Solution de communication sécurisée tout-en-un

Handy Multichannel Proxy

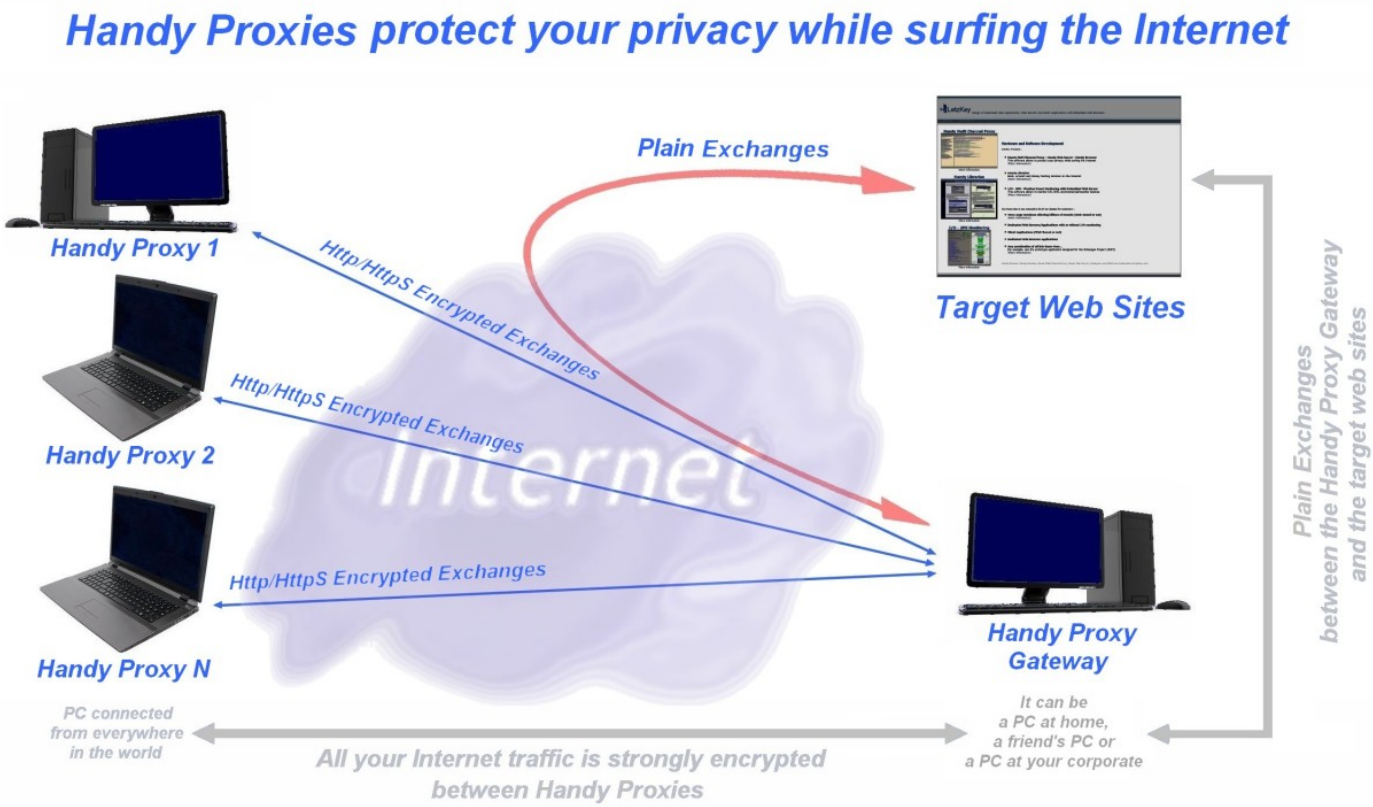
Handy Messaging Server

Handy Web Server

Handy Browser

Manuel

Version 1.0



Handy Proxy, Multichannel Handy Proxy, Handy Messaging Server, Handy Web Server, Handy Browser, Handy Email, Handy Messenger (c) Copyright by Handyserv

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

Manuel **Version 1.0**

1. INTRODUCTION AUX APPLICATIONS HANDY PROXY 4

1.1. Configuration système minimale 8

1.2. Installation 8

1.3. Démarrage rapide & Aperçu des puissantes fonctionnalités du Handy Proxy 8

1.3.1. Premier démarrage en tant qu'utilisateur 8

1.3.2. Configuration de base si vous désirez que votre Handy Proxy devienne un routeur de trafic Internet et/ou un serveur de messagerie pour d'autres utilisateurs 8

1.3.3. A quoi servent et comment exploiter au mieux les 10 canaux de votre Handy Proxy 9

1.3.4. Aller encore plus loin : interconnexion de deux Handy Proxy pour atteindre un autre réseau 13

2. UTILISATION DE VOTRE HANDY PROXY 14

2.1. Comment donner accès à votre Handy Proxy à d'autres utilisateurs 22

2.2. Comment autoriser ou non l'accès à un lien web 23

3. PARTAGER SA LICENCE 25

4. QUEL EST LE POINT DE SORTIE D'UN CANAL (BOUTON « *CHANNEL WHO IS* ») 28

5. HANDY WEB SERVER AVEC OPTION DE PAGES ENCRYPTEES 29

6. ENCRYPTION DE FICHIERS AVEC LE HANDY WEB SERVER 35

7. LE NAVIGATEUR HANDY BROWSER 38

7.1. Les différents modes d'affichage du Handy Browser 41

8. HANDY COMMUNICATION 42

8.1. Introduction 42

8.2. Premières étapes de configuration des applications Handy Email et Handy Messenger 43

8.3. Handy Messenger 46

8.4. Handy Email 52

9. LES FICHIERS DE CONFIGURATION DU HANDY PROXY 59

9.1. Fichier « Handy Proxy Master Configuration » (Multichannel_Proxy_Master_Config.def) 59

Handy Proxy, Multichannel Handy Proxy, Handy Messaging Server, Handy Web Server, Handy Browser, Handy Email, Handy Messenger (c) Copyright by Handyserv

9.2. Fichier « Handy Proxy Configuration » (par défaut : Handy_Proxy_Configuration.cfg) 63

9.3. Fichier Handy Proxy hmp_conf.pac 67

9.4. Fichier Handy Proxy Proxy_Authorized_Connection_List.DEF 68

9.5. Fichier Handy Proxy Proxy_IP_to_Users_Translation_Table.DEF 69

9.6. Fichier Handy Proxy Proxy_Local_URL_Filter_File.DEF 70

9.7. Fichier Handy Proxy Proxy_Routing_Table.DEF 71

9.8. Fichier Handy Proxy Proxy_String_to_IP-Destination_Table.DEF 73

9.9. Fichier Handy Proxy Proxy_White_URL_List.DEF 74

9.10. Fichier Handy Proxy Multichannel_Proxy_Email_List.hpe 76

10. COMMENT INTEGRER VOTRE HANDY PROXY DANS VOS APPLICATIONS ET/OU VOTRE USAGE QUOTIDIEN 77

1. Introduction aux applications Handy Proxy

Cette solution est un service de protection parfaitement adapté aux besoins de toutes les personnes qui sont amenées à accéder à Internet via leur PC ou tablette Windows à partir d'endroits potentiellement « hostiles ». Elle est également le partenaire idéal si vous souhaitez envoyer des e-mails encryptés sans passer par un service tiers ou créer des services web dont l'accès serait strictement limité à des personnes dûment autorisées grâce aux fonctions d'encryption intégrées.

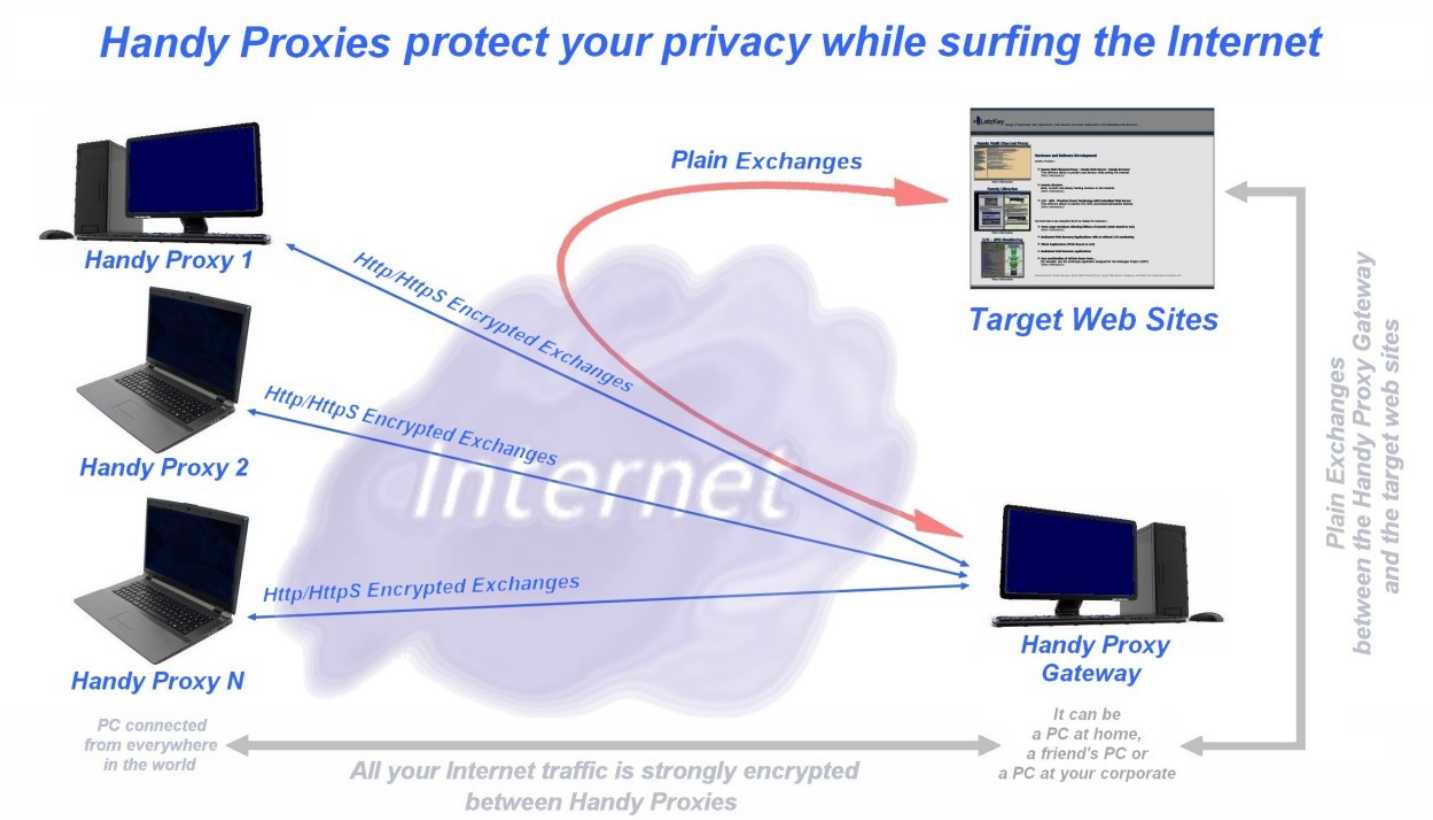
Vos données sont bien évidemment importantes, voire cruciales. Que vous soyez un particulier, un professionnel de l'informatique, un fournisseur Internet, un dirigeant d'entreprise ou toute personne souhaitant protéger des données contre le piratage informatique, notre service sera le maillon indispensable de votre configuration.

Grâce à l'encryption complète des données transférées entre deux Handy Proxy, vous pourrez :

- éviter que des données sensibles et confidentielles telles que votre identifiant et mot de passe ne soient volées ou que vos données ne soient analysées/revendues/stockées pour une utilisation frauduleuse si vous vous connectez à Internet à partir d'une borne WiFi publique, par exemple ;

- éviter, lorsque vous vous connectez à Internet à partir d'un autre endroit que votre habitation ou votre bureau, que vos déplacements ne soient écoutés par les nombreux sites web qui utilisent les données comportementales à des fins de marketing ou par des personnes mal intentionnées ;

- n'accéder à Internet « en clair » qu'à partir de votre habitation ou de votre bureau, même si vous vous trouvez dans un autre endroit ou à l'étranger.



L'installation de votre configuration Handy Proxy peut se faire sur un disque local de votre PC ou sur une clé USB qui dans ce cas stockera l'ensemble de vos fichiers de paramètres ainsi que tout le contenu de votre messagerie sans rien sauvegarder ailleurs dans le PC hôte. De même, le navigateur Handy Browser fourni en standard et basé sur la technologie Chrome sauvera l'ensemble de votre navigation (fichier temporaire) à l'endroit où il est installé, càd sur une clé USB. Une telle installation vous permet donc d'utiliser votre configuration en toute sécurité et confidentialité là où vous le souhaitez.

Cette possibilité d'installer votre Handy Proxy sur une clé USB vous permettra par exemple de faire vos opérations « Home Banking » sur un PC mis à disposition dans un endroit public, occasionnel ou autre non habituel sans prendre le risque de laisser une trace de vos opérations et/ou accès tout en les sécurisant par encryption.

Grâce au Handy Messaging Server intégré au Handy Proxy et aux applications Handy Email et Handy Messenger, vous pourrez :

- **Communiquer avec vos correspondants d'une manière totalement sécurisée et indépendante de tout fournisseur Internet ou de tout service de messagerie instantanée ou d'e-mail et même d'Internet en lui-même puisque vos échanges de messages seront encryptés et qu'Internet ne servira que de transporteur de ces données (ces fonctions ne font pas appel aux protocoles POP3, IMAP ou autres afin d'être totalement autonomes par rapport à ceux-ci). Ce qui est visé par ces applications est la plus stricte confidentialité de vos messages, ce qui est indispensable pour les entreprises notamment.**

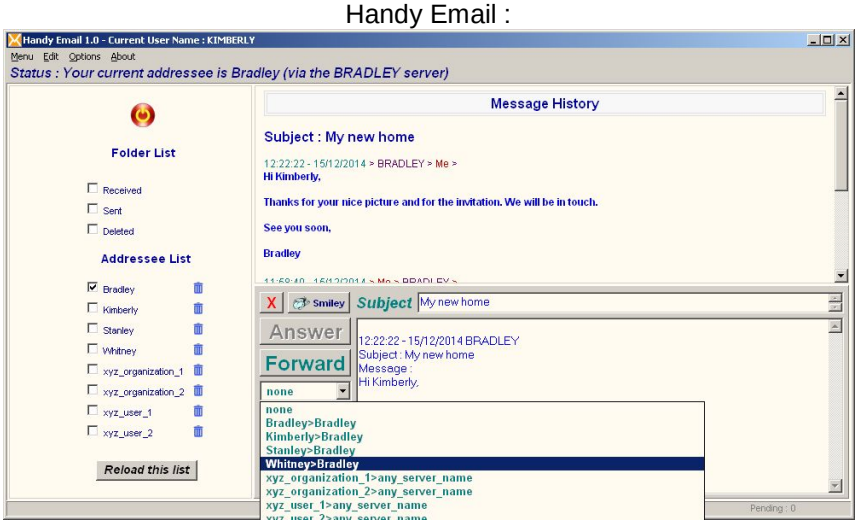
- Créer très facilement votre messagerie privée pour votre famille, association ou société. Celle-ci sera accessible en interne au sein de votre réseau local et/ou via Internet partout dans le monde (accès WiFi, …).

- Envoyer des messages et des fichiers attachés complètement encryptés en mode client-serveur (d'ordinateur à ordinateur), vous permettant une totale confidentialité dans vos échanges privés ou commerciaux. Un filtre sur le type de fichier joint est actif ne permettant pas, par exemple, d'envoyer des programmes qui démarreraient tout seuls. A part cela, tous les types de fichiers peuvent être envoyés en pièces jointes (doc, docx, PDF, photos, …).

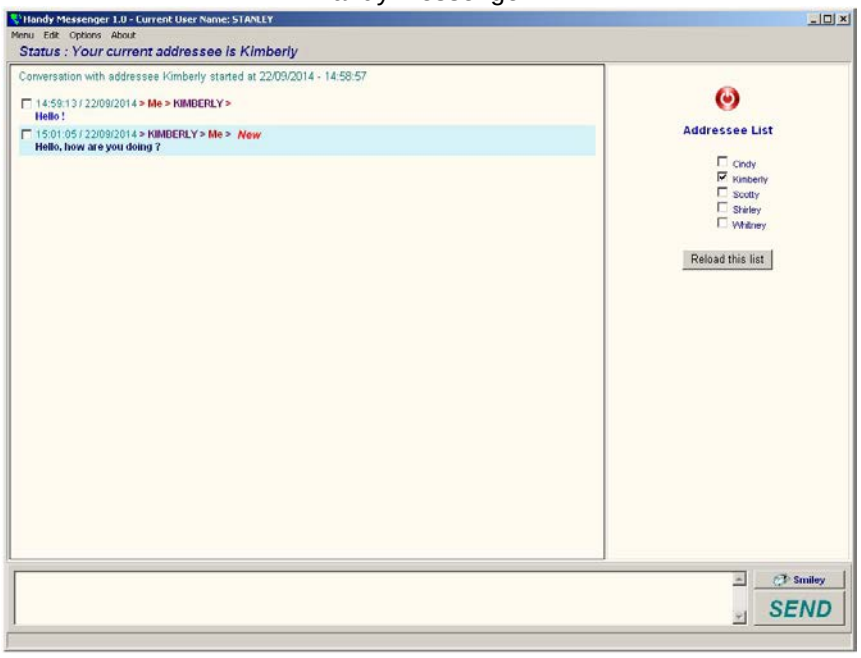
- Utiliser ces outils sans devoir installer une configuration de base de données SQL ou d'autres modules complexes, puisque le Handy Messaging Server se charge de tout pour vous (tout est déjà prêt à fonctionner dès l'installation du package). **C'est donc une fonction utilisable par tout le monde qui s'installe d'elle-même automatiquement, il vous restera uniquement à définir vos destinataires pour pouvoir l'utiliser dans la minute qui suit.**

De plus, un mécanisme de sécurité s'applique automatiquement lors de la création des messages. Ceux-ci ne seront donc pas des vecteurs de transport de virus par l'ajout de micro-programmes Javascripts ou autres.

Handy Email :



Handy Messenger :



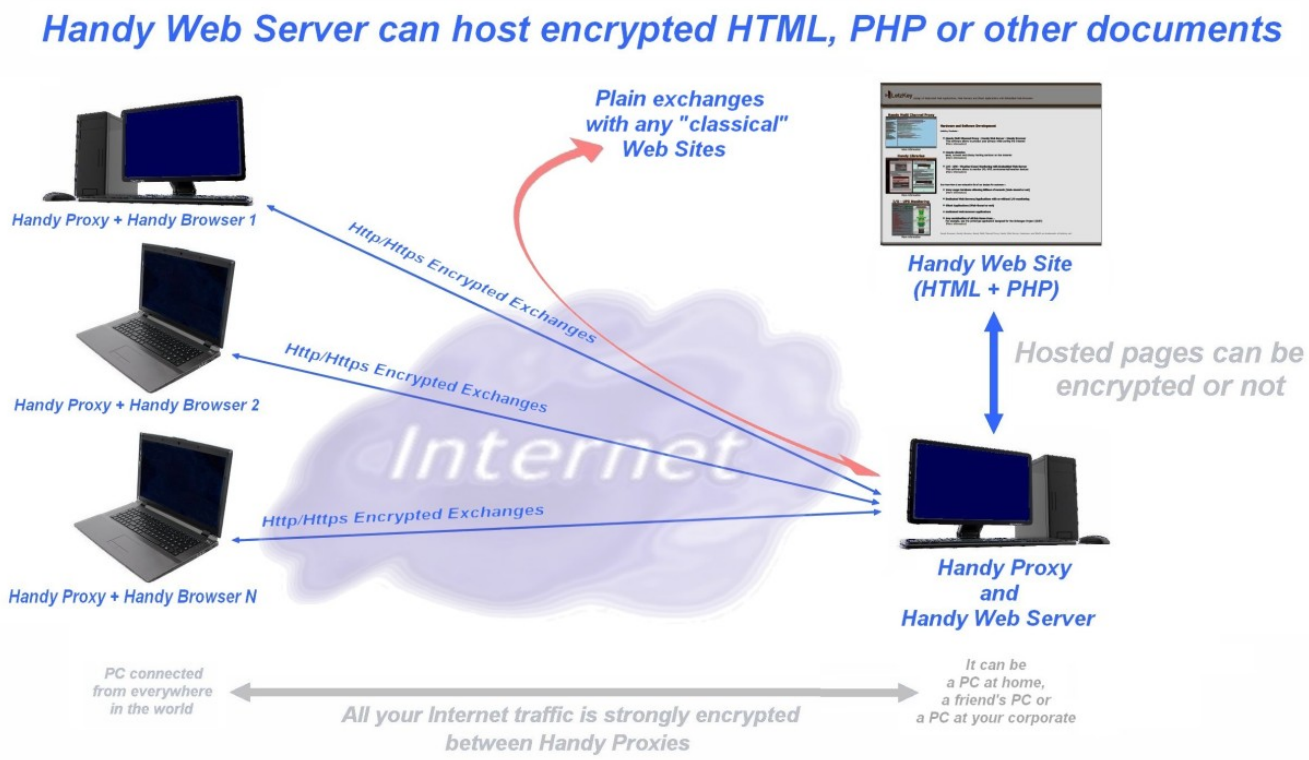
Handy Proxy, Multichannel Handy Proxy, Handy Messaging Server, Handy Web Server, Handy Browser, Handy Email, Handy Messenger (c) Copyright by Handyserv

Grâce au Handy Web Server intégré au Handy Proxy ainsi qu'au Handy Browser fourni par cette solution, vous pourrez :

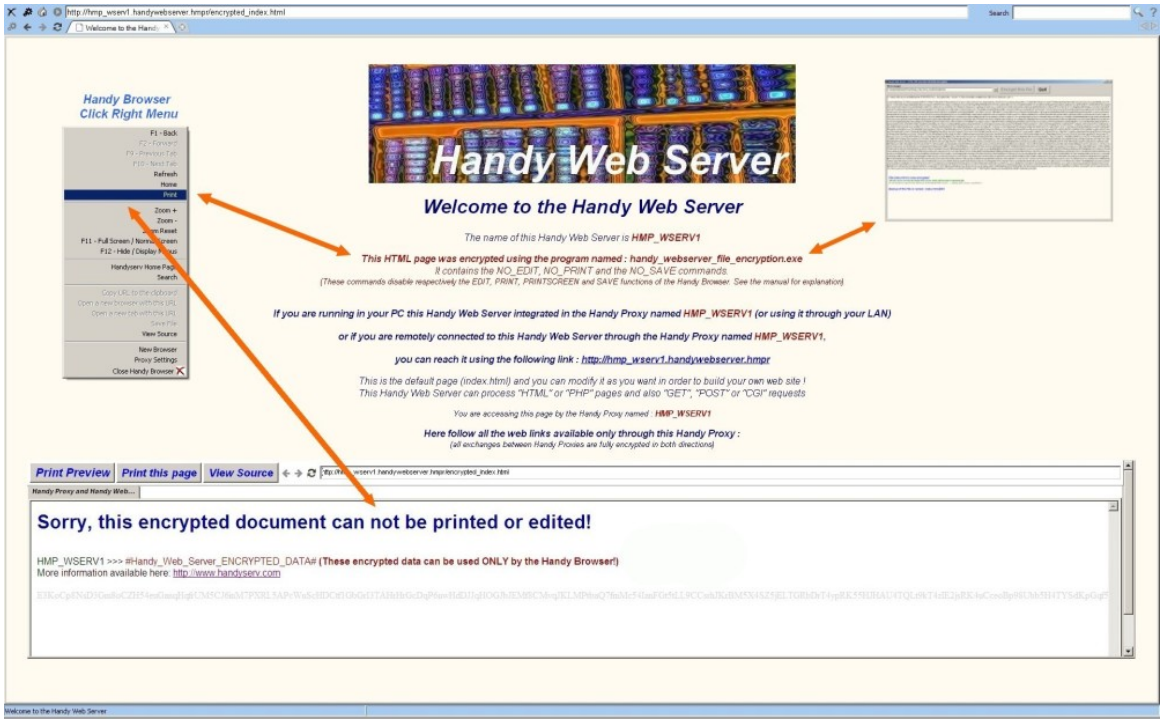
- créer et héberger votre propre site web et décider de le rendre accessible à certaines personnes uniquement, ou au contraire de le rendre public ;

- encrypter vos pages HTML, Javascripts ou code PHP afin de les protéger contre toute modification, impression ou visualisation ;

- obtenir automatiquement un nom de domaine pour votre site web tel que « http://any_name.handywebserver.hmpr » (nom de domaine "public" pour d'autres utilisateurs du Handy Proxy) ou « http://any_name.hmpr » (nom de domaine privé).



Handy Web Server avec pages encryptées



Handy Browser avec pages encryptées

Notre solution de navigation sécurisée vous permettra également de :

- gérer facilement les listes de personnes autorisées à accéder au Handy Proxy partagé que vous avez installé chez vous ou dans votre entreprise ;

- partager votre licence d'utilisation avec autant de membres de votre famille, amis ou collègues que ne le permet le nombre de connexions maximum autorisées par cette licence ;

- définir jusqu'à 10 connexions différentes vers d'autres réseaux, services ou d'autres Handy Proxy selon un site web particulier, un groupe de sites web définis ou un navigateur Internet déterminé ;

- définir des priorités d'accès ou empêcher l'accès à des sites web dont vous ne souhaitez pas qu'ils puissent être visités par votre famille ou vos collègues ;

- éviter en conséquence que certains sites web atteignent vos navigateurs Internet ou installent une application malveillante (*malware*) bien avant que votre antivirus ne soit en mesure de la détecter ;

- passer facilement en mode *off line* alors que vous n'êtes pas devant votre poste de travail, et ceci pour tous les navigateurs et pages web ouvertes dans votre session Windows.

Notre solution de navigation sécurisée est également dynamique puisque :

- chaque Handy Proxy utilise sa propre et unique méthode d'encryption et chaque Handy Proxy peut avoir sa propre clé d'encryption privée (définie et modifiable uniquement par le propriétaire d'une configuration) ;

- la méthode d'encryption du Handy Proxy change automatiquement toutes les 4 heures, d'une manière totalement transparente pour les utilisateurs.

De plus :

- toutes les 24 heures, tous les Handy Proxy en fonctionnement doivent recalculer entièrement la manière dont ils encryptent leurs transferts de données vers les autres Handy Proxy ;

- les échanges HTTPS/SSL peuvent être sur-encryptés de manière à augmenter la protection de vos données ;

- pour 2 Handy Proxy interconnectés et échangeant des données encryptées, Internet n'est utilisé que comme un transporteur de données entre 2 points définis par leurs adresses IP. TOUS les échanges entre ces 2 points sont fortement encryptés, aussi bien les requêtes HTTP ou HTTPS sortantes que les données entrantes et les pages web.

Toutes ces fonctions et méthodes d'encryption rendent inconcevable la possibilité d' « écouter » vos activités sur Internet ou de capter vos données sensibles (telles que données bancaires, identifiants, mots de passe,…) lorsque vous vous connectez à Internet à partir d'un endroit peu sûr ou inconnu.

Toutefois, un Handy Proxy peut être utilisé dans tous les cas, y compris chez soi ou à son bureau, avec ou sans connexion vers un autre Handy Proxy, car les fonctions utiles de filtrage de sites web ainsi que d'autres fonctions seront toujours disponibles.

En outre, notre solution d'intégration de site web dans le Handy Proxy avec ou sans encryption des pages hébergées est idéale afin de vous permettre de créer vos sites web PHP, HTML et Javascript protégés de l'Internet « classique » et d'obtenir un contrôle total sur ce qu'il en est fait et qui est autorisé à les visiter.

Cette fonction d'encryption de pages web uniquement accessibles via un Handy Proxy permet également de protéger votre propriété intellectuelle et/ou vos investissements et/ou vos données contre toute personne qui n'est pas autorisée à y accéder. Vous pouvez ainsi créer des sites web « familiaux » ou « d'entreprise privée » qui peuvent être accédés à partir de n'importe quel endroit du globe pour autant que vous l'ayez autorisé.

Comme atout supplémentaire pour les entreprises ou organisations, nous pouvons fournir l'hébergement de votre propre base de données d'utilisateurs de vos Handy Proxy afin de rendre votre configuration totalement indépendante de celle fournie par défaut. Vous disposeriez alors d'une configuration propre à vos besoins disposant de toutes les fonctionnalités exposées ci-dessus. A nouveau, seules les personnes autorisées à utiliser votre environnement spécifique pourront y accéder.

Handy Proxy, Multichannel Handy Proxy, Handy Messaging Server, Handy Web Server, Handy Browser, Handy Email, Handy Messenger (c) Copyright by Handyserv

1.1. Configuration système minimale

Microsoft Windows 2000, XP, 7, 8
200 MB d'espace disque dur disponible
256 MB RAM
Microsoft Internet Explorer 6 ou ultérieur

1.2. Installation

Le progiciel Handy Proxy est disponible à partir du site web Handyserv (http://www.handyserv.com). Vous pouvez le télécharger et l'installer très facilement, comme tout autre logiciel.

Nous garantissons que nos programmes et modules sont exempts de tout *adware*, *malware* ou virus pour autant qu'ils soient téléchargés à partir de notre site web. Pour vous aider à vérifier cela, il vous est fourni sur notre site un *checksum* de type MD5 qui vous permettra de vérifier si le module à télécharger est bien le nôtre et n'a pas été modifié. De plus les différents programmes (.exe) fournis dans notre package sont eux-mêmes protégés également par un *checksum* de type MD5 qui au cas où il ne serait pas vérifié lors du lancement d'un de nos programmes bloquerait celui-ci en indiquant un message d'erreur.

Des icônes seront créées lors de l'installation. Nous vous invitons à ajouter l'icône Handy Proxy au dossier « Démarrage » du menu « Démarrer » de Windows, ce qui lancera automatiquement votre Handy Proxy.

1.3. Démarrage rapide & Aperçu des puissantes fonctionnalités du Handy Proxy

Voici comment démarrer pour la première fois le Handy Proxy et ses autres fonctionnalités.

1.3.1. Premier démarrage en tant qu'utilisateur

- Téléchargez le package à partir de notre site web et installez-le en suivant les étapes habituelles de cette installation. Lancez le Handy Proxy comme cela vous sera proposé.

- Lors du premier démarrage, le Handy Proxy va vous demander d'introduire le nom de votre configuration. Si le nom souhaité est libre, il sera accepté et votre configuration sera désormais nommée. A ce moment-là, le Handy Proxy sera en état « Proxy disabled ». Cliquez sur le bouton en haut à gauche (« Proxy disabled ») pour que celui-ci se mette en état « Proxy enabled ». Si votre connexion Internet n'est pas active, le Handy Proxy vous le signalera. Dans le cas contraire, il se mettra en attente de communication.

- Lorsque le Handy Proxy va passer en mode « Proxy enabled », il va découvrir que Windows ne reroute pas les communications Internet via son intermédiaire. Le Handy Proxy va donc vous le signaler par un message à l'écran vous précisant les bons paramètres à indiquer à Windows, puis il va ouvrir la fonction Windows « Propriétés d'Internet » qui vous permettra, via l'option « Paramètres réseau », de faire passer le trafic Internet via votre Handy Proxy. Pour plus d'informations, veuillez vous référer au lien suivant :

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

  Certains navigateurs ne vont pas automatiquement suivre les paramètres proxy de Windows. C'est par exemple le cas de Firefox. Il faut alors leur indiquer manuellement d'utiliser les paramètres proxy par défaut de Windows.

- A partir de maintenant, votre Handy Proxy est prêt à fonctionner et configuré par défaut. Si vous désirez utiliser les fonctions de messagerie Handy Email et Handy Messenger, il vous reste alors à configurer le ou les serveurs de messagerie vers lesquels vous allez vous connecter ainsi que la liste de vos destinataires. Sur l'écran de contrôle du Handy Proxy, celui-ci vous indiquera que vous pouvez définir votre configuration optionnellement comme serveur de messagerie mais avant d'utiliser cette fonction, veuillez impérativement lire attentivement le point suivant.

1.3.2. Configuration de base si vous désirez que votre Handy Proxy devienne un routeur de trafic Internet et/ou un serveur de messagerie pour d'autres utilisateurs

Après avoir réalisé la configuration de base expliquée ci-dessus, si vous désirez que votre configuration soit mise en partage en tant que rerouteur sécurisé de trafic Internet et/ou serveur de messagerie pour les applications Handy Email et Handy Messenger, voici les étapes de configuration à suivre.

- Tout d'abord, vous devez définir une adresse IP fixe locale au sein de votre réseau pour que la configuration ait une adresse stable. A défaut, cette adresse risque d'être modifiée dynamiquement et votre configuration pourrait ne plus

être retrouvée par vos correspondants. Pour cela, il faut utiliser les fonctions de Windows qui permettent de rendre fixe l'adresse IP de votre PC.

Pour vous aider, voici un lien vers un site qui vous explique comment procéder pour toutes les versions Windows existantes :

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

- Maintenant que votre PC a une adresse IP fixe, il faut rendre celui-ci accessible par vos correspondants qui seraient connectés à Internet et donc hors de votre réseau local. Pour cela, vous devez paramétrer votre routeur Internet pour qu'il reroute le trafic de vos correspondants vers votre PC connecté à une adresse IP fixe dans votre réseau. Pour ce paramétrage, nous vous invitons à lire le chapitre 2.1. « Comment donner accès à votre Handy Proxy à d'autres utilisateurs ». Ce chapitre explique point par point, avec des liens vers des tutoriaux, comment procéder en fonction du routeur dont vous disposez.

- Maintenant que votre PC est accessible à partir d'Internet via les fonctions NAT de votre routeur et que votre PC a une adresse IP fixe, il est donc potentiellement accessible en mode sécurisé par vos correspondants connectés à votre réseau local ainsi que ceux qui seraient à l'extérieur, via Internet cette fois.

Votre configuration est à présent opérationnelle, soit en tant qu'utilisateur soit en tant qu'utilisateur + mode serveur. Si vous désirez paramétrer davantage votre configuration et augmenter son niveau de sécurité, nous vous invitons à lire le chapitre 9 qui vous fera découvrir tous les fichiers de paramétrage disponibles (le password par défaut est 1234 pour les fichiers sensibles, ceux-ci ne sont modifiables que via le programme Handy Edit spécialement mis au point à cette fin).

Si vous modifiez les paramètres de base de votre Handy Proxy, nous vous invitons à clôturer la session en fermant l'application et en la relançant. Pour tous les fichiers de filtres ou de configuration d'utilisateurs il n'est pas nécessaire de relancer votre Handy Proxy, il existe à cet effet un bouton « Reload URL filter and other files ». De même, vous pouvez en tant qu'utilisateur ouvrir une session sous différents noms et donc différentes configurations de connexion vers d'autres utilisateurs.

Veuillez noter que chaque configuration Handy Proxy peut devenir un serveur de messagerie. Toutefois, nous vous invitons à n'en créer qu'un seul au sein de votre famille, association ou entreprise afin de simplifier les configurations des différentes utilisateurs auxquels il vous suffirait de faire parvenir le fichier de définition de la messagerie. Il est cependant tout à fait possible de paramétrer celui-ci pour que vous ou vos correspondants puissiez être en communication avec plusieurs serveurs (voir à ce sujet les explications complètes disponibles au chapitre 9 du présent manuel). Par exemple, vous pourriez très bien avoir un Handy Messaging Server au sein de votre entreprise et être en connexion avec un ou plusieurs autres serveurs du même type dans d'autres organisations ou divisions avec lesquelles vous souhaitez avoir des échanges sécurisés. Il en va de même pour la fonction Handy Web Server dont l'accès est strictement contrôlé et qui vous permettra également de partager vos informations de manière sécurisée avec les personnes que vous aurez dûment autorisées à y accéder.

Attention : si votre configuration est en mode rerouteur sécurisé de trafic Internet et/ou serveur de messagerie, vous ne pouvez pas changer le nom de votre Handy Proxy puisque vos correspondants utiliseront celui-ci pour se connecter vers vous. Dans le cas contraire, si vous modifiez votre nom de configuration et que vos correspondants ont déjà intégré ce nom dans leurs fichiers de configuration, ils ne vous retrouveront plus et votre serveur sera considéré comme absent ! Nous vous invitons à faire un choix de nom de serveur définitif afin d'éviter que vos correspondants ne doivent modifier leurs configurations.

1.3.3. A quoi servent et comment exploiter au mieux les 10 canaux de votre Handy Proxy

Maintenant que vous êtes configuré en tant qu'utilisateur et/ou serveur de votre Handy Proxy, nous allons voir ce qu'il est possible de faire grâce aux 10 canaux disponibles via un exemple.

Ces canaux (ou « sorties ») permettent à partir d'un navigateur de diriger le trafic Internet de ce navigateur vers l'une de ces sorties.

Chaque canal peut être orienté soit vers Internet en direct (par défaut canal 0) soit vers un autre Handy Proxy ou un autre réseau ou encore un autre service pouvant être lui-même un proxy.

Prenons l'exemple du réseau Tor. Un Handy Proxy ne peut pas s'interfacer directement vers le réseau Tor puisque celui-ci doit s'interfacer en mode « SOCKS » alors qu'un Handy Proxy ne connaît que l'interface « http/https ». Dès lors, pour atteindre le réseau Tor, il faut passer par un interface tiers comme celui qu'offrent les programmes Surfing Tunnel ou ChrisPC Proxy. Un autre service pouvant être interfacé par votre Handy Proxy est le programme UltraSurf qui donne accès à des proxys distants. Il y a bien entendu encore d'autres services possibles, nous ne pouvons pas tous les énumérer ici.

Venons-en à un exemple concret d'utilisation approfondie des fonctionnalités disponibles et de leur puissance :

Imaginons que vous désirez vous interfacer aux trois services susmentionnés en plus de vous connecter à deux autres Handy Proxy, l'un étant on-line chez vous et l'autre on-line dans votre bureau (cas où vous êtes à l'extérieur de ces deux endroits avec votre portable).

Imaginons également que vous désirez ne pas accéder aux bases de données de Handyserv en direct pour des raisons de sécurité en fonction de l'endroit où vous êtes (hotspot Wi-Fi par exemple). De même, dans notre exemple, vous souhaitez que votre Handy Proxy soit un serveur pour d'autres et vous souhaitez passer par une page web de votre choix pour retrouver votre adresse IP publique à nouveau sans passer par le service offert par défaut par Handyserv (veuillez noter que votre adresse IP publique est indispensable dans le cas où vous souhaitez partager votre configuration avec d'autres utilisateurs et/ou devenir serveur de messagerie). **Il s'agit expressément de l'adresse IP que votre fournisseur Internet vous attribue, et en aucun cas de celle qui pourrait apparaître au travers d'un service tel que Tor ou autre**. Cette dernière ne pointe en effet en aucun cas vers votre Handy Proxy, et donc celui-ci ne serait pas accessible par d'autres utilisateurs qui le verraient « absent ».

Pour arriver à une solution telle que décrite dans cet exemple, vous devez configurer votre Handy Proxy et le paramétrer adéquatement. Voir à ce sujet le chapitre 9 du présent manuel, fichiers de configuration Master et autres.

