



Single Product Review



ESET NOD32 Antivirus Business Edition for Linux Desktop

Language: English

May 2011

Last revision: 2011-05-21

www.av-comparatives.org

commissioned by ESET



Table of Contents



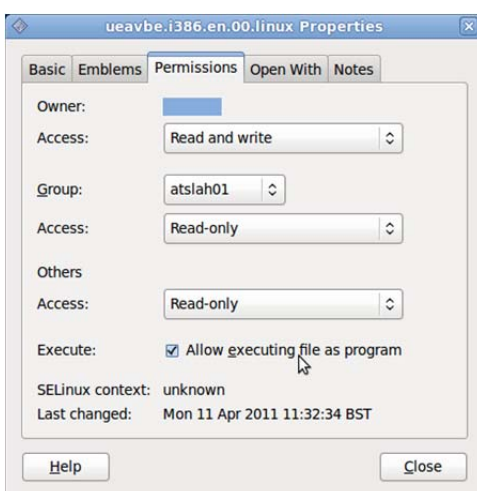
Introduction	3
Installation	3
Program Interface	4
Reaction to malware detection	6
Uninstalling the program	7
Remote Installation	7
Manual	8
Summary	8

Introduction

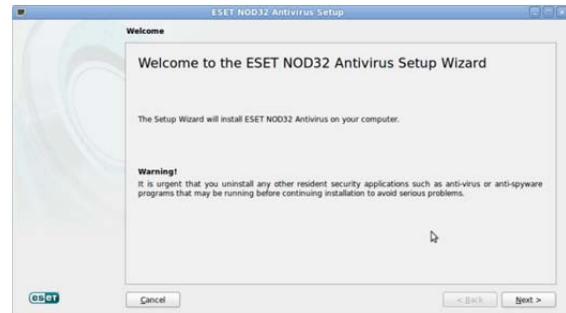
The growing availability of user-friendly Linux operating systems for desktop and laptop PCs, with business support packages available, means that anti-malware solutions for Linux are becoming more important. Security software for Linux is needed not only to protect the computer itself, but also to prevent malicious code aimed at other systems, such as Windows, being passed through the system. To counter such threats, ESET have released ESET NOD32 Antivirus Business Edition for Linux Desktop. For our review, we installed the 32-bit Business Edition, version 4.0.66.0, on 32-bit Ubuntu Desktop Edition version 10.04. ESET also make a Home Edition of the program, and both Home and Business versions come in 32 and 64-bit versions.

Installation

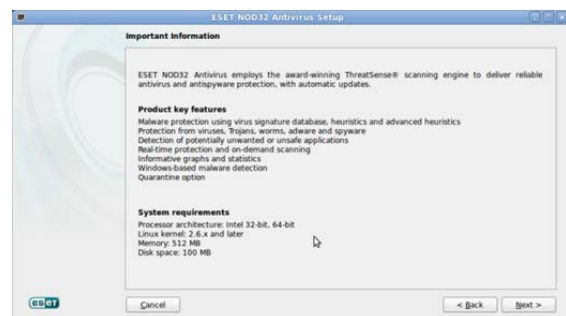
Windows users who are not yet familiar with Linux programs may need to consult the manual to install NOD32 for Linux from an installer downloaded from the Internet, which has a .linux extension. The Installation section of the manual explains that it is necessary to right-click the file, select Properties, Permissions, and tick the box entitled "Allow executing file as a program", as shown below:



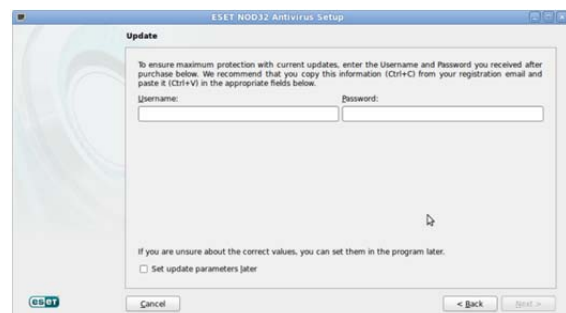
Once this has been done, double-clicking the .linux setup file starts the NOD32 installation wizard. The Welcome page of the wizard tells us to uninstall any existing antivirus software to avoid conflicts:



