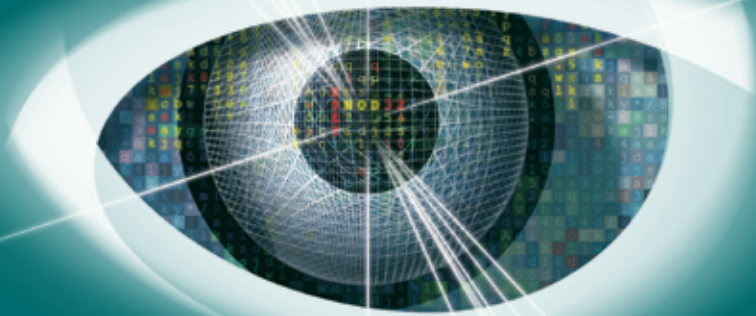




# NOD 32<sup>®</sup>

antivirus system



*Remote Administrator 1.0.14  
and LAN Update Server 2.7*

## **Installation Guide**

NOD32 Version 2.7 Includes Windows Vista and 64-bit protection

---

**Proactive protection**  
against Viruses, Spyware,  
Worms, Trojans, Rootkits,  
Adware and Phishing

**Best Detection**  
**Fastest Performance**  
**Minimal Resource**  
**Utilization**

**Copyright © 1997 – 2007 ESET LLC. All rights reserved.**

No part of this document may be reproduced or transmitted in any form or by any means electronic or mechanical, for any purpose without the express written permission of Eset LLC. Information in this document is subject to change without prior notice.

Certain names of program products and company names used in this document might be registered trademarks or trademarks owned by other entities.

Eset, NOD32 and AMON are trademarks of Eset.

Microsoft and Windows are registered trademarks of Microsoft Corporation.

Version 2 Singapore Pte Limited  
371 Beach Road,  
Keypoint Building #20-07  
Singapore 199597  
<http://www.nod32.com.sg>

**For Sales and Technical Support (Singapore):**

Tel: (65) - 6296 4268

Fax: (65) - 6296 4252

Online purchase: <http://www.nod32.com.sg/shop>

**Sales email:**

[sales@nod32.com.sg](mailto:sales@nod32.com.sg)

**Technical Support:**

<http://www.nod32.com.sg/support>

Then by clicking on your country's name, you can locate the support details closest to you.

This guide is frequently updated to reflect changes in the product. The latest version can always be found at

<http://download1.eset.com/manuals/nod32raman.pdf>

This guide was prepared for NOD32 Remote Administrator Server, Remote Administrator Console version 1.0.14 and the NOD32 LAN Update Server version for Windows, Version 2.7 (December 2006)

	Page
Contents	3
Introduction	4
Minimum System Requirements	5
Section I: Overview	6
What you can do with Remote Administrator	7
Summary of features	8
Section 2: Installation for an office network	9
Installing RAS and RAC	10
Section 3: Running Remote Administrator Console	14
Connecting to server	15
Section 4: Configuration Editor	17
Overview	18
Section 5: Create a package	33
Installation package	34
Section 6: Remote Installation of NOD32	35
Points to watch out for	36
Push installation	37
Export to logon script	39
Export via email	41
Manual installation	42
Section 7: Use of Tasks	43
Creating tasks	44
On-Demand Scan Task	46
Update Now Task	48
Section 8: More Detailed Information	49
Remote Install in detail	50
The file nod32installer.exe	51
Clients window	52
Context menu options	54
Context menu examples	55
Alert log window	56
Event log window	56
Scan log window	56
Tasks window	56
Reports window	57
License key (nod32.lic)	59
RAC connection to RAS + settings	59
RAC server options setup	61
Use RAC more efficiently	63
Section 9: Possible Problems & Error Codes	65
Error messages	66
Section 10: Installation in a multi-site network	70
Installation instructions	71
Section 11: Installation in a small network	74
Installation instructions	75
Creating a Mirror	76
Creating a customized installation	78
Section 12: Additional information	82
Command line parameters	83

## Introduction

Congratulations, you have just purchased NOD32 Enterprise Edition incorporating Eset's Remote Administrator Server & Console, which will help you manage the most advanced antivirus solution available in a network environment.

The following information will help you to get a better understanding of the many features of NOD32 Remote Administrator, so that you get the best protection and administration possible.

**NOD32 is more than just a virus scanner** – being able to scan for known viruses is the bare minimum that should be expected from an anti-virus product, so it should be reassuring to know that NOD32 not only does this faster, and more reliably than other products, but that it also has an excellent track record in discovering new threats. In addition, version 2.7 includes detection for adware, spyware and riskware aswell as rootkit detection with its Anti-Stealth technology. With NOD32 you can be sure you have the most advanced and comprehensive virus protection possible.

## Minimum System Requirements

Please make sure that the computer on which you plan to install NOD32 meets the minimum system requirements for the program to run:

Operating system	CPU	RAM
Windows 98/ME	133 MHz/150 MHz	32 MB
Windows NT4/2000	133 MHz	32 MB/64 MB
Windows XP/2003/XP 64 or 32-bit	300 MHz	128 MB
Windows Vista	800 MHz	512 MB

Disk Space: 30MB free disk space

Graphics: VGA video card. (SVGA 800x600 recommended)



You must only install ONE anti-virus On-Access scanner at one time (a scanner that is always running while your PC is switched on); otherwise you could cause serious system instability.

If you are installing NOD32 with another anti-virus program, please make sure you do not enable both On-Access scanners at once.

**If another anti-virus program has previously been installed on your computer**, its scanner may interfere with NOD32. Usually resident scanners will display an icon in the system tray (the area of the taskbar near the clock). We recommend removing any other antivirus software, including older versions of NOD32, before installing NOD32 Version 2.7, to avoid the possibility of serious problems

Version 2.7 may be installed over your existing NOD32 if it is version 2 or higher, however, if any problems were encountered, a clean installation is recommended.

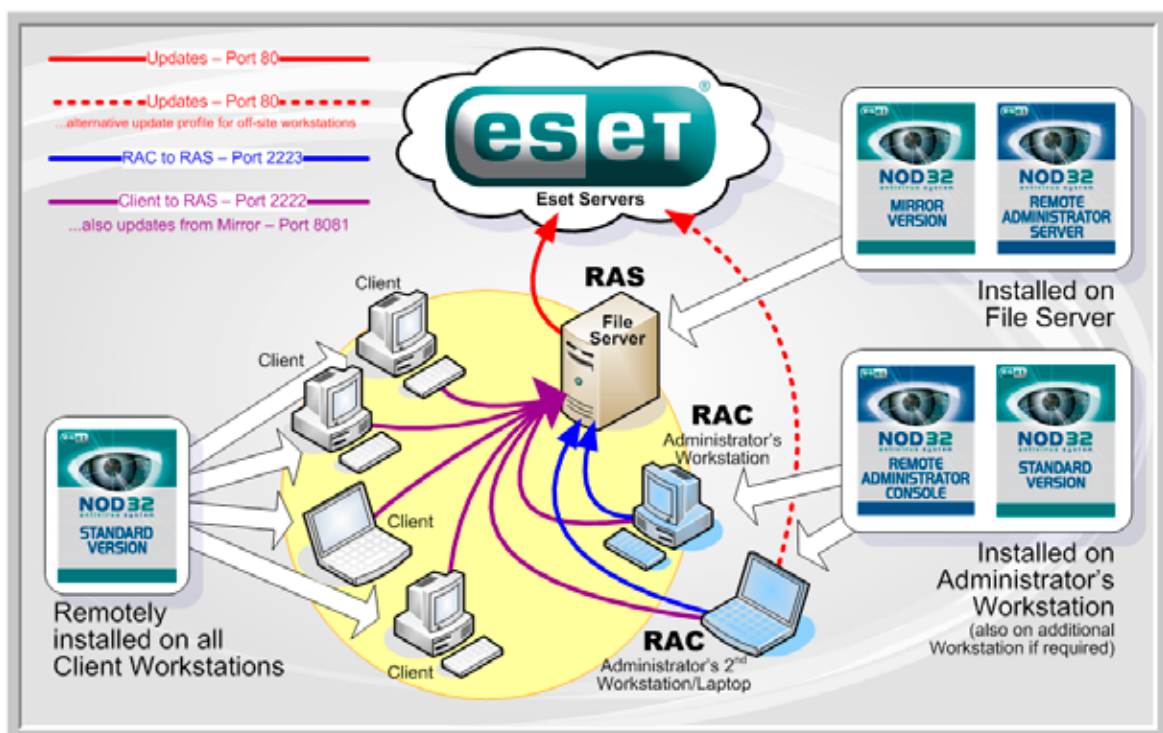
# Overview

## Overview of what you can do with the Enterprise Edition of Remote Administrator

This is the complete package for any medium to large sized business. It comprises of the standard NOD32 antivirus for workstations, the LAN Update Server (Mirror) version which will receive all updates & upgrades from Eset, the Remote Administrator Server which will run on the company's server and the Remote Administrator Console where you can administrate the whole setup.

