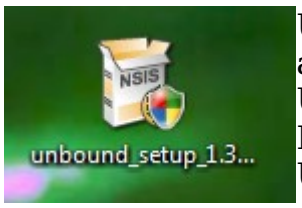
Manual for Unbound on Windows

W.C.A. Wijngaards, NLnet Labs, May 2015

Introduction

This manual aims to provide information about the Unbound server on the Windows platform. Included is installation, uninstallation and some information on configuration specific for Windows. Full details of operating a DNS resolver are not part of this document, and can better be documented in a platform independent document.

What is Unbound and what is DNSSEC



Unbound is a DNS resolver. It supports validation, caching, and DNSSEC. It supports NSEC and NSEC3, Ipv4 and Ipv6. Unbound is written for Unix (posix) machines, and runs on FreeBSD, OpenBSD, NetBSD and Linux (Fedora, Debian, Ubuntu, ...). This document is about the Windows version.

The service that unbound provides is that it performs DNS lookups, and can perform DNSSEC validation on the result. If the result is bad, it is not returned to the client (who sees a temporary error in name resolution). Applications that support DNSSEC can ask to see the verification result.

DNSSEC is a standard for securing the information in the DNS. Your validator needs to have public keys to check the signatures on the data. DNSSEC is explained more fully on http://www.dnssec.net pages.

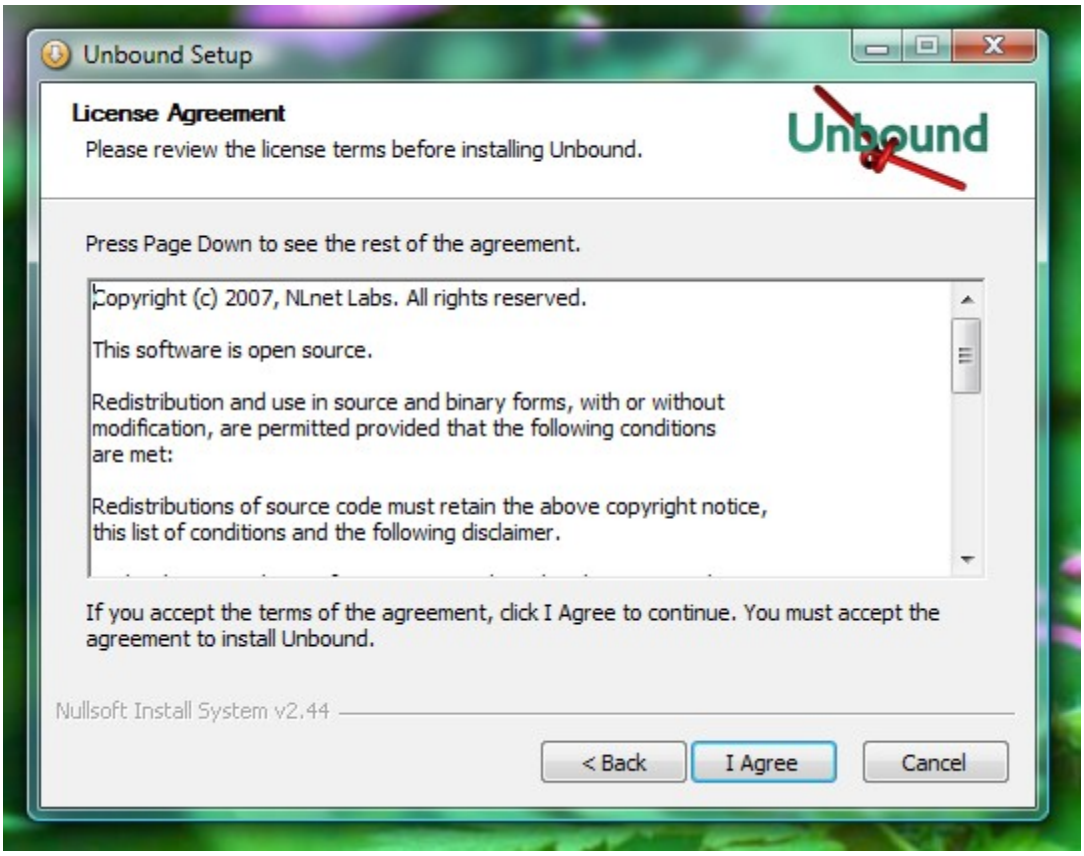
The unbound package for windows provides DNSSEC validation – the client that verifies the signatures published by authoritative DNS servers on the internet.

Installation

Download the installer from the http://unbound.net website. Run the installer. On Windows Vista you have to provide administrator permission.

You are greeted with:

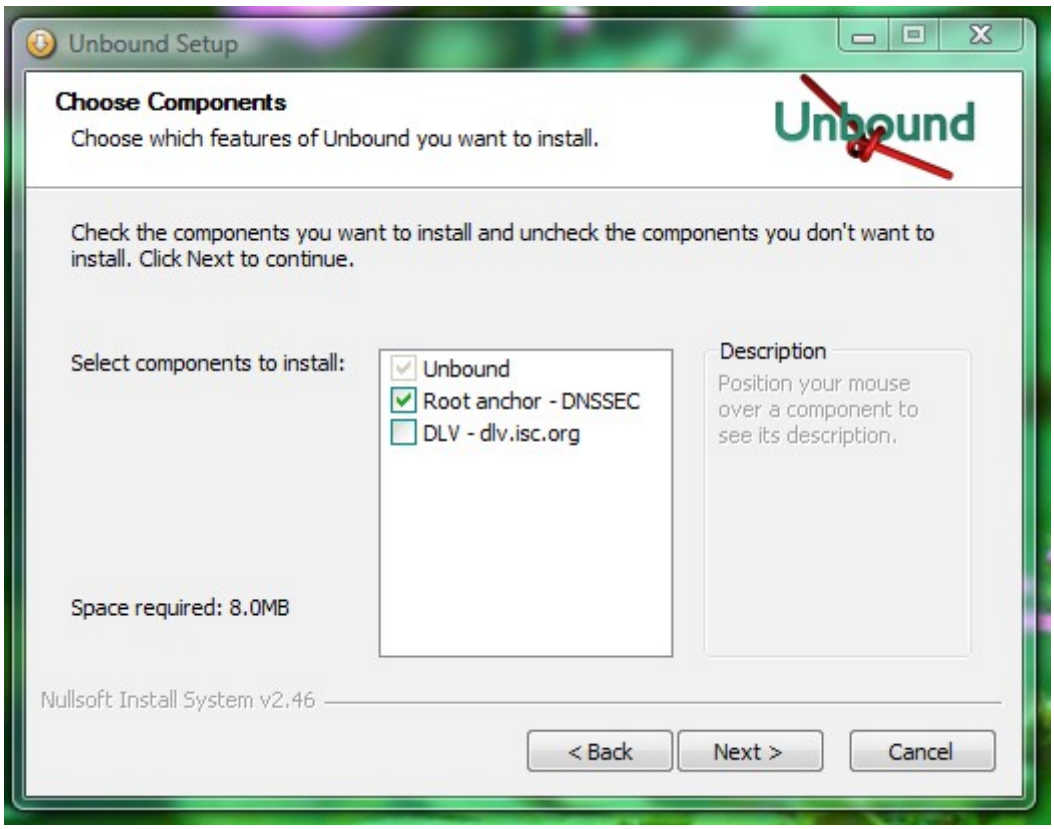
First the license is presented. This is the BSD license used by the source code.



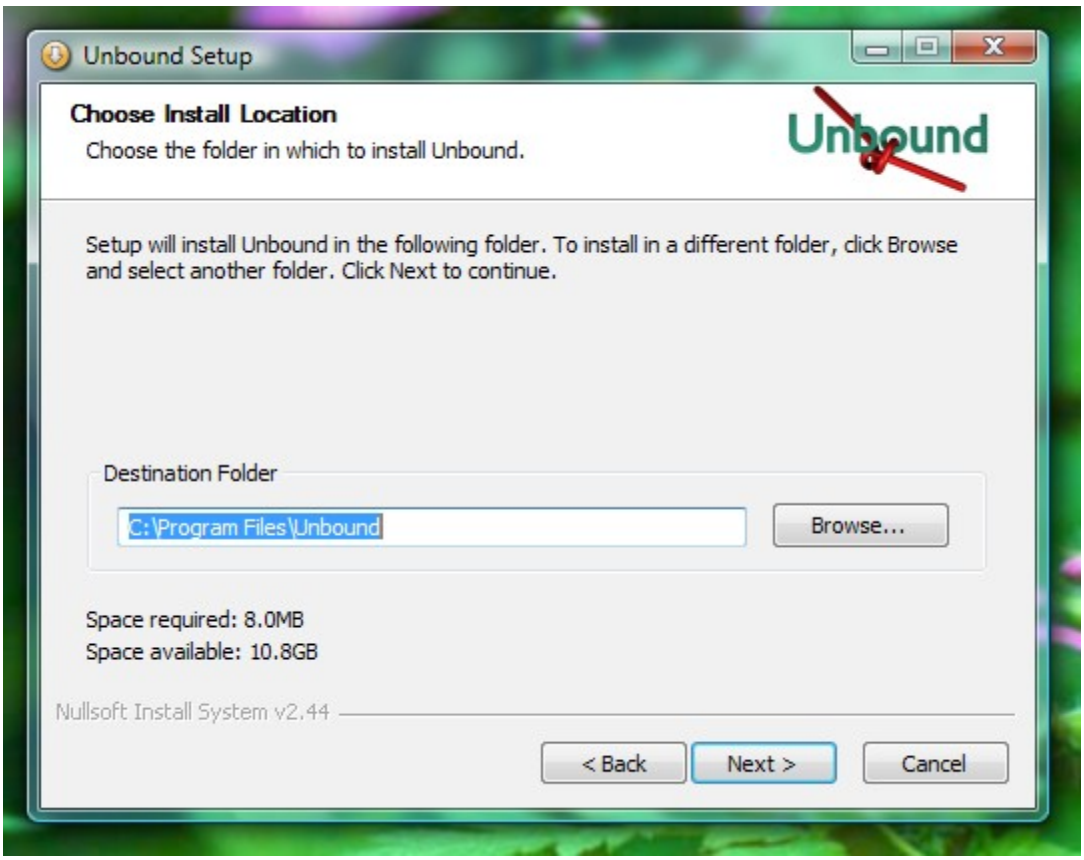
Then choose which components to install. The main component cannot be unselected.

The Root Anchor option enables the root trust anchor so that DNSSEC validation can be performed. It also sets up the update mechanism, that keeps this key up to date.