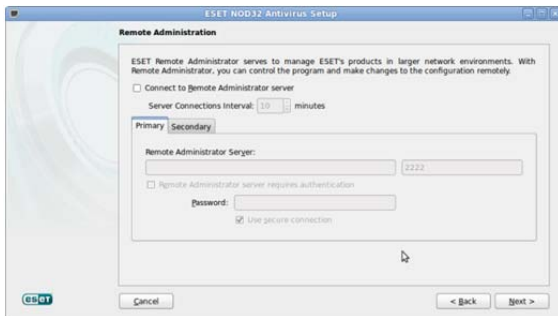
We are then asked if we want to install NOD32, or prepare it for remote installation (the latter is described in a section at the end of this report). We opt for the local installation. The next step gives information about the scope of NOD32, and the system requirements:



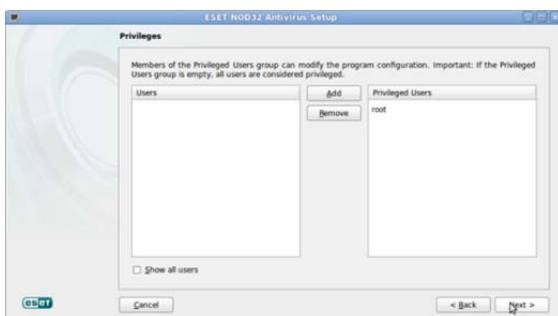
After this comes the obligatory acceptance of the licence agreement, followed by a choice of Typical or Custom installation; we chose Custom, to see the extent of the options available. The first step is to enter a username and password for the licence credentials:



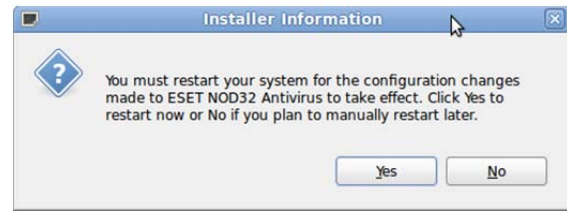
ESET's "Unilicense" model allows a key purchased for a Windows or Mac OS antivirus version of NOD32 to be used for the Linux version, and indeed the Windows licence key we entered worked perfectly for our Linux program. Setup then gives us the chance to enter details of a proxy server if used, and to connect to an ESET Remote Administrator server:



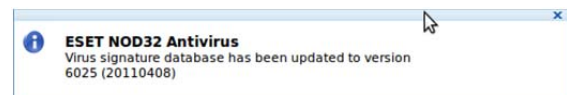
Next, we can enter "Privileged Users" who will have admin rights for configuring the program:



After this, the setup wizard asks whether Threat Sense should be enabled; this is ESET's method of gathering information about malware, via submission of suspicious files from the user's PC to the manufacturer, for analysis. The next step is a choice of whether NOD32 should detect "Potentially Unwanted Applications". After this, installation begins. The process completes very quickly, and the wizard invites us to complete the installation by restarting the computer:



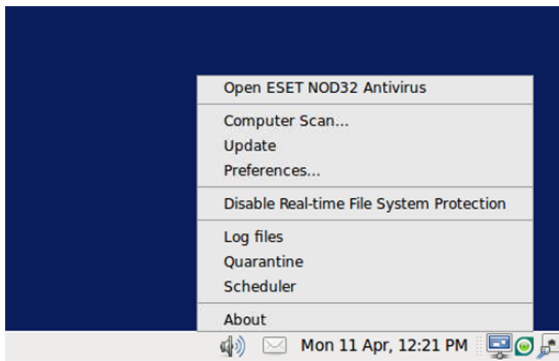
After rebooting and logging on again, a typical ESET small message box appears to inform us that virus signatures have been downloaded and the product is up to date:



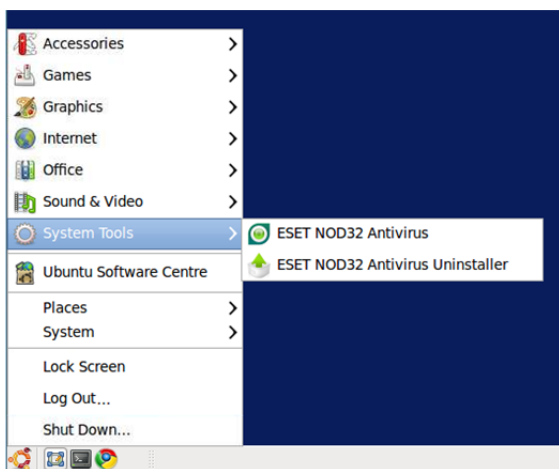
The program is now installed and has the latest signatures. Once the setup file had been correctly configured to start with a double click, we found the installation process to be simple and straightforward, with the sensible choice of a custom setup for advanced users. It would be plain sailing for anyone who is familiar with Windows installation programs, especially if they have ever installed NOD32 for Windows.

Program Interface

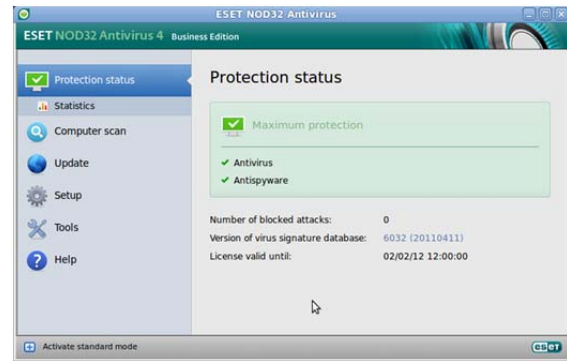
As with its Windows Version, ESET creates a system tray icon for NOD32 in Linux (please see screenshot below). In our Ubuntu 10.04 installation, we found that single-clicking the tray icon would open the NOD32 window; clicking again would then close it. Consequently, double-clicking the icon makes the program window appear for a second and then disappear! This may be confusing for some Windows users at first, but must be regarded as one of the things they have to get used to when using a Linux system. The NOD32 system tray icon can also be right-clicked to produce a useful context menu:



The ESET installer also creates menu items for NOD32 in the applications menu, System Tools folder:



The main program window will be instantly familiar to anyone who has used ESET NOD32 or Smart Security for Windows, being virtually identical to its Windows counterpart. For the benefit of those who are new to ESET programs, the layout of NOD32 for Linux is extremely simple and clear. The window opens on the Protection Status page, which shows “Maximum Protection” if real-time protection is working, signatures are up to date, and there are no other warnings. The same page shows the number of blocked attacks, version of the virus signature database, and the expiry date of the licence:



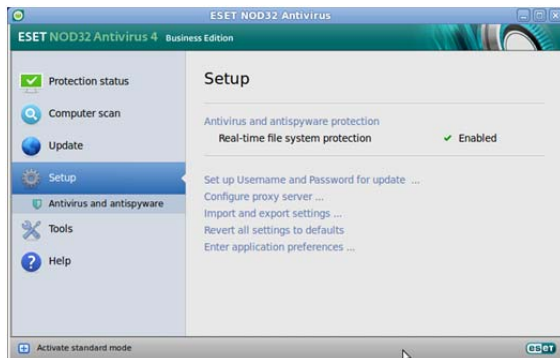
To see how the status page reacts when there is a problem, we switched off real-time protection. The status display immediately changed to “Maximum protection is not ensured” in red, with a link to start the real-time protection:



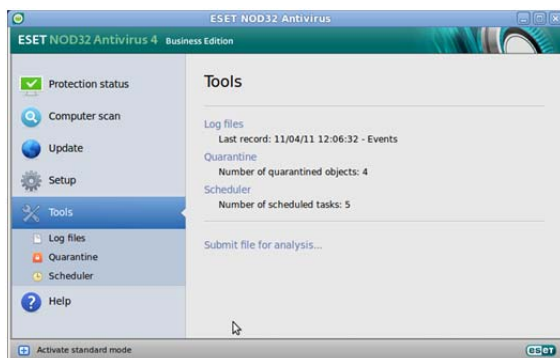
Clicking on the link immediately reactivated the protection.

