


# Manual for Dnssec-Trigger on Windows

W.C.A. Wijngaards, NLnet Labs, June 2012

## Introduction

 This manual aims to provide information about the Dnssec Trigger package on the Windows platform. Included is installation, uninstallation and some information on the implementation specific for Windows.

## What is Dnssec Trigger


This is explained on its webpage <http://www.nlnetlabs.nl/projects/dnssec-trigger>

The package installs a local DNSSEC validator on the windows machine, that checks answers from the DNS for authenticity.

## Installation

Download the installer from the <http://www.nlnetlabs.net> website. Run the installer. On Windows Vista/7 you have to provide administrator permission, because the services that are installed have to run as administrator. You have to accept our license (the BSD open source license).

The software is installed in C:\Program Files\DnssecTrigger by default. The main dnssec-trigger programs are installed, but also some other software is installed to this directory:

 The Unbound service is installed, it is the dnssec validator and DNS server (<http://unbound.net>). This unbound install is especially configured by the installer to work with dnssec-trigger. Keys are generated, and the config is set to do DNSSEC validation (with the root trust anchor). If you installed unbound with its own installer you have to uninstall that; the dnssec-trigger installer contains its own copy of unbound.

The LDNS library is installed as well (as dll in C:\Program Files\DnssecTrigger). It is a library for making DNS and DNSSEC tools.

The expat library is installed (as dll). It is an xml parser used by unbound-anchor to parse root anchors xml files.

The OpenSSL libcrypto and libssl libraries are installed (as dll). It provides the public key crypto that is used for DNSSEC. Dnssec-trigger uses SSL connections (from the local computer to the local computer) for interprocess communication.

The services are started automatically for you after installation (no need to

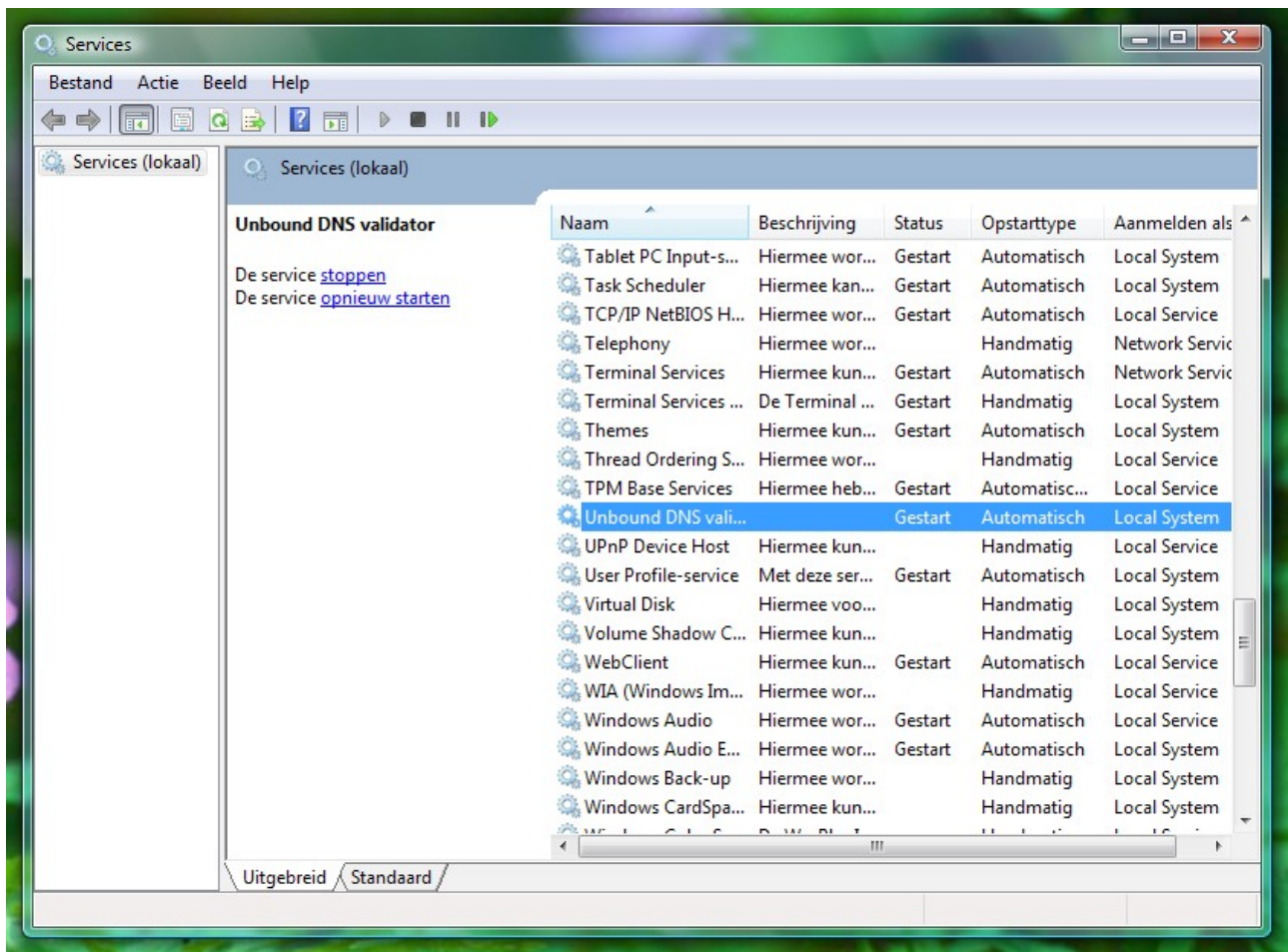
reboot). You should allow unbound.exe, unbound-anchor.exe and dnstsd.exe to access the network when the windows firewall (or your installed firewall) asks for permission.