This will mean that you only have to download updates to your server, thus reducing internet traffic. Naturally, your server should be in operation during the entire working day and should have an NT-based operating system (NT4/2000/XP/2003) but doesn't have to be a 'server' operating system. The updates will be stored there and then picked up by the workstations in your network. So the server acts as a 'mirror' to your clients and is referred to as such in the setup.

Using NOD32 Remote Administrator Console (RAC), the administrator can get a global overview of the NOD32 antivirus system activity on network workstations, and can receive information about threats, or other problems, via email or Windows Messenger. The information retrieved from the workstations is stored centrally on the server (NOD32 Remote Administrator – RAS) which the administrator can access via RAC from his/her own workstation or laptop. The communication takes place both ways and thus the administrator can immediately react to fresh situations, and assign tasks to the relevant NOD32 on client workstations.



## Important features of NOD32 Remote Administrator:

NOD32 Remote Administrator is a powerful tool that enables an administrator to manage large installations of the NOD32 antivirus system in large corporate networks. It consists of two modules - NOD32 RA Server (RAS) and NOD32 RA Console (RAC).

### FEATURES

- ▶ Quick overview of your network security situation
- ▶ Comprehensive statistics in an intuitive graphical form
- ▶ Enables virus scan on remote disks
- ▶ Remote NOD32 client configuration file editing on chosen workstations
- ▶ Remote installation/uninstall of NOD32 antivirus system
- ▶ Localization of unprotected computers in network



# Installation

## for an office network

## Installation instructions for a typical office network setup.

When you received your Enterprise Edition license email, you will have seen the Username and Password required to access the Eset servers for updates and there will have been a .lic key also attached (nod32.lic). This key is specific for your RAS and determines how many clients you can connect to your server and the expiry date of the license.

- ▶ Save the nod32.lic key you received as an attachment with the email from Eset to the desktop for the time being. (Note: do **NOT** use a web based email program to download this attachment. eg: Outlook Web Access, because this will corrupt the key).
- ▶ **AFTER** installation is complete, you should move the **nod32.lic** key to **C:\Program Files\ESET\RA\Server** directory and re-start the RAS service.

Here are the basic, recommended steps to take when setting up Enterprise Edition for NOD32:

## Install Remote Administrator Server (RAS)

- ▶ Using your Username and Password, download and install NOD32 Remote Administrator Server (RAS) onto your server (<http://www.eset.com/download/balance.php?dir=/download/ra/rasrvnten.exe>). The product must be installed on an MS Windows NT based operating system (NT4, 2000, XP, 2003). RAS is installed by running the file rasrvnten.exe.
- ▶ During installation, the program will ask for the location of the license key, ie: the file called nod32.lic, which contains information about its owner, its expiry date as well as about the number of users, for which the RAS was purchased. Alternatively, you can copy the key later into the directory C:\Program Files\Eset\RA\Server (it is activated after restarting the NOD32 Remote Administration Server service). Later on, after connecting to the server from the console (RAC), Information included in the key can be seen in Help > About NOD32 Remote Administrator Console.
- ▶ During the 'Expert' installation, the name of the server, under which workstations in the network recognize it, is required. If not stated otherwise, the server is represented using the name of the machine/ server where RAS is being installed.

Please be careful when entering the name of the server. This name is used by nod32installer, providing remote installation of NOD32 on workstations. If RAS was not visible under this name, the remote installation could fail.


We recommend entering the DNS name of the server.

- ▶ RAS is installed as a service. Note: The service is installed, but not started, during RAS installation. You can control the service manually using these commands:
  - ◆ “c:\program files\eset\ra\server\nod32ra.exe” /installservice
  - ◆ “c:\program files\eset\ra\server\nod32ra.exe” /removeservice
- ▶ You can stop and start the service by going to Start > Control Panel > Administrative Tools > Services > NOD32 Remote Administrator Server > ‘Start the service’,

## Install Remote Administrator Console (RAC)

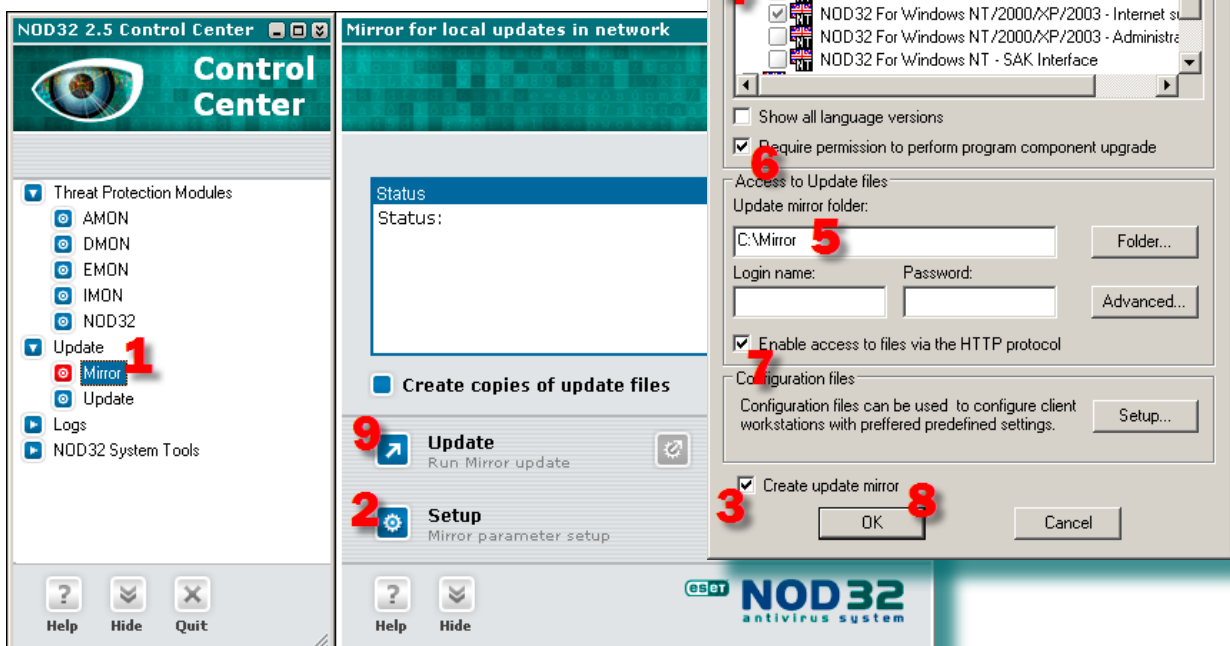
- ▶ Using your Username and Password, download and install NOD32 Remote Administrator Console (RAC) onto your server plus any machine that you want to administrate your clients from. ie: your workstation or laptop as well as the server if you wish. (<http://www.eset.com/download/balance.php?dir=/download/ra/raconsnten.exe>)

## Install NOD32 LAN Update Server

- ▶ Using your Username and Password, download and install NOD32 LAN Update Server (Mirror) version onto your server (<http://www.eset.com/download/balance.php?dir=/download/win/v2ad/ndntenad.exe>). Its virus signature database will form the basis of a so called Mirror for the client workstations.
- ▶ For detailed instructions on downloading and installing NOD32 LAN Update Server (Mirror) version (which is the same as installing the Standard, single-user version) please click here: <http://download1.eset.com/manuals/StandardInstallGuide.pdf>. The IMON module should **not** be running on the server. In fact, the only module that is required on a server is AMON.
- ▶ If you wish, **you may defer the restart until all other installations are completed**. Once installed and you have rebooted your server, NOD32 will automatically update. You should then create a Mirror on the server. Click this icon once  in the system tray, which will open the Control Center.

## Creating a Mirror

1. Click 'Mirror'
2. Click 'Setup'
3. Check 'Create update mirror'
4. Check the 'Available versions' you require for your network. ie: WinNT machines and/or Win9x machines. All versions that will be running on the workstations should be checked.
5. Setup a path to the Mirror on your server. You can choose to create this folder anywhere you wish, but it's recommended to keep the path reasonably short (ie: C:\Mirror or C:\NOD32\Mirror or C:\Program Files\Eset\Mirror)
6. Check 'Require permission to perform program component upgrade'. Besides the virus signatures database update, a license also includes program updates – program component upgrades, which require a restart of the operating system and bring a lot of new features and improvements to NOD32 (it is an upgrade to a completely new version, eg: from 2.5 to 2.7). Choose this to ensure that the program component upgrade will **not** be applied to a local update server immediately it is available on the servers of the Eset company. NOD32 on the workstations will remain in the current version, and the workstations will only accept virus signatures updates from the mirror. It is up to the user to consider this option, especially since before updating all workstations in the network, the new version may be tested in a detached network dedicated to testing.
7. Check 'Enable access to files via the HTTP protocol'
8. Click 'OK'
9. Click the 'Update' button to update your newly created Mirror, since there may be more components mirrored than are used by the local system.