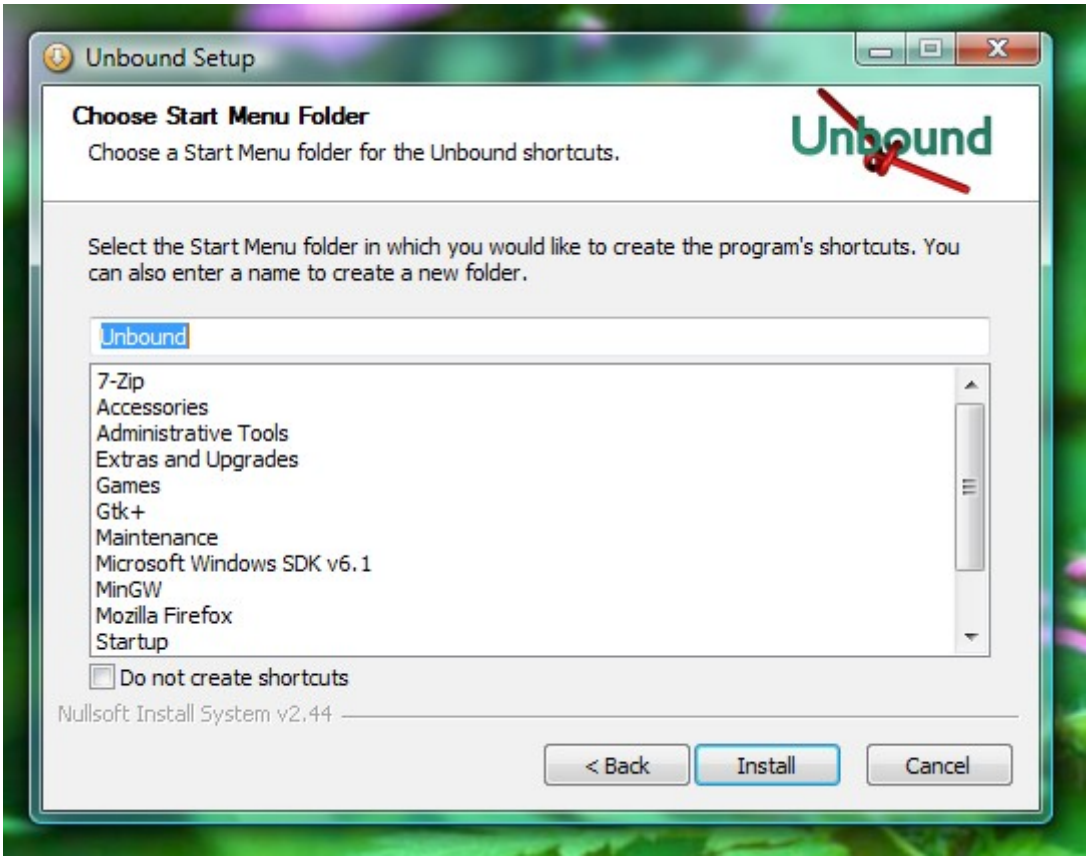
(The DLV option shown in the picture is no longer present, it was useful in the interim period when not all parent domains had been signed with DNSSEC.)

