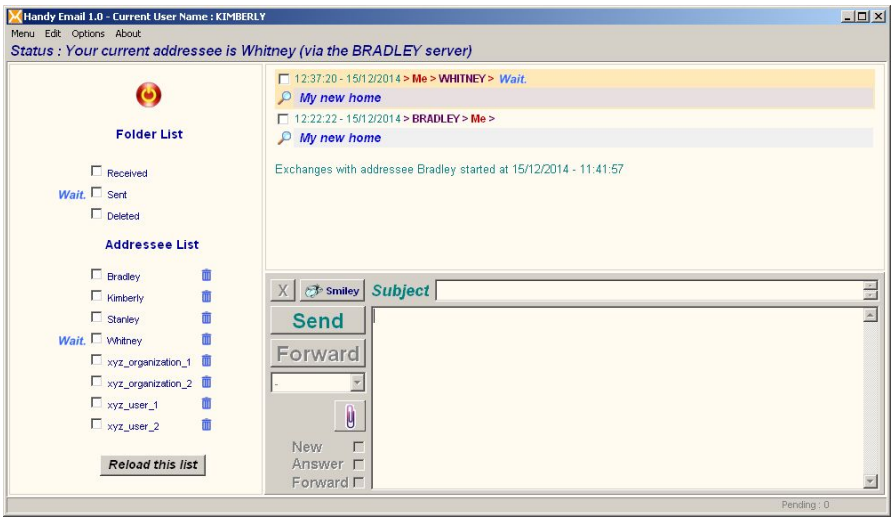
If you want to forward a received message with its attachments to one of your other addressees, here is how to proceed. First, check the “Forward” option at the bottom of the screen, near to the center (other options are “New” and “Answer”).



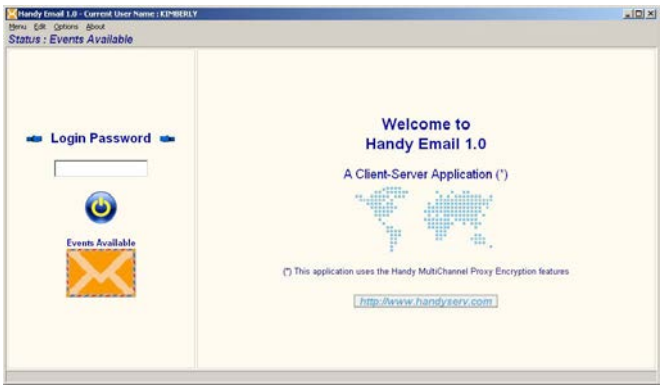
Select now your addressee in the drop-down list of available addressees. You can of course also add text. Click the “Forward” button when you are finished.

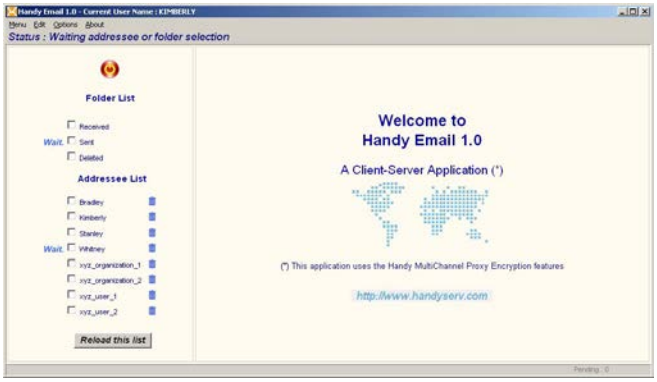


The forwarded message appears in your “Sent” folder, waiting to be read by your addressee.

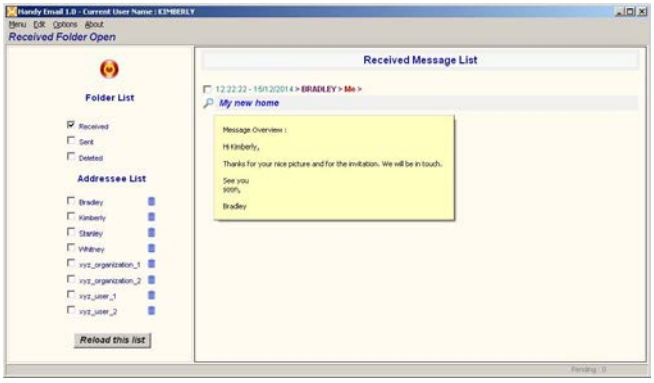


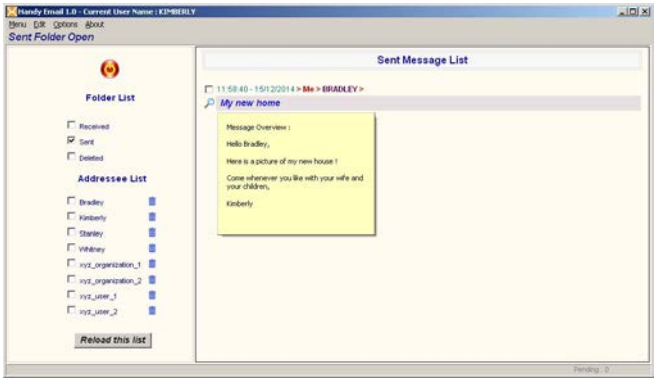
Here is what appears on the home screen if you received a message or event : the blinking “envelope” icon warns you of such reception. After having introduced your password, you gain access to the list of events.





From within the “Received” and “Sent” folders, you also can preview the body of a message, open it, answer it and/or forward it to other addressees.





9. Handy Proxy Configuration Files

9.1. The Handy Proxy Master Configuration File (Multichannel_Proxy_Master_Config.def)

To open this file click on the button below available from within your Handy Proxy's main screen, default password : 1234.

This file must be placed in the **main** directory of the application. It is automatically created at the first runtime of the handyproxy.exe if not found.

You MUST strictly respect the syntax of this file, otherwise parameters or data will not be understood. This file can be edited via Handy Proxy's main screen and the « Edit Master Config File » button.

Role of this file :

This file contains all general parameters of your Handy Proxy. This file will be held into account at the launching of your Handy Proxy. In case of modification, you have to close the Handy Proxy program and restart it.

Possible important remarks are included IN GREEN in the text below ; they are neither comments in this file nor specific parameters. They are additional explanations necessary for the good understanding.