- ▶ If you would prefer a Shared Folder Mirror path, when entering it, please use the UNC path. Let's assume that the shared folder is named NOD32NET and is located on the MAIN server. Then enter the path in this form: **\\MAIN\NOD32NET**
- ▶ In this case, a Logon name and Password should be entered that the clients will use to access the Mirror on the server.

## (Optional) Download NOD32 for Windows, standard, single-user version(s)

- ▶ RAS has **both** of the installers (Windows NT/2000/2003/XP/Vista and Windows 95/98/ME) embedded into the program but because the contents of RAS is not updated as frequently on the Eset website as the standard version of NOD32, you may wish to download the very latest versions to be installed on your client machines as described above, which will save pushing a possible Program Component Upgrade at some point after the initial installation on the client workstations.
- ▶ Using your Username and Password, **download only** NOD32 for Windows NT/2000/2003/XP/Vista 32-bit/64-bit onto your server (<http://www.eset.com/download/balance.php?dir=/download/win/v2st/ndntenst.exe>) assuming you have machines running these operating systems in your network.
- ▶ Using your Username and Password, **download only** NOD32 for Windows 95/98/ME onto your server (<http://www.eset.com/download/balance.php?dir=/download/win/v2st/nd98enst.exe>) assuming you also have machines running these operating systems in your network. If not, there's no need to download this version.
- ▶ **SAVE** these 2 installers into a new folder and call it **NOD32 Installers**, for example, and place the folder in **C:\Program Files\Eset\RA\Server**, or wherever you choose on the server. It is not necessary to install the standard, single-user version of NOD32 at this point.
- ▶ The initial downloading and installing of components is now complete.

# Running RAC

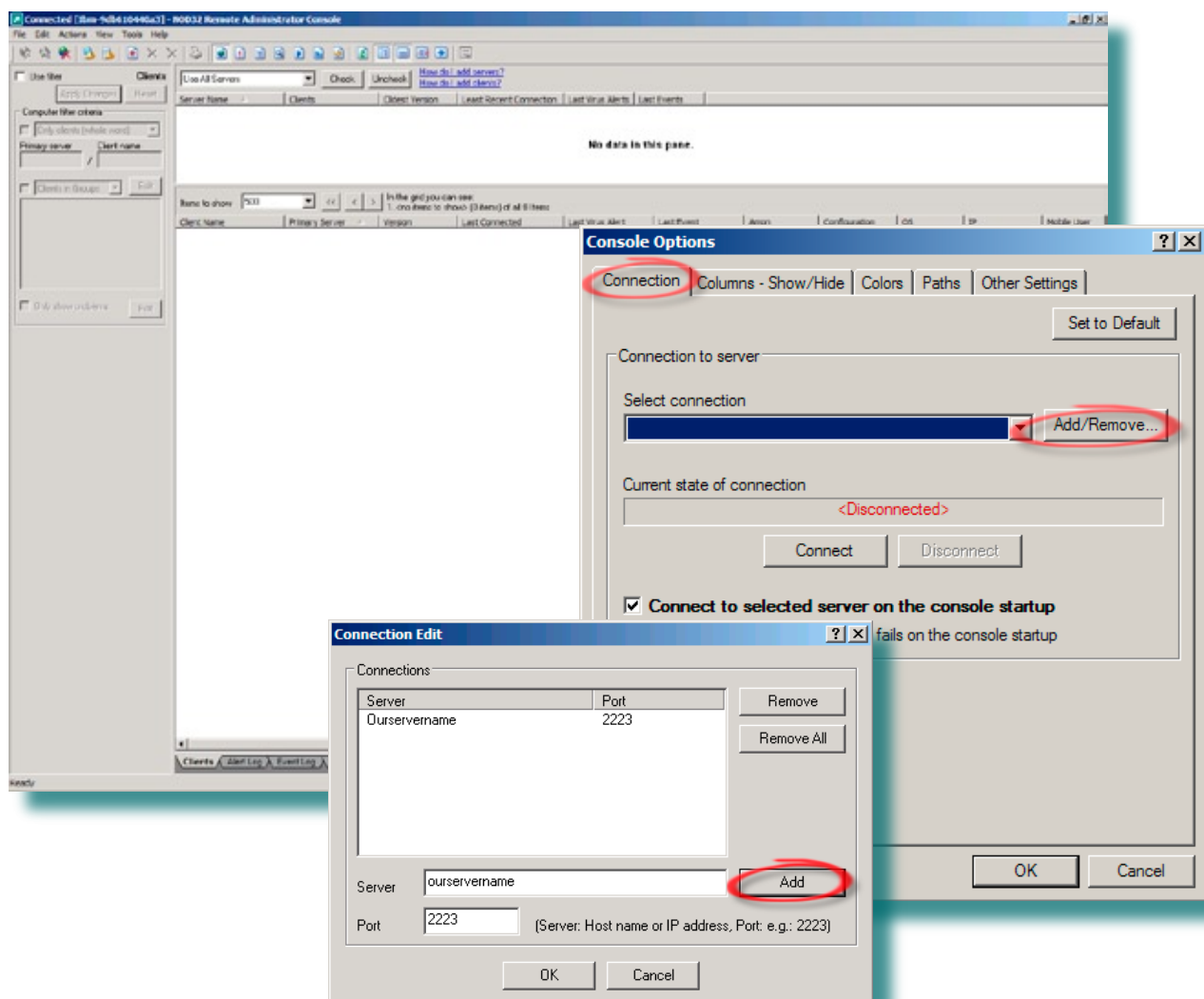
## Setting up RAC connection to the server.

- ▶ Run RAC by double-clicking on this icon  on the desktop of your workstation or laptop.

NOD32 Remote  
Administrator Console

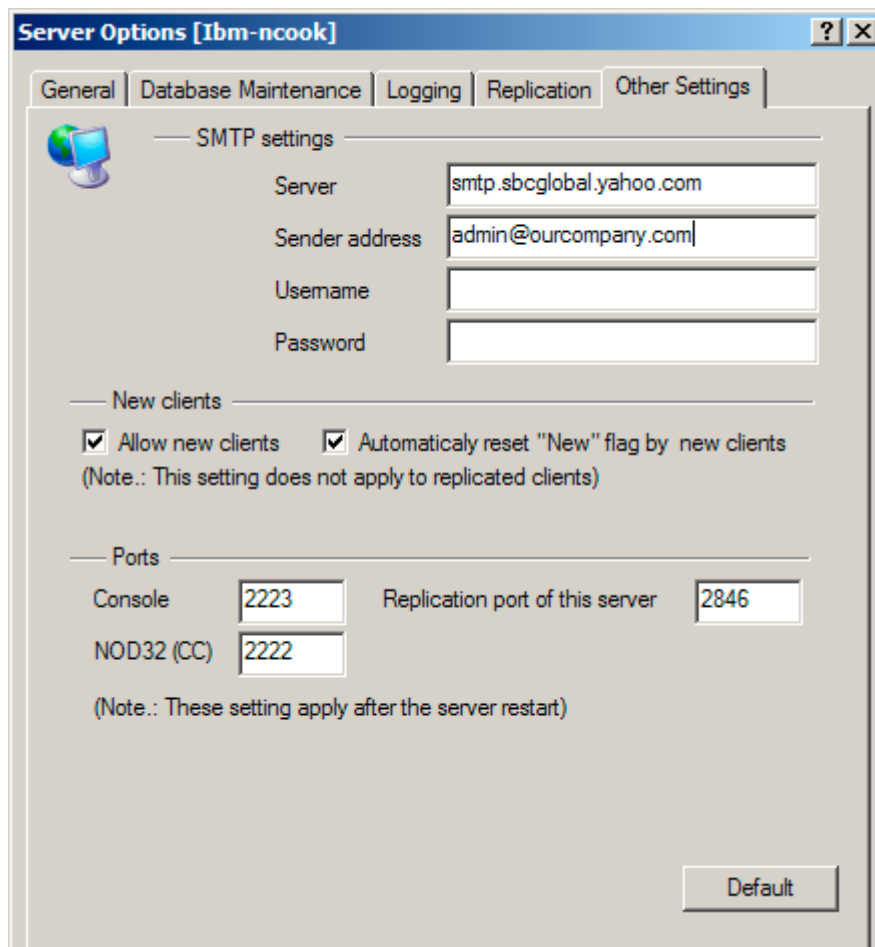
Note: No clients will appear yet, unless you have already manually installed NOD32 onto some workstations and configured them for Remote Administration via their Control Center(s).

- ▶ Go to Tools ---> Console options ---> Connection ---> Add/Remove, and enter the DNS name of your server (You can use the IP address instead but if that ever changed in the future, it might cause a problem) ---> click OK.



- ▶ From the 'Select Connection' box, choose the server name you've just added.
- ▶ Press 'Connect'.
- ▶ In the 'Current state of connection' window, you should see the name of the server. If true, press OK. Note: The server will not show up in the upper section of the RAC until it has at least one client connected.

