DNS Privacy…
there must be an app for that?

dnsprivacy.org @DNSPrivacyproj

Sara Dickinson sara@sinodun.com

Overview

- Review of client side of DNS Privacy (DoT and DoH)
- What is next client side…
- Stubby GUI overview

Client vs server

- Server side now has many implementations/solutions
- Several large resolvers, increasing number of ISPs (EDDI), many other services…

- Client side picture more varied:
  - Browsers (and other applications…)
  - Desktop systems
  - Mobile
  - Other (Libraries/forwarders/routers)

Client vs server

- Server side now has many implementations/solutions
- Several large resolvers, increasing number of ISPs (EDDI), many other services…

Not covered in this talk

- Client side picture more varied:
  - Browsers (and other applications…)
  - Desktop systems
  - Mobile
  - Other (Libraries/forwarders/routers)

Client vs server

- Server side now has many implementations/solutions
- Several large resolvers, increasing number of ISPs (EDDI), many other services…

Not covered in this talk

- Client side picture more varied:
  - Browsers (and other applications…)
  - Desktop systems
  - Mobile
  - Other (Libraries/forwarders/routers)

Simplified, non-exhaustive review provided here

Desktop Browsers

	DoH	DoT	Notes	Configured Resolvers	Fallback?	Detects managed env?
Firefox (2018)	✓	✗	• Turned on by default in US to a TRR • Otherwise user config	• Cloudflare • NextDNS • Comcast	Configurable	✓
Chrome (2020)	✓	✗	• Same-provider DoH upgrade (fixed list) • Or user config available	Currently 8	Depends	✓
Edge[1]	(✓)	✗	• In Edge Dev (diff list)	• Cloudflare • Google • Quad9	Depends	✓
Brave[1]	(✓)	✗	• WIP - not exposed in config but can use chrome://flags			

1. Based on Chromium code base

Desktop Browsers

	DoH	DoT	Notes	Configured Resolvers	Fallback?	Detects managed env?
Firefox (2018)	✓	✗	• Turned on by default in US to a TRR • Otherwise user config	• Cloudflare • NextDNS • Comcast	Configurable	✓
Chrome (2020)	✓	✗	• Same-provider DoH upgrade (fixed list) • Or user config available	Currently 8	Depends	✓
Edge[1]	(✓)	✗	• In Edge Dev (diff list)	• Cloudflare • Google • Quad9	Depends	✓
Brave[1]	(✓)	✗	• WIP - not exposed in config but can use chrome://flags			

1. Based on Chromium code base

Standard feature, but defaults differ!

Desktop Systems

	System config option	Native API	GUI Apps
Windows (2020)	DoH[1]	✗	• Cloudflare 1.1.1.1[2] (Beta release - Sept 2020) • (Simple DNSCrypt)
macOS (2020)	✗	DoH + DoT[3]	• Cloudflare 1.1.1.1[2] (Beta release - Sept 2020) • NextDNS • (Stubby prototype)
Linux (systemd-resolvd) (2018)	DoT	✗	• ?

1. Windows Preview only, same policy as Chrome
2. Can only use 1.1.1.1, no user config of resolver
3. Detailed video - Note makes easy for an app to offer system wide DoH/DoT

Mobile OS

	System config option	Native API	Apps
Android (2018)	DoT[1]	✗	• Chrome supports DoH • Quad 9 Connect • Cloudflare 1.1.1.1 • BraveDNS • NextDNS
iOS (2020)	✗	DoT + DoH	• Cloudflare 1.1.1.1 • NextDNS • DNS Cloak

1. Opportunistic DoT by default

Other…

	DoH	DoT	Notes
dnsmasq	✗	✗	
Stubby (getdns)	✗	✓	DoH is WIP
Unbound	✗	✓	DoH is WIP
OpenWRT	(✓)	(✓)	• DoH with Dnsmasq and https-dns-proxy • DoT with Dnsmasq and Stubby • DoT with Unbound • DNSCrypt with Dnsmasq and dnscrypt-proxy
Asuswrt-Merlin	✗	✓	• Uses Stubby
Pi-Hole	(✓)	(✗)	• Officially document how to use DoH via cloudflared binary • (Unofficial documentation for using DoT with Unbound)

But…how to discover resolvers?

- Biggest challenge now for client side is resolver choice and discovery…
- ADD WG and predecessors have been churning for ~1 yr
  - Use cases are still unclear
    - Home/open wifi/mobile
    - Auto-upgrade/user interaction
    - Authentication mechanisms (DHCP/PKIX/…)?
- Solutions are some way off

Absolutely a work in progress!

But…how to discover resolvers?

- Biggest challenge now for client side is resolver choice and discovery…
- ADD WG and predecessors have been churning for ~1 yr
  - Use cases are still unclear
    - Home/open wifi/mobile
    - Auto-upgrade/user interaction
    - Authentication mechanisms (DHCP/PKIX/…)?
- Solutions are some way off

Absolutely a work in progress!

Not covered in this talk

Windows GUI for Stubby

Stubby

- A privacy enabling stub resolver, daemon listening on localhost, effectively a **smart DoT proxy** (DoH support is coming)
  - Has stub **DNSSEC validation** capabilities (based on ***getdns***)
- Originally a cross-platform command line tool for expert users
- **macOS**: GUI prototype in 2018 (very basic)
- **Windows** is largest user base (not so much in this audience!)
- Windows GUI project pre-dates Windows DoH support
  (there were no other DoT or DoH GUI options on Windows)
- Still questions around good GUI design for DNS: **'Usable Security',** particularly in the absence of discovery mechanisms

