



Your Freedom

User Guide

A Step By Step Introduction and Reference Guide to Your Freedom

<https://www.your-freedom.net/>

Version 3.0

Release Date: 2013-06-26

All trademarks used in this guide are trademarks of their respective owners and only used for reference.

The most current version of this guide is available from our web page, <https://www.your-freedom.net/>, in the Documentation section. Please check if there is a later copy available if you encounter problems or you cannot find needed information in this copy.

This guide is © Copyright 2006-2013 by resolution Reichert Network Solutions GmbH, Zweibrücken, Germany. All rights reserved. You are welcome to copy and distribute this guide in both electronic and paper form as long as you distribute it as a whole and not in parts, you do not modify it in any way, and the reference to the original location is kept intact. Please advise all recipients that distributed copies may not be the latest version of the document, and that they can always download the latest version from our web site.

Version 3.0

Release Date: 2013-06-26

1	Introduction	8
1.1	What is Your Freedom?	8
1.2	What is it not?	8
1.3	What can I use it for?	9
1.4	How does it work?	9
1.5	Is it secure? Is it anonymous? Does it compromise my security? Can I catch a virus?	10
1.6	What does it cost?	11
1.7	Is Your Freedom “Spyware” or “AdWare”?	11
1.8	How many servers do you have? Are they all the same?	12
2	Getting Started	14
2.1	Registration process	14
2.2	Getting and installing the client software	15
2.3	Connecting for the first time	16
	<i>On a PC</i>	16
	<i>On an Android device</i>	25
2.4	Configure applications	27
	2.4.1 <i>Automatically</i>	27
	2.4.2 <i>Manually</i>	28
2.5	Manual Configuration	34
	2.5.1 <i>The Your Freedom configuration dialog</i>	34
2.6	Starting and stopping the connection	37
	2.6.1 <i>Each user may only log in once</i>	37
2.7	Choosing the right server	38
	2.7.1 <i>Server location</i>	38
	2.7.2 <i>Protocols</i>	38
	2.7.3 <i>CGI relays</i>	39
3	Connecting applications and games	41
3.1	Introduction	41
3.2	Using “socksifiers”	41
	3.2.1 <i>Windows</i>	41
	3.2.2 <i>Linux and other Unix derivates</i>	42
	3.2.3 <i>Mac OS X</i>	42
3.3	OpenVPN support	42
	3.3.1 <i>Introduction</i>	42
	3.3.2 <i>Prerequisites</i>	43
	3.3.3 <i>Configuration tasks</i>	44
	3.3.4 <i>Configure your applications</i>	45
	3.3.5 <i>Troubleshooting</i>	45

4 Using Your Freedom without client app.....	47
4.1 PPTP.....	47
4.1.1 General information.....	47
4.1.2 Is PPTP safe?	48
4.1.3 How to configure PPTP?.....	48
4.1.4 What if it doesn't work?.....	59
4.1.5 Sharing the PPTP connection.....	61
4.1.6 DNS servers.....	61
4.1.7 More than one pre-defined PPTP connection?.....	61
5 Account types: Time-based upgrades and vouchers.....	62
5.1 FreeFreedom (usage free of charge).....	62
5.2 Upgrades and vouchers.....	63
5.2.1 Vouchers.....	64
5.3 Test drives.....	65
6 Advanced Topics	66
6.1 Port Forwards.....	66
6.1.1 Local port forwards.....	66
6.1.2 SIP forwards.....	66
6.1.3 Server port forwards.....	67
6.2 Connection Sharing	68
6.2.1 Relaying	68
6.2.2 Using OpenVPN and ICS to connect other PCs, Playstations, Xbox, etc.....	68
6.2.3 Will tethering on Android work with Your Freedom?.....	68
6.3 IPv6.....	69
6.4 Fine tuning CGI mode.....	69
Appendix A. Troubleshooting	71
Why does my app/game not work?.....	71
Performing a speed test.....	71
Creating a "dump" file.....	72
Using a packet sniffer.....	72
Updating the client	73
Appendix B. Country information	74
Country specific plans.....	74
Server availability by country	74
Tweaks.....	74
Appendix C. The Your Freedom client configuration file	76
Where's my home directory?	76
Configuration options.....	77

1 Introduction

1.1 What is Your Freedom?

Is your Internet access somehow restricted? Are some web pages not accessible to you, or are you unable to run applications because of such restrictions? Are you in a place where there is Internet connectivity via a public hotspot but you don't have a login to it? Then Your Freedom is for you. Although the techniques used by Your Freedom to break through such restrictions are fairly complicated, it is not difficult to use.

Your Freedom is a **Connectivity Service** that allows you to overcome connectivity restrictions imposed upon you by your network administrators, your provider or your country. It also provides a certain level of **anonymization**, and it **hides** from your administrators and other nosy people close to you **what you are doing** on the Internet.

Your Freedom works by turning your local PC into a **web proxy** and a **SOCKS proxy** that can be used by your applications (web browser, games, whatever). Instead of connecting directly, applications can send connection requests to these "proxy servers" provided by the client part of the Your Freedom software running on your PC, and the client part will then forward these requests to the server part running on our connectivity servers through a **connection protocol** that is still available to you and through which the client part can reach the server part. There is also a transparent mode that does not require any application configuration, and on **Android** phones and other devices Your Freedom will simply work without any additional configuration.

Your Freedom **tunnels** through firewalls, web proxies, FTP proxies, DNS servers and the like. Sounds complicated? Well it is, but the good news is you don't have to worry about it, that's our job. :-)

1.2 What is it not?

Your Freedom is **not a private VPN software**. It does not provide a connection to a *private* network but to the Internet. Some call this a VPN software but it is really a connectivity solution.

Your Freedom is **not a firewall solution**, it is meant to break through firewalls, not to be one. It does not make your PC any safer. But that's likely not your concern because someone is probably protecting you too well anyway.

Your Freedom is **not a perfect anonymizer**. The service does provide a certain level of anonymization by hiding your IP address. Instead, the connection request appears to come (in fact it does come) from one of our connectivity server IP addresses. But it cannot protect you from your own mistakes or flaws in applications and protocols. You are anonymous unless you make mistakes.

Your Freedom is **not in any way "enhancing" your connection**. It does not provide data compression¹ and it cannot speed your connection up in any way; in fact, there is a certain

¹ This is not entirely true. If you connect through PPTP or use OpenVPN mode, your data is compressed.

amount of overhead which is dependent on the connectivity protocol used, so things will probably run slower, not faster.²

1.3 What can I use it for?

Your Freedom can be used to overcome:

- **Protocol restrictions.**
If you cannot use certain applications or services because these applications cannot connect to the Internet in the usual way, Your Freedom may be able to help you. For example, if your favorite online game does not work in your place because someone decided that you shouldn't play it, then try Your Freedom. Games known to work well include: World of Warcraft, EVE Online, Counterstrike and many others. You may not use P2P protocols because someone thinks it is illegal³? Most P2Pclients work nicely with Your Freedom, and you can even get a server port, which gives you a "high id".
- **Censorship.**
You may not visit certain web pages? Try Your Freedom. It turns your local PC into an unrestricted web proxy that provides access to all web pages that are generally accessible, or connects it transparently to the Internet
- **Time restrictions.**
We have heard from users that they use Your Freedom to avoid time restrictions. In most cases, existing connections are not disrupted by such restrictions, and therefore all they need to do is to start the Your Freedom client before the restriction is in place, and keep it open. The connection between the client and the server part is persistent (this depends on the connection protocol, however).
- **Access restrictions.**
If there is Internet connectivity (through a hotspot or a similar facility) but you need a login that you don't have, we'll likely be able to get you fully connected.

1.4 How does it work?

You need to run the client part of the Your Freedom software on your local PC. It is written in Java and should normally run on nearly every PC without the need for administrator rights. We also provide installer versions that do not require Java to be installed, but you may need administrator rights to install these.

On Android, just install our Your Freedom app, and launch it.

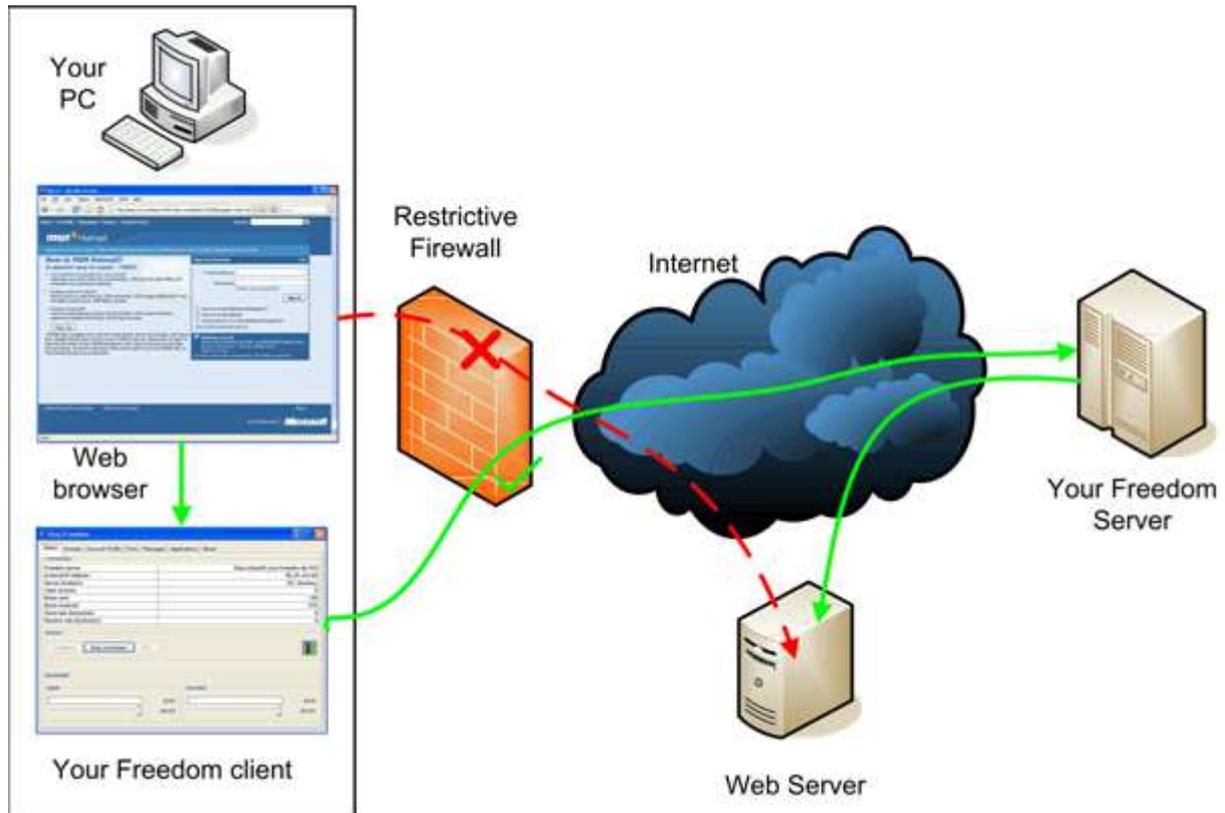
The client software then connects to one of our servers through a connection protocol that is still available to you. In most cases this will probably be an HTTP connection through a web proxy that you may use, or an "HTTPS" or FTP connection. In many places, UDP or ICMP ECHO may be used as well. Nearly everyone everywhere can use DNS mode.

Have a look at the picture below. The box on the left is your PC. Let's say the restrictive firewall won't let you access hotmail.com and you want to read your private email from your workplace; fire up the Your Freedom client and let it connect to one of our servers, configure

² There are cases, however, where Your Freedom is able to actually enhance your connection for a particular purpose, for example by disguising your traffic as traffic that is put into a better service class by your provider, or by overcoming routing issues.

³The protocol is of course not illegal and it is therefore silly to block it; we know best because we had to block it on some servers as well but it remains open on most. Your actions may be illegal though – Your Freedom can't do anything about this, it remains your responsibility.

your web browser to use it as a proxy, and your web browser will be able to connect to hotmail.com by connecting to the Your Freedom client, which will forward the requests to one of our servers, which will then forward the request to the hotmail.com server. The replies from the hotmail.com server will take the same route backwards.



This is only a very simple scenario but it illustrates that the Your Freedom client application and the Your Freedom server act as intermediate hops for your application connections.

1.5 Is it secure? Is it anonymous? Does it compromise my security? Can I catch a virus?

Connecting to the Internet through Your Freedom is generally less dangerous than connecting through a dial-up or DSL connection. As long as you do not explicitly configure a server port forward, no-one can connect to your PC or phone through Your Freedom. But since you may download data from the Internet that may then be executed on your PC (intentionally or unintentionally because of application bugs) there is a certain amount of risk; it is the same as if you were connecting through any other means to the Internet and download data from there. However it is possible that your company or whatever uses sophisticated protection mechanisms (e.g. virus checking for downloads from servers on the Internet) that we do not provide; in this case it is indeed less secure. But please consider that it is less secure because it allows you to do things that you would otherwise not be able to do – the most secure protection from the dangers of the Internet is an Air Gap Firewall™, i.e.: pull the plug. You'll be safe but also lonely.

It has been said before that Your Freedom is not a full-blown anonymization service. It will however hide your IP address, unless your application communicates it “in-band”. Web server admins will not be able to see where the access comes from initially; they will instead see one of our IP addresses. But we do not take any further anonymization measures: we do not remove tracking cookies, nor do we “wash” the request headers that your web browser sends.

For those looking for privacy, the client offers a **high level of encryption** using the AES encryption standard, public/private keys, and strong session keys. Details can be found on our web page on <https://www.your-freedom.net/?id=encryption> (you need to be logged in). Unless you explicitly disable encryption, you’ll be safe from spying eyes.

With regards to viruses: we do not have any virus protection mechanisms built into the service and therefore do not provide any virus protection⁴. Please install anti-virus software on your PC or phone; you should do that anyway.

1.6 What does it cost?

A fundamental service is provided for free. It is restricted in bandwidth and the number of simultaneous streams⁵, and there is a time limit of one hour for the connection between the client and the servers (but you may reconnect immediately). Daily usage time is limited to two hour, and weekly usage time is limited to 5 hours. Some of our servers are not available for FreeFreedom users. If this is good enough for you, you are welcome to stick with it.

We provide upgrades that remove all usage time restrictions, expand or remove the bandwidth restriction, and that allow for more simultaneous streams, and there are server ports that you can use to allow inbound connections to your PC or another PC in your network if you like. The upgrades are available as one month, three months, six months or twelve months upgrades, and come in three different levels that we call BasicFreedom, EnhancedFreedom, and TotalFreedom. As an alternative to time-based upgrades there are vouchers carnets. Vouchers can be used to temporarily upgrade your Your Freedom account without having to pay for a full month and not use parts of it. Details can be found in chapter 0 of this guide.

1.7 Is Your Freedom “Spyware” or “AdWare”?

No! Rest assured that the Your Freedom client application does not contain any code to spy on you or to cause any annoyances (other than the restrictions of the FreeFreedom service, which are of course there to convince you of the benefits of buying an upgrade). The only reason why we don’t publish the source code is because much of the code is also used in the server, and we don’t want to expose it. We don’t want to help those developing blocking appliances either.

We do our best to protect your privacy by not storing any more details on our servers than technically or legally required – and permitted. In fact, the connectivity servers themselves do not keep *any* logs that could be of interest to anyone but the developers and operators

⁴Actually this is not entirely accurate. Outbound email sent through Your Freedom is scanned for viruses. We do this to avoid blacklisting of our IP addresses, which would make it impossible for our users to send email through Your Freedom. It does not protect you; it protects others (and us) *from* you.

⁵ In PPTP mode, OpenVPN mode and on Android, the number of concurrent streams is not limited.

(they only contain things like server load and exceptional occurrences in server operation); all logs containing user details are instead kept on a server in Germany. However we will cooperate with legal authorities in Germany to the extent required to protect us from having to take responsibility for your actions. This means that we may unveil your account and payment details as well as the source IP address used to connect to our servers if we are forced to do so (and able to determine who is responsible for some action).

We do not log what you access on the Internet; *German telecommunications laws do not even permit this.* We do log the fact that you have used our service, from where you have logged in to our service (if we know it at all! With DNS mode, we usually don't), the lowest 16 bits of IP addresses you have connected to (but not the full address, only the last two numbers!) and statistical data about your usage needed for accounting and quality assurance. This information is typically held on file for only a few days and no longer than 4 weeks. We do not use this information in any other way except for statistical, debugging and accounting purposes and for combating violations of our terms, unless required by legal authorities *in Germany*. We will *never* provide any details to *private parties* or *oppressive regimes*.

There is a control console on the servers that theoretically allows us to see what our users are currently doing. We only use this for troubleshooting, and all data there is transient and not stored anywhere. The moment you log off it's all gone. Trust us; we have better ways to pass our time than peeping on you.

You might say "but others claim they don't log at all!" Well, they are either naïve or lying. Our competitors need to protect themselves against abuse too, and they can only do that if they have data. We have decided to be honest with you.

1.8 How many servers do you have? Are they all the same?

This point is subject to change frequently. At the time of writing we have 23 servers online, in 9 different countries. All will be able to support basic web surfing or chatting but some will refuse P2P connections (particularly the ones located in the United States) to comply with provider policies. Some can handle more traffic than others. Have a look at the live statistics page at <https://www.your-freedom.net/?id=servers>; servers that are not in the "p2p" server group are not well suited for P2P applications, servers that are not in the "volume" group are not suitable for large file transfers, and so on – you'll get the drift.

Everyone may use all servers in the "free" group, the others are reserved to paying customers. Some servers may not be available to users connecting from certain countries, or only available to users connecting from some countries. The Your Freedom client will tell you about such restrictions when you connect ("authentication not valid for your country of residence"). If this happens to you, please use another server. We only do this when we need to defend ourselves, i.e. not at all if we can avoid it.

Look at the server load too. The higher the number, the more loaded the server. Loads below 40000 are considered low, loads above 125000 are considered high, and very high numbers indicate you'll likely only get a degraded service. We use a traffic light scheme to quickly indicate the server state. A "green" light indicates that the server is fine and can accept your connection. A "yellow" light would indicate that the server is up and running but currently rather busy, already slightly overloaded or otherwise in trouble (connectivity

problems are a possible reason) and probably won't be able to provide the best service to you – you are still welcome to use it, and the service may still be pretty good. A “red” light indicates that the server is down or otherwise unable to serve you.

2 Getting Started

2.1 Registration process

Your first step in using our service is to **register on our web site**.⁶ You need to visit <https://www.your-freedom.net/> and create an account there. There is a link underneath the login and password form fields in the red part of the page banner.

On the registration page, choose a username (preferably one that is not likely already used) and provide a password. Please make it long enough; this is for *your* protection, not ours. Both username and password may contain uppercase and lowercase ASCII letters, digits, dashes, and underscores (spaces are permitted in the password too); other characters *may* work as well (particularly in the password) but it is not a good idea to try. The only other required field is your email address. Everything else is not mandatory; please do not fill in rubbish if you do not want to provide the information, leave these fields empty instead. You can always come back later and provide information (for example, if you need a qualified invoice).

Once you have filled everything in, click on the “Create account” button. You will be asked to confirm your details by clicking on “Create account now”. If there is a problem with your data, red messages will appear telling you what is wrong; just correct your input and try again.

Within a few minutes you should receive an email containing an activation link. If your email address is protected by anti-spam measures, please ensure that email sent from the “your-freedom.net” domain (i.e. ending in “@your-freedom.net”) is permitted before you click on the “Create account now” link. Activate your account by clicking on the link in the email (or cut & paste it into your browser). You can also simply reply to the email, quoting it in its entirety, in your email reader. If you haven’t received the email or if the link doesn’t work for whatever reason, please send an email to our support staff, they can create or activate the account for you if you write to support@your-freedom.net, *telling them the username you have chosen, but not your password*.

What if you cannot register on our web site because it’s blocked? Well, it’s a hen and egg problem then. Either you ask someone else to create an account for you (or do it from somewhere else) and modify it later, or obtain the client software from another source than our server, and use the username “unregistered” and the password “unregistered” in it. This account will only provide FreeFreedom access, however. Alternatively, if you are able to send an email to our customer support, ask them to create an account for you. Just write to support@your-freedom.net telling them about your problem, suggest a username (please limit yourself to ASCII letters and numbers, dashes and underscores) and a password. If you want to receive the YF client by email just write a blank email to get@your-freedom.net; you’ll be given further instructions on how to proceed. If all the odds are against you and you can’t get the client software from anywhere else we’ll mail you a CD as well.

⁶ It is *recommended* that you use a personal account, but if you only make use of our FreeFreedom offer you do not need a personal account. Just use username “unregistered” and password “unregistered” in the client application. The Android app does this by default.

2.2 Getting and installing the client software

Once you've created an account you may use it to log in on our web page.⁷ Log in (to check that your account is active), then click on "Downloads" (you don't have to be logged in to download). There are several ways to run the Your Freedom client, and consequently there is more than one option for download:

- **Windows Installer**

Windows users who already have a suitable Java Runtime Environment⁸ installed on their system and who have enough rights to install software should be able to use this version. The download is about 2 megabytes in size. If you are unable to download files ending in .exe, try to copy the link location and paste it in the URL field of a new browser window, then change the .exe to .txt. Rename the downloaded file on your PC to .exe when done.

- **Windows Full Installer**

This version comes bundled with a JRE of its own so there are no prerequisites. Every Windows user should be able to use this one, provided that you may install software on your PC. The download is rather fat, about 14 megabytes. Again, this is an .exe file, try changing the ending to .txt if this is a problem. A benefit of this version is that it is compiled to native code and will consume fewer resources.

Both Windows installer versions are installed by running the .exe file. Just follow the instructions in the installer and you should be done in a minute. (If you are updating from an earlier version we recommend to un-install the previous version first; your settings will be kept. If you change installer type, you *must* uninstall the old version first.) Once the client software is installed, proceed to chapter 2.3.

If you are not running Windows or if you cannot install software on your PC, your best choice is the **Java archive** version. Download the ZIP file and extract the contents into a folder to which you may write. This could also be a memory stick, or a CDROM, by the way. Then run the Java interpreter with the "freedom.jar" file. With Windows it is usually sufficient if you double-click on the JAR file, but you may want to open a "cmd" window instead, "cd" to the directory and run "javaw -jar freedom.jar" instead. On UNIX boxes you'd normally use "java -jar freedom.jar" or "kaffe -jar freedom.jar" or something similar; UNIX users normally know.

Generally, the Java archive version of the Your Freedom client should run on every computer that has a suitable JRE – and enough memory. We love to hear from you if you've managed to run it on an exotic piece of hardware (or in an unusual place)! We also offer a **Mac OSX installer** version. Even though Mac OSX editions often ship with a pre-installed JRE, there are versions like Leopard that ship with JRE 5 which is no longer supported so you may need to install JRE 6 or 7 manually. Additional hints for Mac OSX and other operating systems can be found in the documentation section on our website.

⁷ Logging in is optional, of course; most content is available to everyone without a login. The special "unregistered" account cannot be used on the web site.

⁸ The Java Runtime Environment is required to be compliant to Java 6 or newer. If in doubt, visit <http://java.oracle.com/>, click on "Java SE" in the "Top Downloads" section on the right hand side of the screen, then download the "JRE" or a "JDK" (which contains the "JRE") and install it on your PC. Oracle provides these downloads for free, but please have a look at their license terms.



The YF client only runs with Java 6, not Java 5. Mac OSX does not ship with Java 6 but you can get it from <http://developer.apple.com/java/download/> (download "Java for Mac OS X 10.x Update (whatever)"). Once you've installed it, Java 5 may still be activated by default. The installer we provide should be able to automatically ensure the right version is taken; if that doesn't work try to change the default: Open Finder, go to Applications, Utilities, Java, run "Java Preferences". Move "Java SE 6" to the top for applications.