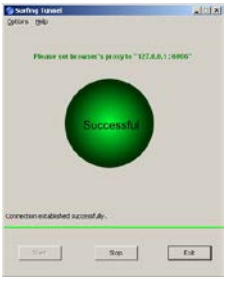
Dans notre exemple, lorsque vous démarrerez votre programme Handy Proxy vous obtiendrez à l'écran les informations suivantes :

Extrait de l'écran principal de votre Handy Proxy

On voit dans cette copie d'écran tout d'abord que votre Handy Proxy a été rechercher votre adresse IP publique via une page définie par le paramètre « Link_to_fetch_the_Multichannel_Proxy_Public_IP_Address » (fichier Multichannel_Proxy_Master_Config.def ; cliquez sur le bouton ci-dessous, password d'accès par défaut : 1234).

Ensuite il a été défini (toujours dans le même fichier) d'atteindre le réseau Tor pour accéder aux bases de données de Handyserv via le paramètre « Fetch_Multichannel_Proxy_Database_Address/Port » afin qu'il pointe vers l'adresse et le port du programme d'interface Surfing Tunnel (vers le réseau Tor) qui dans notre cas se trouve à l'adresse 127.0.0.1 et le port 6006.

Via l'interface Surfing Tunnel et le réseau Tor le Handy Proxy de notre exemple apparaît sous une autre adresse IP que son adresse publique. Cette information vous est indiquée sous la forme d'une géolocalisation à la fois pour indiquer que votre emplacement est bien retrouvé via votre adresse IP publique et sous quelle autre adresse IP vous apparaissez au serveur d'Handyserv. Veuillez noter que tous ces échanges sont dûment codés et encryptés pour toutes les informations sensibles échangées entre votre Handy Proxy et les serveurs de bases de données de Handyserv.



Copie de l'écran de Surfing Tunnel de ZqWare

Vous voyez dans la copie de l'écran principal de votre Handy Proxy l'énumération des 10 canaux et vers quoi ils pointent ainsi que le résultat d'un test de connexion. Dans cet exemple il est donc utilisé 5 canaux qui pointent vers des services

différents de l'accès direct vers Internet dévolu au canal 0, les canaux 8 et 9 pointant quant à eux vers deux autres Handy Proxy configurés pour être rerouteurs (ils sont donc présumés accessibles).

En fonction des configurations choisies, vos différents navigateurs Internet peuvent voir leur trafic aiguillé vers l'un de ces 10 canaux. Par défaut c'est toujours le canal 0 qui sera sélectionné, c'est-à-dire que vos navigateurs vont atteindre Internet en direct sauf si des ordres d'aiguillage différents sont indiqués via les différents fichiers de configuration et de filtrages (voir à ce sujet le chapitre 9 du présent manuel). Il est donc possible d'aiguiller l'entièreté du trafic d'un navigateur vers un canal bien précis ou de n'en dévier qu'une partie.

Prenons l'exemple où l'on désire rerouter le trafic Facebook, Google et YouTube par exemple pour tous vos navigateurs vers l'un des 10 canaux précis de votre Handy Proxy. Pour cela, éditez le fichier « Handy_Proxy_Routing_Table.def » et indiquez-y selon la syntaxe bien précise que vous devez impérativement respecter (de même que pour tous les autres fichiers de configuration) les noms ou parties de noms de domaine des sites dont vous voulez forcer le reroutage comme suit dans notre exemple où l'accès à Facebook passera entièrement par le canal 0 tandis que le trafic vers Google passera par le canal 8. Votre Handy Proxy met en place une hiérarchie de priorités dont celle qui est indiquée ici outrepasse toutes les autres sauf l'interdiction d'accès à une page déterminée qui est appliquée avant tout.

Proxy_Routing_Table.DEF

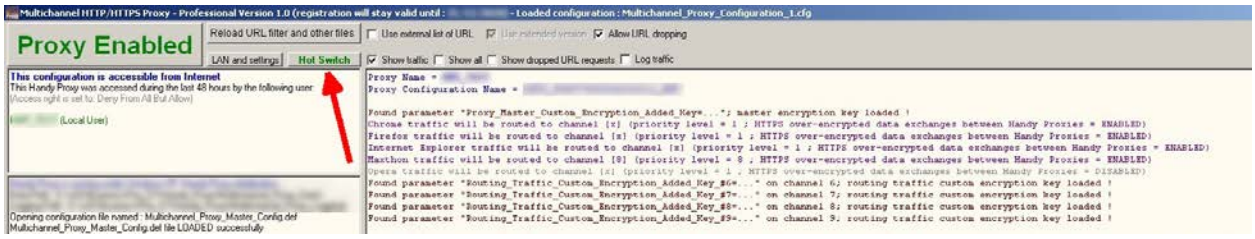
```
1
2  //================================================================================
3  //
4  // Handy Proxy Routing Table - File name must be : Handy_Proxy_Routing_Table.def
5  // Line starting with // or ! or ( or * are comments
6  //
7  // Handy Proxy (c) Copyright Handyserv - http://www.handyserv.com
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
```

Pourquoi forcer le passage du trafic d'un site déterminé par un canal bien précis de votre Handy Proxy : certains sites sont sensibles à votre stabilité géographique, comme Facebook. Si vous passez par le réseau Tor, Facebook vous interpellera tôt ou tard en vous disant que vous accédez « géographiquement » à son service d'une manière aléatoire parce que votre adresse IP change régulièrement (plusieurs fois par heure). Vous pouvez malgré tout procéder de la sorte mais il y a une autre alternative beaucoup plus confortable qui est celle de passer par un autre Handy Proxy en mode routeur dont l'adresse IP sera fixe ou beaucoup plus stable (adresse IP dynamique fournie par votre fournisseur Internet qui change de temps en temps tout en vous faisant apparaître dans la même région géographique et auprès du même fournisseur d'accès). De cette manière votre géolocalisation pour ces services sensibles sera stable puisque le Handy Proxy routeur peut être chez vous ou localisé dans votre bureau qui est un endroit géographiquement stable par définition. Dès lors, forcer le trafic pour certains sites vers un canal déterminé permet d'éviter les difficultés d'une adresse IP qui « voyage » d'un pays à l'autre à la vitesse de l'éclair telle que proposée par le réseau Tor. Toutefois, ce réseau a un intérêt indéniable pour tous les sites dont l'accès ne serait pas protégé via la géolocalisation. Nous vous conseillons de forcer le trafic pour toutes données volumineuses (vidéos, musique etc.) directement vers Internet sans passer par un réseau comme celui de Tor qui peut parfois être très lent, ce qui n'est pas le cas si vous routez ce trafic vers un autre Handy Proxy pour autant que vous soyez connecté vers lui moyennant des accès Internet rapides.

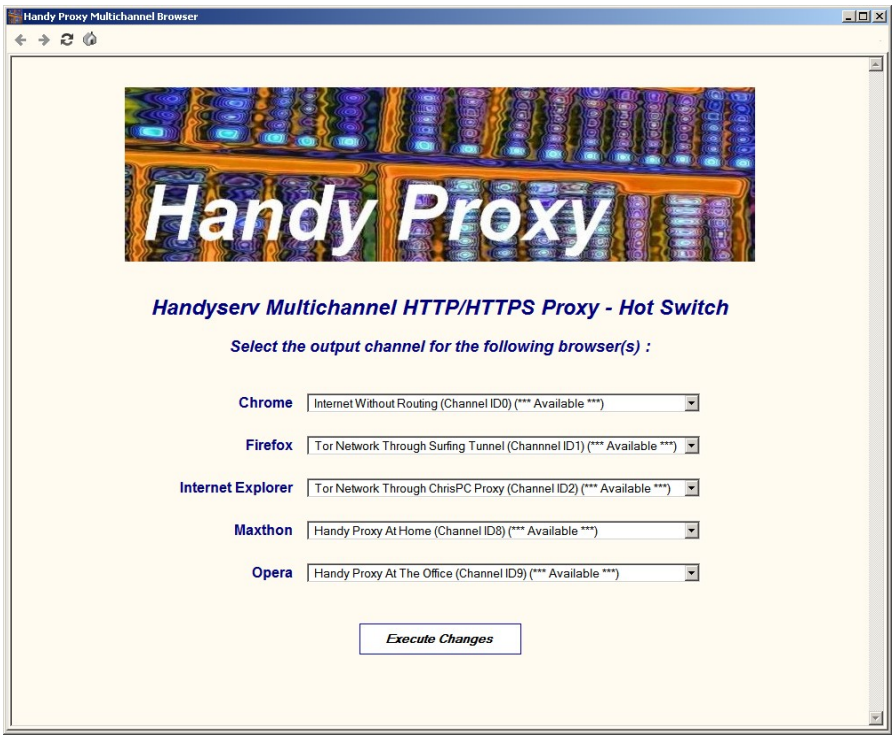
Votre Handy Proxy vous permet donc d'agir au cas par cas pour router le trafic Internet selon vos besoins ou critères de sécurité, de vitesse et en fonction des critères auxquels font appel les sites que vous visitez.

Votre Handy Proxy intègre également pour faciliter votre navigation sur les différents sites une fonction « Hot Switch » qui permet de passer instantanément d'un canal à l'autre de votre Handy Proxy pour vos navigateurs.

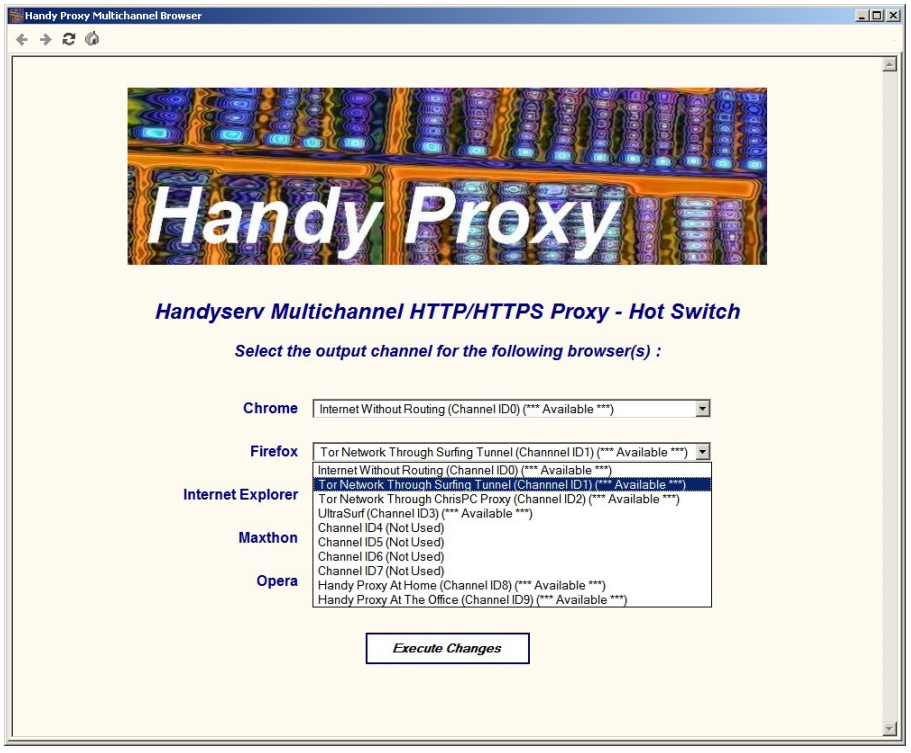
Pour cela, et à partir du moment où vous avez configuré votre Handy Proxy comme dans l'exemple qui nous occupe et qui correspondrait à votre utilisation, il vous suffit de cliquer sur le bouton « Hot Switch » :



Vous obtiendrez alors l'écran suivant qui vous indique l'état de connexion de vos différents navigateurs. Dans ce cas-ci, nous avons installé 5 navigateurs dans Windows :



Lorsque vous déroulez l'un des menus à droite du nom de chaque navigateur, vous obtenez l'écran suivant :



Dans ce menu déroulant vous retrouverez les 10 canaux de votre Handy Proxy et leur état de connexion. Vous pouvez donc à tout moment choisir le canal de sortie pour l'un de vos navigateurs déterminés en fonction de vos besoins. Après avoir sélectionné un canal de sortie pour un navigateur et cliqué sur la confirmation « Execute Changes », votre Handy Proxy va se reconfigurer instantanément et tout le trafic du navigateur choisi va être routé vers le canal redéfini à l'exception des sites dont le routage est filtré ou forcé vers un autre canal, comme expliqué ci-dessus.

Vous voilà à présent dans un état de configuration complète où vous tirez tous les avantages des différents canaux de sortie de votre Handy Proxy en plus d'être, comme nous l'avons vu dans les paragraphes précédentes, dans une configuration d'utilisateur, rerouteur de trafic et serveur de messagerie pour autant que votre Handy Proxy soit accessible via le NAT setup de votre routeur comme déjà expliqué.

1.3.4. Aller encore plus loin : interconnexion de deux Handy Proxy pour atteindre un autre réseau

Maintenant que vous avez découvert au paragraphe 1.3.3. ce qu'il est possible de faire grâce aux 10 canaux disponibles de votre Handy Proxy, voyons comment aller encore plus loin en réalisant une configuration plus sophistiquée.

Pour cela il faut partir du principe que vous avez deux Handy Proxy (Proxy A et Proxy B), le Proxy A étant connecté au Proxy B (celui-ci étant accessible via le NAT setup du routeur Internet, voir chapitre 2.1). Par défaut tous leurs échanges sont encryptés et dans cet exemple nous avons autorisé la surencryption des échanges HTTPS et SSL. Nous avons également mis en place de part et d'autre des clés d'encryption privées (voir les paramètres associés à ces différentes fonctions au chapitre 9).

A partir de cette configuration nous avons prévu que ce soit le canal 9 du Proxy A qui permette de se connecter au Proxy B. Pour qu'un de vos navigateurs (par exemple Firefox) du Proxy A puisse atteindre le Proxy B, il faut que tous les échanges de ce navigateur soient déviés vers le canal 9 du Proxy A (voir la fonction « Hot Switch » et paramètre associé au chapitre 9).

Mettons-nous maintenant au niveau du Proxy B : si rien n'est défini en ce qui concerne le reroutage du trafic de Firefox (local et/ou en provenance du Proxy A), l'ensemble de celui-ci va sortir sur le canal 0 du Proxy B. Toutefois, si au niveau du Proxy B on paramètre le reroutage du trafic de Firefox vers par exemple le canal 5, à ce moment-là tout le trafic de Firefox local et/ou en provenance du Proxy A (passant par le canal 9 de ce dernier dans notre exemple) passera cette fois par le canal 5 du Proxy B.

Imaginons maintenant que le canal 5 du Proxy B ne pointe pas directement sur Internet mais sur une autre adresse IP et un autre port. Dans ce cas, comme vous le comprenez, tout le trafic de Firefox local et/ou en provenance du Proxy A va cette fois passer par cette autre adresse IP et cet autre port.

Imaginons maintenant que cette autre adresse IP et cet autre port soient ceux par exemple du programme SurfingTunnel dont nous avons parlé au paragraphe 1.3.3. Dans ce cas tout le trafic du navigateur Firefox local et/ou en provenance du Proxy A (sortant à son niveau du canal 9 dans notre exemple) va transiter par le canal 5 du Proxy B qui lui-même va renvoyer toutes les données vers le réseau Tor grâce à l'interface qu'offre le programme SurfingTunnel.

Dans cet exemple, nous venons de vous expliquer qu'il est possible d'atteindre le réseau Tor ou tout autre réseau interne ou externe en passant au préalable par deux Handy Proxy interconnectés. Autrement dit, le Proxy A ne doit pas obligatoirement avoir accès directement au réseau cible puisqu'il va d'abord passer par le Proxy B pour enfin atteindre sa cible.

Toujours dans notre exemple, la cible du Proxy B pourrait être un troisième Handy Proxy (Proxy C) qui permettrait alors d'atteindre Internet en 3 étapes. Toutefois, à chaque ajout de passerelle le trafic ralentit en fonction des différentes vitesses de connexion Internet de chaque Handy Proxy (il faut privilégier les connexions VDSL ou plus rapides encore). Nous suggérons de ne pas passer par plus de 3 passerelles, sans quoi le trafic risque d'être fort lent. Veuillez noter que dans notre exemple le Proxy C ne peut pas être le Proxy A puisque le Proxy A doit d'abord se connecter au Proxy B, lui-même devant se connecter au Proxy C. Ce dernier n'arrivera jamais à se connecter au Proxy A (une telle situation créerait un deadlock, or les Handy Proxy ont un système de protection anti-deadlock).

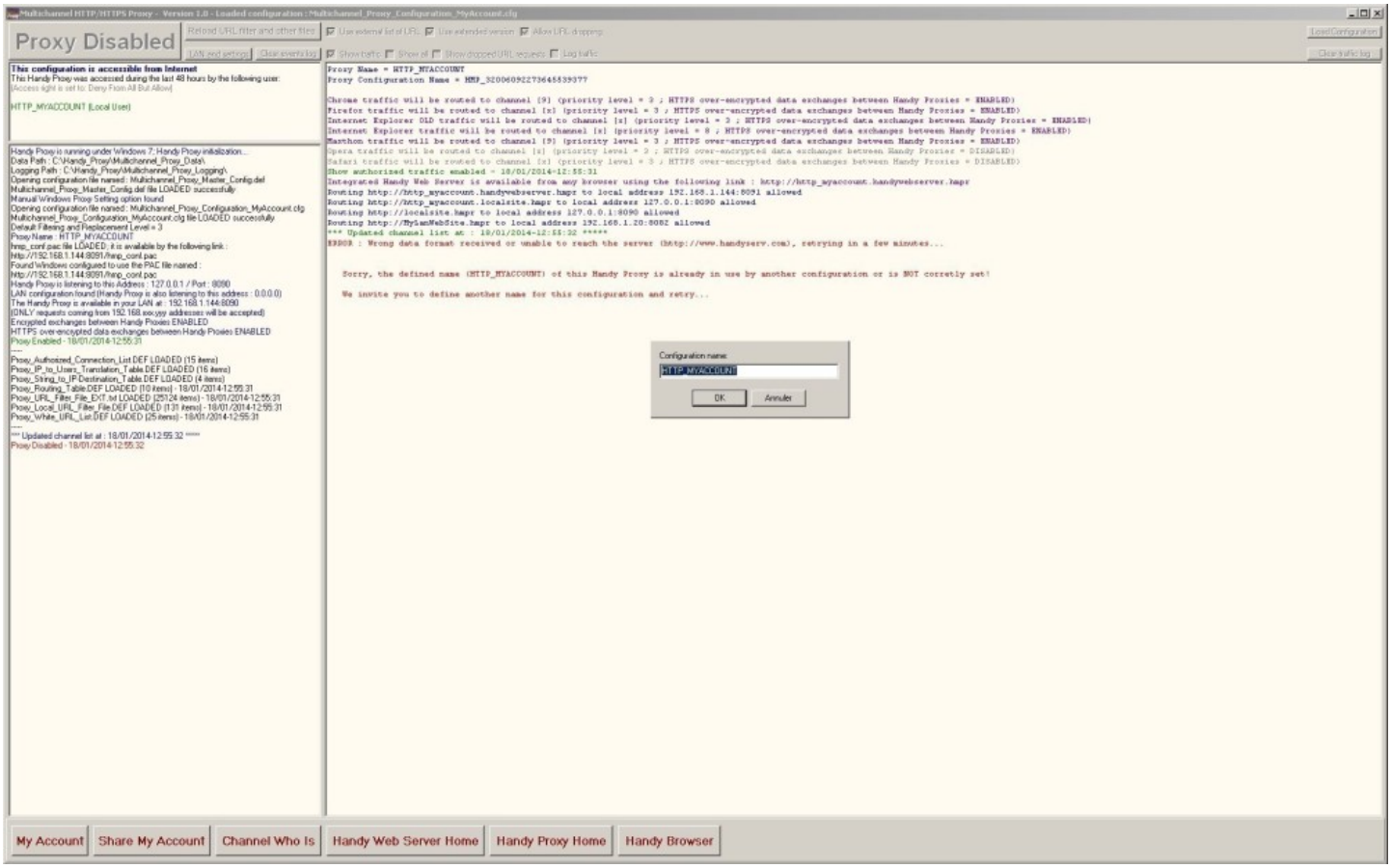
Un autre exemple très utile que vous pourriez imaginer avec 2 Handy Proxy serait de permettre de passer de n'importe où dans le monde à partir d'un Proxy A (via un accès wifi) pour atteindre un Proxy B (situé chez vous ou au bureau), le Proxy B étant par exemple paramétré pour atteindre votre Intranet via l'un des 10 canaux à disposition. A nouveau, vous pourriez faire en sorte que tout le trafic de Firefox, par exemple, passe par ces 2 proxys et atteigne au final un serveur Apache qui ne serait pas public puisqu'en Intranet. Toutes les protections d'accès des Handy Proxy sont à votre disposition pour vous garantir que seules les personnes dûment autorisées puissent atteindre la cible finale de votre configuration.

Remarque : si l'un des maillons de la chaîne construite connaissait une défaillance, ce serait toute la chaîne qui s'arrêterait ou qui pourrait devenir très lente comme dans le cas du réseau Tor où le trafic peut passer momentanément par un nœud Tor relativement lent.

Ce genre de configuration est à votre disposition pour autant que vous respectiez scrupuleusement les paramétrages de chacun des Handy Proxy mis ainsi à la chaîne l'un de l'autre. Si vos paramétrages ne sont pas cohérents entre eux, vous risquez de faire sortir le trafic du navigateur choisi par une autre voie et donc de passer à côté de la passerelle souhaitée. Pour arriver à faire fonctionner ce genre de configuration plus sophistiquée, il est impératif de bien comprendre ce que sont les adresses IP et les ports que l'on utilise sur Internet.

2. Utilisation de votre Handy Proxy

Lorsque vous aurez installé le progiciel Handy Proxy, vous obtiendrez le premier écran ci-dessous :



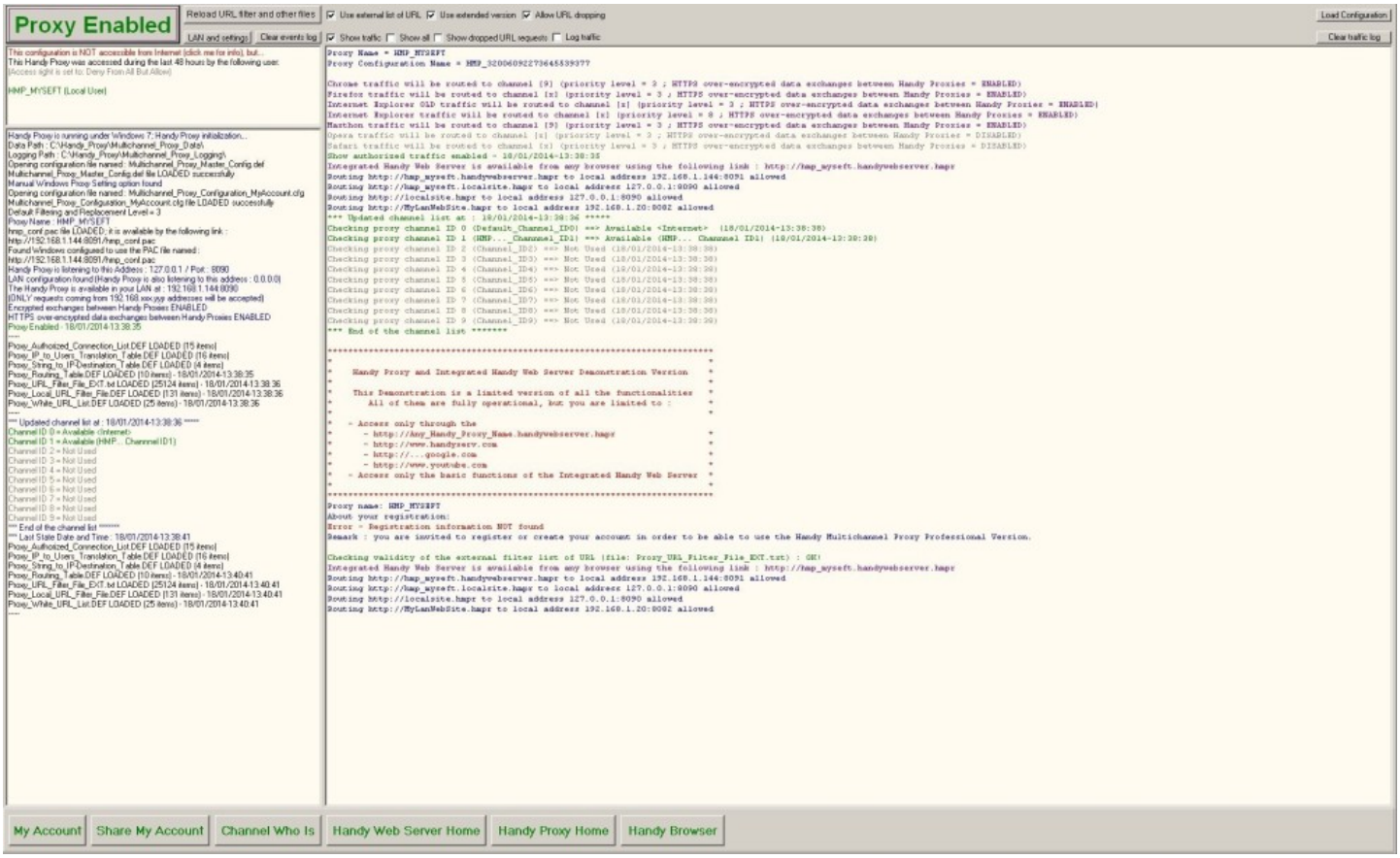
Vous devez à présent choisir un nom pour votre Handy Proxy. Ce nom doit contenir au minimum 10 caractères, avec un maximum de 50.

Pour la configuration de votre Handy Proxy, veuillez vous référer aux paragraphes suivants de ce manuel (voir chapitre 9 « Fichiers de configuration du Handy Proxy ») :

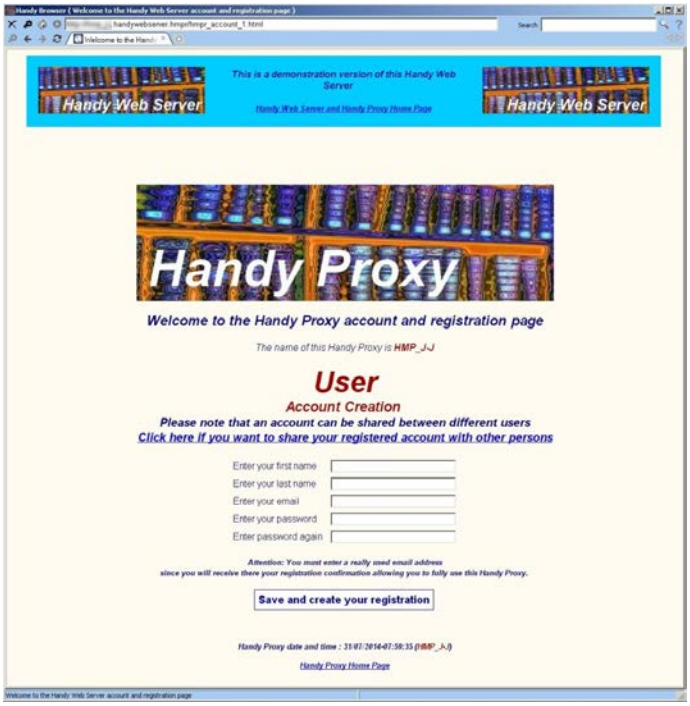
Handy Proxy Master Configuration File (Multichannel_Proxy_Master_Config.def)
Handy Proxy Configuration File (Default name : Handy_Proxy_Configuration.cfg)

Ces deux fichiers de configuration régissent l'ensemble du fonctionnement de votre Handy Proxy et de ses autres modules. Il y a aussi un ensemble de fichiers de configuration annexes (voir chapitre 9 « Fichiers de configuration du Handy Proxy »).

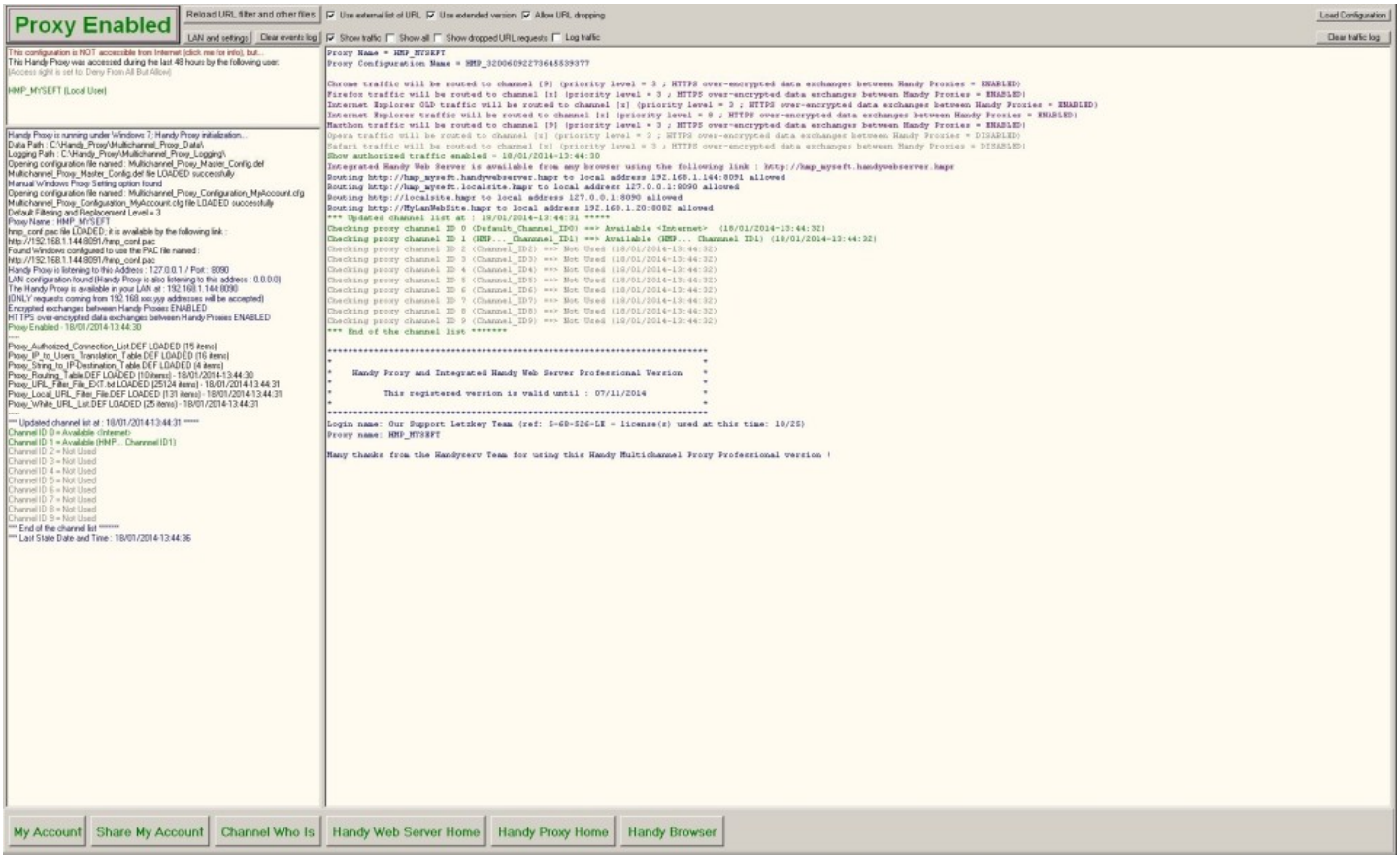
Lorsque vous aurez donné un nom à votre Handy Proxy, vous obtiendrez l'écran suivant vous indiquant cette fois que vous êtes autorisé à utiliser le Handy Proxy avec le nom donné. Toutefois, vous serez à ce stade-là (encore) en mode « démonstration ». Ce mode permet d'accéder à certains sites web comme Google ou Youtube. Tous les autres sites sont inaccessibles dans ce mode de démonstration. Ce mode vous permet donc d'évaluer les fonctions de votre Handy Proxy sans engagement de votre part.



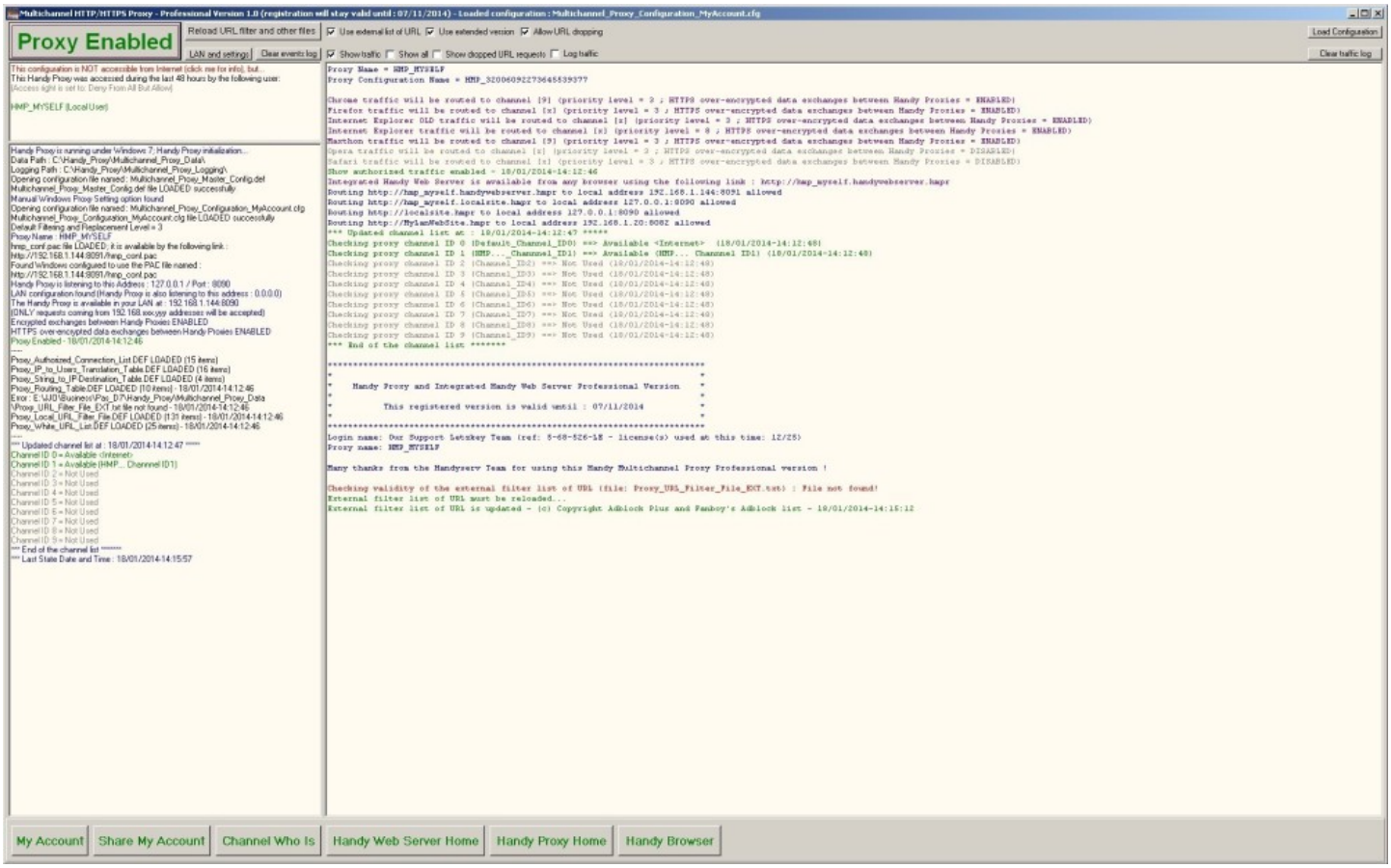
Si vous souhaitez ensuite utiliser sans limites votre Handy Proxy, cliquez sur le bouton « *My Account* » en bas à gauche de l'écran ci-dessus pour obtenir l'écran ci-dessous qui vous permettra de vous enregistrer et d'obtenir votre licence d'utilisation. Celle-ci peut être obtenue pour un seul utilisateur ou plusieurs, en fonction de vos besoins. Lors de votre inscription, vous obtiendrez un e-mail de confirmation. Vous pourrez ensuite partager votre licence avec par exemple votre famille, vos amis ou vos collègues. Voyez à ce sujet le chapitre 3 « Partager sa licence » de ce manuel. Seule la personne qui a créé et obtenu la licence pourra partager et modifier celle-ci.



Après vous être enregistré et avoir obtenu votre licence d'utilisation, voici l'écran qui apparaîtra :

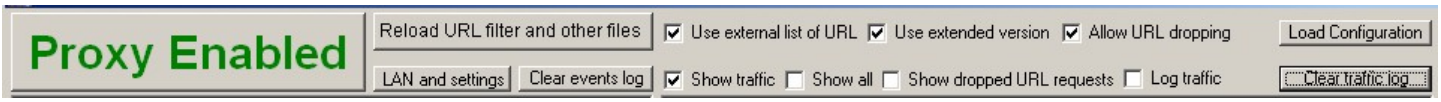


Quelques instants après le lancement de votre Handy Proxy, celui-ci va se mettre à jour notamment en téléchargeant automatiquement la liste des liens par défaut que le Handy Proxy devra filtrer. A ceux-ci s'ajouteront vos propres filtres (voir à ce sujet le paragraphe 9.6 « Fichier Handy Proxy Proxy_Local_URL_Filter_File.DEF »).



Explication des différentes parties de l'écran du Handy Proxy :

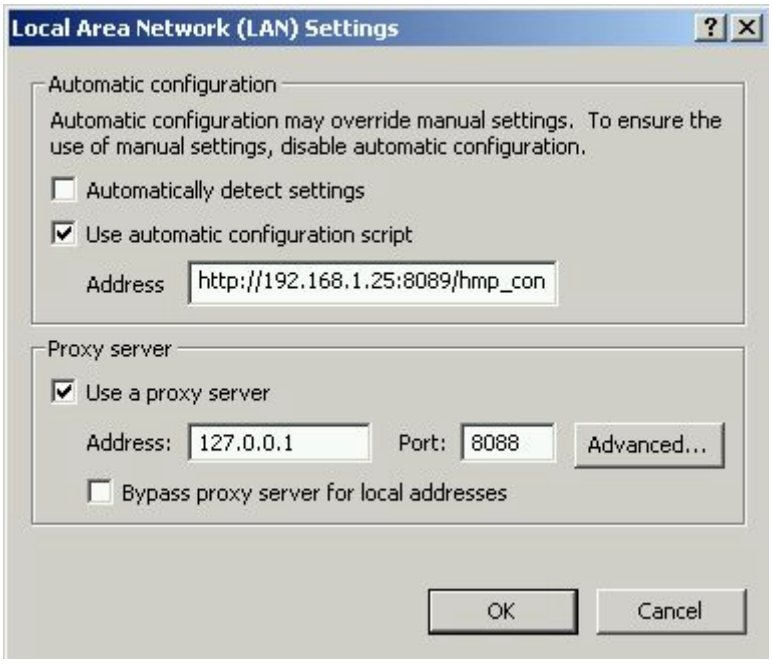
Options et boutons principaux de votre Handy Proxy :



- **Bouton « *Proxy Enabled* »** : ce bouton sert à autoriser ou bloquer tout le trafic qui traversera votre Handy Proxy. Vous pouvez grâce à ce bouton empêcher tout échange entre votre navigateur et les sites web qui seraient ouverts dans celui-ci. Il existe la possibilité de rendre le Handy Proxy « transparent » pour certains sites. Voir à ce sujet le paragraphe 9.3 « Fichier Handy Proxy hmp_conf.pac ». Vous pouvez gérer site par site l'autorisation d'accès/priorité qui lui sera donnée. Voir à ce sujet le paragraphe 9.9 « Fichier Handy Proxy Proxy_White_URL_List.DEF ». Il est également possible de définir, pour un site donné, le canal du Handy Proxy qui va « router » le trafic entre votre navigateur et le site en question. Voir à ce sujet le paragraphe 9.7 « Fichier Handy Proxy Proxy_Routing_Table.DEF ».

