

# DNSCrypt

## Windows Guide

Securing Communications



## I. Introduction

---

DNSCrypt is a software application (tool) for securing communications between a client (YOUR PC) and a DNS resolver (THEIR Server).

**What's wrong with DNS queries?** For one, they're not encrypted. That opens the door to:

- **Spying:** Attackers use DNS to spy on Internet users' online activity via DNS replay, observation, and timing attacks.
- **Man-in-the-middle attacks:** When an attacker intercepts the communication stream and impersonates both the local and remote station.
- **Resolver impersonation:** Intermediaries hijack DNS traffic destined for trusted naming servers, rerouting them to malicious name servers; which in turn, provide fraudulent query responses.

When you type a name in the URL field of a web browser, you expect to go to the appropriate web site. But if something or someone is messing with the DNS query, that may not be the case. For example, instead of going to your bank's website, you may be sent to a very good copy of the actual website specifically to steal your banking credentials.

This guide describes how to install and configure DNSCrypt on your Windows PC.

## II. Specifications and Requirements (2013-09-15)

---

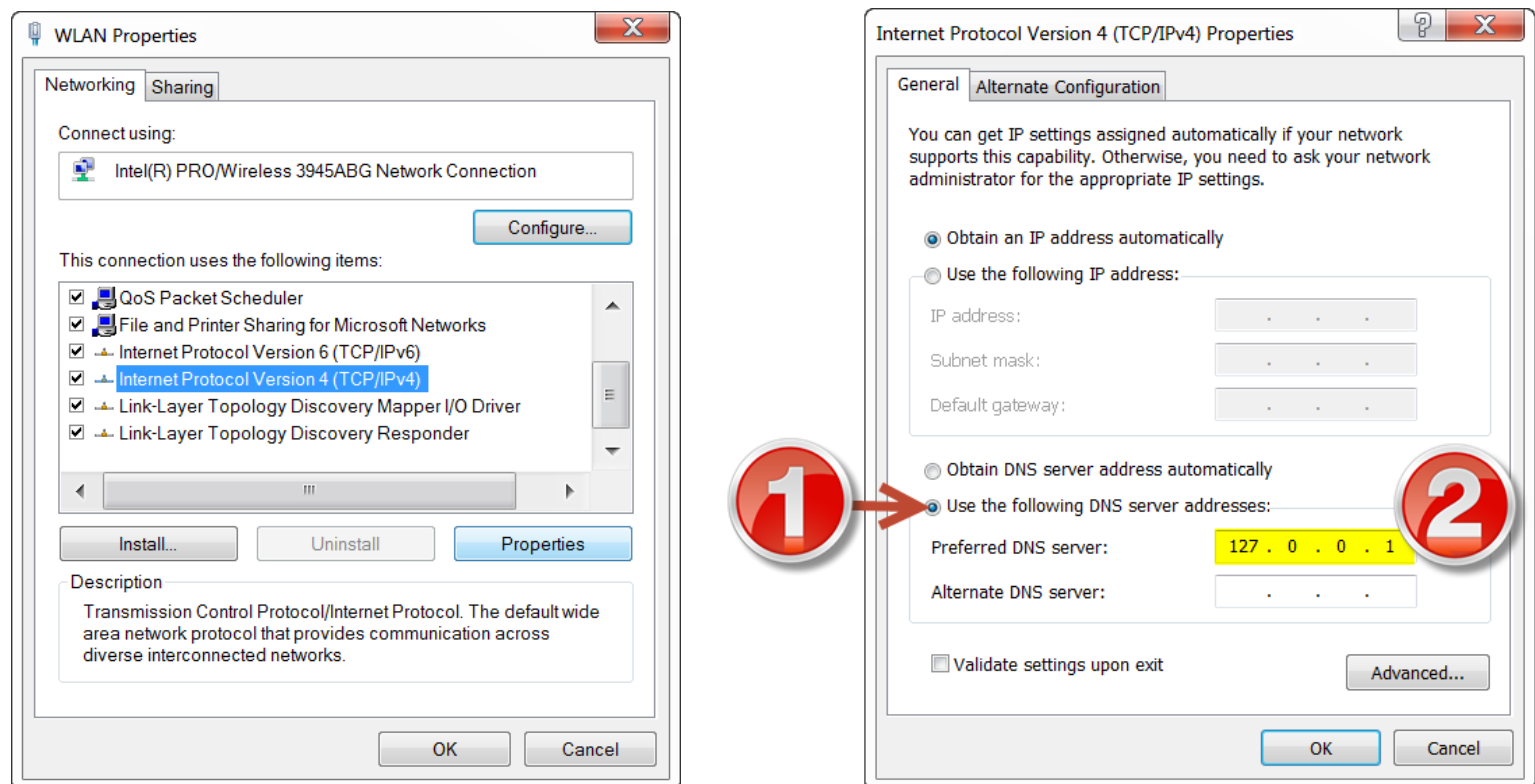
1. DNSCrypt Site: <http://dnscrypt.org>
2. Download Page: <http://download.dnscrypt.org/dnscrypt-proxy>
3. [dnscrypt-proxy-win32-full-1.3.3.zip](#) 766KB MD5: **AD85A550B011369FAC9AA478E2B3B8A3**
4. Windows XP SP3, Vista, 7, 8, 8.1