- ▶ The attribute **Primary Server** denotes the name of the server with RAS installed, to which the remote client is connected via NOD32 Control Center. If there is another server showing other than the one which the administrator is currently connected to, then it is a result of replication.
- ▶ You may add a connection via SMTP server also if you have a mail server address and you wish to be contacted via email from your clients about alerts, etc. or you wish to install on some clients via email: Tools ---> Server Options ---> Other Settings tab.





# Configuration Editor

## Overview of the Configuration Editor

If you're already familiar with the standard version of NOD32 for Windows, you'll know that the program has a vast array of options when it comes to scanning, updating, scheduling and reporting infiltrations.

The Configuration Editor does exactly the same job but is designed for you, the administrator of your network, to create a universal set, or various sets, of parameters associated with the installation package(s) you will soon create.

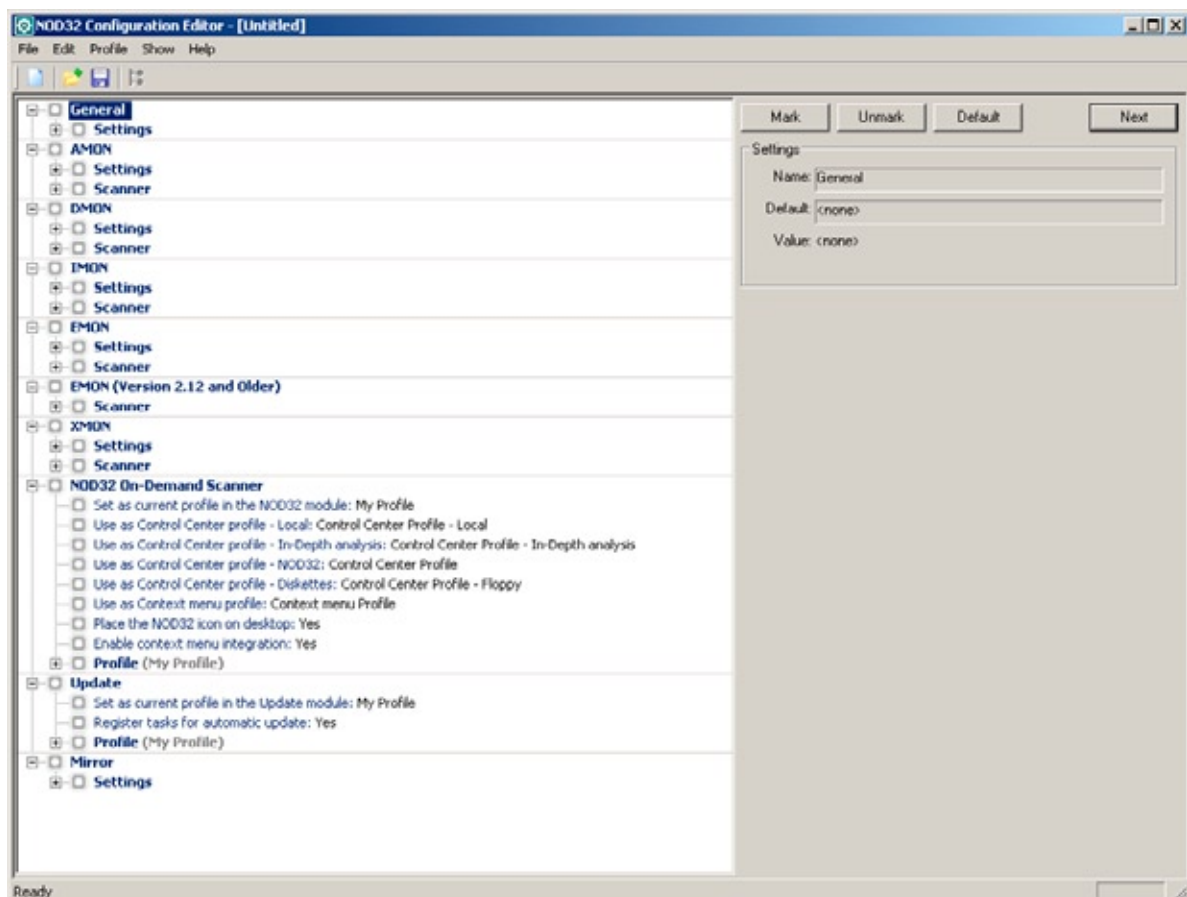
The Configuration will be saved as an .xml file. You can set this up before or during the creation of your installation package. Here are 3 ways to do this:

- 1.** Start ---> Program Files ---> Eset ---> Configuration Editor. Now make the necessary changes to your configuration as described on the next page and save, with a title and directory of your choice, on the server.
- 2.** RAC ---> Tools ---> Configuration Editor. Now make the necessary changes to your configuration as described on the next page and save, with a title and directory of your choice, on the server.
- 3.** During the setup of an installation package. Details on page 33.

## The Configuration Editor setup

- ▶ The configuration file (.xml) may be created on the server or, you can **also** install NOD32 LAN Update Server version on your workstation and create the configuration there and then copy it to the server (C:\Program Files\Eset\RA\Server\MyConfiguration.xml).
- ▶ Start
- ▶ Program Files
- ▶ Eset
- ▶ Configuration Editor.

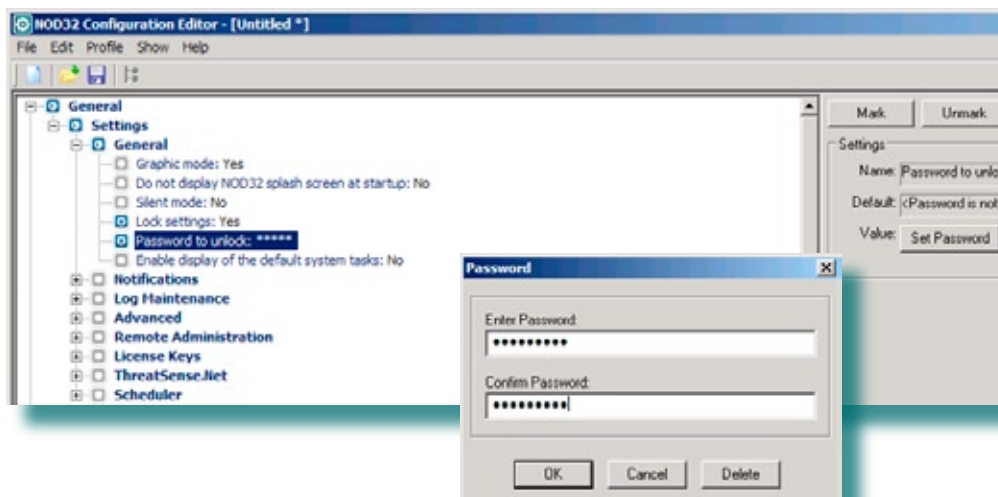
You will now see a window like this:



Rather than look at every single option in the editor, we'll take a look at the crucial areas that should be considered when setting up a configuration, but obviously, you can change as many options as you wish. Further in-depth information can be found on page 49.

When an item is changed, the radio button beside it turns blue. This helps you to identify quickly the areas of alteration that you've made. Also, in future configuration amendments, the client workstations will only look for any new items that have been modified.

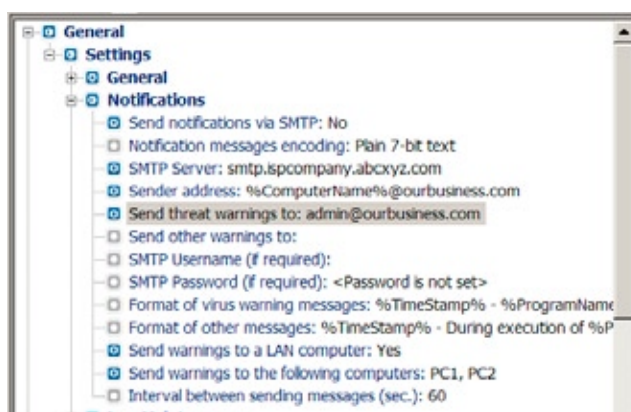
The first section is **General** and we'll look at the Settings area. Here it is advisable to 'lock' the settings in NOD32 and Password Protect them with a password of your choosing, so that only **you** can alter the configuration on any workstation, and not your clients.



The next section is **Notifications**. If you choose to have messages sent to you about alerts/infiltrations on your client machines, you will need to enter the SMTP server address (or IP address) that you use plus the sender address should be entered **exactly** as **%ComputerName%@yourcompany.com** which will enable you to identify the relevant machine in your network. Pay close attention to the way %ComputerName% is entered as this is case-sensitive.

Also, enter the email address you'd like the warnings sent to.

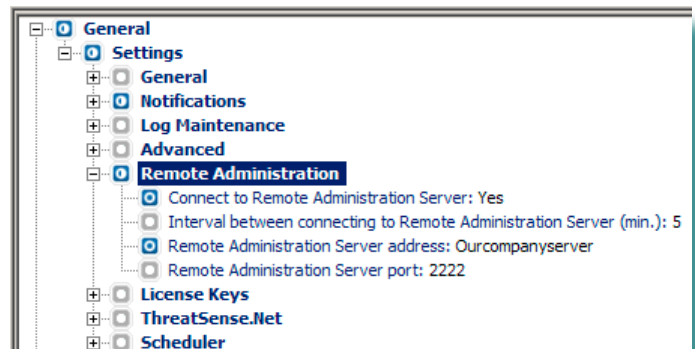
Also you can choose to have Windows Messenger messages sent via your LAN instead of, or in addition to, the email method. Here, you will just need to enter the name(s) of the PC(s) you'd like the messages sent to, delimited by a semicolon or comma.