- **Bouton « *Reload URL filter and other files* »** : ce bouton sert à recharger tous les fichiers de configuration mentionnés ci-dessus, à l'exception du fichier hmp_conf.pac qui est utilisé par les navigateurs en temps réel.

- **Bouton « *LAN and settings* »** : ce bouton sert à ouvrir le menu Windows (paramètres réseau) permettant de définir l'accès à Internet via le Handy Proxy pour votre navigateur. L'idéal est d'utiliser le fichier hmp_conf.pac qui est configuré automatiquement par le Handy Proxy. Voir zone « Utiliser un script de configuration automatique » qu'il faut cocher, et indiquer le chemin d'accès par exemple comme suit : http:\\192.168.1.x:80xx/hmp_conf.pac. Ce chemin vous est indiqué dans l'écran de votre Handy Proxy, voir zone « **hmp_conf.pac file LOADED** ». Veuillez noter que le nom hmp_conf.pac NE peut PAS être modifié et que le port à utiliser est celui de votre **Handy Proxy + 1**.



En plus de cela ou en alternative, vous pouvez aussi définir manuellement dans cette fonction à quelle adresse et quel port se trouve le Handy Proxy que votre navigateur va devoir utiliser. Voir à ce sujet la zone « Utiliser un serveur Proxy pour votre réseau local » que vous devez cocher et ensuite, dans la zone adresse et la zone port, encodez les informations comme indiqué dans l'écran de votre Handy Proxy. Voir zone « ***The Handy Proxy is available in your LAN at*** …». Veuillez noter que votre Handy Proxy peut paramétrer cette zone automatiquement à son démarrage en fonction du paramètre « Automatic_Windows_Proxy_Setting ». Voir paragraphe 9.1, fichier « Handy Proxy Master Configuration (Multichannel_Proxy_Master_Config.def) ».

Zone d'événements de fonctionnement du Handy Proxy :

- **Boutons « *Clear events log* » et « *Clear traffic log* »** : ces boutons permettent d'effacer les zones respectives de l'écran du Handy Proxy.

- **Zone à cocher « *Use external list of URL* »** : cette option permet de demander ou non au Handy Proxy de filtrer les sites ou liens repris dans la liste téléchargée automatiquement. Celle-ci est mise à jour toutes les 24h.

- **Zone à cocher « *Use extended version* »** : il existe deux listes de sites ou liens à filtrer, une simplifiée et une étendue. Vous pouvez choisir celle qui vous convient le mieux.

- **Zone à cocher « *Allow URL dropping* »** : cette option permet d'autoriser ou non le Handy Proxy à filtrer les sites définis dans les différents fichiers de configuration mentionnés plus haut.

- **Zone à cocher « *Show traffic* »** : cette option permet de lister les échanges entre votre navigateur et les sites web. Si vous n'avez pas besoin de celle-ci, nous vous conseillons de la décocher mais vous ne pourrez alors plus cliquer sur un lien listé pour le filtrer (ou le réautoriser). Voir les explications à ce sujet plus bas dans le présent manuel.
  Si votre Handy Proxy est un « nœud de trafic » pour d'autres utilisateurs de Handy Proxy, la mise à l'écran d'un événement est différente. Celle-ci ne contiendra pas le lien demandé par un autre utilisateur, par souci de confidentialité. Cet événement contiendra qui a demandé un lien, à quelle heure, et quelle référence d'encryption des échanges est choisie à l'instant *T* entre votre Handy Proxy et celui de votre correspondant qui s'est connecté au préalable. Pour rappel, le mode d'encryption entre deux Handy Proxy change automatiquement toutes les 4 heures et entièrement toutes les 24 heures.

- **Zone à cocher « *Show all* »** : cette option permet de lister tous les échanges en fonction de leur priorité.

- **Zone à cocher « *Show dropped URL requests* »** : cette option permet de lister le trafic vers des sites filtrés afin de les réautoriser le cas échéant.

- **Zone à cocher « *Log traffic* »** : cette fonction permet de sauver sur disque tous les échanges listés en fonction des options précédentes. Cette sauvegarde se fait dans la sous-directory ..\MULTICHANNEL_PROXY_LOGGING. Cette fonction n'est à utiliser que si absolument nécessaire, parce que l'écriture sur disque se fait à chaque fois qu'un lien

est demandé par votre navigateur. Ceci inclut, pour une page, à la fois une écriture sur disque pour le lien vers la page mais aussi tout ce qu'elle contient et qui doit être affiché dans la page. Vous pouvez ainsi obtenir, pour une seule page, 10 écritures sur disque s'il y avait par exemple 9 images. Ceci ralentira bien entendu le fonctionnement de votre Handy Proxy.

- **Bouton « *Load configuration* »** : ce bouton permet de reconfigurer votre Handy Proxy si vous avez besoin de faire appel à plusieurs modes d'utilisation ou de vous connecter à différents autres Handy Proxy. Attention : le fichier de configuration « maître » n'est chargé qu'une seule fois au lancement de votre Handy Proxy. En revanche, vous pouvez recharger les sous-fichiers de configuration. Voir à ce sujet le paragraphe 9.2 « Fichier Handy Proxy Configuration (Default name : Handy_Proxy_Configuration.cfg) ». Vous pouvez créer autant de sous-fichiers de configuration que vous le souhaitez avec l'extension .cfg et les utiliser à votre guise pour autant que vous respectiez scrupuleusement la syntaxe nécessaire à ce fichier.

Voici ci-dessous un exemple de lancement de votre Handy Proxy avec un fichier .cfg donné :
Vous pouvez donc définir par exemple quel canal du Handy Proxy sera utilisé par un navigateur donné.

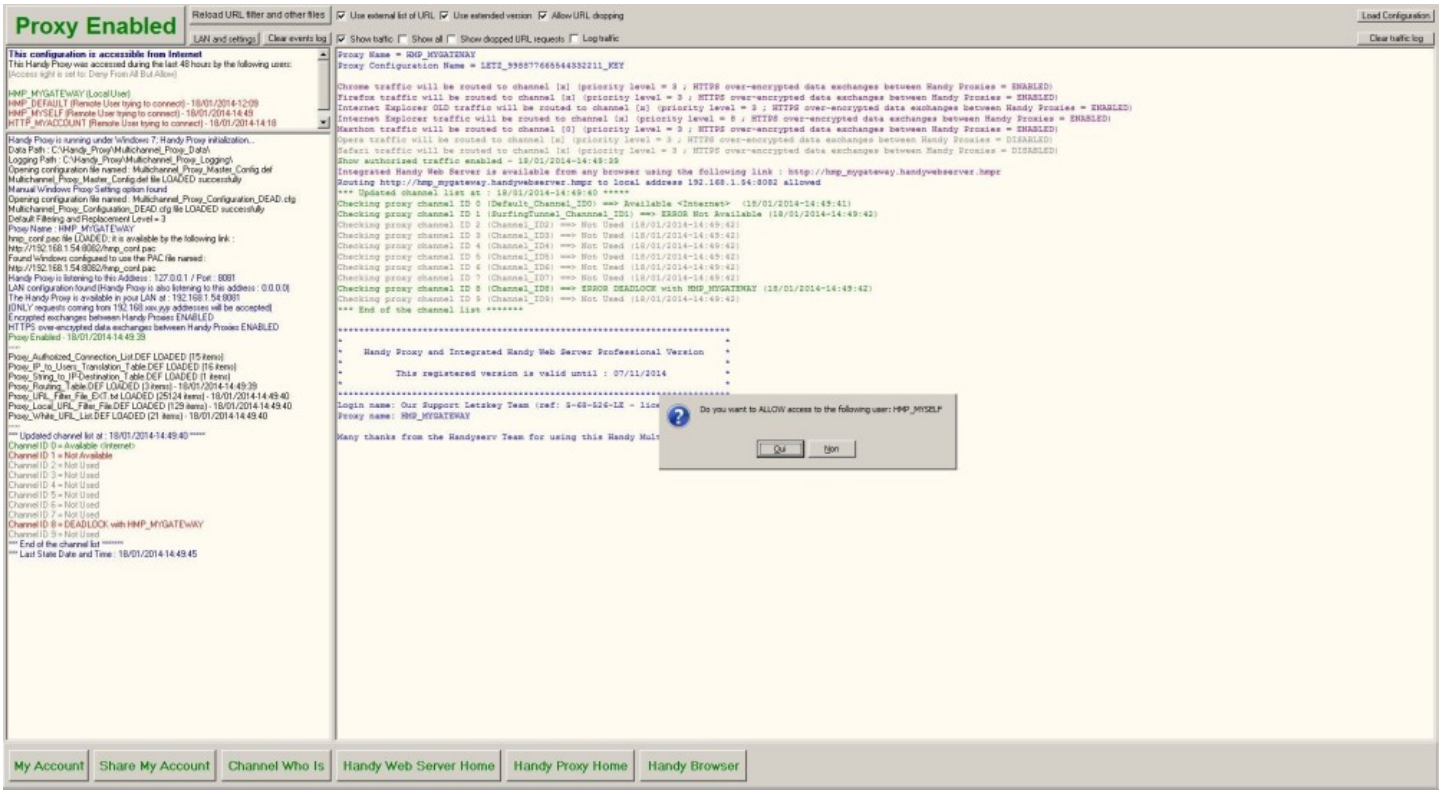
Zone des canaux du Handy Proxy connectés au monde extérieur :

Cette zone vous indique comment et vers qui sont connectés les 10 canaux de votre Handy Proxy. Par défaut et automatiquement, le canal 0 est toujours connecté vers Internet via votre routeur. Tous les autres canaux (de 1 à 9) peuvent être connectés vers une adresse et un port prédéfinis ou vers un autre utilisateur d'un Handy Proxy. Dans ces cas, plusieurs messages affichés dans cette zone sont possibles :

- Les messages écrits en vert indiquent que la connexion est opérationnelle.
- Les messages écrits en rouge indiquent toujours une erreur : soit la destination choisie n'existe pas ou n'est pas disponible, soit vous avez routé un canal vers votre propre Handy Proxy (cas du *deadlock*, càd « boucle sans fin »), soit le message indique « *Access denied* » ce qui signifie que la destination existe, qu'elle est disponible, mais que vous n'y avez pas accès. Vous devez donc demander à cette destination de vous autoriser à accéder son Handy Proxy. Voir les explications ci-après.

Dans l'écran suivant, on voit en haut à gauche que le Handy Proxy est disponible sur Internet pour d'autres utilisateurs (« This configuration is accessible from Internet ») (voir plus bas comment procéder).

Lorsqu'un utilisateur veut se connecter à votre Handy Proxy qui devient alors un routeur, cet utilisateur doit être autorisé. Voici comment faire :



Tout d'abord, l'utilisateur voulant se connecter à votre Handy Proxy (qui deviendra routeur pour cet utilisateur) apparaît dans la liste représentée ci-dessous. Cliquez sur l'utilisateur en question. Dans notre exemple, nous cliquons sur l'utilisateur « HMP_MYSELF ».

Lorsque vous aurez cliqué sur l'utilisateur que vous voulez autoriser, la fenêtre de confirmation ci-dessous apparaîtra.

Si vous confirmez, l'utilisateur sélectionné sera automatiquement ajouté à ceux autorisés à accéder, comme on le voit ci-dessous. Dans cette liste, « *Local User* » indique que le Handy Proxy est autorisé lui-même à accéder à Internet.

Pour autoriser un utilisateur à se servir de votre Handy Proxy comme routeur entre lui et Internet, vous pouvez, soit procéder comme nous venons de le voir au cas par cas, soit définir un ensemble d'utilisateurs via le fichier de configuration suivant : fichier Handy Proxy Proxy_Authorized_Connection_List.DEF (voir paragraphe 9.4). Dans ce fichier de configuration existe une fonction permettant d'autoriser n'importe quel utilisateur à se servir de votre Handy Proxy comme routeur. Attention, cette option est évidemment à utiliser avec précaution. Il vaut mieux définir les utilisateurs un à un.

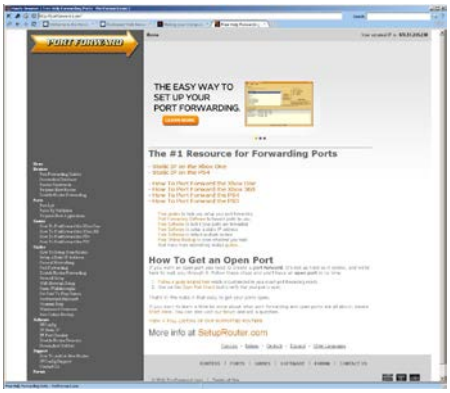
2.1. Comment donner accès à votre Handy Proxy à d'autres utilisateurs

Outre ce qui est expliqué ci-avant pour autoriser les utilisateurs distants à accéder à votre Handy Proxy, il est nécessaire que celui-ci soit accessible depuis Internet. Pour cela, il faut configurer votre routeur et plus particulièrement la fonction NAT. Chaque routeur étant différent puisqu'il existe un grand nombre de fournisseurs possibles, il nous est impossible d'expliquer dans le présent manuel comment procéder pour chacun d'eux. Nous vous mettons ici à disposition trois sites où les explications sont exhaustives. Le premier vous donnera une vue d'ensemble avec une vidéo d'explication, le second vous permettra de retrouver quel routeur vous utilisez et donc la méthode à suivre pour modifier la table NAT qui devra pointer vers votre Handy Proxy (adresse et port retrouvés via l'écran principal du Handy Proxy). Le troisième site est également très utile pour la définition de la table NAT de votre routeur.

Ce n'est pas très compliqué à réaliser, et cette méthode est très généralement utilisée.

Veuillez noter qu'aucun des utilisateurs connectés à votre Handy Proxy ne connaîtra l'adresse et le port de votre Handy Proxy ainsi que l'adresse Internet qui vous est octroyée si vous êtes configuré en adresse IP dynamique (idem si vous utilisez une adresse IP fixe). A ce sujet, le Handy Proxy contient une fonction permettant la mise à jour de l'adresse IP dynamique que vous utilisez, ceci afin de permettre aux personnes connectées de pouvoir travailler en mode transparent. Remarque : lorsque votre adresse IP dynamique est changée par votre provider Internet, votre Handy Proxy s'en rendra compte dans un délai très court et la mise à jour se fera alors instantanément de telle manière que votre Handy Proxy soit indisponible pendant le délai le plus court possible (quelques secondes en général).

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



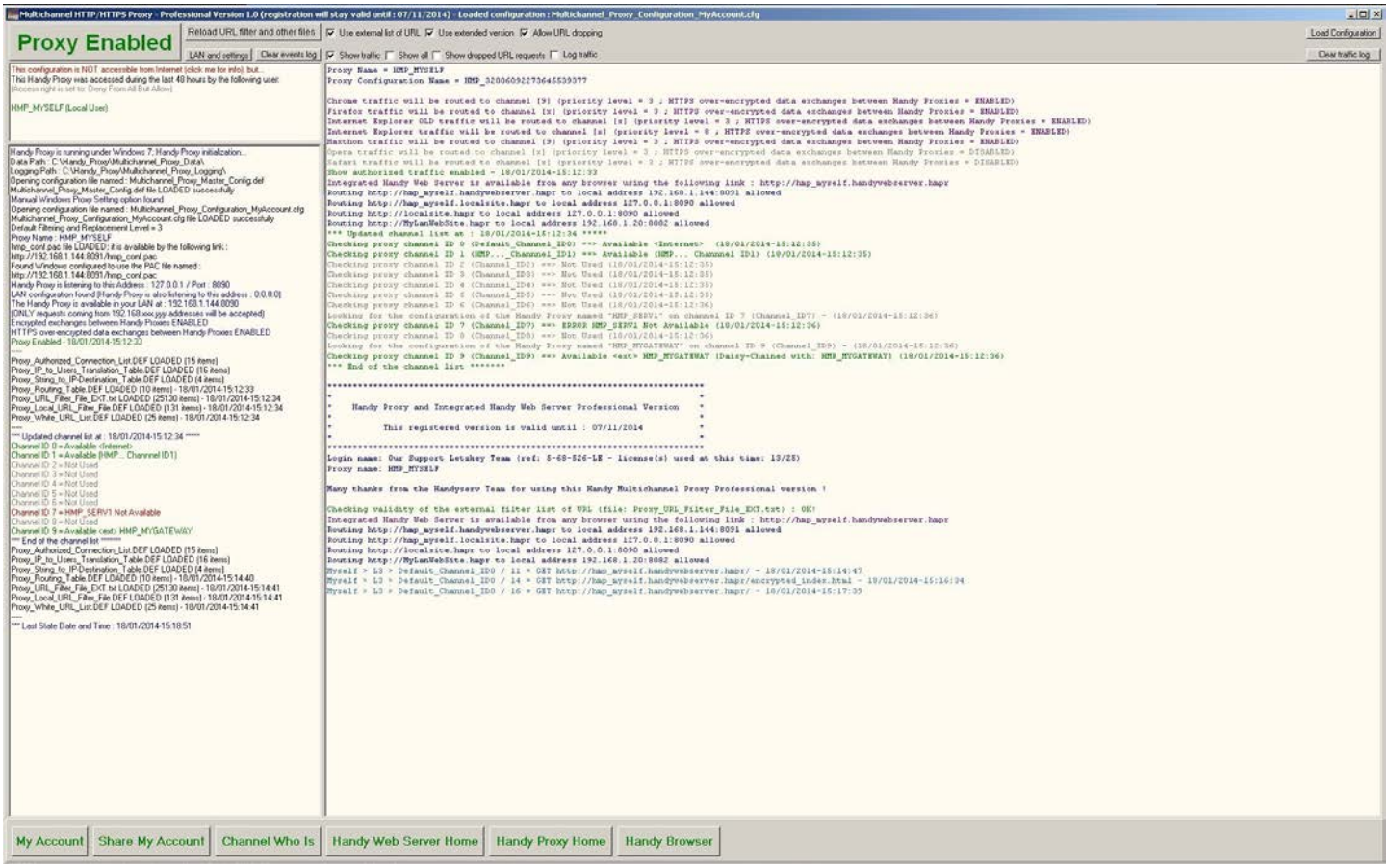
http://portforward.com

http://setuprouter.com

Remarque importante pour certains routeurs : certains routeurs de votre réseau local vers Internet ne permettent pas à un PC de votre réseau local d'envoyer des données vers un site Internet qui pointerait sur votre propre réseau. Imaginons par exemple que votre PC sur lequel vous faites fonctionner votre Handy Proxy (nom : HMP-1) ait l'adresse locale 192.168.1.25 et que vous souhaitiez utiliser les fonctionnalités d'un autre Handy Proxy sur votre même réseau qui serait configuré en tant que routeur à l'adresse 192.168.1.50 (port 8085, nom HMP-2). En paramétrant HMP-1 pour qu'il route les échanges avec HMP-2, vous risqueriez alors, si votre routeur est dans le cas expliqué ici, de ne pas pouvoir vous connecter de HMP-1 vers HMP-2. Bien évidemment, ceci n'a de sens dans un réseau local que dans l'éventualité où l'on souhaite tester des fonctionnalités. En effet il ne sert à rien, dans un réseau local, de passer par Internet pour revenir vers un autre PC de votre propre réseau. Si votre routeur est dans le cas expliqué, il est malgré tout possible de vous connecter de HMP-1 à HMP-2, mais en utilisant le paramétrage de HMP-1 en indiquant pour le canal choisi l'adresse IP de HMP-2 et non pas son nom (voir les paramètres de votre Handy Proxy). Ce qui précède concerne aussi le cas où vous aimeriez rendre disponibles les fonctions de votre Handy Web Server et Handy Messaging Server de votre HMP-2 pour votre propre réseau et pour les utilisateurs extérieurs.
En résumé, les utilisateurs internes de votre réseau local devront paramétrer leur Handy Proxy pour pointer vers le Handy Proxy en mode routeur et en mode Web Server/Messaging Server via l'adresse physique de ce PC dans votre réseau, par exemple 192.168.1.50 (port 8085). En revanche, les utilsateurs externes de votre LAN et de votre Handy Proxy en mode routeur (et en mode Web Server/Messaging Server) devront indiquer qu'ils souhaitent se connecter vers le nom de ce Handy Proxy (dans cet exemple : HMP-2).
En pratique, pour les personnes qui devraient utiliser les services d'un de vos Handy Proxy en mode routeur à la fois en interne et en externe de votre réseau local, il est suggéré de créer deux fichiers de configuration à utiliser en fonction du cas d'utilisation (interne ou externe).

2.2. Comment autoriser ou non l'accès à un lien web

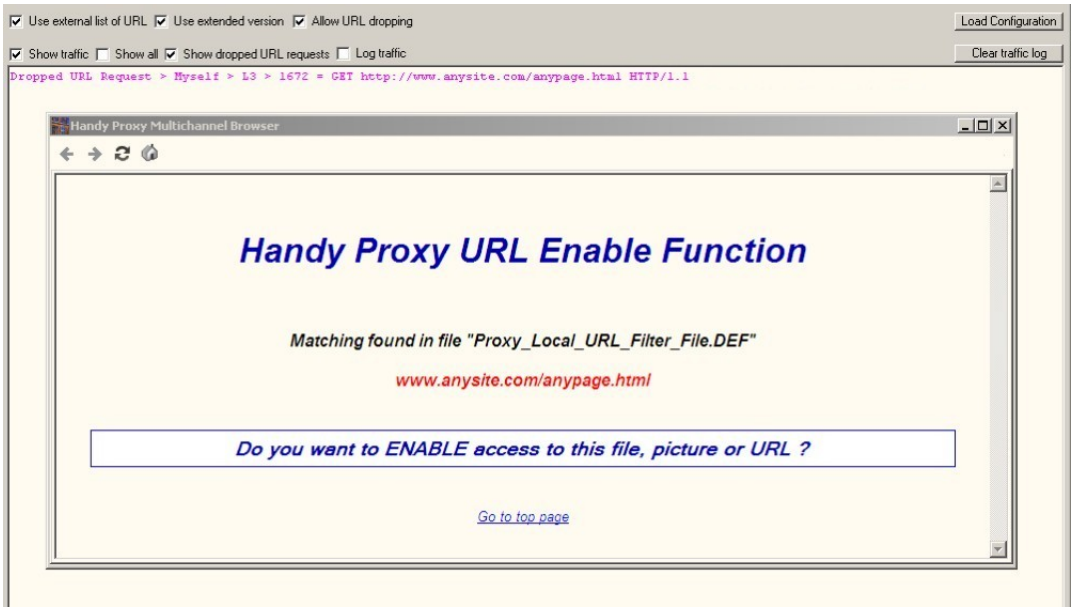
Lorsque vous utiliserez votre Handy Proxy et lorsque vous aurez autorisé l'affichage du trafic, tous les liens des pages HTML, PHP, etc. seront listés. Si l'un de ces liens ne vous convient pas ou ne vous est pas utile, vous pouvez le rendre inaccessible afin de diminuer votre trafic et augmenter ainsi vos performances d'accès Internet. Pour cela, il suffit de cliquer dessus.



Voici l'écran qui apparaîtra si vous cliquez sur le lien « http://www.anysite.com/anypage.html » dans notre exemple.

Dans cette fenêtre, vous pouvez dérouler la liste qui vous permettra de choisir quel degré d'autorisation vous allez retirer à la page, au lien ou à tout le site en question. Soyez très prudent en utilisant cette fonction, parce qu'elle permet de bloquer jusqu'à tous les sites qui se termineraient par « .com », par exemple. Cela peut avoir du sens au cas où vous

aimeriez justement bloquer tous les sites d'un type ou d'une extension donnée. Nous déconseillons cependant de le faire et d'agir plutôt au cas par cas. En général, il est préférable de ne pas autoriser une page donnée, voire un site complet. Lorsqu'une page ou un site a été rendu inaccessible, il est alors possible de le réautoriser. Pour cela, vous devez d'abord cocher l'option « *Show dropped URL requests* » du menu principal et demander à votre navigateur d'ouvrir la page ou le site en question. Ensuite, sur l'écran de votre Handy Proxy, il faut cliquer sur le lien en question. L'écran suivant apparaît alors. Vous n'avez plus qu'à confirmer la réautorisation. Veuillez noter que vous pouvez aussi utiliser le fichier Proxy_Authorized_Connection_List.DEF qui reprend l'ensemble de vos liens, pages et sites filtrés.

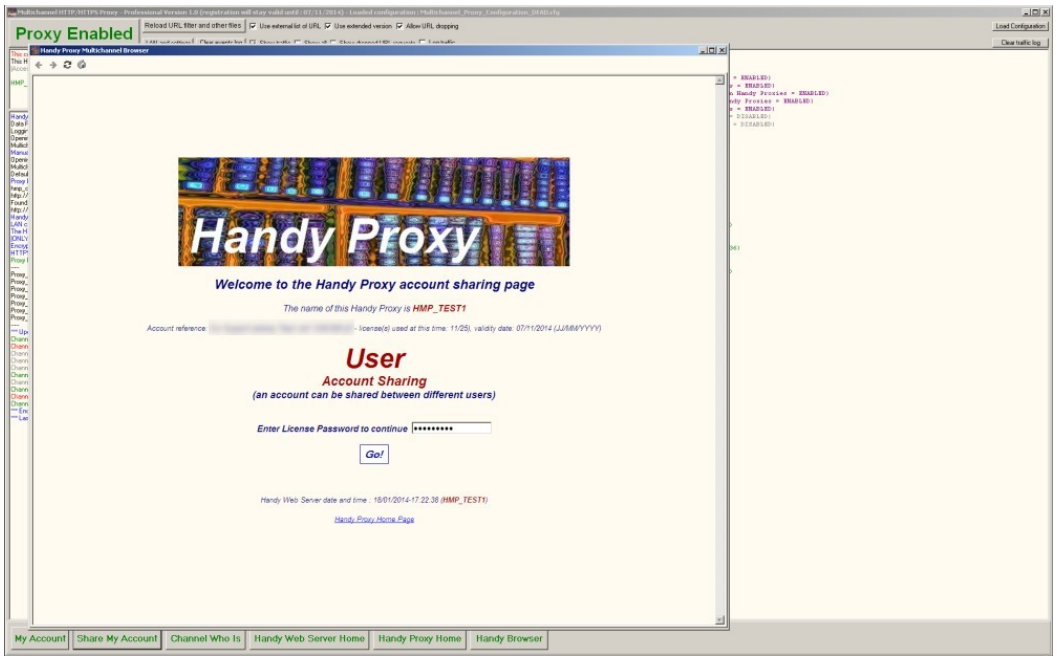


3. Partager sa licence

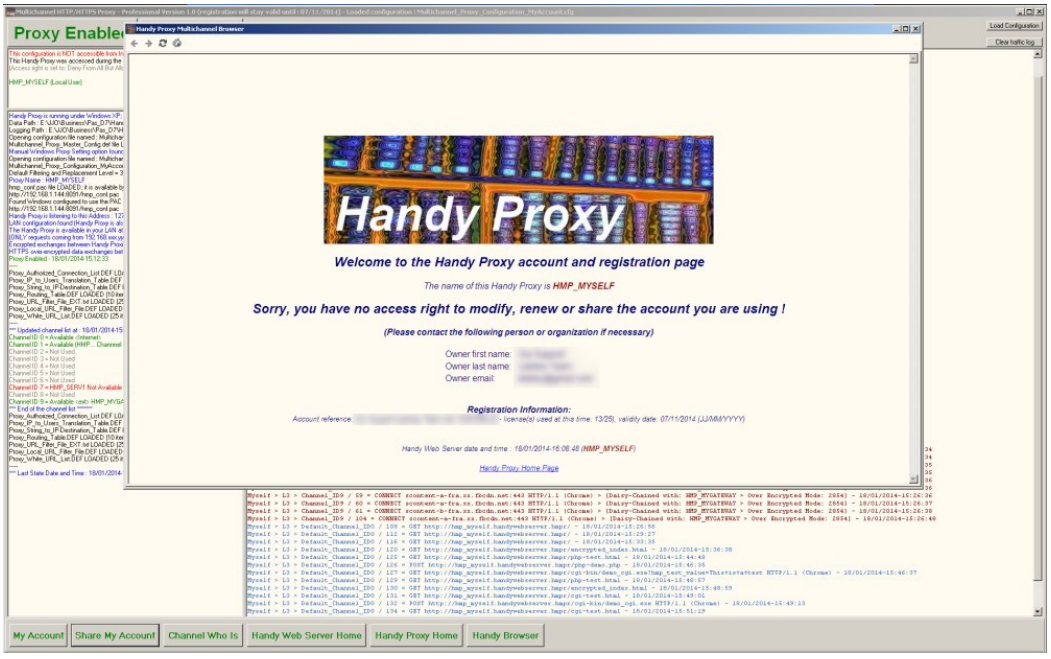
Lorsque vous êtes un utilisateur enregistré, vous pouvez partager votre licence avec d'autres personnes de votre choix en fonction du type de licence dont vous disposez. Seul le propriétaire de la licence peut la partager. Toutes les autres personnes qui utiliseraient votre licence ne pourront jamais partager votre licence avec d'autres personnes.

Lorsque vous vous enregistrez, vous devez donc bien définir vos besoins en termes de nombre de Handy Proxy que vous allez utiliser avec votre famille, vos amis ou dans votre entreprise. Prévoyez à cet effet quelques licences de plus, vous permettant d'avoir un peu de marge et de ne pas être limité trop rapidement. Par exemple, si vous êtes 5 personnes dans votre famille à vouloir utiliser Handy Proxy sur 5 PC différents, nous vous conseillons d'utiliser la licence supérieure (par exemple 10 utilisateurs).

Pour partager votre licence, cliquez sur le bouton « *Share My Account* » qui se trouve dans le menu du bas de votre Handy Proxy. Vous obtiendrez alors l'écran suivant, dans lequel il vous est demandé d'introduire votre mot de passe (voir les paramètres standards dans les fichiers de configuration de votre Handy Proxy) :



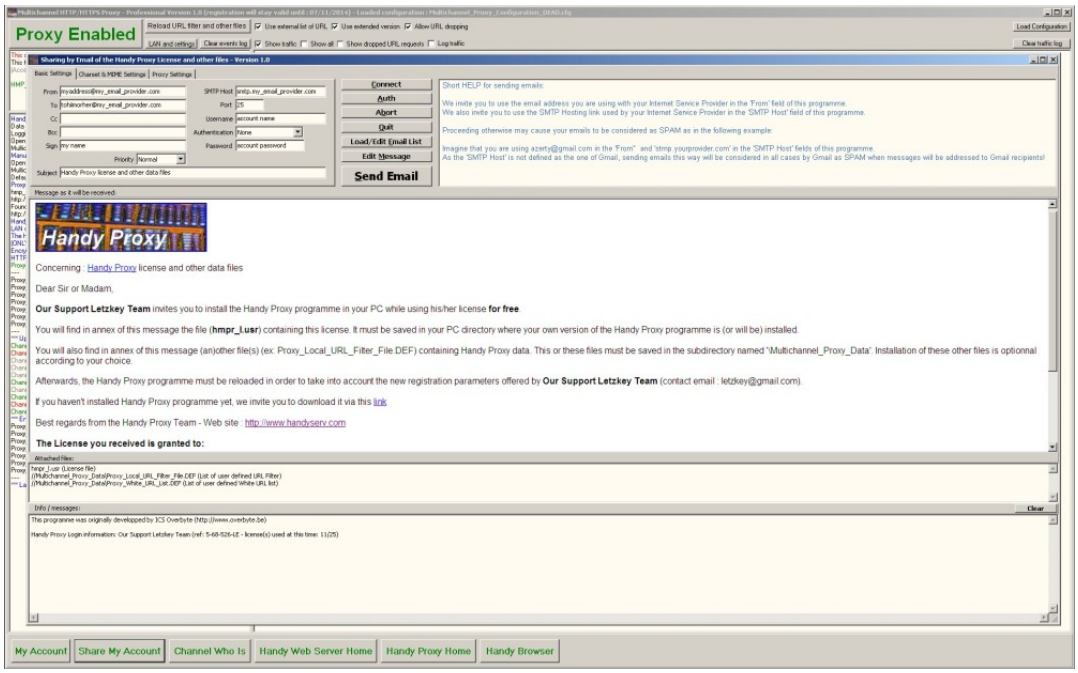
L'écran suivant apparaîtra si vous n'êtes pas le propriétaire de la licence que vous utilisez :



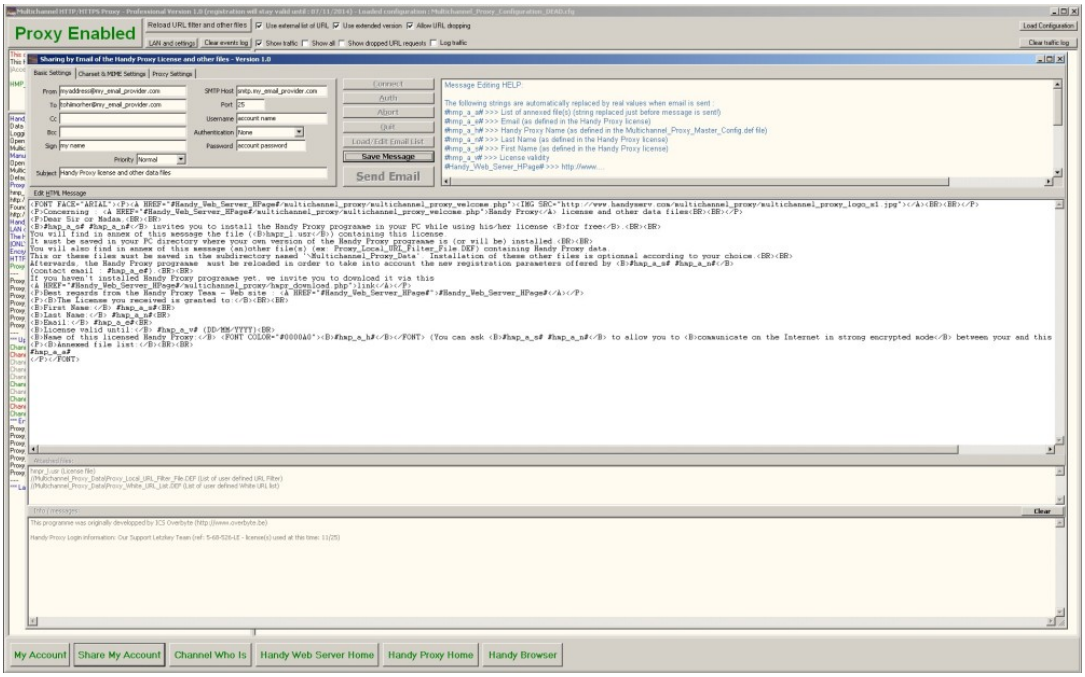
Si vous êtes le propriétaire de la licence, l'écran suivant apparaîtra. Ce module est un générateur d'e-mails dans lequel vous pouvez personnaliser le message qui sera envoyé aux correspondants repris dans la(les) liste(s) de diffusion.

Ce générateur d'e-mails est dédicacé à la diffusion de la licence et éventuellement d'autres fichiers de votre Handy Proxy. La syntaxe du message doit contenir certaines informations indispensables, sans quoi le message sera refusé.

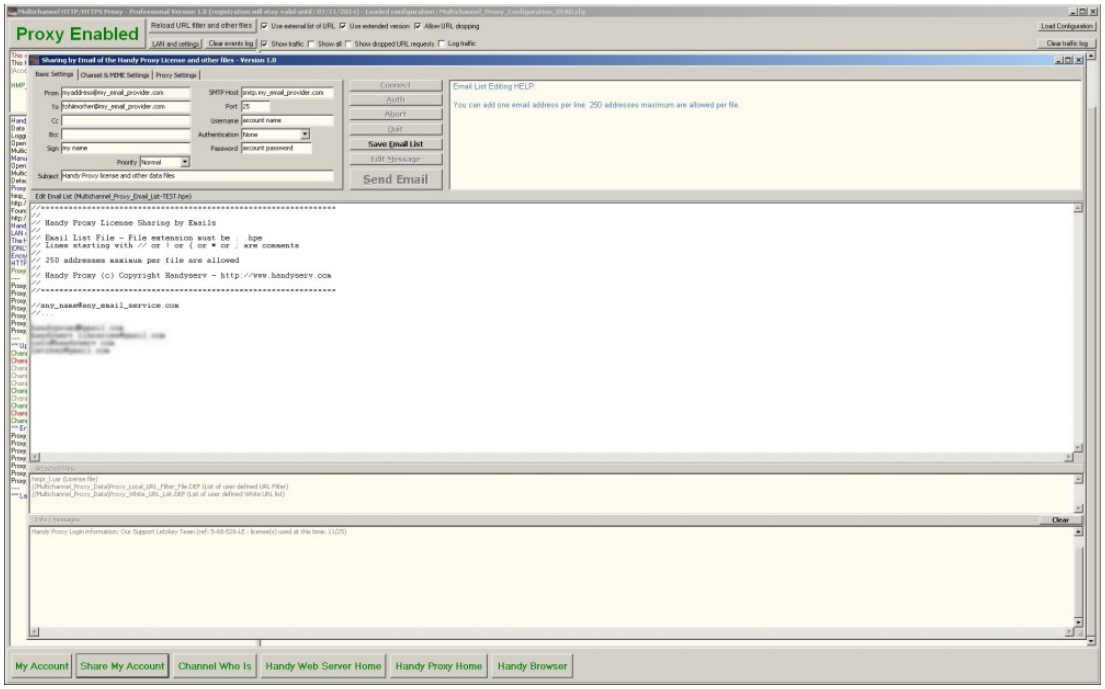
Le corps du message peut contenir certains mots-clés comme repris dans l'aide intégrée à ce module. Ces mots-clés seront remplacés dynamiquement par le programme en fonction des paramètres de votre Handy Proxy. **Il faut impérativement respecter scrupuleusement la syntaxe de ces mots-clés**, sans quoi vous n'obtiendrez pas le résultat escompté.



Ce programme intègre un éditeur de texte vous permettant de modifier le corps du message qui va être envoyé aux personnes de votre choix.



Dans ce programme, vous pouvez encoder les adresses e-mail de vos correspondants et les sauvegarder dans différents fichiers, chacun pouvant contenir maximum 250 adresses.



Vers le milieu de l'écran de ce module, vous pouvez joindre à la licence envoyée à vos correspondants d'autres fichiers de votre Handy Proxy, comme par exemple votre fichier de filtres d'adresses de sites et de liens.

Ce module utilise les services de votre provider Internet pour envoyer les e-mails. Il faut donc paramétrer ce module en fonction de votre provider, et plus particulièrement la zone « *SMTP Host* » dans laquelle vous devez encoder le lien vers le serveur SMTP de votre provider Internet. Consultez la documentation de celui-ci pour identifier quel est ce serveur. Vous devez également personnaliser la zone « *From* », sans quoi les messages ne partiront pas.

La zone « *To* » permet d'envoyer un seul message à la fois, sans passer par une liste de diffusion.

Il existe d'autres paramètres dans les autres onglets, mais en principe vous ne devrez pas y toucher, ceux-ci étant positionnés en mode standard.