- **Android APK**

The Your Freedom app will only run on **Android 4.0 and above** devices. Older Android versions are not supported, no matter if the phone is new or not. We cannot support older versions because they are lacking the necessary VPN API. If you are unsure, open the settings, go all the way down to "About phone" and check "Android version" in there. If it's 1.x, 2.x or 3.x then Your Freedom will not work on your phone. Check with your manufacturer if there is a firmware update and complain if not. We suggest that you also check on <http://www.cyanogenmod.org/>; they might have an aftermarket firmware for your phone.

There are no other requirements; contrary to other VPN applications **your phone does not have to be "rooted"**.

We suggest that you configure your device to **allow installation of applications from external sources**; this will allow you to download and install the app from our website and receive updates. Open the settings, go to the Security section, find the "Device Administration" section and tick "Unknown sources". It does not jeopardize your phone, it only jeopardizes Google's business model. Now download the Your Freedom APK file or obtain it through email (write to get@your-freedom.net and put the word Android in the subject line). Click on it, and install it.

Alternatively, search for "Your Freedom" in Google Play if you can use it. Play has the additional benefit that you can configure fully automated updates.

2.3 Connecting for the first time

On a PC

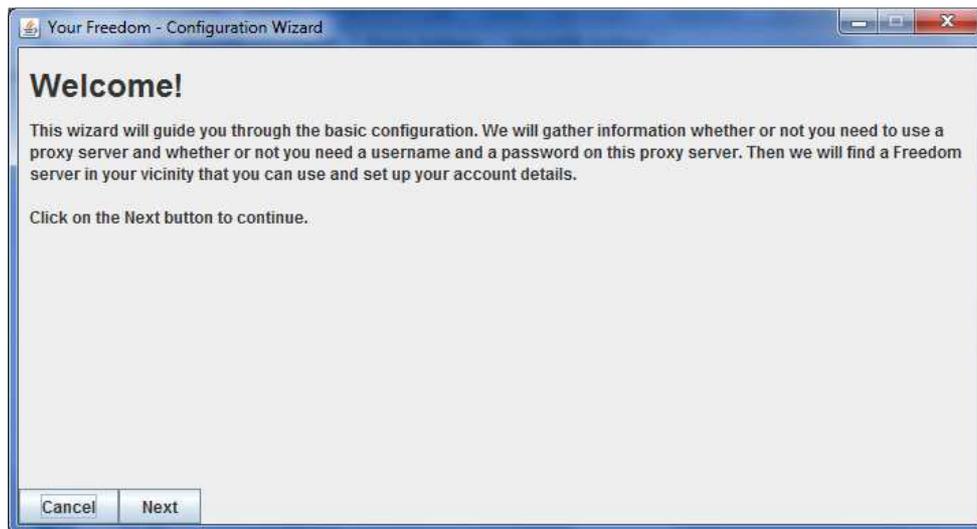
When you start the Your Freedom client application for the first time, you'll be asked for your preferred language⁹. Click a button (you can always change the setting later).

⁹ Not all texts have been translated to all languages. You may encounter some parts that appear in the default language, which is English (US), and it is quite possible that you encounter bad translations. Please let us know!

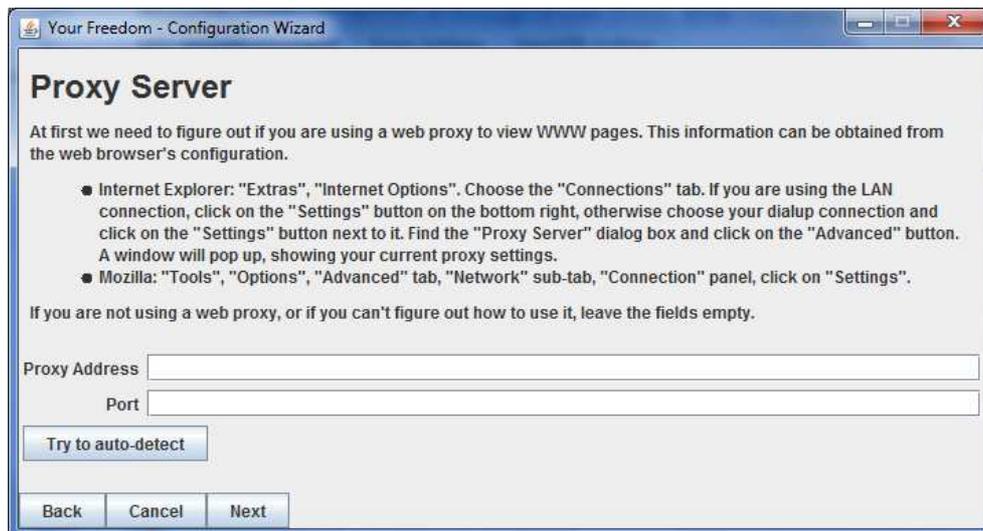


After you choose the language of your preference a “Wizard” will show up. It is safe not to use it and enter all required information manually, but if you are unsure, give it a try first. Manual configuration may be required in difficult connection scenarios; please refer to chapter 2.5 on page 34 for details.

Now let’s assume that you are using the wizard. It will first present a Welcome page:



Do as you are told and click on the “Next” button. You’ll see this page:

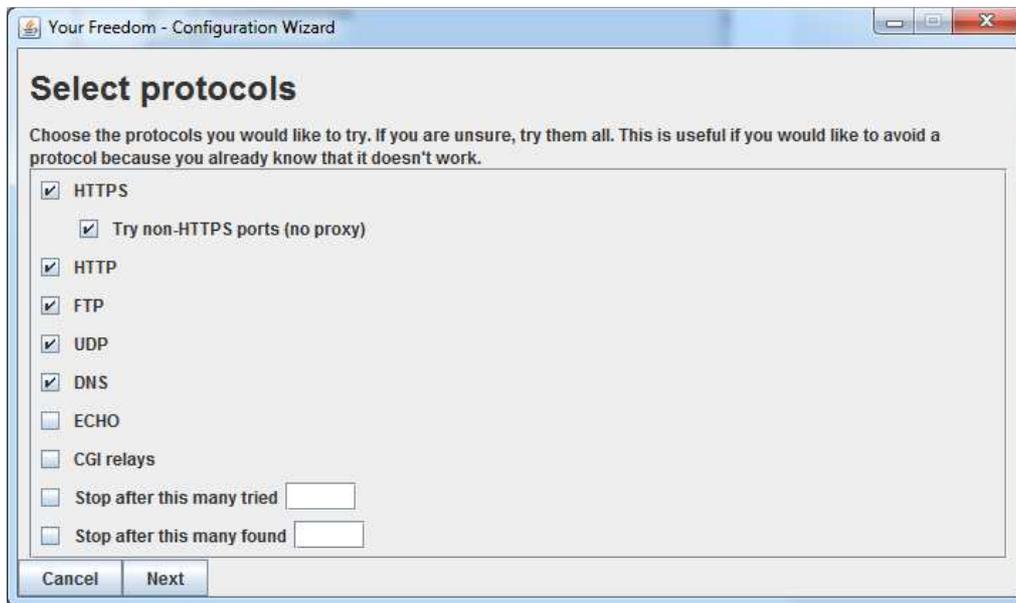


We have taken great effort to ensure right-to-left languages are properly formatted; please bear with us if this is not always the case; none of us is able to read any of these languages so we don’t notice. (And... let us know!)

Version 3.0

Release Date: 2013-06-26

If your Internet connection is through a web proxy, enter the details here. If you are unsure, try to click “Next” for now.



You'll find a Window asking you to select which protocols will be used to connect to YF servers. Selected protocols will affect the way the Wizard checks reachability of servers. Some connection modes may not be available to you, depending on the platform and whether or not you are running the Your Freedom client as administrator (this is a prerequisite for ECHO mode).

If you are unsure, leave the default selection. Click “Next”:

If all you get is an empty list of available servers like this:

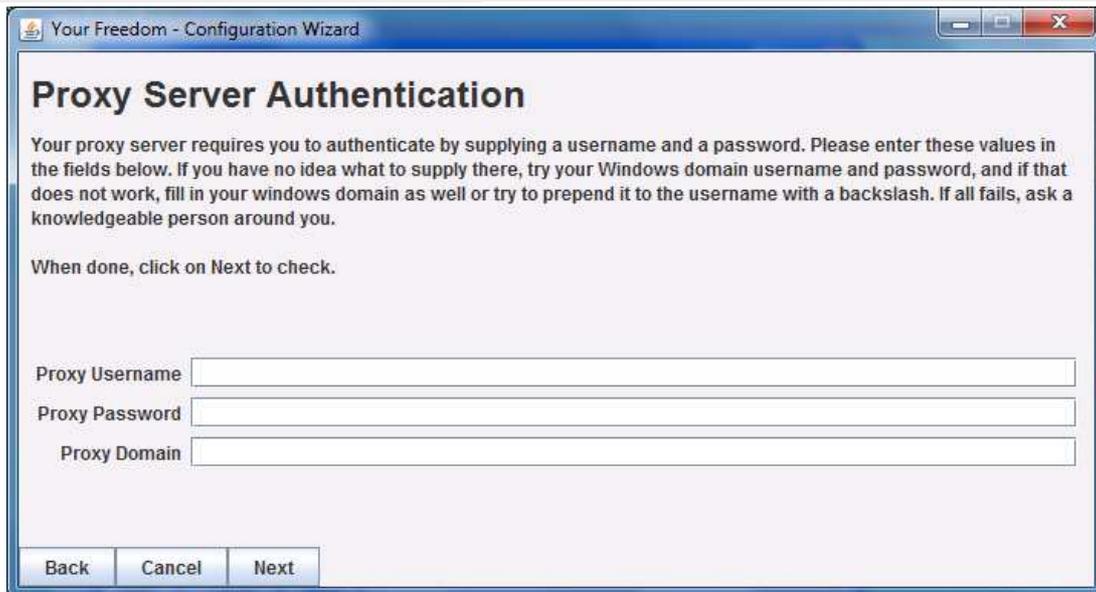


you might need to figure out about your web proxy (or configure everything manually, e.g. if you want to use an FTP proxy!).

If you get this however,

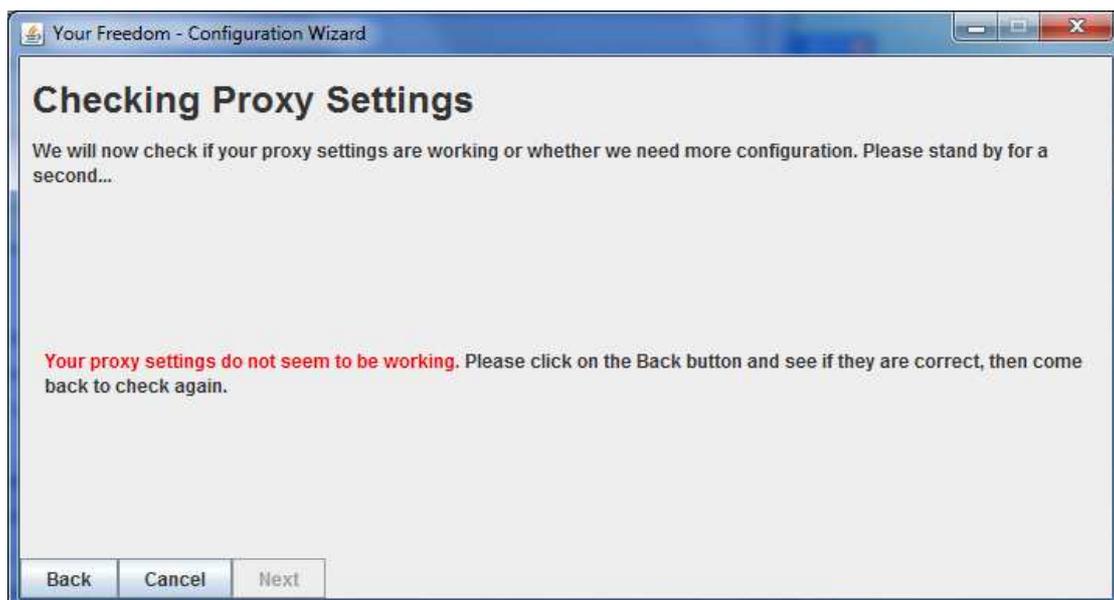


then you've filled in the proxy details properly but you need to authenticate on the proxy. Click on "Next"...



and fill in suitable login credentials. In many cases this will be your Windows Domain login (don't forget to fill in the domain as well!). Just try until it works, you can click "Next" to try.

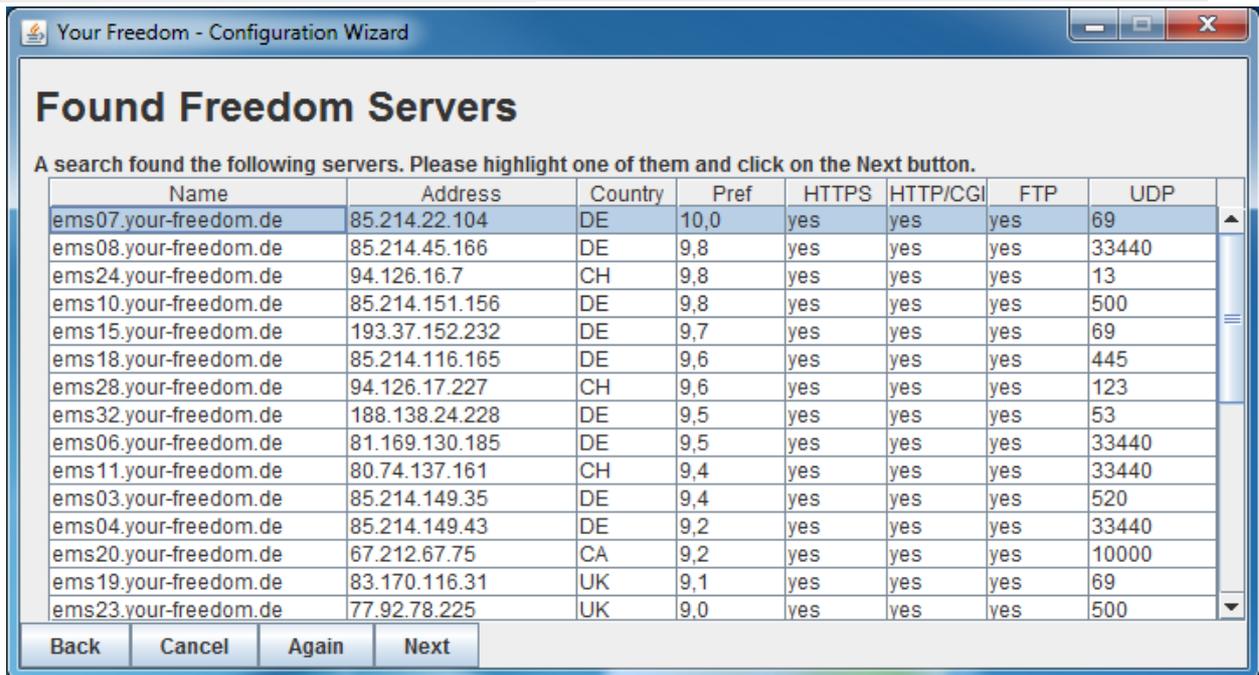
If you see this page:



it means that you have not provided a working proxy configuration. Click on "Back" and modify the hostname/IP address and/or the port setting. Many proxies "listen" on port 80, 8080 or 3128, to name the most popular ports. Check your web browser's configuration; it should be able to tell you.

Oh by the way, if you find that the wizard has the proxy details already filled in, then it's not magic – it just found them in your PC's registry and probably has made life easier for you.

Let's assume you've been able to make it work. (If not, please ask a knowledge person around you how you can use the web proxy, or click "Cancel" and try a manual configuration). It worked if you see something like this:



It is important that you see a “yes” or a number in any of the columns HTTP, HTTPS, FTP or UDP. A “yes” means that the client has been able to use this protocol to connect to the server using the default port settings, a number would mean that it has been able to connect but on a different port, and a “no” means that the protocol could not be used to connect to this server. The results are sorted by preference (a number between 0 and 10); it indicates how well the server fits your requirements (if you’ve set any). Choose a server, and then click on “Next”.

Configure Freedom Account

Please fill in your Freedom username and password in the form below. Click the Next button when you are done.
To obtain a Freedom account go to <http://www.your-freedom.net/> and register there.

Username:

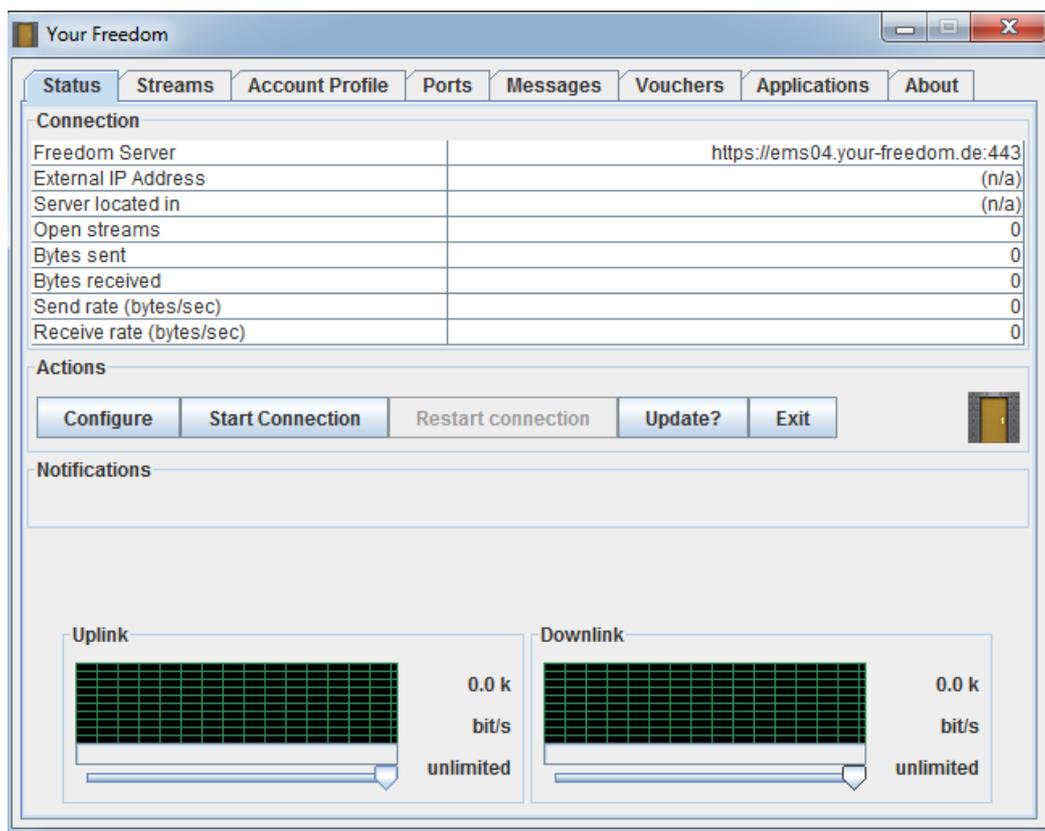
Password:

Back Cancel Next

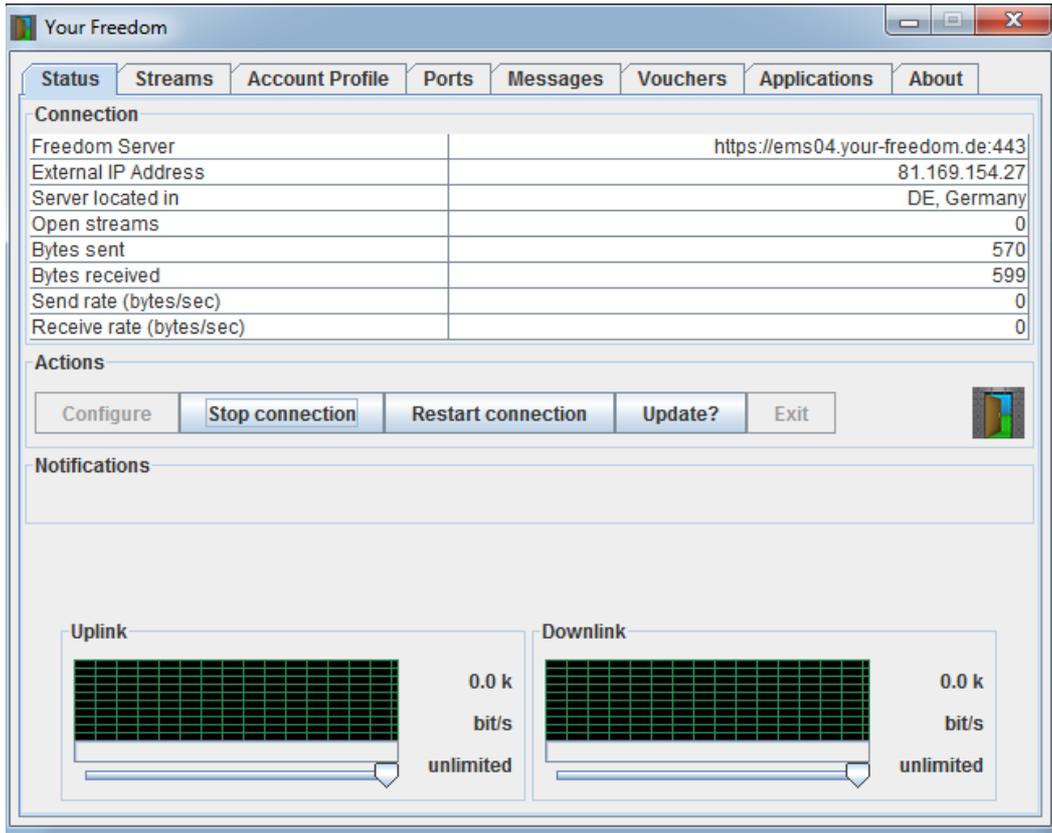
On this page, enter your Your Freedom username and password. Click on “Next”.



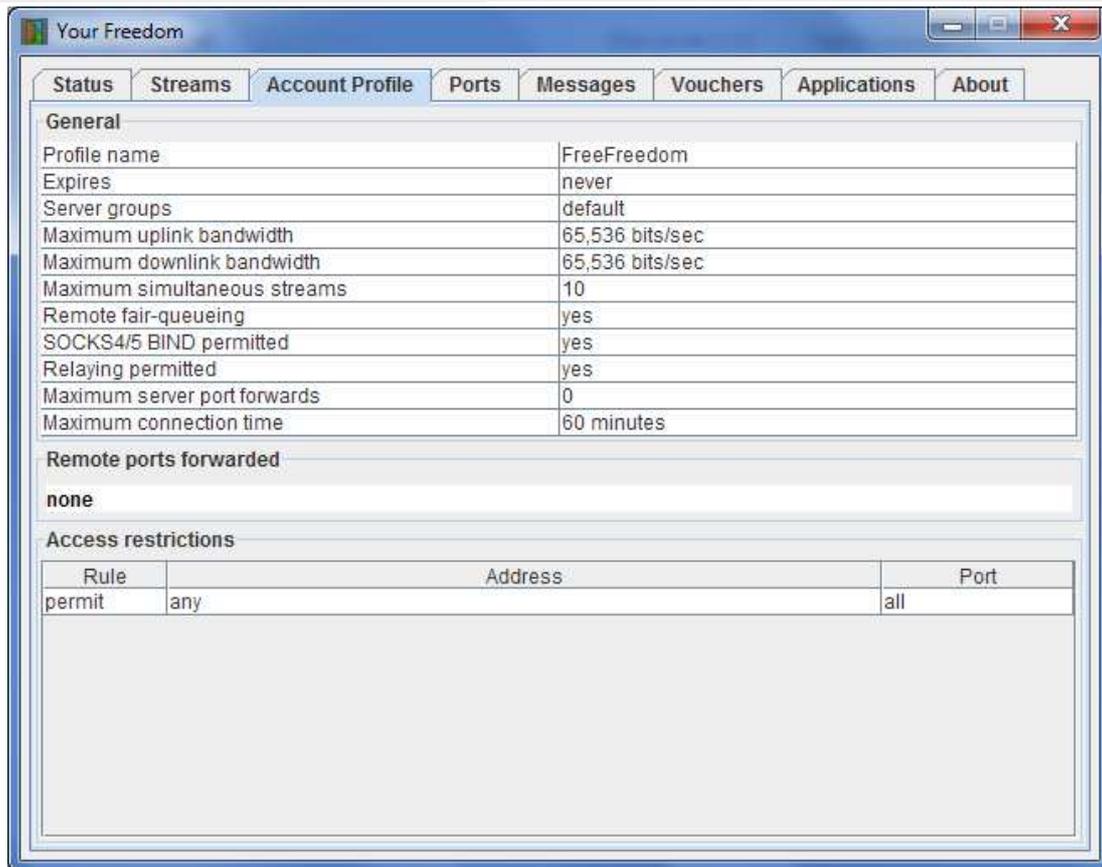
It seems you're done now! Click on "Save and Exit". The main window of the Your Freedom client should now look like this:



Note that the client just doesn't know anything about the server and your account's profile before you've connected to the server, that's why some of the values seem to be somewhat odd (including the bandwidth – it's not unlimited unless you've bought a package). Click on "Start connection" and you should see something like this after a few seconds:



Note that all the details are now filled in, and the bandwidth reads “64.0k”. That’s kilobits, about the speed of an ISDN connection or a bit faster than with a high-speed modem. Click on “Account Profile” now.