## Uninstallation

Run the uninstaller, the executable from the ProgramFiles directory, from the start menu, or from the software control panel. Services are stopped, and the normal DNS resolution behaviour is reinstated.

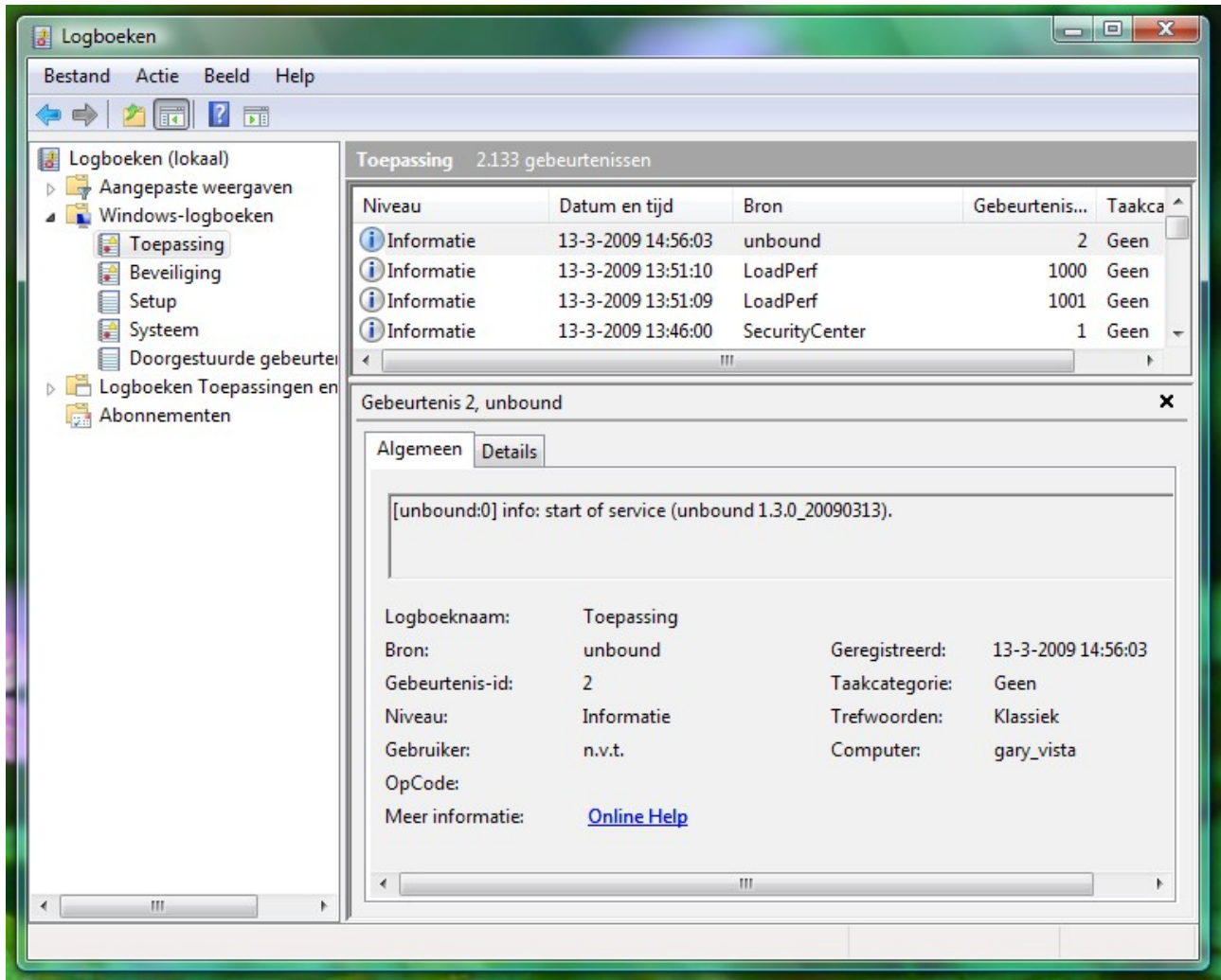
## Check if it is running

Open the Control Panels\System Administration\Services:



There are two services: the unbound service and the dnssec-trigger service. The unbound service runs on localhost (listens to 127.0.0.1) and provides DNS and DNSSEC services. The dnssec-trigger service listens to (wifi-)network changes and probes the new networks and then instructs unbound what to do.