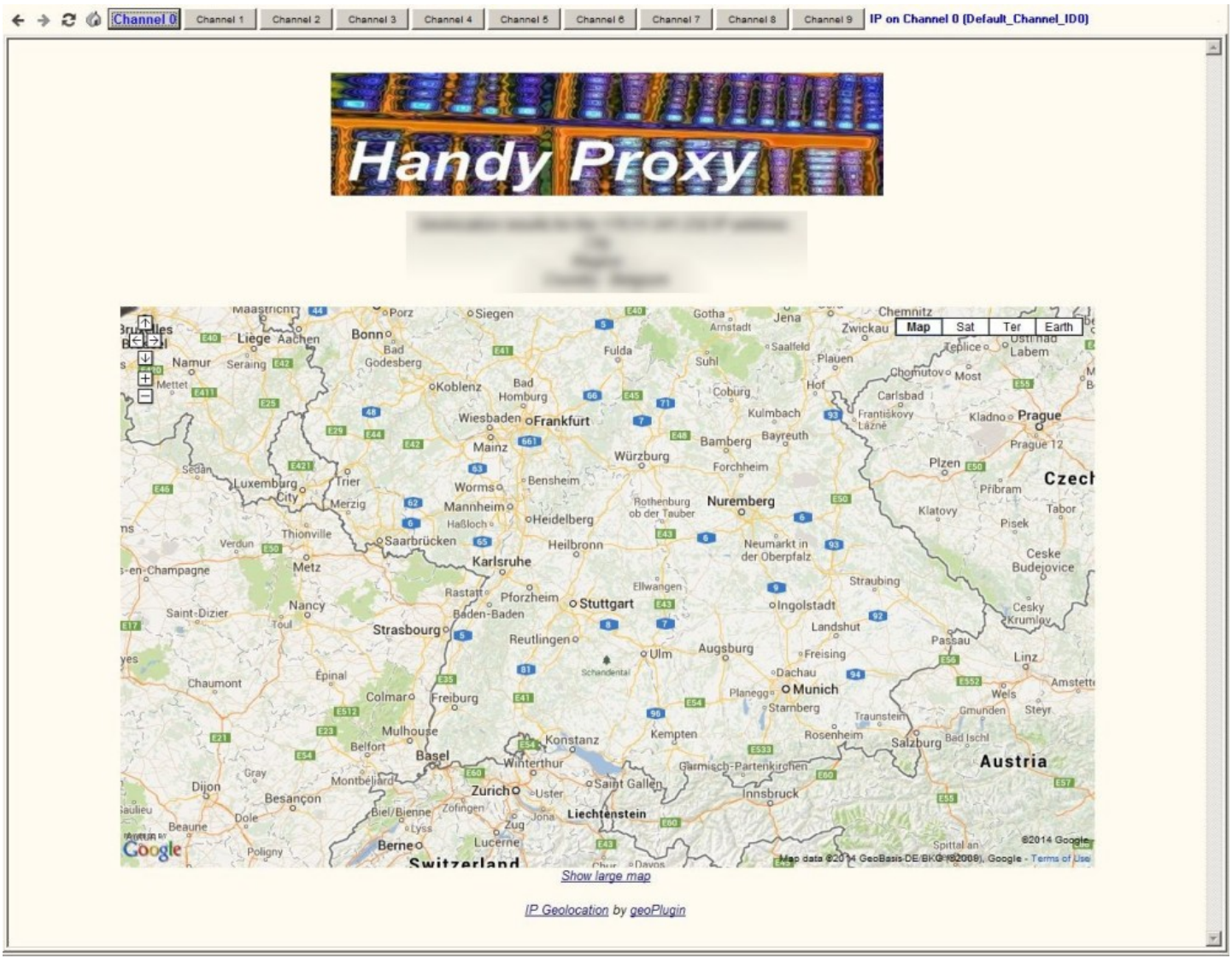
Remarque importante : il est strictement interdit d'utiliser ce module à d'autres fins que la diffusion de la licence de votre Handy Proxy. Toute utilisation non conforme pourra amener à la résiliation immédiate et sans avis préalable de votre licence.

4. Quel est le point de sortie d'un canal (bouton « *Channel Who Is* »)

Si vous utilisez différents canaux de votre Handy Proxy, que ce soit pour accéder à un autre Handy Proxy distant ou n'importe quel autre nœud de routage (proxy), il est intéressant de savoir à partir d'où vos accès à des pages Internet vont se faire. Vous avez pour cela la fonction « *Channel Who Is* » qui est accessible à partir du bouton du même nom.

Lorsque l'écran ci-après apparaîtra, choisissez le canal qui vous intéresse (en cliquant sur le bouton adéquat). Votre Handy Proxy va alors envoyer une requête de reconnaissance de l'adresse IP publique qui sera obtenue par le canal sélectionné. Par exemple, si le canal 9 de votre Handy Proxy pointe vers un autre Handy Proxy aux Etats-Unis, l'adresse IP publique qui en reviendra sera une adresse américaine. Sur la base de cette information, une géolocalisation sera effectuée et une carte Google Maps (c) correctement positionnée par rapport à l'adresse IP apparaîtra à l'écran. Ceci vous permettra de savoir à partir d'où vous entrez sur le réseau Internet en réalité.

Pour rappel, tous les échanges entre 2 Handy Proxy sont encryptés, ce qui veut dire que vos échanges à partir de l'endroit où vous êtes n'apparaîtront jamais en clair, jusqu'au point où se trouve l'autre Handy Proxy avec lequel vous correspondez et qui vous permettra quant à lui de fonctionner en mode non crypté sur Internet.



5. Handy Web Server avec option de pages encryptées

Votre Handy Proxy intègre en standard un module complémentaire qui est un serveur web complet : le Handy Web Server. Celui-ci permet d'héberger des pages HTML, des Javascripts, des images (JPG, GIF, PNG) ainsi que des pages PHP.

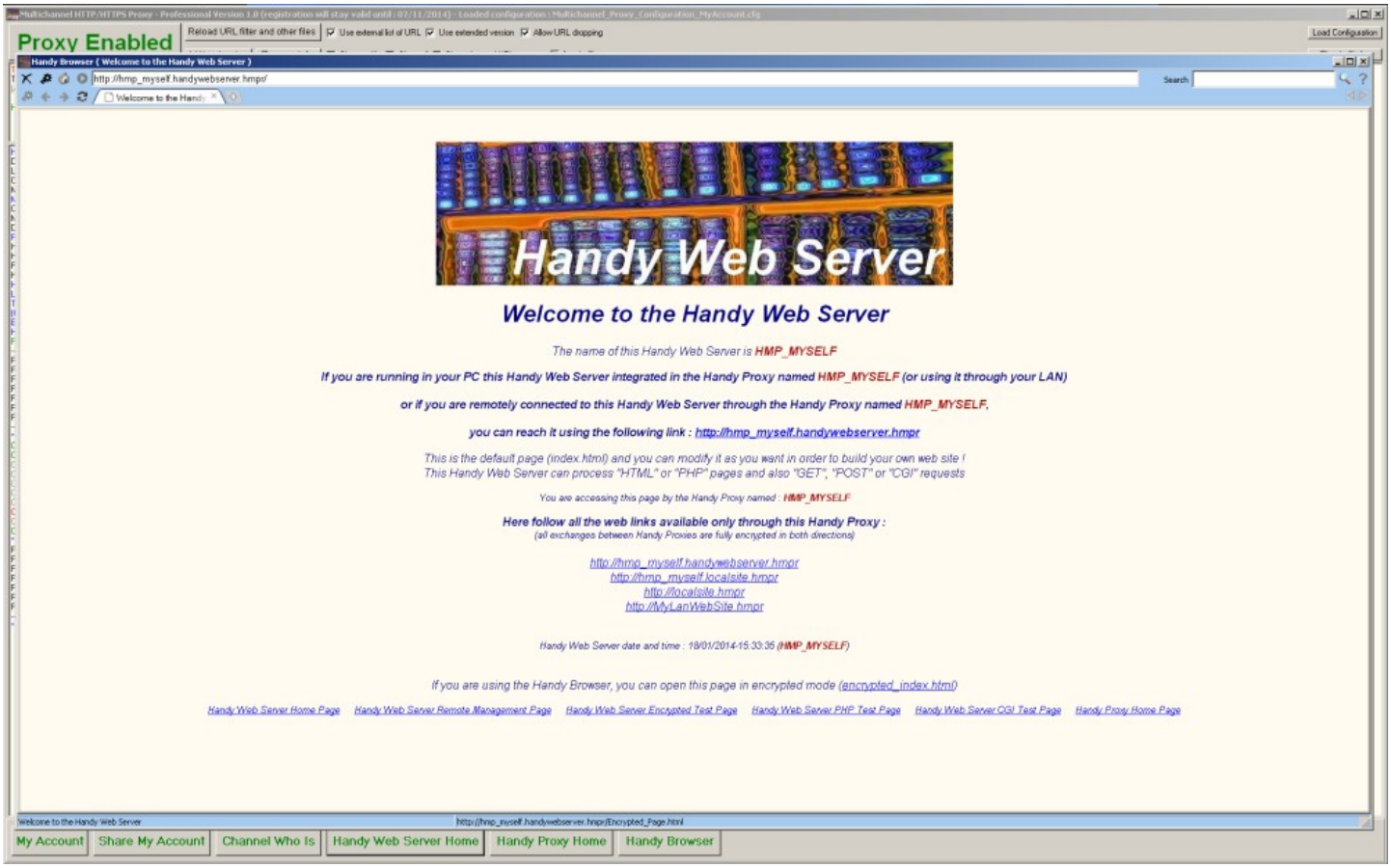
Ce serveur web n'est accessible qu'en passant par votre Handy Proxy, ce qui veut dire que les pages hébergées ne seront disponibles que pour les utilisateurs d'un Handy Proxy qui auront été autorisés à accéder à celui-ci**. Autrement dit, vous pouvez créer des sites web totalement privés**. Outre cela, comme les données qui circuleront entre les Handy Proxy sont encryptées, vos pages web hébergées par votre serveur web intégré ne seront jamais indexées par les moteurs de recherche. La confidentialité de vos données, pages, etc. est alors parfaitement préservée. Au-delà de cela, il est également possible d'encrypter vos pages, comme nous le verrons au chapitre suivant.

Pour les pages PHP, il vous est fourni lors de l'installation une copie des modules PHP originaux (qui sont dans le domaine public). Toutefois, vous n'êtes pas obligé d'utiliser cette installation car il est possible de spécifier au serveur web d'en utiliser une autre. Voir au paragraphe 9.1, fichier « Handy Proxy Master Configuration (Multichannel_Proxy_Master_Config.def) ».

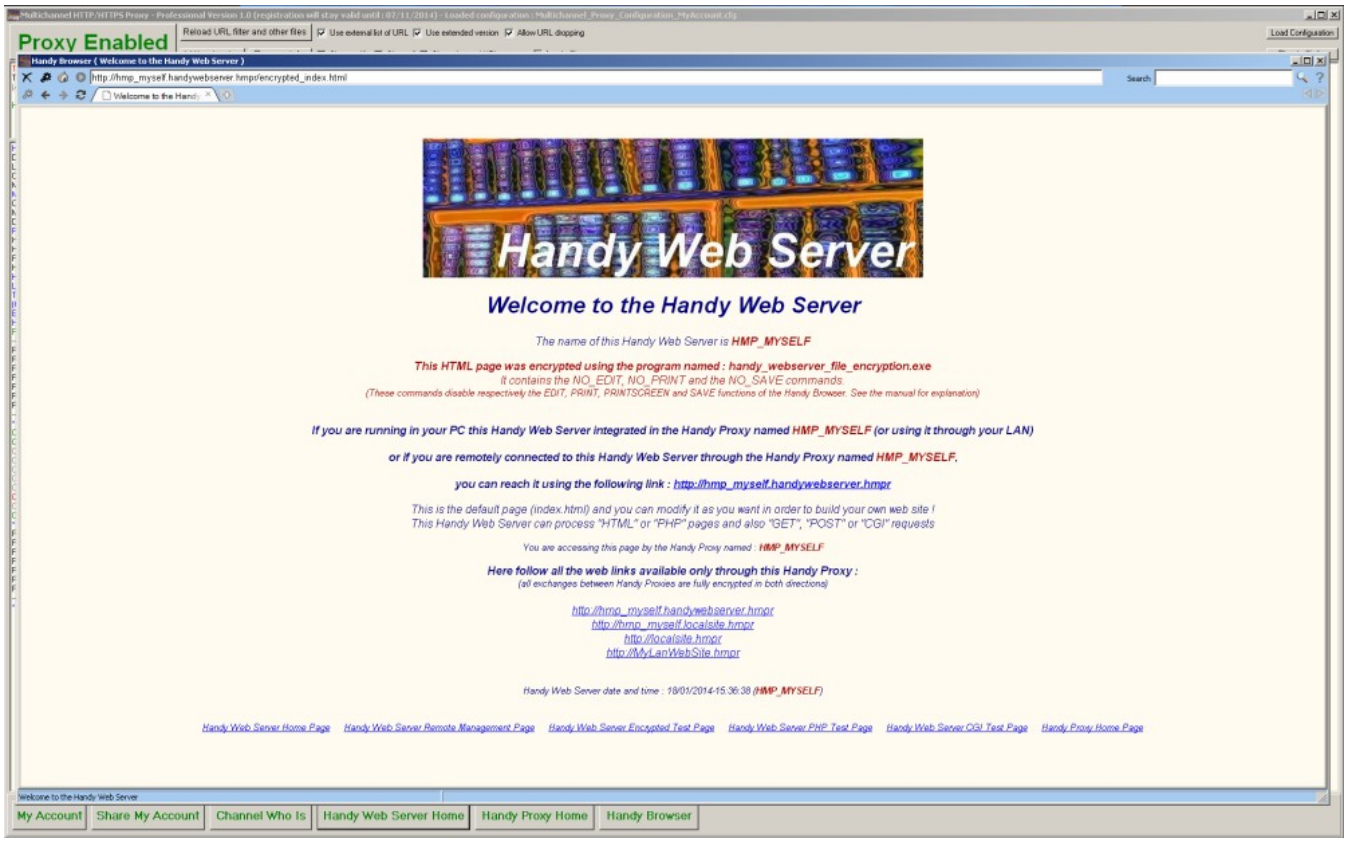
Les fichiers HTML, Javascript, PHP etc. doivent se trouver dans la directory …\Handy_Web_Server_wwwRoot de votre Handy Proxy. Attention : les fichiers INCLUDE de PHP doivent se trouver dans une directory différente (voir plus loin).

En cliquant sur le bouton « *Handy Proxy Home* » (en bas de l'écran de votre Handy Proxy), vous ouvrirez votre Handy Browser qui fait l'objet d'un chapitre spécifique plus loin dans ce manuel.

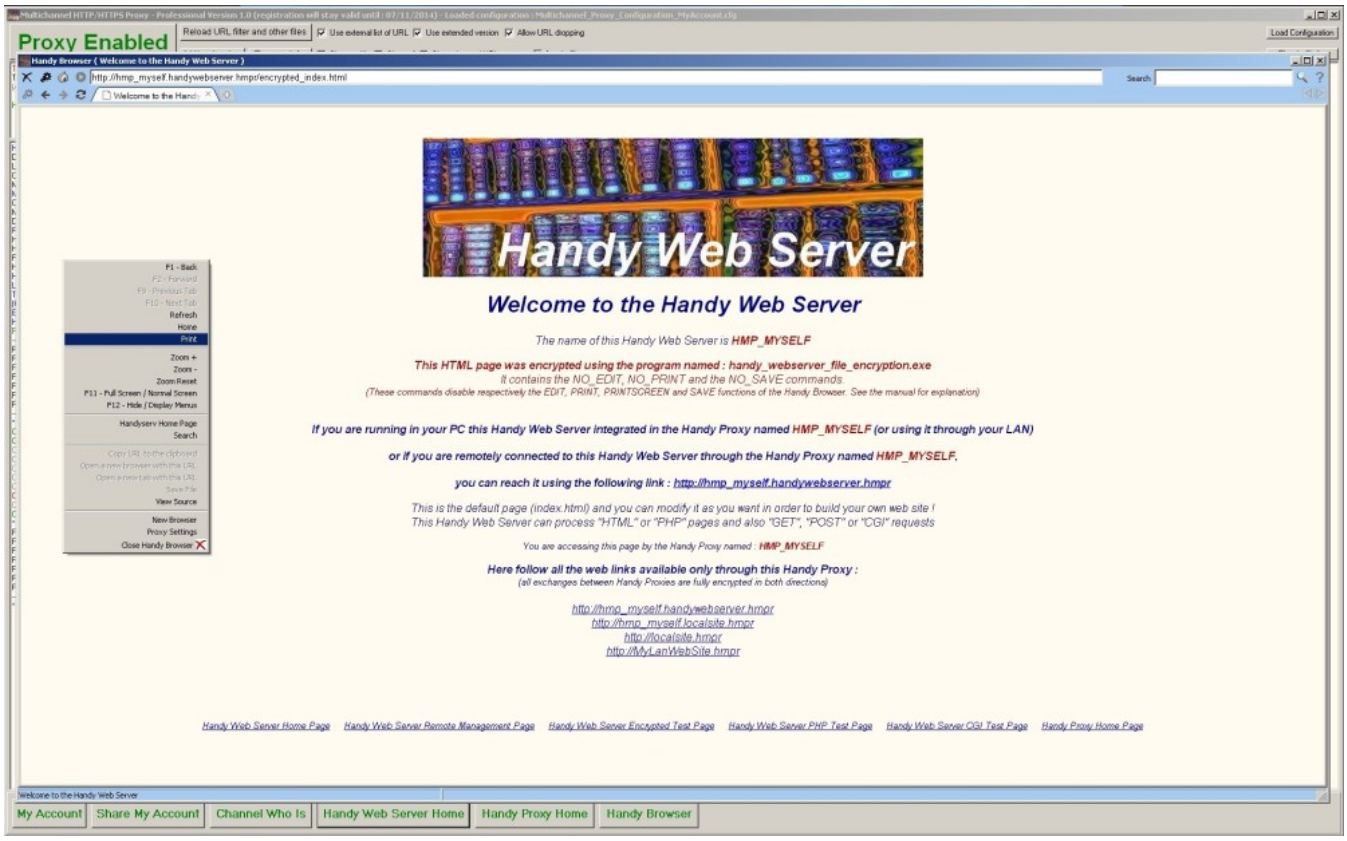
Vous obtiendrez la page par défaut de votre Handy Web Server qui a été générée à l'installation. Son nom est index.html, que vous pouvez modifier selon vos besoins et le type de services que vous souhaitez offrir à vos correspondants. Clairement, vous pouvez créer toutes les pages de votre choix en utilisant le langage HTML et/ou PHP.



Dans l'écran suivant est affichée la page nommée « encrypted_index.html ». Cette page a été préalablement encryptée par le programme d'encryption de page (qui fait l'objet d'un chapitre spécifique) fourni en standard.



Remarque : en cliquant avec le bouton droit dans l'écran de votre Handy Browser, vous obtiendrez le menu que vous voyez apparaître à gauche ci-dessous. Ce menu contient les options standard de navigation. Il peut également être obtenu à partir du menu principal situé en haut à gauche de ce navigateur.



Il est possible d'intégrer dans vos pages web des commandes spécifiques uniquement comprises par le Handy Browser fourni dans le package. Ces commandes sont :

- NO_EDIT : cette commande interdit l'édition de vos pages si celles-ci sont accédées via votre Handy Browser
- NO_PRINT : cette commande interdit l'impression de vos pages si celles-ci sont accédées via votre Handy Browser
- NO_SAVE : cette commande interdit la sauvegarde de vos pages si celles-ci sont accédées via votre Handy Browser

Pour rendre ces commandes incontournables, il faut encrypter vos pages via les fonctions fournies en standard dans ce package. Grâce à cela, ces pages ne seront visualisables qu'avec un Handy Browser. Dans l'exemple suivant, une page web a été créée contenant les trois commandes ci-dessus. Celle-ci a été encryptée et n'est donc accessible que via votre Handy Browser.

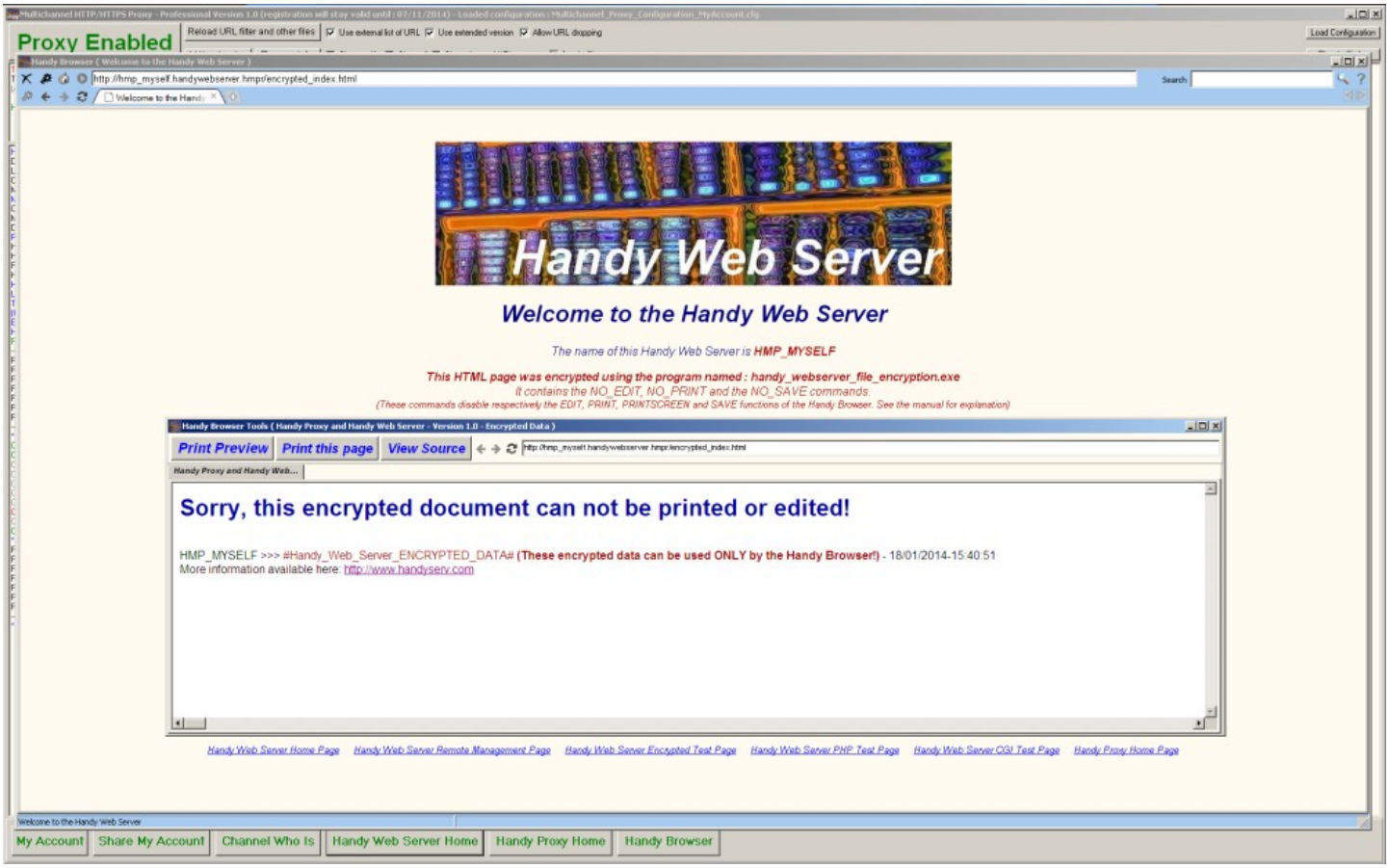
La syntaxe de ces commandes est la suivante :

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

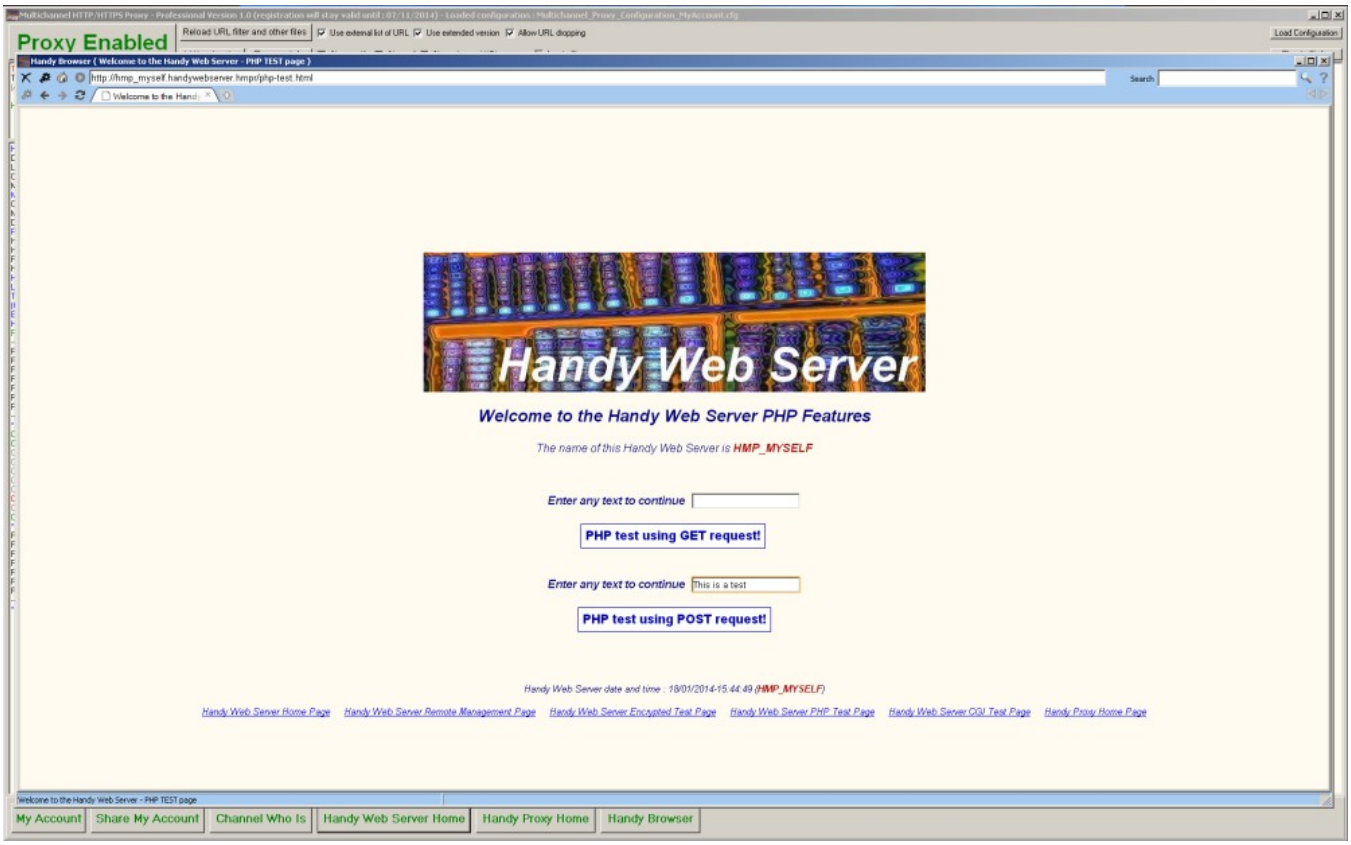
Dans cette syntaxe qui est en fait un commentaire HTML que votre Handy Browser va comprendre et interpréter, « command » doit être remplacé par NO_EDIT, NO_PRINT ou NO_SAVE. Les autres navigateurs ne feront rien de cette commande, qu'ils verront comme un simple commentaire.

Si vous utilisez plusieurs de ces commandes, il faut une ligne par commande dans vos pages. La syntaxe de ces commandes doit être scrupuleusement respectée, y compris majuscules et minuscules. Par exemple :

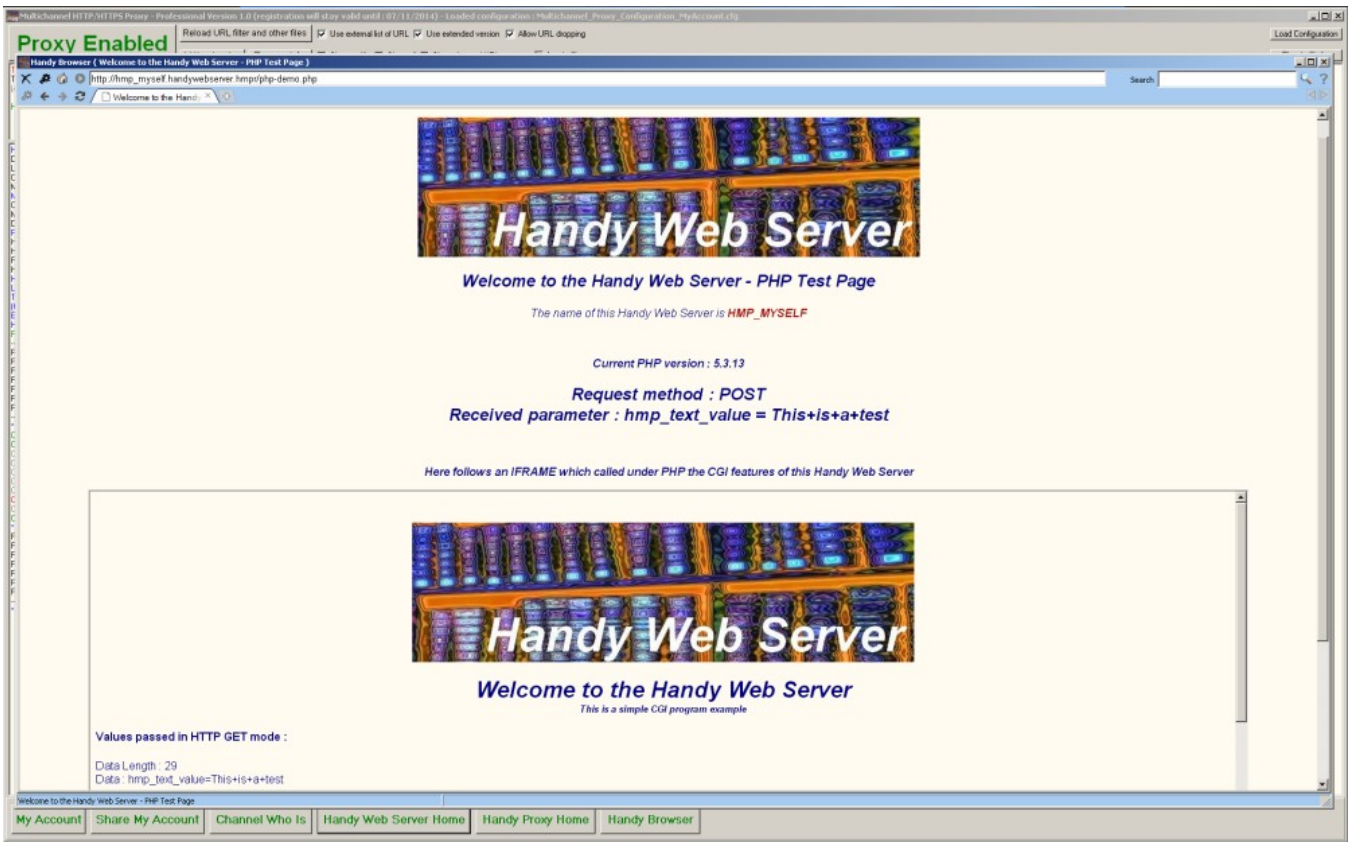
```
<!-- #Handy_Web_Server_NO_PRINT# -->
```



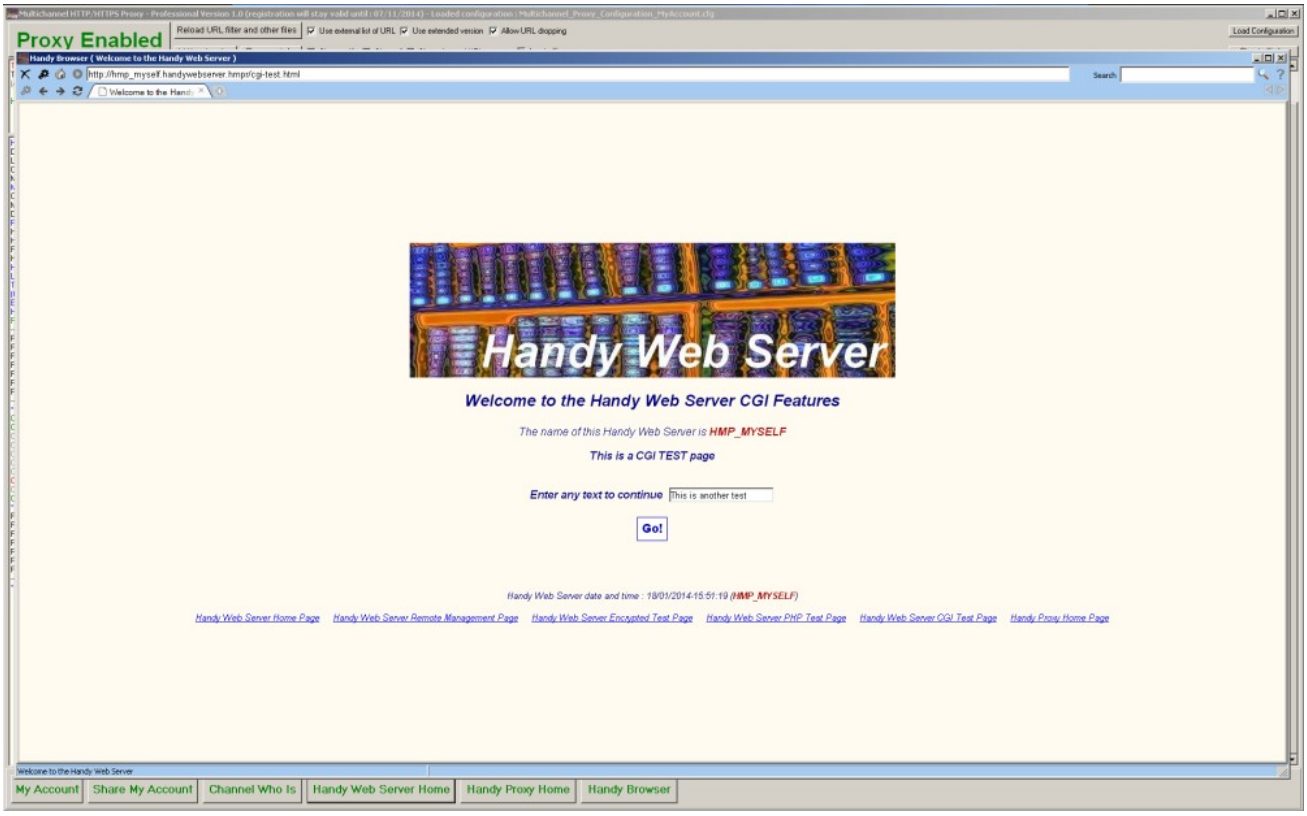
A partir de la page web par défaut, il est possible d'accéder à une autre page qui permet de tester votre intégration des modules PHP à partir de la page « php-test.html ». Cette page vous permettra d'appeler les modules PHP par une commande GET ou POST.



En cliquant sur le bouton GET ou POST de la page de test précédente, par l'appel de la page « php-demo.php », vous obtiendrez le résultat suivant dans lequel sont énumérés la version des modules PHP installés ainsi que le résultat de la requête. Vous pouvez donc créer les pages PHP de votre choix et les rendre disponibles via votre Handy Web Server.



A partir de la page web par défaut, il est possible d'accéder à une autre page qui permet de tester les fonctions CGI de votre Handy Web Server à partir de la page « cgi-test.html ». Cette page vous permettra d'appeler un module CGI mis à votre disposition lors de l'installation dans la directory ..\cgi-bin sous le nom « demo_cgi.exe ».



En cliquant sur le bouton « *Go !* » de la page précédente, par l'appel du module « demo_cgi.exe », vous obtiendrez le résultat suivant dans lequel sont énumérés tous les paramètres CGI classiques. Vous pouvez donc créer vos modules CGI et les rendre disponibles via votre Handy Web Server.

Remarques importantes :

Tous les fichiers HTML, Javascript, PHP ou images doivent être placés dans la directory **…\Handy_Web_Server_wwwRoot**.
Vous pouvez créer des sous-directories dans lesquelles ces fichiers peuvent également être sauvegardés.

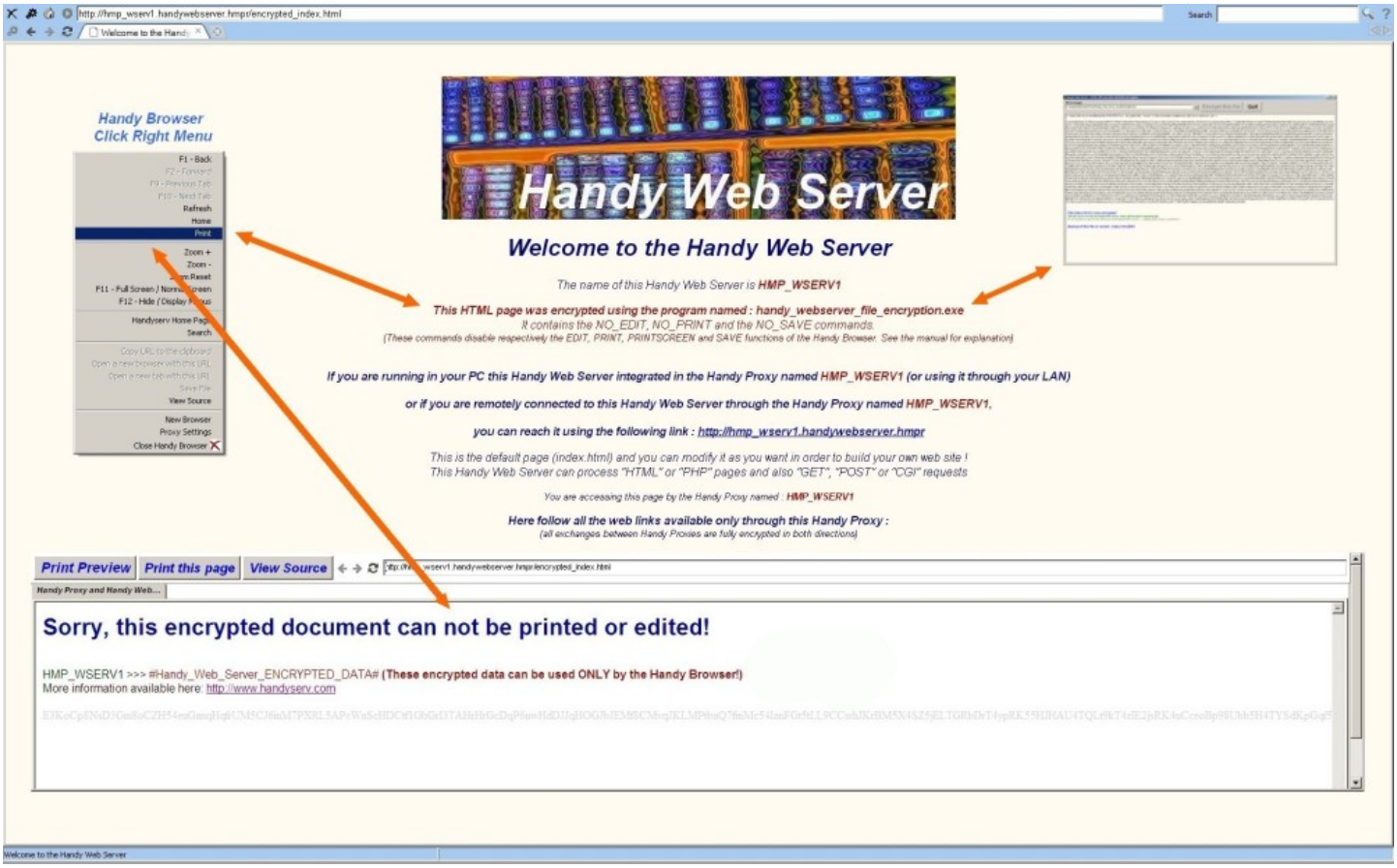
Tous les fichiers PHP « include » doivent être placés dans la directory **…\Handy_Web_Server_wwwRoot\php_includes**
Voir le fichier Handy Proxy Master Configuration (Multichannel_Proxy_Master_Config.def ; parameter name : Path_To_PHP_Apps) et le fichier de configuration PHP (php.ini ; parameter name : include_path).