//==
// Handy Proxy Master Configuration File - File name must be :
// Multichannel_Proxy_Master_Config.def
// Lines starting with // or ! or { or * or ; are comments
//
// Handy Proxy (c) Copyright Handyserv - http://www.handyserv.com
//==

//Handy Web Server password to access the remote management web page
//Usage : password can be any string or "none" in order to disable access to the remote management web page
Handy_Web_Server_Remote_Management_Password=none
This password allows to protect this configuration file against any modification, which makes it possible to provide this file to your friends or organisations while keeping control over the configuration that will be used. **Attention : if you lose the password, you will definitively lose access to this configuration file, and this is irreversible !** We do not provide any way to override this password. This password also protects the access to the subconfiguration files as well as to the configuration file of Handy Messenger and Handy Email servers and addressees. All these files might become un-modifiable if you lose or forget your password.
The default password is : 1234

//Handy Messenger and Handy Email programmes password
//Usage : password can be any string or "none" in order to avoid having to login to these 2 programmes
Handy_Messenger_and_Handy_Email_Password=none
This password allows to access Handy Messenger and Handy Email. If you provide this main configuraiton file to your users in your local network for example, they will be able to use them, but not to modify the configuration and the name of their Handy Proxy (see « Handy_Proxy_Configuration.cfg » file where it is possible to indicate a name replacing the one which appears below under the label « Proxy_Name »).
The default password is : 1234

//Name of this Handy Proxy (Required and also used in case of daisy-chaining Handy Proxy)
//(Min. length of this parameter = 7 characters ; max. length = 30 characters ; accent or special characters are NOT allowed)
Proxy_Name=HMP_DEFAULT
Each Handy Proxy must have its own name, different from all others. At its launching, your Handy Proxy will check whether the chosen name is already used by another user. If it is not the case, the chosen name will definitively be yours. You have 30 characters at your disposal for this name, for example we suggest to start by a prefix followed by the initials or the name of each of the users in your family or company, for example mycompany-myname, mycompany-thisname,…
ATTENTION : if your Handy Proxy is a router for other users and/or if your configuration is also used as a messaging server, you cannot change the name of your Handy Proxy since users will use your machine as a router or server. If this name changes they will not retrieve you and will have to reconfigure themselves, which is unmanageable.

//Configuration name of this Handy Proxy (Required and also used in case of daisy-chaining Handy Proxy)
//(Min. length of this parameter = 10 characters ; max. length = 50 characters ; accent or special characters are NOT allowed)
Proxy_Configuration_Name=HMP_ABCDEFGHIJKLMNOPQRSTUVWXYZ
Each Handy Proxy needs a unique identity. This function is automatic at the first launching of your Handy Proxy. However you can create a users group for your family and your company. You can then replace this unique name by a name of your choice, for example HMP-MYCOMPANY.

//Proxy Master Custom Encryption Added Key (This parameter allows to have a unique encryption method in case of daisy-
//chaining Handy Proxies)
//ATTENTION : If you use this parameter, this Handy Proxy and any other remote (daisy-chained) Handy Proxy connected with
//it MUST use the same Custom Encryption Key,
// otherwise they will not be able to understand each other ! See user's manual for more explanations.
//Please note that this Custom Encryption Key will be ADDED at the end of the default one.
//Usage : length of this parameter must be 12 characters (0..9 and A..Z are the ONLY characters allowed).
Proxy_Master_Custom_Encryption_Added_Key=0
This parameter is fundamentally important : it will allow you to define a higher degree of security for your exchanges between Handy Proxies. You can, via this parameter, define a part of the encryption key used to encrypt your data. This private key WILL NEVER BE EXCHANGED between your Handy Proxy and those who would like to communicate with it. Consequently, your correspondents must know this key, otherwise the Handy Proxies will not be able to understand each other. You must disclose to your correspondents the key you are using via any means other than the ones offered by the Handy Proxies. It is up to you to select the best way to share this encryption key. Avoid if possible to send it by the Internet, which would decrease its confidentiality. If you do not use this function, a default encryption key will be used, which is common to all Handy Proxies that do not use this function neither. Your correspondents will have to properly setup their Handy Proxy so that they use the same key as you, otherwise no exchange will be possible.

//Enable Handy Web Server remote management (yes/no)
Handy_Web_Server_Remote_Management_Enabled=yes

//Handy Web Server password to access the remote management web page
//Usage : password can be any string or "none" in order to disable access to the remote management web page
Handy_Web_Server_Remote_Management_Password=none

//Allow to view Handy Proxy "LAN and settings" button (yes/no)
Allow_to_view_Multichannel_Proxy_settings=yes

//Authorize Handy Proxy to modify automatically the local Windows Proxy Settings (yes/no)
Automatic_Windows_Proxy_Setting=yes
We advise to use this function in automatic mode to be certain not to forget to launch your Handy Proxy when switching your PC on. Do not forget to place the handyproxy.exe module in the Windows startup so that it is automatically launched when you start up Windows.

//Handy Proxy will listen to the Internet traffic from this address and port :
//Use address "0.0.0.0" and port "8080" to make Handy Proxy a LAN proxy configuration available for everyone at the local IP
//address:port of the PC running the Handy Proxy
//or use address "127.0.0.1" to make Handy Proxy an individual proxy available locally only.
*Set_Proxy_Server_to=127.0.0.1
Set_Proxy_Server_to=0.0.0.0
*Set_Proxy_Port_to=3128
Set_Proxy_Port_to=8080
This default parameter will generally be convenient. If necessary you can modify it, namely the port (8080 being an example) but in most cases it can stay this way. This parameter will be made available to Windows as a proxy parameter.

//Web link to use in order to fetch the Multichannel HTTP/HTTPS Proxy Configuration and Users Database
//WARNING : DO NOT CHANGE THIS PARAMETER IF YOU ARE NOT INVITED TO DO SO !!! In case of difficulties to reach the
//http://www.handyserv.com Web Site, try to use the following parameters named
//"Fetch_Multichannel_Proxy_DataBase_Address/port"
Web_Link_To_Fetch_The_Multichannel_Proxy_Users_Database=http://www.handyserv.com
The link to the web site which hosts the Handy Proxy users database might change one day. We have thus provided for the possibility to modify this parameter. In such event you will be warned of a modification via your Handy Proxy's main screen. If you do not get such warning, do NOT modify this parameter otherwise the database will not be retrieved ! This parameter allows to customize your configuration to a great extent, and even to make it completely independent from the default one. For more information about this, please refer to chapter 10 of this manual.

//Address and Port to use in order to fetch the Multichannel HTTP/HTTPS Proxy Configuration and Users Database
//Use these two parameters if you need to pass through another proxy to access this database. The "Default" values indicate
//a direct access.
//ATTENTION : your configuration will probably NOT be shareable with other users if you use this function (see next
//parameter that completes this one).
*Fetch_Multichannel_Proxy_DataBase_Address=127.0.0.1
*Fetch_Multichannel_Proxy_DataBase_Port=6006
Fetch_Multichannel_Proxy_DataBase_Address=Default
Fetch_Multichannel_Proxy_DataBase_Port=Default
This parameter allows to pass through another proxy to fetch in Handyserv's database the necessary information to configure your Handy Proxy. Please refer to chapter 1.3.3. of this manual which explains what can be done thanks to these parameters.