The next item of note is **Remote Administration**. This is vital to ensure the clients will connect to the RAS.

The Configuration Editor will, by default, pick up the name of the server where RAS has been installed.

The default time for clients to connect to RAS is 5 minutes, but you can alter this if you wish. The default port, that is opened on the server for the workstations to connect via, is 2222.



In the **License Keys** section, you can locate and add the license key (nod32.lic) that you have purchased. This only allows your clients to see when your license will expire for information purposes.

If you use MS Exchange Server, you will need a 2nd license key for **XMON** which can also be added to this folder.

Now move further down the list to **Update > Profile(My Profile) > Settings:**

## Update server address

In the Update section, again, the majority of the default settings should prove satisfactory, however, there are a couple of absolutely vital settings that you must enter in this section.

'**Internet connection type**' should be defined. In a network environment, it's highly likely that your company will connect to the internet via a Local Area Network (LAN).

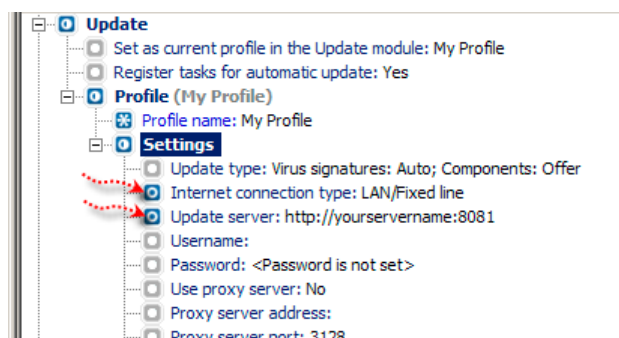
The '**Update server**' must be specified so that your clients will know where to look for their updates on the local server.

Using an HTTP connection is recommended and therefore you should enter:

**http://yourservername:8081.**

If you prefer to use a shared folder, you should enter:

**\\yourservername\sharename.**



Now let's move back to the first section again: **General > Settings**

**ThreatSense.Net** is recommended to leave with default setup but you may review the settings if you wish.

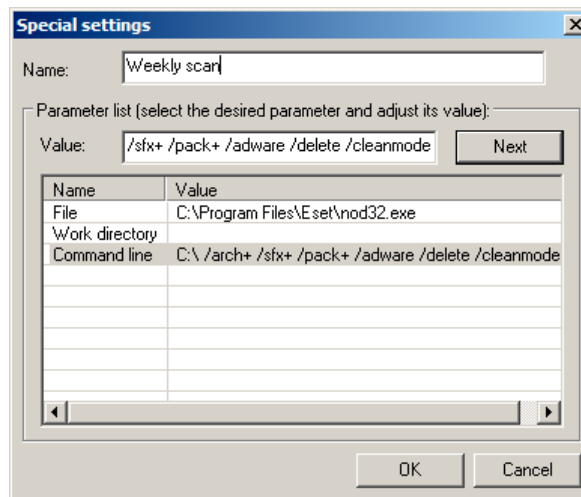
**Scheduler** is useful if you would like to run a scheduled scan on all your workstations once a day, a week or a month, for example. Click the 'Edit' button in the right hand side of the Editor's window and in the new window click 'Add'.

Select the type of task you wish to add. *Hint: if you wish to run a scan with specific command line parameters, choose 'Execution of an external application'.*

The next few windows will be quite self-explanatory, ie: giving the task a name, when you want it to run, etc.

After you click the 'Finish' button you will need to enter the name of the task again and also the path to NOD32 on the client workstations. By default, this would be C:\Program Files\Eset\nod32.exe

A list of the command line switches is shown on page 83 & 84.

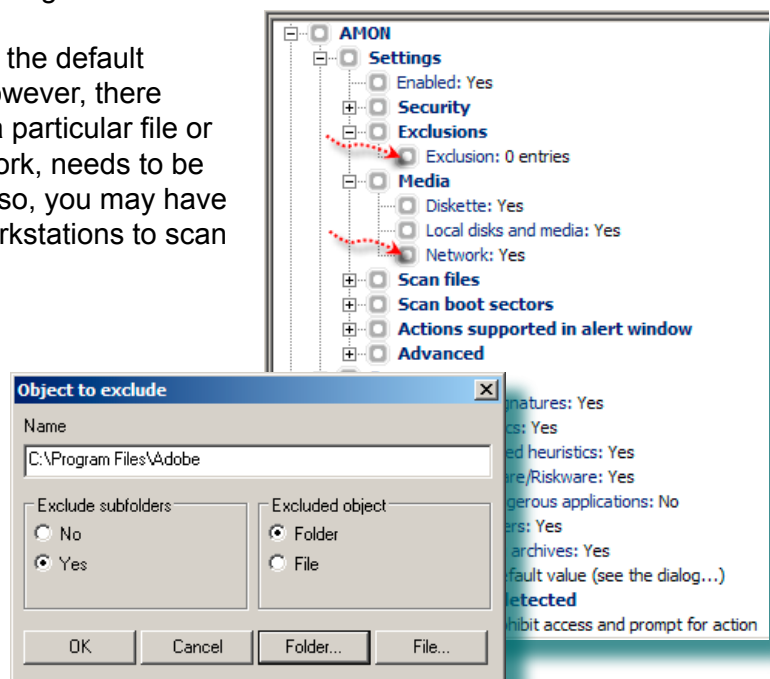


## AMON

AMON (Access MONitor) is a memory-resident (always running when computer is on) file scanning program. Automatic starting of AMON after computer restart is a fundamental defense against malicious code. Quitting AMON is not recommended and should only be done under special circumstances. Execution of two different antivirus monitors (from different products or companies) is not recommended since it may make the client's computer slower and/or cause a system crash, especially on Windows NT systems, and might lead to serious problems.

AMON is the most important line of antivirus defense. AMON monitors all potentially threatening actions on protected computers such as opening, executing, creating or renaming files.

It is recommended to leave the default settings for this module. However, there may be an instance when a particular file or program used in your network, needs to be excluded from scanning. Also, you may have reason to not want your workstations to scan network files.



## DMON

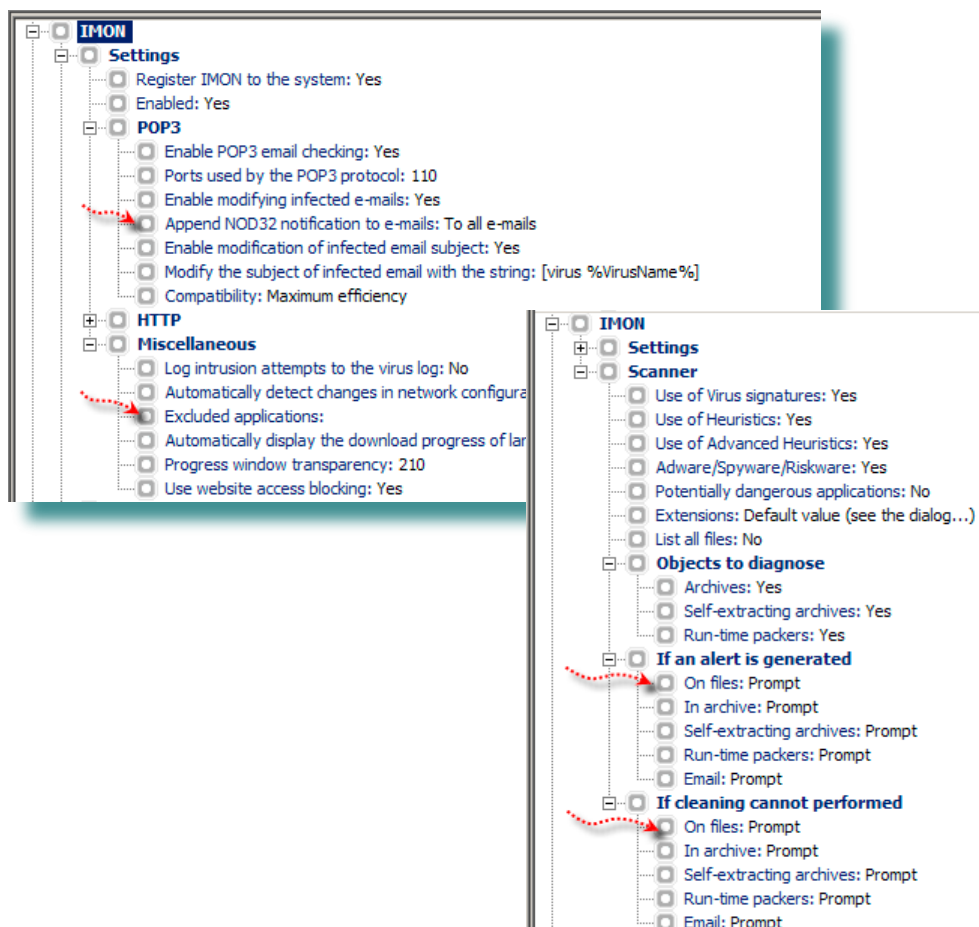
Microsoft Office documents (Word, Excel, etc.) can sometimes contain viruses which infect other files when the document is opened. Document MONitor (DMON) provides protection against this sort of threat. Later versions of Internet Explorer allow Microsoft Office documents to be opened within the browser, directly from the internet. DMON will monitor these documents and prevent infiltration of a virus should an infected document be opened. Generally speaking, the default settings should prove adequate.