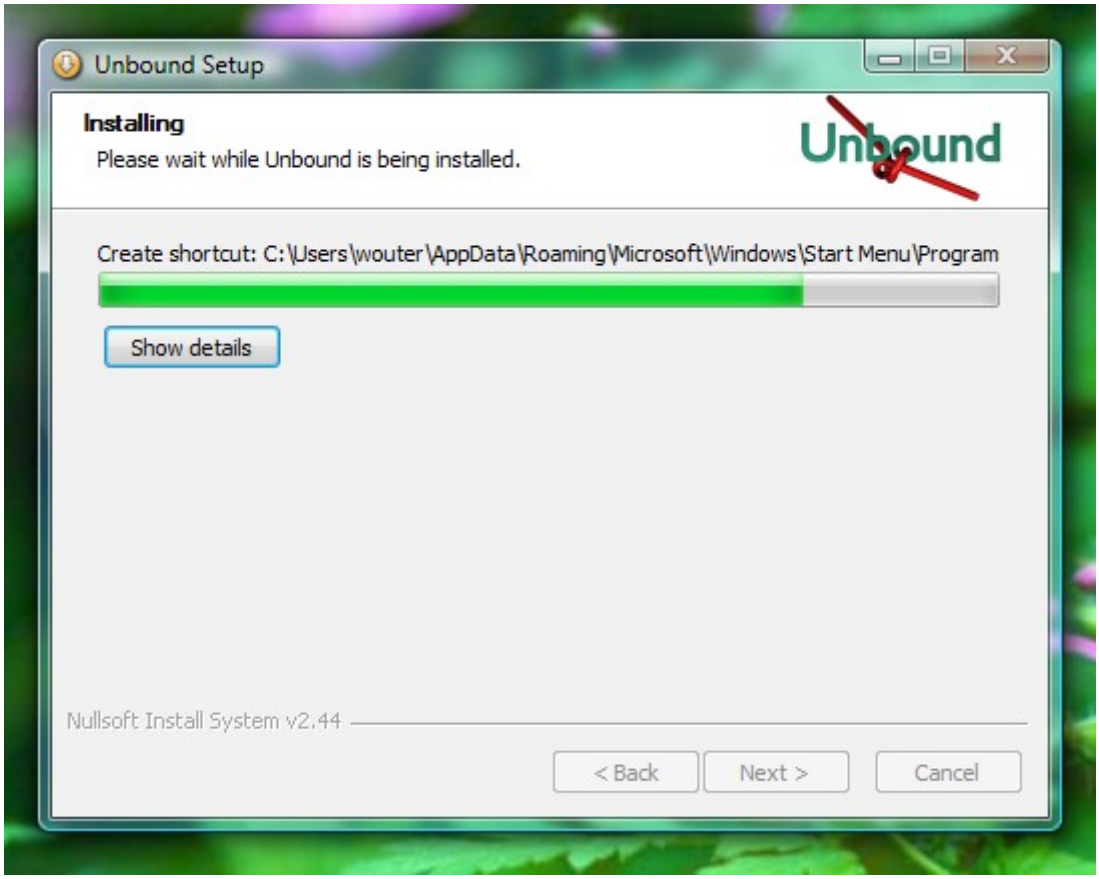


Choose the directory to install into, the default is C:\Program Files\Unbound

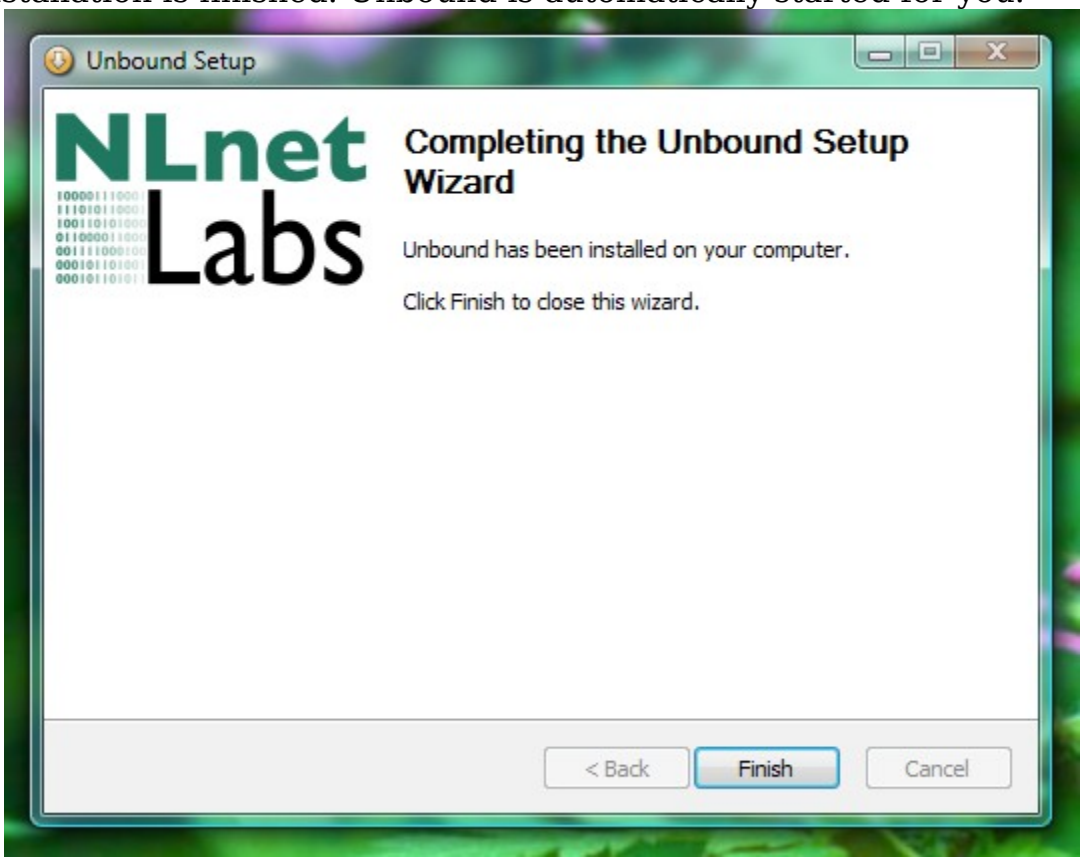


Choose if you want shortcuts in the Start Menu. See a later section of this manual for a description of the shortcuts installed.





The installation is finished. Unbound is automatically started for you.

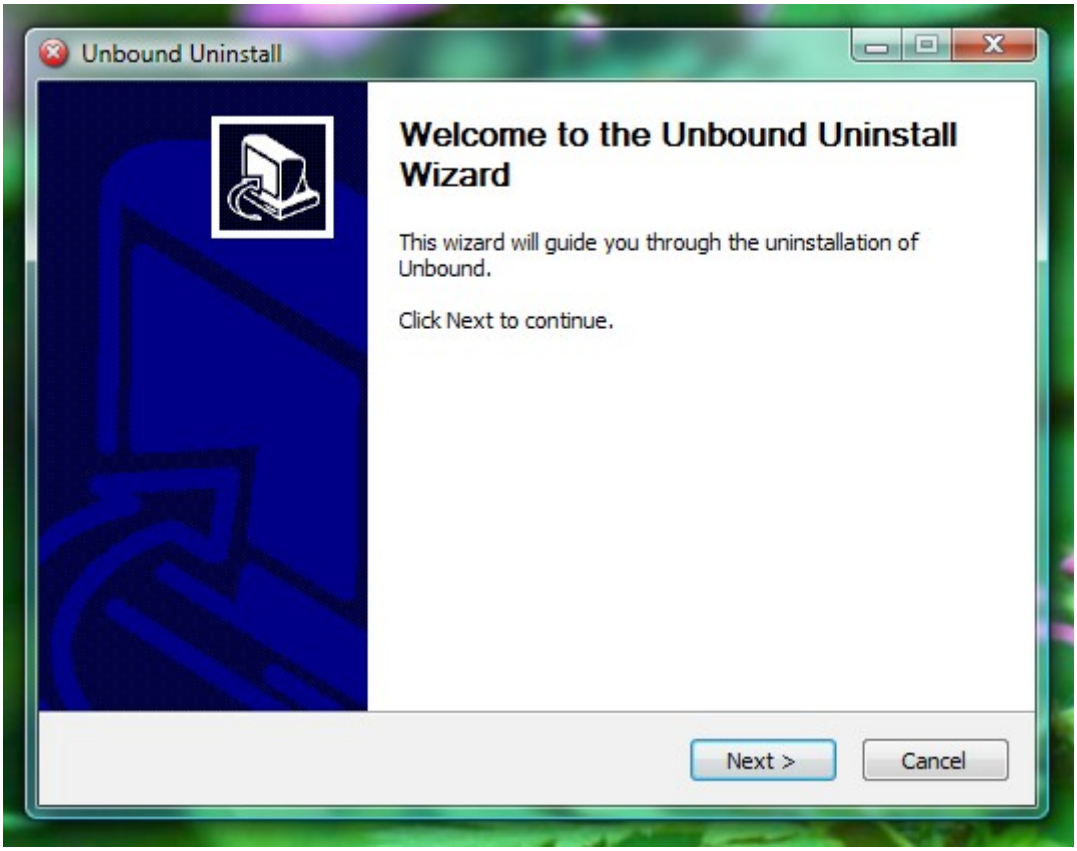


Allow unbound to access the network when the windows firewall (or your installed firewall) asks for permission.