//Link to fetch the Multichannel HTTP/HTTPS Proxy Public IP address (mandatory in order to share it with other users)
//ATTENTION : if your public IP address is missing, your configuration will not be shareable!
//This parameter completes the previous one (Fetch_Multichannel_Proxy_DataBase_Port),
//use it if you encounter difficulties to get the Handy Proxy public IP using the default fetching tool integrated in the Handy //Proxy.
//Usage : You can put any link as soon as the linked PHP page contains only the following small PHP code :
//<?php echo $REMOTE_ADDR; ?>
//Attention : the Handy Proxy has no parser able to extract your Public IP from any other PHP code!
//Example : Link_to_fetch_the_Multichannel_Proxy_Public_IP_Address=http://www.mywebsite/what_is_my_public_ip.php
Link_to_fetch_the_Multichannel_Proxy_Public_IP_Address=Default
Please refer to chapter 1.3.3. of this manual which explains what can be done thanks to these parameters.
//Allow to dynamically modify the browser output channel (yes/no)
Allow_Browser_Channel_Hot_Switch=yes
Please refer to chapter 1.3.3. of this manual which explains what can be done thanks to these parameters.

//Allow Logging on hard disk (yes/no)
Allow_Logging_On_Hard_Disk=no

//Editor for the different List Files (default : notepad.exe) ; path must be added for another editor if any
//(ex : c:\notepad++\notepad++.exe - http://notepad-plus-plus.org/)
List_File_Editor=notepad.exe

//Handy Email viewer programme for the different picture file formats as JPG, GIF, PNG, etc
//(default : handyproxybrowser.exe)
//Path must be added for another viewer if any (ex : c:\myviewer\viewer.exe)
Picture_File_Viewer=handyproxybrowser.exe
By default, if the attachment of an email is an image, Handy Email will open the indicated programme to view the said image. You can indicate here another viewer with its path (for example the well-known application IrfanView or any other application allowing to view picture files).

//Path to the PHP programmes and application files (Warning : a '\' character is mandatory at the end of this path)
Path_To_PHP_Apps=[Path]:\…\PHP_Apps\
A version of the PHP programs is provided by default. If it does not suit you because you are already using another one, you can enter here its access path.

//Path to save all the Handy Messaging Server Database Files (Warning : a "\" character is mandatory at the end of this path)
//By default these files will be saved in the current directory of the Handy Proxy. You can use any local or
//any LAN hard disk path in order to save all the files of the Handy Messaging Server Database.
//ATTENTION : In case of a LAN path, the Handy Proxy MUST have all create/delete/modify/read/write rights on
//sub-directories and files!
//Examples of use : (on a local hard disk) E:\Any_Directory\Multichannel_Proxy_Data\Communication
// (on a LAN hard disk) \\LAN-PC-NAME\LAN-Backup-Disk-C\Any_Directory\Multichannel_Proxy_Data\Communication
Path_To_Save_the_Messaging_Database=Default
This parameter allows to define a directory on a hard disk different from the one that is used by default by your Handy Proxy to save all the client and server files of the Handy Messaging Server function. You can thus save all these files on another disk than the one which runs Handy Proxy, for instance you can save these files an a disk which is saved on a daily basis or on a NAS system that would be shared in your network.
Your Handy Messaging Server database files are the only ones that MUST be saved to avoid messages to be lost in case of a crash of the PC hosting the Handy Proxy functions. *This parameter is thus very important since it allows you to save all these files elsewhere than on the local hard disk of the host PC. Using this option you might have two PCs configured in Handy Proxies exactly the same way and with the same license, one of them turned on and active and the second one turned off, in the event of a breakdown of the first one. In case of a breakdown you would simply have to turn off the first PC and to turn on the second one so that your messaging service is up and running within seconds. An alternative to having a second PC, you can install your Handy Proxy on a USB key that could be used on another PC in case of a breakdown. However, you must then take into account the fact that the replacement PC must be accessible to the other users (please refer to chapter 2.1 Making your Handy Proxy accessible for other users)*
ATTENTION : two or more different Handy Messaging Servers cannot share the same directory on a same disk. They must be separated from each other and the databases of the different servers must be totally independent. This parameter concerns exclusively the Handy Messaging Server files.

//Path to save and share with other users all the Handy Proxy Data Files (Warning : a '\' character is mandatory at the end of //this path)
//By default these files will be saved locally in the current directory of the Handy Proxy. You can use any local or //any LAN hard disk path in order to save and share all the Data files of the Handy Proxy.
//ATTENTION : In case of a LAN path, the Handy Proxy MUST have all create/delete/modify/read/write rights on sub-//directories and files!
//Examples of use : (on a local hard disk) E:\Any_Directory\Multichannel_Proxy_Data
// (on a LAN hard disk) \\LAN-PC-NAME\LAN-Backup-Disk-C\Any_Directory\Multichannel_Proxy_Data
Path_To_Save_and_Share_All_the_Data_Files=Default
This parameter allows to centralize on a disk and directory of one's choice, local or in a LAN, all parameter files which are not the configuration files of the Handy Proxy itself as the Multichannel_ProxyMaster_Configuration.def file, the Multichannel_Proxy_ Configuration.cfg file and several other personal configuration files. Those will stay local ; they are located where the Handy Proxy is installed (these files are mainly those concerning the Handy Web Server and all temporary files).

This parameter allows, in a LAN, to give acess to a configuration that is common to all users who have access to the same disk and directory of a hard disk shared in a LAN. In this case, all changes occurring to these common files are made available to all users. The files which are shared this way are the filtering or forced URL routing files (Proxy_Local_URL_Filter_File.DEF, Proxy_Routing_ Table.DEF, Proxy_White_URL_List.DEF), the hmp_conf.pac file (see following subchapters for more information) and the Communication_Server_and_User_List.DEF file (list of servers and addressees for applications Handy Email and Handy Messenger, see chapter 8.2).

Access to these shared files can be password-protected (see parameter Handy_Web_Server_Remote_Management_Password).

The directories allowing to share the Handy Proxy files can be created for a work group, a department, or globally. In order to create a configuration used by a group of persons, we suggest to preconfigure each group from a same Handy Proxy and to forward the Multichannel_ProxyMaster_Configuration.def file to these groups, and possibly to do the same with the second file Multichannel_Proxy_Configuration.cfg. In this case, the creation of all other files will happen at the first launching of Handy Proxy on a PC except for the files that already exist as is the case for the ones that are shared.

***ATTENTION :** the files concerned by this parameter are not protected by competitor access. They can be modified by all Handy Proxy users as long as they know the password (if any).*

//===
// End of Multichannel_ProxyMaster_Configuration.def file
//===

9.2. The Handy Proxy Configuration File (Default name : Handy_Proxy_Configuration.cfg)

To open this file click on the button below available from within your Handy Proxy's main screen, default password : 1234.

This file must be placed in the **main** directory of the application. It is automatically created at the first runtime of the handyproxy.exe if not found.

You MUST strictly respect the syntax of this file, otherwise parameters or data will not be understood. This file can be edited via Handy Proxy's main screen and the « Edit Master Config File » button.

Role of this file :

This file contains the specific parameters for a given configuration of your Handy Proxy. This file will be held into account at the launching of your Handy Proxy, but it can be reloaded during use, either with the same parameters or with other ones if you have several configuration files. You do not have to restart your Handy Proxy when the configuration is modified, the parameters included in this file are held into account at each modification.

Possible important remarks are included IN GREEN in the text below ; they are neither comments in this file nor specific parameters. They are additional explanations necessary for the good understanding.