## IMON

While the role of AMON is to provide real-time, resident, anti-virus monitoring of a system and user actions, the IMON module protects your computer from email and internet threats. To allow scanning of POP3 email and while also using the internet, we recommend having IMON enabled. IMON's primary role is to monitor incoming email. There is virtually no setup necessary since this module works with all email programs. IMON works on the winsock level (operating system level). Again, the default settings are recommended, but there are a couple of items you may want to look at: You may **not** want IMON to append a message at the bottom of every email that your clients receive, so this can be changed to only infected emails or no notification at all.

Also, you may have reason to want certain applications excluded from IMON's scanning, so the program(s) can be added to an exclusion list here.

IMON's Scanner is generally setup to optimum performance but in the areas titled 'If an alert is generated' and also 'If cleaning cannot be performed' the default setting is to Prompt the user to take some action in both cases. However, you may prefer to have 'Files' cleaned as the first action and if that cannot be performed to have them deleted. This is merely an example of the various choices you have, not a recommendation necessarily.



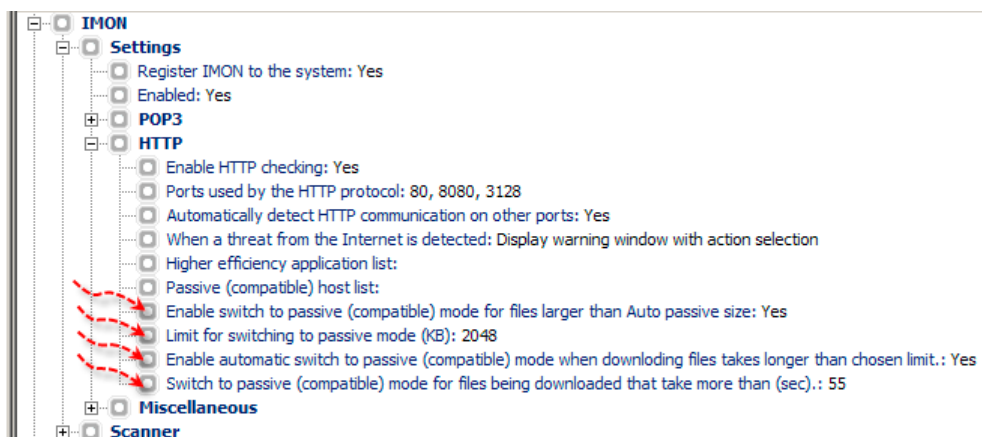


## HTTP: Active & Passive modes

The download popup window is shown only for applications set to **Active mode** (Higher efficiency) in the HTTP scanner compatibility (default).

With IMON in **Passive mode**, portions of a downloaded file are continuously passed on to the target application whilst IMON stores a temporary copy of each of the fragments. When the last fragment is detected, the whole file is scanned for viruses. If an infiltration is detected, a warning window appears and the connection with the particular server is terminated. A disadvantage of that is that the already downloaded portion of the file may already contain a fundamental portion of a malicious code. What's more, if the application repeatedly attempts to download an infected file, it may use the already downloaded data and request only the rest of the file. In this case, IMON may not find anything suspicious in the remaining portion.

In **Active mode** (default), IMON first downloads and scans the whole file and then passes it on to the target application. This procedure is safer because in the case of an infiltration, the application does not receive any portion of the downloaded file. A disadvantage is that the application receives all the data at once, therefore it cannot show the download status properly. Therefore, if the download lasts for more than 55 seconds (default, but can be altered), a small window showing the download progress pops up. Active mode is not suitable for certain types of data which requires a continual data flow (e.g. multimedia, streaming video/audio).



## EMON

EMON (Email MONitor), a complementary resident module, scans emails incoming via MAPI interface. The MAPI interface hooks into the different interfaces of Microsoft Outlook. MAPI interface is used also when receiving emails from the Microsoft Exchange Mail Server via the Exchange protocol.

Even if the MAPI Interface is **not** used on the computer, EMON will still be installed. E-mails incoming via the POP3 protocol **will be checked by IMON**.

As with IMON, you may want to alter similar scanning features within this module.

## XMON

XMON stands for MS Exchange MONitor which serves for scanning incoming **and** outgoing email, utilizing the MS VSAPI interface on MS Exchange servers. The minimum requirements are MS Exchange 5.5 SP3, MS Exchange Server 2000 SP1, MS Exchange 2003 or higher. The newer the version of MS Exchange server you have, the more features are available in XMON.

The removal of entire infected email is supported from MS Exchange server 2003. Otherwise, this option is unavailable and the appropriate check-box is grayed out.

Using XMON requires a 2nd license file. In the **License Keys** section (top of the Configuration Editor list: General / Settings), you can locate and add the license key for XMON (nod32.lic) that you have purchased.

## NOD32 On-Demand Scanner

Profiles are so you can save a set of pre-set scanning parameters when running on-demand scans. Any of the following profiles can be set as the primary, default scanning profile:

- ▶ **Control Center Profile - NOD32:** the default setup for on-demand scans and/or scheduled scans. Set parameters when selecting desired disks, drives or specific folders, etc.
- ▶ **Context Menu Profile:** parameters when running an 'instant' scan on any desired file or folder (Right click on the file and choose 'NOD32 antivirus system')
- ▶ **Control Center Profile - Local:** parameters when only scanning local disks.
- ▶ **Control Center Profile - In-Depth Analysis:** parameters when running an in-depth analysis.
- ▶ **Control Center Profile - Diskettes:** parameters when only scanning floppy diskettes.
- ▶ **My Profile:** create and save a profile with your own settings.

The above headings are to give the user a selection of names for specific scans. You can create, and name, as many new profiles as you wish. You might like to create names that are more specific for your clients, or easier to understand perhaps. To create, click Profile in the toolbar and choose 'New profile' or right click on a 'Profile' in the Configuration Editor window and choose 'New profile' from the context menu.

Again, generally speaking, the default settings for NOD32's On-Demand Scanning are probably adequate, secure and recommended. Eset's developers have designed NOD32 to be 'ready-to-go' without the necessity for major setup changes.

Under the 'Settings' sub-heading in 'My profile', the '**Run this profile in cleaning mode**' option, enables the NOD32 scanner to run in a cleaning mode. ie: The actions taken when a virus is found depend on those set under 'If an alert is generated' (and 'If cleaning cannot be performed').

So, looking through **Profile (My Profile)**, most of the items in 'Settings' are self-explanatory and you will probably be familiar with, if you've tested the standard, single-user version of NOD32. However, there are one or two items of note which we should look at.

In the '**Scanner**' section, you will notice '**Use of Advanced Heuristics**' is not enabled by default. This is because Advanced Heuristics main purpose is detecting as yet unknown threats that arrive at a workstation either via the internet or through removable media disks, etc. Therefore, Advanced Heuristics are an absolute 'must' to have enabled in AMON / IMON / DMON / EMON / XMON. By enabling Advanced Heuristics in an On-Demand Scan, there is a higher chance of the scan flagging a legitimate file or program as a 'False Positive' plus the scanning time may be slightly longer than normal.

'Potentially dangerous applications' is also not checked by default (this also applies to all the other scanning modules in NOD32) because there is a chance that your company may use some other remote access programs which NOD32 might mistake for some hacker's tools. Therefore, this option should be enabled with caution.

'**List all files**' is not enabled by default because the resultant scan log could be enormous and therefore difficult to plough through when checking for threats.

'**Run-time packers**', '**Archives**' and '**Self-extracting archives**' are not set to be scanned by default because of the slow-down in scan time plus there is a much higher chance that scanning in archives could lead to a greater number of incidents like "Why can't I delete that nasty infiltration" or "What exactly is this archive?" If the user opened any such file, AMON will immediately flag the enclosed malware.

'**Mailbox databases**' are also not scanned by default for the following reasons:

- ▶ Mail files can be massive in size and take a very long time to scan.
- ▶ If the scanner is configured to delete infected files, then the entire mail file will be deleted instead of just the infected message. To eliminate a virus in an infected message the individual message should be deleted.

'**MIME files**' or NTFS streams are not scanned by default because exploitation of them has been exceptionally small.

