Table of Contents

Introduction 1.1

Your Devices 1.2

- Android 1.2.1
- iPhone / iPad 1.2.2
- Windows 1.2.3
- MAC/OSX 1.2.4
- Linux 1.2.5

Email 1.3

- RiseUp Email 1.3.1
- Configuring Thunderbird 1.3.2

Remote Access (VPN) 1.4

MemoryHole 1.5

Browsing Securely 1.6

Password Management 1.7

Freshet Collective Tech Manual

This book contains everything you need to get started on accessing services and troubleshooting technical issues with Freshet services

Device Security

Whether a mobile device or a PC/Mac, all your devices will need some configuration changes in order to keep you and your clients safe.

Here we provide instructions for all major device operating systems and desktop operating systems.

- Android
- iPhone / iPad
- Windows
- MAC/OSX
- Linux

Android Device Security

iPhone/iPad - iOS Device Security

Windows Device Security

Mac/OSX Device Security

Linux Device Security

Email

Configuring Thunderbird

Using Remote Access (VPN)

When working or volunteering for freshet, you will need to use the VPN to access services like memoryhole, tresorit, etc.

> ***Note:*** Currently, protected services are available without the VPN temporarily until everyone who will need them is familiar with and using the VPN

Setup

These instructions will help you to get your PC, Mac, and/or smart phone set up to encrypt all of your traffic when you are working for the collective.

You should only need to follow them once for each device. Following that, you can refer to Daily Use to learn what steps, if any, you need to follow to continue using it.

Step 1) Install VPN apps on your devices

	Client Name	**Download Link**
Windows	OpenVPN?	
Linux	OpenVPN?	
Max/OSX	TunnelBlick	
Android	OpenVPN?	
iOS (iPhone, iPad)	TunnelBlick?	

Step 2) Connect to the VPN

Using your credentials you received via email, now you can configure your client to connect to the network.

Step 3) Confirm the VPN is working

Visit this site in a browser: <User Friendly DNS Leak Test>

Daily Use

Connecting/Disconnecting from the VPN

FAQ

Why a VPN?

The primary reasons we are using a VPN for all offsite collaborators are:

- to encrypt your internet traffic
- to obscure the source of your internet traffic
- to ensure that _protected services _are only exposed to trusted users

Why protect services?

1. **Visibility -** Currently, anyone can visit freshetdata.org. This means that potential attackers don't need credentials to begin looking for ways to gain access to the server using a variety of methods. We try our best to prevent these attacks, but ensuring that only a short list of users can even see freshetdata.org gives us many advantages in protecting our data.
2. **Encrypted Traffic -** It ensures another layer of encryption in addition to SSL. Though SSL is the best in-transit encryption method available for the web, a diversity of encryption tactics is always key, especially since barely a year goes by before a major SSL vulnerability is discovered.

When should I be using the VPN?

Any time you are doing work/volunteering for the collective are not connected to the local WiFi network at the apartments/office.

Troubleshooting

1) I can't access the protected services

If you see a 404 error when trying to access memoryhole, or Tresorit is refusing connections:

- Make sure you are connected to the VPN
- If not, connect and try again

2) I'm not sure if I'm connected to the VPN

3) The internet is slow when i'm connected to the VPN

Unfortuantely, this will always be somewhat of an issue

Using Memoryhole