Tous les fichiers CGI doivent être placés dans la directory **…\Handy_Web_Server_wwwRoot\cgi-bin**

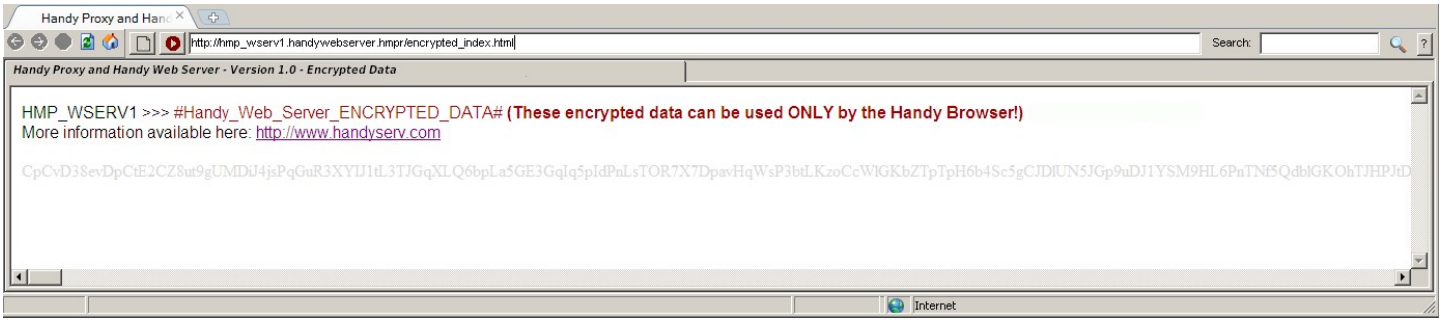
6. Encryption de fichiers avec le Handy Web Server

Comme expliqué au chapitre précédent, il vous est possible d'encrypter vos pages HTML, PHP, etc. afin de protéger vos développements et/ou modifications de ceux-ci au cas où vous partageriez vos pages avec d'autres personnes utilisant elles-mêmes un Handy Proxy.

Dans le synoptique suivant apparaît à droite la fenêtre du programme d'encryption de pages, celles-ci pouvant contenir des commandes spécifiques (voir chapitre précédent) qui seront comprises par votre Handy Browser. En cliquant dans celui-ci avec le bouton droit de la souris, le menu que vous voyez à gauche s'ouvrira et, si vous tentez d'imprimer la page affichée, une fenêtre s'ouvrira vous indiquant que cette fonction n'est pas autorisée.

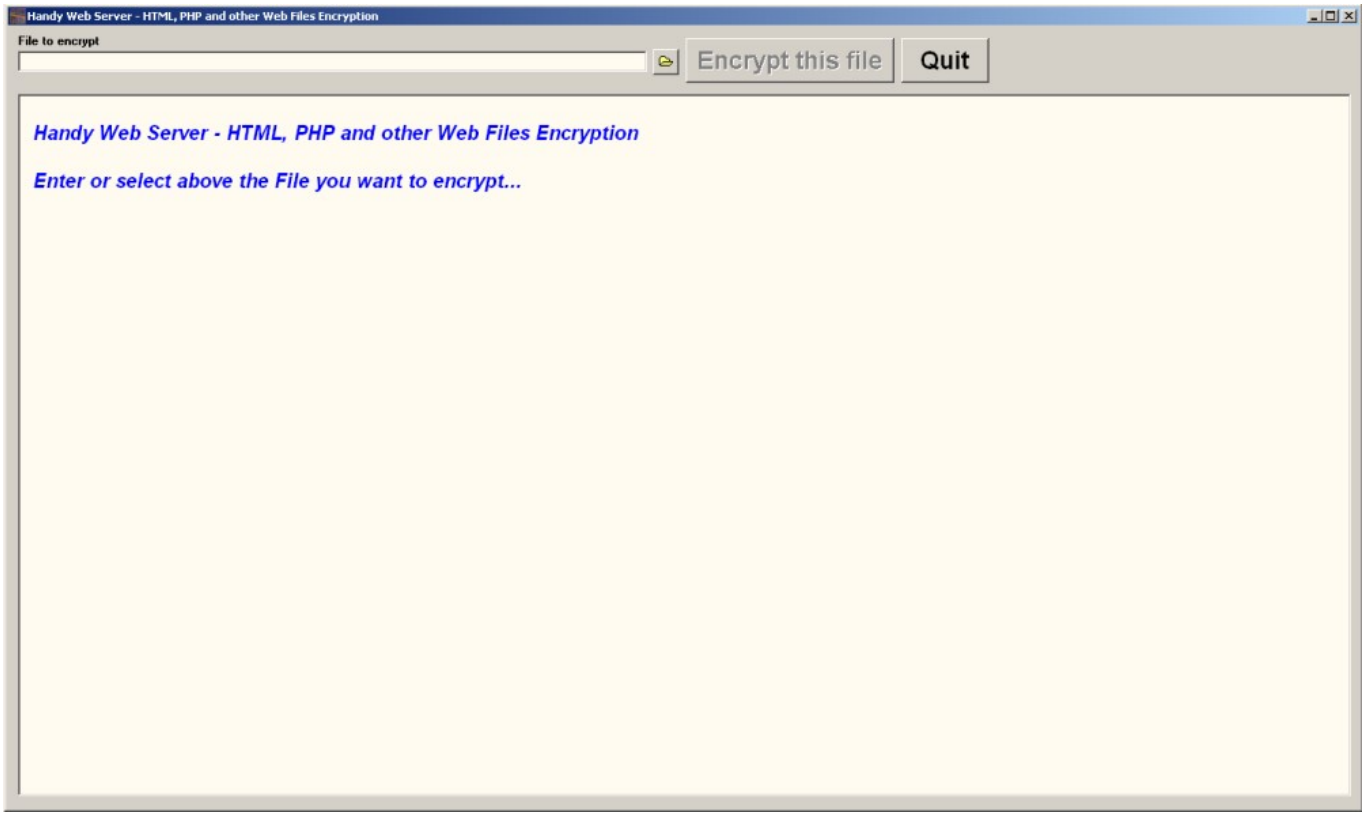


Tout autre navigateur qui serait utilisé pour afficher cette page préalablement encryptée affichera le message suivant. Les pages encryptées doivent donc impérativement être accédées via votre Handy Browser.

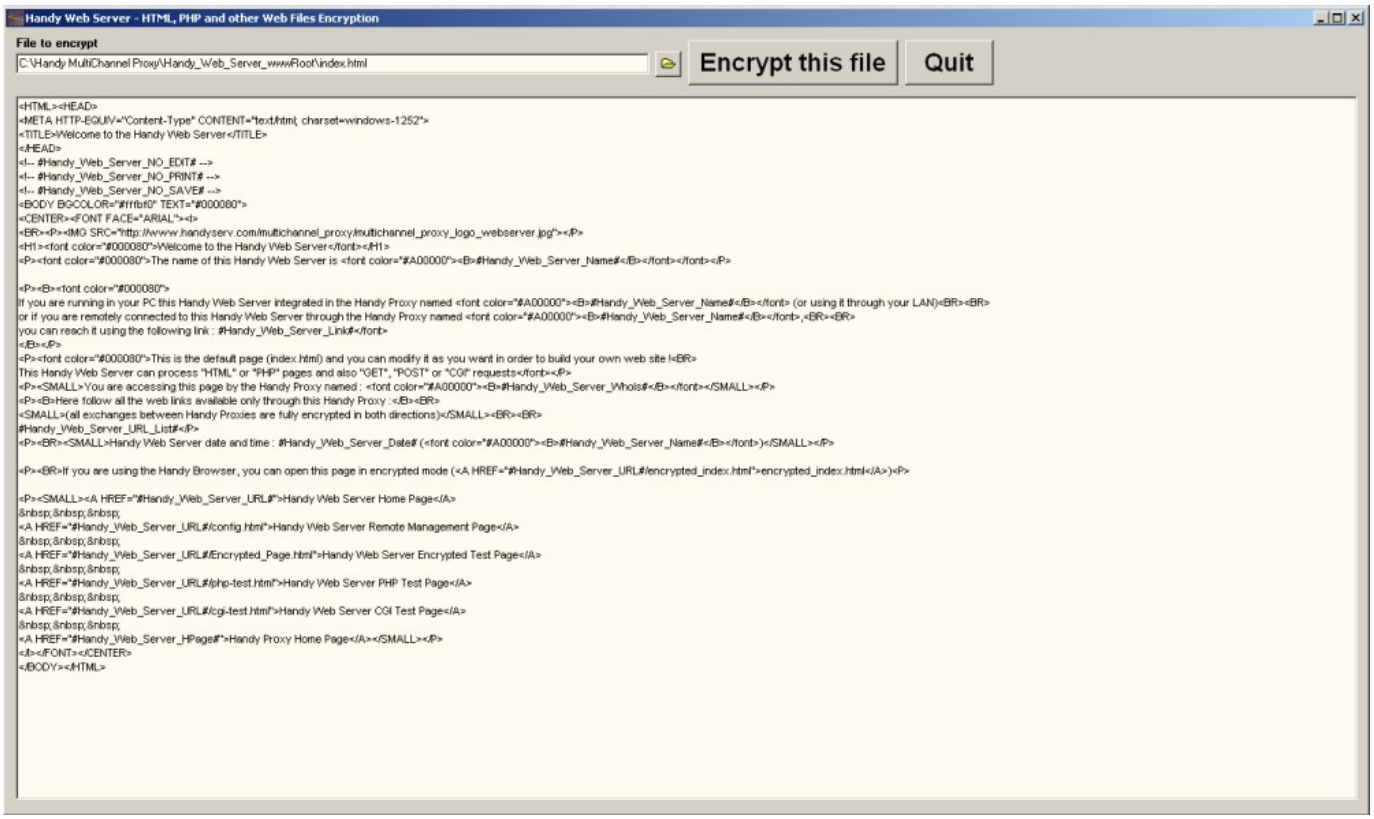


Voici comment crypter vos fichiers :

Allez dans la directory de votre Handy Proxy et lancez le programme « handy_webserver_file_encryption.exe ». Vous obtiendrez alors l'écran suivant :



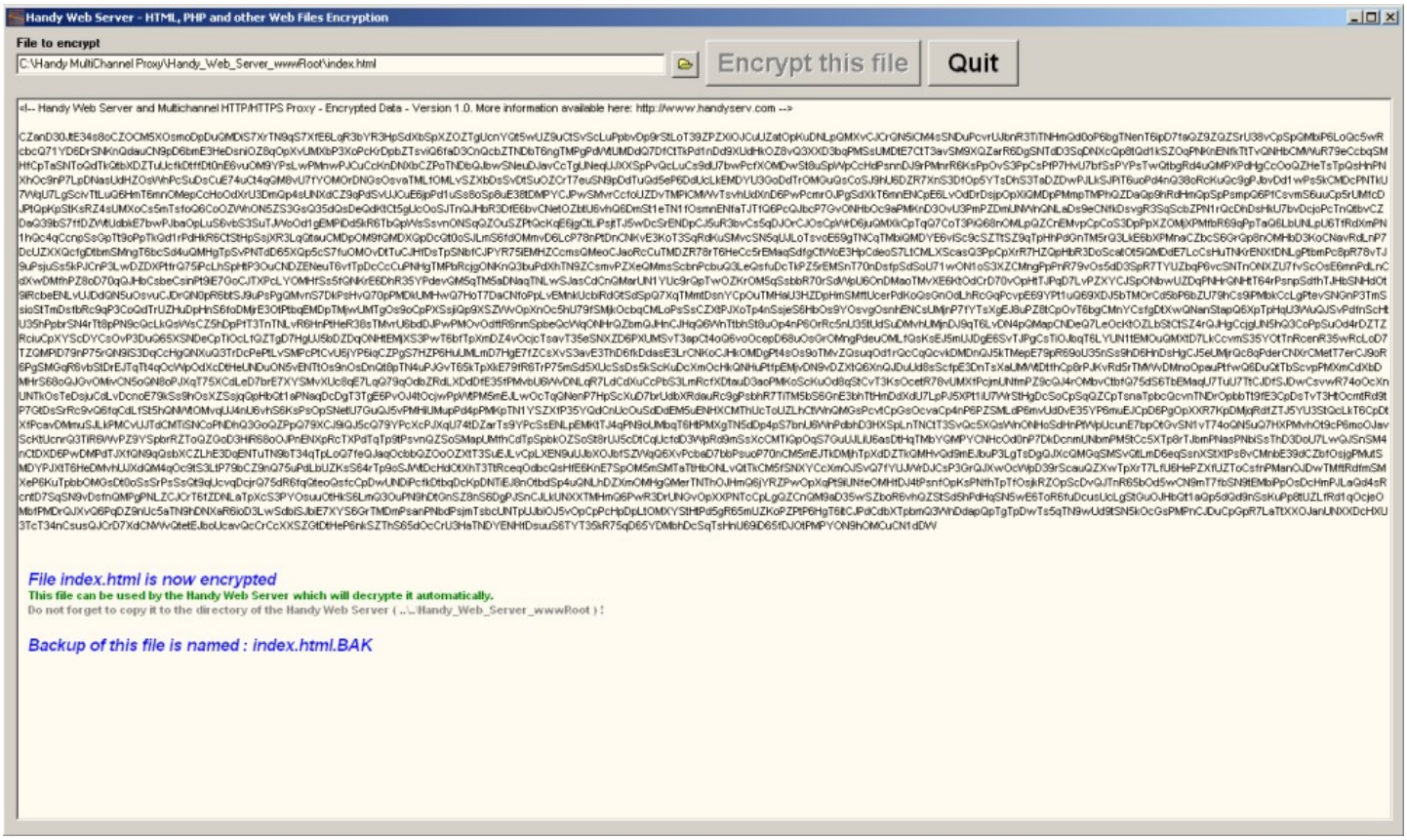
Sélectionnez, dans la directory de votre choix, le fichier HTML, Javascript, PHP de votre choix ou tout autre fichier texte que vous voulez encrypter. Le fichier apparaît à l'écran en clair. Cliquez alors sur le bouton « *Encrypt this file* ».



Le programme va alors encrypter votre fichier en créant un back-up de celui-ci avec son nom original suivi d'une extension .bak. Le fichier encrypté porte donc le nom du fichier original. Ce fichier doit être placé par vos soins dans la directory **…\Handy_Web_Server_wwwRoot** du serveur web.

Nous vous déconseillons d'encrypter les fichiers dans cette directory parce que vous pourriez oublier de supprimer les fichiers .bak et dans le cas où vous supprimeriez les fichiers .bak dans la directory du serveur web vous risqueriez de supprimer les fichiers sources non cryptés. Soyez donc très prudent en utilisant ce programme d'encryption, car il est irréversible. En effet, nous ne fournissons pas de module de décryption hormis le fait que votre Handy Web Server et votre Handy Browser sont capables de décrypter ces pages. Si nous fournissions un tel programme, vos pages seraient décryptables par des tiers, ce qui retirerait toute son utilité à cette fonction.

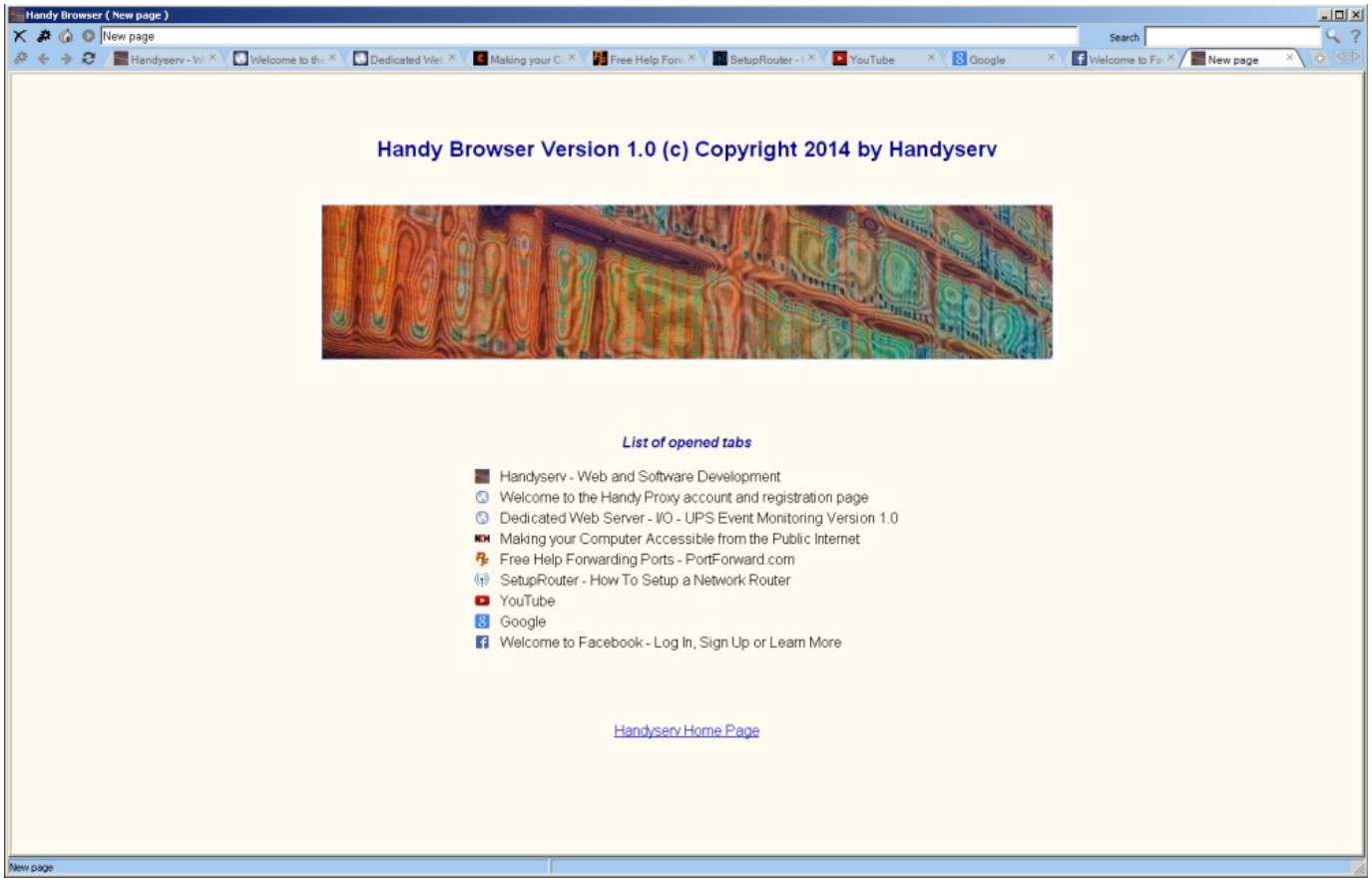
Pour éviter toute perte de données, nous vous invitons à créer vos pages web dans une directory « X », ensuite de les copier dans une directory « Y » pour les y encrypter à l'aide de ce programme, et enfin de les copier dans la directory de votre Handy Web Server.



7. Le navigateur Handy Browser

Votre package contient, comme expliqué plus haut, un navigateur portant le nom de Handy Browser. Celui-ci est un navigateur comme il en existe beaucoup d'autres, il est basé sur la technologie Chromium (c) et est donc compatible avec les technologies Internet du jour. Vous pouvez donc l'utiliser pour vous rendre sur Facebook, Youtube, etc. Toutefois, la version actuelle de ce navigateur ne permet pas d'ajouter des modules additionnels comme Java ou d'autres outils tels que des barres de navigation personnalisées, etc.

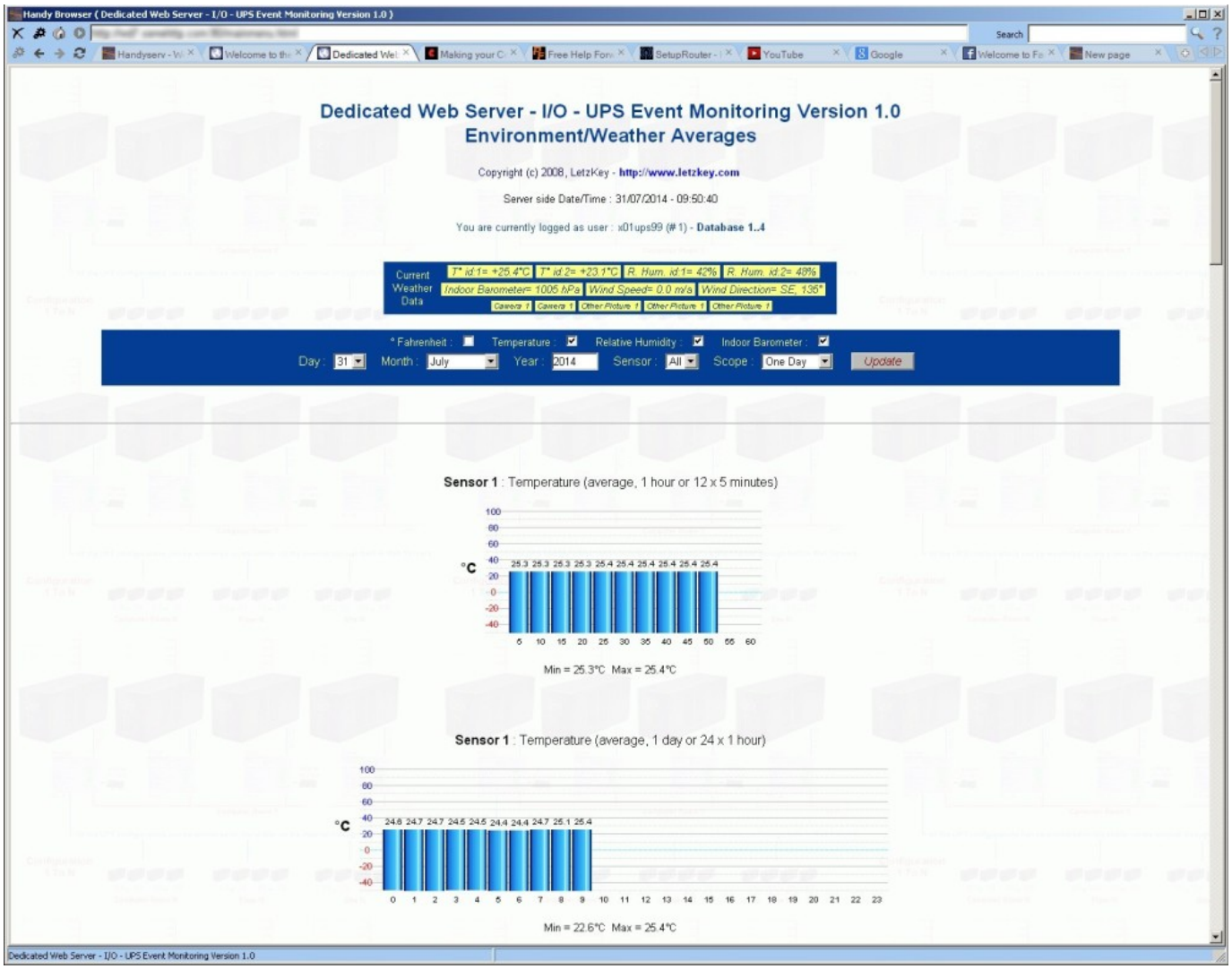
Handy Browser n'est donc pas un navigateur « toutes fonctions ». Toutefois, il a une fonction bien précise, c'est-à-dire de pouvoir afficher les pages encryptées par le programme « handy_webserver_file_encryption.exe » (fourni dans le package) et mises à disposition via votre Handy Web Server. Pour plus d'informations à ce sujet, veuillez vous référer au chapitre précédent.



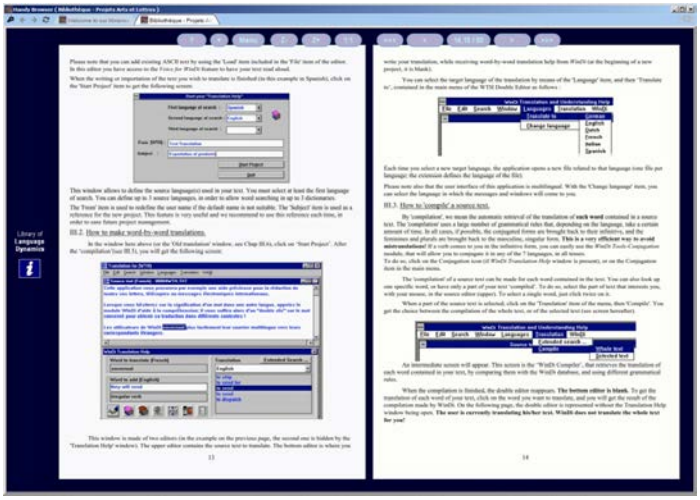
Handy Browser vous met à disposition, outre la fonction multi-onglets, les possibilités de navigation classiques en plus de fonctions « plein écran » qui sont décrites plus bas.

Voici ci-dessous un exemple de l'appel d'un service web accessible via les fonctions de reroutage d'adresse et de lien que nous allons voir plus loin dans ce manuel. Il s'agit d'un site web non public et totalement encrypté par les soins d'un Handy Proxy.

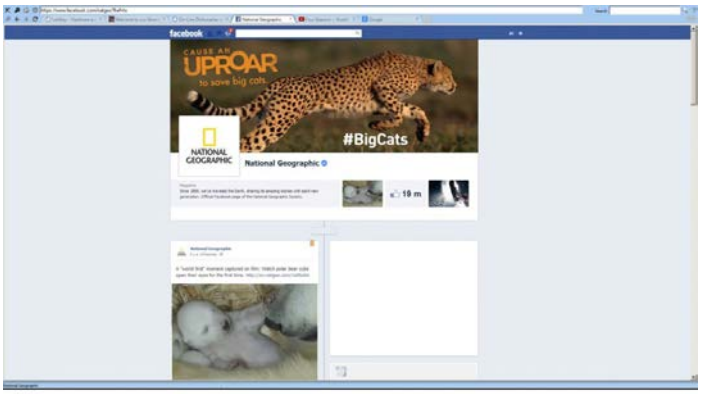
Comme vous le voyez, votre Handy Browser permet les fonctions multi-onglets. Vous pouvez voir que l'un de ceux-ci est ouvert sur Youtube, un autre sur Google et un troisième sur Facebook.



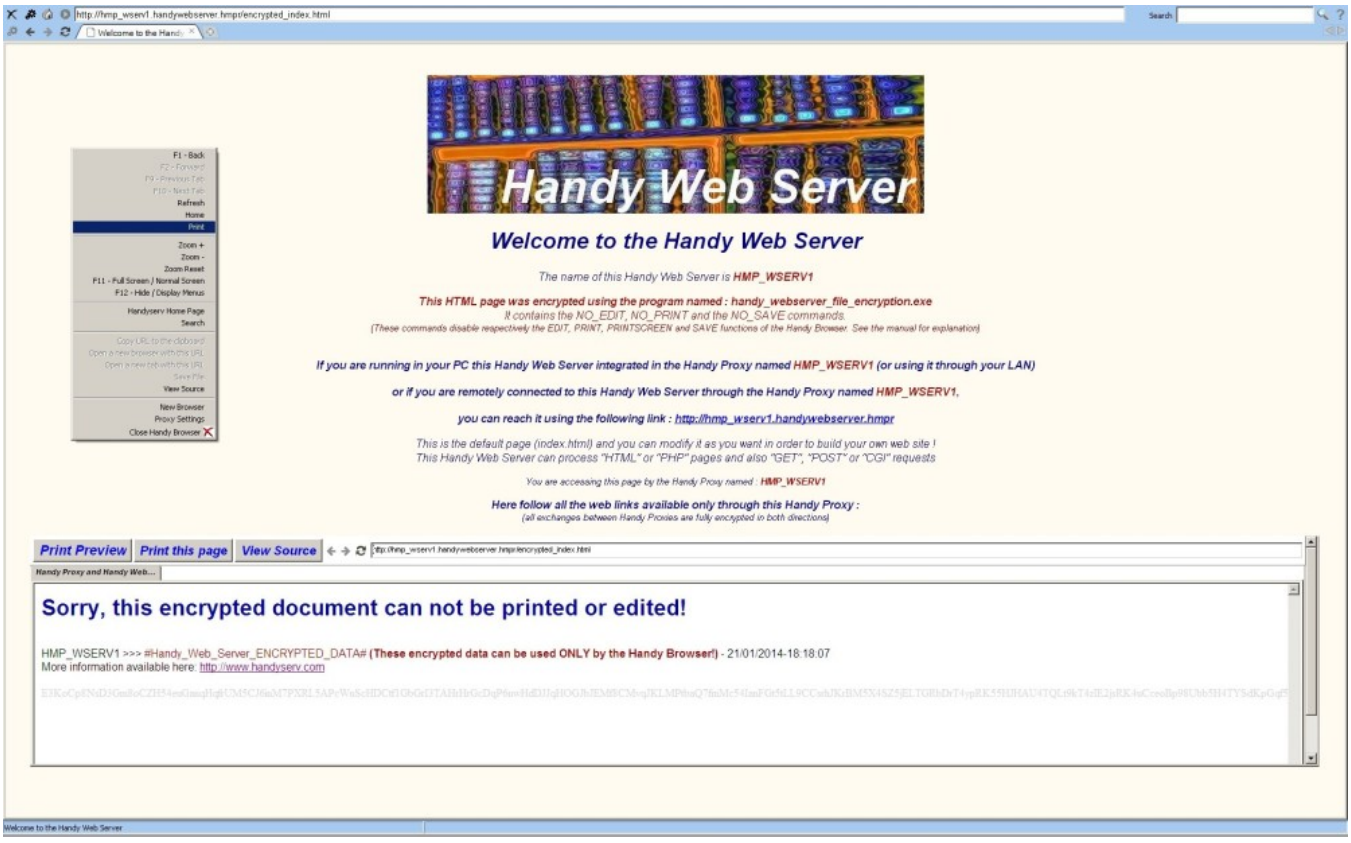
Voici des exemples d'utilisation sur des sites Internet publics :



Les deux exemples suivants vous montrent des pages ouvertes par votre Handy Browser sur Youtube et Facebook :



Voici l'utilisation de votre Handy Browser sur une page encryptée contenant des commandes spécifiques (pour plus d'informations, veuillez vous référer aux chapitres précédents) :



7.1. Les différents modes d'affichage du Handy Browser

Votre Handy Browser offre 4 modes d'affichage « plein écran ». Soit vous faites appel à ceux-ci via le menu principal de ce navigateur, soit en cliquant sur le bouton droit de votre souris vous obtiendrez le menu suivant dans lequel vous pourrez utiliser les fonctions F11 et F12, ce qui veut dire que ces deux fonctions sont également disponibles via le clavier et les touches F11 et F12.

Les 4 modes sont, comme illustré par les écrans ci-dessous :

- Affichage complet des menus, des onglets et de la barre de titre Windows ;
- Affichage d'une partie des menus, des onglets et de la barre de titre Windows ;
- Affichage d'une partie des menus et des onglets ;
- Affichage uniquement de la page web (contrairement aux autres navigateurs, vous gardez dans ce mode l'accès à la barre de tâches de Windows).

8. Handy Communication

8.1. Introduction

Votre Handy Proxy contient deux applications complémentaires permettant de communiquer avec des personnes disposant elles-mêmes d'une installation identique. Ces deux programmes sont dénommés Handy Email et Handy Messenger.

Comme déjà expliqué, tous les échanges entre les Handy Proxy sont sécurisés et encryptés. Il en va de même pour ces deux programmes qui eux aussi échangeront les données de façon sécurisée et totalement encryptée via l'envoi de ces messages par votre Handy Proxy.

Ces deux applications fonctionnent exclusivement en mode « ordinateur à ordinateur » (client-serveur) sans passer par un site internet intermédiaire de stockage, ce qui garantit une totale confidentialité des échanges entre vous et vos correspondants. **Le principe est de créer un serveur de messagerie via un Handy Proxy. Il s'agit d'un PC qui serait dévolu à cette fonction au sein d'une famille, d'un groupe d'amis ou d'une entreprise. Celui-ci devrait être idéalement accessible 24h/24h et 7j/7j,** mais ce PC peut également servir à d'autres applications puisque votre Handy Proxy est une tâche Windows comme une autre, non exclusive. Si vous envisagez un volume d'échanges important entre ce serveur et vos correspondants, il vaut mieux dédicacer ce PC à cette fonction et ne pas l'utiliser à autre chose. Il sera alors un véritable serveur puisque son temps machine sera entièrement mis à disposition du Handy Proxy et de ses fonctions serveur. La version Windows de ce PC peut être Windows 2000, XP, 7 ou 8, ce qui veut dire que tout PC, même ancien, peut être utilisé pour un fonctionnement de ce type.

Pour le répéter, si un serveur de messagerie auquel vous aimeriez vous connecter n'est pas disponible (pas on-line ou pas allumé), il vous sera impossible d'envoyer des messages à des correspondants via ce serveur. Il faut donc impérativement que cette ou ces machines soient accessibles via Internet au moment où vous allez envoyer vos messages. Veuillez vous référer au chapitre 2.1 qui explique comment procéder. Malgré cela, il est tout de même possible de correspondre avec des serveurs qui seraient présents par intermittence seulement ; vos messages ne seront alors traités que lors des moments d'accessibilité de ces serveurs. Cette situation peut rendre les échanges entre vous et vos correspondants relativement longs, puisqu'il faudrait que vous vous connectiez au moment où les serveurs seraient là, et de même pour vos correspondants. Ceci aurait pour résultat de fortement ralentir les échanges. Les délais seraient dès lors par définition assez aléatoires.

Fonctionnement des applications

Si votre correspondant est connecté à votre réseau local (LAN), les échanges se feront en interne sans passer par Internet. Dans le cas d'un correspondant hors de votre réseau local, ces deux programmes vont alors utiliser Internet comme transporteur de données, en mode client-serveur comme expliqué et totalement sécurisé puisque les données passeront exclusivement par les Handy Proxy (celui du serveur et celui de votre correspondant).

Pour ce faire, ces programmes vont d'abord essayer de se connecter au(x) serveur(s) en interne (au sein de votre LAN) et au cas où cette tentative n'aboutirait pas, ils vont lancer automatiquement une tentative de communication externe, mais cette fois en utilisant Internet comme transporteur de données et toujours en mode client-serveur via les Handy Proxy.

Tous les échanges de messages sont basés exclusivement sur le protocole « http », ce qui veut dire qu'aucun autre protocole de communication n'est utilisé et qu'aucun port spécifique de communication n'est ouvert chez vous ou chez vos correspondants. A nouveau, cette méthode garantit une sécurité des échanges en ne nécessitant pas d'ouverture de port susceptible d'être atteint autrement que via le passage obligatoire par votre Handy Proxy qui contient les protections d'accès indispensables comme expliqué dans les chapitres précédents.

Comme ces deux programmes se connectent d'ordinateur à ordinateur en mode client-serveur, il est alors indispensable de gérer les potentielles difficultés de connexions entre votre configuration (serveur et/ou client) et celles de vos correspondants. Pour remédier à ce type de problèmes qui se produiront inévitablement puisque les Handy Proxy des serveurs cibles pourraient ne pas être on-line à un moment donné, votre Handy Proxy contient, en plus de toutes ses autres fonctions, un serveur de messages qui aura pour but de délivrer en toute sécurité les messages qui seraient en attente chez vous. Il est indispensable de comprendre ici que les messages qui ne partent pas immédiatement parce que les serveurs cibles ne seraient pas on-line restent *chez vous* en attente d'être délivrés. Si un ou plusieurs messages vers un ou plusieurs correspondants n'étai(en)t pas envoyé(s) immédiatement, le serveur de messages inclus dans votre Handy Proxy va tenter, pendant 8 jours (en mode prioritaire), d'atteindre le(s) serveur(s) cible(s) pour lui(leur) livrer le(s) message(s) en attente le plus vite possible. Ensuite (mode sans priorité), lorsque les serveurs cibles seront à nouveau à disposition, votre serveur de messages communiquera immédiatement les messages qui seraient encore en attente chez vous et qui seraient datés de plus de 8 jours.

Ainsi, la meilleure manière d'utiliser ces deux applications est donc de laisser les Handy Proxy qui seraient utilisés en tant que serveurs de messagerie fonctionner le plus souvent possible de telle manière que votre serveur de messages puisse arriver à envoyer vos messages en attente à vos correspondants. De même, ce mode de fonctionnement vous permettra de recevoir le plus vite possible les messages qui vous seraient envoyés.

Les différents serveurs définis vont être contactés de deux manières différentes :

- **Mode « lent »** : ce mode est celui par défaut lorsque les applications Handy Email et Handy Messenger ne sont pas actives. En cas de réception d'un message, votre Handy Proxy va démarrer l'application concernée (si elle n'est pas déjà active) et le mode « rapide » va s'enclencher. Le mode « lent » est un cycle de 10 minutes (« slow polling »).
- **Mode « rapide »** : ce mode va permettre d'aller chercher ou envoyer vos messages vers les serveurs définis de manière rapide. Le mode « rapide » est un cycle de 1 minute pour Handy Email, et de 30 secondes pour Handy Messenger (« fast polling »). Ce mode se déclenchera pour revenir au mode lent après 15 minutes.

Sur l'écran de contrôle de votre Handy Proxy, l'état de vos serveurs de messagerie vous sera affiché au rythme du mode de fonctionnement (« lent » ou « rapide »). Vous pouvez annuler cette visualisation au moyen d'un paramètre (voir le fichier Multichannel_Proxy_Master_Config.def au chapitre 9).

Pour écrire un message instantané ou un e-mail à un correspondant, vous devez connaître à la fois le nom de son Handy Proxy ainsi que le nom du serveur sur lequel il se connecte, c'est-à-dire le nom du Handy Proxy qui fonctionne en serveur de messagerie. Il faut alors ajouter manuellement ces deux informations dans le fichier de définition des correspondants et des serveurs cibles (voir paragraphe suivant).