//==
//
// Handy Proxy Configuration File - File extension must be : .cfg
// Lines starting with // or ! or { or * or ; are comments
//
// Handy Proxy (c) Copyright Handyserv - http://www.handyserv.com
//
//==

//Overwrite the Name of this Handy Proxy
//You can use here (and in case of multi configuration files) the "Proxy_Name" parameter in order to overwrite
//the proxy name saved in the "Multichannel_Proxy_Master_Config.def" configuration file
//(Min. length of this parameter = 7 characters ; max. length = 30 characters ; accent or special characters are NOT allowed)
//Proxy_Name=HMP_DEFAULT
This parameter is redundant with the main configuration file, so that you can change your name in order to connect in a different way to other Handy Proxy users.
ATTENTION : if your Handy Proxy is a router for other users and/or if your configuration is also used as a messaging server, you cannot change the name of your Handy Proxy since users will use your machine as a router or server. If this name changes they will not retrieve you and will have to reconfigure themselves, which is unmanageable.

//Default filtering and replacement level for all unlisted URLs (default = 3 ; value can be 0 up to 8 ; see the
//"Proxy_White_URL_List.DEF" file for definitions)
Default_Filtering_And_Replacement_Level=3

//Allow HTTPS over-encrypted data exchanges between Handy Proxies (yes/no)
//If this parameter is set to 'yes', HTTPS datas will be over-encrypted between Handy Proxies
//This function is in relation with the user-defined White URL list (see the file named : Proxy_White_URL_List.DEF)
//Please note that HTTPS, GET and POST URL requests are always encrypted between Handy Proxies even if this parameter
//is set to 'no'
Allow_HTTPS_Over-Encrypted_Exchanges=yes
This parameter allows to over-encrypt HTTPS (and SSL) exchanges in order to increase dramatically the confidentiality of your exchanges with sites as Facebook, PC banking or others. Thanks to this, your user name and password already encrypted will be doubly encrypted by the powerful encryption functions of your Handy Proxy. This is of course valid only if you pass through a remote Handy Proxy router. For example, if you use your Handy Proxy from a public place by passing through a Handy Proxy router, your Internet security will be maximum.

//Browsers recognition list ; many browsers (and their different versions) can be defined by adding each time a line with this
//parameter (a complete list of "user agent" strings and definitions can be found here : http://www.useragentstring.com)
//
//Usage : Browser=Name;Over-Encryption;Level;Channel;"user agent"
//
//Where :

//Name is the name that will appear on logging screen (multiple definitions are possible if different browser versions are //used)
//Over-Encryption (value 'Y' or 'N') will allow HTTPS over-encrypted data exchanges between Handy Proxies if this function //is enabled (see above)
//Level is the filtering and replacement level (value can be 0 up to 8 ; see above and the "Proxy_White_URL_List.DEF" file for //definitions)
//(Please note that this parameter does NOT bypass the level definition found in the "Proxy_White_URL_List.DEF" file list //for a specific web site)
//Channel will define a dedicated Handy Proxy channel for the defined browser (value can be x, 0 up to 9 ; x means no //dedicated channel)
//(Please note that this parameter does NOT bypass the channel definition found in the "Proxy_Routing_Table.DEF" file list //for a specific web site)
//"user agent" is the string or full user agent to be recognized for the defined browser (the " before and after this parameter //are mandatory)
//
//Examples of use
//Browser=Prism;N;0;x;" prism/" (this example will recognize all versions of the Prism browser as only one version in the //traffic log screen)
//Browser=Prism_0.8;Y;3;1;" prism/0.8" (this example shows how to recognize a specific version of the Prism browser)
//Browser=Prism_1.0b4;Y;8;9;"Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10.6; en-US; rv:1.9.2.3) Gecko/20100402 //Prism/1.0b4"
//
//Active browser definition lines here after will recognize all browser versions as only one since a short string is used rather //than the complete user agent
//In the examples below, concerning Internet Explorer, the active line represents the most recent versions (8, 9 and 10)
//
//Level 3 is the best choice if the AdBlock functions are installed in Chrome, Firefox, etc (visit AdBlock web site for more //information : http://adblockplus.org**)**
//
Browser=Chrome;Y;3;x;"Gecko) Chrome/"
Browser=Firefox;Y;3;x;" Firefox/"
Browser=Internet Explorer;Y;3;x;"; Trident/"
Browser=Maxthon;Y;3;x;" Maxthon"
Browser=Opera;Y;3;x;" Opera "
This parameter allows you to define, browser by browser, the channel and the priority of the filters used. For example, you can use one of your browsers via the main channel of your Handy Proxy in a totally transparent mode while you are using another browser that would pass through another channel of your Handy Proxy being connected to another Handy Proxy in router mode. The first browser would be a « general purposes » browser, while the second one, protected by the encrypted exchanges between Handy Proxies, would be used for all sensitive sites as home banking or any site requiring to enter a login and password. Another way to proceed is to create several configuration files of this kind and to load the necessary configuration according to each case,.

//Allow only local URL Filter List (never download the file "Proxy_URL_Filter_File.txt" from the Handy Proxy Web Site) – //(yes/no)
//"no" means that Handy Proxy will only use the local URL filter file (see below)
//Allow_Extended_URL_List_File_Download=yes
//Load additional URL filter list file (yes/no ; this list will be regularly and automatically downloaded by this program, this file //is then "read only")
Load_Additional_URL_Filter_List_File=yes
Your Handy Proxy can use a URL filter list. If your browser already uses AdBlock's functionalities (see web site https://adblockplus.org*), for example, this function is redundant and it is thus not necessary to use this list. Please note that if your Handy Proxy is configured in router mode, in contrast with a local use, this list will not be used for all the traffic routed by your Handy Proxy. This parameter can be configured at any time from within the main menu of your Handy Proxy.*

//Use extended version of the additional URL filter list file (see above) - (yes/no)
Load_Additional_URL_Filter_List_File_Extended_Version=yes
There are two versions of the list described above. We advise to use the extended version.
This parameter can be configured at any time from within the main menu of your Handy Proxy.

//Allow URL Dropping (don't drop any URLs included in the above filter files, proxy will be totally "transparent") - (yes/no)
Allow_URL_Dropping=yes
Your Handy Proxy can be made transparent, which means that it will not filter any link, neither the links in the lists described above, nor the links you might have added into the proper files. This parameter can be configured at any time from within the main menu of your Handy Proxy.

//What to do with filtered links ? - Answer can be 0 up to 99 where :
//0 = Don't show anything
//1 = Display a small explanation during 5 seconds, then clear the message
//2 = Display a small explanation
//3 = Display a small proxy logo
//4 up to 19 = reserved for future upgrades
//x = Display replacement pictures ; x is a value between 20 and 99
What_To_Do_With_Filtered_Links=20

There are several ways to replace links to images that would be filtered by the lists above. By default, your Handy Proxy will replace these images by nice landscapes from everywhere on the planet. Those will evolve from day to day, since this list is updated every 24h.
//If "Display replacement pictures" (20..99) is selected as parameter here above, what will be the height of displayed pictures //in pixel (default is 75 ; min. = 25 ; max. = 250)
//Please note that this parameter can modify the layout of the visited pages if selected pictures height is too large!
Display_Replacement_Pictures_Using_This_Height=75

//Routing traffic to address and port ID 0 (default ; if not modified to another address and port, traffic will be sent directly to //the Internet by this proxy)
ID0_Name=Default Channel ID0
Routing_Traffic_to_this_address_#0=0.0.0.0
Routing_Traffic_to_this_port_#0=0
Channel 0 of your Handy Proxy is the channel that is mandatorily reserved to connect directly to the Internet. However you can change the address and port of this access if necessary and according to the configuration of your network.