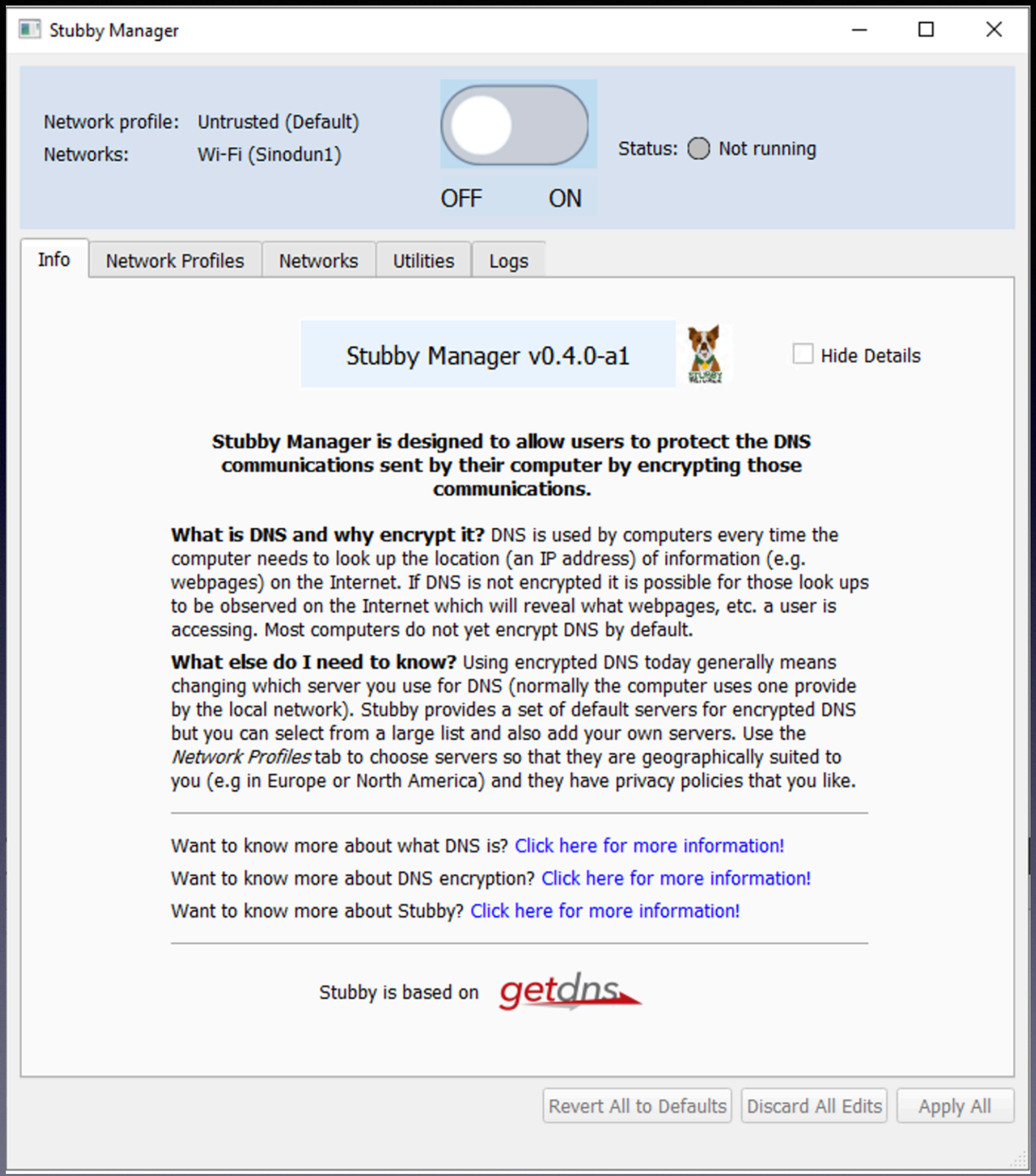
Stubby GUI

- Funded by **Comcast Innovation Fund** to dnsprivacy.org (Thank you!) (Sinodun, NLnet Labs, etc. involved)

1. v0.3.0 (getdns 1.6.0) moved to ***cmake*** -> 1st class support for Windows
2. getdns added to **vcpkg** (widely used Windows package mgr)
    - In absence of Windows API makes application dev easy
3. Next release (v0.4.0) Stubby will be a **fully fledged Windows service**
4. **Development of GUI** to research how to provide usable security for DNS
    - Windows GUI built natively with Qt, manages stubby as a native service
    - Target both non-technical and somewhat technical users…..