In the areas titled '**If an alert is generated**' and also '**If cleaning cannot be performed**' you will have already made similar choices perhaps, in the IMON / DMON / EMON / XMON module setups. The default setting is to Prompt the user to take some action in both cases. However, you may prefer to have 'Files' cleaned as the first action and if that cannot be performed to have them deleted. This is merely an example of the various choices you have, not a recommendation necessarily.

## How many clients can I connect to my server?

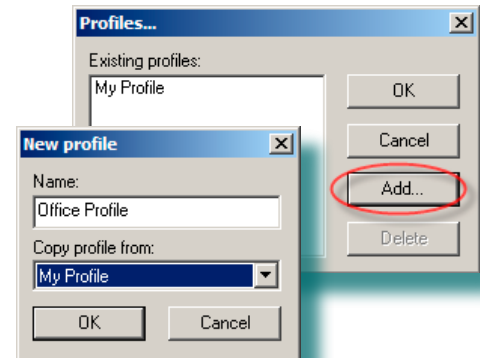
*Experience has shown us that it is recommended to allow 5 times the number of connected sessions for any given operating system to calculate a practical number of clients that will connect to a given server. However, it's possible that even if using the recommended maximum number of users per Mirror, there will be situations when some clients might get an error message during update. The only way to totally guarantee no connection errors, is to set the ratio to 1:1 (operating system allowed connections : number of clients) but we have found 1:5 is an acceptable ratio.*

*Client computers probably do not have their scheduled updates completely synchronized. Automatic update occurs an hour after the last update, so even if all clients were installed exactly at let's say 8:00 then the first automatic update will be scheduled for all of them at 9:00. But in the meantime one client could hit the 'Update Now' button or has restarted (and thus update occurred during logon) let's say at 8:30. Even if there was actually no fresh update available at that time, the next regular update check for this client will move to 9:30 while the rest of the clients will check it at 9:00. So as time passes and clients shut down or restart their computers, the time interval of update spreads to the point where there is not big risk of downloading the update with too many clients simultaneously. Also there is the possibility to improve this further by ticking **Disconnect from server after update has completed** in Advanced Mirror Setup. By ticking this option, the update of more clients from one Mirror can be achieved.*

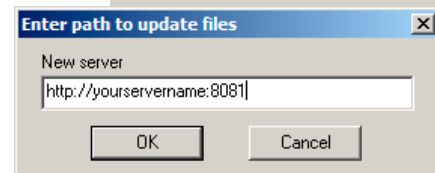
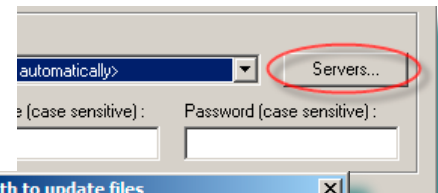
## Secondary update profile

You may have clients in your network that use laptops that are regularly taken away from the LAN and therefore need to update from another source, ie: Eset's servers via the internet. This will require setting up a secondary profile. Follow these steps to set this up:

- ▶ Download and install the standard, single-user version of NOD32 onto any workstation - maybe your own PC or laptop.
- ▶ Open the Control Center and go to the **Update > Setup** section and click on the **Profiles** button.

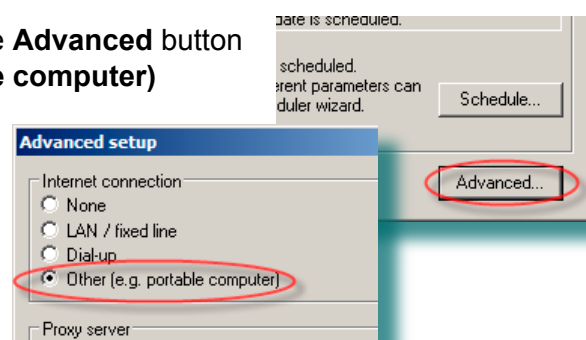


- ▶ Press **Add** and copy from the default **My Profile** and call the new profile a name of your choice, like **Office Profile** maybe. This should be set to update from your local DNS server, ie: **Add** a new server and enter: **http://myservername:8081**

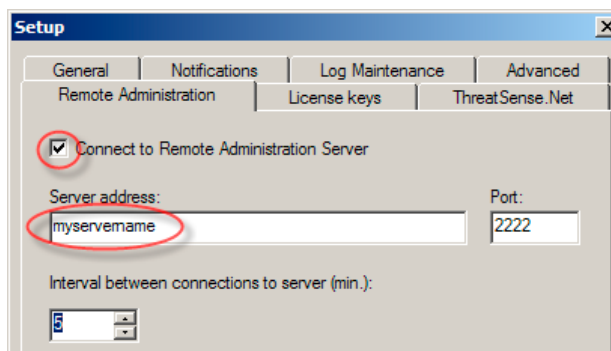


- ▶ Now **Add** another new profile. Copy it from the default **My Profile** and call it **Out of Office Profile** for example, which will update via the internet (Choose automatically). This will need to have the Username and Password entered that you received with your license.

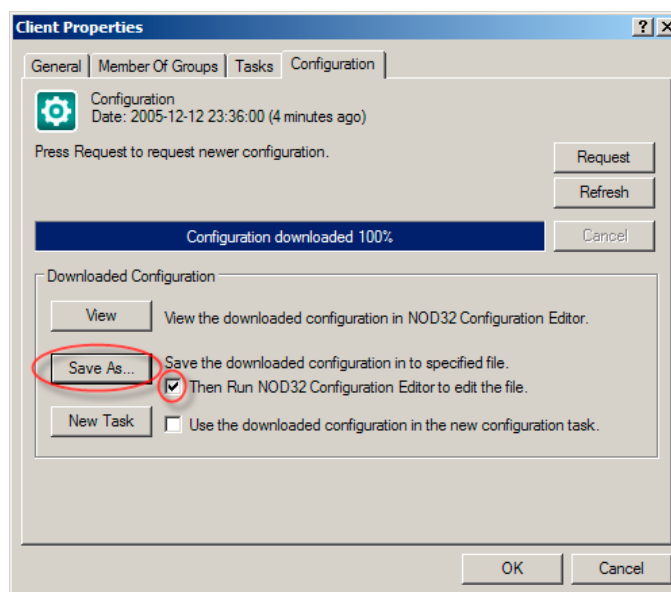
- ▶ Now for **both** profiles, press the **Advanced** button and select **Other (e.g. portable computer)**



- ▶ Next, go to NOD32 System Tools > NOD32 System Setup > Setup > Remote Administration tab and check the box by **Connect to Remote Administrator Server** and enter the name **only** of your server.
- ▶ Now go to NOD32 System Tools > Scheduler/Planner and right-click on **Regular automatic update** and choose **Edit** and skip through the following 5 windows until you reach the Profile Selection window, whereupon you can select **Office Profile** as the main one and **Out of Office Profile** as the secondary one.
- ▶ Next, open RAC, wait 5 minutes (default) for the workstation to appear in the Client list and then right-click on the client and select **Configuration** from the context menu.



- ▶ In the next window, select **Save as...** and give the configuration a name of your choice. The setup will then open in the Configuration Editor with the settings you've just arranged in NOD32 on your workstation.
- ▶ You can now alter any other settings as previously described from pages 19 to 28.



- ▶ A couple of items that you'll need to alter at this point:
  1. Under: General > Settings > Advanced > Quarantine folder, change the text to this: **%INSTALLDIR%\infected**
  2. And under: General > Settings > ThreatSense > Files excluded from submitting, enter: **\*.doc|\*.rtf|\*.xl?|\*.dbf|\*.mdb|\*.sxw|\*.sxc**

*Note: The secondary profile will **not** work if the client tries to manually update by pressing 'Update now' from their NOD32 Control Center. The secondary profile only takes effect when the Regular automatic update fails to connect to your LAN server. ie: every hour.*

## Mirror

This section is only required if you intend to 'push' an installation of NOD32 Administration version to any of your clients. This is unlikely as you will already have installed this version on your server and created the Mirror (see page 11) from which all your clients will pick up their updates, but the Configuration Editor gives you this option in case another Mirror needs to be created remotely in your network.