//Routing traffic to address and port ID 1 :
//Possible parameter syntax may be
//"Routing_Traffic_to_this_address_#x=Target:Any_Remote_Existing_Handy_Proxy_Name". If this parameter is used as //explained here, the "Routing_Traffic_Custom_Encryption_Added_Key_#x" must be exactly the same value/string as the //parameter named "Proxy_Master_Custom_Encryption_Added_Key" used on the remote Handy Proxy, otherwise Handy //Proxies will not be able to understand each other ! See user's manual for more explanations.
ID1_Name=Channel ID1
Routing_Traffic_Custom_Encryption_Added_Key_#1=0
Routing_Traffic_to_this_address_#1=0.0.0.0
Routing_Traffic_to_this_port_#1=0
The explanation below is valid for Handy Proxy channels from 1 to 9.
You can give a name to each channel according to your needs.
If you wish to connect to another Handy Proxy via one of the channels from 1 to 9, you must either indicate its physical IP address in your network in the case of a local use, or indicate the name of the Handy Proxy such as defined by your correspondent in the case of a remote use (parameter « port » must remain 0 : Routing_Traffic_to_this_port_#x=0). In this case, the main parameter of each channel is the definition, if necessary,of the remote Handy Proxy's encryption key. Check with the remote Handy Proxy user whether he/she uses a private encryption key or not. If both keys are not identical, no exchange is possible between the two systems.

//Routing traffic to address and port ID 2 :
//Possible parameter syntax may be
//"Routing_Traffic_to_this_address_#x=Target:Any_Remote_Existing_Handy_Proxy_Name". If this parameter is used as //explained here, the "Routing_Traffic_Custom_Encryption_Added_Key_#x" must be exactly the same value/string as the //parameter named "Proxy_Master_Custom_Encryption_Added_Key" used on the remote Handy Proxy, otherwise Handy //Proxies will not be able to understand each other ! See user's manual for more explanations.
ID2_Name=Channel ID2
Routing_Traffic_Custom_Encryption_Added_Key_#2=0
Routing_Traffic_to_this_address_#2=0.0.0.0
Routing_Traffic_to_this_port_#2=0

//Routing traffic to address and port ID 3 :
//Possible parameter syntax may be
//"Routing_Traffic_to_this_address_#x=Target:Any_Remote_Existing_Handy_Proxy_Name". If this parameter is used as //explained here, the "Routing_Traffic_Custom_Encryption_Added_Key_#x" must be exactly the same value/string as the //parameter named "Proxy_Master_Custom_Encryption_Added_Key" used on the remote Handy Proxy, otherwise Handy //Proxies will not be able to understand each other ! See user's manual for more explanations.
ID3_Name=Channel ID3
Routing_Traffic_Custom_Encryption_Added_Key_#3=0
Routing_Traffic_to_this_address_#3=0.0.0.0
Routing_Traffic_to_this_port_#3=0

//Routing traffic to address and port ID 4 :
//Possible parameter syntax may be
//"Routing_Traffic_to_this_address_#x=Target:Any_Remote_Existing_Handy_Proxy_Name". If this parameter is used as //explained here, the "Routing_Traffic_Custom_Encryption_Added_Key_#x" must be exactly the same value/string as the //parameter named "Proxy_Master_Custom_Encryption_Added_Key" used on the remote Handy Proxy, otherwise Handy //Proxies will not be able to understand each other ! See user's manual for more explanations.
ID4_Name=Channel ID4
Routing_Traffic_Custom_Encryption_Added_Key_#4=0
Routing_Traffic_to_this_address_#4=0.0.0.0
Routing_Traffic_to_this_port_#4=0

//Routing traffic to address and port ID 5 :
//Possible parameter syntax may be
//"Routing_Traffic_to_this_address_#x=Target:Any_Remote_Existing_Handy_Proxy_Name". If this parameter is used as //explained here, the "Routing_Traffic_Custom_Encryption_Added_Key_#x" must be exactly the same value/string as the //parameter named "Proxy_Master_Custom_Encryption_Added_Key" used on the remote Handy Proxy, otherwise Handy //Proxies will not be able to understand each other ! See user's manual for more explanations.

ID5_Name=Channel ID5
Routing_Traffic_Custom_Encryption_Added_Key_#5=0
Routing_Traffic_to_this_address_#5=0.0.0.0
Routing_Traffic_to_this_port_#5=0

//Routing traffic to address and port ID 6 :
//Possible parameter syntax may be
//"Routing_Traffic_to_this_address_#x=Target:Any_Remote_Existing_Handy_Proxy_Name". If this parameter is used as
//explained here, the "Routing_Traffic_Custom_Encryption_Added_Key_#x" must be exactly the same value/string as the
//parameter named "Proxy_Master_Custom_Encryption_Added_Key" used on the remote Handy Proxy, otherwise Handy
//Proxies will not be able to understand each other ! See user's manual for more explanations.
ID6_Name=Channel ID6
Routing_Traffic_Custom_Encryption_Added_Key_#6=0
Routing_Traffic_to_this_address_#6=0.0.0.0
Routing_Traffic_to_this_port_#6=0

//Routing traffic to address and port ID 7 :
//Possible parameter syntax may be
//"Routing_Traffic_to_this_address_#x=Target:Any_Remote_Existing_Handy_Proxy_Name". If this parameter is used as
//explained here, the "Routing_Traffic_Custom_Encryption_Added_Key_#x" must be exactly the same value/string as the
//parameter named "Proxy_Master_Custom_Encryption_Added_Key" used on the remote Handy Proxy, otherwise Handy
//Proxies will not be able to understand each other ! See user's manual for more explanations.
ID7_Name=Channel ID7
Routing_Traffic_Custom_Encryption_Added_Key_#7=0
Routing_Traffic_to_this_address_#7=0.0.0.0
Routing_Traffic_to_this_port_#7=0

//Routing traffic to address and port ID 8 :
//Possible parameter syntax may be
//"Routing_Traffic_to_this_address_#x=Target:Any_Remote_Existing_Handy_Proxy_Name". If this parameter is used as
//explained here, the "Routing_Traffic_Custom_Encryption_Added_Key_#x" must be exactly the same value/string as the
//parameter named "Proxy_Master_Custom_Encryption_Added_Key" used on the remote Handy Proxy, otherwise Handy
//Proxies will not be able to understand each other ! See user's manual for more explanations.
ID8_Name=Channel ID8
Routing_Traffic_Custom_Encryption_Added_Key_#8=0
Routing_Traffic_to_this_address_#8=0.0.0.0
Routing_Traffic_to_this_port_#8=0