GUI is designed to be native Windows looking so not the purdiest thing…

Welcome page

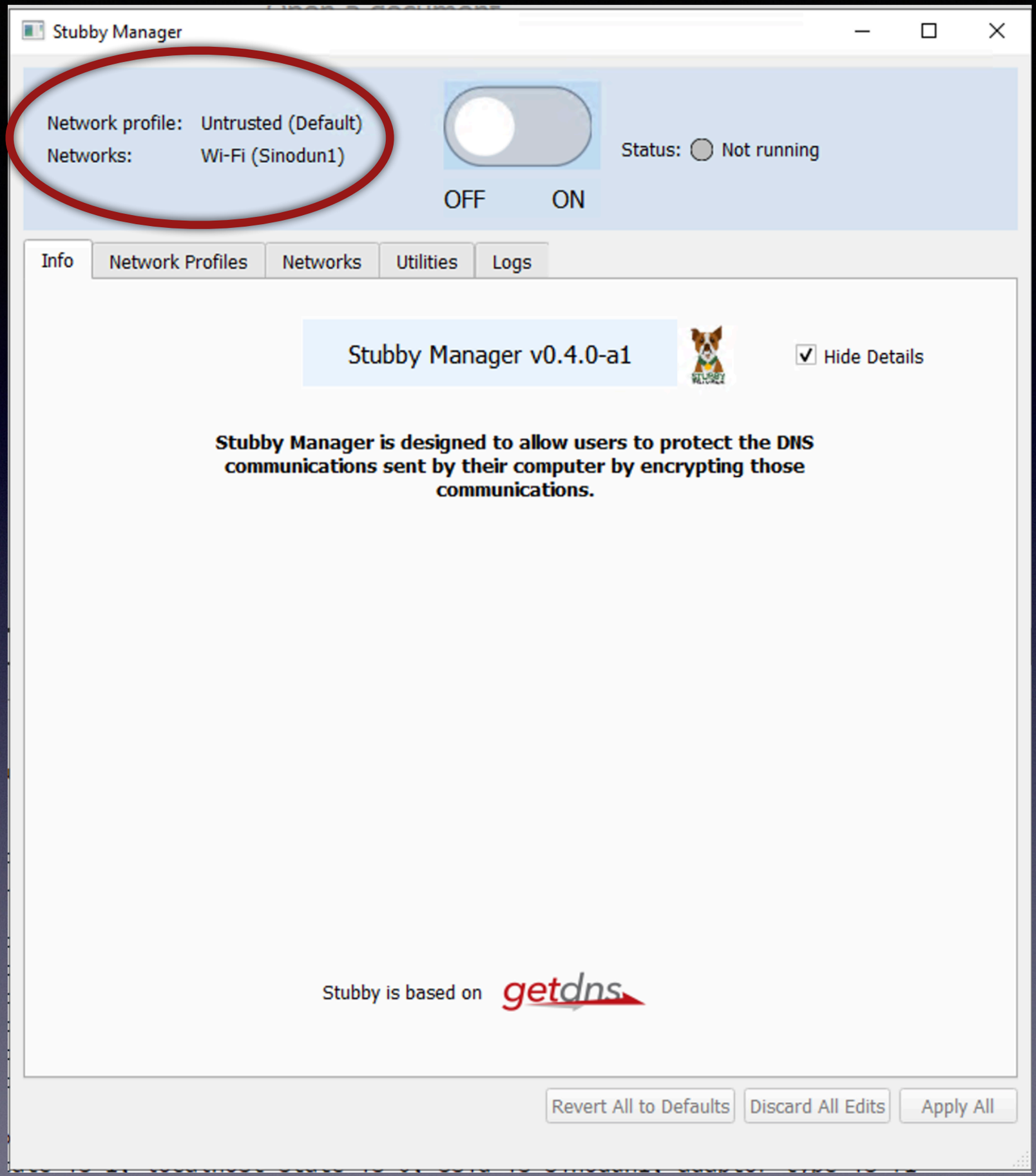


- **Provide background** with links to more detailed info
- **Single on/off button** (like a VPN)
- Show network and profile
- First run has dialog for ‘Just turn stubby on to encrypt your DNS’ and then warns which resolvers are used by default

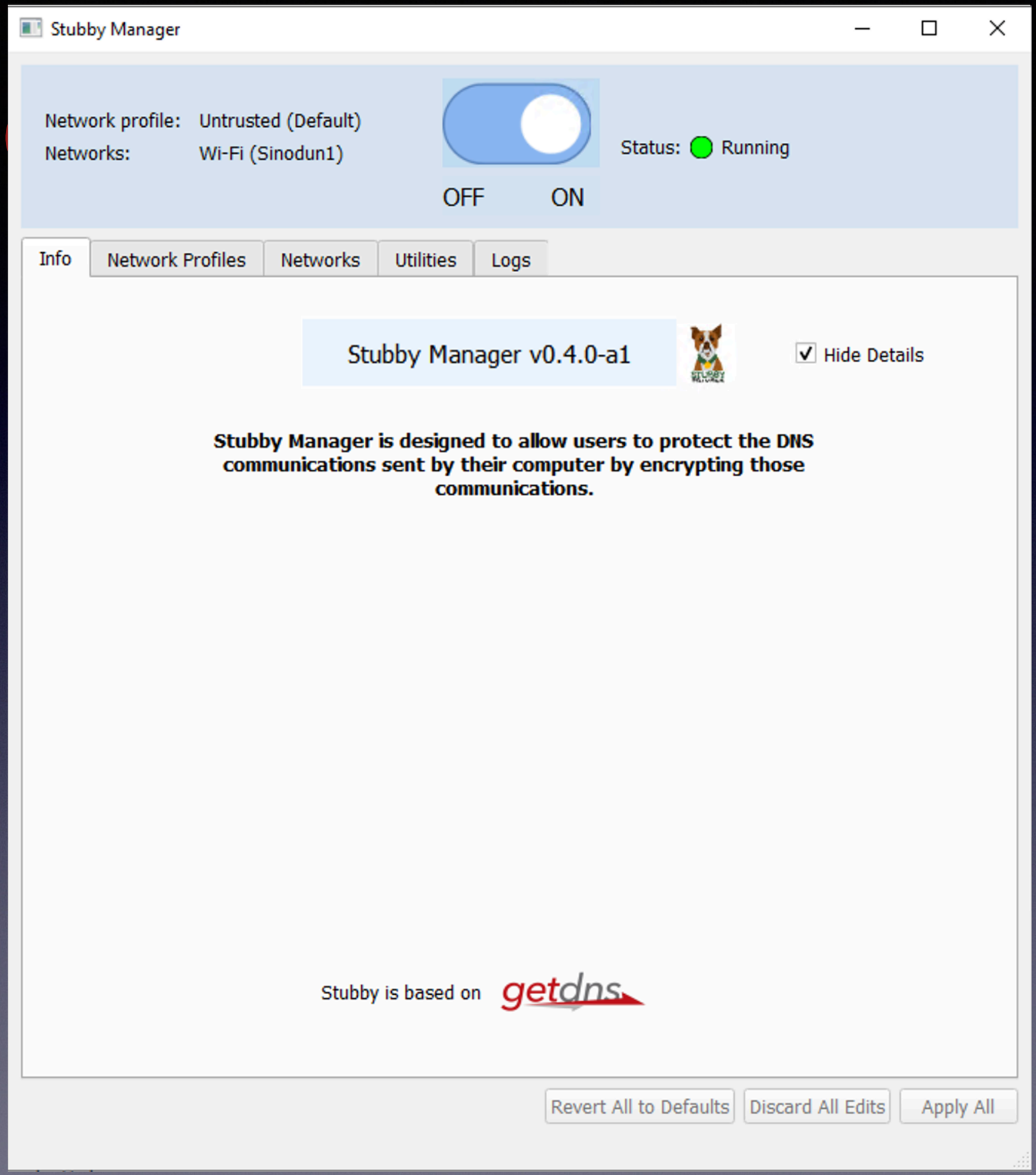
Welcome page

- **Provide background** with links to more detailed info
- **Single on/off button** (like a VPN)
- Show network and profile
- First run has dialog for ‘Just turn stubby on to encrypt your DNS’ and then warns which resolvers are used by default