Cette méthode impliquant de devoir ajouter manuellement les noms des Handy Proxy de vos correspondants pour pouvoir leur écrire est classique et tout à fait similaire à d'autres services. La méthode que nous présentons offre un avantage considérable : vous ne pourrez communiquer qu'avec les personnes reprises dans cette liste de correspondants et personne d'autre ne pourra vous envoyer des messages. Ce système permet donc de rester exclusivement dans un cercle de correspondants bien déterminés sans jamais recevoir des messages indésirables de correspondants inconnus (anti-spam incontournable). Toutefois, l'équipe de développement du Handy Proxy a pensé qu'il était intéressant de laisser un correspondant (non inclus dans votre liste) vous écrire afin que ses messages vous parviennent et restent en attente, mais dans un état totalement invisible. Bien entendu, ceci ne fonctionnera que si votre correspondant connaît le nom de votre Handy Proxy. Cette méthode permet alors de commencer les échanges dans un sens en vous permettant d'ajouter le(s) correspondant(s) dont nous parlons dans votre liste si vous voulez qu'ils rejoignent votre cercle de destinataires. Les applications vous indiqueront qu'il y a des messages de ce type en attente. Vous ne serez alors pas obligé d'inclure ces correspondants dans votre liste, car il existe une fonction de prévisualisation du contenu des messages reçus. Si un message ne vous convient pas vous pourrez le supprimer sans même l'ouvrir, et le correspondant qui vous a écrit n'apparaîtra plus. En revanche, si le correspondant est une personne avec laquelle vous souhaitez échanger, vous pourrez en un clic l'inclure dans la liste et son message sera alors mis à votre disposition afin que vous puissiez y répondre, le transférer éventuellement à d'autres, etc.

8.2. Premières étapes de configuration des applications Handy Email et Handy Messenger

Avant tout, et avant de pouvoir envoyer le moindre message instantané ou e-mail, vous devez créer votre liste de destinataires (« addressees ») ainsi que la liste des serveurs de messagerie avec lesquels vous allez être connecté. C'est exactement le même principe que pour envoyer un e-mail via vos applications habituelles, puisque vous ajoutez dans la liste de vos destinataires le nom de celui-ci suivi du nom du serveur, les deux étant séparés par le caractère @ comme par exemple : john@emailserver.com. La différence ici n'est qu'une différence de syntaxe, puisque vous utiliserez le caractère « > » à la place du « @ ». Par exemple, comme nous le verrons plus bas : « Kimberly>Bradley » qui se traduit par : « Kimberly » est atteignable via le serveur dénommé « Bradley ». Ceci est tout à fait identique au fonctionnement de votre messagerie habituelle. La différence de syntaxe, via le caractère « > », permet de clairement différencier les deux afin de ne pas intégrer d'adresses e-mail classiques dans les applications présentées ici et inversément.

Le fichier de la liste de vos destinataires n'est pas accessible autrement que par l'éditeur que nous avons intégré dans le package puisque ce fichier est encrypté. Si vous définissez un mot de passe d'accès à ce fichier, son accès est protégé par celui-ci. Vous pourriez alors diffuser auprès de votre famille, de vos amis, de votre organisation, ce fichier qui ne sera pas modifiable par d'autres que vous qui connaissez le mot de passe. Pour plus d'informations à ce sujet, veuillez vous référer aux fichiers de configuration de votre Handy Proxy, et plus particulièrement au fichier « Multichannel_Proxy_Master_Config.def », lui-même étant encrypté et aussi protégé par un mot de passe (par défaut : 1234).

Le fichier de vos destinataires a une syntaxe qu'il faut scrupuleusement respecter, sans quoi, soit son utilisation sera refusée (par les applications qui y font appel) avec un message d'erreur vous indiquant quelles sont les anomalies rencontrées, soit vous ne parviendrez pas à envoyer des messages à un destinataire parce que par exemple son serveur serait mal défini (ou inexistant) dans ce fichier.

Remarque importante : les applications vont systématiquement vérifier à la fois si les serveurs définis existent et s'ils sont dûment répertoriés dans les bases de données de Handyserv en tant qu'utilisateurs reconnus. La même vérification se fait également pour les destinataires (« addressees »). En cas d'erreur de syntaxe, de duplication d'un serveur ou d'un destinataire, les applications vont refuser de fonctionner aussi longtemps que ces erreurs ne sont pas corrigées, ceci afin de garantir que vos messages seront envoyés aux bons destinataires vers les bons serveurs. Il est donc de votre responsabilité de créer des serveurs et adresses de destinataires existants et cohérents.

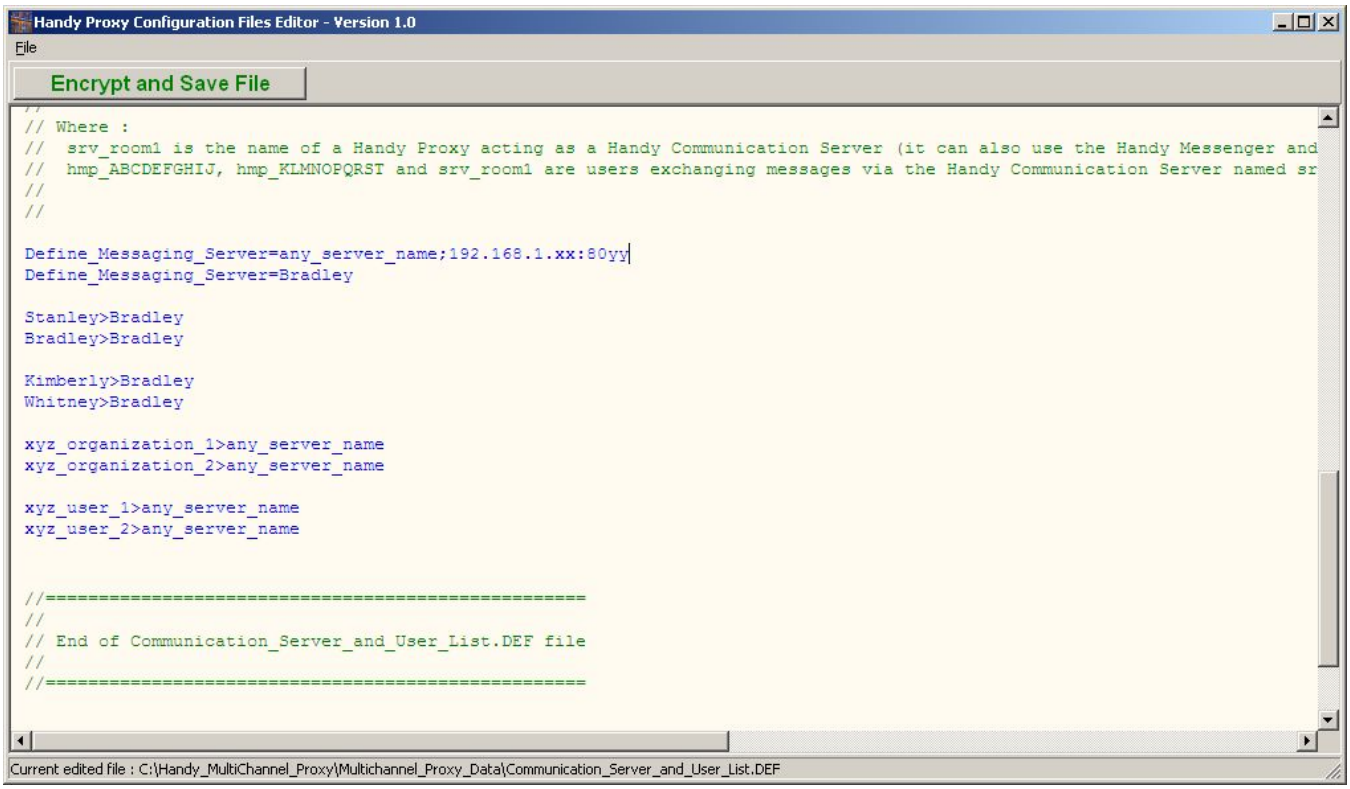
Si vous démarrez votre installation, vous devez d'abord mettre en fonctionnement votre Handy Proxy avec un nom de votre choix qui pourra être ensuite, et uniquement ensuite, défini comme serveur de messagerie. Si vous tentez d'atteindre un serveur qui n'est pas encore défini, les applications vont déterminer qu'il y a une anomalie et vont refuser de démarrer en affichant un message d'erreur à l'écran. Ce PC devra être accessible via Internet s'il n'est pas connecté à votre réseau local. Veuillez vous référer au chapitre 2.1 du présent manuel qui explique comment procéder et mettre en partage votre Handy Proxy et ses fonctions de serveur de messagerie.

ATTENTION : si votre configuration est également utilisée comme serveur de messagerie, vous ne pouvez pas changer le nom de votre Handy Proxy puisque des utilisateurs vont utiliser votre machine comme serveur. Si ce nom change, ils ne pourront plus vous retrouver.

A présent, prenons un exemple de définition via le programme d'édition des fichiers de configuration du Handy Proxy.

Dans ce fichier, il faut **d'abord** définir le(s) serveur(s) auxquels vous et vos correspondants serez connectés. Tout serveur qui serait défini après la liste de vos destinataires ne sera pas pris en compte et un message d'erreur apparaîtra automatiquement afin de signaler qu'il manque une définition. Ce n'est qu'après la liste de définition des serveurs de messagerie que vous pourrez insérer la liste de vos destinataires, comme dans l'exemple qui suit.

Voici l'écran de cet éditeur ouvert sur le fichier de définition de vos destinataires. Celui-ci est accessible via le menu « Edit », option « Edit Addressee List » des applications Handy Messenger et Handy Email :



Pour la définition de vos serveurs de messagerie, qu'ils soient locaux ou distants, celle-ci doit être faite selon la syntaxe qui suit :

Define_Messaging_Server=[nom du serveur];[adresse IP locale dans votre réseau]:[port]

Les paramètres « adresse IP » et « port » sont optionnels, et ne sont à utiliser que si vous devez atteindre votre serveur à partir de votre réseau local et éventuellement à partir d'Internet via un portable si par exemple vous êtes à l'extérieur de votre réseau local.

Define_Messaging_Server=any_server_name;192.168.1.xx:80yy

Ceci indique que le serveur « any_server_name » pourra être accessible via Internet ou via son adresse « IP:port » dans votre réseau local. Veuillez aussi vous référer au chapitre 2.1 du présent manuel.

Si vous n'avez jamais accès au réseau local du serveur vers lequel vous voulez vous connecter, définissez-le ainsi :

Define_Messaging_Server=Bradley

Dans le cas ci-dessus, « Bradley » est un exemple de nom d'un Handy Proxy agissant en tant que serveur et devant être défini comme expliqué dans l'exemple ci-dessus.

Remarque : chaque définition de serveur que vous allez ajouter fera qu'il sera nécessaire de se connecter à celui-ci afin de voir si des messages vous sont adressés ou pour que vous déposiez vos messages. C'est une opération qui peut prendre du temps. Il est donc conseillé de limiter le nombre de serveurs avec lesquels vous allez être en connexion ; pour des raisons de rapidité, il nous semble raisonnable de ne pas dépasser 10 à 15 serveurs maximum. Nous vous conseillons donc de regrouper vos correspondants sur un même serveur ou sur un faible nombre de serveurs.

Après, et seulement après cette définition de serveur(s), vous pourrez lister vos correspondants comme suit :

Any_user>any_server_name

Plus concrètement, et comme dans l'exemple ci-dessus :

Kimberly>Bradley

Cette adresse se traduit par : « Kimberly » est atteignable via le serveur dénommé « Bradley ».

Après la définition de votre fichier de configuration de vos destinataires et de vos serveurs, vous pourrez vérifier cette configuration comme suit :

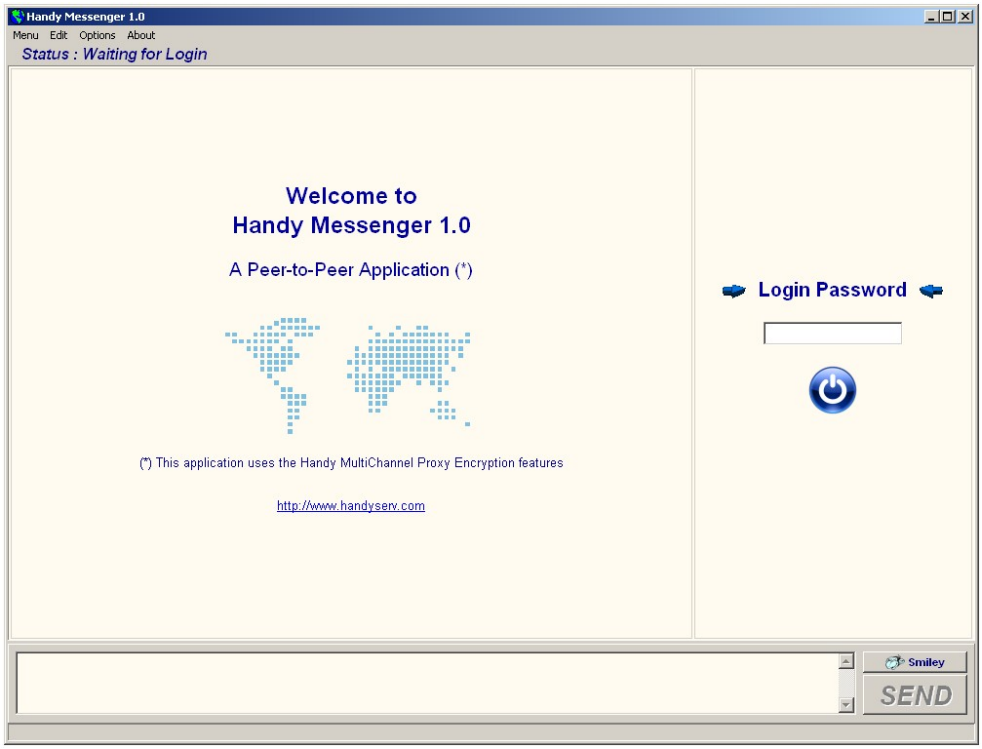
Dans les menus des applications Handy Messenger et Handy Email, à partir de la fonction « About », l'option « List of my remote Handy Messaging Servers » vous donnera l'état de vos connexions avec les différents serveurs avec lesquels vous êtes en contact. Il y a plusieurs cas possibles : soit un serveur peut être situé dans votre réseau local, soit il est accessible par Internet uniquement. Si ce serveur n'est pas accessible, cela vous sera clairement indiqué et vous pourrez voir si vous êtes connecté à ce serveur via votre réseau ou via Internet.
Cette liste se met à jour régulièrement mais elle n'est pas à jour en temps réel. En cas de changement d'un état d'un serveur, il faut un certain délai pour que vous en soyez averti via cette option. La reconnexion, si nécessaire, se fera automatiquement et toujours après un délai de quelques minutes.

Il est impératif que les PC qui seraient serveurs de messagerie via le Handy Proxy restent en fonctionnement ! A défaut, ils ne seront évidemment pas accessibles et vous ne pourrez pas envoyer de messages vers ces serveurs. Toutefois, vous pouvez créer vos messages qui resteront en attente (état « Pending ») jusqu'au moment où la connexion sera rétablie avec le(s) serveur(s) en question.

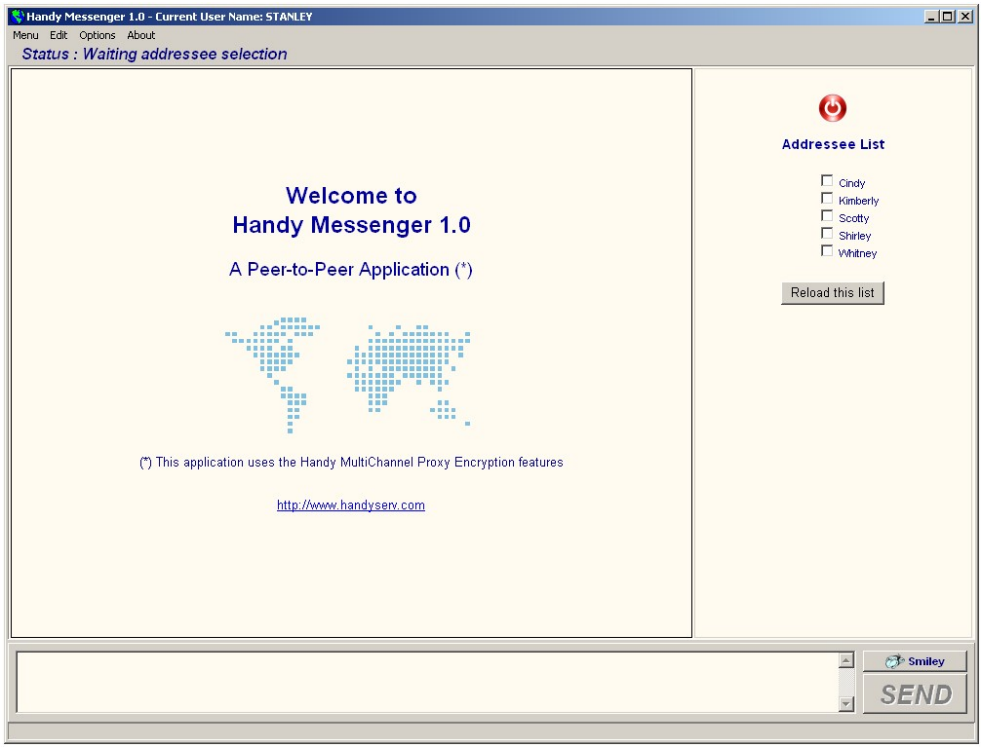
8.3. Handy Messenger

Comme expliqué dans l'introduction de ce chapitre, nous rappelons que ce programme d'échange de messages est entièrement sécurisé et ne fonctionnera qu'entre utilisateurs de Handy Proxy. Il faut donc impérativement que votre Handy Proxy soit opérationnel dans votre PC, sans quoi ce programme ne fonctionnera pas puisqu'il ne disposera pas de son canal de communication sécurisé et encrypté.

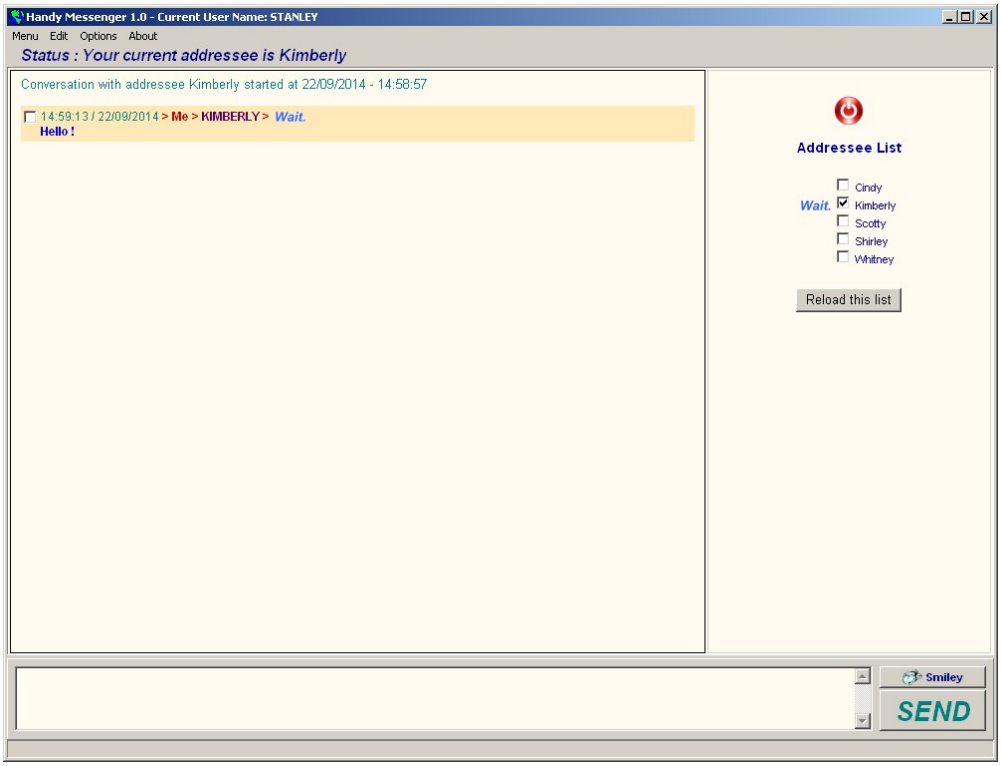
Voici l'écran d'accueil qui vous suggère de vous identifier par votre mot de passe (voir les fichiers de configuration à ce sujet) :



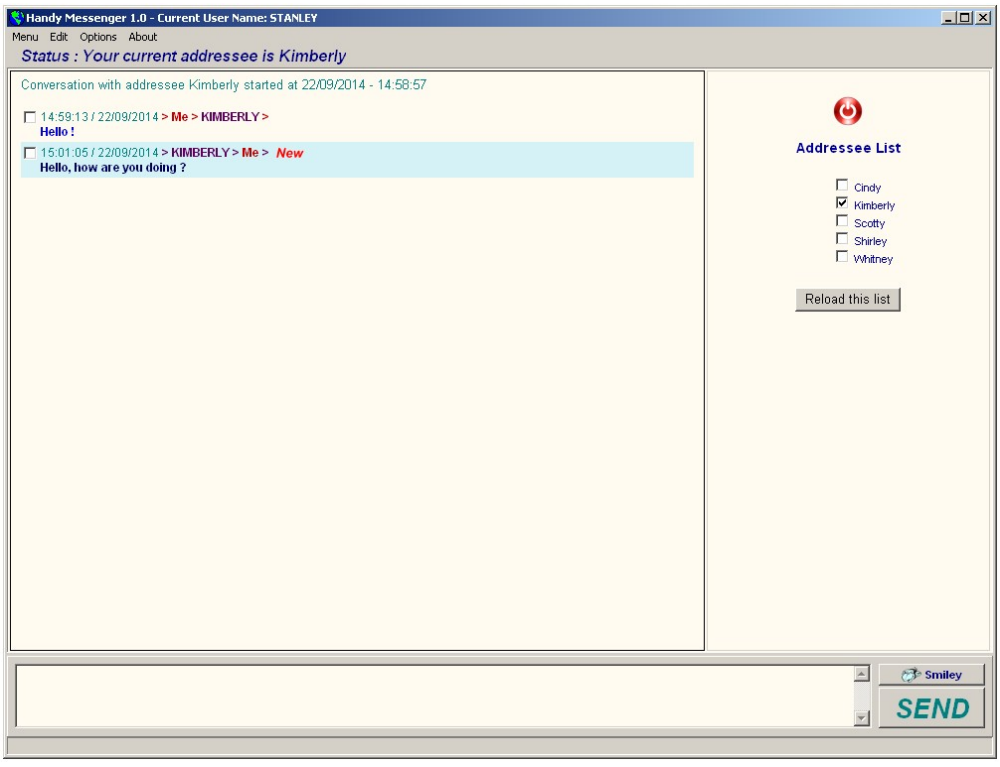
Après vous être identifié, vous obtiendrez la liste de vos correspondants :



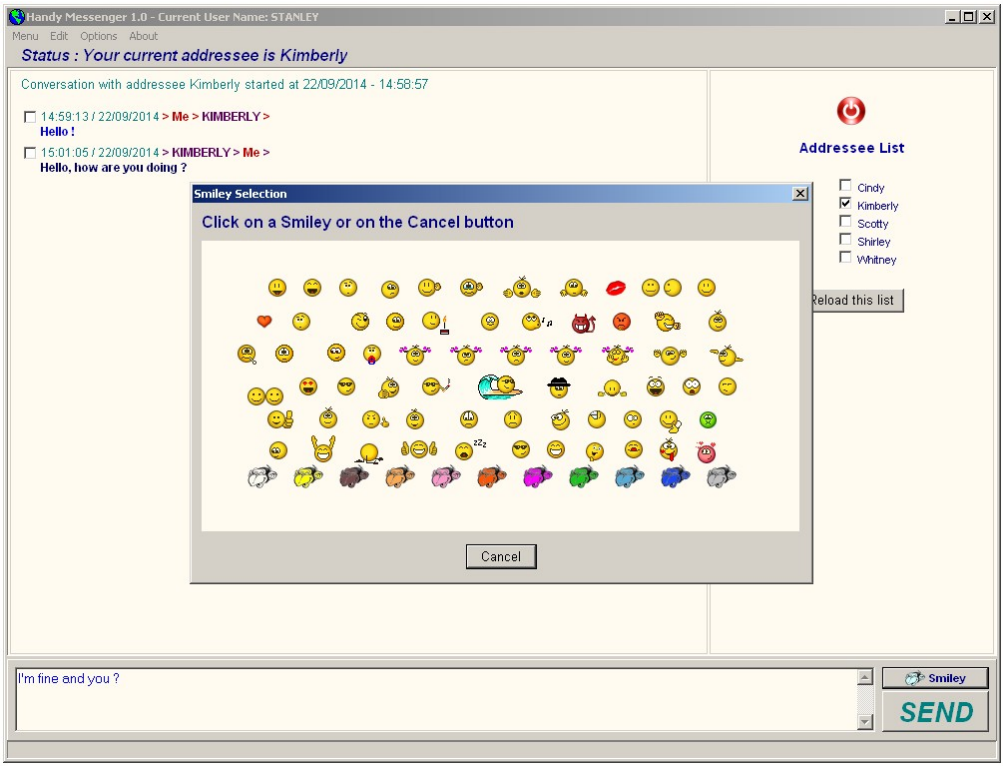
Lorsque vous avez choisi un correspondant, vous pouvez commencer à correspondre avec lui en écrivant vos messages dans la partie basse de l'application réservée à cet effet. Pour envoyer votre message, appuyez sur le bouton « Send ». A ce moment-là votre message apparaît dans la partie haute de l'application et il est envoyé immédiatement à votre correspondant pour autant que son Handy Proxy soit on-line. Si ce n'est pas le cas, comme nous le verrons plus loin, vos messages seront mis en attente (état « pending ») pour être envoyés ultérieurement. Il a été ajouté, pour suivre l'état de vos messages, une série d'indicateurs clignotants. Dans le cas ci-dessous le message est « Wait. », ce qui signifie « Waiting to be read » ou « en attente d'être lu » par votre correspondant qui a déjà reçu ce message. De plus, les nouveaux messages non encore lus sont apparaissent sur un fond coloré orangé.



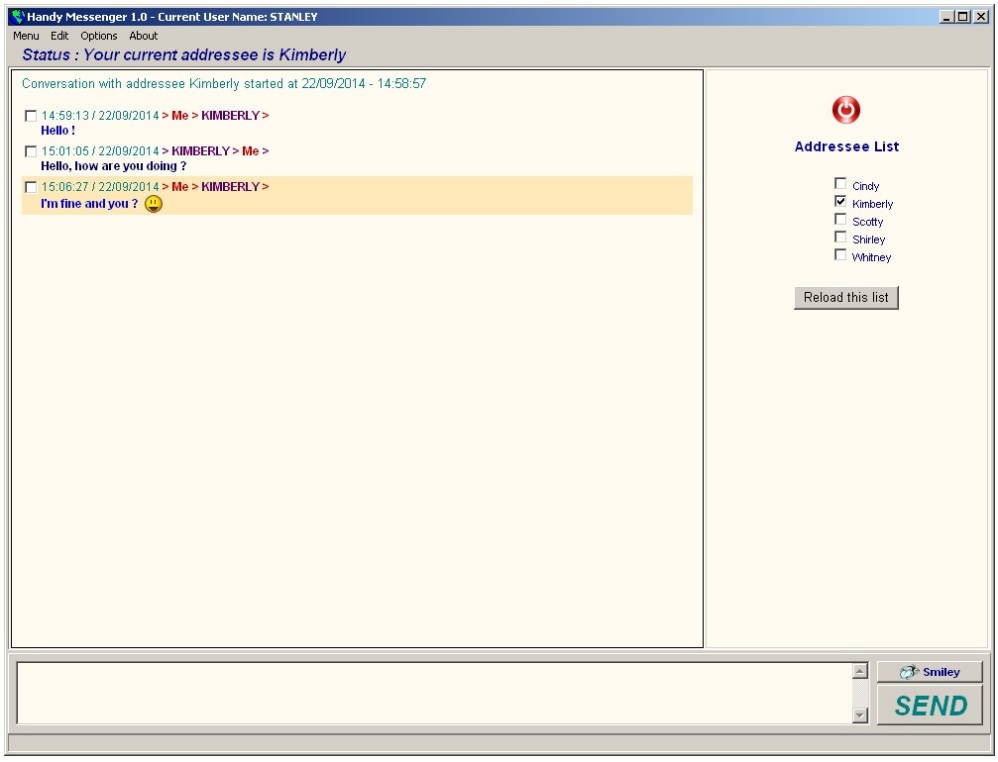
Dans l'écran suivant on peut voir que votre correspondant a lu le message, car son état n'est plus « en attente d'être lu ». On voit aussi que votre correspondant a répondu, le message en question est en état « New » (nouveau) et apparaît sur fond bleu. Pour votre correspondant, ce message restera dans l'état « en attente d'être lu » jusqu'au moment où vous aurez vu l'écran présenté ici.



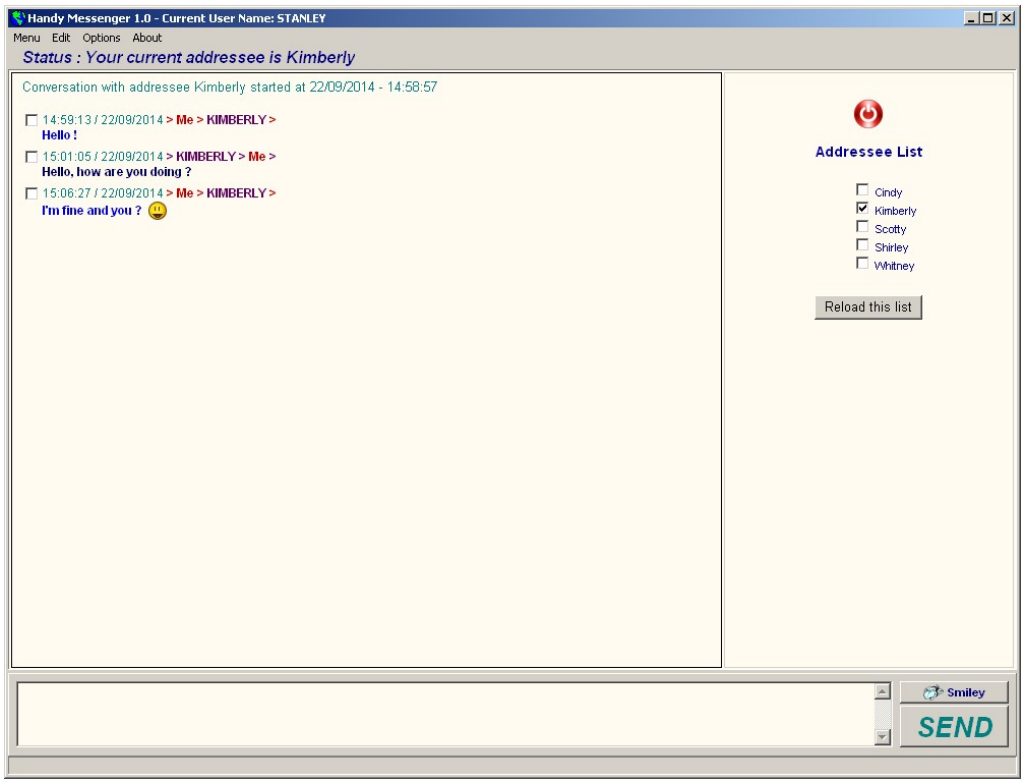
Vous avez à disposition une série de smileys pour agrémenter vos messages. Il suffit de cliquer sur le bouton « Smiley » en bas à droite pour que la fenêtre suivante s'ouvre, ce qui vous permet de sélectionner le smiley de votre choix.



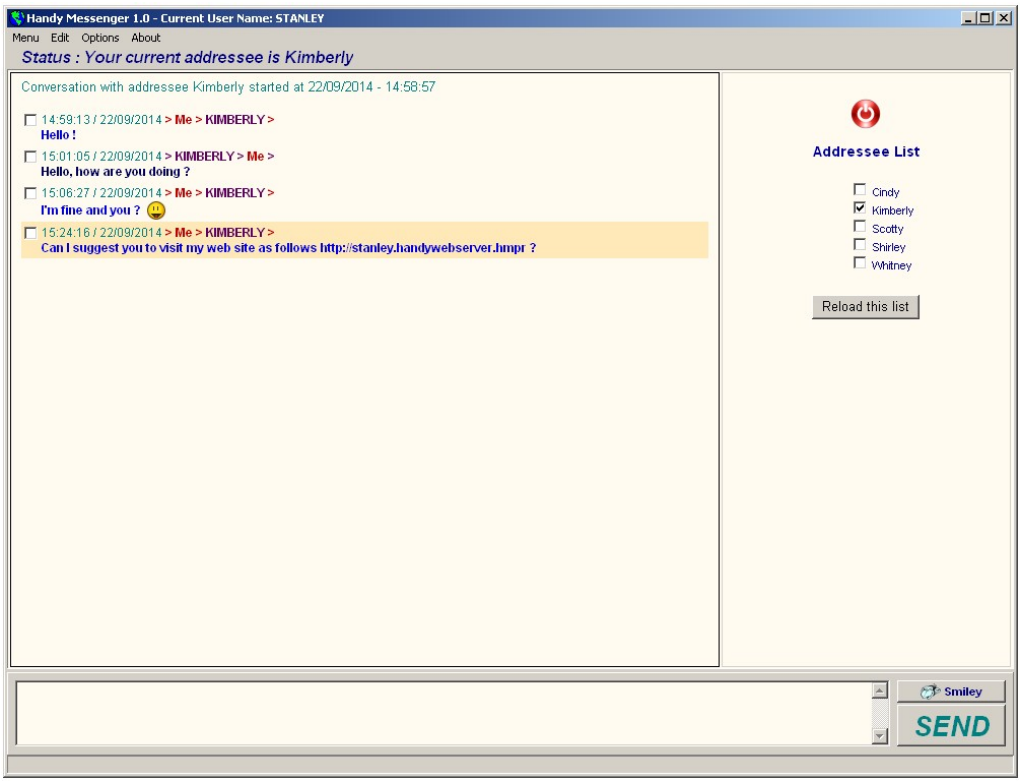
Ici, à nouveau, votre message est parti immédiatement à destination de votre correspondant :



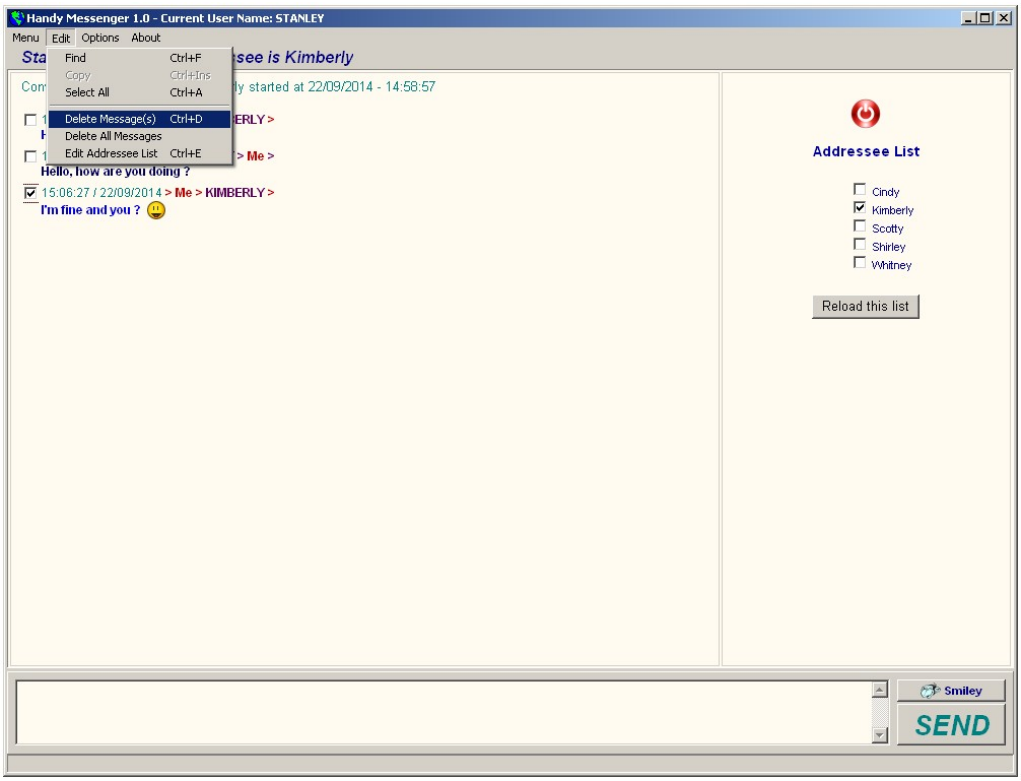
L’écran suivant vous indique que tous vos messages ont été envoyés et ont été lus par votre correspondant :



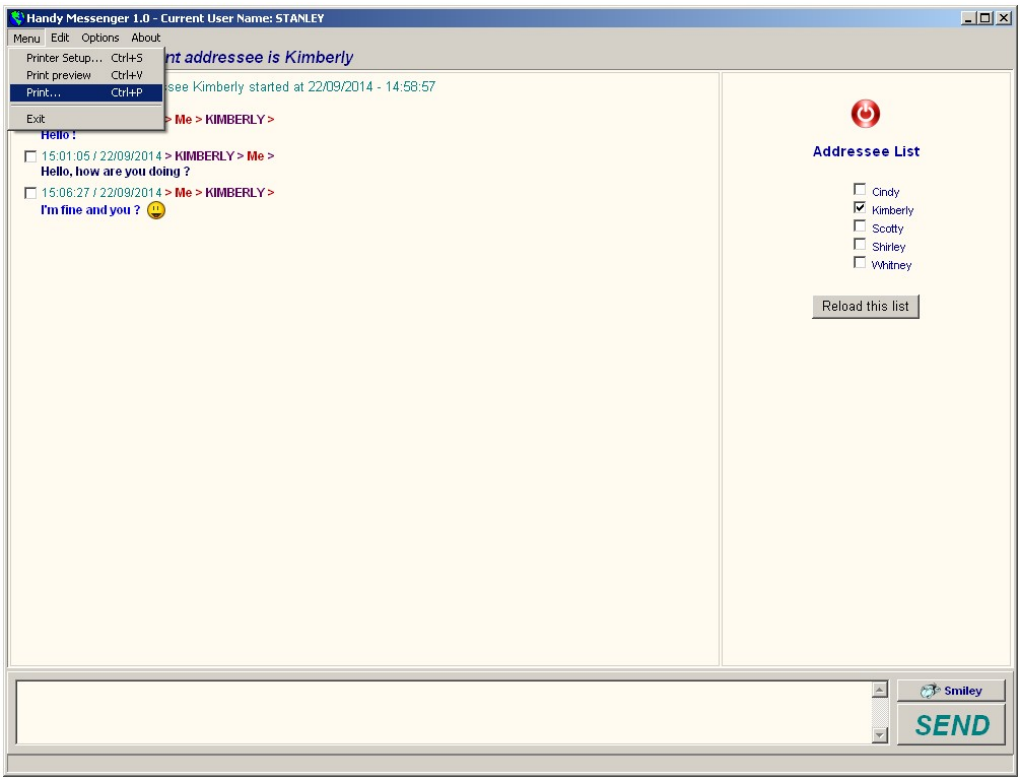
Il est possible d’envoyer des liens vers des pages ou sites web sur lesquels vous pouvez cliquer. Votre Handy Browser s’ouvrira alors sur la page appelée. En bas de l’écran apparaît le lien lorsque vous passez la souris dessus pour vous montrer que c’est bien celui qui est indiqué.