//Routing traffic to address and port ID 9 :
//Possible parameter syntax may be
//"Routing_Traffic_to_this_address_#x=Target:Any_Remote_Existing_Handy_Proxy_Name". If this parameter is used as
//explained here, the "Routing_Traffic_Custom_Encryption_Added_Key_#x" must be exactly the same value/string as the
//parameter named "Proxy_Master_Custom_Encryption_Added_Key" used on the remote Handy Proxy, otherwise Handy
//Proxies will not be able to understand each other ! See user's manual for more explanations.
ID9_Name=Channel ID9
Routing_Traffic_Custom_Encryption_Added_Key_#9=0
Routing_Traffic_to_this_address_#9=0.0.0.0
Routing_Traffic_to_this_port_#9=0

//==
// End of Multichannel_Proxy_Configuration.cfg file
//==

9.3. The Handy Proxy hmp_conf.pac file

This file must be placed in the **…\Multichannel_Proxy_Data** directory.

You MUST strictly respect the syntax of this file, otherwise parameters or data will not be understood.

Role of this file :

This file can be used by your browsers and will be made available to them by your Handy Proxy. This file will be accessible only as a web page. Its syntax is Javascript (or assimilated to). This file will behave as a micro-program that your browsers will execute, hence the fundamental importance of respecting the syntax and the keywords definitions.

Thanks to this micro-program you will be able to specify that some web sites or physical addresses of sites or pages will not pass through your Handy Proxy. For example, we suggest not to pass through your Handy Proxy to access your Internet router. By default, this file contains direct access to the address 192.168.1.1 which is usually the physical address of your Internet router. Of course, you must tell your browsers that they have to use the hmp_conf.pac file. Please refer to chapter 2 « Handy Proxy Usage » of this manual.

```
/// Lines starting with "///" are Handy Proxy comments and they are removed at runtime (same for empty lines)
/// Lines starting with "//" are Javascript comments

/// For explanations, you can visit these web pages :

/// http://web.archive.org/web/20060424005037/wp.netscape.com/eng/mozilla/2.0/relnotes/demo/proxy-live.html
/// or
/// http://technet.microsoft.com/en-us/library/dd361918.aspx

function FindProxyForURL(url, host)
{

///Example of EXCEPTION RULE (in this example, ".anysite.ext" will be NOT routed by the Handy Proxy)
//If the hostname matches, send direct :
//if (shExpMatch(url, "http://www.anysite.ext/*"))
//return "DIRECT";

///Example of use :
//If the hostname matches, send direct :
if (url.substring(0, 18) == "http://192.168.1.1")
 { return "DIRECT"; }

///In the following case, "#Handy_Web_Server_URL#" and "#Current_LAN_HMP_Address/Port#" will be dynamically replaced
///at runtime by the Handy Web Server link (hostname) and by the LAN Address and Port of the current Handy Proxy
//If the hostname matches, send through the Handy Proxy :
if (shExpMatch(url, "#Handy_Web_Server_URL#"))
return "PROXY #Current_LAN_HMP_Address#:#Current_LAN_HMP_Port#";

///DEFAULT RULE: All other traffic will use the following Handy Proxy :
///In the following case, "#Current_LAN_HMP_Address/Port#" will be dynamically replaced at runtime by the LAN Address
///and Port of the current Handy Proxy. Example of replacement at runtine : return "PROXY 192.168.1.14:8086";
return "PROXY #Current_LAN_HMP_Address#:#Current_LAN_HMP_Port#";

///Other possible examples of use :
///return "PROXY 127.0.0.1:808x";
///return "PROXY 192.168.1.X:8x";

}
```

9.4. The Handy Proxy Proxy_Authorized_Connection_List.DEF file

This file must be placed in the **…\Multichannel_Proxy_Data** directory.

You MUST strictly respect the syntax of this file, otherwise parameters or data will not be understood.

Role of this file :

This file allows to define who can access your Handy Proxy that will then become a router for other users. You can edit this file and add as many lines (while respecting the syntax) as you will allow users according to the way you share your Handy Proxy on the Internet. You can list here members of your family, friends or colleagues. This list can be updated at any time from within the main screen of your Handy Proxy. For more information about this, please refer to chapter 2 « Handy Proxy Usage » of this manual.

You can authorize any user to access the Internet via your Handy Proxy in router mode, but we advise against opening this access very widely except if you want to make available a « public » router. The « Satisfy= » parameter allows this function according to precisely defined keywords as you can see here below.
The « Allow_From_All » parameter makes your Handy Proxy public, while the « Deny_From_All_But_Allow » parameter will make it unaccessible to any user not listed in the file.

```
//=============================================================================
//
// Handy Proxy Authorized Connection List - File name must be : Multichannel_Proxy_Authorized_Connection_List.DEF
// Lines starting with // or ! or { or * or ; are comments
//
// Usage :
//  - You can add in this list any Handy Proxy name that will be allowed to remotely use this proxy
//  - To be valid, a line must start with "Satisfy=" string
//    Example : Satisfy=HMP_myproxy
//  - Each line of this file must contain only one name followed by a CR + LF
//  - There are 2 predefined and reserved keywords :
//     - Satisfy=Allow_From_All
//     - Satisfy=Deny_From_All_But_Allow (the following list)
//  - At installation time the "Satisfy=Allow_From_All" line is set to be active
//
// Example of use : Satisfy=HMP_xyz
//
// Handy Proxy (c) Copyright Handyserv - http://www.handyserv.com
//
//=============================================================================

//Satisfy=Allow_From_All
Satisfy=Deny_From_All_But_Allow

//Satisfy=HMP_abc
//Satisfy=HMP_def
//...
//Satisfy=HMP_xyz
//...
```

9.5. The Handy Proxy Proxy_IP_to_Users_Translation_Table.DEF file

This file must be placed in the **…\Multichannel_Proxy_Data** directory.

You MUST strictly respect the syntax of this file, otherwise parameters or data will not be understood.

Role of this file :

This file allows, when displaying page web calls, to modify the physical addresses of your PCs connected in your LAN and that pass through your Handy Proxy by names of your choice that are more representative than physical IP addresses.

```
//=============================================================================
//
// Handy Proxy IP to Users Translation Table - File name must be : Multichannel_Proxy_IP_to_Users_Translation_Table.def
// Lines starting with // or ! or { or * or ; are comments
//
// Handy Proxy (c) Copyright Handyserv - http://www.handyserv.com
//
//=============================================================================

127.0.0.1=LocalHost
192.168.1.1=User_1
192.168.1.2=User_2
//...
192.168.1.10=User_10
192.168.1.11=User_11
192.168.1.12=User_12
192.168.1.13=User_13
192.168.1.14=User_14
192.168.1.15=User_15
//...
192.168.1.50=User_50
//...
192.168.1.255=User_255
//...
```

9.6. The Handy Proxy Proxy_Local_URL_Filter_File.DEF file

This file must be placed in the **…\Multichannel_Proxy_Data** directory.