### III. DNSCrypt Installation and Configuration

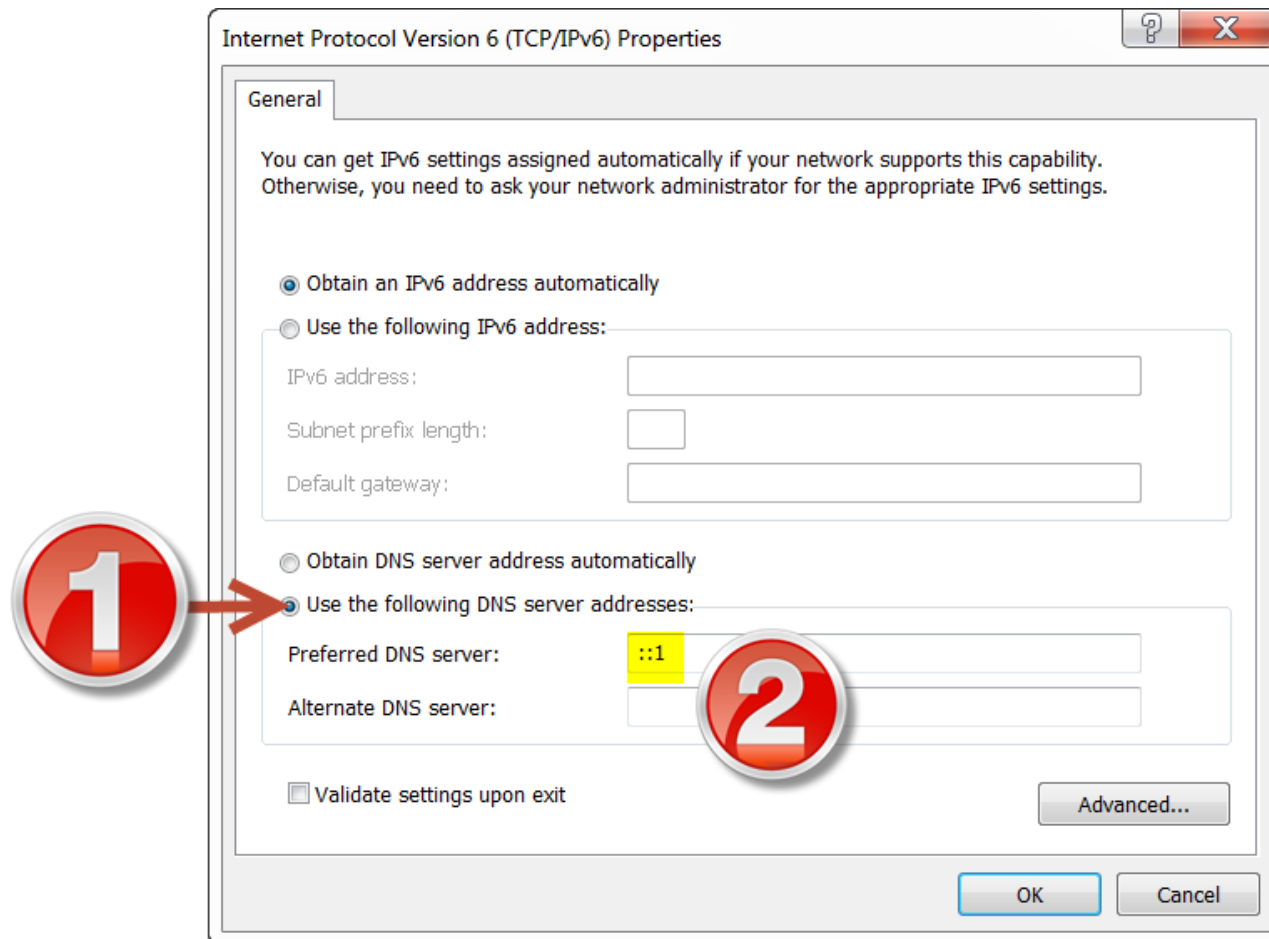
1. Download [dnscrypt-proxy-win32-full-1.3.3.zip](#) and confirm the MD5 hash integrity for authenticity by using [HashTab](#). It's a free Windows Explorer extension that adds a "File Hash" Tab.
2. Under the `Program Files\` directory create the following `DNSCrypt` folder. Then copy or move the following files into this folder you just made; `dnscrypt-proxy.exe`, `libldns-1.dll`, `libsodium-4.dll`.
3. Next open a terminal (run `cmd.exe`) and type (you may need to specify the full path to the file): `dnscrypt-proxy.exe --install` (if later you want uninstall use `dnscrypt-proxy.exe --uninstall`)
4. Change your DNS settings to `127.0.0.1` for IPv4 and `::1` for IPv6.