Welcome page



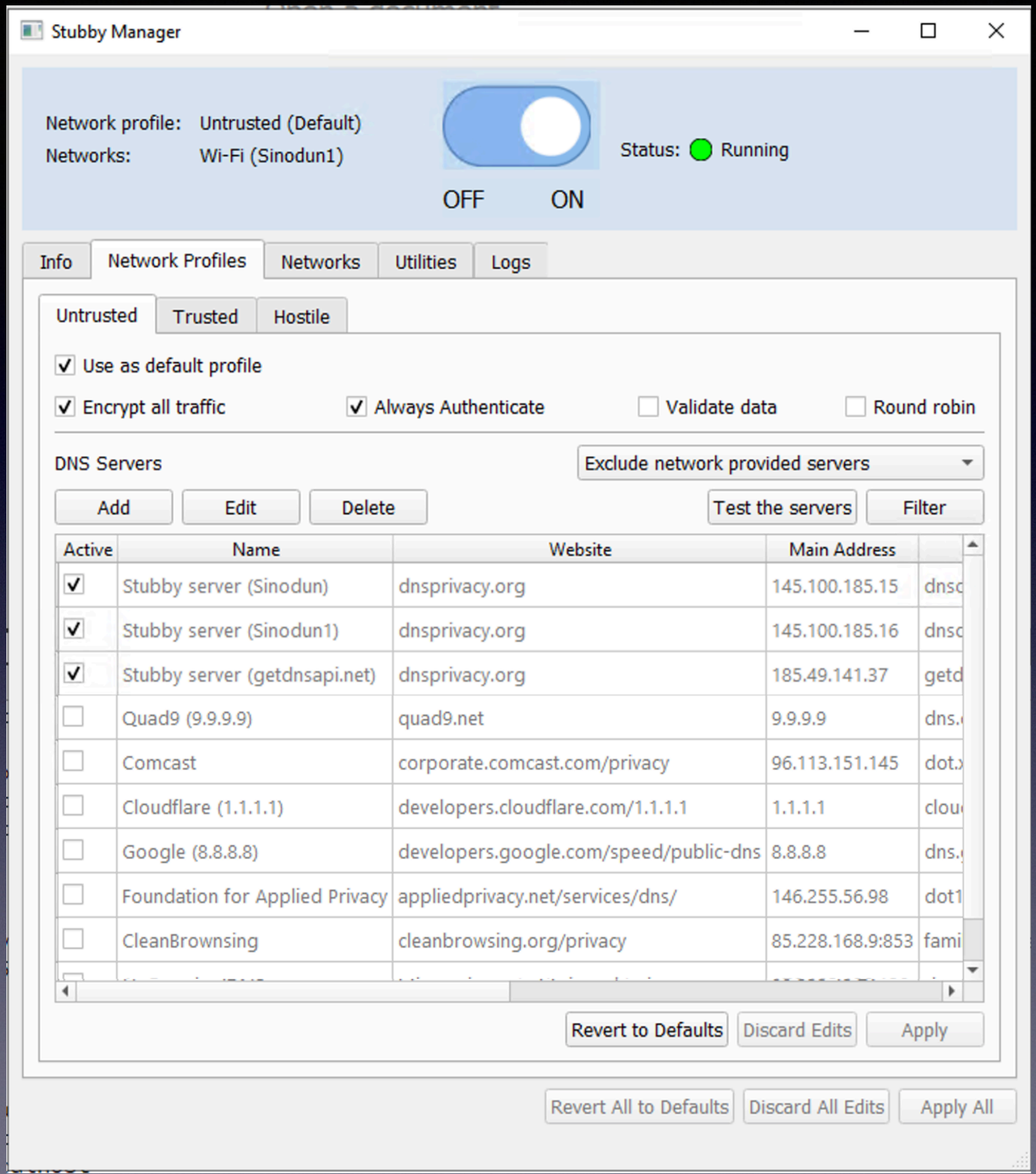
- **Provide background** with links to more detailed info
- **Single on/off button** (like a VPN)
- Show network and profile
- First run has dialog for ‘Just turn stubby on to encrypt your DNS’ and then warns which resolvers are used by default



Welcome page

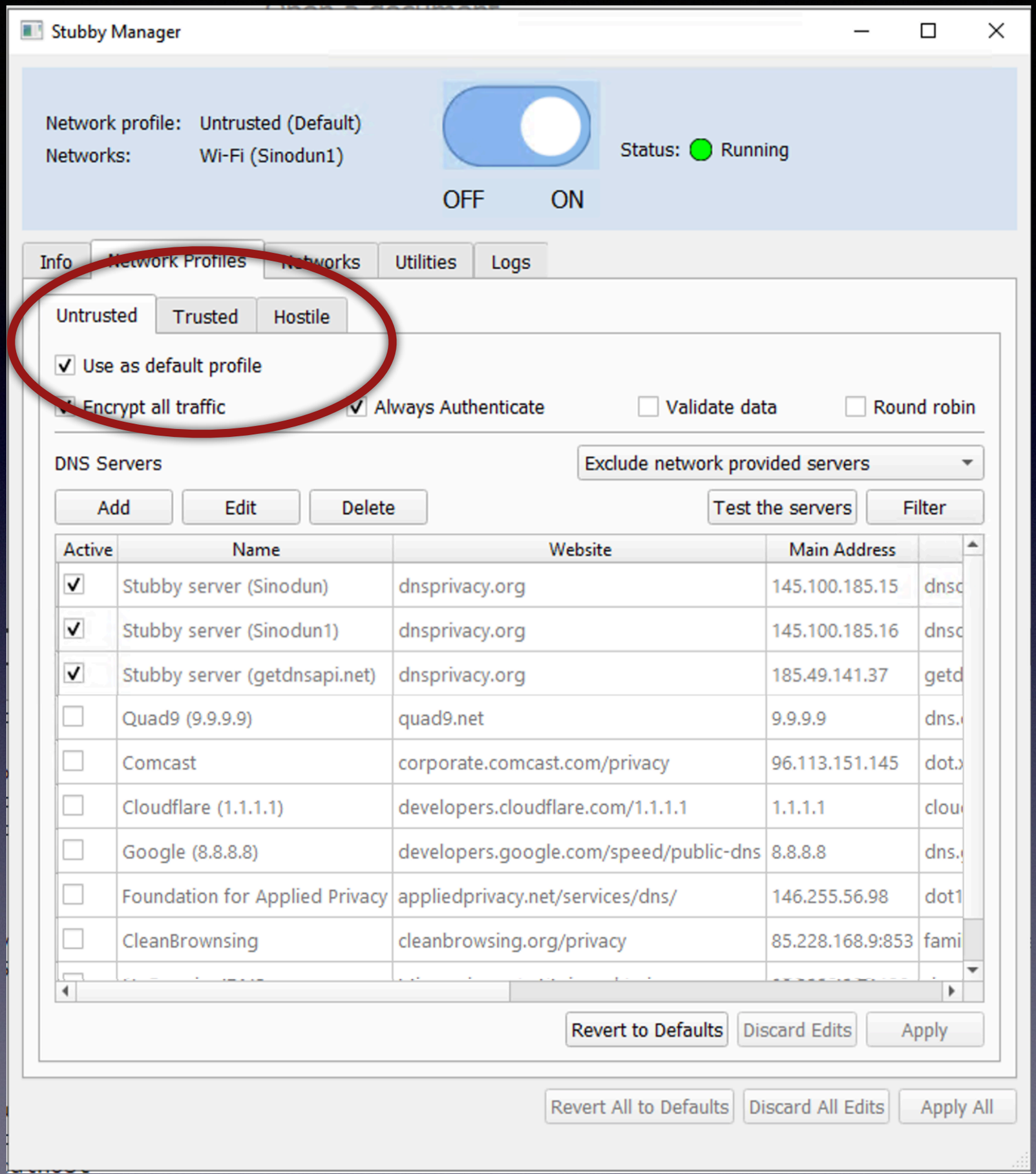
- **Provide background** with links to more detailed info
- **Single on/off button** (like a VPN)
- Show network and profile
- First run has dialog for ‘Just turn stubby on to encrypt your DNS’ and then warns which resolvers are used by default