A tout moment, vous pouvez effacer la conversation entière ou un ou plusieurs messages y étant contenus. Il suffit de cocher les messages que vous voulez supprimer et d'aller dans le menu "Edit" pour utiliser la fonction "Delete Message(s)", également accessible via les touches Ctrl+D. Attention, contrairement à la fonction d'effacement de toute la conversation ("Delete All Messages"), la suppression de messages individuels n'appelle aucun sous-menu de confirmation et n'est pas réversible.

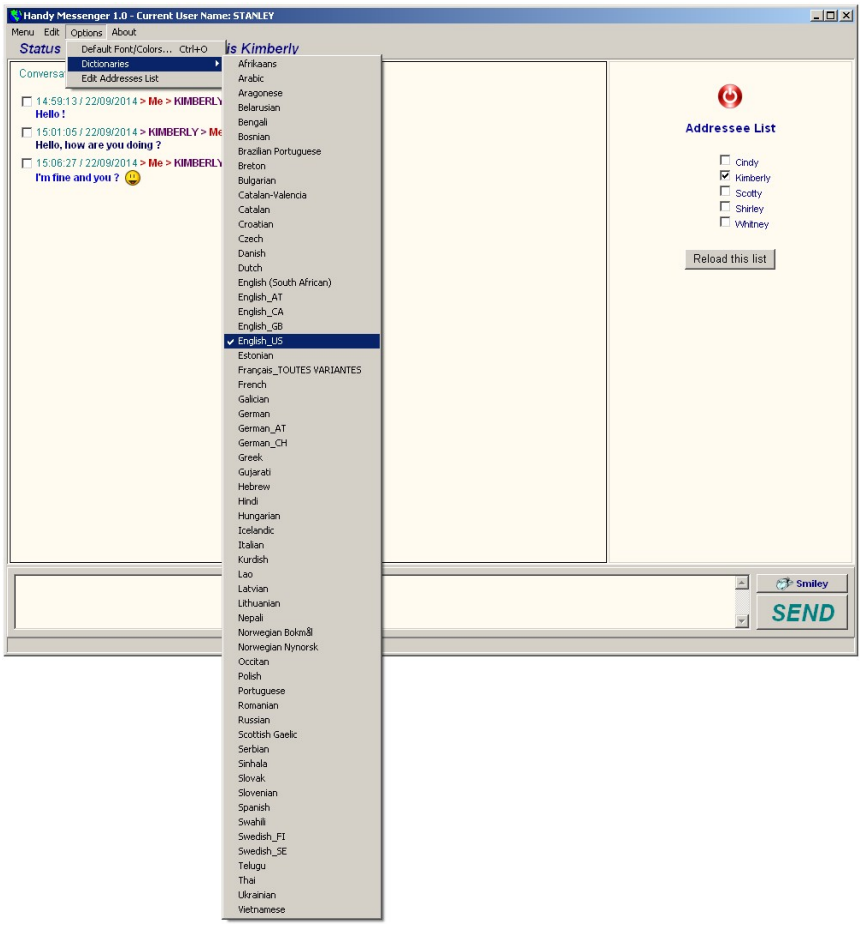


Vous pouvez imprimer toute la conversation si vous le souhaitez, comme illustré ci-dessous :

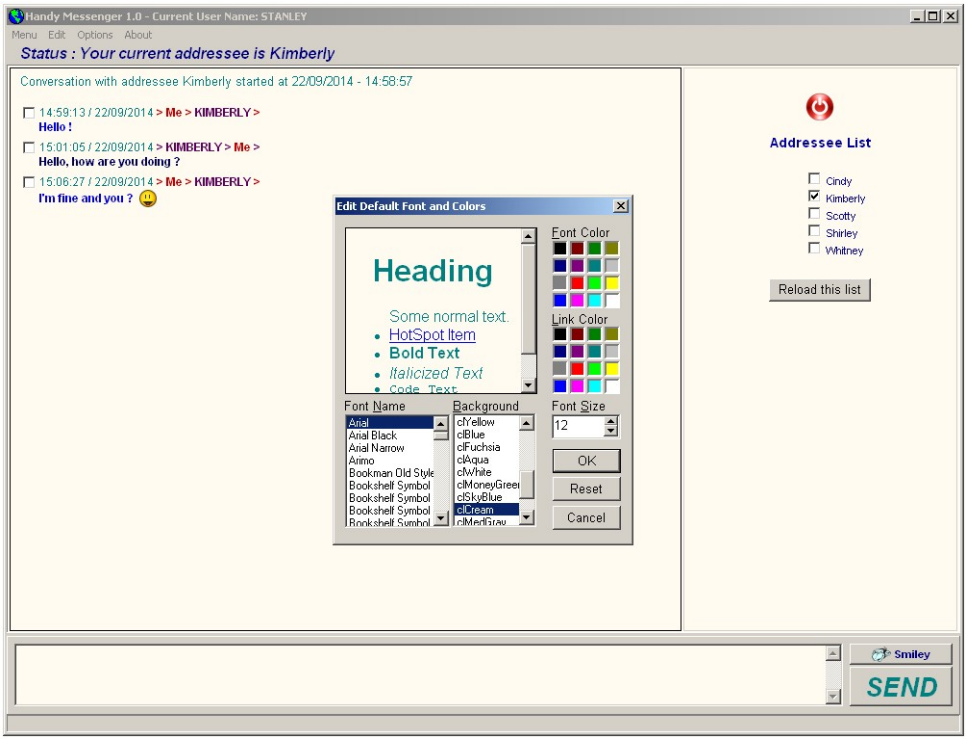


Lors de la rédaction de vos messages, vous avez à votre disposition une série de dictionnaires orthographiques que vous pouvez sélectionner. Dans votre message à la rédaction, si un mot apparaît souligné en rouge, vous pouvez cliquer dessus avec le bouton droit de la souris pour obtenir des suggestions si possible.

Dans le même menu “Options”, vous avez à disposition la fonction “Edit Addressees List” qui vous permet de modifier la liste de vos correspondants via le programme d’édition spécialement dédié à cette fonction, puisque ce fichier est encrypté et que son accès est protégé par un mot de passe. Veuillez vous référer au chapitre des fichiers de configuration pour la méthode à suivre.



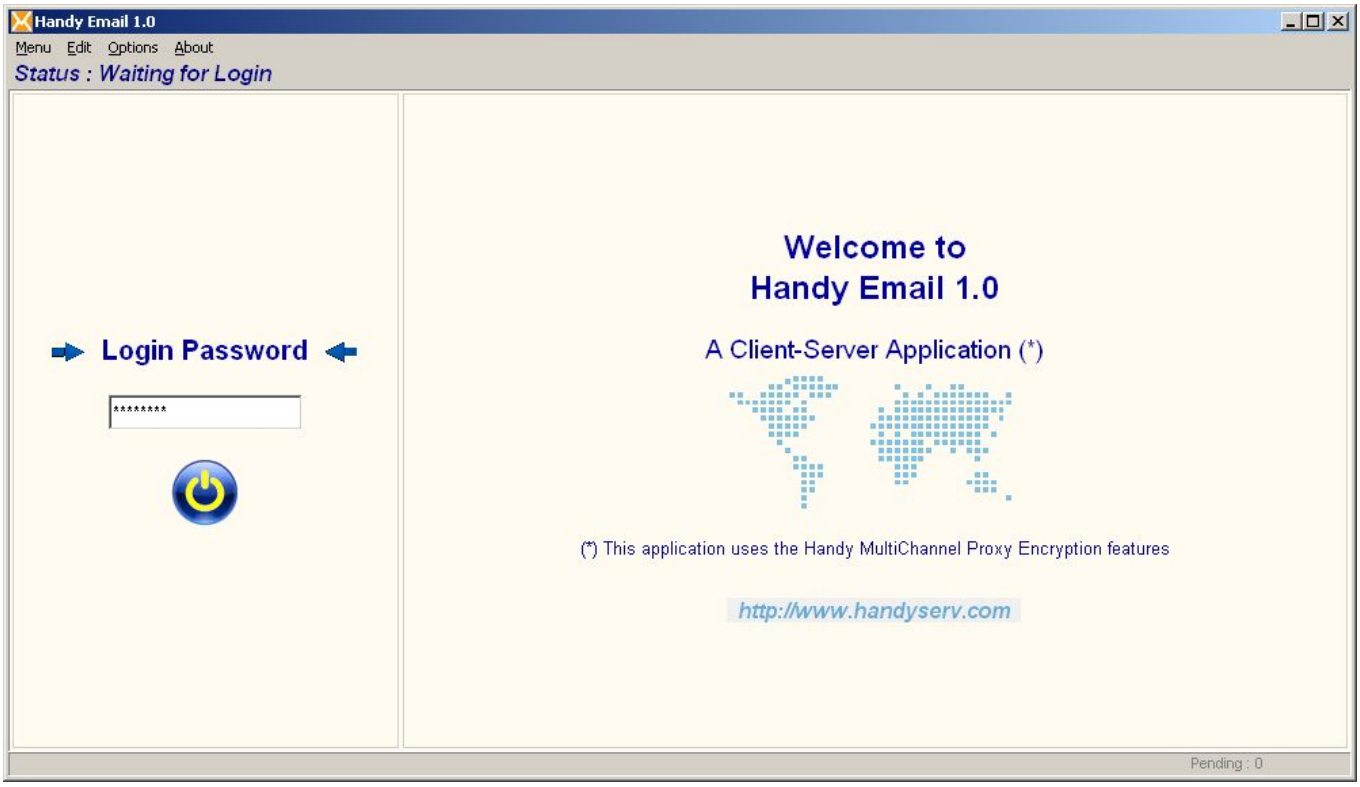
Vous pouvez également choisir la fonte de caractères et sa taille, sa couleur, ainsi que la couleur de fond des écrans de l’application.



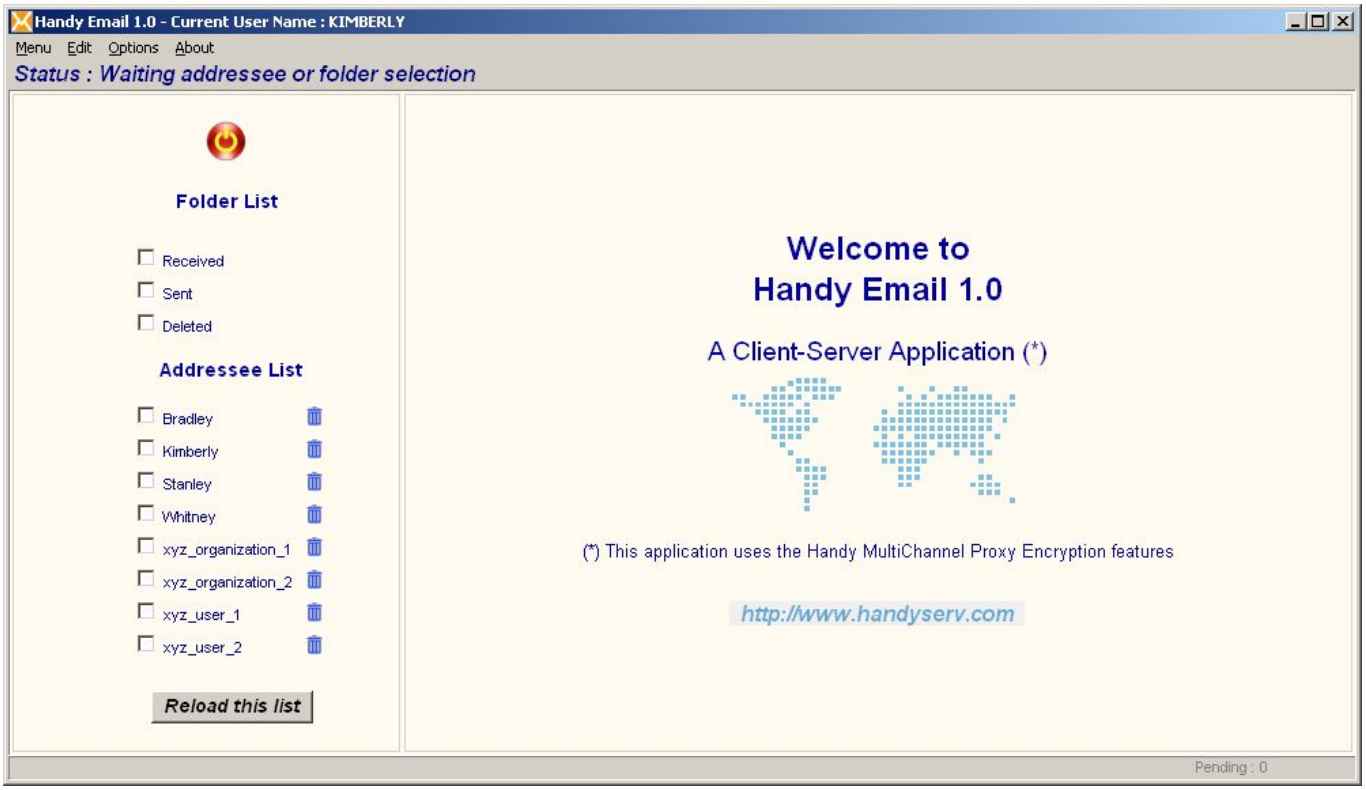
8.4. Handy Email

Comme expliqué dans l'introduction de ce chapitre, nous rappelons que ce programme d'échange de messages est entièrement sécurisé et ne fonctionnera qu'entre utilisateurs de Handy Proxy. Il faut donc impérativement que votre Handy Proxy soit opérationnel dans votre PC, sans quoi ce programme ne fonctionnera pas puisqu'il ne disposera pas de son canal de communication sécurisé et encrypté.

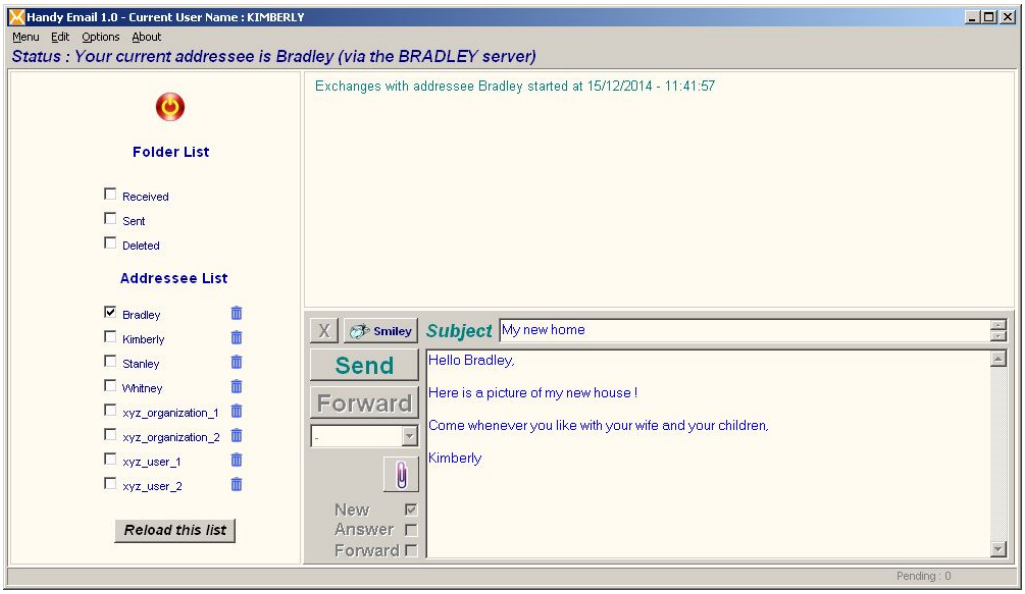
Voici l'écran d'accueil qui vous suggère de vous identifier par votre mot de passe (voir les fichiers de configuration à ce sujet) :



Après vous être identifié, vous obtiendrez la liste de vos correspondants et la liste des différents dossiers disponibles :

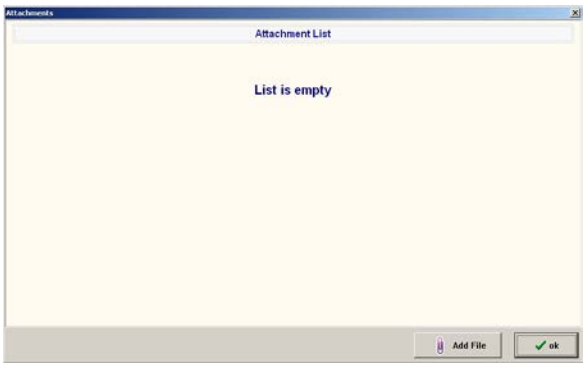


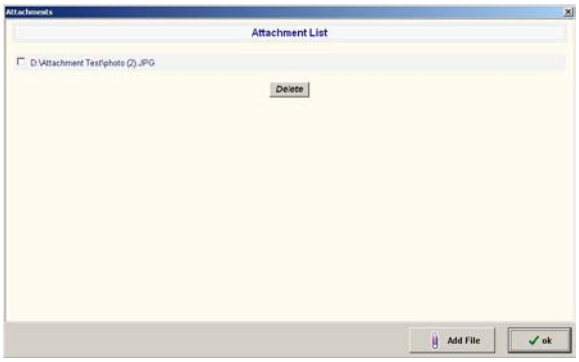
Lorsque vous avez choisi un correspondant, vous pouvez commencer à correspondre avec lui en écrivant vos messages dans la partie basse de l'application réservée à cet effet. Pour envoyer votre message, appuyez sur le bouton « Send ». A ce moment-là votre message apparaît dans la partie haute de l'application et il est envoyé immédiatement à votre correspondant pour autant que son Handy Proxy soit on-line. Si ce n'est pas le cas, comme nous le verrons plus loin, vos messages seront mis en attente (état « pending ») pour être envoyés ultérieurement.

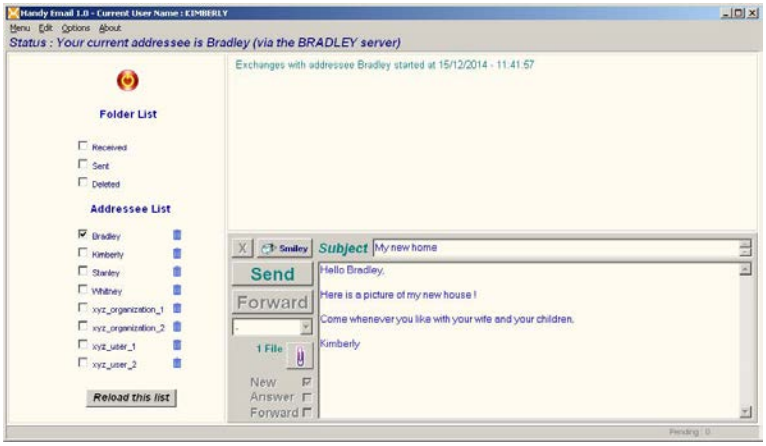


Quand vous écrivez un message, vous pouvez y joindre un ou plusieurs fichiers (images ou autres, tous les formats sont supportés). Si vous cliquez sur le bouton "trombone", voici les écrans que vous obtiendrez. Il suffit de cliquer sur le bouton "Add File" (ajouter fichier) et de sélectionner le ou les fichiers que vous souhaitez envoyer. A tout moment vous pouvez modifier cette liste en supprimant (bouton "Delete") ou ajoutant un autre fichier à la liste. Confirmez votre sélection (bouton "OK"). Vous verrez apparaître le nombre de fichiers annexés à côté du bouton "trombone".

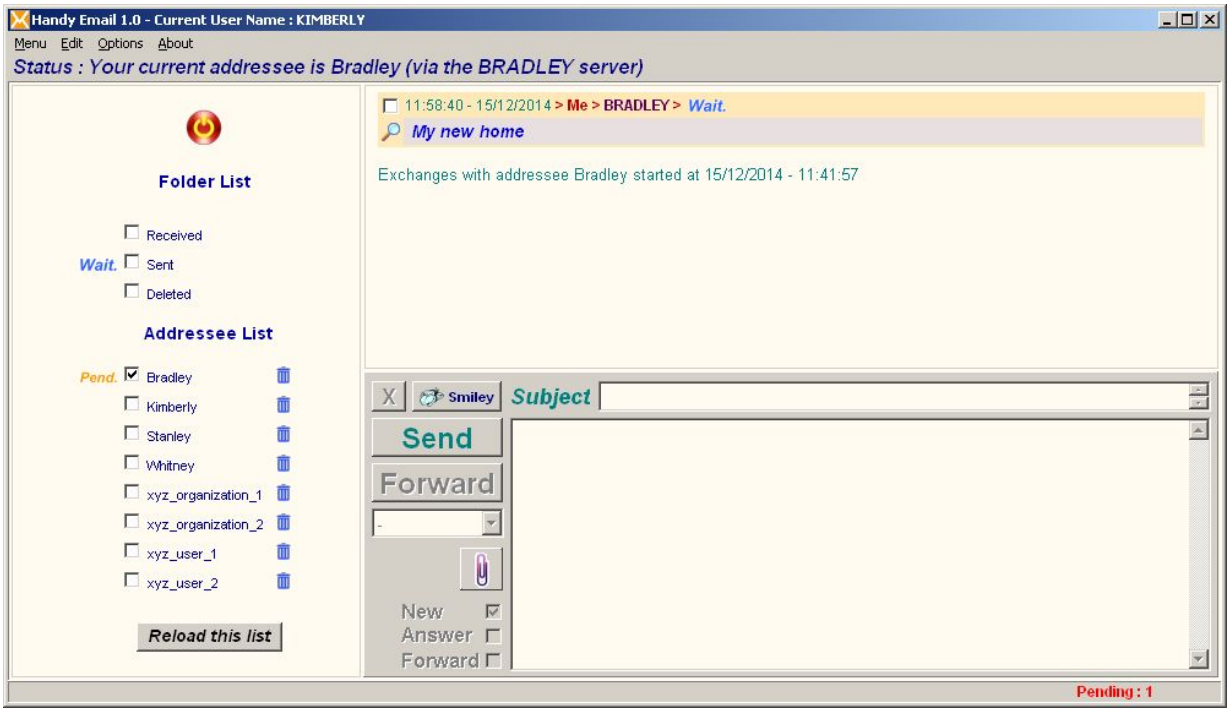
De même que les messages en eux-mêmes qui seront encryptés, vos fichiers originaux et joints à ces messages seront recopiés dans un répertoire temporaire de votre Handy Proxy et encryptés avant d'être envoyés à vos correspondants, de telle manière que ces fichiers ne circuleront pas en clair entre vous et votre/vos correspondant(s). Le nom du fichier original et son format n'apparaîtront chez votre correspondant qu'au moment où il voudra visualiser l'image (si c'en est une) ou sauver le fichier sur son disque dur.



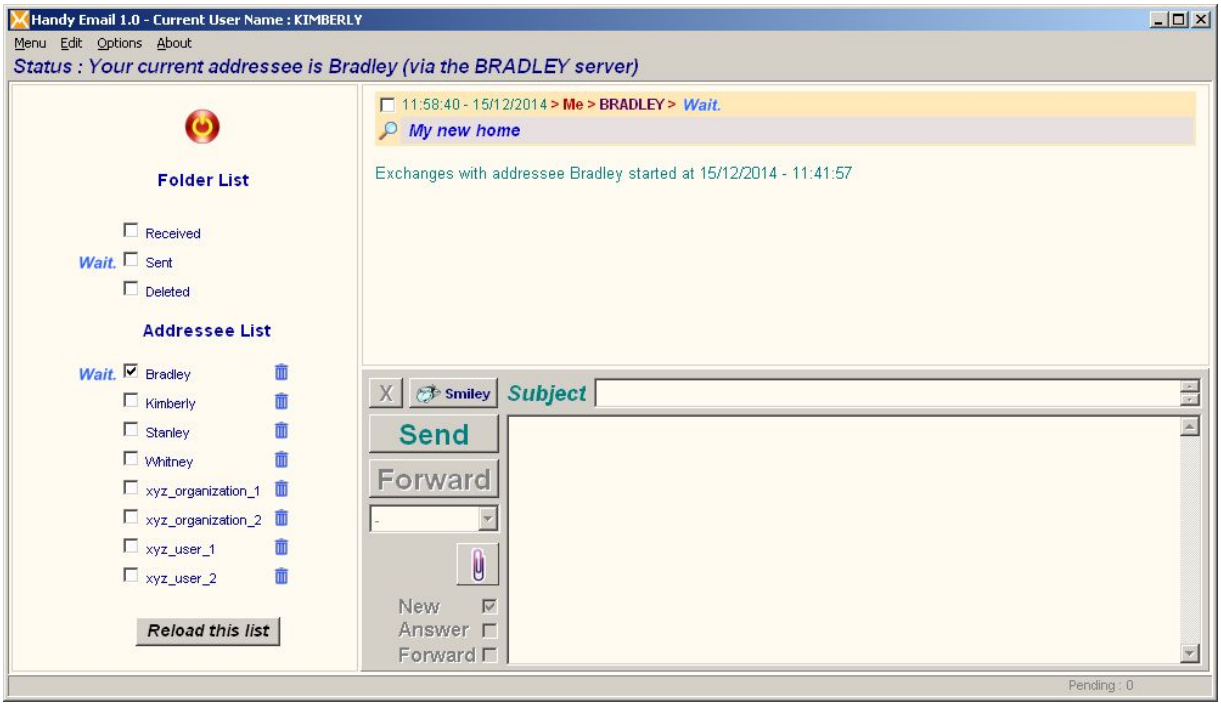




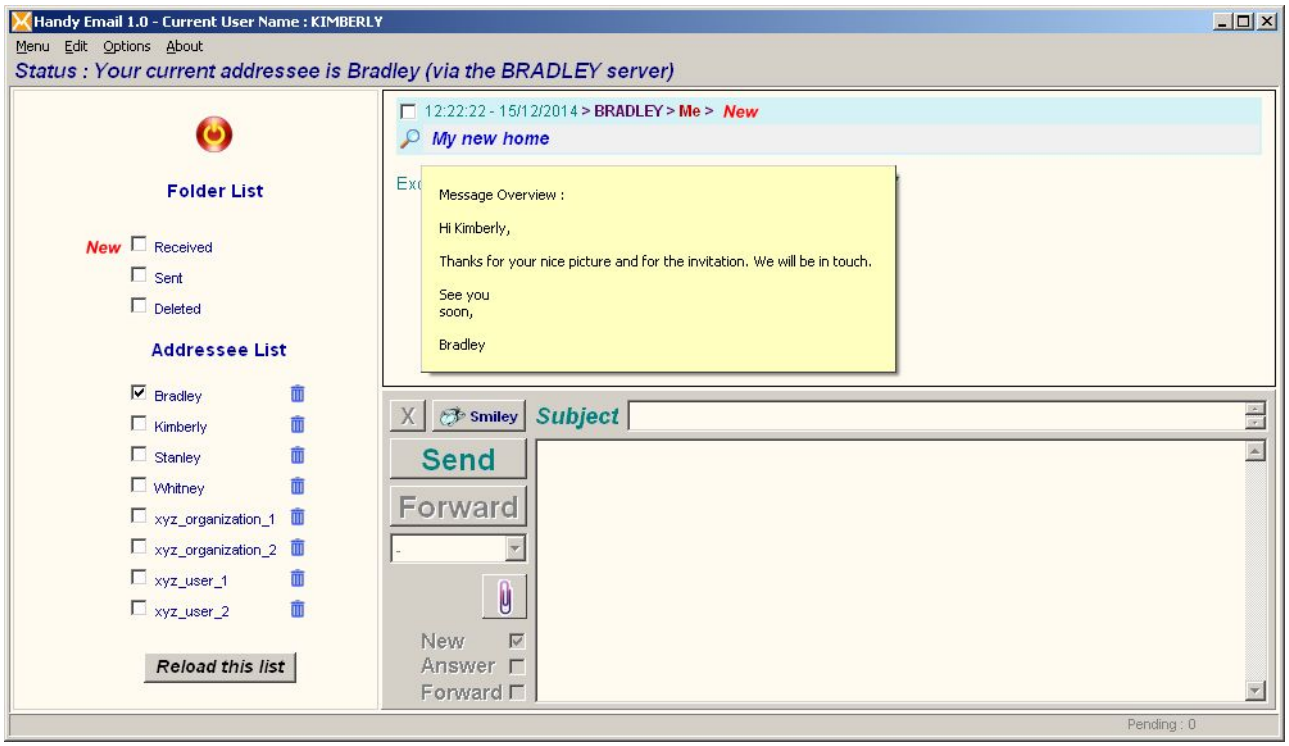
Lorsque vous aurez cliqué sur le bouton “Send” (“envoyer”), les fichiers en annexe seront d’abord transmis vers le serveur de votre correspondant. Pendant ce temps, votre message est en attente jusqu’au moment où toutes les annexes seront transmises. Ces annexes et ce message sont chez vous, et le resteront aussi longtemps que toute l’émission du message dans son ensemble n’est pas finalisée. Pour vous aider à suivre l’état de vos messages, il suffit de se référer à l’indicateur situé en bas à droite de l’écran ci-dessous. Si cet indicateur n’est pas à zéro, cela signifie que vous avez des messages encore chez vous et non transmis. Ceci veut dire, et c’est important, qu’il ne faut pas fermer les applications Handyserv aussi longtemps que des messages ne sont pas partis ; dans le cas contraire, ils ne pourront être envoyés qu’au moment où vous relancerez vos applications Handyserv.



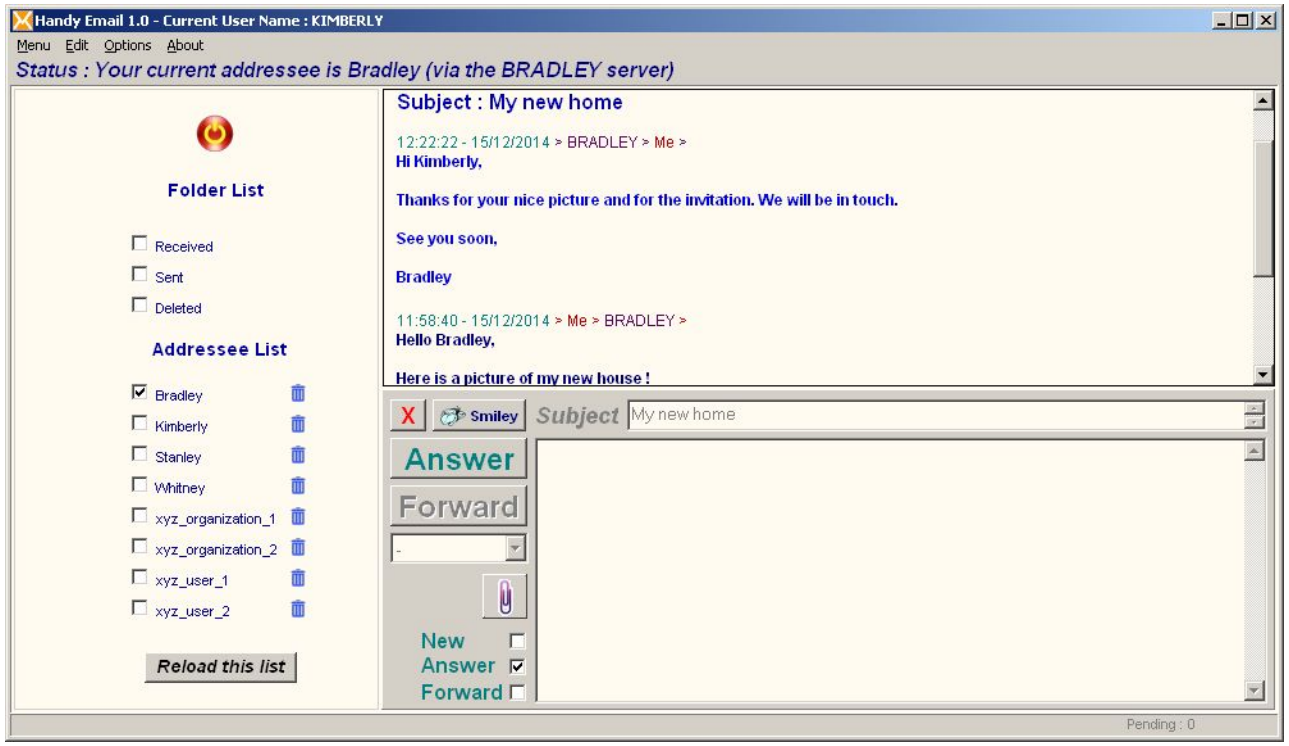
L’écran suivant vous indique que votre message a été entièrement transmis, avec ses annexes, vers le serveur de votre correspondant. En effet, l’indicateur “Pending” en bas à droite de l’écran est à zéro (et est grisé).



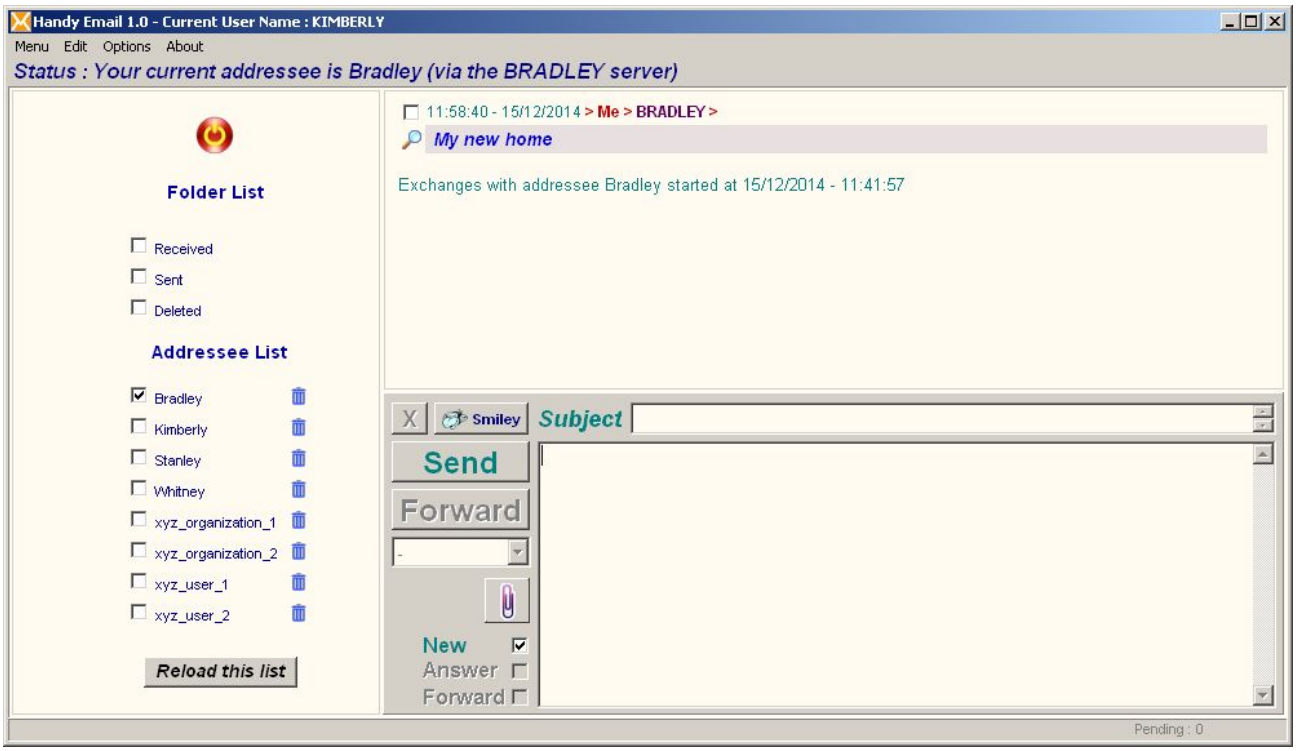
Mettons-nous maintenant au niveau de votre destinataire et du message qu'il aura reçu de votre part. Celui-ci lui sera indiqué avec le voyant clignotant "New" ("nouveau") à côté du dossier "Received" ("reçu"). Votre correspondant pourra visualiser ce message en passant sa souris sur la loupe qui se trouve à côté du sujet du message dans la liste de ceux-ci.



Lorsque votre correspondant cliquera sur le sujet du message, ce dernier s'ouvrira et il pourra en lire le contenu. Un accusé de réception partira à votre attention à ce moment-là.

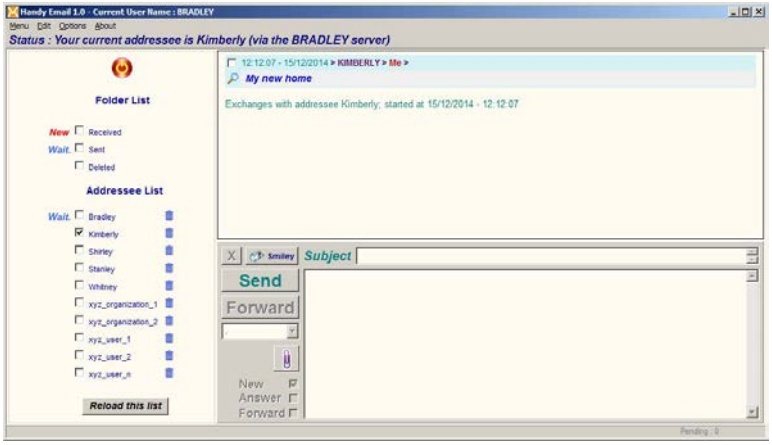


Lorsque votre correspondant aura lu votre message, l'état "Waiting" ("en attente") de celui-ci chez vous disparaît.

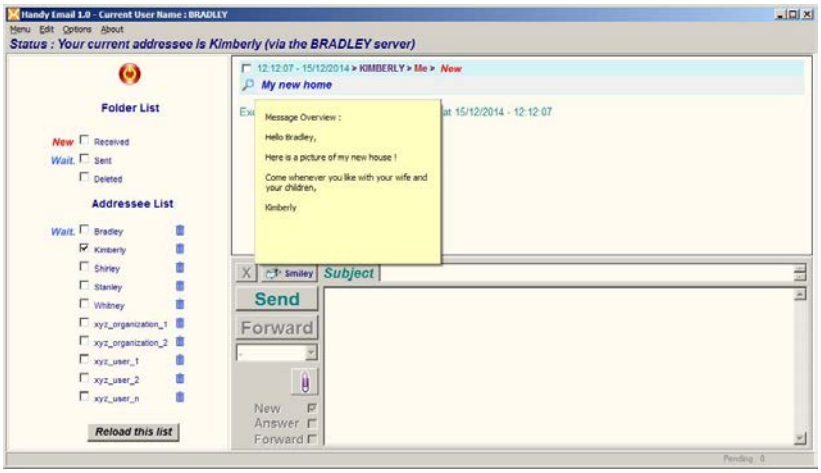


Revenons à votre correspondant qui a reçu votre message et un fichier en annexe. En cliquant sur le bouton "image" ou "fichier" contenu dans le corps du message, il obtient l'écran suivant qui lui permettra de visualiser l'image si c'en est une et/ou de sauver le fichier sur son disque dur. C'est à ce moment-là que le fichier encrypté chez vous sera décrypté, et son nom original apparaîtra à votre destinataire.