## Reading the error log



Open the Control Panel\System Administration\Log books. The unbound and dnssec-trigger entries are in the Application log. Depending on the verbosity level (that you configured), more or less log entries are shown. For help with errors see documentation on the website, user community and bug tracker. The entry shown is the notification that unbound has started. Resolvers run into errors, local or remote, more frequently than other software, many are handled by the resolver automatically. The default verbosity setting logs only serious errors; errors that cause the program to terminate abnormally, for example.

## Advanced – editing the config file

Two config files are stored, by default in C:\Program Files\DnssecTrigger.

The unbound.conf file contains the unbound service configuration settings. The installer added settings that enable DNSSEC and allow the inter-process communication. There is full documentation for the options at

<http://unbound.net/documentation/unbound.conf.html>.

The `dnssec-trigger.conf` file contains `dnssectrigger` service configuration settings. The installed added settings that allow inter-process communication. There is documentation for the options in the file itself and at <http://www.nlnetlabs.nl/projects/dnssec-trigger/dnssec-trigger.8.html>.

You can edit the config files using a text editor. Notepad won't understand the unix line endings (but unbound understands both unix and windows line endings). Use a better editor, such as Notepad++ to edit the config files.

The unbound config file has an option called `val-log-level`: 0 it is 0 by default, but setting it to 2 will cause a system log message for every validation error. This may help with troubleshooting. The config file is reread when you restart the service.

## Advanced – tools installed

The following files and tools are installed into `C:\Program Files\DnssecTrigger`

- `LICENSE`: this is a text file with the source code license.
- `unbound.conf`: file with unbound configuration options.
- `dnssec-trigger.conf`: file with dnssec trigger configuration options.
- `dnssec-triggerd.exe`: the daemon, dnssec trigger main service file. Can also be run from the command line if you like.
- `dnssec-trigger-panel.exe`: the userspace tray icon. Started for every user. It appears in the taskbar and provides a menu. Its main functionality is to show the security pop up dialogs. Multiple users logged in is supported (they all get a tray icon).
- `dnssec-trigger-control.exe`: commandline tool to control the dnssec trigger daemon.
- `dnssec-trigger-keygen.exe`: Used by the installer to generate ssl keys for the inter-process communication (between the panel, `dnssec-triggerd` and `unbound`).
- `unbound.exe`: the daemon, the unbound main service file. Can also be run from the command line if you like.
- `unbound-checkconf.exe`: commandline tool that checks for errors in the configuration file
- `unbound-host.exe`: commandline tool to perform DNS lookups standalone.
- `unbound-control.exe`: commandline tool to control the unbound daemon. Used for inter-process communication too.
- `unbound-anchor.exe`: commandline tool that updates the root trust anchor. It is called by the main daemon before it starts.
- `uninst.exe`: the uninstaller.
- `root.key`: This file contains the public key for the root. It is updated by `unbound-anchor` (at boot) and by `unbound` itself (during operation).
- `alert.ico` and `status.ico`: icons used by the tray icon for normal and alert images.

## Advanced – registry entries

The following registry settings are affected

HKLM\Software\Unbound:

- DnssecTrigger: set to yes to note that unbound was installed by dnssec-trigger setup.
- InstallLocation: The directory where unbound files reside..
- ConfigFile: The config file to use, unbound.conf by default.
- CronAction: The executable and its arguments started to update trust anchors.
- CronTime: Number of seconds between cron actions, default 24 hours.
- RootAnchor: empty or not present, nothing is performed by the daemon. If it contains the path to the installed unbound-anchor.exe then that is started to update the root key. The unbound service daemon calls the executable right when the services start, at boot time. If the root key was changed by using the (builtin) keys from unbound-anchor, then a log notification (“The root trust anchor has been updated”) is generated (regular RFC5011 rollover does not cause this message).

HKLM\Software\DnssecTrigger:

- InstallLocation: The directory where the files reside.
- ConfigFile: The config file to use, dnssec-trigger.conf by default.
- CronAction: The executable and its arguments for a timed action.
- CronTime: Number of seconds between cron actions, default 24 hours.
- StartMenuFolder: which folder the start menu items were installed in (if any were installed).

Also registry settings for the uninstall information in Add/Remove programs are made (in HKLM\Software\Microsoft\Windows\CurrentVersion\ Uninstall\ DnssecTrigger).