This panel contains your account details. Without a package, you may not use any special servers (just the default ones), your bandwidth is limited, your maximum number of simultaneous streams is rather low and your server connection will be terminated after 60 minutes (but you may reconnect when it happens). No server ports are assigned to you so none of them are forwarded to you. But at least, there are no access restrictions; you may access everything on the Internet¹⁰.

If you are using the HTTP protocol to connect and your connection does not fully work, try the POST or the CGI connection model instead (see manual configuration in chapter 2.5 on page 34).

OK, time to configure your applications. Please refer to chapter 2.4 on page 27 to learn how to do this. Once you've set up at least a web browser to use Your Freedom the main objective should be reached: you should be able to access the web freely!



If the version of the YF client you're using to connect is too outdated you may see a message saying the *client [is] too old*. This means you must update to the latest YF client version as yours is not supported anymore. The preferred method would be to download the most recent one, uninstall the old version and install the new one.

¹⁰In fact there are some restrictions but you can't see them. They are only there to protect our servers and won't get in your way. Promise!

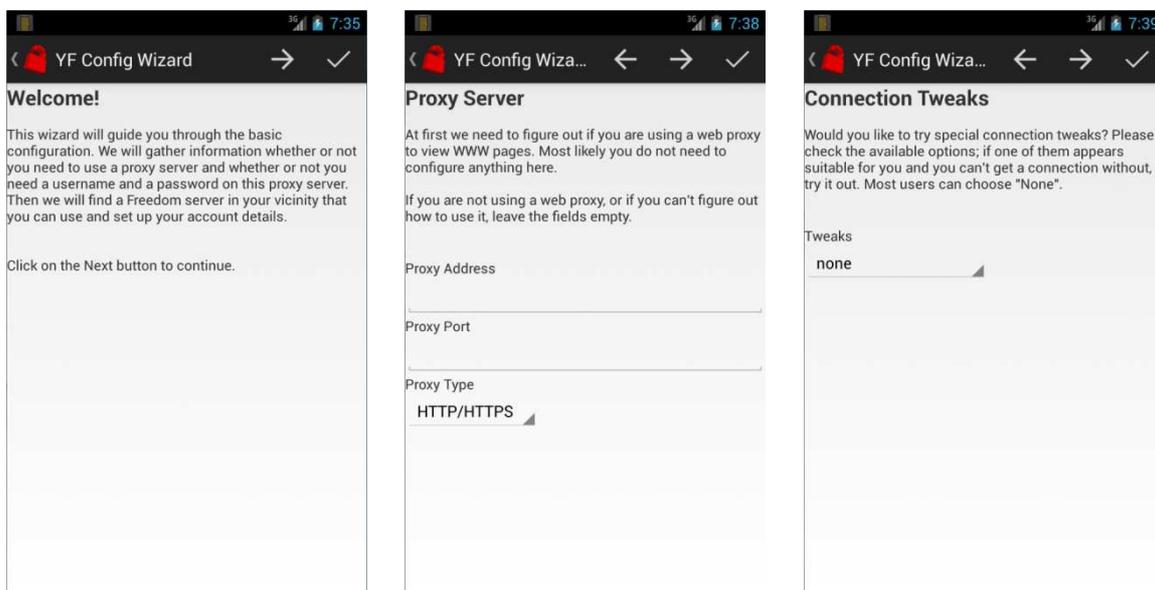
On an Android device

Find the icon shown on the right, and launch the Your Freedom status application by tapping on it. You'll see a welcome banner similar to the one shown on the right, briefly explaining the most important things. You must scroll through it (and while you are at it anyway, may we suggest that you read it as well) and click either "OK" or "Use wizard". Please click "Use wizard". (If you happen to have clicked "OK" instead, click the Settings button in the top right corner, choose "Exit", and start over again.) The app will now guide you through the initial steps of the setup. When you are done with filling in requested information, click the right arrow to jump to the next step. You can always go back using the left arrow. If the configuration is complete and you are happy with it, click on the tick mark.



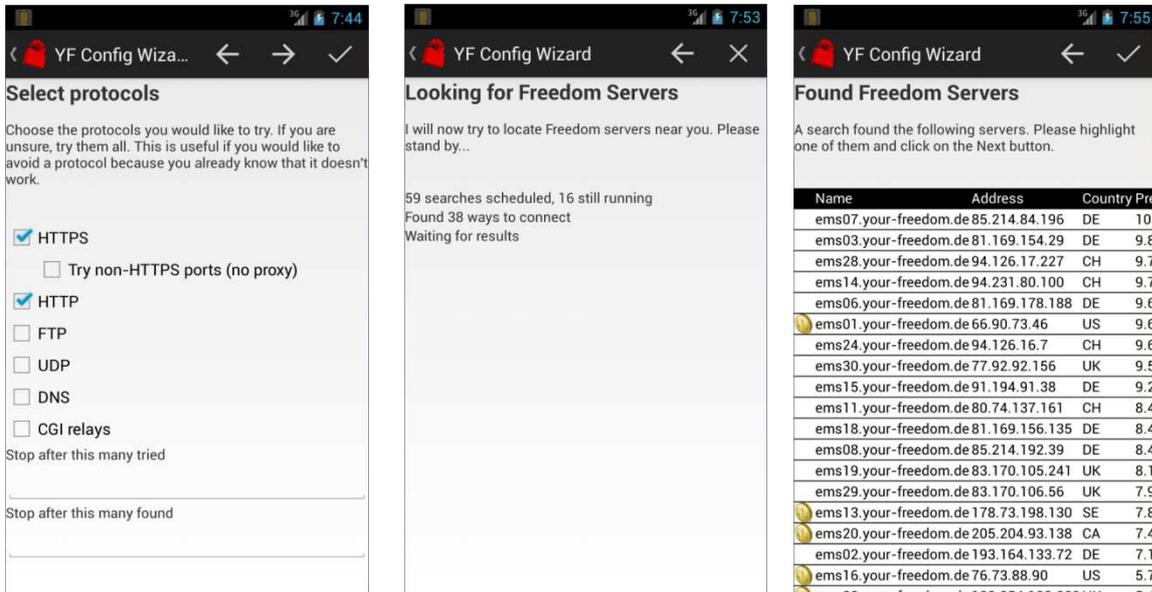
You'll likely not have to configure a proxy server. If you need to, type in its address or DNS name and its port, and if it is a SOCKS proxy change the proxy type. The app will try to find out whether or not you need authentication credentials; if you need them, it will ask you for them.

We have some useful "tweaks" for some countries and/or networks. If yours is among them, make the correct choice on the next page. Most likely you'll not need this, and if you do you can always come back later.

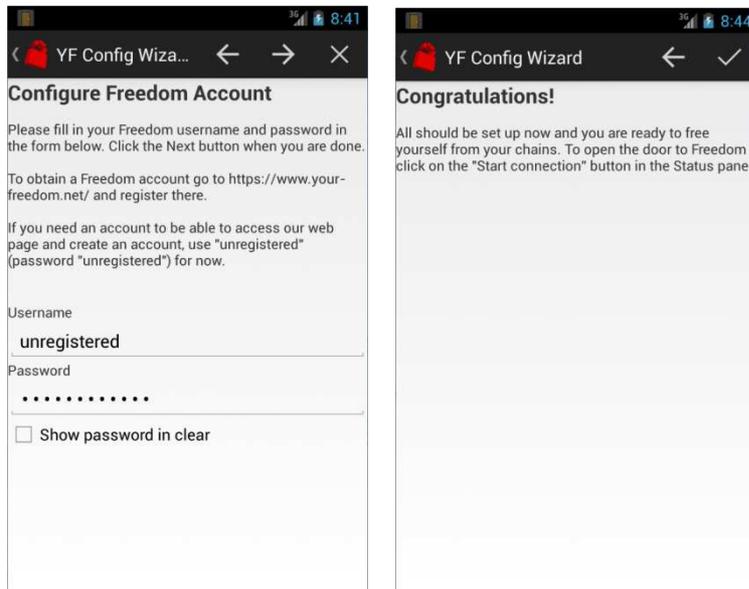


The next page provides a list of connection models available and lets you select which ones to try. We suggest that you tick HTTPS, HTTP and DNS. Generally, the more ticks you make, the longer it will take, but your chances of finding a way to connect will also improve. If you are happy with partial results, use the input fields on the bottom to stop searching after a given number of attempts have been made, or a given number of connection options has been found. Click the right arrow to start searching for connection options now. Once the

search is completed, you'll see a list of Your Freedom servers. The table can be scrolled vertically and horizontally. It is ordered by "preference", a number between 0 and 10 calculated based on your configured server preferences (you haven't done that yet) and the likely server performance. Some of the found servers will have a coin symbol; these servers are only available to paying customers, while others are available to everyone. Tap on one of the records to highlight it, and then tap on the right arrow.



On the last screen, enter your username and password (if you have one already). You may use the pre-configured "unregistered" with password "unregistered" if you do not have your own account with us yet. You only need a personal account if you intend to make use of our BasicFreedom, EnhancedFreedom or TotalFreedom offers.



When all is done, click on the tick mark.

On Android, you do not have to configure any applications; just skip the next section.

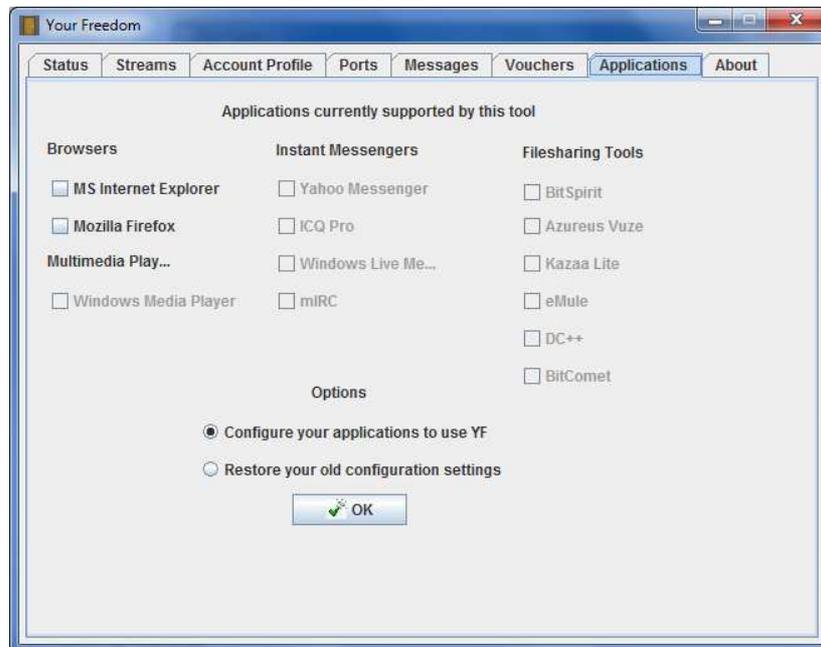
2.4 Configure applications

This section only applies to PCs, not Android devices.

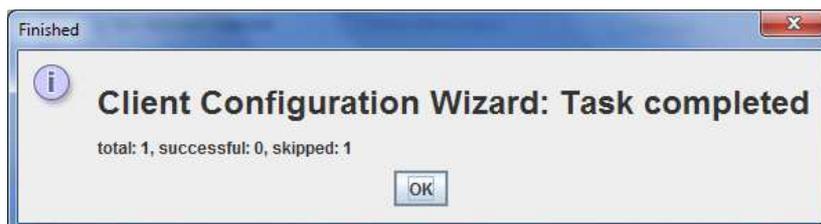
2.4.1 Automatically

Please note: We recommend manual configuration. This feature is only provided for your convenience and you should probably not use it.

Windows users can simply click on the “Applications” tab and see something like this:

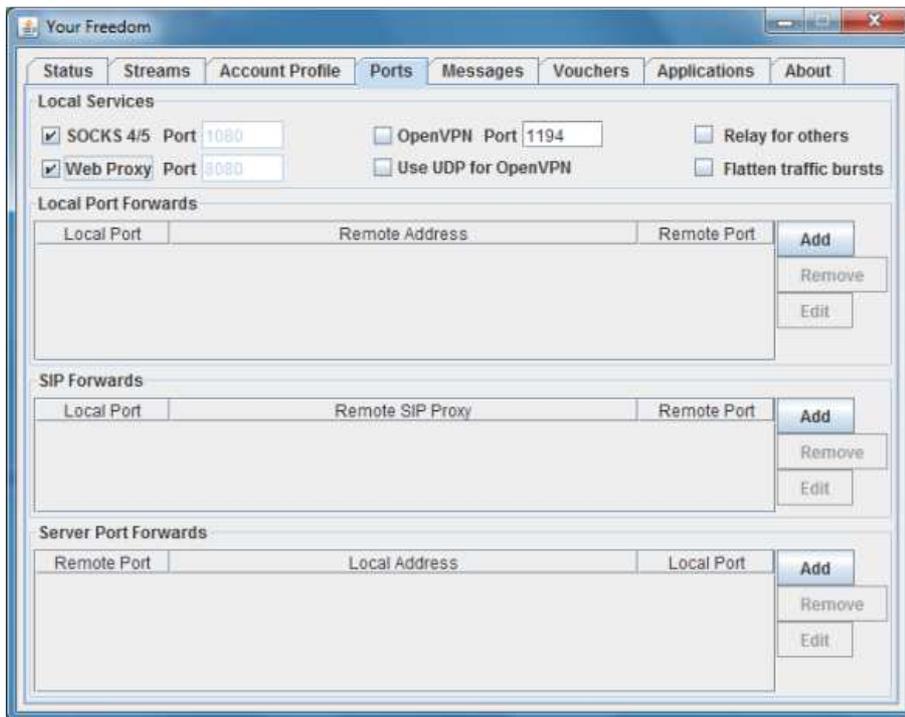


This is a list of applications whose configurations can be modified automatically by Your Freedom. The ones that are installed on your system have working checkboxes, the other ones are grayed out. Tick the ones you wish to use with Your-Freedom, and then click “OK”. You’ll see something like this:



Hope it’s all successful! Then click “OK”. To restore the previous configuration of your applications, choose “Restore”, and then tick the ones you would like to restore, and click “OK”. Note that applications that you’ve configured to use Your Freedom will only work properly if the Your Freedom connection to the server is up and running. Also, don’t forget to restore all your settings *before* de-installing the Your Freedom client!

To manually configure your applications, have a look at the Ports tab first:



Note the “SOCKS 4/5” and “Web Proxy” checkmarks; this tells you that your local PC is now acting as a SOCKS4/5 proxy on port 1080 and as a Web Proxy on port 8080. To change these values, untick the service, then modify the port, then re-activate (this can be done on-the-fly while you are connected!). Everything below is pretty sophisticated stuff and certainly not aimed at first time users, and will be covered in chapter 0.

If for some reason you cannot configure your applications from within the Your Freedom client, you need to manually configure them to use web proxy “localhost” on port “8080” or SOCKS proxy “localhost” on port “1080” (if you’ve got the choice, use SOCKS version 5). Please refer to the application’s documentation to learn how to do this (or ask someone who knows – we’ve got some examples in the FAQ/Docu section of our web page <https://www.your-freedom.net/?id=fag> as well).

OpenVPN support is not enabled by default – please see chapter 3.3 on page 42.

2.4.2 Manually

Of course we cannot provide detailed configuration guides for all applications that can be used with Your Freedom. There are basically only 4 ways how applications are made to work via Your Freedom:

- 1) By configuring them to use a web proxy. Applications that offer you to access the Internet through a web proxy need to be setup to use your local PC (the hostname is “localhost”, the IP address is “127.0.0.1”) on port 8080 as the web proxy and everything should be fine.
- 2) By configuring them to use a SOCKS4/5 proxy. Applications that offer you to access the Internet through a SOCKS proxy need to be set up to use your local PC (again, the hostname is “localhost” and the IP address is “127.0.0.1”) on port 1080 as SOCKS proxy. This is preferable over the web proxy configuration (if you’ve got the

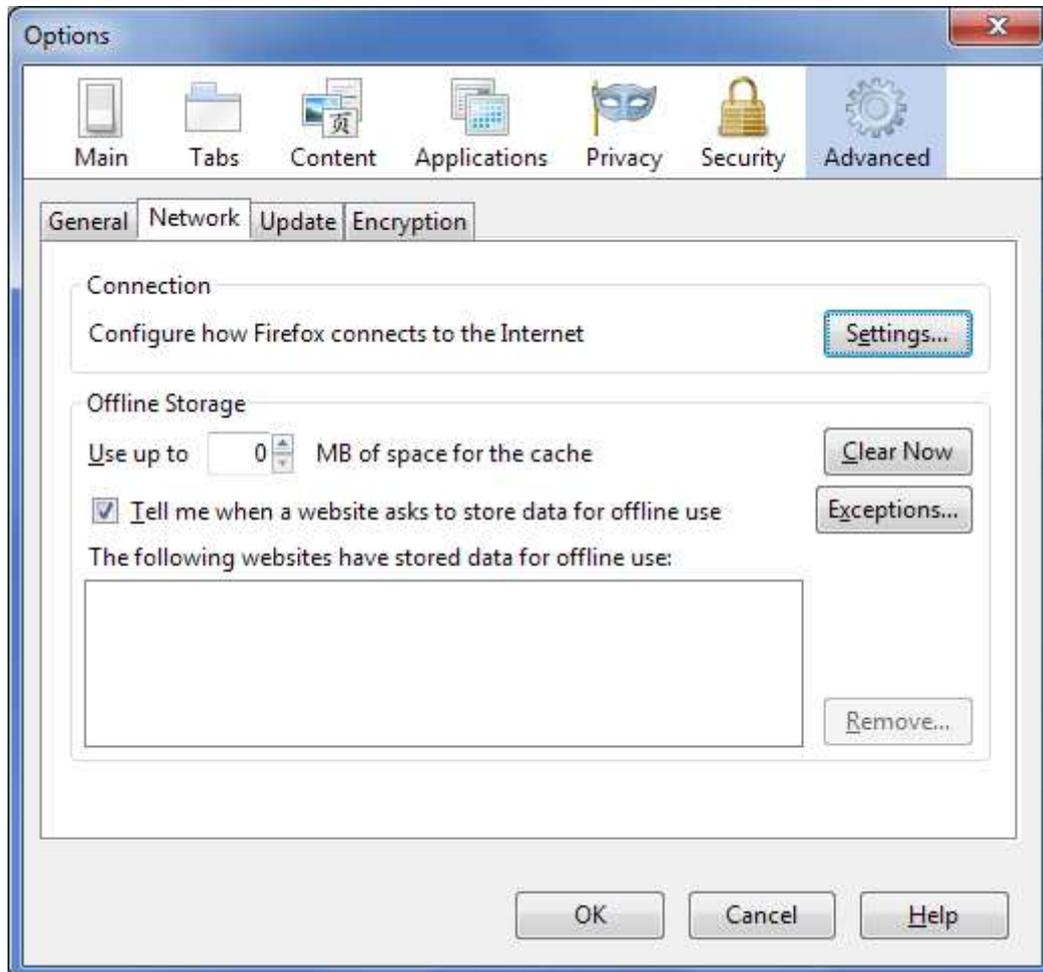
- choice) but both will normally do. Use SOCKS5 if you can. If it doesn't work (some applications have buggy SOCKS implementations) trySOCKS4.
- 3) By using a "socksifying" application to run your application from. Many applications are not designed with your networking problems in mind and do not offer to run using a web or SOCKS proxy. Many of them work well with Your Freedom if you run them from inside a "socksifier". That's an application that foists a modified Winsock DLL to the application which redirects all network requests to a SOCKS proxy, in this case to the Your Freedom client. Examples for such applications on Windows are: SocksCap (32bit only!), ProxyCap and FreeCap. They are covered in chapter 3.2 on page 41. Using a "socksifier" might also be an option if you cannot configure your application, e.g. because you don't have administrative rights. It's tricky however to override existing proxy configurations this way.
 - 4) By using outbound and inbound port forwards. If your application only needs to access one particular server via atop connection on a particular port, it's probably most convenient if you create a mirror image of this port on your PC, and access your local PC on the mirror port instead. Similarly, you can create a mirror image of a port on your PC on our servers and make it accessible to others on the Internet¹¹. This is covered in chapter 6.1 on page 66.

¹¹Your account profile needs to permit this. Currently, only owners of TotalFreedom packages can redirect server ports to their local PC.

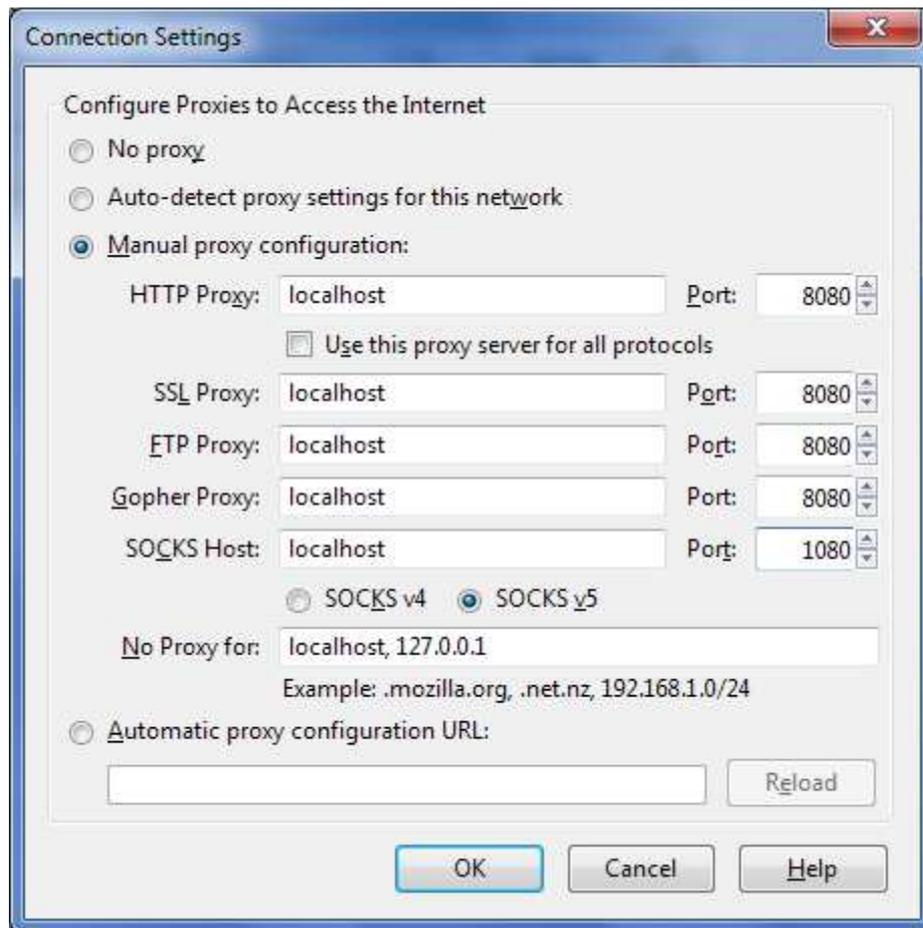
Setting up Mozilla Firefox

All web browsers support the use of web proxies, and option 1) should be just fine.