The left-hand pane of the main window is a very simple menu bar, containing the menus Protection Status, Computer Scan, Update, Setup, Tools, and Help. Protection Status has the sub-menu Statistics, which shows a graphical display of the numbers of infected and cleaned objects. Computer Scan not surprisingly allows the user to scan the computer, with the options Smart Scan and Custom Scan, the latter giving the choice of disks and folders to be scanned. There is also a link to Scan Setup, i.e. more detailed scan options. Update enables the user to run a manual update of virus signatures, and displays the date and time of the last successful update, as well as the version number of the signature database last downloaded. This page also displays the licence key being used, and allows this to be changed via a link entitled “Username and Password setup”. Clicking on the Setup menu also allows the username and password for the

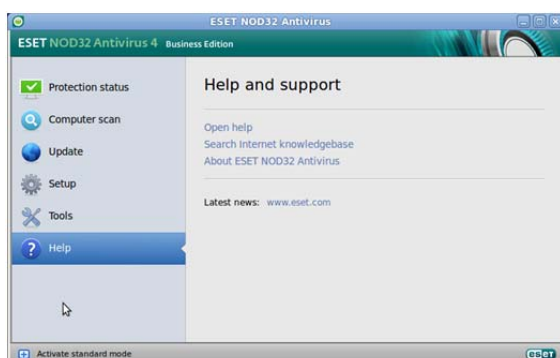
licence credentials to be changed, as well as allowing real-time protection to be disabled, and other options:



There is an Antivirus and Antispyware submenu, which allows configuration of real-time protection and scans. The Tools menu provides options for viewing log files, quarantined items, and scheduled tasks:

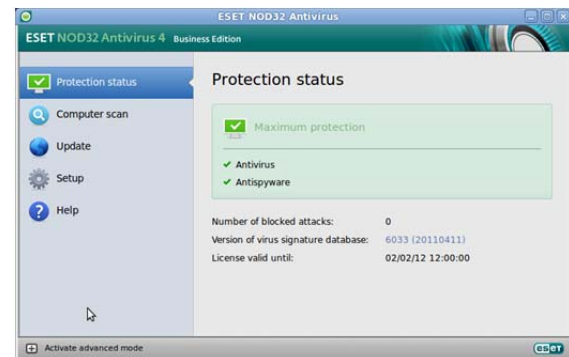


The Help page of the program has links to the html-based local help files, ESET's Internet knowledge base, and program information ("About"):



In the bottom left-hand corner of the window is a link entitled "Activate standard mode". Clicking on this switches to a simplified

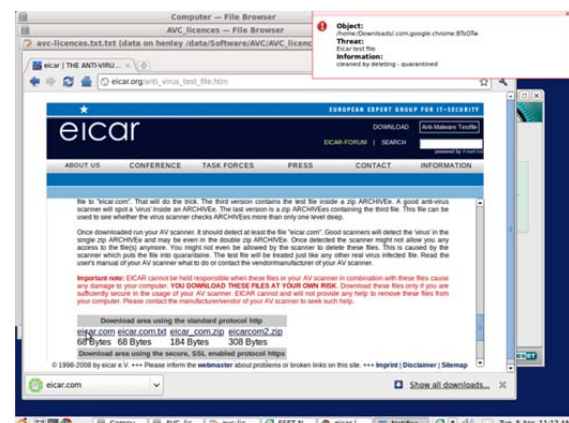
version of the interface, with the Tools menu and all of the submenus hidden. Standard Mode would be ideal for less experienced users.



We were pleased to see that when we adjusted the screen resolution of our test system to 640x480 pixels, the NOD32 program window resized itself, leaving all features fully accessible and useable, even in Advanced Mode. The program could thus be used comfortably on a netbook.

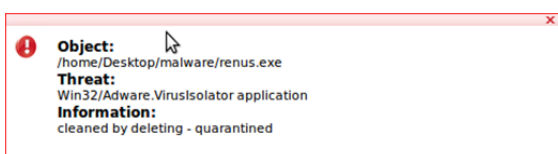
Reaction to malware detection

To see how antimalware programs for Windows react when a threat is discovered, we attempt to download the EICAR test file, a harmless string of characters which antivirus programs are normally programmed to recognise as a virus, for testing purposes. We tried this test with NOD32 for Linux, and noted that it reacted exactly as its Windows counterpart would, by quarantining the file and displaying a pop-up message to this effect:



The principal function of an antivirus program for Linux must of course be to protect against malware specifically designed to attack Linux systems. However, an antivirus program which only stopped Linux-specific malware would enable the Linux system to act as a conduit for passing on the much more common Windows malware, e.g. if the user were to forward an email containing a Windows-specific Trojan. Clearly, a responsible manufacturer of Linux antivirus software would enable the program to recognise and remove Windows malware as well, even though it presented no threat to the system in question.