You MUST strictly respect the syntax of this file, otherwise parameters or data will not be understood.

Role of this file :

This file allows to define the sites, pages, images, etc. that your Handy Proxy will have to filter. The syntax of this file is simple : each line corresponds to a link or part of a link, or to a determined file name. Only exact string matching will allow filtering.

This list can be updated at any time from within the main screen of your Handy Proxy. For more information about this, please refer to chapter 2 « Handy Proxy Usage » of this manual.

```
//=================================================================
//
// List of user-defined URL Filters
// File name must be : Proxy_Local_URL_Filter_File.DEF
// Lines starting with // or ! or { or * or ; are comments
//
// This list will help you to reduce your Internet traffic
//
// Handy Proxy (c) Copyright Handyserv - http://www.handyserv.com
//
//=================================================================

//http://www.any_website.me
//.any_page.me
//.thiswebsite.
//...
```

9.7. The Handy Proxy Proxy_Routing_Table.DEF file

This file must be placed in the **…\Multichannel_Proxy_Data** directory.

You MUST strictly respect the syntax of this file, otherwise parameters or data will not be understood.

Role of this file :

This file allows to define which channel of your Handy Proxy will route such site, link or link part. For example, you can access all sensitive web sites via a remote Handy Proxy in order to avoid your user name and password to flow in an unencrypted way on the Internet from where you are.

The first characters of each line contained in this file indicate the channel to use (from 0 to 9). By default, we suggest several video or music web sites (as Youtube, for example) that will be accessed via channel 0 of your Handy Proxy, i.e. directly. We advise against making video or music pass through a remote Handy Proxy since these data are not sensitive.

```
//=============================================================================================
//
// Handy Proxy Routing Table - File name must be : Multichannel_Proxy_Routing_Table.def
// Lines starting with // or ! or { or * or ; are comments
//
// Handy Proxy (c) Copyright Handyserv - http://www.handyserv.com
//
//=============================================================================================

//=========================
//=== URL Routed to ID0 ===
//=========================
#0:.googleusercontent.com
#0:.googlevideo.com
#0:.vimeo.com
#0:.vimeocdn.com
#0:.youtube.
#0:.ytimg.com

//=========================
//=== URL Routed to ID1 ===
//=========================
#1:mywebsite.me

//=========================
//=== URL Routed to ID2 ===
//=========================
//#2:mywebsite.me

//=========================
//=== URL Routed to ID3 ===
//=========================
//#3:mywebsite.me

//=========================
//=== URL Routed to ID4 ===
//=========================
//#4:mywebsite.me

//=========================
//=== URL Routed to ID5 ===
//=========================
//#5:mywebsite.me

//=========================
//=== URL Routed to ID6 ===
//=========================
//#6:mywebsite.me

//=========================
//=== URL Routed to ID7 ===
//=========================
//#7:mywebsite.me
```

```
//=========================
//=== URL Routed to ID8 ===
//=========================
//#8:mywebsite.me

//=========================
//=== URL Routed to ID9 ===
//=========================
//#9:mywebsite.me
```

9.8. The Handy Proxy Proxy_String_to_IP-Destination_Table.DEF file

This file must be placed in the **…\Multichannel_Proxy_Data** directory.

You MUST strictly respect the syntax of this file, otherwise parameters or data will not be understood.

Role of this file :

In addition to a default domain name as « http://any_name.handywebserver.hmpr », this file allows to define domain names that are specific to your Handy Proxy. This function is necessary and advised namely if you make web pages available via your Handy Web Server. This function is not limited to this : indeed, you also can create a domain name that your Handy Proxy will route to a physical address in your network or in your PC where another web server would be installed. For example, if there are one or several web servers (Apache or other) in your network, this domain name creation function will be very useful if you want your web sites to be accessible between 2 Handy Proxies, i.e. in encrypted mode. This method will make these web sites accessible only by your correspondents also using a Handy Proxy and that you have authorized to use your shared configuration.

For obvious reasons of security and copyright (where appropriate), Handy Proxy does not allow to create a domain name that routes to a site located outside of your LAN or PC. The program will reject any domain name which does not comply to the syntax below. Similarly, routing is authorized only to addresses which are internal to your network or PC.

```
//=============================================================================================================
//
// Handy Proxy String to IP-Destination Table - File name must be : Multichannel_Proxy_String_to_IP-Destination_Table.def
// Lines starting with // or ! or { or * or ; are comments
// Lines containing  " or ' or ? or & or = or / or ; characters or "www." string are considered as syntax error
//
// Please note that HTTPS, GET and POST requests are always encrypted between Handy Proxies (and the integrated Handy Web Server
// or other web server linked througt this String to IP-Destination Table)
//
// REMARK : the '.hmpr' or 'http://#HMP_Proxy_Name#' string is required in each line, otherwise the line will be considered as syntax error
//
// Examples of use : http://HmprCompatibleString=:=Local_IP_Address:Port
// http://AnyString.hmpr=:=127.0.0.1:8080
// http://MyLocalWebsiteName.hmpr=:=192.1.1.200:8081
// http://#HMP_Proxy_Name#AnyString.hmpr=:=192.168.1.6:80
// http://#HMP_Proxy_Name#AnyLocalWebServer.hmpr=:=127.0.0.1:80
// http://#HMP_Proxy_Name#.hmpr=:=127.0.0.1:80
//
// Where :
//  - http://HmprCompatibleString = any string where the 'http://' and '.hmpr' or '#HMP_Proxy_Name#' strings are found
//    - If the string 'http://#HMP_Proxy_Name#...' is used, then the string '.hmpr' MUST also be used at the end of the 'HmprCompatibleString'
//    - If the string 'http://#HMP_Proxy_Name#' is used, it will be replaced by the name of the Handy Proxy followed by a '.' character
//      ex : If the Handy Proxy name is 'HMP_XYZ', then 'http://#HMP_Proxy_Name#anystring.hmpr' will become 'http://hmp_xyz.anystring.hmpr'
//    - 'www.' and subdirectories or the '?' or '&' characters in the 'http://HmprCompatibleString' string will NOT be accepted in this file
//  - Local_IP_Address:Port = any IP Address and Port that can be reached locally or inside the Handy Proxy LAN
//  - The '127.0.0.1' IP address is also accepted
//
// WARNING :
//  - Only 'http GET' requests will be accepted by the integraded Handy Web Server
//  - The defined IP Address and Port cannot point to the Handy Proxy itself (this will produce a deadlock error)
//
// Handy Proxy (c) Copyright Handyserv - http://www.handyserv.com
//
//=============================================================================================================
//
//http://AnyFavoriteString.hmpr=:=127.0.0.1:8080
//...
```

9.9. The Handy Proxy Proxy_White_URL_List.DEF file

This file must be placed in the **…\Multichannel_Proxy_Data** directory.

You MUST strictly respect the syntax of this file, otherwise parameters or data will not be understood.