Click on “Tools”, “Options”. Choose the “Advanced” panel. Then click on the “Network” tab. The configuration windows should now look like this:



Now click on “Settings”

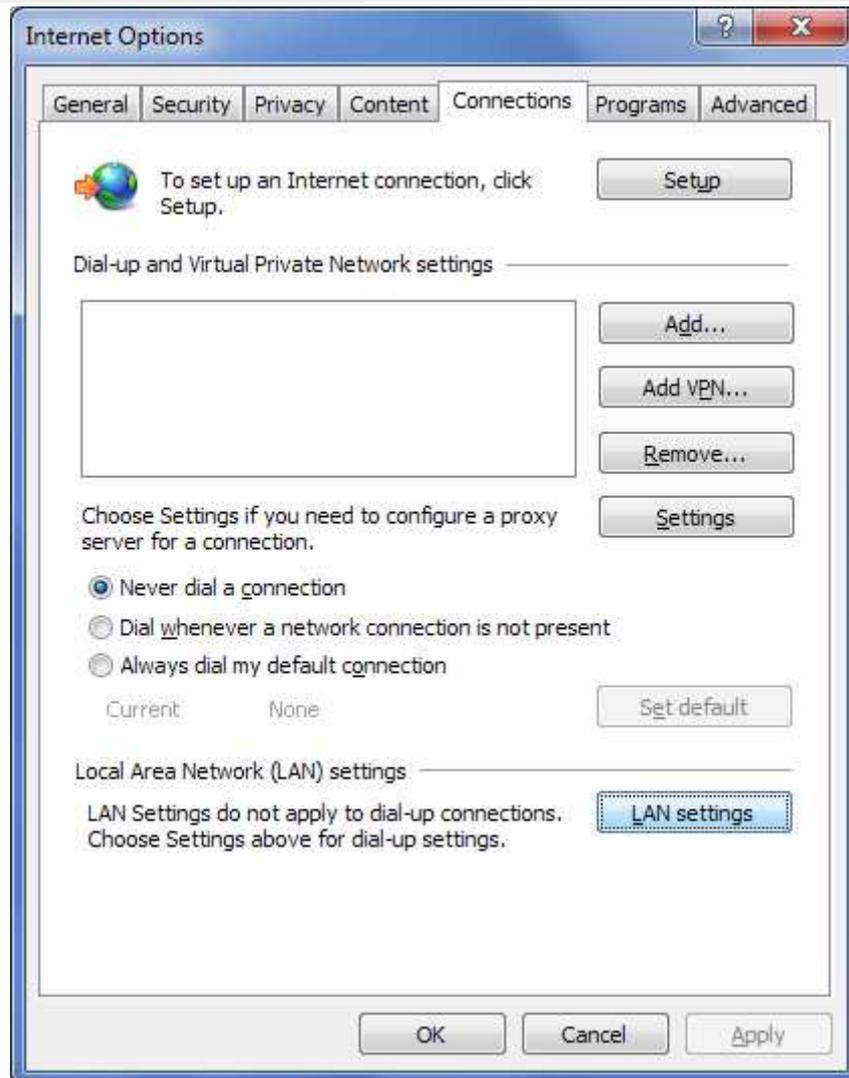


Fill in the values as shown (making a note of the original values so you can revert to you previous configuration when you are not using Your Freedom), then click OK in both windows. Firefox now uses the Your Freedom connection.

Setting up Internet Explorer

Like all browsers, IE supports proxies directly. What's more, IE's proxy configuration is actually shared by many other applications as well.

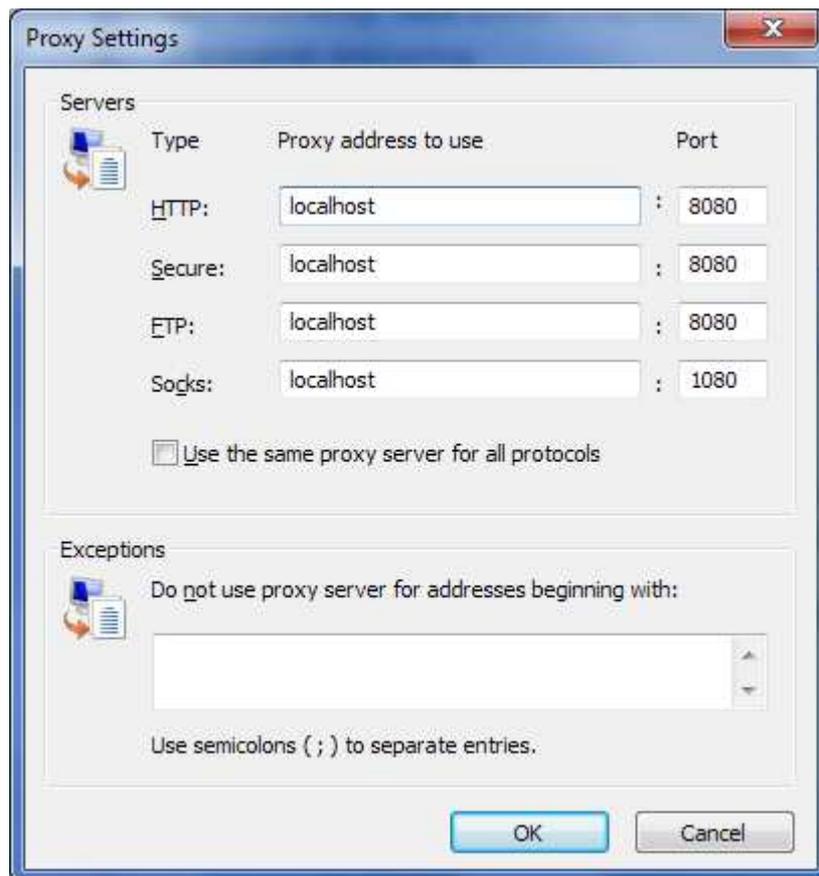
Select “Tools”, “Internet Options”. Then click on the “Connections” tab. You'll see something like this:



If you are using a LAN connection, click on “LAN Settings”, otherwise choose the connection you use to connect to the Internet and click on “Settings”. A window similar to this one will open:



Tick the checkboxes for “Use a proxy server” and for “bypass proxy server for local addresses”. Then click on “Advanced”. Another window will open:



Fill in the values as shown. Then click “OK” in all the windows. Internet Explorer now uses the Your Freedom connection (and consequently only works when the connection is up).

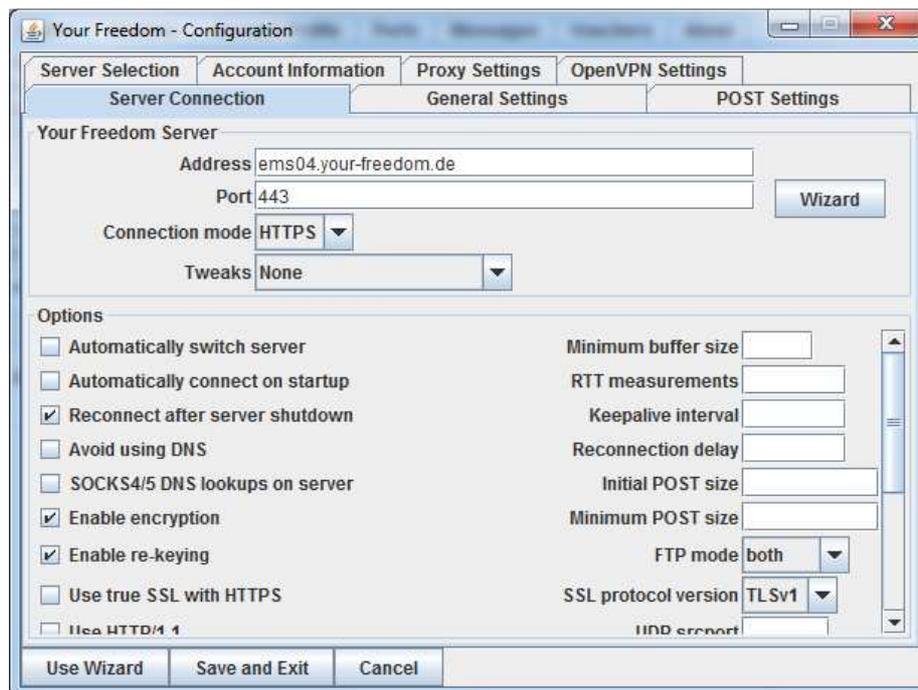
We recommend you make a note of the original settings that allows you to revert them when you are not using Your Freedom.

2.5 Manual Configuration

Most options can be configured using the “Configure” dialog available from the Status tab, but a few are only available via the configuration file. We recommend that you avoid messing with the configuration file unless you are advised by us or think you know what you are doing. ☺

2.5.1 The Your Freedom configuration dialog

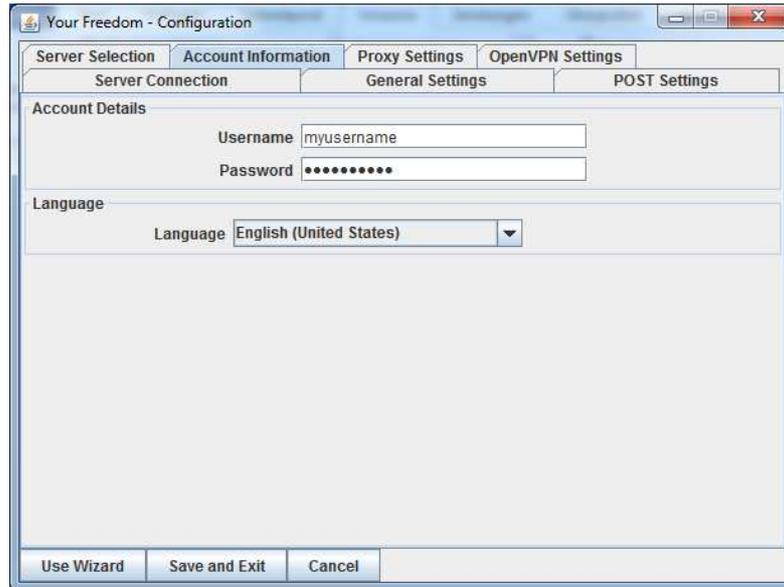
Go to the “Status” tab of the Your Freedom client, then click “Configure”. A dialog window like this should open up:



On the “Server Connection” tab, configure the Your Freedom server name or IP address (several names or IPs can be separated by semicolon – but no additional spaces!). Select the connection protocol from the pull-down menu, and the default port should automatically appear (change if necessary). Or use the wizard to see your server connection options and let the client choose the best way (but configure the proxy settings first if you need to use a proxy!).

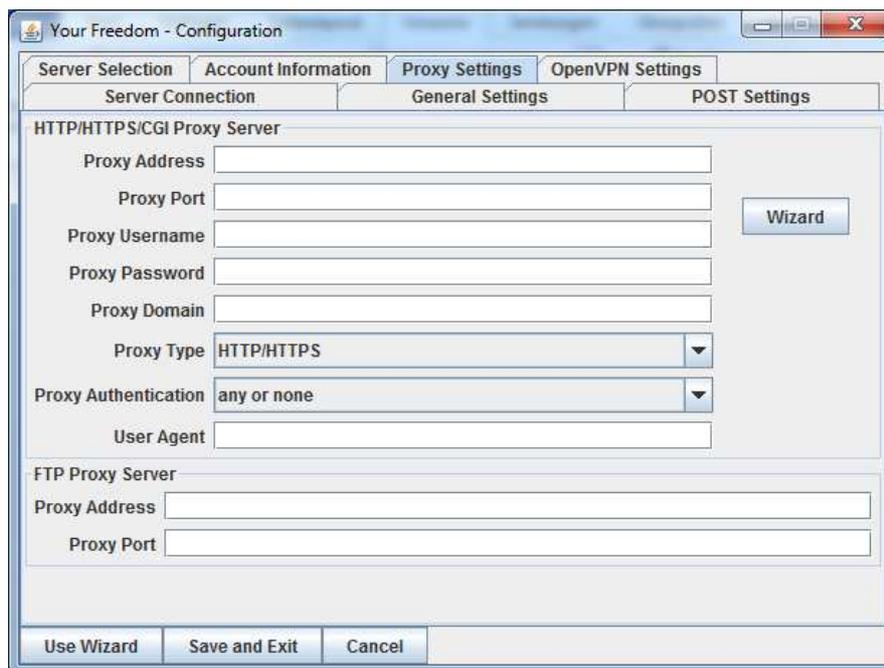
Also, select the connection options as well. For most people the defaults should be OK; you might want to tick “Avoid using DNS” as well if you only want to try known IP addresses for the YF servers and not ask your local DNS server. It is not advisable you enable the “Automatically switch server” option, and it will likely not be available anymore in new releases.

If you click on the “Account” tab, you’ll see this:



The screenshot shows the 'Your Freedom - Configuration' dialog box with the 'Account Information' tab selected. The 'Server Connection' sub-tab is active. Under 'Account Details', the 'Username' field contains 'myusername' and the 'Password' field is masked with dots. The 'Language' dropdown menu is set to 'English (United States)'. At the bottom, there are buttons for 'Use Wizard', 'Save and Exit', and 'Cancel'.

Fill in your Your Freedom username and password, and choose a different language if you like. Many texts and messages are available in other languages and it may be easier if you change the setting. Note that you have to restart the client to make the change effective when you are all done.



The screenshot shows the 'Your Freedom - Configuration' dialog box with the 'Proxy Settings' tab selected. The 'General Settings' sub-tab is active. It features sections for 'HTTP/HTTPS/CGI Proxy Server' and 'FTP Proxy Server'. The 'HTTP/HTTPS/CGI Proxy Server' section includes fields for 'Proxy Address', 'Proxy Port', 'Proxy Username', 'Proxy Password', 'Proxy Domain', 'Proxy Type' (set to 'HTTP/HTTPS'), 'Proxy Authentication' (set to 'any or none'), and 'User Agent'. A 'Wizard' button is located to the right of these fields. The 'FTP Proxy Server' section has fields for 'Proxy Address' and 'Proxy Port'. At the bottom, there are buttons for 'Use Wizard', 'Save and Exit', and 'Cancel'.

There's a lot you can configure here. You might want to use the wizard to configure a web proxy but you don't have to, there's not much difference but the client will check if your settings appear to be correct. If you know the details, just fill them in. You'll probably need to configure the address (host name or IP address) and the port. If you need to authenticate on the web proxy, fill in username and password as well, and if it's an NTLM authenticated proxy add the windows domain name as well. (In this case, username, password and domain are probably the same values that you use to log in to your PC!)

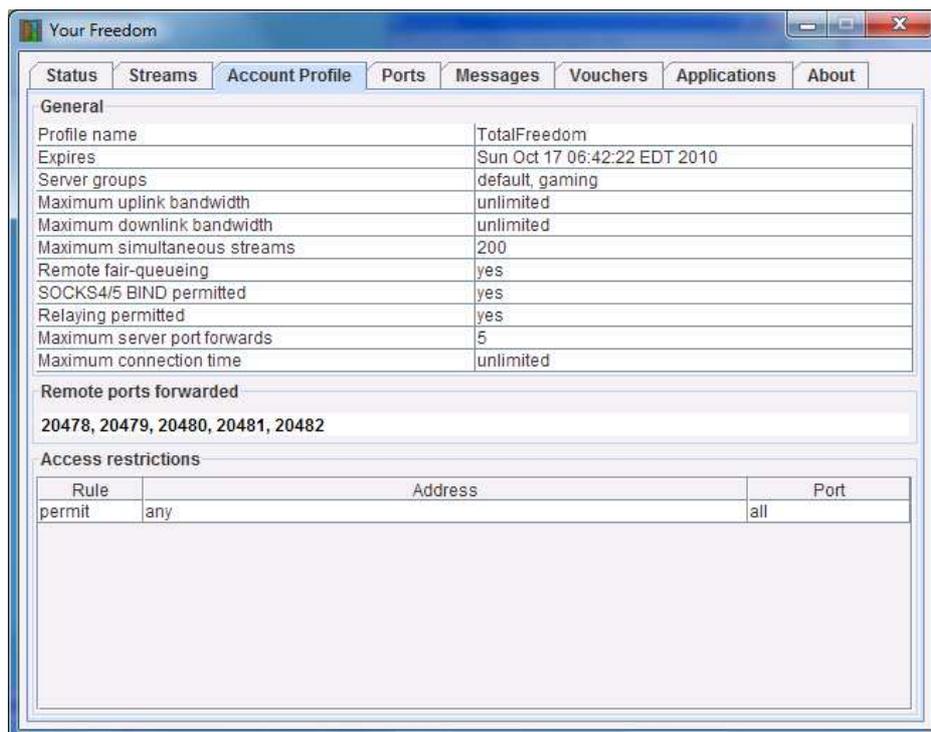
If you intend to use the FTP connection method and you cannot directly FTP to servers on the Internet, there may be an “FTP proxy” on your network. (Don’t bother to configure anything if you can use the “ftp” command line tool!) The port will likely be 21, but you’ll need the hostname or the IP address as well – ask someone who knows, there are legitimate needs to use FTP outside web browsers.

The most common connection scenarios are also covered by the Wizard available through the button on the bottom – it’s the same that is run when you start the client for the first time and it’s described in detail in chapter 2.3 on page 16.

When you are done, click on “Save and Exit” to save your changes, or on “Cancel” to abort them.

So much for setting up the connection. You should now be able to start it up from the Status panel. The connection indicator (the door) should open, a question mark should appear while client and server negotiate, and disappear after a few seconds. If it doesn’t disappear, your connection settings don’t work. Have a look at the “Messages” panel. If you can’t get the connection to work, check out chapter Appendix A to see how you can help us to help you.

Once you are connected, check out your connection profile by clicking on the “Account Profile” tab. It should look somewhat similar to this:

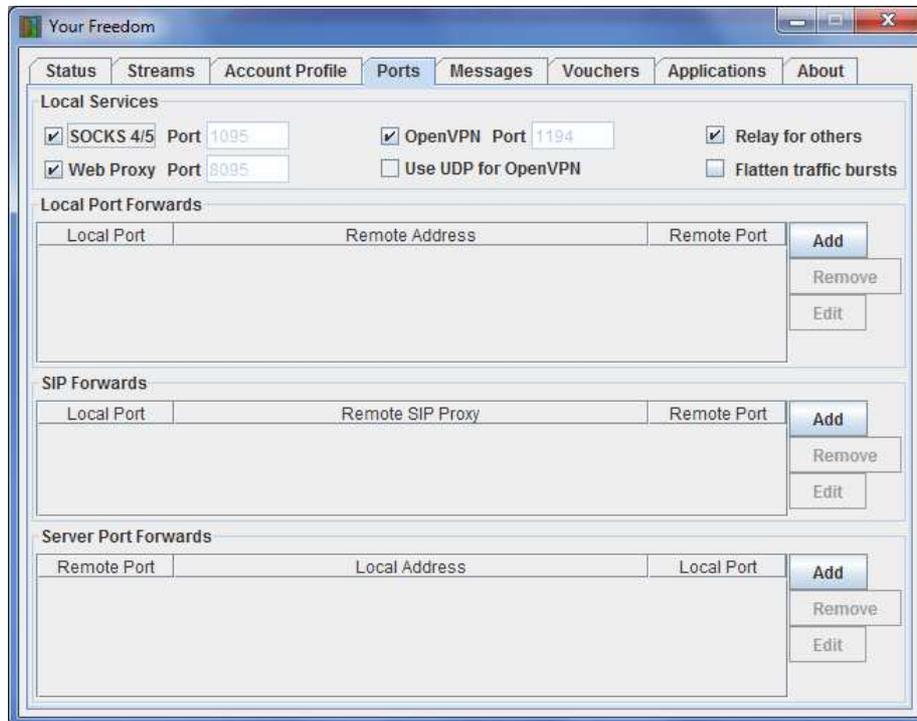


Most things in here should be fairly self-explanatory, except maybe for “server groups” and “remote port forwards”.

“Server groups” will indicate the groups of servers to which you may connect. Multiple permitted groups are separated by comma. Everyone will have the “default” server group on their profile, meaning that you may connect to every Your Freedom server in the “default” group (at the time of writing, all servers are in this group, but this may change).Some

accounts have additional server groups in their profile, depending on bought packages. “All” will not show up in customer profiles.

If your profile has any server ports assigned, they will show up in the “remote ports forwarded” line. The numbers there mean that these ports on the Your Freedom server will be forwarded to your PC when you are connected, and you may use them in the “server port forwards” configuration (see below).



All options in here can be changed while the connection is active and will have immediate effect. If you wish to modify the local ports on which your PC becomes a web or SOCKS proxy, uncheck the service first, then change the port number, and tick the box again. If you would like your PC to accept requests from other PCs on the local network and forward them through your Your Freedom connection, tick the “Relay for others” box. Note that this will only have an effect if your profile permits it (check the “Relaying permitted” line in the “Account Profile” panel as shown above).

2.6 Starting and stopping the connection

2.6.1 Each user may only log in once

That’s right. Each user can only log in from one PC at the same time. If you try to log in using the same user account from another PC or another instance of the client, the previous session will be terminated. This means that you will always be able to log in, but so will everyone else who knows your details –and he or she will kick you off. The servers talk to each other, it doesn’t help to just use different servers.

2.7 Choosing the right server

2.7.1 Server location

The YF server should ideally be close to the YF client or close to the servers you intend to use through YF. Just think about it as a triangle: the corners are your PC, the service on the Internet, and the YF server on top. The more the triangle looks like a straight line between you and the service (i.e. the flatter it is), the better.

Let me give you an example. If you are located in the US and the service you are using (let's say you are playing an online game) is also US based, a server in Europe will probably be a bad choice. The laws of physics make it impossible for information to travel faster than the speed of light¹² and putting 20.000 kilometers of additional wires or fibers and a dozen of routers between you and the service will increase latency.

It is ideal to use a YF server that is close to yourself. Why? Because you'd normally use more than one server on the Internet and you cannot find a YF server that is topologically close to *all* of them, but you may be able to find one that is close to *you*. On the other hand, for applications that don't care too much about latency (like large file transfers) the server's location is not important. Try the different servers to see which one is good for you.

The YF client will tell you where the server is located when you are connected (and also in the connection wizard). Unfortunately we don't have many servers outside Europe, simply because

- a) They are unaffordable – unmetered high-bandwidth dedicated servers are vastly expensive in most places outside Europe.
- b) the providers are too restrictive in what you may do with the servers and what not – we are sick and tired of endless and fruitless discussions with US based providers and explaining their droid staff what we do and what we don't do, and why it's not illegal, and why it's rubbish that the server's IP appeared in some robot email.

If you know about good providers we would like to hear from you! But please consider that an average Your Freedom server generates between 1 and 8 terabytes of traffic per month and needs at least 2 GB of RAM and a decent multi-core CPU. And it should come with Debian Linux. If it's less than 100 US dollars per month, that would be great. ☺

2.7.2 Protocols

Not all our servers permit¹³ all protocols. Some providers (you got it – they are mostly US based) place protocol restrictions on us and are having kittens every time they believe that they have spotted something, and what's even worse, they won't listen to any arguments. So if we want servers there (and we do, to provide a good, responsive service to those of you who need it!) we need to restrict some protocols on them.