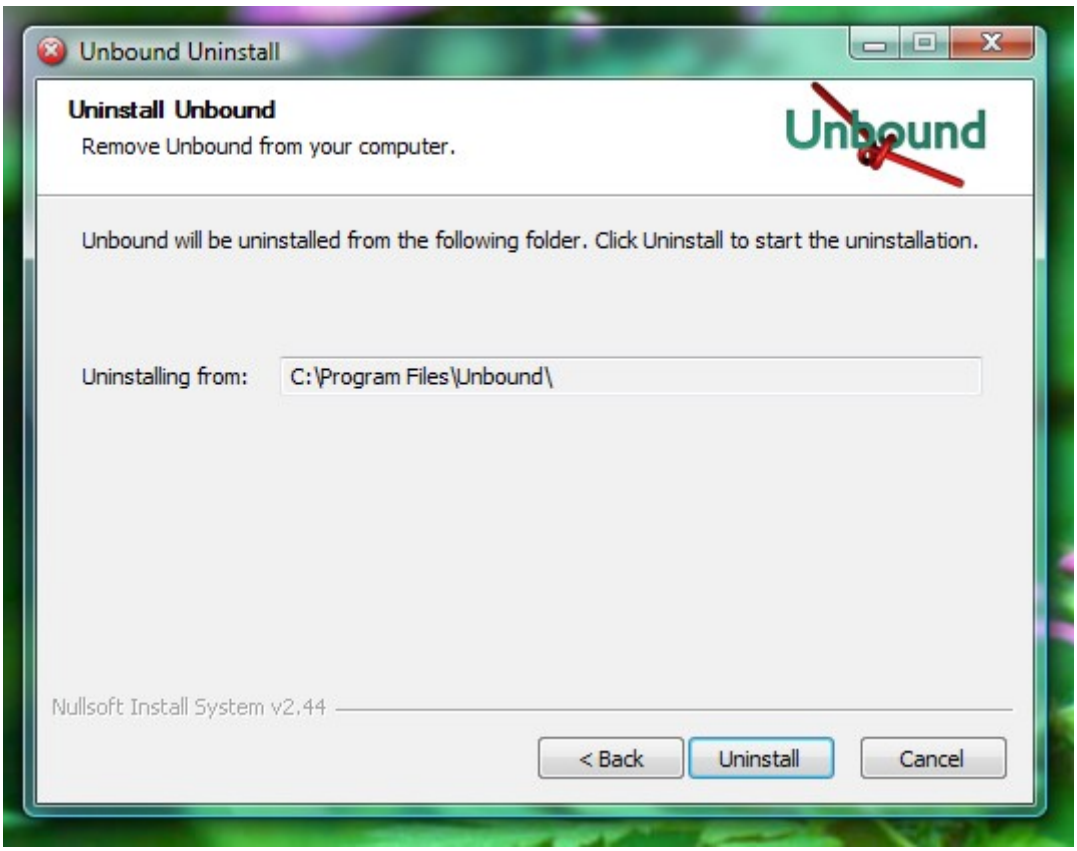
Uninstallation

If you installed start menu shortcuts, run the uninstaller from the menu. Otherwise, press the Remove button for Unbound in the Control Panels\Add Remove Software. On Vista you have to give administrator permission.

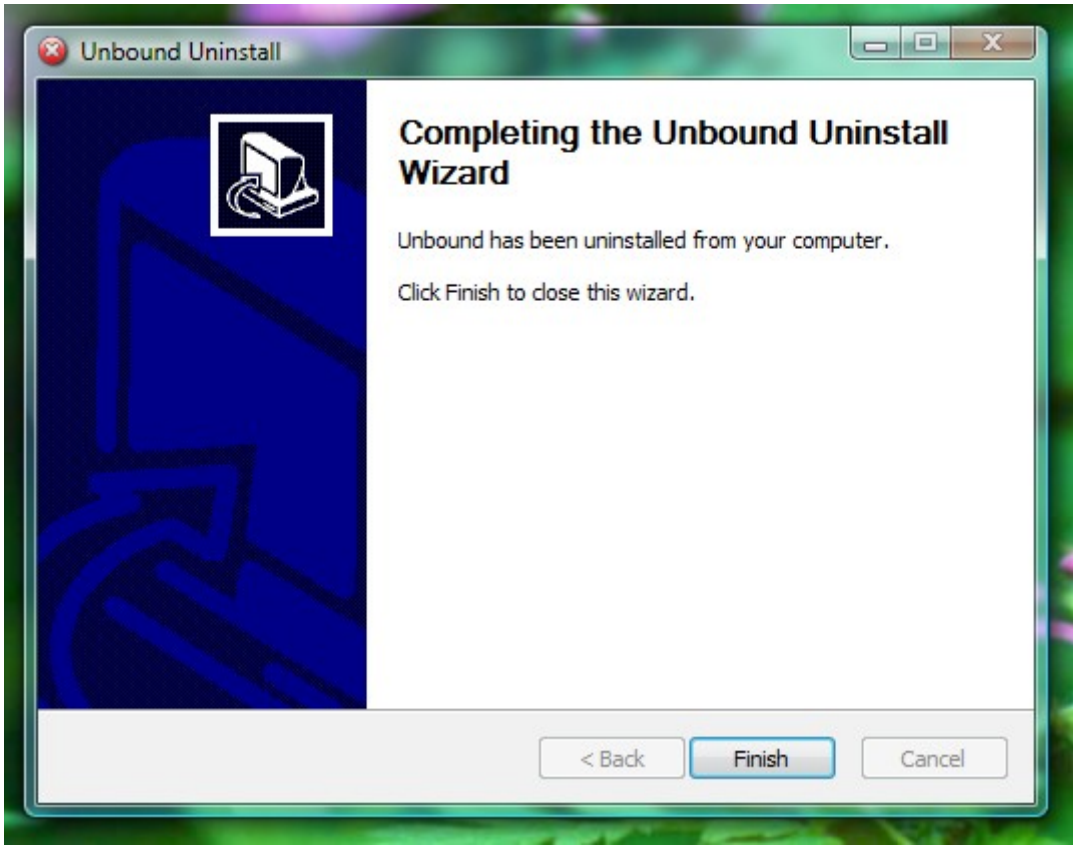
If unbound is running, the service is stopped before uninstall. The uninstaller starts like this:



The location is checked:

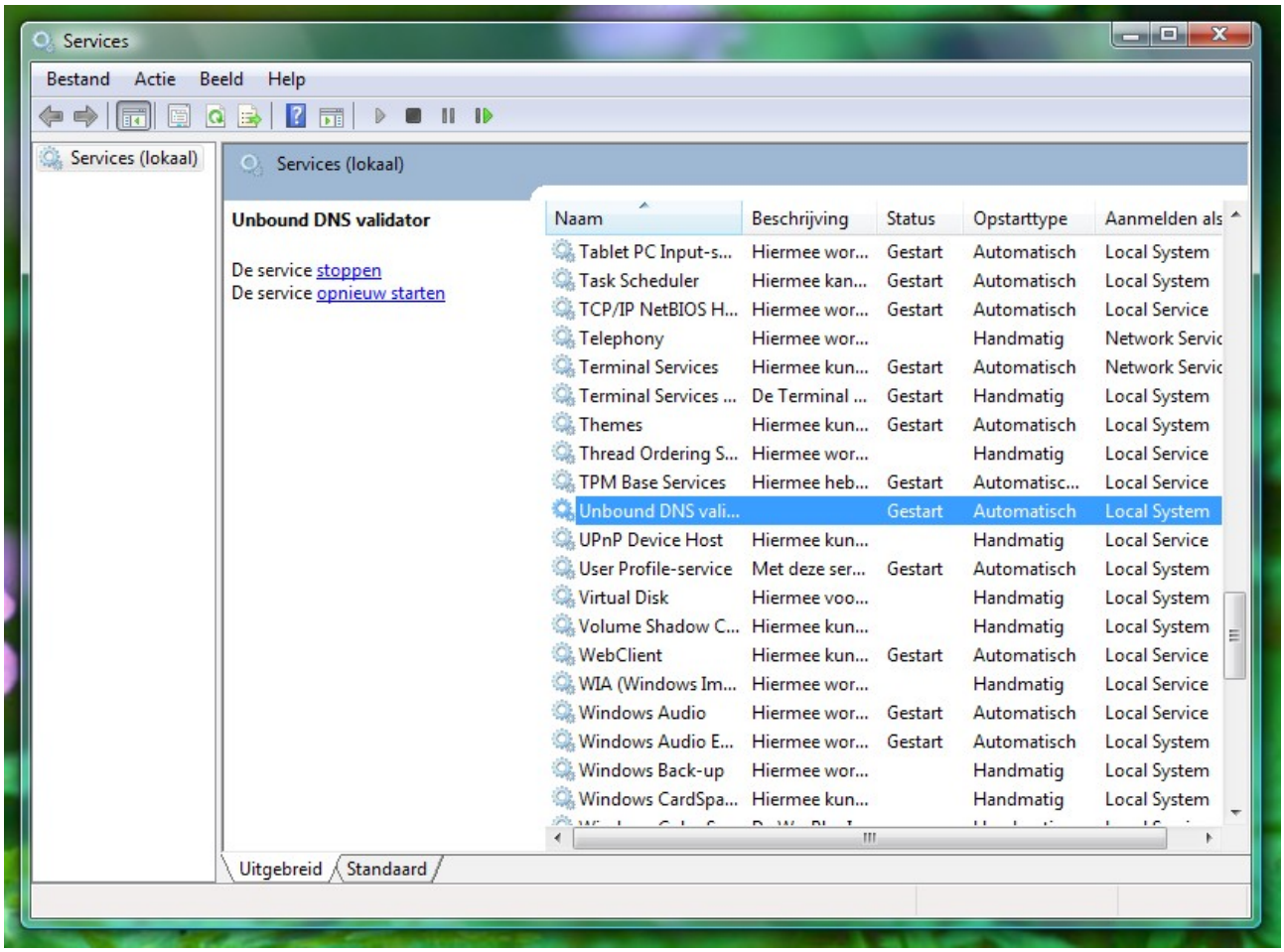


Files are removed and the uninstallation has been completed.