Network profiles



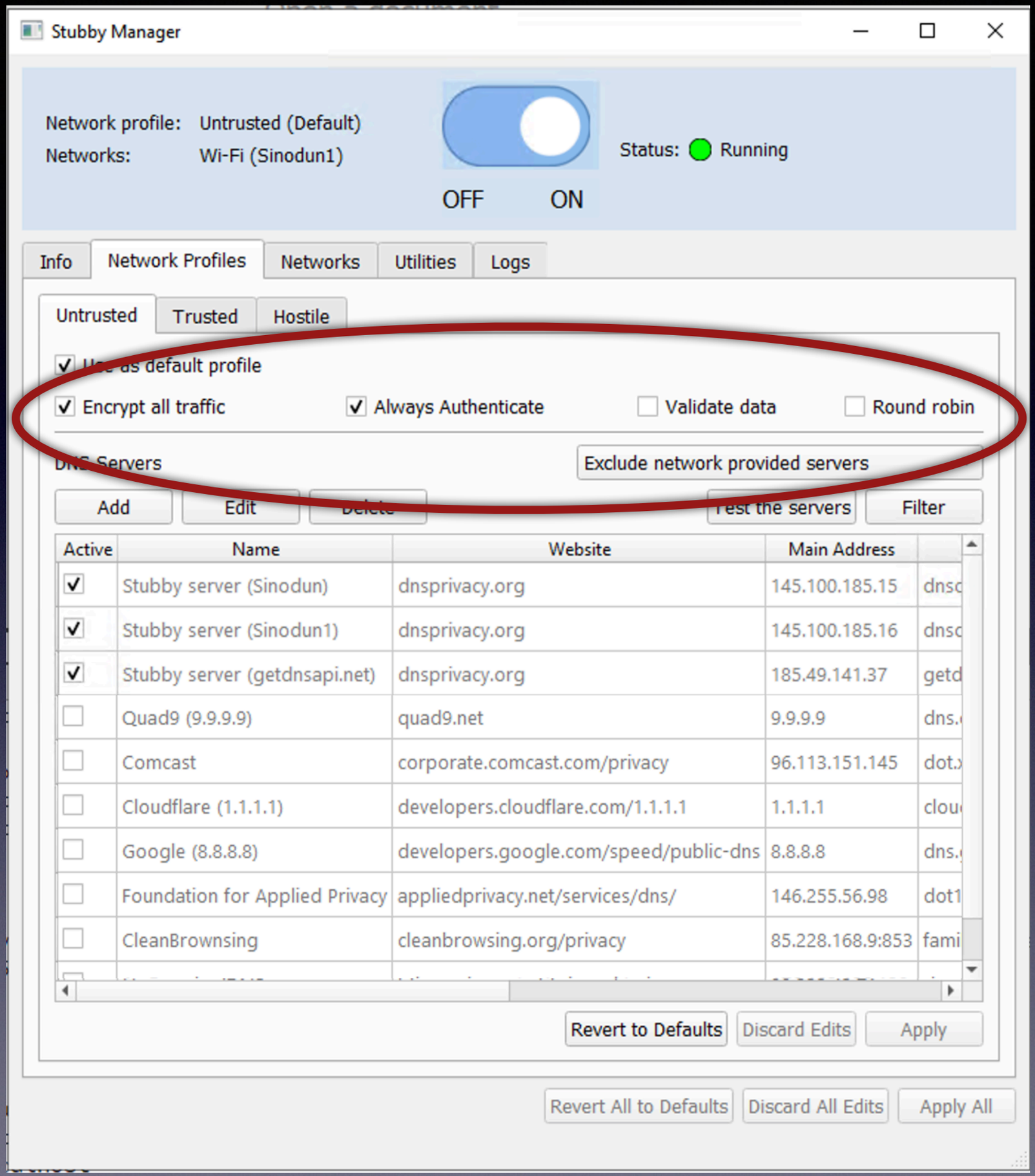
- **Untrusted** (Strict DoT to user configured resolver)
- **Trusted** (Op DoT to network resolver)
- **Hostile** (DoH, but VPN better?)
- Default can be set
- Minimum options/maximum flexibility here (expert mode for anything else)
- Links to resolver information