If your application doesn't work as you would expect, have a look at the message window of the YF client. Are you seeing messages about a denied protocol? It means that you'll have to use a different server.

¹² I know this may be not entirely correct, but it is for the Internet.

¹³ All servers allow all *connection* models; this is not about how you connect with the Your Freedom client to the Your Freedom server, but what you do through the connection.

Generally speaking, use a server in Europe whenever you can if you are worried about protocol restrictions.

There is one restriction that applies to all servers: SMTP to remote servers is not permitted. Instead, all SMTP connections are redirected to one of our servers where submitted email is checked for viruses and SPAM content before it is passed on. This is only important if your mail application must connect to a specific mail relay – normally it won't be a problem (but it means that you'll likely have to disable transport level encryption). Also, we have extensive protection mechanisms against spamming built into the servers – you won't be able to rapid-fire deliver emails via Your Freedom. A normal user won't notice at all but for spammers it's a pain in the backside, and meant to be one. ☺

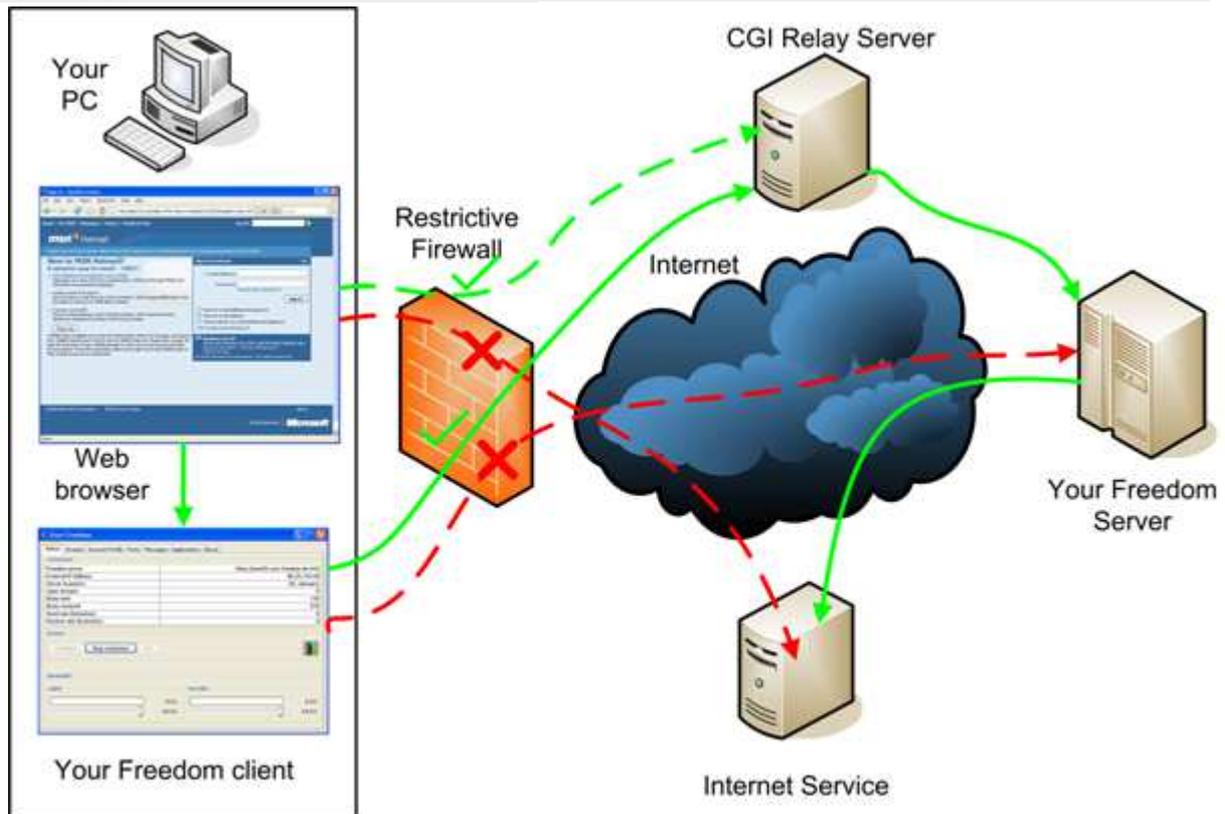
2.7.3 CGI relays

The CGI connection method adheres so much to the standards that it does not only fool proxies, it also enables us to put an intermediate CGI script in-between. Yes, that's right, there is a simple PHP script that people can put on any web servers they control, that can in turn provide a Your Freedom connection to those who don't have access anymore to any of our servers. Our idea is that it's fairly simple to block all our IP addresses as they pop up because we cannot have new ones every day, but it won't be possible to do something about thousands of new URLs every day that haven't got anything in common.

It is quite obvious why people would like to use such a "CGI relay" – because they have to. There is no other reason because obviously, this method is not as fast and interactive as the other connection methods. But when you're desperate and no other way of connecting is left, it's better than nothing. But why would people put the script on their web servers when all they get for it is a lot of additional traffic?

That's simple. There is a rewarding scheme. Every time you use their relay server, they'll get bonus points that they can use towards purchases on our web site. If you are considering providing a relay, check out <https://www.your-freedom.net/?id=cgirelays> for details. But be aware that such a relay could easily create hundreds of gigabytes of traffic per month, and that your provider probably doesn't like it if you run it on a virtual server.

So how do you use such a CGI relay? You need to know the "URL". I put it in double quotes because you don't need a full-fledged URL – you need the server name and the URI. For example, if the script could be accessed in a web browser using the URL `http://some.server.somewhere/some/path/script.php`, the CGI relay would be called `some.server.somewhere/some/path/script.php` in Your Freedom. Simply use it as the server name, choose CGI as the connection model, and definitely disable automatic server switching.



And how do you know about these? Well, that's another matter entirely. We won't publish any lists and we would ask that you do neither. Why? Because we don't want these lists to simply get imported into URL blacklists. But the YF client finds the relays. No, we won't say how, figure it out. :-)

If you would like to set up such a CGI relay, you can download the script at https://www.your-freedom.net/ems-dist/enduring_freedom.php-RENAME. Have a look at the first lines – you need to choose which server you would like to relay to and put the server's name in. Save it under an inconspicuous name (use the right ending). Then test it please (use your web browser– you should see a long text page with loads of garbage – don't worry, that's fine). If it works, register it on our web page (<https://www.your-freedom.net/?id=cqirelays>, log in first to ensure you get the credit!). Our scripts will test it automatically and if it works they will add it to the database and make sure that clients can find it (it takes a while though; don't expect clients to use it immediately).

Btw. you are welcome to set up CGI relays for your own personal use only as well, you don't have to register them. Feel free to tell others about it, and publish the URL if you like. Just if you decide to register it, don't publish it. If you have before, simply change the name or the path or set up a copy. Do that frequently, it helps! Remove very old copies from time to time, they get unregistered on our web page automatically since our servers check their existence from time to time (but you can do so as well).

3 Connecting applications and games

Please note: This whole chapter is only applicable to the desktop version, not the Android application. On Android, you do not need to configure anything to make your other applications work with Your Freedom.

3.1 Introduction

Apart from browsers, there are many applications that can benefit from Your Freedom and connect to the Internet. From terminal clients, chat and instant messengers (like GTalk, Pandion or Yahoo Messenger), P2P technologies (like BitTorrent), to games can be configured to connect via your-freedom.

This chapter covers some concepts necessary to make your particular application work.



For more specific techniques like local and server port forwards see chapter 6.1 Port Forwards on page 66

3.2 Using “socksifiers”

If your particular application does not support the use of web or SOCKS proxies, it still doesn't mean that it cannot run with Your Freedom. Since the Your Freedom client is a full-blown SOCKS server, all you need is to “socksify” your application. There are several ways to do this, all of them basically use a feature called dynamic link library preloading. Since people hate re-inventing the wheel they came up with code libraries that get dynamically linked to the application at execution time. Like every other operating system, Windows, Linux, MacOS etc. ship with such libraries, and one particular of them offers networking functions. The first time such a function is referred to by the application, the library automatically gets loaded – but only if it hasn't been loaded within the application's context already! The trick is to make sure that the library has already been loaded before the application starts – but a “hacked” version of it that knows what to do with a SOCKS server.

3.2.1 Windows

There are many socksification tools on the market; here are some examples:

WideCap

WideCap is a free socksifier that integrates with the system network stack and does not rely on pre-loading a library like some other socksifiers. It works with many games and applications that cannot be used with socksifiers like SocksCap and FreeCap. We know it works well with Steam powered games. Find it on <http://www.widecap.ru/eng/>.

SocksCap

This is an old but popular socksifier free for non-commercial home use (and not available anymore commercially). You must google for “sc32r240.exe” if you want to download it.

FreeCap

FreeCap is, as the name suggests, freeware and is available for download from the project's home page at <http://www.freecap.ru/eng/>. There is also additional documentation there but its use with Your Freedom is simple enough. We like this best because it's free and easy to use, and it's good enough for many (but not all) applications.

ProxyCap

A commercial product. Have a look at <http://proxylabs.netwu.com/>.

Proxifier

Proxifier is also a very clever piece of software. Testing for 31 days is free, a license costs USD 40. Plus it's also available for Mac OS X. Check it out on the Proxifier home page at <http://www.proxifier.com/>.

HummingbirdSocks

The OpenText Exceed connectivity suite contains a socksifier as well. It can be found on <http://connectivity.opentext.com/>.

3.2.2 Linux and other Unix derivatives

Dante

Dante is the de-facto standard in the Unix/Linux world. It's free. Download available from <http://www.inet.no/dante/>. Many Linux distributions contain a "dante-client" package. Once installed, you would normally have to configure /etc/dante.conf to redirect traffic appropriately to your local SOCKS server, and then use the "socksify" script to run applications.

Tsocks

Tsocks is another Unix/Linux world socksification tool, also free. It can be found on Sourceforge. There is a Mac OS X version as well.

3.2.3 Mac OS X

Proxifier

Proxifier is also available for MacOSX.

Tsocks

Check out <http://forums.macosxhints.com/archive/index.php/t-55338.html> for hints about tsocks for MacOSX.

3.3 OpenVPN support

3.3.1 Introduction

There is another way to make your applications connect to the Internet through Your Freedom without the need to configure them in any way! This is pretty well tested and so far has proven to be almost bullet proof versus its socksifier cousins. In theory every application that works behind a DSL or cable router also should work well though OpenVPN mode.

3.3.2 Prerequisites

The OpenVPN way unfortunately has a few prerequisites that you need to meet for it to work on your PC:

Administrative rights

There's no way around it: you need to be able to install OpenVPN and use it, so you need administrative rights (on UNIX like systems: you need to be able to install the OpenVPN binary setuid root in your path). On typical company PCs with domain login you won't have administrative rights.

With Vista, you also need to explicitly run the Your Freedom client with administrative privileges (right-click, "Run as administrator"). Alternatively, right-click on the link in the start menu, choose "Properties", click on the "Compatibility" tab, then tick the "run as administrator" checkbox -- this will fix it once and for all, as long as you always use this link to run the YF client.

OpenVPN needs to be installed

OpenVPN is Freeware and Open Source (but please consider donating). If you have the ability to install software on your PC, go to <http://openvpn.net/download.html> and download OpenVPN. It needs to be at least 2.1_rc20, newest release should do. For Windows there is an installer, others need to compile OpenVPN from source – or maybe it ships with your OS's distribution? In any way, if you open a command shell and type `openvpn` you should see hundreds of lines of instructions; if not, it's not properly installed. OpenVPN needs to install a tunnel interface on your PC; on Windows it's called `TAP- WIN32`, on Linux this would be `tun0`.

For users of Windows Vista, Windows 7 and above it's recommended to configure the `openvpn.exe` executable to run under administrative privileges. Go to "C:\Program Files\OpenVPN\bin", right click on the `openvpn` executable, select "Properties", "Compatibility", and mark the "Run as Administrator" checkbox. This will ensure the `openvpn` process gets launched with the necessary privileges.



Before making use of OpenVPN please make sure your computer is properly protected and not infected by some virus/worm or a Trojan. Ensure that it is not part of a bot net. If you don't our servers might have to close down your account to protect our systems. If you do not have a proper security suite installed on your PC please open Internet Explorer now and visit this web page for a free check (it is a Microsoft tool and will therefore only work in Internet Explorer): <http://onecare.live.com/site/en-US/default.htm>

We strongly advise that you repeat this from time to time. It is for your own protection! If you haven't got other protection consider installing free protection software like Microsoft Security Essentials, Avira Antivir or avast.

You don't need a Your Freedom package, FreeFreedom will suffice

That's right. Our OpenVPN support is not only available to paying users. Although running an OpenVPN tunnel endpoint uses considerably more resources than just forwarding connections; we decided to offer it to everyone for free. Although we know that it wouldn't be much fun with 64k.

3.3.3 Configuration tasks

Know your networking environment

If you are behind a firewall and need to be able to reach servers that have Internet IP addresses but are not reachable from the Internet, you need to add route exclusion lines to your config file (see Appendix: YF client configuration file).

99% of all users won't have to configure excludes. All non-Internet IP addresses are automatically excluded anyway (this covers 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16). Networks that are already routed on your PC are excluded as well.

For all others, add an `openvpn_exclude` line per IP or network as described in Appendix C, e.g.

```
openvpn_exclude 1.2.3.4
openvpn_exclude 2.3.0.0 255.255.0.0
```

Note that Your Freedom is clever enough to automatically exclude all IP addresses that it needs to be able to reach in order to maintain the connection to the Your Freedom server.

Tick the OpenVPN box

Go to the Ports panel and tick the OpenVPN checkbox. Leave the port number as it is, unless there are reasons why you need to use a different port.

Start the Your Freedom connection

The connection set-up should look like usual, but approximately 10 seconds after the door opens, it should open a bit more. ☺The message log should tell you as well when it happens. Have a look at your PC's routing table (in Windows, run "cmd", then type "route print"; Unix users type "netstat -rn" or "route -n"); you should see a whole bunch of routes there all going to some 169.254.xxx.yyy address. These routes cover the whole Internet address space minus the exclusions mentioned above. We cannot replace your PC's default route; that would very likely cut you off from your local network and make the Your Freedom server unreachable.

Relay for others?

Yes, you can and you may. But unless your PC masquerades the other PCs they need to run their own OpenVPN session. When you start the connection, the Your Freedom client creates some config files in your home directory (please see Appendix C for location details) all starting with "client" or "server"; copy them to their PCs into some directory, edit "client.ovpn" and replace 127.0.0.1 with your PC's internal IP address, then right-click on the "client.ovpn" file and choose the second option (Start OpenVPN with this config file). Of course they need to install OpenVPN first!



For a more general technique to share your Your Freedom connection with miscellaneous equipment like XBox, Playstations or other PCs see chapter 6.2.2 on page 68.

What about the Windows firewall?

Feel free to use it, but don't complain if it breaks things. ☺ Seriously, there is no reason why you would need it, only outbound connections work on the tunnel interface. However if you suspect your applications to secretly open connections, then yes, use it! If something doesn't work, try without.

3.3.4 Configure your applications

Now that's the part you'll like most: you don't have to! No need to configure a proxy, no need for socksifiers. Just make sure your applications are not using any proxy and that should be it.

Note however that since your PC is not connectable from the Internet through the OpenVPN tunnel, applications who rely on this won't work. If the manufacturer's web page says something about ports that have to be opened inbound in your firewall, it likely won't work.

It is possible to combine OpenVPN tunneling with server port forwards, however. See chapter 6.1.3 on page 67 for details.

3.3.5 Troubleshooting

The OpenVPN tunnel is not coming up properly

Have a look at the message log, it may tell you why. If it doesn't, create a dump file and mail it to us (see chapter Appendix A: "creating a dump file") – or check it out yourself.

Check if there is still another OpenVPN process running when the Your Freedom connection is shut down. Hit Ctrl-Alt-Del, sort the tasks by name, and look for "openvpn". Terminate it before you restart the Your Freedom connection. This can happen if the Your Freedom client is terminated abnormally before it has a chance of shutting down OpenVPN.

The OpenVPN tunnel opens, but then the Your Freedom connection fails

The tunnel routes somehow cut off your connection to the Your Freedom server. Please generate a dump file for us; the Your Freedom client should be clever enough to avoid this but seemingly isn't.

What are these 169.254.xxx.yyy addresses?

That's a class B network reserved for ad-hoc networking on a broadcast medium like Ethernet. Every station just rolls a dice for an IP address and does some checking whether it's already in use. If not, it uses it.

No-one uses this network for anything, only Windows does in the absence of a DHCP server or a static configuration. The network is not routed on the Internet and no-one uses it

privately, that's why we chose it. It's very unlikely that it causes any addressing conflict anywhere.

The other end of your OpenVPN tunnel is always 169.254.0.1 or 169.254.128.1; if you want to check what packet delay is added by Your Freedom, just ping this IP address!

Your PC will get an odd address from a /30 subnet within this range and it will route everything to the even counterpart address in this subnet.

4 Using Your Freedom without client app

4.1 PPTP

4.1.1 General information

The normal way to use our service is through the Your Freedom client software. It will let you do things that you normally cannot do with VPN software. But there are times (and places) where you only need to ensure you get connected without someone spying on you, or you only need to appear to be elsewhere and not where you really are. If this sounds like you, read on.

The Your Freedom connectivity servers are now able to accept PPTP VPN connections too. PPTP is a VPN tunnel protocol developed by Microsoft and some more companies not renowned for designing good protocols; in fact, PPTP is pretty much broken by design in many aspects. However, it does have one advantage: nearly every PC, nearly every smartphone speaks PPTP without any additional software. Contrary to well-designed protocols like OpenVPN, PPTP uses a combination of TCP for the control connection and GRE encapsulated PPP frames for the data transport. That by itself is not too bad. But if you consider that you need to use MSCHAPv2 and MPPE-128 for authentication and encryption if you want at least some bit of protection, and that each of these two are again completely broken by design, this is where the mess starts. But you don't have to worry about the dirty details, we have done that for you.

Nevertheless, it's "the" standard and it is very widespread, plus it is relatively secure when used properly. And it gets the job done.

When would you want to use PPTP? Here are some examples:

- When connected to a public wireless hot spot without encryption, using PPTP will ensure that no-one can see what you are doing.
- If you live in country A and you would like to make it look to some Internet service like you actually live in country B (great if you want to watch TV broadcasts not available for your country!).
- If you are in a censoring environment but the censoring is only very subtle -- some things just don't work and it always looks like technical faults.
- If your provider is throttling a service you'd like to use, using PPTP might make things work properly (for example: YouTube is slow in some places because the local provider *wants* it to be slow).

Of course, the YF client will help you in all these situations as well. A Swiss army knife will let you turn screws too, but a screwdriver might be the better tool at times, even though you cannot cut anything with it. Should the screwdriver turn out not to be powerful enough, you can always resort to your trusted Swiss army knife.

The service level you receive (FreeFreedom, BasicFreedom, EnhancedFreedom, TotalFreedom) is the same as with the YF client application. Vouchers can be sent through our web page. You may use your account with both the client and PPTP, but not both at the same time. You'll use a shared IP address just as with the YF client.

4.1.2 Is PPTP safe?

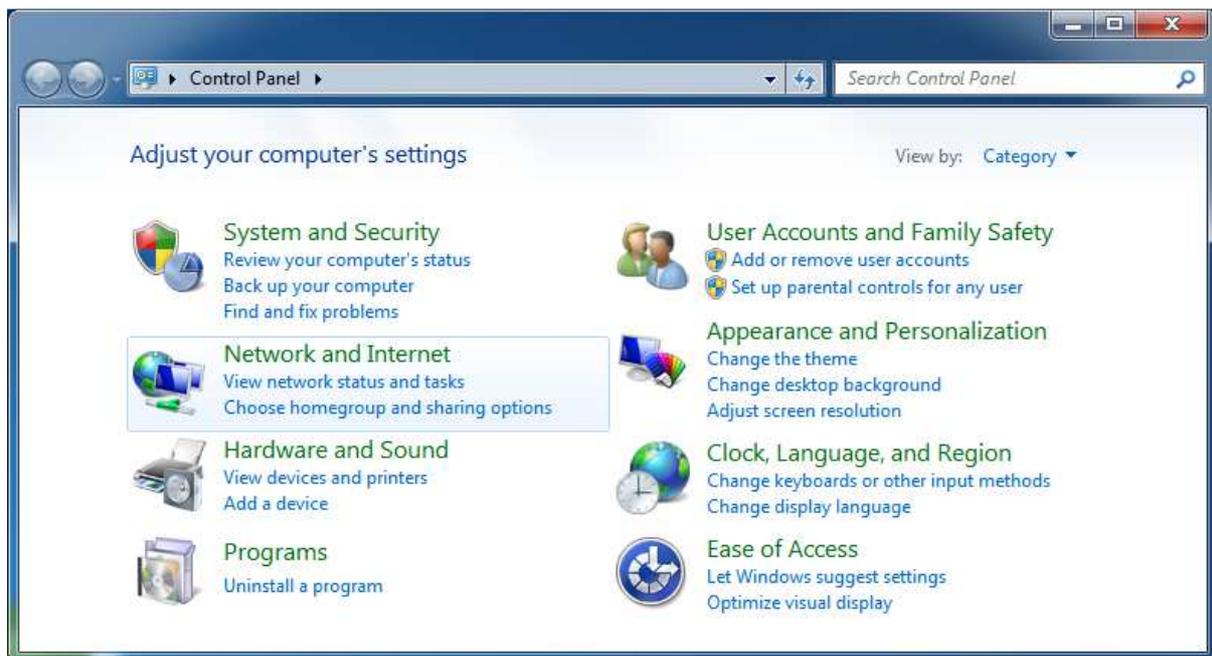
The YF client uses stronger encryption and protects your privacy better than PPTP. Still, PPTP is about as strong as using HTTPS to access web servers. It uses RC4 with a 128 bit master key and generates session keys every so often. Not exactly state-of-the-art, but it will probably do. Its biggest weakness is that it relies on a sufficiently strong password.

You might have read about attacks against MSCHAPv2. This is not exactly news. MSCHAPv2 and MPPE both rely on the secrecy of an MD4 hash of your password. If someone is able to obtain this MD4 hash, he cannot only impersonate you but also decrypt recorded data. The big problem here is that Microsoft has not "salted" the hash, and this means that pre-computed dictionaries can be used for brute-force attacks on recorded MSCHAPv2 authentication packets. Our advice is: use a very strong password. If you do, PPTP using MSCHAPv2 and MPPE is relatively secure.