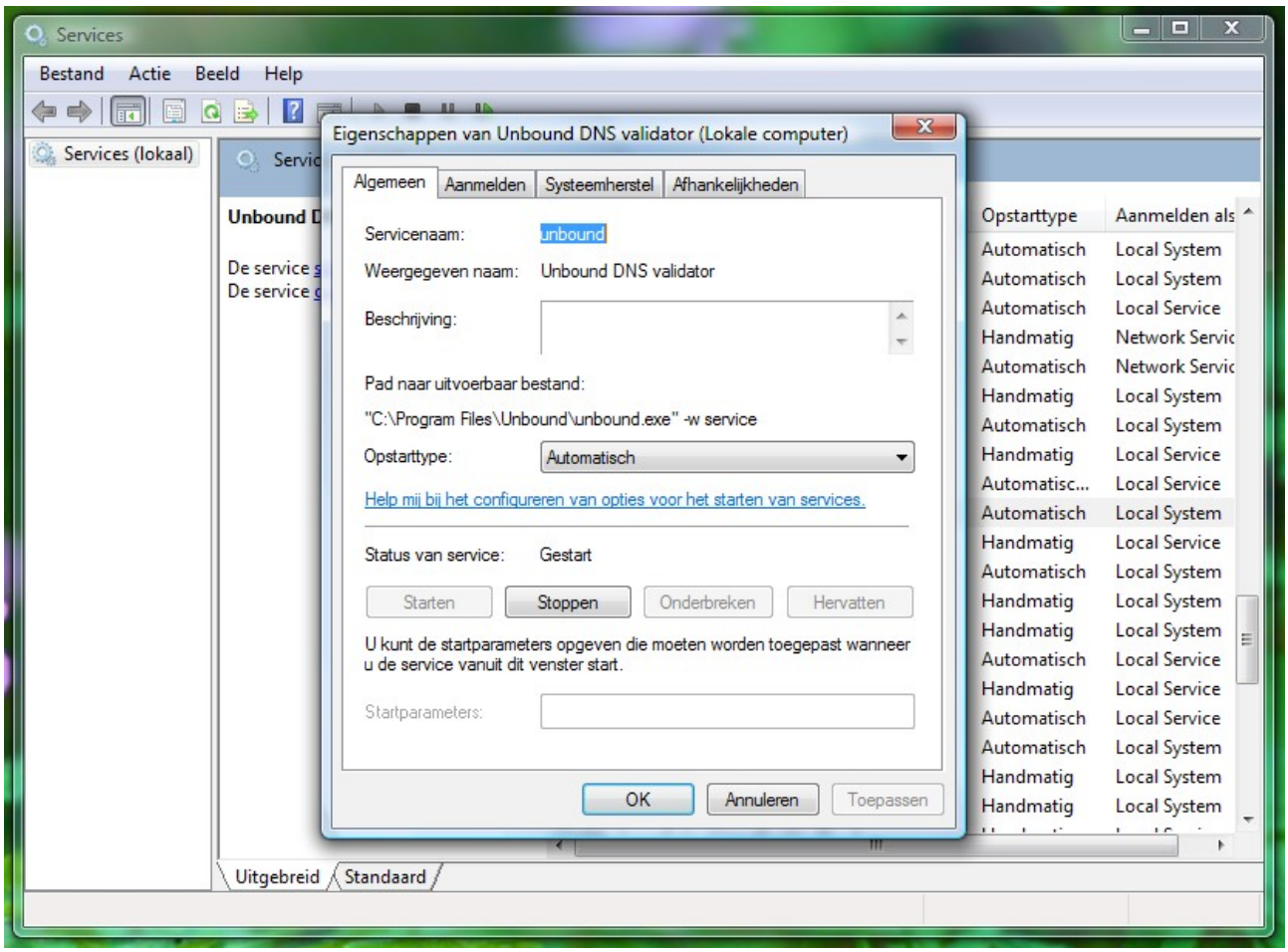


Check if it is running

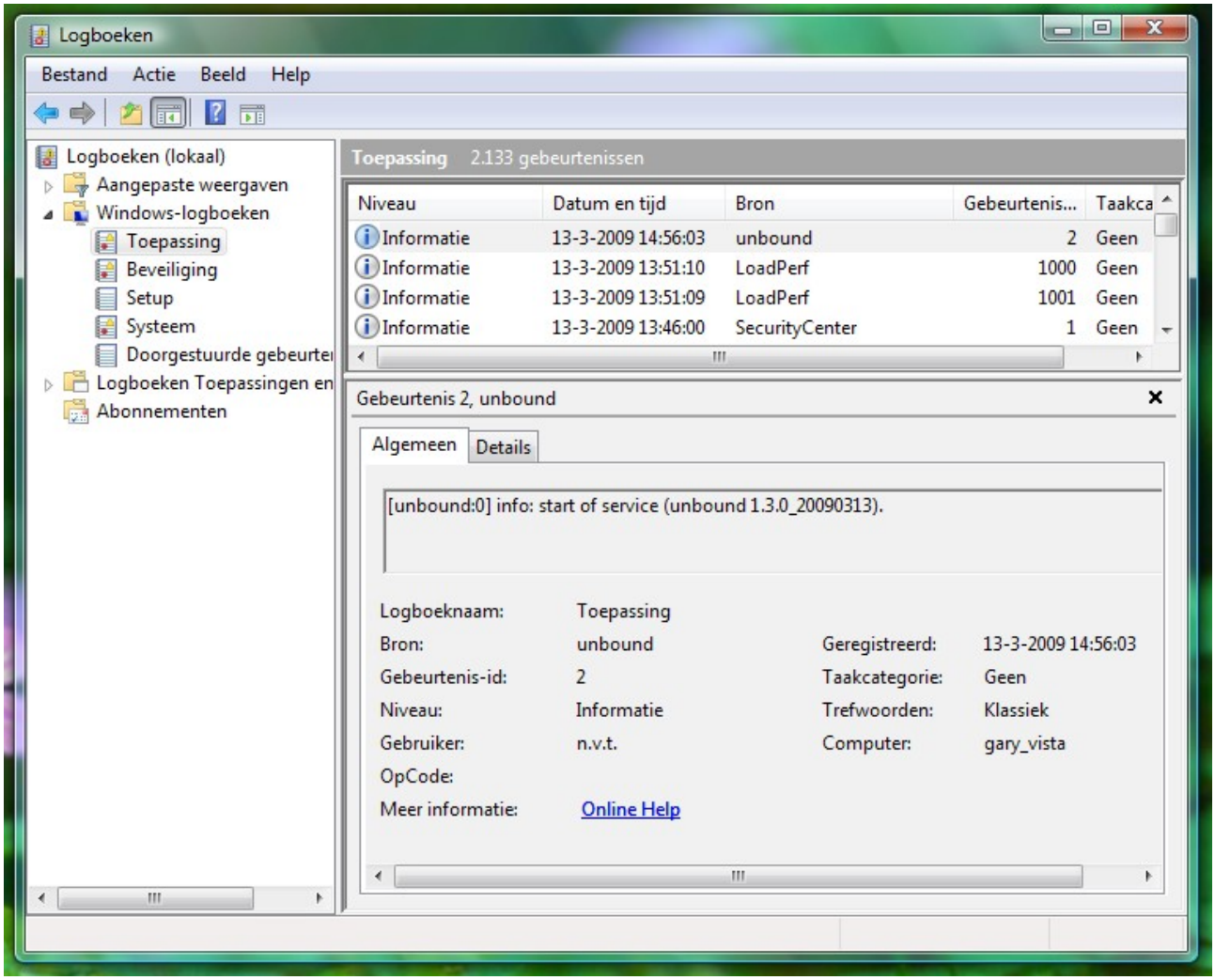
Open the Control Panels\System Administration\Services and select the unbound service:



The detailed properties look like this:


Services
Bestand Actie Beeld Help
Services (lokaal)
Eigenschappen van Unbound DNS validator (Lokale computer)
Algemeen Aanmelden Systeemherstel Afhankelijkheden
Servicenaam: unbound
Weergegeven naam: Unbound DNS validator
Beschrijving:
Pad naar uitvoerbaar bestand:
"C:\Program Files\Unbound\unbound.exe" -w service
Opstarttype: Automatisch
Help mij bij het configureren van opties voor het starten van services.
Status van service: Gestart
Starten Stoppen Onderbreken Hervatten
U kunt de startparameters opgeven die moeten worden toegepast wanneer u de service vanuit dit venster start.
Startparameters:
OK Annuleren Toepassen
Opstarttype Aanmelden als
Automatisch Local System
Automatisch Local System
Automatisch Local Service
Handmatig Network Servic
Automatisch Network Servic
Handmatig Local System
Automatisch Local System
Handmatig Local Service
Automatisc... Local Service
Automatisch Local System
Handmatig Local Service
Automatisch Local System
Handmatig Local System
Handmatig Local System
Automatisch Local Service
Handmatig Local Service
Automatisch Local Service
Automatisch Local System
Handmatig Local System
Handmatig Local System
Uitgebreid Standaard

Reading the error log



Open the Control Panel\System Administration\Log books. The unbound entries are in the Application log. Depending on the verbosity level, more or less log entries are shown. For help with errors see the documentation on the unbound website. The error 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.

The Items in the Start Menu

- unbound website: URL that opens the web browser to the http://unbound.net website.
- uninstall: performs uninstall of unbound.

Advanced – editing the config file

Unbound is configured with a config file. The default config file is C:\Program Files\Unbound\service.conf and the example.conf file shows the various configuration options. You can edit the config file 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. More information about configuration options can be found on the unbound website in the documentation section.

Advanced – tools installed

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

- LICENSE: this is a text file with the source code license.
- example.conf: file with example configuration options
- service.conf: configuration file used by default.
- unbound-website.url: link to the unbound website
- unbound.exe: the daemon, the 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, to use this you need to generate certificates on a unix machine, and put remote control into the configuration.
- Unbound-anchor: commandline tool that updates the root trust anchor. It is called by the main daemon before it starts if the registry says the root anchor is in use, the installer creates this registry entry if you select the root key option.
- unbound-service-install.exe: tool that when started registers unbound.exe as a service. Can be used to 'install' unbound lightweight. Called by the installer.
- unbound-service-remove.exe: tool that when started removes unbound.exe as a service. The reverse of unbound-service-install.exe. Called by the uninstaller.
- anchor-update.exe: tool to update trust anchor files. Called by the unbound service about once a day, one hour after starting.
- uninst.exe: the uninstaller.
- root.key: if you enabled the root anchor option, this file contains the public key for the root. It is loaded from the service.conf file and updated by unbound-anchor (at boot) and by unbound itself (during operation).

Advanced – registry entries

The following registry settings are affected by unbound HKLM\Sofware\Unbound:

- InstallLocation: The directory where unbound files reside.
- ConfigFile: The config file to use, service.conf by default.

- CronAction: The executable and its arguments started to update trust anchors. It is “” nowadays, but was used in older versions.
- 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).
- 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\ Unbound).

Setup as Local Server

The default install results in unbound performing service for localhost, running on 127.0.0.1. This section explains how to set up unbound to provide service for the local network.

Edit the config file, see earlier section on how to edit it, and add the permissions to serve the local network. Add these lines:

```
# this is a comment.
# provide Ipv4 service.
interface: 0.0.0.0
# provide ipv6 service, uncomment on Vista or if ipv6 is available.
#interface: ::0
# allow access by the local network.
access-control: 192.168.0.0/16 allow
# if you have Ipv6 enter your /64 as well and uncomment.
#access-control: 2001:db8::/64 allow
```

You also have to open the DNS port (port 53) in the firewall for incoming UDP and TCP traffic to the unbound server.