Network profiles



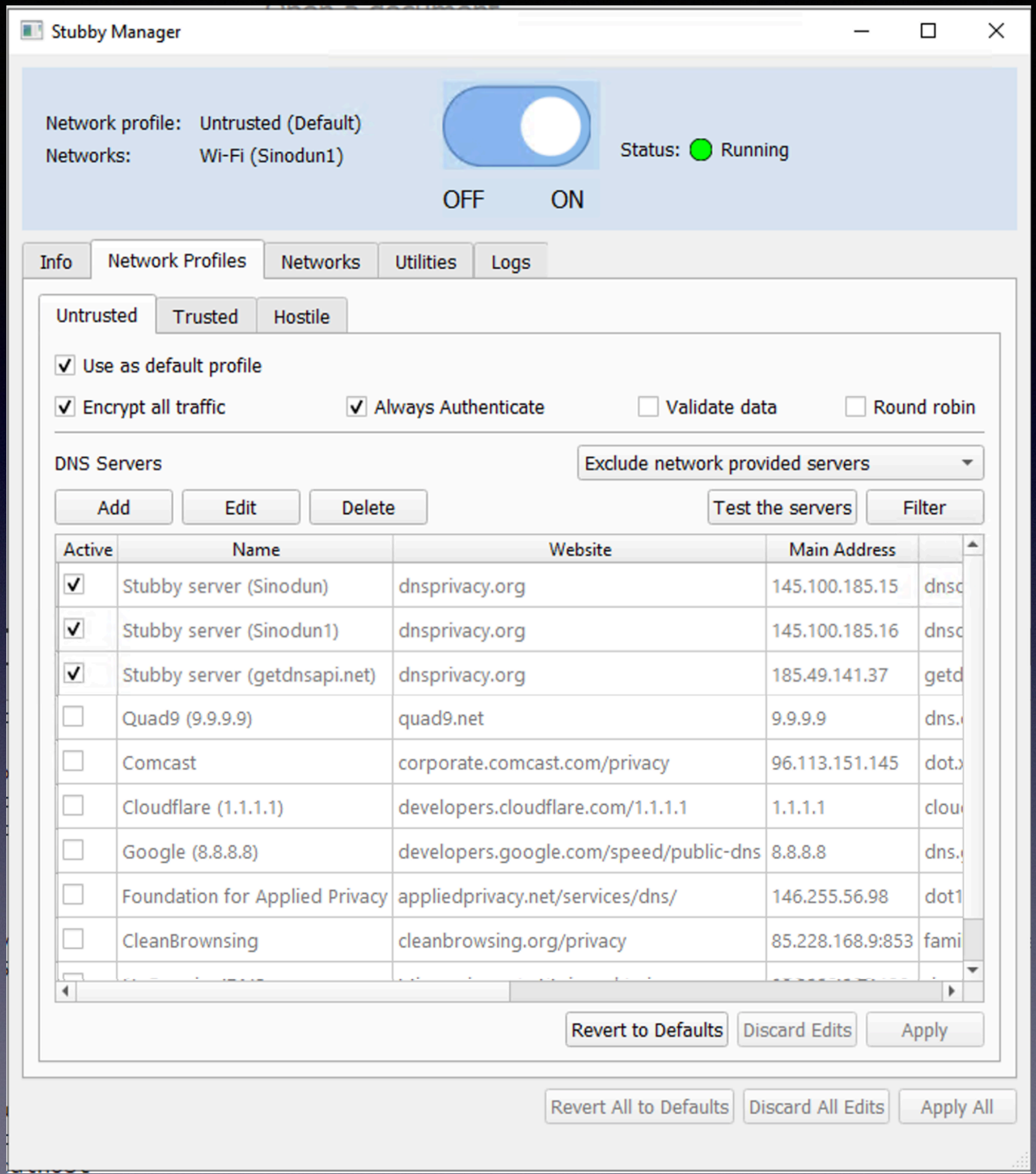
- **Untrusted** (Strict DoT to user configured resolver)
- **Trusted** (Op DoT to network resolver)
- **Hostile** (DoH, but VPN better?)
- Default can be set
- Minimum options/maximum flexibility here (expert mode for anything else)
- Links to resolver information

Network profiles



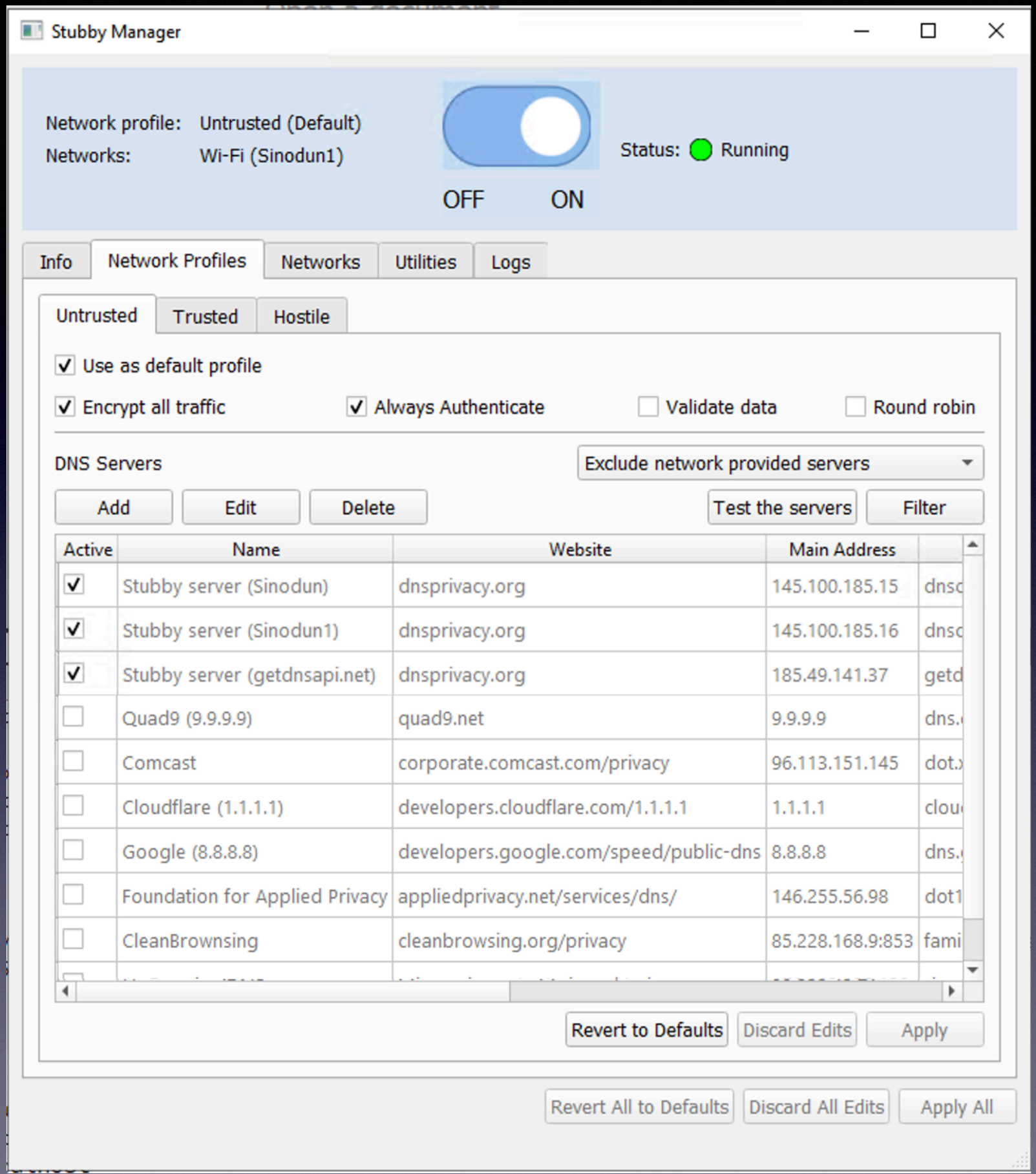
- **Untrusted** (Strict DoT to user configured resolver)
- **Trusted** (Op DoT to network resolver)
- **Hostile** (DoH, but VPN better?)
- Default can be set
- Minimum options/maximum flexibility here (expert mode for anything else)
- Links to resolver information