Role of this file :

This file allows to define a specific filtering priority for a site, a link, a link part or a file. There are 8 priority degrees, 8 being the highest one.
We advise against filtering video or music traffic above 0, which could make this traffic not functional. In case of problem with this kind of sites, either you can make them directly accessible on the Internet by your browsers via the « hmp_conf.pac » file (see chapter 9.3), or you can access them via channel 0 of your Handy Proxy by means of a definition to add into the « Proxy_Routing_Table.DEF » file (see chapter 9.7).
If your browser already uses AdBlock (see web site https://adblockplus.org), this function is redundant. Unless you have specific needs, it is not necessary to use this list since it is only a matter of filtering.

```
//=============================================================================================================
//
// List of user-defined White URL list
// File name must be : Proxy_White_URL_List.DEF
// Lines starting with // or ! or { or * or ; are comments
//
// Examples of use : Level==any_web_site.xyz (Level value can be 0 up to 8 or can be void including the "==" separator)
//
// any_trusted_web_site.xyz
// 0==any_other_trusted_web_site.xyz
// 1==any_web_page\any_subdirectory
// 2==any_web_site.xyz
// 3==any_account.thisWebSite.xyz
// 5==any_other_web_site.xyz
// 8==any_unknown_web_site.xyz
//
// Default is set with parameter "Default_Filtering_And_Replacement_Value" (see the "Multichannel_Proxy_Configuration.cfg" file)
//
// Where :
//  0==Any_Web_Site = Proxy is "transparent" and
//     the HTTPS over-encrypted data exchanges between Handy Proxies is DISABLED (color of logging events on screen : black)
//  1==Any_Web_Site = NO proxy EXTENDED URL filtering and replacement (color of logging events on screen : light blue)
//  2==Any_Web_Site = NO proxy LOCAL URL filtering and replacement (color of logging events on screen : light blue)
//  3==Any_Web_Site = NO proxy EXTENDED URL filtering BUT replacement (color of logging events on screen : light blue)
//  4==Any_Web_Site = NO proxy LOCAL URL filtering BUT replacement (color of logging events on screen : light blue)
//  5==Any_Web_Site = NO proxy URL replacement of any kind (color of logging events on screen : light blue)
//  6==Any_Web_Site = NO proxy EXTENDED URL replacement (color of logging events on screen : light blue)
//  7==Any_Web_Site = NO proxy LOCAL URL replacement (color of logging events on screen : light blue)
//  8==Any_Web_Site = Proxy will perform FULL filtering and replacement (color of logging events on screen : blue)
//
//  "transparent" means that there is NO proxy URL filtering/replacement of any kind
//  "filtering" means that listed links will not be accessible
//  "replacement" means that listed links are replaced (see configuration file ; only "scr=" HTML tags are concerned)
//
// Handy Proxy (c) Copyright Handyserv - http://www.handyserv.com
//
//=============================================================================================================

//Real examples :
3==.akamaihd.net
3==.facebook.com
0==static.panoramio.com.storage.googleapis.com
0==mail.google.com
3==.google.com
0==.googleusercontent.com
0==.googlevideo.com
1==grooveshark.com
8==handyserv.com
0==maps.gstatic.com
3==.ning.com
0==.real.com
0==.sndcdn.com
0==soundcloud.com
```

0==.sun.com
0==.vimeo.com
0==.vimeocdn.com
0==.youtube.
0==.ytimg.com

9.10. The Handy Proxy Multichannel_Proxy_Email_List.hpe file

This file must be placed in the **…\Multichannel_Proxy_Data\License_Sharing** directory.

You MUST strictly respect the syntax of this file, otherwise parameters or data will not be understood.

Role of this file :

This file allows to share your Handy Proxy's user license. Please refer to chapter 3 « Sharing your account » of this manual.

```
//================================================================
//
// Handy Proxy License Sharing by Emails
//
// Email List File - File extension must be : .hpe
// Lines starting with // or ! or { or * or ; are comments
//
// 250 addresses maximum per file are allowed
//
// Handy Proxy (c) Copyright Handyserv - http://www.handyserv.com
//
//================================================================

//any_name@any_email_service.com
//...
```

10. How to integrate exchanges between your application and a Handy Proxy

In addition to via your browsers, there are other ways to integrate your Handy Proxy in your daily use of the Internet.

If you sometimes use specific applications allowing to indicate the name of a Proxy or a link to a determined site or page, you can use a function allowing you to define by which Handy Proxy channel you will pass through.

The syntax of this function is the following :

hmp_target_channel_id=x (x = number of the chosen channel)

Its usage is the following : this command must be added at the end of a web link.

For example :

http://www.anysite.web?hmp_target_channel_id=9

In this example the site anysite.web will be routed by channel 9 of your Handy Proxy.

This command MUST be inserted after the URL of the site to reach, preceded by the character « ? » if it is alone or character « & » if it is not the case. This command will be entirely removed by your Handy Proxy before calling the site in order to avoid sending it a command that will not be understood. This command must be added to every call of the site including the page that will be reached but also images, Javascripts or sub-pages contained in this page. Otherwise, only the page will be rerouted. You must consequently, in your applications and integrations, not forget to insert the command for each link that will have to be called. If it is not possible, you will have to define this call via the « Proxy_Routing_Table.DEF » file (see chapter 9.7) that will automatically route all which is related to the accessed link. This function is convenient if you have to integrate in a given web page the access to a site hosted by your Handy Web Server or to a part of it (via for example an iframe function).

Figure out that you have a web site hosted in a classical way by a hosting service. In this web site, you would like to give access (in a private way) to a page, a part of a page or even an image which is hosted by your Handy Web Server. This page, part of a page or image is unaccessible, as you know, without passing through a Handy Proxy. It will become accessible as long as, in your hosted site, you indicate the domain name (see chapter 9.8) of your Handy Proxy followed by the command described here. In this case, and if the defined channel is for example number 9 for this command, all Handy Proxies that want to access this service MUST be configured to access your Handy Web Server via channel 9. If it is not the case your command will not work, either because the channel of a Handy Proxy will not point properly to your Handy Proxy, or this channel will be routed to another Handy Proxy where the requested service does not exist.

If you do not need to use a specific domain name for your Handy Web Server (see chapter 9.8), you can use direct access to your Handy Web Server by its default domain name, for example « http://hmp_12345.handywebserver.hmpr », that will be retrieved automatically by the Handy Proxies being connected to the Handy Proxy named « hmp_12345 ». This method allows to avoid having to respect a determined channel number in your applications.

Your Handy Proxy makes also available other commands for your Handy Web Server and your Handy Browser (see chapters 5, 6 and 7).

If you wish to benefit from the integration of specific commands or keywords allowing to add functionalities matching your needs, we invite you to contact us. Our developers will gladly analyze your request.

Concerning the Internet traffic routing and messaging server functions of your Handy Proxy, it is possible to create an configuration independent from the one we provide by default. For example, a group or cluster of servers could be set up if the traffic routing and messaging services of your Handy Proxy(ies) were to be made available to a large number of users.

As well, we can provide the hosting of your own Handy Proxy users database in order to make your configuration totally independent from the default one.

For all these specific functions and custom developments, we also invite your to contact us : http://www.handyserv.com.