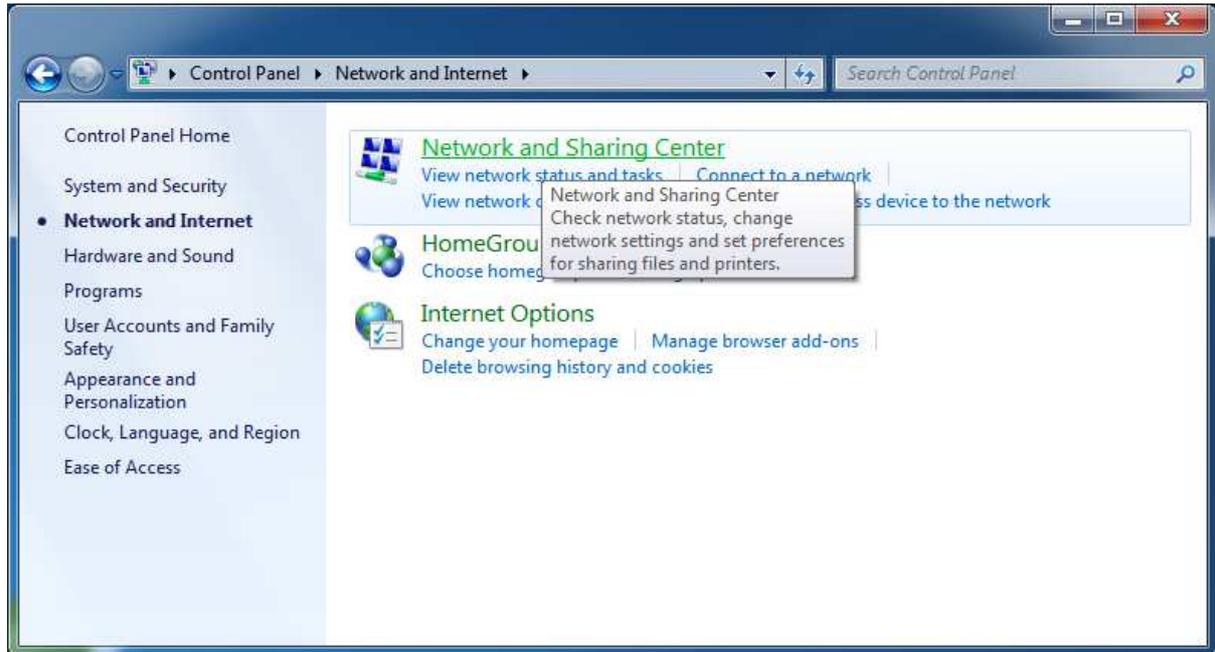
4.1.3 How to configure PPTP?

We'll explain here how to do it on Windows 7. You'll surely find information about how to do it on your system if you google for it; there is nothing particular about our PPTP service.

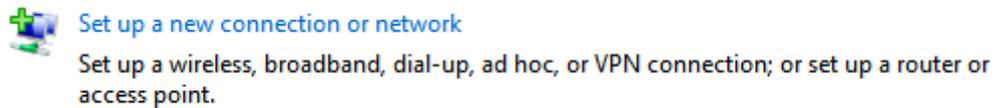
First, click the Windows button in the down left corner of the screen and chose "Control Panel". It will look like this:



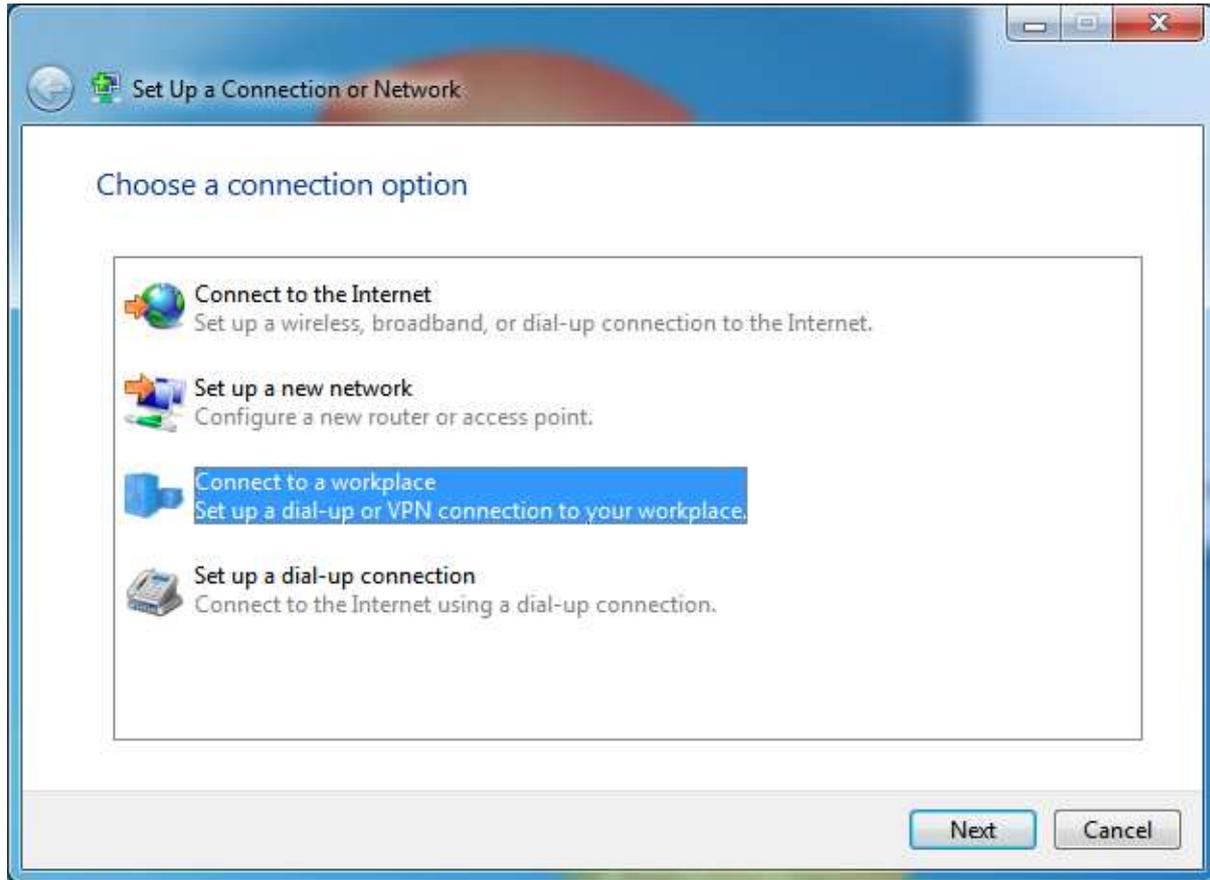
Now choose "Network and Internet":



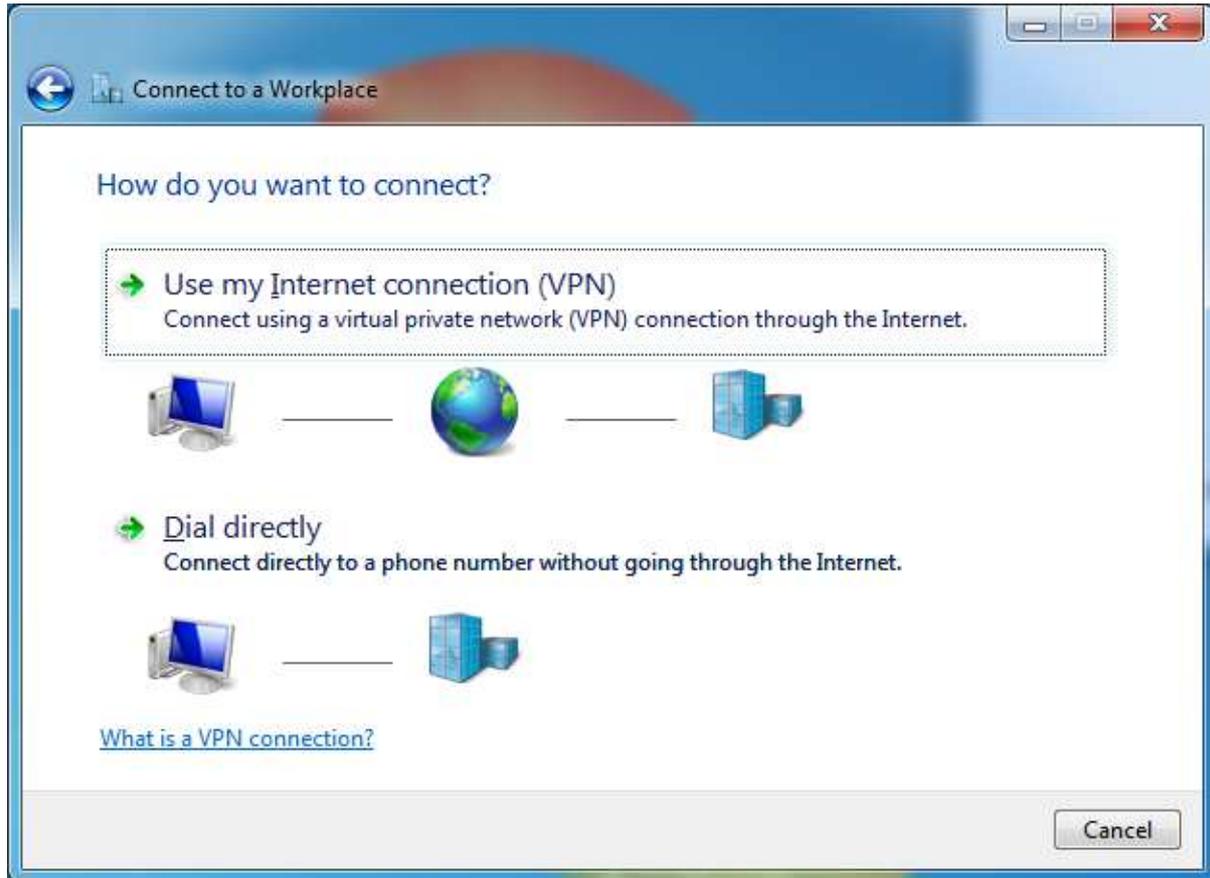
Click on "Network and Sharing Center". In the network and sharing center panel, click on "Set up a new connection or network", the link looks like this:



Choose "Connect to a workplace", even if that sounds silly (and you are probably trying to escape one), then click the Next button:

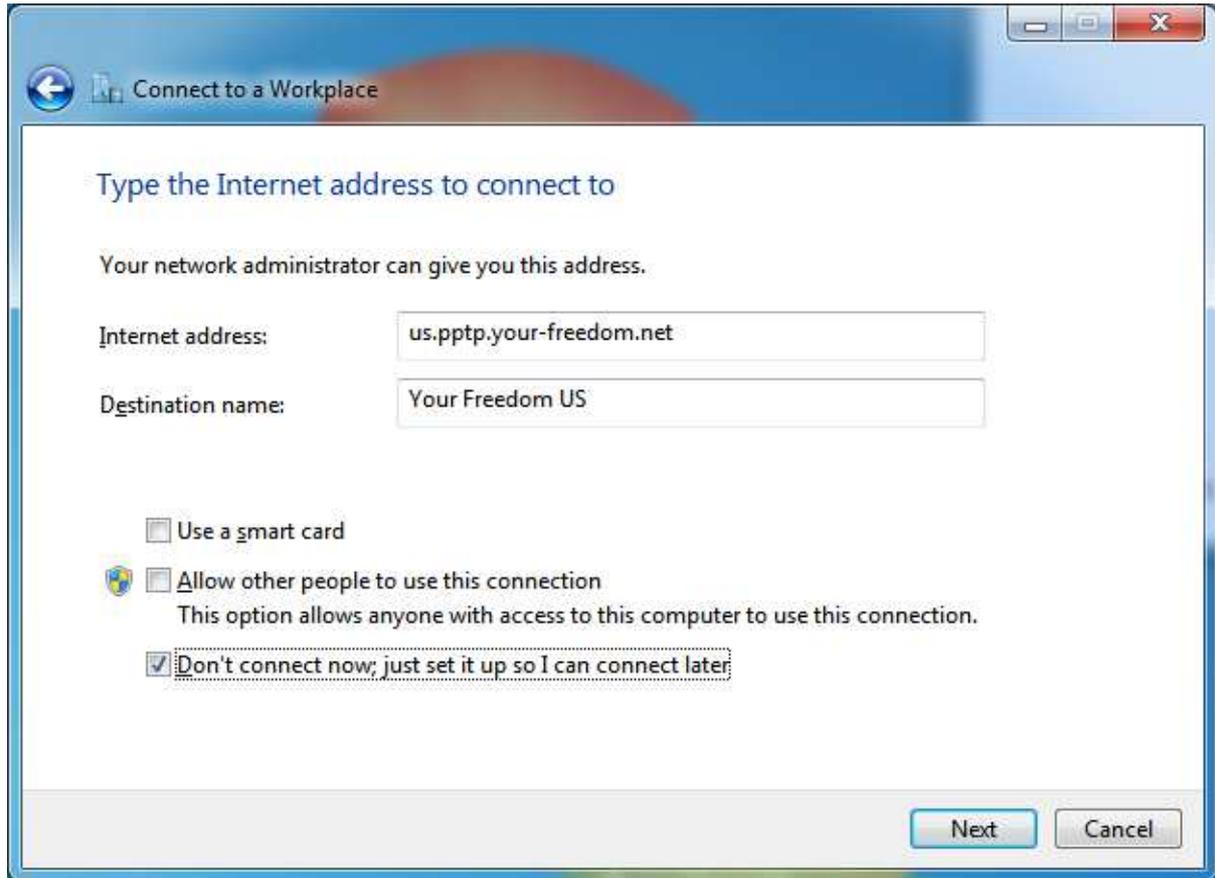


Now choose "Use my Internet connection (VPN)", because that's what we are trying to do, set up a new connection through your existing Internet connection:



In the next step, you are asked to enter an Internet address to connect to. Fill in the PPTP server of your choice. If you know the IP address or the server's name you may use this, but we suggest you use the generic by-country names we provide. In this example, we want a US based server but it could be "de" for Germany or "uk" for the United Kingdom as well. You may of course use "emsXX.your-freedom.de" as with the YF client application as well, or an IP address. The "Destination name" is what you want to call it, it has no technical meaning.

Tick "Don't connect now" -- we need to change some parameters before the connection is finally set up. When done, click Next.



In the next step, you are asked to provide your user name and password. This is the Your Freedom user name and password, as you would use it to log on to our web page or as you would use it in the Your Freedom client software. If you want, tick "show characters" (it will make typing cryptic passwords easier and is safe as long as no-one is glancing over your shoulder) and "remember password" (safe if this is your computer and access to it is restricted). Do not put in a domain. When done, click "Create".



Connect to a Workplace

Type your user name and password

User name: example

Password: mypassword

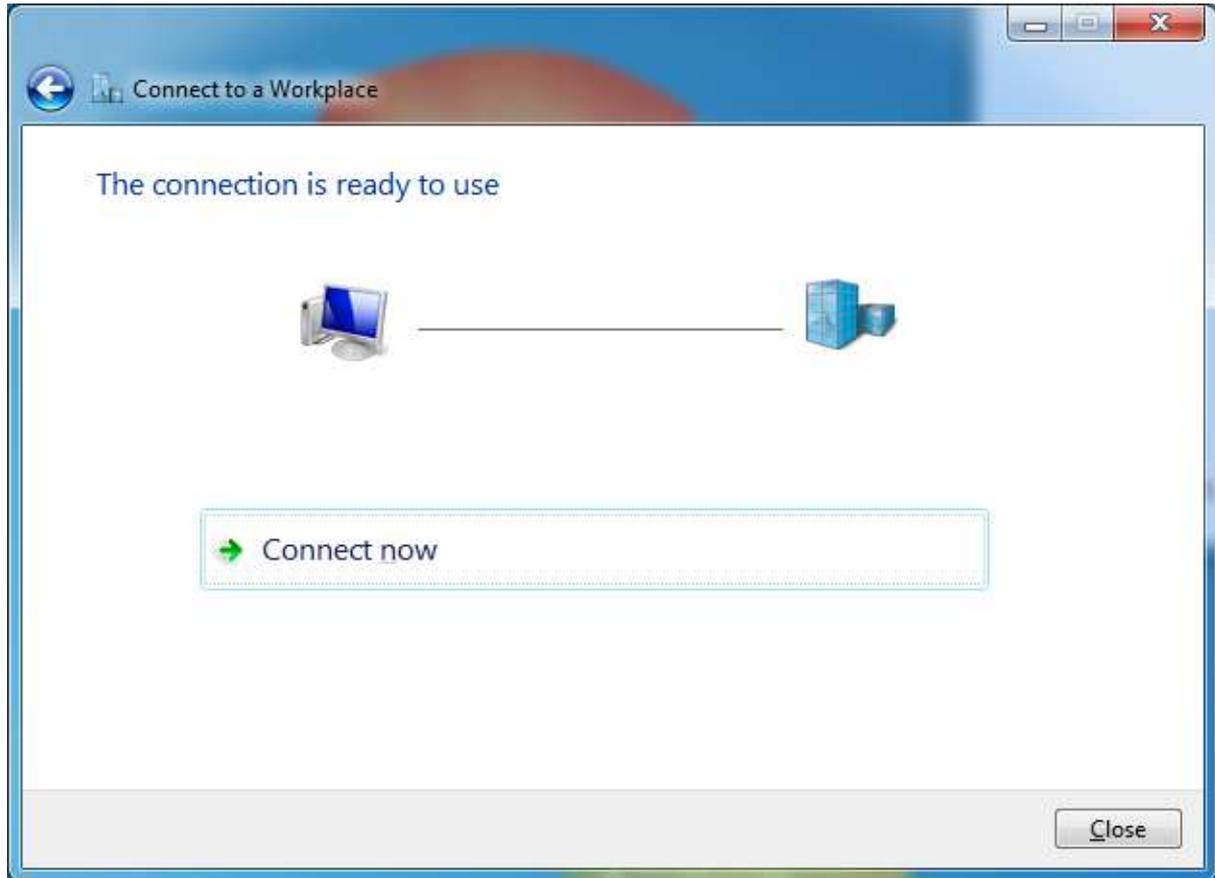
Show characters

Remember this password

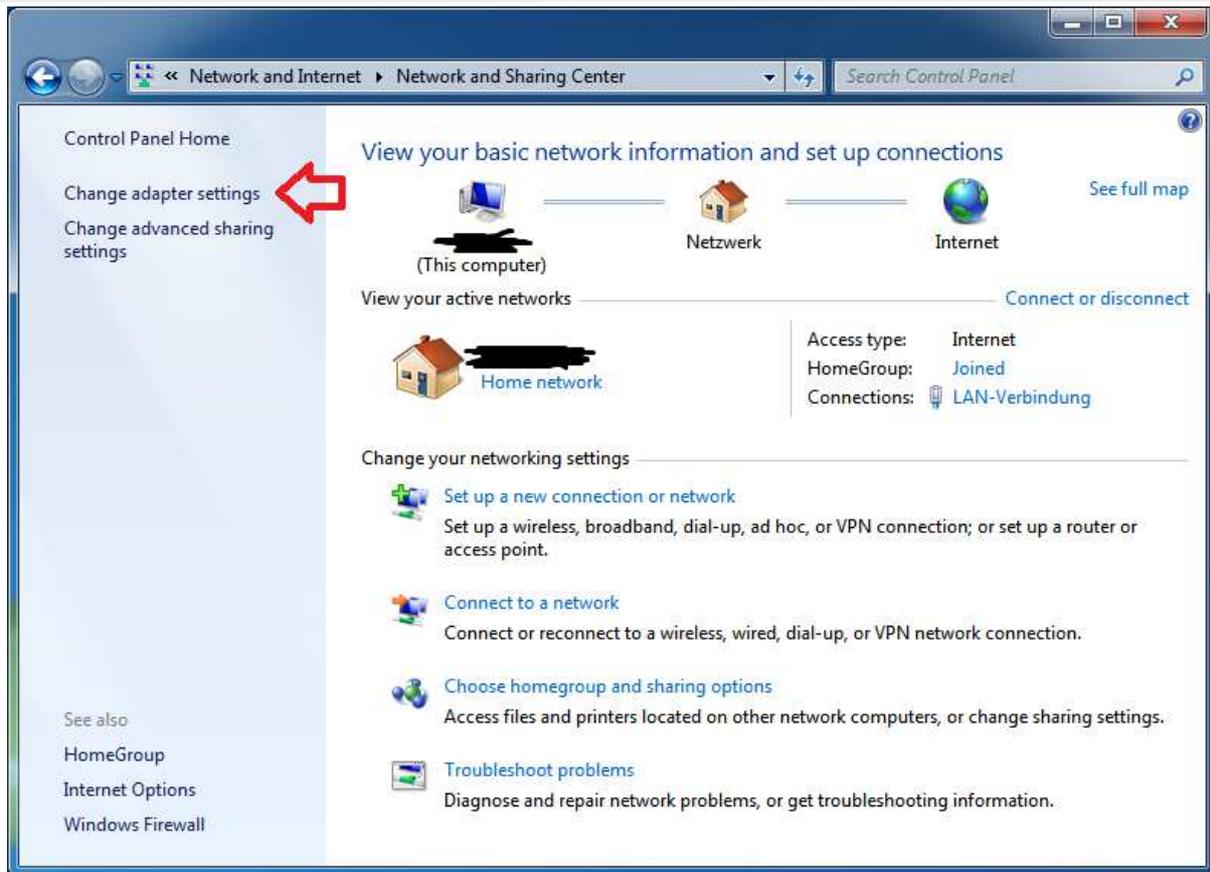
Domain (optional):

Create Cancel

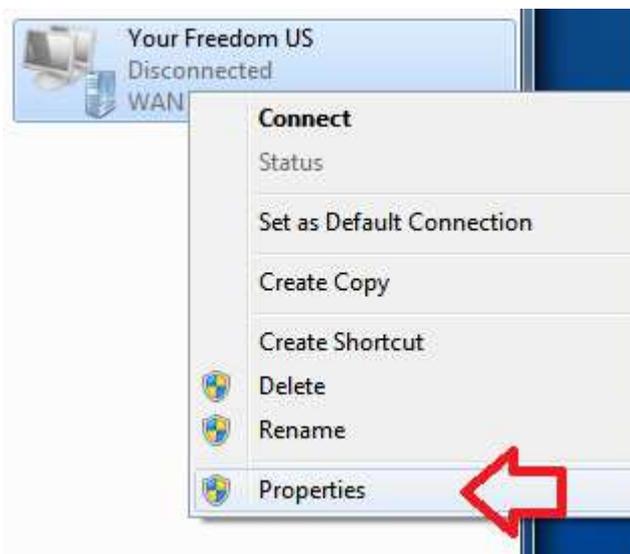
Windows will now tell you that the connection is ready to use, but it isn't. That's why you should click the Close button now.