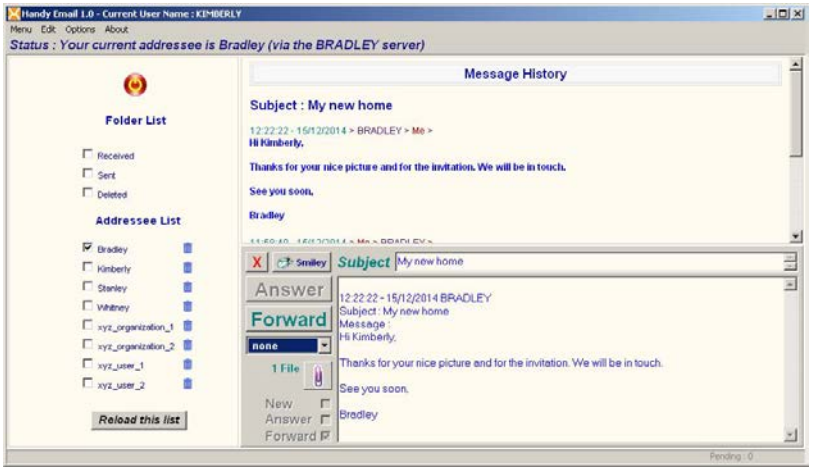
Imaginons que votre correspondant souhaite vous répondre et qu'il rédige un message qu'il fait partir. Voici ce que vous obtiendrez, càd un nouveau message en attente d'être lu par vous-même :



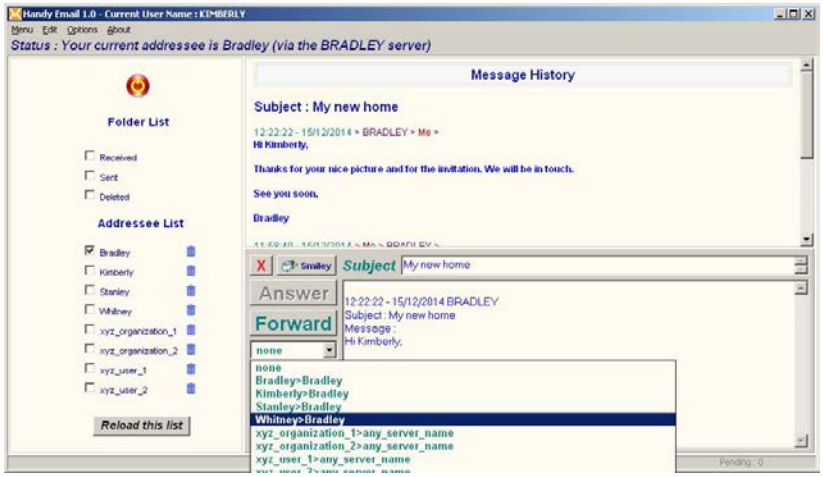
Comme expliqué précédemment, vous pouvez prévisualiser le contenu de ce message qui vous revient en passant la souris sur la loupe :



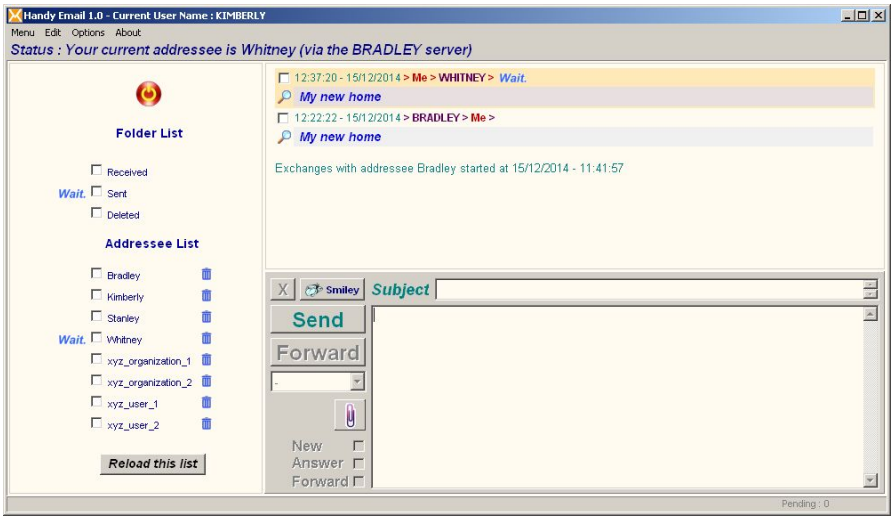
Si vous souhaitez retransmettre un message reçu et ses éventuelles annexes à un autre de vos destinataires, voici comment procéder. Tout d'abord, cochez l'option "Forward" ("faire suivre") en bas de l'écran, vers le milieu.



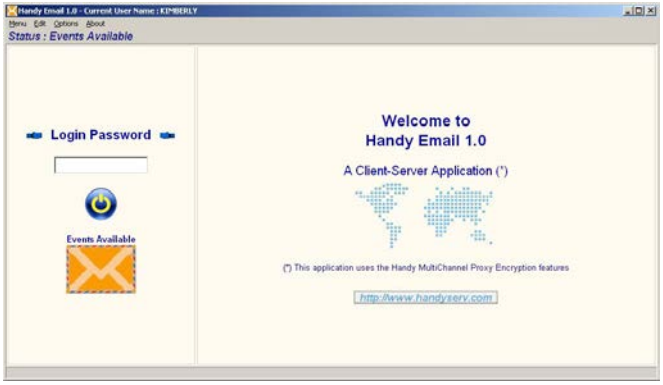
Ensuite, sélectionnez votre destinataire dans la liste déroulante des destinataires accessibles. Vous pouvez également, bien entendu, ajouter du texte.

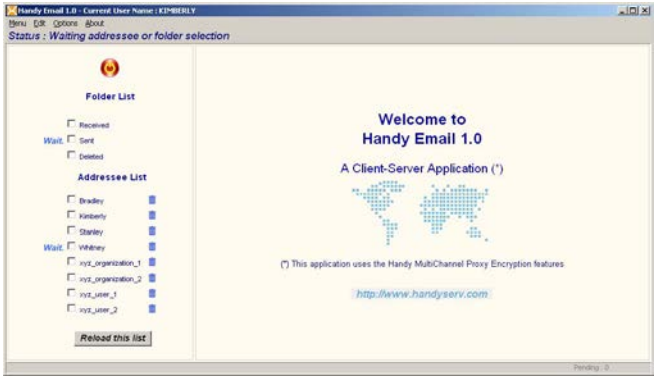


Le message ainsi retransmis se trouve alors parmi vos messages envoyés (“Sent”), en attente de lecture par votre correspondant.

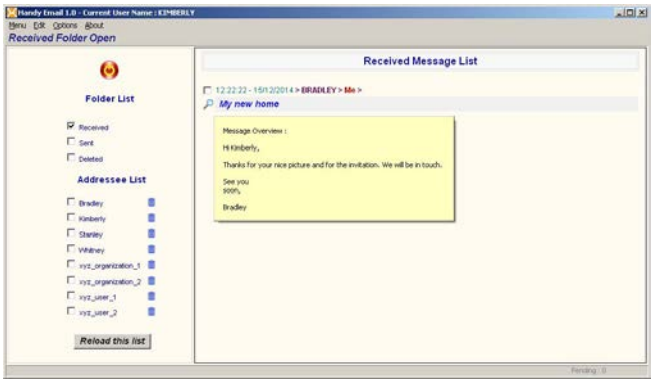


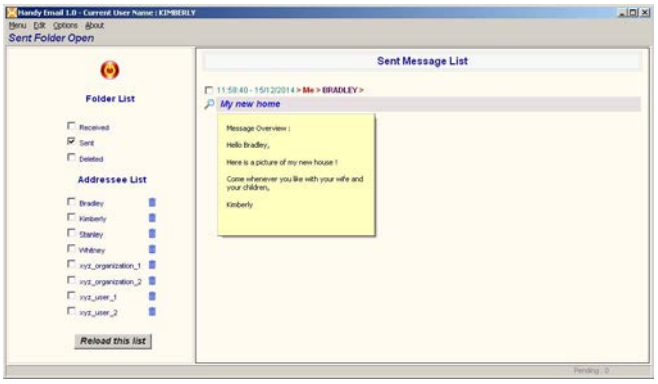
Voici ce qui apparaît sur l’écran d’accueil en cas de réception d’un message ou événement : l’icône “enveloppe” clignotante vous en avertit. Après avoir introduit votre login, vous avez accès à la liste des événements.





A partir des dossiers “Received” et “Sent”, vous pouvez aussi prévisualiser le contenu d’un message, l’ouvrir, y répondre et/ou le faire suivre à d’autres correspondants.





9. Les fichiers de configuration du Handy Proxy

9.1. Fichier « Handy Proxy Master Configuration » (Multichannel_Proxy_Master_Config.def)

Pour ouvrir ce fichier cliquez sur le bouton ci-dessous disponible dans l'écran principal de votre Handy Proxy, password d'accès par défaut : 1234.

Ce fichier doit être placé dans la directory **principale** de l'application. Il est automatiquement créé et encrypté lors du premier lancement de handyproxy.exe s'il n'est pas trouvé.

Vous devez impérativement respecter scrupuleusement la syntaxe de ce fichier, sans quoi les paramètres ou données ne seront pas compris. L'édition de ce fichier peut se faire via l'écran principal du Handy Proxy et le bouton « Edit Master Config File ».

Rôle de ce fichier :

Ce fichier contient les paramètres généraux de votre Handy Proxy. Ce fichier sera pris en compte au moment du lancement de votre Handy Proxy. En cas de modification, vous devez refermer le programme Handy Proxy et le relancer.

D'éventuelles remarques importantes sont insérées EN VERT dans le texte ci-dessous ; il ne s'agit ni de commentaires dans ce fichier ni de paramètres spécifiques. Il s'agit d'explications complémentaires indispensables à la bonne compréhension.

//==
// 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
Ce password vous permet de protéger ce fichier de configuration contre toute modification et d'ainsi pouvoir diffuser ce fichier auprès de vos amis ou de votre organisation tout en ayant le contrôle sur la configuration qui sera utilisée autour de vous. **Attention : si vous perdez le password, vous n'aurez plus jamais accès à ce fichier de configuration, et ceci est irréversible !** Nous ne fournissons en effet pas le moyen d'outrepasser ce password. Ce password protège également l'accès aux fichiers de sous-configuration ainsi qu'au fichier de configuration des serveurs et destinataires Handy Messenger et Handy Email. L'ensemble de ces fichiers risque de devenir non modifiables ni vous perdez ou oubliez votre password.
La valeur de ce password par défaut est : 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
Ce password est celui qui autorise l'ouverture des applications susmentionnées. Si vous diffusez ce fichier principal de configuration à vos utilisateurs dans votre réseau par exemple, ceux-ci pourront utiliser ces applications sans pouvoir changer l'état de configuration ainsi que le nom de leur Handy Proxy (voir le fichier « Handy_Proxy_Configuration.cfg » dans lequel il est possible d'indiquer un nom qui remplacerait celui indiqué ci-après sous le libellé « Proxy_Name »).
La valeur de ce password par défaut est : 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
Chaque Handy Proxy doit avoir son propre nom, différent de tous les autres. Lors du lancement de celui-ci, votre Handy Proxy va demander si le nom choisi est déjà utilisé ou pas par un autre utilisateur. Si ce n'est pas le cas, le nom choisi vous appartiendra à titre définitif. Vous avez à votre disposition 30 caractères pour ce nom, par exemple nous vous suggérons dans ce nom de commencer par un préfixe suivi des initiales ou du nom de chacun des utilisateurs de votre famille ou de votre entreprise, par exemple mycompany-myname, mycompany-thisname,…
ATTENTION : si votre Handy Proxy est un routeur pour d'autres utilisateurs et/ou si votre configuration est également utilisée comme serveur de messagerie, vous ne pouvez pas changer le nom de votre Handy Proxy puisque des utilisateurs vont utiliser votre machine comme routeur ou serveur. Si ce nom change, ils ne pourront plus vous retrouver et devront eux-mêmes se reconfigurer, ce qui serait ingérable.

//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
Chaque Handy Proxy a besoin d'une identité unique. Cette fonction est automatiquement réalisée lors du premier lancement de votre Handy Proxy. Il est toutefois possible de créer un groupe d'utilisateurs pour votre famille et votre entreprise. Vous pouvez alors remplacer ce nom unique par un nom de votre choix, par exemple 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
Ce paramètre est fondamentalement important : il va vous permettre de définir un plus haut degré de sécurité dans vos échanges entre Handy Proxy. Vous pouvez alors, pour ce paramètre, définir une partie de la clé d'encryption avec laquelle vos données vont être encryptées. Cette clé privée NE SERA JAMAIS ECHANGEE entre votre Handy Proxy et ceux qui voudraient communiquer avec celui-ci. Il est donc indispensable que vos correspondants connaissent cette clé, sans quoi les Handy Proxy ne pourront jamais se comprendre. Vous devez alors faire connaître la clé que vous utilisez à vos correspondants par un moyen autre que ceux qu'offrent les Handy Proxy. A vous de choisir le meilleur moyen pour partager cette clé d'encryption. Evitez si possible de l'envoyer par un moyen Internet qui pourrait ainsi diminuer sa confidentialité. Si vous n'utilisez pas cette fonction, c'est une clé d'encryption par défaut qui sera utilisée, et donc commune à tous les Handy Proxy ne faisant pas non plus appel à cette fonction. Vos correspondants devront paramétrer convenablement leur Handy Proxy pour qu'ils utilisent la même clé que vous, sans quoi il n'y aura pas d'échanges possibles.

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

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

//Allow to show Handy Messaging Server status (yes/no)
Allow_to_show_Messaging_Server_status=yes
Ce paramètre permet de voir ou cacher l'état de vos serveurs de messagerie. Si ce paramètre n'est pas actif (« no »), vous pourrez quand même voir l'état de ces serveurs à partir des applications Handy Email ou Handy Messenger pour autant que vous ayez accès à celles-ci via le password de protection. Ainsi, la confidentialité concernant vos destinataires et serveurs de messagerie sera maximale.

//Authorize Handy Proxy to modify automatically the local Windows Proxy Settings (yes/no)
Automatic_Windows_Proxy_Setting=yes
Nous conseillons d'utiliser cette fonction en mode automatique pour ne pas oublier de lancer votre Handy Proxy lorsque votre PC est mis en fonctionnement. N'oubliez alors pas de placer le module handyproxy.exe dans le startup de Windows afin qu'il soit lancé systématiquement au démarrage de 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
Ce paramètre par défaut conviendra en général. En cas de nécessité vous pouvez le modifier, principalement le port (8080 étant un exemple) mais en général il restera tel quel. Ce paramètre sera mis à disposition de Windows en tant que paramètre de proxy.

//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
Il est possible qu'un jour le lien vers le site web qui héberge la base de données des utilisateurs du Handy Proxy soit modifié. Nous avons donc prévu la possibilité de modifier ce paramètre. Vous serez averti, le cas échéant, d'une modification via l'écran principal de votre Handy Proxy. En l'absence d'un avis préalable il ne faut en aucun cas modifier ce paramètre, sans quoi la base de données ne sera pas retrouvée ! Ce paramètre permet une personnalisation très importante de votre configuration, voire de la rendre totalement indépendante de celle fournie par défaut. Pour plus d'informations à ce sujet, veuillez vous référer au chapitre 10 de ce manuel.

//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
Ce paramètre permet de passer par un autre proxy pour aller rechercher dans la base de données de Handyserv les informations nécessaires à la configuration de votre Handy Proxy. Voir à ce sujet le chapitre 1.3.3. du présent manuel qui vous explique plus longuement ce qu'il est possible de faire avec ces deux paramètres.

//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
Voir à ce sujet le chapitre 1.3.3. du présent manuel qui vous explique plus longuement ce qu'il est possible de faire avec ce paramètre.

//Allow to dynamically modify the browser output channel (yes/no)
Allow_Browser_Channel_Hot_Switch=yes
Voir à ce sujet le chapitre 1.3.3. du présent manuel qui vous explique plus longuement ce qu'il est possible de faire avec ce paramètre.

//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
Par défaut si un e-mail est accompagné d'une pièce jointe qui est une image, le programme Handy Email ouvrira le programme indiqué pour visualiser l'image en question. Vous pouvez indiquer ici un autre programme de visualisation avec son chemin (par exemple le programme bien connu IrfanView ou toute autre application de visualisation de fichiers graphiques).

//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\
Par défaut est fournie une version des programmes PHP. Si elle ne vous convient pas parce que vous en utilisez déjà une autre, vous pouvez indiquer ici son chemin d'accès.

//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
Ce paramètre permet de définir un répertoire sur un disque dur différent de celui que votre Handy Proxy utilise par défaut pour sauvegarder tous les fichiers clients et serveurs de la fonction Handy Messaging Server. Vous pouvez dès lors sauvegarder tous ces fichiers sur un autre disque que celui où fonctionne le Handy Proxy, par exemple vous pouvez sauver ces fichiers sur un disque qui est sauvegardé tous les jours ou un système NAS qui serait en partage sur votre réseau.
***Les fichiers de la base de données de votre Handy Messaging Server sont les seuls qu'il faut impérativement sauvegarder afin qu'aucun message ne soit perdu en cas de crash du PC qui hébergera les fonctions du Handy Proxy**. Ce paramètre est donc très important puisqu'il vous permet de sauvegarder tous ces fichiers ailleurs que sur le disque dur local du PC hôte. En utilisant cette option, vous pourriez très bien avoir deux PCs configurés tous les deux en Handy Proxy exactement de la même manière et avec la même licence, l'un étant actif et l'autre éteint en attente d'une éventuelle panne du premier. Si une telle panne arrivait il vous suffirait de débrancher le premier PC et d'activer le second de telle manière que votre messagerie soit opérationnelle dans les secondes qui suivent. En alternative à un second PC en attente, il est possible d'installer votre Handy Proxy sur une clé USB qui pourrait être donc mise en place sur un autre PC en cas de panne. Toutefois, il faut alors tenir compte du fait que le PC de remplacement doit être accessible par les autres utilisateurs (voir pour cela le chapitre 2.1 « Comment donner accès à votre Handy Proxy à d'autres utilisateurs")*
ATTENTION : deux ou plusieurs Handy Messaging Servers distincts ne peuvent pas partager le même répertoire sur un même disque. Il faut les dissocier et rendre chacune des bases de données des différents serveurs totalement indépendantes. Ce paramètre ne concerne que les fichiers du Handy Messaging Server uniquement.

//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
Ce paramètre sert à centraliser sur le disque et répertoire de son choix, local ou en réseau, tous les fichiers de paramétrage autres que les fichiers de configuration du Proxy lui-même qui sont les fichiers Multichannel_ProxyMaster_Configuration.def et Multichannel_Proxy_Configuration.cfg et quelques autres fichiers personnels à la configuration. Ceux-ci resteront locaux et placés à l'endroit où est installé le Handy Proxy (il s'agit principalement des fichiers qui concernent le Handy Web Server et de tous les fichiers temporaires).

Ce paramètre permet donc, dans un réseau local, de donner accès à une configuration commune à tous les utilisateurs qui auraient accès au même disque et répertoire d'un disque dur partagé en réseau. Tout changement dans les fichiers ainsi mis en commun serait donc mis à disposition de tous ses utilisateurs. Ces fichiers ainsi partagés sont les fichiers de filtrage ou de routage forcé d'URLs dont voici la liste : Proxy_Local_URL_Filter_File.DEF, Proxy_Routing_Table.DEF, Proxy_White_URL_List.DEF, le fichier hmp_conf.pac (voir les points suivants du présent chapitre pour plus de détails) et le fichier Communication_Server_and_User_List.DEF (liste des serveurs et des destinataires pour les applications Handy Email et Handy Messenger, voir chapitre 8.2).

L'accès à ces fichiers partagés peut être protégé par un mot de passe (voir paramètre Handy_Web_Server_Remote_Management_ Password).

Il est tout à fait possible de créer des répertoires de partage des fichiers du Handy Proxy par groupe de travail, par département ou encore d'une manière globale. Pour réaliser une configuration par groupes de personnes, il est suggéré de préconfigurer chaque groupe à partir d'un même Handy Proxy et de diffuser le fichier Multichannel_ProxyMaster_Configuration.def auprès de ces groupes, et éventuellement de faire la même chose avec le second fichier Multichannel_Proxy_Configuration.cfg. Ensuite, la création de tous les autres fichiers se fera lors du premier lancement du Handy Proxy sur un PC sauf pour les fichiers déjà existants comme ceux qui seraient déjà mis en partage.

***ATTENTION :** les fichiers concernés par ce paramètre ne sont pas protégés par des accès concurrents. Il sera possible de les modifier à partir de chacun des Handy Proxy utilisateurs pour autant que le mot de passe d'accès leur soit connu (s'il existe).*

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

9.2. Fichier « Handy Proxy Configuration » (par défaut : Handy_Proxy_Configuration.cfg)

Pour ouvrir ce fichier cliquez sur le bouton ci-dessous disponible dans l'écran principal de votre Handy Proxy, password d'accès par défaut : 1234.

Ce fichier doit être placé dans la directory **principale** de l'application. Il est automatiquement créé et encrypté lors du premier lancement de handyproxy.exe s'il n'est pas trouvé.

Vous devez impérativement respecter scrupuleusement la syntaxe de ce fichier, sans quoi les paramètres ou données ne seront pas compris. L'édition de ce fichier peut se faire via l'écran principal du Handy Proxy et le bouton « Edit Current Config File ».

Rôle de ce fichier :

Ce fichier contient les paramètres spécifiques pour une configuration donnée de votre Handy Proxy. Ce fichier sera pris en compte au moment du lancement de votre Handy Proxy, mais il peut être rechargé en cours d'utilisation, soit avec les mêmes paramètres soit avec d'autres si vous avez plusieurs fichiers de configuration. Il n'est pas nécessaire de relancer votre Handy Proxy lors d'un changement de configuration, les paramètres contenus dans ce fichier seront pris en compte à chaque changement.

D'éventuelles remarques importantes sont insérées EN VERT dans le texte ci-dessous ; il ne s'agit ni de commentaires dans ce fichier ni de paramètres spécifiques. Il s'agit d'explications complémentaires indispensables à la bonne compréhension.

//==
//
// 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
Ce paramètre est redondant avec le fichier de configuration principal, de telle manière que vous puissiez éventuellement changer de nom pour vous connecter différemment avec d'autres utilisateurs du Handy Proxy.
ATTENTION : si votre Handy Proxy est un routeur pour d'autres utilisateurs et/ou si votre configuration est également utilisée comme serveur de messagerie, vous ne pouvez pas changer le nom de votre Handy Proxy puisque des utilisateurs vont utiliser votre machine comme routeur ou serveur. Si ce nom change, ils ne pourront plus vous retrouver et devront eux-mêmes se reconfigurer, ce qui serait ingérable.

//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
Ce paramètre va permettre de surencrypter les échanges HTTPS (et SSL) afin d'augmenter de manière considérable la confidentialité de vos échanges avec des sites comme Facebook, PC banking et autres. Grâce à cela, vos nom d'utilisateur et password déjà encryptés seront doublement encryptés par les puissantes fonctions d'encryption de votre Handy Proxy. Ceci n'est évidemment valable que si vous passez par un Handy Proxy routeur distant de l'endroit où vous vous trouvez, par exemple si vous utilisez votre Handy Proxy à partir d'un lieu public en passant par un Handy Proxy routeur, votre sécurité d'utilisation Internet sera optimale.

//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 "
Ce paramètre va vous permettre de définir, navigateur par navigateur, le canal et la priorité des filtres utilisés. Par exemple, vous pouvez utiliser un de vos navigateurs sur le canal principal de votre Handy Proxy en mode totalement transparent tandis que vous utilisez un second navigateur qui, lui, passerait par un autre canal de votre Handy Proxy lui-même connecté à un autre Handy Proxy en mode routeur. Le premier navigateur vous servant alors de navigateur à usage général, tandis que le second, protégé par les échanges encryptés entre Handy Proxy, serait utilisé pour tous les sites sensibles comme le home banking ou tout site nécessitant d'introduire un nom d'utilisateur et un mot de passe pour y accéder. Une autre méthode est de créer plusieurs fichiers de configuration de ce type et, en fonction des cas, de charger la configuration requise.

//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
Votre Handy Proxy peut utiliser une liste de liens à filtrer. Si votre navigateur utilise déjà les fonctionnalités de AdBlock (voir le site https://adblockplus.org*), par exemple, cette fonction est redondante. Il n'est donc pas nécessaire d'utiliser cette liste. Veuillez noter que si votre Handy Proxy est configuré en mode routeur, contrairement à un usage local, cette liste ne sera pas utilisée pour tous les échanges qui seront routés par votre Handy Proxy.*
Ce paramètre est configurable à tout moment à partir du menu principal de votre 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
Il existe deux versions de la liste décrite ci-dessus. Nous conseillons l'utilisation de la version étendue.
Ce paramètre est configurable à tout moment à partir du menu principal de votre 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
Il est possible de rendre votre Handy Proxy transparent, c'est-à-dire qu'il ne filtrera aucun lien, que ce soient les liens des listes décrites ci-dessus ou des liens que vous auriez ajoutés vous-même dans les fichiers adéquats.
Ce paramètre est configurable à tout moment à partir du menu principal de votre 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
Il y a plusieurs méthodes pour remplacer des liens d'images qui seraient filtrés par les listes ci-dessus. Par défaut, votre Handy Proxy remplacera ces images par de jolies photos de paysages du monde entier. Celles-ci évolueront de jour en jour, puisque cette liste est mise à jour toutes les 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
Le canal 0 de votre Handy Proxy est le canal réservé obligatoirement pour atteindre Internet en direct. Il est malgré tout possible de changer l'adresse et le port de cet accès le cas échéant et en fonction de votre configuration de réseau.

//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
L'explication qui suit est valable pour les canaux allant de 1 à 9 de votre Handy Proxy.
Vous pouvez donner un nom à chaque canal en fonction de vos besoins.
Si vous souhaitez vous connecter à un autre Handy Proxy via l'un des canaux de 1 à 9, il faut soit indiquer son adresse IP physique dans votre réseau en cas d'utilisation locale, soit mettre le nom du Handy Proxy tel qu'il a été défini par votre correspondant en cas d'utilisation distante (le paramètre « port » doit rester à 0 : Routing_Traffic_to_this_port_#x=0). Dans ce cas, le paramètre principal de chaque canal est de définir le cas échéant l'éventuelle clé d'encryption du Handy Proxy distant. Voir à ce sujet avec l'utilisateur du Handy Proxy distant s'il utilise une clé d'encryption privée ou non. Si les deux clés ne sont pas identiques, aucun échange n'est possible entre les deux systèmes.

//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. Fichier Handy Proxy hmp_conf.pac

Ce fichier doit être placé dans la directory **…\Multichannel_Proxy_Data**

Vous devez impérativement respecter scrupuleusement la syntaxe de ce fichier, sans quoi les paramètres ou données ne seront pas compris.

Rôle de ce fichier :

Ce fichier sera le cas échéant utilisé par vos navigateurs et mis à disposition par votre Handy Proxy à ceux-ci. Ce fichier ne sera accessible que comme s'il était une page web. Sa syntaxe est du Javascript (ou assimilé à). Ce fichier se comportera donc comme un micro-programme que vos navigateurs vont exécuter, d'où l'importance fondamentale de respecter la syntaxe et les définitions des mots-clés.

Grâce à ce micro-programme vous allez pouvoir éventuellement spécifier que certains sites web ou adresses physiques de sites ou de pages ne passeront pas par votre Handy Proxy. Par exemple, il vous est suggéré de ne pas passer par votre Handy Proxy pour accéder à votre routeur Internet. Par défaut, ce fichier contient l'accès direct à l'adresse 192.168.1.1 qui est en général l'adresse physique de votre routeur Internet. Bien entendu, vous devez déclarer à vos navigateurs qu'ils doivent utiliser le fichier hmp_conf.pac. Voir à ce sujet le chapitre 2 « Utilisation de votre Handy Proxy » du présent manuel.

```
///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. Fichier Handy Proxy Proxy_Authorized_Connection_List.DEF

Ce fichier doit être placé dans la directory **…\Multichannel_Proxy_Data**

Vous devez impérativement respecter scrupuleusement la syntaxe de ce fichier, sans quoi les paramètres ou données ne seront pas compris.

Rôle de ce fichier :

Ce fichier permet de définir qui peut accéder à votre Handy Proxy qui deviendrait alors un routeur pour d'autres utilisateurs. Vous pouvez éditer ce fichier et y ajouter autant de lignes (en respectant la syntaxe) que vous autoriserez d'utilisateurs en fonction de la manière dont vous allez partager votre Handy Proxy sur Internet. Vous pouvez lister ici tous les membres de votre famille, vos amis ou tous vos collègues. Cette liste peut être mise à jour à tout moment à partir de l'écran principal de votre Handy Proxy. Voir à ce sujet le chapitre 2 « Utilisation de votre Handy Proxy » du présent manuel.

Vous pouvez autoriser n'importe quel utilisateur à accéder à Internet via votre Handy Proxy en mode routeur, mais nous vous déconseillons d'ouvrir très largement cet accès sauf en cas de volonté de mettre à disposition un routeur « public ». Le paramètre « Satisfy=» permet cette fonction selon les mots-clés définis scrupuleusement comme on le voit ci-dessous. Le paramètre « Allow_From_All » rend public votre Handy Proxy, tandis que le paramètre « Deny_From_All_But_Allow » le rendra inaccessible à tout utilisateur non listé dans ce fichier.

```
//============================================================================
//
// 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. Fichier Handy Proxy Proxy_IP_to_Users_Translation_Table.DEF

Ce fichier doit être placé dans la directory **…\Multichannel_Proxy_Data**

Vous devez impérativement respecter scrupuleusement la syntaxe de ce fichier, sans quoi les paramètres ou données ne seront pas compris.

Rôle de ce fichier :

Ce fichier permet lors de l'affichage des appels de pages web de transformer les adresses physiques de vos différents PC connectés sur votre LAN et qui passeraient par votre Handy Proxy par des noms de votre choix plus représentatifs que des adresses IP physiques.

```
//=============================================================================
//
// 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. Fichier Handy Proxy Proxy_Local_URL_Filter_File.DEF

Ce fichier doit être placé dans la directory **…\Multichannel_Proxy_Data**

Vous devez impérativement respecter scrupuleusement la syntaxe de ce fichier, sans quoi les paramètres ou données ne seront pas compris.

Rôle de ce fichier :

Ce fichier permet de définir quels sont les sites, les pages ou les images etc. que votre Handy Proxy devra filtrer. La syntaxe de ce fichier est simple : chaque ligne correspond à un lien ou une partie de lien, ou à un nom de fichier déterminé. Seule la correspondance exacte des strings sera filtrée.

Cette liste peut être mise à jour à tout moment à partir de l'écran principal de votre Handy Proxy. Voir à ce sujet le chapitre 2 « Utilisation de votre Handy Proxy » du présent manuel.

```
//================================================================
//
// 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. Fichier Handy Proxy Proxy_Routing_Table.DEF

Ce fichier doit être placé dans la directory **…\Multichannel_Proxy_Data**

Vous devez impérativement respecter scrupuleusement la syntaxe de ce fichier, sans quoi les paramètres ou données ne seront pas compris.

Rôle de ce fichier :

Ce fichier permet de définir par quel canal de votre Handy Proxy tel site, lien ou partie de lien sera routé. Par exemple, vous pouvez faire passer tous les sites sensibles par un Handy Proxy distant de là où vous êtes afin d'éviter que vos nom d'utilisateur et password ne circulent en clair sur Internet à partir de l'endroit où vous êtes.

L'en-tête de chaque ligne contenue dans ce fichier indique le canal à utiliser (de 0 à 9). Par défaut, vous sont proposés certains sites de vidéo ou musicaux (comme Youtube, par exemple) qui passeront par le canal 0 de votre Handy Proxy, c'est-à-dire directement vers Internet. Nous vous déconseillons en effet de faire passer des vidéos ou de la musique par un Handy Proxy distant étant donné que ces données ne sont pas sensibles.

```
//=============================================================================
//
// 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. Fichier Handy Proxy Proxy_String_to_IP-Destination_Table.DEF

Ce fichier doit être placé dans la directory **…\Multichannel_Proxy_Data**

Vous devez impérativement respecter scrupuleusement la syntaxe de ce fichier, sans quoi les paramètres ou données ne seront pas compris.

Rôle de ce fichier :

Outre un nom de domaine par défaut comme suit « http://any_name.handywebserver.hmpr », ce fichier permet de définir des noms de domaines propres à votre Handy Proxy. Cette fonction est surtout nécessaire et conseillée si vous mettez à disposition des pages web via votre Handy Web Server. Cette fonction n'est pas limitée à cela : vous pouvez en effet créer un nom de domaine que votre Handy Proxy va router vers une adresse physique de votre réseau ou de votre PC où résiderait un autre serveur web. Par exemple si dans votre réseau vous avez un ou plusieurs serveurs web (Apache ou autre) cette fonction de création de nom de domaine vous sera fort utile si vous souhaitez que vos sites web soient accessibles entre deux Handy Proxy, càd en mode encrypté. Cette méthode rendra à ce moment-là ces sites uniquement accessibles par vos correspondants utilisant eux aussi un Handy Proxy et que vous auriez autorisés à utiliser votre configuration mise en partage.

Pour des raisons évidentes de sécurité et de copyright (le cas échéant), il n'est pas autorisé via un Handy Proxy de créer un nom de domaine qui routerait vers un site extérieur à votre LAN ou à votre PC. Le programme rejettera tout nom de domaine non conforme à la syntaxe ci-dessous. De même, ne sont autorisés que des routages vers des adresses internes à votre réseau ou à votre 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. Fichier Handy Proxy Proxy_White_URL_List.DEF

Ce fichier doit être placé dans la directory**…\Multichannel_Proxy_Data**

Vous devez impérativement respecter scrupuleusement la syntaxe de ce fichier, sans quoi les paramètres ou données ne seront pas compris.

Rôle de ce fichier :

Ce fichier permet de définir pour un site, un lien, une partie de lien ou un fichier quelle priorité de filtrage lui sera attribuée. Il existe 8 degrés de priorité, 8 étant le plus élevé.
Nous vous déconseillons de filtrer le trafic vidéo ou musical au-delà de 0, ce qui pourrait rendre ce trafic non fonctionnel.
En cas de problème avec ce genre de site, soit vous les rendez accessibles par vos navigateurs en direct avec Internet via le fichier « hmp_conf.pac » (voir chapitre 9.3 du présent manuel), soit vous les faites passer uniquement par le canal 0 de votre Handy Proxy via une définition à ajouter dans le fichier « Proxy_Routing_Table.DEF » (voir chapitre 9.7 du présent manuel).
Si votre navigateur utilise déjà les fonctionnalités de AdBlock (voir le site https://adblockplus.org) cette fonction est redondante. A moins que vous n'ayez un besoin spécifique, il n'est donc pas nécessaire d'utiliser cette liste puisqu'il s'agit uniquement de filtrage.

```
//=================================================================================================================
//
// 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. Fichier Handy Proxy Multichannel_Proxy_Email_List.hpe

Ce fichier doit être placé dans la directory **…\Multichannel_Proxy_Data\License_Sharing**

Vous devez impérativement respecter scrupuleusement la syntaxe de ce fichier, sans quoi les paramètres ou données ne seront pas compris.

Rôle de ce fichier :

Ce fichier permet de partager votre licence d'utilisation de votre Handy Proxy. Veuillez vous référer au chapitre 3 « Partager sa licence » du présent manuel.

```
//================================================================
//
// 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. Comment intégrer votre Handy Proxy dans vos applications et/ou votre usage quotidien

Outre via vos navigateurs, il y a d'autres moyens d'intégrer votre Handy Proxy dans votre utilisation d'Internet de tous les jours.

Si celle-ci fait appel à l'utilisation d'applications spécifiques permettant d'indiquer le nom d'un Proxy ou un lien vers un site ou une page déterminé(e), vous pouvez utiliser une fonction qui vous permettra de définir par quel canal de votre Handy Proxy vous voulez passer.

La syntaxe de celle-ci est la suivante :

hmp_target_channel_id=x (x = le numéro du canal souhaité)

Son utilisation est la suivante : cette commande doit être ajoutée à la fin d'un lien web.

Par exemple :

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

Dans cet exemple le site anysite.web sera routé par le canal 9 de votre Handy Proxy.

Cette commande doit impérativement être insérée après le lien vers le site à atteindre précédée du caractère « ? » si elle est la seule ou du caractère « & » si ce n'est pas le cas. Cette commande sera entièrement retirée par votre Handy Proxy avant l'appel du site en question afin de ne pas lui envoyer des commandes qu'il ne comprendrait pas. Cette commande doit être ajoutée à tout appel au site en question, ce y compris la page accédée elle-même mais aussi les images, Javascripts ou sous-pages contenus dans la page accédée. Sans cela, seule la page accédée sera reroutée. Vous devez alors, dans vos applications et intégrations, ne pas oublier de mettre la commande pour chaque lien qui devra être appelé. Si ce n'est pas possible, vous devez alors définir cet appel via le fichier « Proxy_Routing_Table.DEF » (voir chapitre 9.7 du présent manuel) qui rendra automatique le routage de tout ce qui concerne le lien accédé. Cette fonction est pratique si vous deviez éventuellement intégrer dans une page web donnée l'accès à un site hébergé par votre Handy Web Server ou à une partie de celui-ci (via par exemple une fonction iframe).

Imaginons que vous ayez un site web hébergé de manière classique par votre hébergeur. Dans celui-ci, vous aimeriez donner accès (de manière privée) à une page, une partie de page ou encore une image, qui est quant à elle hébergée sur votre Handy Web Server. Celle-ci est inaccessible, comme vous le savez, sans passer par un Handy Proxy. Elle deviendrait accessible pour autant que dans votre site hébergé vous indiquiez le nom de domaine (voir point 9.8 du présent manuel) de votre Handy Proxy suivi de la commande dont il est question ici. Dans ce cas, et si le canal défini est par exemple le numéro 9 par cette commande, il faut impérativement que tous les Handy Proxy voulant accéder à ce service soient configurés pour atteindre votre Handy Web Server via le canal 9. Si ce n'est pas le cas votre commande ne fonctionnera pas, soit parce que le canal d'un Handy Proxy ne pointera pas correctement vers votre Handy Proxy, soit ce canal sera routé vers un autre Handy Proxy où le service demandé n'existerait pas.

Si vous n'avez pas besoin d'utiliser un nom de domaine spécifique pour votre Handy Web Server (voir point 9.8 du présent manuel), vous pouvez alors utiliser l'accès direct à votre Handy Web Server par le nom de domaine par défaut de celui-ci, par exemple « http://hmp_12345.handywebserver.hmpr » qui sera retrouvé automatiquement par les Handy Proxy qui seraient connectés au Handy Proxy dont le nom est « hmp_12345 ». Cette méthode permet alors d'éviter de devoir respecter un numéro de canal bien déterminé dans vos applications.

Votre Handy Proxy met également à votre disposition d'autres commandes disponibles pour votre Handy Web Server et votre Handy Browser (voir à ce sujet les chapitres 5, 6 et 7 du présent manuel).

Si vous souhaitez bénéficier d'une intégration spécifique de commandes ou de mots-clés permettant des fonctionnalités à ajouter pour répondre à vos besoins, nous vous invitons à nous contacter pour que votre demande soit analysée par nos développeurs.

Concernant les fonctions routeur de trafic Internet et serveur de messagerie de votre Handy Proxy, il est tout à fait envisageable de créer une configuration indépendante de celle que nous offrons par défaut. Il serait dans cette hypothèse possible de créer par exemple un ensemble de serveurs au cas où le routage de trafic et la messagerie de votre/vos Handy Proxy seraient à mettre à disposition d'un grand nombre d'utilisateurs.

De même, nous pouvons fournir l'hébergement de votre propre base de données d'utilisateurs de vos Handy Proxy afin de rendre votre configuration totalement indépendante de celle fournie par défaut.

Pour toutes ces fonctions spécifiques ou développements sur mesure, nous vous invitons également à nous contacter : http://www.handyserv.com.