To do that go to the following location;

**Control Panel\Network and Internet\Network Connections** and right click over the network adapter (RJ-45 Ethernet and or WLAN) that your wanting to use DNSCrypt with by selecting "**properties**". On the networking tab scroll down and right click over IPv4 selecting "**properties**" and enter `127.0.0.1` as the preferred DNS server address.



Then do the same for IPv6 except enter **::1** as the preferred DNS server address.



5. DNSCrypt v1.1.3 comes setup by default to use the [OpenDNS](#) service for the DNS resolving server. However, you can easily insert any other DNSCrypt-enable resolver address such as [DNSCrypt.EU](#).
6. Copy the following text (below) into a text file (txt) and rename the file extension from "txt" to "reg" so later you can MERGE the parameter values into the registry or manually import them yourself.

Windows Registry Editor Version 5.00

```
[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\dnscrypt-proxy\Parameters]
"ProviderKey"="67C0:0F2C:21C5:5481:45DD:7CB4:6A27:1AF2:EB96:9931:40A3:09B6:2B8D:1653:1185:9C66"
"ProviderName"="2.dnscrypt-cert.dnscrypt.eu"
"ResolverAddress"="176.56.237.171:443"
"LocalAddress"="127.0.0.1"
```

After importing the REG file reboot the PC. Then check <https://www.dnsleaktest.com> to see if everything is working correctly after you've set it up.

## IV. Current List of **FREE** DNSCrypt-enabled resolvers

---

### [DNSCrypt.eu \(no logs\)](#)

Holland Server address: **176.56.237.171:443**

Provider name: **2.dnscrypt-cert.dnscrypt.eu**

Public key: 67C0:0F2C:21C5:5481:45DD:7CB4:6A27:1AF2:EB96:9931:40A3:09B6:2B8D:1653:1185:9C66

### [OpenDNS](#)

San Francisco, U.S. Server address: **208.67.220.220:443**

Provider name: **2.dnscrypt-cert.dnscrypt.org**

Public key: B735:1140:206F:225D:3E2B:D822:D7FD:691E:A1C3:3CC8:D666:8D0C:BE04:BFAB:CA43:FB79

### [CloudNS \(no logs\)](#)

Canberra, Australia

Server address: **113.20.6.2:443** or **gc2tzw6lbmeagrp3.onion:443**

Provider name: **2.dnscrypt-cert.cloudns.com.au**

Public key 1971:7C1A:C550:6C09:F09B:ACB1:1AF7:C349:6425:2676:247F:B738:1C5A:243A:C1CC:89F4

Sydney, Australia

Server address: **113.20.8.17:443** or **l65q62lf7wnfme7m.onion:443**

Provider name: **2.dnscrypt-cert-2.cloudns.com.au**

Public key: 67A4:323E:581F:79B9:BC54:825F:54FE:1025:8B4F:37EB:0D07:0BCE:4010:6195:D94F:E330

### [OpenNIC \(no logs\)](#)

Japan Server address: **106.186.17.181:2053**

Provider name: **2.dnscrypt-cert.ns2.jp.dns.opennic.glue**

Public key: 8768:C3DB:F70A:FBC6:3B64:8630:8167:2FD4:EE6F:E175:ECFD:46C9:22FC:7674:A1AC:2E2A

## V. Have a suggestion to improve this Guide?

---

What to know more about DNSCrypt?

- 1) <http://shinobi.dempsky.org/~matthew/dnscurve.org-20090517/index.html>
- 2) <http://www.opendns.com/technology/dnscrypt>

You may find it interesting to discover the video documentary "[Paradise or Oblivion](#)" and "[Thrive](#)".