In the "Network and Sharing Center" which should still be on your screen (if not, click the Windows button, "Control Panel", "Network and Sharing Center" to bring it up), click on "Change adapter settings" on the left hand side:

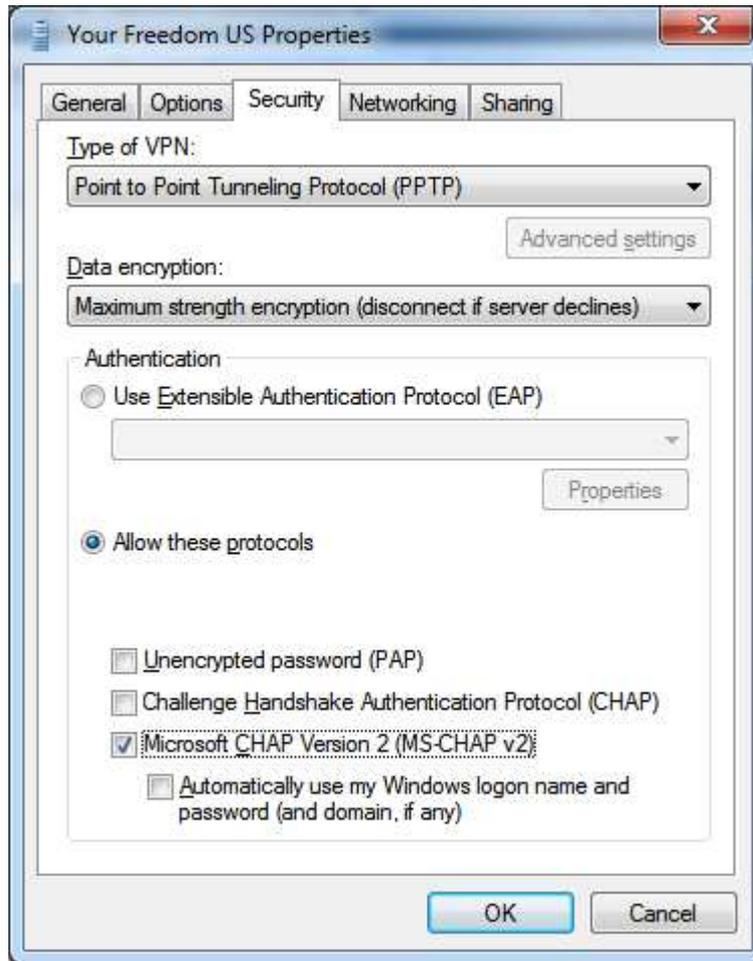


This will show your network adapters, both physical and virtual. The newly created "WAN Miniport" adapter should be among them (it will claim it is an IKEv2 type adapter, and that's why we need to modify it). Right-click on it and choose "Properties":

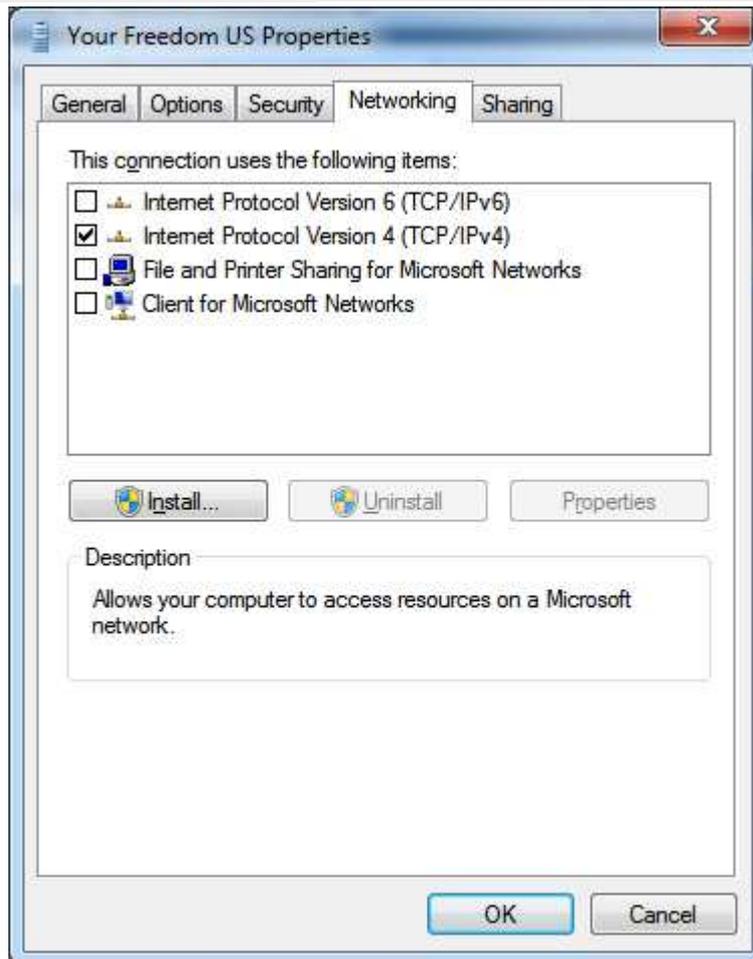


Click on the "Security" tab, then change the default settings. The type of the VPN needs to be set to "PPTP", and you should set data encryption to maximum strength encryption (though our server will negotiate that anyway). Remove the tick from "Challenge Handshake Authentication Protocol" and leave the tick on "Microsoft CHAP Version 2" -- we need to use

MS-CHAPv2 instead of standard CHAP because this is a prerequisite for MPPE data encryption. The whole tab should now look like this:



Now click on the "Networking" tab and untick everything except IPv4 (it will make the VPN connection less "noisy", conserve bandwidth and slightly speed up the connection set-up). You cannot use IPv6 at this time because our servers do not support it yet:



When done, click "OK".

Now you are ready to go. There are several ways to bring up the connection. What works for everyone is this: click the Windows button, then "Control Panel", "Network and Sharing Center", "Connect to a network". (If there is a networking icon in your task bar you may simply click on it instead.) This brings up your list of available connections:



Click on the one you want, then click "connect":



Version 3.0

Release Date: 2013-06-26

Put in your password if you haven't saved it during the set-up process, then click "connect", and off you go! There will be several status messages popping up, and once they are gone you should be connected. You can verify this in your connection list (see above) -- it will now tell you that you are connected via the Your Freedom connection. To disconnect, click on the connection in the connection list and choose "disconnect" -- simple as that.

At one point, a pop-up window will ask you to set a "network location" for the new connection. We recommend that you choose "public network" to avoid unnecessary security risks:



4.1.4 What if it doesn't work?

Are you receiving this message during the connection set-up?



It means that our server has denied your login, either because username and/or password were not correct, or your account has been disabled, or you are (as a FreeFreedom user) over the account's time budget, or there is a problem with our server. Unfortunately we cannot tell you which one of these is the reason. If the problem persists and you are sure your username and password are correct, try to log in to our web page and see if your account has been disabled. If not, check whether you are over the time budget (FreeFreedom users only -- just log in, then click on "Account"). Enabling logging won't help you at all.

If you happen to see this during the connection:



it most likely means that our server has kicked you out. Your FreeFreedom account might be over the time budget, or your account got disabled. Try to reconnect. If that works, it was most likely some technical problem (a timeout or whatever). If problems persist, note down the exact time and contact support about it.

4.1.5 Sharing the PPTP connection

You can use Windows' Internet connection sharing functionality. You'll find it in the properties of the virtual network adapter (see above). Please note that you cannot share your connection with other computers that are on the same network that you use to run the PPTP tunnel over. An example would be someone in a computer lab connected through Ethernet -- you cannot share the connection with other PCs on the same Ethernet. In order to share the connection, the other computers (Play Stations, whatever) need to be connected to an Ethernet interface that you do not use for anything else -- so put in a second Ethernet card if your computer does not have a second Ethernet interface. It is not a good idea to use the same physical infrastructure, i.e. the same Ethernet switch, since ICS runs its own DHCP service and will confuse the upstream connection.

4.1.6 DNS servers

Unless you explicitly configure something else, the PPTP connection will negotiate the use of Google's DNS servers. Google will not know who you are, they only see our server's IP address.

4.1.7 More than one pre-defined PPTP connection?

You may configure as many connections as you want, but it is not recommendable to bring up more than one at a time. For example, you could define different connections for different countries. Just follow the procedure above to set up more connections. To remove them again, open the adapter panel and delete the adapter (this is where you can rename a connection, too).

If you are asking whether you and your friend can use the same account at the same time, the answer is no. Your Freedom accounts generally only work for one person at a time. If a second connection is established, the previous connection is terminated. If you are at the same place, you can share the connection as explained above, though.

5 Account types: Time-based upgrades and vouchers

5.1 FreeFreedom (usage free of charge)

We offer a very basic service for free. It is good enough to make yourself familiar with Your Freedom and test whether or not your application will work with Your Freedom. It might be all you need, in which case you are welcome to use it as much as you like.

There are several restrictions in the FreeFreedom profile. First of all the bandwidth is low and the number of concurrent streams is low as well (but enough for chatting, web surfing, etc.). Then there is a connection time limit –you can only be connected 5 hours in a week interval, and only 2 hours in any 24 hours interval, also after one hour your session is disconnected, but you may connect again immediately.

After the daily or weekly usage limit is reached, users won't be able to connect again. You will see a message telling you about this, indicating the approximate time at which you will be able to connect again.

5.2 Upgrades and vouchers

If you would like to have more bandwidth, more concurrent streams, or other additional features, or you would simply like to support our efforts to provide unrestricted Internet access to everyone, consider buying an upgrade. The table below details all available time-based upgrades, their features, and their prices (in Euros).

	Free	Basic	Enhanced	Total
Bandwidth	64 Kbit/s	256 Kbit/s	4 Mbit/s	unlimited
Concurrent Streams	15	50	100	200
Web Proxy	✓	✓	✓	✓
Socks Proxy	✓	✓	✓	✓
OpenVPN mode	✓	✓	✓	✓
PPTP mode	✓	✓	✓	✓
SOCKS5 mode	✓	✓	✓	✓
Link encryption	✓	✓	✓	✓
HTTP connection	✓	✓	✓	✓
HTTPS connection	✓	✓	✓	✓
CGI connection	✓	✓	✓	✓
FTP connection	✓	✓	✓	✓
UDP connection	✓	✓	✓	✓
DNS connection	✓	✓	✓	✓
ECHO connection	✓	✓	✓	✓
Relaying permitted	✓	✓	✓	✓
Connection time	6 hours	unlimited	unlimited	unlimited
Server Ports	✗	✗	✗	✓ (5)
1 month package	Free	€ 4.00	€ 10.00	€ 19.99
3 month package	Free	€ 10.00	€ 28.00	€ 57.99
6 month package	Free	€ 17.00	€ 50.00	€ 109.99
12 month package	Free	€ 30.00	€ 95.00	€ 199.99

Version 3.0

Release Date: 2013-06-26

To buy upgrades, please visit our web page at <https://www.your-freedom.net/>, log in with your account, then click on the “Account” tab. There is a currency calculator as well if you’d like to convert the price in Euros to your local currency or at least one known to you. For your orientation, 1 € roughly corresponds to 1.30 US\$ (at the time of writing).

On Android, just visit the in-app shop. It will let you purchase account upgrades the same way as you can purchase apps.

When you buy an upgrade, your account profile usually gets updated within minutes (you’ll receive an email when it happens and you’ll notice if you are connected). However some payment methods take longer than others to complete. Please visit our “Prices” page on <https://www.your-freedom.net/> to learn about details (log in first to see everything). Newly bought packages are instantly activated; other packages that have not expired yet get suspended. However you may use the arrow buttons on the “Prices” page to move your packages around anytime and decide which of your packages is currently active and which are suspended¹⁴.



Please consider buying a package if you use Your Freedom regularly, even if FreeFreedom is enough for you. Servers don’t grow on trees and support staff and developers like the occasional pay-check as well.

5.2.1 Vouchers

Voucher codes are sequences of characters that you can fill into a form either in the website or directly into the Your Freedom client to create packages. You receive a voucher code from us as part of a promotion or as a compensation for service problems, or as an expression of our gratitude for something you helped us with. You can also buy vouchers from us in several denominations as voucher carnets. Our vouchers are valid for one year from the day of purchase.

Our voucher carnets can be used to temporarily upgrade your Your Freedom account with a package without having to pay for a full month and not use parts of it. Also voucher carnets are transferrable (i.e. not linked to an account) and can be used separately at any time.

Voucher codes can be added to the voucher panel in the YF client. Simply type in the code (case does not matter) and click “Add”. You can import whole voucher carnets in one go if you use the “label” we’ve emailed you instead of individual voucher codes.¹⁵ If you don’t have our confirmation email at hand, just log in to our web site and visit the ACCOUNT section. It is safe to add vouchers or whole carnets on several installations of YF and even with different accounts, but you may use each voucher code only once. Click “update” to automatically check which codes have been used in the meantime, and “clean up” to remove all used codes from the list.

¹⁴Yes, this can be used to protect a more expensive package from expiring.

¹⁵ On Android, if you purchase voucher carnets from the built-in shop they will get added automatically.

To use a particular voucher code, highlight it then click “send sel.”. On Android, if you highlight a category of codes, the first unused voucher code in this category will be sent.

If, for whatever reason, you cannot use voucher codes directly from within the Your Freedom application, you can send them through the web site instead.

Please see the Voucher FAQ on our web site for further details.

5.3 Test drives

If you are considering buying a package but are not sure whether it will be what you expect, how about a test drive? Log in to our web page at <https://www.your-freedom.net/> on “Prices”, and click on the “Try Before You Buy” link on the left. Everyone is welcome to try, but notice that we only allow test drives for accounts that have not just been created and that haven't tested extensively already. Also, we refuse test drives for accounts that have been involved in payment reversals before. However, our support staff can help you out should you need additional testing; just send an email to support@your-freedom.net.

During a test drive you'll receive all the benefits of the selected package, and what's more, you may even switch from one package type to another to test them all. Simply visit the “Try Before You Buy” page again to modify or end your test drive.

As with bought packages, it may take a few minutes for updates to propagate to all servers, and you may have to restart your connection or even the Your Freedom client to see the difference.

With the latest client versions, you can activate “test drives” from the “Account Profile” panel (desktop) or the built-in app shop (Android). You need to be connected to an YF server to initiate tests.

6 Advanced Topics

6.1 Port Forwards

Please note that this chapter only applies to the desktop version of Your Freedom, not the Android app.

6.1.1 Local port forwards

One possibility to allow an application to connect to a service on the Internet via Your Freedom is to “mirror” a port on the Internet. Just imagine there’s a server out there with a certain IP address and it’s listening to SSH connections. You would like to SSH to the server but your SSH client does not support SOCKS. In this case you would simply configure a local port forward similar to this one:



Now instead of connecting via SSH to “some.host.somewhere” on port 22, you simply instruct your SSH client to connect to “localhost” on port 2222. Your Freedom will put the connection through for you. Note however that if the remote host is unreachable the SSH client will still see a working connection, but it will time out quickly.

This is just one of many examples how you can use this feature. Generally speaking, if your application needs to only connect to a particular host on a particular port, local port forwards are the right choice.

6.1.2 SIP forwards

Yes, that’s true! You can use SIP phones with Your Freedom as well! We have seen reports that audio only worked in one direction. Once we can find the time we’ll continue to work on it. Note however that this is still in early beta phase and it may not work properly; in any case, OpenVPN mode will likely work.

If you’d like to give it a try, here is what you need to do. Assume you are using a SIP server called “sip.sipgate.de” on port 5060, the well-known port for SIP. If you configure a SIP port forward likes this one ...



... it will turn your local PC into a mirror image of the SIP server. So instead of configuring “sip.sipgate.de” in your SIP phone, configure “localhost”. Disable STUN if you can, it’s meaningless in this context (but will only make things slower).

SIP forwarding is a complex task; not only does the YF client have to forward all requests, it also has to set up UDP forwards dynamically for all audio and (that’s right!) video streams. We haven’t tested this with many different SIP providers and phones, so it’s likely that many of them don’t work yet. We like to hear from you!



SIP forwarding will only work with UDP, not TCP. Nearly all clients and servers use UDP. Also, note that using a SIP phone consumes a certain amount of bandwidth (depending on the Codecs you are using); the FreeFreedom profile will likely not be fast enough to support SIP forwarding (the voice will break up).

6.1.3 Server port forwards

Would you like to make your PC reachable from the Internet? Then server port forwards are for you. Check out the “Account Profile” panel after connecting; if you see “remote ports forwarded” there you can use this feature. (You can configure it as well if no ports are forwarded to you, but it won’t do a thing.) Forwarded server ports are able to handle both TCP and UDP traffic.

It is important to understand that you can only forward server ports that are assigned to you (i.e. appear in the list of “remote ports forwarded”). So let’s assume you have ports assigned. Add forwards like this:

A screenshot of a Windows-style dialog box titled "Your Freedom - Server Port Forward". The dialog has a blue title bar with standard minimize, maximize, and close buttons. Inside, there are three input fields: "Remote Port" (a small text box), "Local Host" (a larger text box), and "Local Port" (a small text box). At the bottom of the dialog, there are two buttons: "Accept" and "Cancel".

It is not absolutely necessary to use the same numbers for “remote port” and “local port”, but we have found that many applications are too silly to announce another port to “the network” than they actually listen on. For example, BitTorrent clients usually can announce different external IP addresses and ports, but 99 % of all trackers will simply ignore this. So use the same port on both ends (by configuring your application accordingly) and it will all work by sheer magic.

Also, we cannot assign ports that you request, for the simple reason that everyone wants 6881 and such. Please don’t ask, you can only use the ports that have been automatically assigned to your profile.

Typical usages:

- Getting Remote Access to your PC, e.g. rdesktop, VNC, SSH
- Getting High ID in eMule
- Speeding up of BitTorrent downloads.



Currently Server Port Forwards are only included in the TotalFreedom upgrade

6.2 Connection Sharing

6.2.1 Relaying

If your profile supports relaying and you have turned on the "relay for others" option, other people in your local network will be able to configure their browsers and applications to use your computer as a proxy server just the same way as you do. All they have to do is specify your computer IP number and 8080 (or whatever port you have under web proxy) or 1080 (sock proxy) in their applications where a proxy server: port is required.

Typical use is for roommates in a dorm or colleagues in the same office.

6.2.2 Using OpenVPN and ICS to connect other PCs, Playstations, XBox, etc.

If you would like to connect other PCs, PlayStations, VoIP phones, whatever to the Internet through the Your Freedom connection, all you need is a second network interface installed in your PC. Make sure it isn't used for anything else. You need to connect your other PCs/PlayStation/etc. to this network interface, either directly (crossover cable) or via a small switch/hub. Do not use the same switch/hub as for your other Ethernet interface (unless it provides VLANs)! Another thing that you need to ensure is that your other Ethernet interface does not use the 192.168.0.0/24 network -- if it does, reconfigure your DSL/cable router to use a different network.

Open Start -> Control Panel -> Network Connections. Find the unused LAN interface (it's probably called "Local Area Connection 2" but don't rely on it) -- you need the exact name. Then find the TAP32 interface of OpenVPN. Right-click on it and choose "Properties". Click on the "Advanced" tab. Tick the "Allow other network users to connect through this computer's Internet connection" box and choose the network interface in the drop-down menu below that connects to your other PCs or PlayStation. Click "OK" and close the Network Connections window.

That's it; your other PCs/Playstations should now be able to connect to the Internet through Your Freedom's OpenVPN connection when it's up.

6.2.3 Will tethering on Android work with Your Freedom?

The short but unsatisfactory is: no, unfortunately not.

There are several reasons for it. First of all, the Android VPN API does not provide a means to set up address translation on tunnel interfaces. The second reason is that tethering will not provide a default gateway to your PC when a VPN connection is active. We are sure Google considers these shortcomings a security feature.

You can of course install the PC version of Your Freedom on your PC and run this version instead the Android app, while using your phone's connectivity to get connected.

6.3 IPv6

The YF client can use IPv6 to connect to YF servers. IPv6 addresses can be reached through the SOCKS5 and local port forward facility, but not via OpenVPN mode or web proxy. Please note however that not all of our servers support IPv6.

If you are having problems connecting to YF servers (or even find them), it is a good idea to try and enable IPv6 on your PC (if it is not already enabled). Also, enable all kinds of tunneling mechanisms, you never know -- one of them might work where you are. :-)

On Windows Vista and Windows 7, both IPv6 and Teredo tunneling are enabled by default but unless your PC has a global IP address tunnel mechanisms won't work out of the box. To make it work, click on "Start", then type "cmd" but do not hit Enter. Wait until the "cmd.exe" application appears in the search list, then right-click on it, choose "Run as administrator" and confirm the dialog. In the black cmd window, type

```
netsh interface ipv6 show teredo
```

If "status" is "offline" try this command:

```
netsh interface ipv6 set teredo enterpriseclient
```

Wait a bit then check the state again:

```
netsh interface ipv6 show teredo
```

It should tell you that "status" is "qualified" or "dormant". When done type "exit".

With Windows XP SP1/SP2, Teredo is shipped as well but not installed by default. You can easily sort that though by opening a cmd window (click Start, then click Run and type cmd) and typing "netsh interface ipv6 install", then proceed as above (or just type "netsh interface ipv6 set teredo enterpriseclient").

You might want to use a different Teredo gateway than the default; if yes append it to the "set state enterpriseclient" command. If your PC is not behind a NAT router you can use "set state client" instead.

Unless someone filters Teredo this should give your PC full IPv6 connectivity. The YF client will automatically notice and try IPv6.

6.4 Fine tuning CGI mode

Generally, CGI connection mode is the slowest of all possible connection modes. This is due to the way it works; it needs to accumulate data before it sends it off to the other side. But you can adjust a few knobs and try to make it faster.

First, locate the "ems.cfg" config file (see Appendix C). This file can be edited with any text editor, for example Notepad. Ensure the YF client is NOT running when you edit the file or your changes may be lost. It is difficult to break this file so don't hesitate to try...

There are four values that control the timing of CGI connections and you can change any of them. We'd not recommend changing any of these limits except perhaps

"cgi_uplink_maxdelay". Here are the parameters with their default values and their meaning:

- `cgi_uplink_maxdelay`. Defaults to 500 milliseconds. The YF client will accumulate data for at most this time until it initiates a new uplink connection no matter how much data has been accumulated. You might want to set this to a lower value, maybe 200 milliseconds.

- `cgi_uplink_urgentdelay`. Defaults to 20milliseconds. The YF client will use this value instead of the previous value when it has frames to deliver that are considered urgent, for example acknowledgements.
- `cgi_uplink_threshold`. Defaults to 3. If this many frames (YF data units) are to be delivered, a new uplink connection will be made right away. Setting this to 1 will effectively disable data accumulation and make your connection much more responsive, but it will also create much more overhead. If you don't care about how many connections are made and how much overhead it generates, set this to 1 and don't worry about the rest.
- `cgi_uplink_mindelay`. Defaults to 1 millisecond. This is the minimum amount of time between two uplink connections. You should not set it to 0 and most people should not have to increase it, but if your network connection drops connection attempts that appear in bursts, try setting it to a higher value!
- `cgi_downlink_connect_timeout`

All these values normally do not appear in the config file and are not configurable through the front end. Just add lines to the file (it does not matter where) that contain the name of the value, a space, and the numeric value to which you would like to set it (no unit).

Optimum performance is probably achieved by setting `cgi_uplink_threshold` to 1 and `cgi_uplink_mindelay` to maybe 20. Try it, you can't break anything, if it doesn't work just remove the lines again.

Appendices

Appendix A. Troubleshooting

The Your Freedom client comes with built-in troubleshooting facilities. There is the message log that you can access from the Messages tab (you may save it to a file as well) but this will only help you in everyday situations. For more detailed troubleshooting you need to run Your Freedom in “dump” mode, and you might have to use a packet sniffer as well.

Why does my app/game not work?*

There is of course no off-the-shelf answer to this question. But the first thing you should look at is the streams panel of the Your Freedom client. Does the application create streams there when you use it before it complains that it cannot connect? If no, then it is likely not properly configured. See if you’ve got the proxy settings in the application right –if it’s running on the same PC as the Your Freedom client, use “localhost” or “127.0.0.1” as the proxy host address, and 1080 (SOCKS) or 8080 (web/http/https) as the proxy port. If it’s running on another PC, be sure you have relaying enabled (Ports panel) and it’s permitted by your profile† (Account Profile panel), and you’ve used the Your Freedom PC’s local LAN address as the proxy host address.

Then check the message panel in the Your Freedom client – do you see blocked protocol messages there? You need to use another Your Freedom server then, the one you are using right now is not supporting a protocol that you need.

Please have a look at our online documentation if you are having trouble. We know it’s not perfect and the introduction page is an outright shame but have a look anyway, there is more in there than you might think. <https://www.your-freedom.net/4/>

Another plan might be to have a look at the user forums. Maybe someone else had the same problem before? The forums can be found at <https://www.your-freedom.net/2/>.

Performing a speed test‡

A speed test is a very express way to know how much traffic per unit of time your Your Freedom connection can handle. For this you need to generate enough application traffic to saturate the link between the Your Freedom client and the Your Freedom server -- in both directions. So either run an application of which you know that it will use the full bandwidth, or use Your Freedom’s built-in traffic generator. In order to use it, start the client and create a local port forward from some port (e.g. 1234) to a virtual host called “speed test” on port 0. Then open a command shell (in Windows, click on “Start”, choose “Run”, then type “cmd”). In this shell, type “telnet localhost 1234” (or whatever port you’ve used) -- the speed test will then run for one minute, at the highest speed possible. Note that during the speed test, all speed restrictions still apply. You won’t get a higher bandwidth reading than your profile or slider settings permit, but you should see the bandwidth go up to your slider settings - - if you don’t, something else is limiting your speed. It could be (and likely is) the speed of your

* No applicable to Android app

† At the time of writing, relaying is permitted to all users.