Network profiles



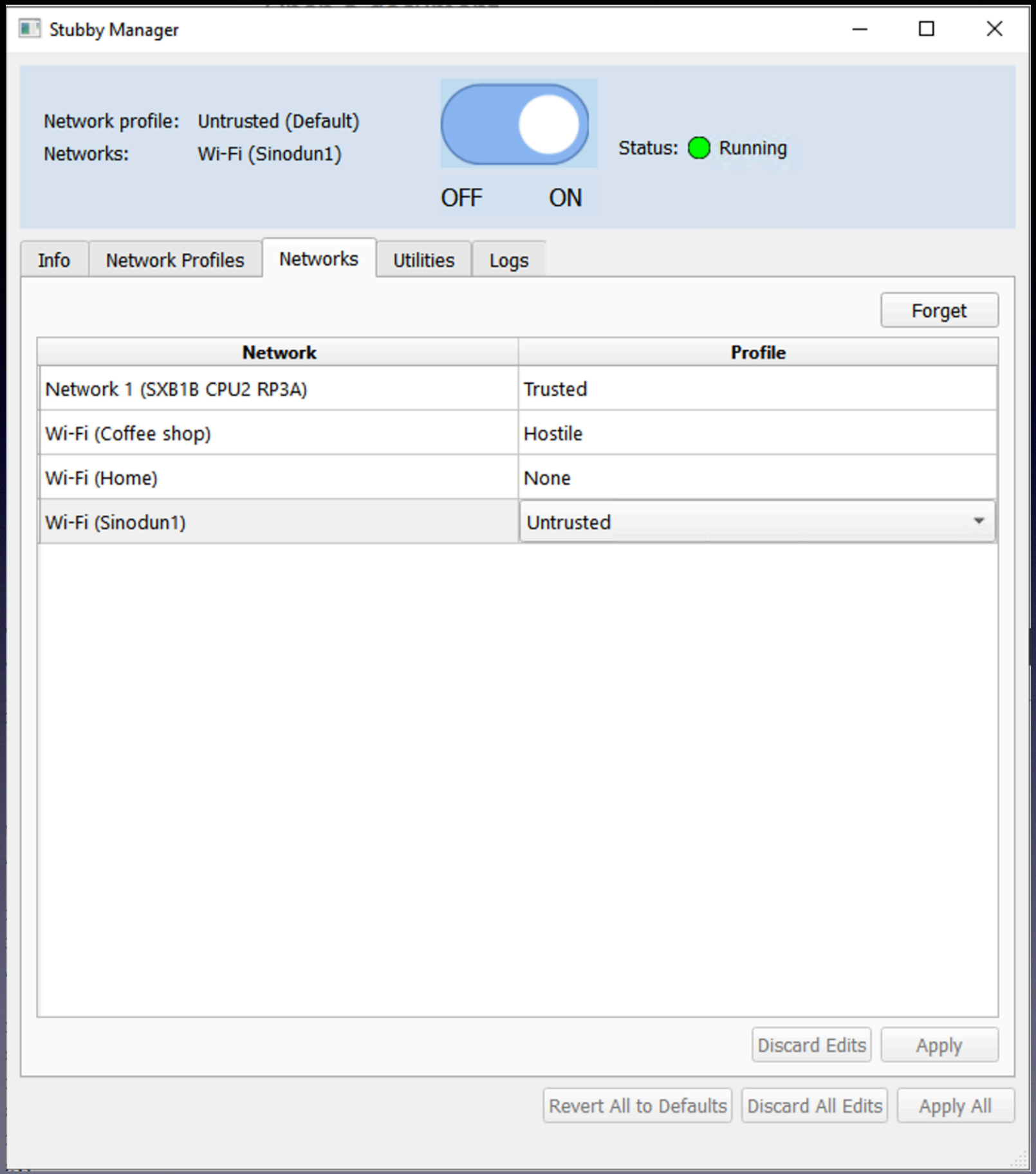
- **Untrusted** (Strict DoT to user configured resolver)
- **Trusted** (Op DoT to network resolver)
- **Hostile** (DoH, but VPN better?)
- Default can be set
- Minimum options/maximum flexibility here (expert mode for anything else)
- Links to resolver information

Network profiles



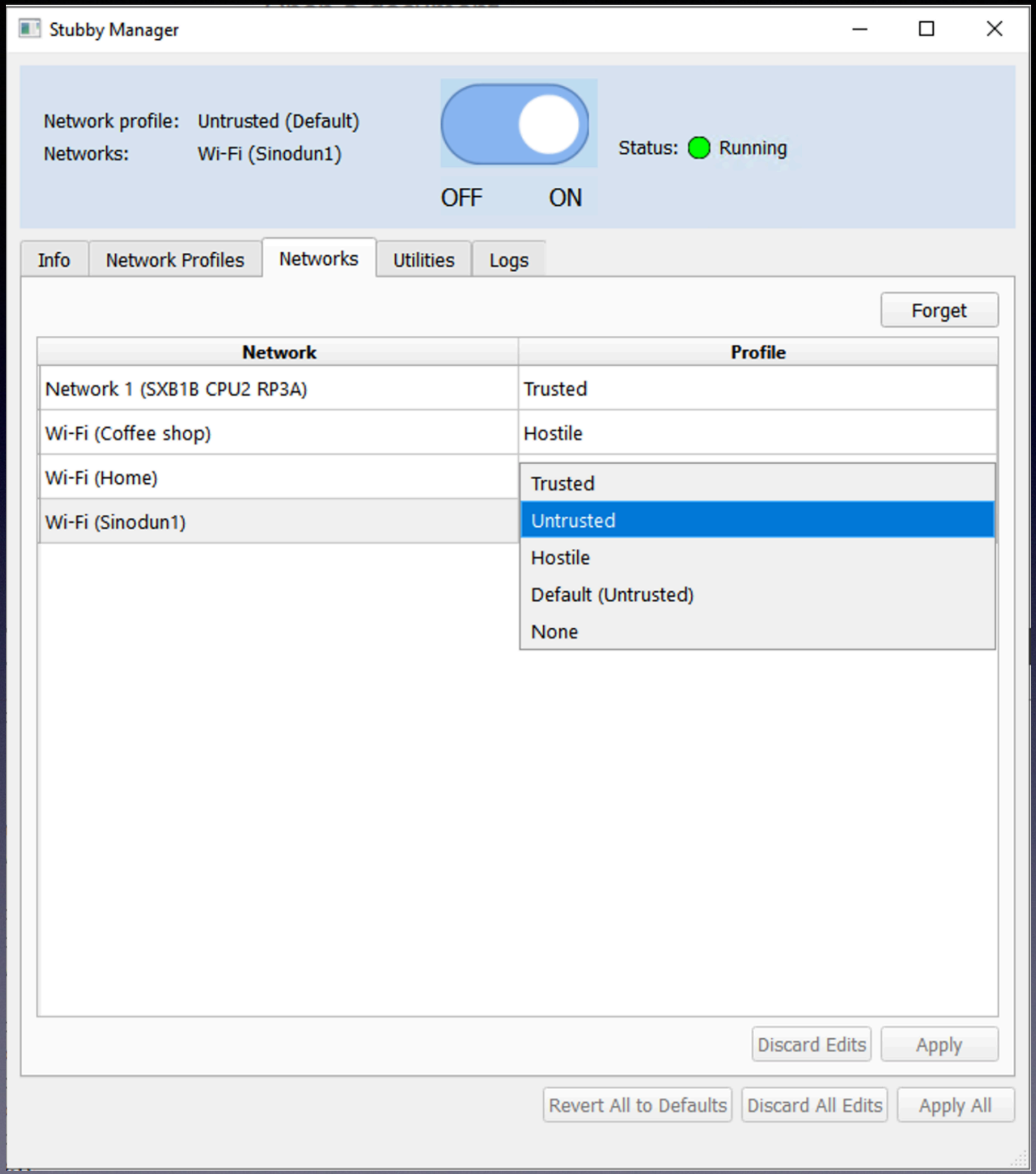
- **Untrusted** (Strict DoT to user configured resolver)
- **Trusted** (Op DoT to network resolver)
- **Hostile** (DoH, but VPN better?)
- Default can be set
- Minimum options/maximum flexibility here (expert mode for anything else)
- Links to resolver information