In the NOD32 for Linux manual, ESET state “ESET NOD32 Antivirus includes the ability to deflect Windows threats, protecting Linux users as they interact with Windows users and vice versa”. In a very simple experiment to see how NOD32 for Linux would react to Windows malware, we copied 5 executable files from Windows rogue antivirus programs, which are detected by NOD32 for Windows, onto our Linux test machine. We were pleased to note that ESET’s Linux program detected and quarantined all of these files, just as the Windows version would have done:



This very simple test MUST NOT be taken as any indication of the overall ability of NOD32 for Linux to detect and remove Windows malware, but would support ESET’s claim that it has not limited its virus signatures for its Linux program to Linux-specific malware.

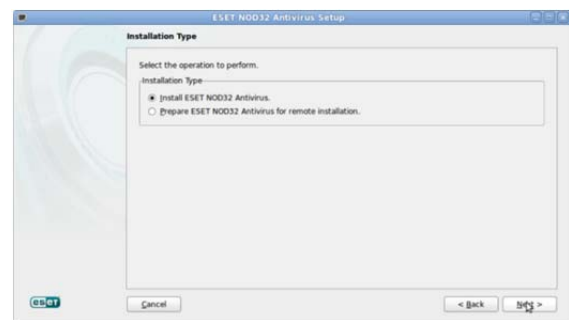
Uninstalling the program

ESET NOD32 for Linux is very simple to remove from the computer. In the program’s folder in the applications menu there is a link to the uninstaller, which quickly and easily removes

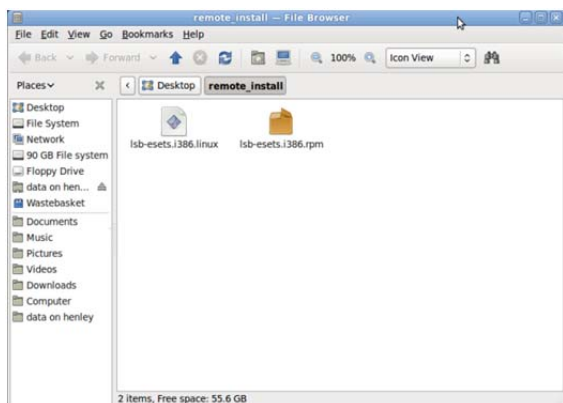
the program in just a few clicks. There is the opportunity to submit feedback to ESET as to why you are uninstalling the program, but this is optional.

Remote Installation

As it is intended for use in business networks, the Business Edition of NOD32 for Linux has the ability to create a remote installation package, which the system administrator can install to multiple machines over the network, e.g. by scripting. Creating this package is very simple, and involves running the setup program again. One of the options listed at the beginning of the wizard is “Prepare ESET NOD32 Antivirus for remote Installation”:



After selecting this option, much of the setup wizard is identical to the installation of the program on the local machine. There are pages for the licence agreement, Typical or Custom installation, username/password, and Threat Sense. The final page asks the administrator to select a folder in which the package should be created. Opening this folder on completion of the wizard shows the installation files:



Manual

ESET NOD32 for Linux includes a detailed 23-page manual which can be downloaded in .pdf format. This has 6 sections: an introduction to the program and system requirements; an installation guide; a beginners' guide to the Standard Mode interface; working with the program, i.e. performing essential tasks such as scanning and rectifying status problems; advanced user options, useful for administrators of business networks; and a glossary.

The installation guide covers configuring the downloaded setup file, and preparation/installation of the remote installer package. The glossary is a very well-written, clear guide to the major types of malware and what to do if they are detected on your computer. This is something every computer user should read, regardless of which operating system or security software they use. The manual as a whole is informative and easy to read.

Summary

With NOD32 for Linux, ESET have retained all the excellent features of the Windows version. The program is easy to install, and it provides a clear, simple interface for beginners, with one-click access to more advanced options for advanced users. It is apparent that this Linux version not only protects the system against Linux-specific malware, but also detects Windows malware, thus preventing attacks on other systems being passed through unchallenged.