‡ Not available on Android

Internet connection. Try adjusting the uplink speed to the actual speed of your Internet connection (e.g. many DSL connections only allow 256Kbit/s or 384 Kbit/s in uplink direction; adjust the slider slightly below this value), this might improve your throughput in the opposite direction. Please note: This traffic generator feature is meant to be used for troubleshooting; please do not use it frequently. The best reason to run a speed test is that we've asked you to!

For best test results, you need to run multiple speed tests in parallel. An individual stream will likely not be able to saturate a fast connection.

Creating a “dump” file

Desktop

Depending on how you start Your Freedom, there are different ways how to start it in dump mode. The Windows installer version can be run in dump mode from the Start menu; if you are running the client from the command line, use the option `--dump[=outputfile]` to activate the dump mode. If it is run using the Start menu or if the "outputfile" is left omitted, the dump file will be produced on your desktop except for Unix like systems, in which case they will be stored in your home directory. Note that there is a drop in performance when you activate this mode, and the dump file may grow pretty big over time.

Normally, the client does not dump any actual packet data; if that's needed we'll provide a modified client on request that does.

Don't hesitate to have a look at the file, some of it probably makes sense to you, some of it will only make sense to the developers. If you mail us a big dump, please compress it! Put it in a ZIP or 7z or whatever archive file, but please avoid any proprietary features (e.g. WinZIP 10's AES encryption mode).

If you are having connection problems, it helps if you run the Wizard in dump mode as well.

Android

Open the configuration menu then click “General Settings”. Tick the “enable dump mode” checkbox, It is recommended that you also tick “compress using GZIP”; it will spare you the additional step of compressing the dump file by compressing it on-the-fly. Do not tick “extensive” unless we have asked you to (or you are really curious). Your dump file will appear on the SD card in a directory called “Your Freedom Dumps”. You'll probably need an app like “ES File Explorer” (highly recommended!) to email it to us, or access it by connecting your phone or tablet to your PC.

Using a packet sniffer[§]

This is bare metal debugging and not for the faint-hearted. There may be situations where our support staff asks you if you can use a packet sniffer to troubleshoot connection or application problems. If you can, we recommend using Wireshark (available from www.wireshark.org or www.ethereal.org – Ethereal is the historical name of Wireshark). In most cases you should run Wireshark on the same PC as the YF client, and you should either capture on the interface that connects the YF client to the YF server or on the interface that connects other PCs to the YF client PC, depending on the nature of your

[§] Hardly applicable to Android I guess ☺

problem. Let the capture run, then re-create the problem, then stop the capture. Save the capture to a file and mail it to us (again, we like it if you compress it).

Updating the client

It is highly recommended that you update your installation from time to time to ensure you've got the latest bug fixes and features.

Updating the YF client installation is very easy on Windows and on Android: just use the built-in update functionality and follow the individual steps. If, for whatever reason, you need to update manually, follow this simple procedure (Windows -- on other systems the procedure is similar -- download, uninstall, install):

1. Check on <https://www.your-freedom.net/index.php?id=downloads> for new versions, compare the version number to the one displayed on the "About" screen of the YF client.
2. If there is a newer version available, consider downloading it. We suggest you always keep the downloaded files of previous installations until you are sure that the new version is working properly for you so you can revert to it. Previous versions are also available from our web site in case you need to roll back.
3. Once you've downloaded the new version, disconnect, then exit the YF client.
4. Uninstall the current version through Start - Programs - Your Freedom - Uninstall or through the control panel of Windows. While it is safe to install new versions over previous versions if you ensure that you always use the same installer type, we do not recommend it. Your settings will not be lost by uninstalling the YF client.
5. Install the new version by running the downloaded file and following the steps on the screen.

If you find that the new version fails to do something properly that the previous version did, please let us know (include both version numbers if possible, and tell us which installer you are using, NSI -- the small one -- or JET -- the large one). Tell us too if it fixes a previous problem. (No need to tell us you are now able to get connected again when you weren't able previously -- we'll notice it statistically. :-)

The release versions of the client are generated as follows:

YYYYMMDD-Serial

YYYY = Year

MM = Month

DD = Day

Serial = Counting up on that Day.

Example: 20040507-02, 2nd Version on the 7th of May 2004.

Version 3.0

Release Date: 2013-06-26

On Android, updates are automatically provided through Google Play (and we recommend that you enable automatic updating in Google Play). If you prefer to use our own built-in updating functionality, find it in the settings menu.

Appendix B. Country information

Country specific plans

Your Freedom has special plans created for those connecting from certain countries in which access to the Internet is highly restricted. We omit the list of those countries here. More information can be found on our website.

In those countries, the FreeFreedom account type behaves different. Depending on the country you're connecting from, the FreeFreedom can exhibit variations in the usage limits. As a general rule usage limits are eased allowing for an uninterrupted connection time. Also the usual 64kbps bandwidth can go up to 512kbps in some cases. They become active once the user connects from the affected country. The usual outcome is the users can stay connected for as long as they want without limitation from our side.

Please note that it is sometimes technically impossible to determine whether or not a connection is coming from a country that is on our list, particularly if you use DNS connection mode.

Server availability by country

Some of our servers may not be available to users from all places at all times. We may set up such limitations to prevent servers that are strategically positioned to those in need from being overloaded by those who should really use other servers.

Another reason might be self-defense, like protecting a server from being abused by spammers. Most of the SPAM we have to fight comes from only a handful of countries; we might at times be required by our providers to close the floodgates.

There are servers for everyone nevertheless and connection is always possible to them, no matter what country you are in. Just try the servers on the list.



A few servers may deny connection from certain countries as a measure of protection against abuse. When a user gets denied its connection attempt because of a policy applied to the country they are trying to connect from, the YF client will produce an error saying "AUTHENTICATION NOT VALID FOR YOUR COUNTRY OF RESIDENCE". Trying a different server is recommended.

Tweaks

"Tweaks" are basically set of rules and hard-coded behavior in the YF client to make connections possible in some specific network conditions. Most people don't need these and can safely leave them disabled; so if you are able to connect, do not enable tweaks.

Their names are very explicit. They have been added after we have learned how to make the YF client connect in certain conditions (normally very well represented in certain countries) when normal techniques don't seem to work. If you've got a clever way to configure the YF client to connect to its servers in some unusual networking situation, please tell us about it.

Appendix C. The Your Freedom client configuration file**

The configuration file is stored in your "home directory" and it's called "ems.cfg" on Windows and OSX and ".ems.cfg" on Unix platforms (yes, two dots).

If you want to copy the file or edit it, be sure that the Your Freedom client is not running! The file is plaintext and you may edit it with your favorite text editor (for example, pico or vi on Unix systems, or notepad in Windows).

Where's my home directory?

With Unix like systems you probably know because you are there all the time. In most cases there is a directory called "/home" containing a subdirectory for each user, by his or her username -- you should find your "home directory" there. The config file "ems.cfg" or ".ems.cfg" is in there, you just might not see it because it's a "hidden" file in Unix terminology, starting with a dot. Try to append "-a" to the "ls" command.

With Windows Vista and Windows 7, open an Explorer and go to "C:\Users". In there, there is a directory for each user; the directory name is usually equivalent to your login name. This directory is your "home directory", or "%HOMEPATH%" in Windows environment terms. In there you should find a directory called "AppData" (if you don't, disable hiding of system files as explained on <http://www.techrepublic.com/blog/window-on-windows/quick-tip-reveal-hidden-system-files-in-windows-explorer/2467>), then "Local", then "Your Freedom", and the config file "ems.cfg" is in there.

In older versions of Windows the home path is located in "C:\Documents and Settings" (or equivalent in your language); again, there's a directory for each user's home directory.

A rule of thumb to find your home directory would be executing "cmd" from the "Run" window.



You'll find yourself in front of a black terminal with a blinking cursor. The text at the left is the path for your home directory.

```
C:\Users\myusername>_
```

** There is no "config file" on Android.

Configuration options

Note! Some of the options below are marked as “hidden”, which means that they are not accessible through the “Configuration” window but only through a text editor. These options are for those who know exactly what they are doing (or at least think they do). Please consult our support staff first if you are unsure.

All options are case sensitive, be sure to use lowercase! There are options that can only appear once in the config file (type: single), others can appear more than once (type: multi). Options that take only a single value will treat everything after the leading whitespace as part of the value, including whitespace, so watch out and don't put whitespace at the end of the line if you don't want to. You may use comments as well (they start with a # in the first column) but they will be gone next time the client saves the config.

Now here comes the alphabetical list... enjoy!

Option	Description	Type	Arguments
aes	Enable or disable strong (AES) encryption	boolean optional	“true” (default) or “false”
autoscroll_messages	Scroll message window automatically when new messages appear	boolean optional	“true” or “false”(default)
avoid_dns	Use the server's IP address, not the host name (if known)	boolean optional	“true” or “false”(default)
bandwidth_unit	Display unit for bandwidths	integer optional	"bit/s" (default) or "Bytes/s" (EXACTLY!)
barf	Crash reports	multiple base64 fyi	Contains base64 encoded crash reports not yet sent to us. These reports do not contain any personal data.
bw_downlink	Desired downlink (server to client) bandwidth in bits per second (slider setting)	integer optional	Bits per second. 0 means “unlimited”.
bw_uplink	Desired uplink (client to server) bandwidth in bits per second (slider setting)	integer optional	Bits per second. 0 means “unlimited”.
cgi_downlink_connect_timeout	Downlink connection timeout in CGI mode, in milliseconds	integer hidden	Defaults to connect_timeout

cgi_downlink_reconnect_delay	Downlink reconnection delay in CGI mode, in milliseconds	integer hidden	Default 500 ms
cgi_uplink_maxdelay	Maximum delay before queued frames trigger a connection	integer hidden	After this time, the queue is flushed no matter how much data is to be sent (if any). Default to 500ms
cgi_uplink_mindelay	Minimum delay before a new connection is triggered	integer hidden	The minimum delay between two queue flushes (POSTs). Default to 1ms.
cgi_uplink_threshold	Number of queued frames that cause mindelay to be used instead of maydelay	single hidden	0 to disable, or any (low) number. Defaults to 3 ⁺⁺
cgi_uplink_urgentdelay	Maximum delay for urgent data.	integer hidden	The maximum delay if urgent data is in the queue (e.g. small frame belonging to a stream that has not sent data for a while - - - interactivity! --). Defaults to 20ms.
connect_on_startup	Fire up connection when client is started	boolean optional	“true” or “false”(default)
connect_timeout	General connection timeout, in milliseconds	integer hidden	Defaults to 10000 ms.
debuglevel	Turn on debugging on the Java console (not the message panel!)	integer hidden	The lower, the more verbose. Default is “999”. It probably doesn’t do much anymore these days.
dns_domain	Domain to use in DNS mode	string optional	You should not manually configure this option, use the config panel instead.

dns_max_tx_interval	Maximum delay between sending two queries in DNS mode, in milliseconds	integer optional	Default 1000 ms.
dns_min_tx_interval	Minimum delay between sending two queries in DNS mode, in milliseconds	integer optional	Default: 1/500 of dns_max_tx_interval.
dns_no_direct_connection	Avoid directly sending queries to the YF server in DNS mode, force the use of a configured nameserver	boolean optional	“true” or “false” (default)
dns_rep_interval	Repeat unreplied queries in DNS mode after this many milliseconds	integer optional	5 times dns_max_tx_interval
dns_tx_adaption_factor	Adaption speed in DNS mode	float optional	Between 1.1 and 5.0, default 1.5. Higher values are more aggressive.
dont_show_popups	Avoid popping up notification windows on the screen	boolean optional	“true” or “false” (default).
echo_max_tx_interval	Maximum interval between two ICMP ECHO requests in ECHO mode	integer optional	Default 1000 ms
echo_min_tx_interval	Minimum interval between two ICMP ECHO requests in ECHO mode	integer optional	Default 1/200 of echo_max_tx_interval
echo_tx_adaption_factor	Adaption speed in ECHO mode	float optional	Between 1.1 and 5.0, default 1.5. Higher values are more aggressive
echo_max_payload_size	Maximum payload size in ECHO mode	integer optional	Default 1464 (the maximum value)
encryption	Turn on connection encryption	boolean optional	“true” or “false” (default). Note that the wizard turns this on for you. You should only turn encryption off for debugging!

file_extip	Write server's external IP to a file when connecting	string optional	This allows you to use the server's external IP in scripts
flatten_bursts	Slow down frame transmission in bursty periods to obtain a smoother traffic pattern	boolean optional	"true" or "false" (default). Set if you notice connection hangs on bursts.
follow_server_recommendations	Allow the client to follow the server's recommendations to use another server	boolean optional	"true" or "false" (default). DEPRECATED.
fool_pix	Try a hack that can fool old PixOS versions into bypassing WebSense	boolean hidden	"true" or "false" (default). Only turn on if you know that your connection is passing through an old PIX firewall using WebSense and you cannot connect; it may work with this set to "true".
found_servers	Base64 encoded records of servers found in last server search	multiple base64 optional	Don't mess with it unless you know what you are doing.
ftp_mode	Data connection set-up style to use in FTP mode.	string optional	"both" (default), "normal" or "passive". "normal" will cause the YF server to initiate the data connection (this is what FTP normally does), "both" will use whatever works
ftpproxy	Use a non-transparent FTP proxy with the FTP connection protocol	string optional	Put in the FTP proxy's host name or IP address. Remove if you don't need one (very likely).
ftpproxyport	Use a non-transparent FTP proxy with the FTP connection protocol	integer optional	Put in the FTP proxy's control port (normally 21). Remove if you don't need an FTP proxy (very likely)..

header	Additional headers when sending requests to the web proxy	multiple string optional	If you need additional headers or wish to override things like "User-Agent", do it here. For example: "headers User-Agent: NoneOfYourBusiness 1.0"
hide_tray_icon	On Windows, do not display a tray icon	boolean optional	"true" or "false" (default)
http_flush	Close and re-open the HTTP uplink connection at intervals	integer optional	Time in milliseconds. If you need this, use the CGI connection protocol instead. This is outdated.
http_postfix	In HTTP mode, append this after a ? to the URL	string hidden	Can be used to craft special URLs
https_ssl	Wrap connection in "HTTPS mode" in SSL (TLS).	boolean optional	Helps with picky filters that perform protocol detection
idle_kill	Kill connection when idle for this many milliseconds	integer optional	This is obsolete and doesn't work as expected anymore, don't use it.
initial_post_size	When doing a HTTP POST, use this initial size	integer hidden	Default is 10000000 or 10 Megabytes. The client decreases this by a factor 0.8 until the web proxy accepts it or the value falls below minimum_post_size. If you know your proxy's limits put it in here, it saves connection time.
keepalive_interval	Send a keepalive frame every this many milliseconds	integer optional	Default is 20000 ms. Connection fault detection is 2.5 times.
level_messages	Only show messages above this level in Messages panel	integer optional	0 is "debug", 7 is "emergency". Default is 1 "informational".

locale	Your preferred "locale" language (ISO 2 letters, lowercase, optionally followed by an underscore and an ISO 2 letters country code in uppercase)	string optional	Defaults to "en". Only a few languages are supported, see the Configuration dialog.
location_x	Coordinates of the Your Freedom window on the screen	integer optional	0 is top left corner, higher values are further right
location_y	Coordinates of the Your Freedom window on the screen	integer optional	0 is top left corner, higher values are further down
minimum_post_size	Minimum HTTP POST size	integer hidden	Default is 20000 or 20Kilobytes. Only lower if you know that your proxy will refuse POSTs above 20k and you really have to.
min_buffersize	Minimum buffer size for streams.	integer optional	Defaults to 1500. Try to increase this if you want to achieve individual stream bandwidths of more than several megabits per second. Maximum is 8192.
openvpn	OpenVPN port	integer optional	Default is 1194, only change if you need this port for something else.
openvpn_exclude	IPs and networks to be excluded from routing through the OpenVPN tunnel	multiple string optional	For every IP or network (IP address, an optional space and net mask) that should not be routed through the OpenVPN tunnel, add a line to the config.

openvpn_nat_interface	List of interfaces that you want to re-route to the OpenVPN connection using Network Address Translation	multiple string optional	Useful only on Windows. Lets you connect your Play Station or XBox or other PCs to a second LAN interface and use the YF OpenVPN connection.
openvpn_option	Additional OpenVPN options	multiple string hidden	Pass these additional options as if they were lines in the OpenVPN config file.
openvpn_path	Configure full path of OpenVPN executable	string optional	Use this if the OpenVPN executable is not in your executable path
openvpn_tap_sleep	Set "tap-sleep" option in OpenVPN to this value	integer optional	Default is 2 seconds. Relevant only on Windows.
openvpn_route_delay	Set "route-delay" option in OpenVPN to this value	integer hidden	Default is 2 seconds (second parameter is always 30). Relevant only on Windows.
openvpn_route_method	Configure OpenVPN route method	string hidden	Default is "exe". See OpenVPN documentation for more options. Relevant only on Windows.
openvpn_ip_method	Configure OpenVPN "ip-win32" method	string hidden	Default is "dynamic". See OpenVPN documentation for more options. Relevant only on Windows.
openvpn_tmp	Temporary directory to be used for OpenVPN config files and certificates	string hidden	Default is your "home folder", or a sub-directory below it. Configure an absolute path here.

openvpn_udp	Make OpenVPN tunnel through UDP forwarding instead of TCP forwarding in YF	boolean optional	Use UDP instead of TCP forwarding for the OpenVPN tunnel connection if "true".
password	Your Your Freedom password	string required	your Your Freedom password, or an obfuscated form of it
portaccept	Forwards a server port to a local port	multiple string optional	server port local host local port
portforward	Forwards a local port to a remote port	multiple string optional	local port remote host remote port
post_avg_uplink_dur	POST mode average uplink duration, in milliseconds	integer optional	In POST mode, how long should an uplink transfer take on average (in milliseconds)? Influences the maximum POST length. Default is 500 ms.
post_err_holdoff	POST mode error holdoff time, in milliseconds	integer optional	In POST mode, wait this many milliseconds in an error condition before trying again.
post_max_connections	Maximum number of concurrent connections in POST mode.	integer optional	Some people might have to lower this to one. It is safe to use bigger numbers but at some point it will only increase overhead. Default (2) is good for most people.
post_min_holdoff	Time to wait before new connection is made. (milliseconds)	integer optional	Defaults to 5000.
post_min_post_size	Minimum size of a POST request.	integer optional	Never lower the maximum POST size below this limit. It could starve the uplink path. (Default: 3000)

post_min_queue	Mimumum queue size for fast transmission in POST mode.	integer optional	Number of queued frames that trigger a new connection after only minimum holdoff time (default: 3)
post_typ_holdoff	Typical holdoff time in POST mode, in milliseconds	integer optional	Wait this long for more frames before triggering a connection (default: 500 ms)
protocol	The connection protocol to use	string required	One of: "http", "https", "cgi", "post", "ftp", "udp", "dns", "echo".
proxy	The proxy port	integer optional	Make your PC a web proxy by supplying the port number. Set to 0 or remove to turn off. Default is 8080.
proxyauth	Force a particular authentication method on web proxy.	string optional	One of "any ore none" (default), "basic or none", "NTLM or none", "Digest or none". Default is to use whatever is offered by the proxy and prefer more secure methods over less secure methods.
proxypass	Your password to authenticate on the web proxy	string optional	A password, if authentication is needed.
proxydomain	Your domain for web proxy authentication, if needed (NTLM proxies only)	string optional	A Windows domain name, if you need one to authenticate on your web proxy.
proxyhost	The web proxy hostname or IP through which to tunnel when using "http", "https" or "cgi"	string optional	A host name or IP address. Leave empty or remove if you don't need to use a proxy.

proxyport	The web proxy's port.	integer optional	A port number. Set to 0 or remove if you don't need to use a web proxy.
proxytype	Use non-standard proxy type for TCP based connection modes (HTTPS, HTTP, POST, CGI)	string optional	When using TCP based connection modes and a "web proxy" is configured, assume it is of this type. Can be "HTTP/HTTPS" (default), "SOCKSv4" or "SOCKSv5".
proxyuser	Your username to authenticate on the web proxy	string optional	A username, if authentication is needed.
rcport	"remote control" port	integer hidden	Use a particular TCP port for singularization (i.e. ensuring that YF is running only once). Default is 62799, bound to 127.253.19.87.
reconnect_after_shut down	If server shuts down, try to reconnect automatically after a while	boolean optional	"true" (default) or "false"
reconnect_delay	If a reconnect is required, wait this many milliseconds before an attempt	integer optional	Default is 5000 milliseconds.
redirect_dns	Don't resolve host names locally when using SOCKS	boolean optional	"true" or "false" (default). Use this if your local name server cannot resolve Internet names (or you don't <i>want</i> it to)

rekey	Change encryption key frequently	boolean optional	“true” or “false” (default). The wizard will set this to “true”, and there’s normally no reason why you would want to set it to “false” unless you suspect that there’s a bug in our key negotiation code and you lose connection. We highly recommend that you set this value to “true”.
relay	Allow others to share your YF session	boolean optional	Set to “true” or “false” (or remove). Note that this only works if your profile permits it as well.
rtt_interval	Measure round trip time every this many milliseconds	integer optional	0 to turn off (i.e. only measure once after 10 seconds)
server_connection_protocol	Set tunnel protocol preference (influences DNS name resolution only)	integer optional	0: whatever works 4: IPv4 only 6: IPv6 only 46: prefer IPv4 64: prefer IPv6
server_criterion	Define criteria by which to automatically select servers	multiple string optional	name of criterion number between 0 (refused) and 10 (required), default is 5 (don’t care)
sipforward	Mirror a remote SIP gateway	multiple string optional	local port SIP gateway addr SIP gateway port
sip_fixup_audiostream	Fix destination IP address in UDP stream for SIP audio	boolean optional	Try this if SIP audiostreams are unidirectional only

socks	The SOCKS port	integer optional	Make your PC a SOCKS proxy by supplying the port number. Remove or set to 0 to turn SOCKS off.
sslproto	If https_ssl is configured, define SSL/TLS protocol version to use	string optional	“any” (default), “SSLv2” or “TLSv1”
start_minimized	Start in system tray (Windows only)	single optional	“true” or “false” (the default)
stopafter_found	When searching for servers, stop search after this many servers have been found.	integer optional	0 to try until no more potential ways are known
stopafter_tried	When searching for servers, stop after this many attempts have been made.	integer optional	0 to try until no more potential ways are known
tunnelhost	The Your Freedom server to use	string required	A host name, an IP address, multiple IP addresses separated by semicolon, or a CGI relay URL. In DNS mode, DNS servers (separated by comma) can be appended with semicolon to a host name (not an IP). In HTTP/POST mode, can contain a host name and an URI.
tunnelport	The Your Freedom server port	integer required	A port number
tweaks	Use this “tweak set”	string optional	Name of tweak setting (use config window, don’t set manually), or remove for none
udp_newsrtcportevery	Use a new UDP source port (UDP/DNS mode) every this many packets	integer optional	Value may be as low as 1 but this will impact performance. Use with care. Default is 0 (no change)

udp_newsrcporttime	Use a new UDP source port (UDP/DNS mode) every this many milliseconds	integer optional	Port changes if this many milliseconds have passed since the last change. Default is 0 (don't change based on time)
udp_srcport	Use a particular UDP source port (UDP/DNS mode)	integer optional	0 or remove to use an ephemeral port
use_http11	Use HTTP/1.1 instead of HTTP/1.0 in requests	boolean optional	If your proxy is acting stupid, try if this fixes the problem. Can either be "true" or "false" (default)
useragent	Send this "user agent" header in requests	string optional	Used to fake a particular browser.
	Your YF username	stringrequired	Your Your Freedom username
vm_code	Voucher code information	multiple string optional	Information about known voucher codes
vpn	Use new-style VPN mode	boolean hidden	Experimental, not yet effective
webproxy	Port for new-style web proxy implementation	integer hidden	Experimental: use new-style web proxy implementation for your applications