Networks



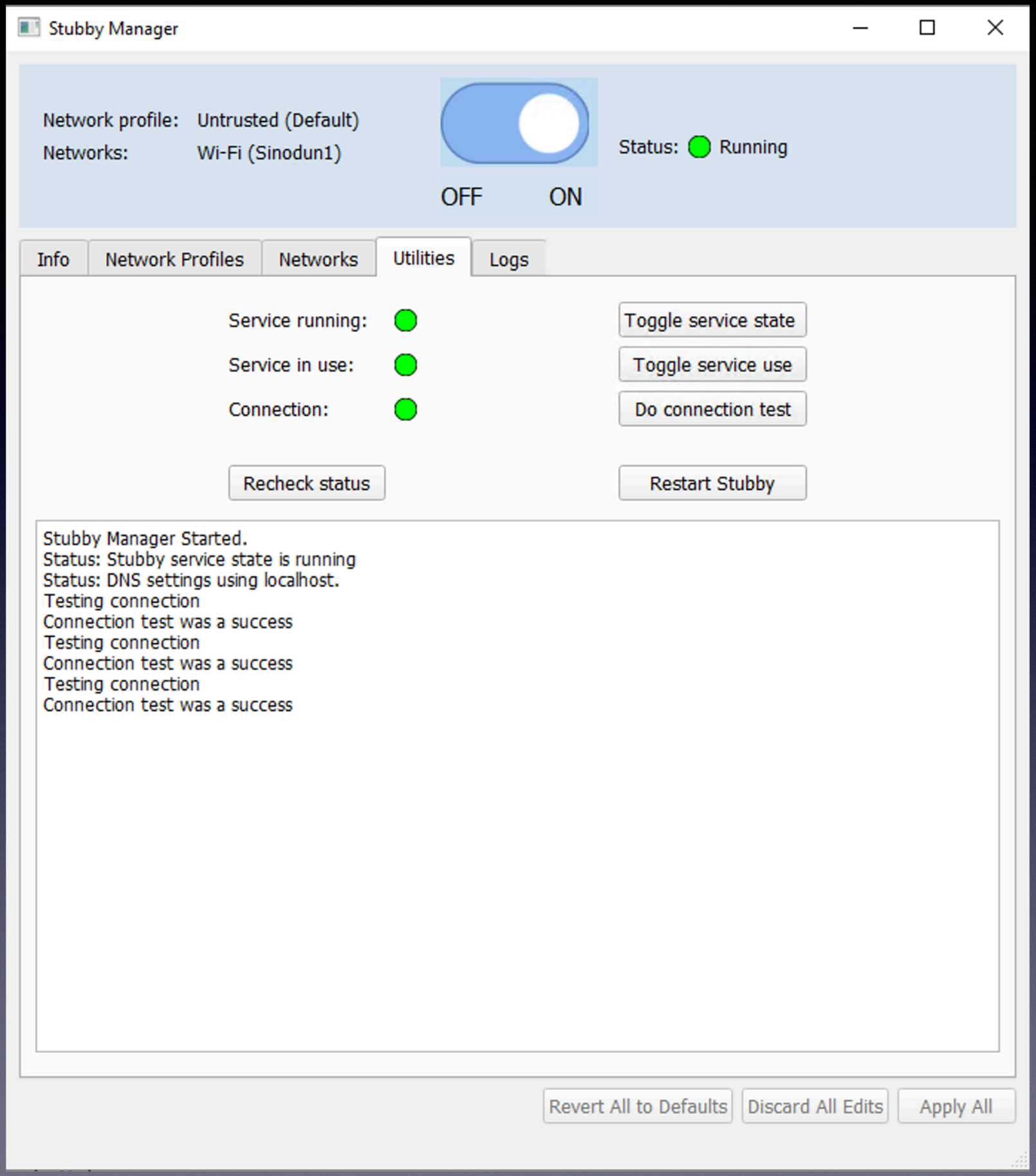
- Drop down enables **selection of profile** or override of default
- When new networks are joined default used if set, dialog for profile selection if not
- **System tray icon** indicates service state

Networks



- Drop down enables **selection of profile** or override of default
- When new networks are joined default used if set, dialog for profile selection if not
- **System tray icon** indicates service state

Utilities



- For **troubleshooting**/ advanced users show more detail and controls
- **Periodic probe query** checks connection to report issues via alerts and logs
- **Logs** also available on another tab (stubby service and DNS query logging)

Stubby GUI Status

- **Alpha release** (0.4.0-a1) has just been made
  Code: https://github.com/Sinodun/Stubby_Manager
  Documentation: On dnsprivacy.org
  Beta release is coming…. still a work in progress!

- Future features
  - **Probe mode for servers** to detect connectivity and measurable properties (DNSSEC, padding, etc)
  - **Custom profile** and expert mode for config edit

- Future work ongoing… get in touch if interested!

Thank you!

Any Questions?

dnsprivacy.org