## Save the configuration

**Make sure you save the configuration by selecting File > Save from the toolbar and not by just closing the configuration window which will cause the Settings ID to NOT be written correctly, which may cause problems with clients not picking up the configuration properly.**

**If you created a configuration using method 3 as described on page 18, ie: whilst setting up a package, then it will be saved in:**

**C:\Program Files\ESET\RA\Server\Packages\Default\nod32\_nt.nip and/or nod32\_98.nip and is not accessible afterwards, other than via the package editor, however, you could choose File ---> Export and save the file in a location of your choice.**

**If you created a configuration with another method, you can save the XML file anywhere you wish, but we recommend:**

**C:\Program Files\ESET\RA\Server**



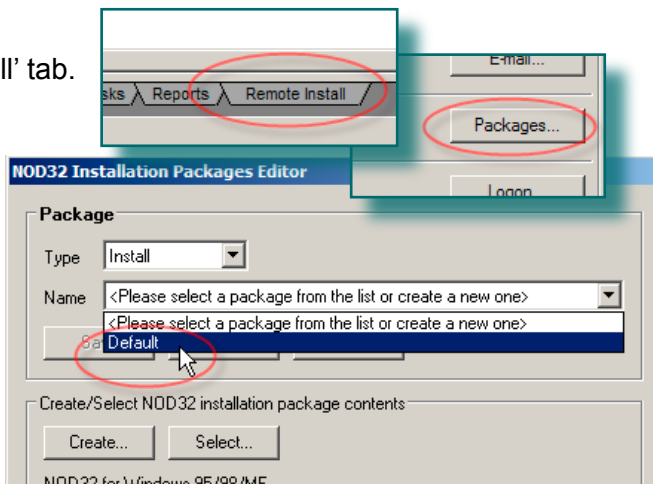
# Create a package

## Create an installation package

Follow these steps to create an installation package: files with a \*.nip extension or installers for specific workstations (according to their operating system) with a preset configuration.

- ▶ From RAC, click on 'Remote Install' tab.
- ▶ Choose 'Packages'.

- ▶ **Option 1:** Select the "Default" package. This will use the versions of NOD32 embedded in RAS, but they may not necessarily be the most current versions, as NOD32 is periodically updated and a new version is made available on the Eset website. Save the package with a name of your choice. The default saving directory is **C:\Program Files\Eset\RA\Server\packages**



- ▶ **Option 2: (Recommended)** Press 'Create' to setup your own package using previously downloaded, and very latest, installers for NOD32 (as described on page 13). In the following window, press the "..." browse button to locate the installer(s) for NOD32. Choose to 'Create' this package to 'Server' with a name of your choice, click OK and you will move back to the 'Packages Editor' window.
- ▶ **Option 3:** Press 'Select' and you can choose a pre-designed package that you may have already created or select either, or both, of the built-in installers (eg: C:\Program Files\ESET\RA\Server\packages\Default\nod32\_nt.nip and/or nod32\_98.nip)

**Whichever method you chose, you will now be back in the 'Packages Editor' window again.**

- ▶ In the *'Edit/Select configuration associated with this package'* section, press 'Edit' to create a new configuration or 'Select' and choose the configuration that you have already created and saved to **C:\Program Files\ESET\RA\Server\MyConfig.xml**
- ▶ You can choose either or both operating system platforms: Win9x and/or WinNT and click 'Save'.
- ▶ In the section *'Edit/Select command line associated with this package'* you can define command line parameters, which will be used with the package. The default is: /INSTMFC /SILENTMODE.
- ▶ In the lower right hand corner of the window, you can select 'Show me command line options' which will provide details of the available options. Full details are on page 80.
- ▶ Press 'Save' and the complete package will be saved, by default, to **C:\Program Files\ESET\RA\Server\packages\MyPackage**

# Remote Installation

## General points to watch out for when installing remotely

- ▶ Especially on computers with the MS Windows XP operating system, 'Simple file sharing' should NOT be enabled. This will stop connections to the server. To disable this option, go to Start > Control Panel > Folder Options > View tab.

In Windows registry, it is: **HKLM\SYSTEM\CurrentControlSet\Control\Lsa** ...the **forceguest** item. Set its value to 0.

- ▶ Make sure any firewalls on the clients does not also interfere with connections during installation.
- ▶ As a rule of thumb, IMON should not be enabled on your server. IMON monitors port activity at the winsock level. A typical server (depending on the number of clients accessing) running an application which opens and closes a large number of "winsock" connections, over a long period of time, may result in a significant resource drain. In the case of IMON (coupled with Windows), it may not be able to keep up with this incredibly fast paced I/O (Input/Output). IMON may not be able to open and close sockets fast enough (or not at all) and use all the available memory for (possibly pending) operations causing the affected server to reboot itself to regain resources as a protective measure.
- ▶ Given that a server is not used as a workstation for accessing email or surfing the internet, IMON is therefore not necessary anyway.
- ▶ Make sure, as you are the administrator of your network, that you have set your admin's logon name and password to access all your clients. If the password is left blank, connection to your clients will not work.
- ▶ If installing onto WinNT/2000/XP machines via logon script or email, a logon name and password must be defined in the RA console. To set it up, go the **Remote Install** tab and in the **Set Default Logon for E-mail and Logon Script**, click the **Logon** button.
- ▶ Whichever method of remote installation you choose, the TCP/IP connection between target workstations and RAS is established on port 2224 (only for the installation process). That's why a properly configured TCP/IP protocol is among the minimal requirements for a successful installation.
- ▶ For WinNT/2000/XP/2003 operating systems it is necessary to provide:
  - ◆ Client workstations in a Microsoft Windows Network.
  - ◆ "File & Print Sharing for Microsoft Networks" must be enabled (Control Panel -> Network Connections > Network > Properties)
  - ◆ The Remote Procedure Call (RPC) service needs to be running on the target.
  - ◆ The Remote Registry service needs to be running on the target.
  - ◆ The RPC Locator service should be set to "manual" and need not be running.

## Remote Installation

NOD32 Remote Administrator enables installations of NOD32 for Windows to remote workstations in a network. In RAC, navigate to the “Remote Install” tab.

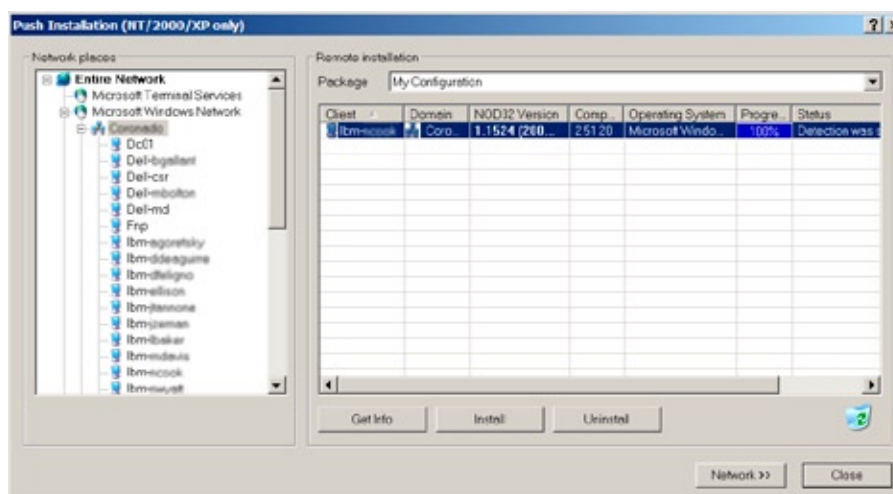
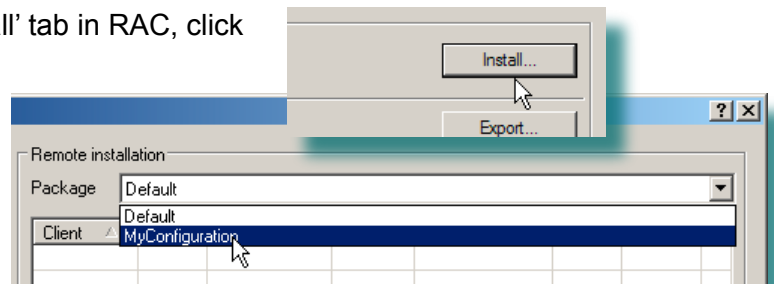
RA offers three basic ways of how to install NOD32 for Windows remotely. In all cases, a TCP/IP connection between the target workstations and RAS is established on port 2224. That’s why a properly configured TCP/IP protocol is among minimal requirements for a successful remote installation.

### 1. Push the installation

(only for workstations with WinNT/2000/XP/2003/Vista operating systems)

The installation is “pushed” to remote workstations directly on the administrator’s command.

- ▶ While on the ‘Remote Install’ tab in RAC, click on the ‘Install...’ button.
- ▶ In the new window: ‘Package’ text box - select your new package.
- ▶ In the left hand panel, select maybe one client to start with, drag him over to the right hand panel and click the ‘Install’ button at the foot of the panel. The console will ask for the administrator’s username and password for this situation. You will need to specify whether the workstation is located in a domain or in a workgroup.



- ▶ By ‘pushing’ to just one client, you can make sure you get the result you were hoping for.

- ▶ The client's machine needs to be restarted to complete the installation. This can either be done remotely, manually at the workstation or automatically by a command line when setting up the installation package (see page 34)
- ▶ Within 5 minutes, this client will show up in the RA Console under the 'Clients' tab. This is because 5 minutes is the default time period that the clients will contact the server. You can of course alter this time period in the installation package. (see Configuration Editor chapter, page 17)
- ▶ If successful, choose some more, or all, of the other clients and 'push' the installation to them also.
- ▶ Go to the 'Clients' tab in RAC, and you'll see the rest of your clients appear in the list after the default 5 minute period.

## 2. Export to logon script

(for all workstation platforms but specifically for Win95/98/ME operating systems)

This remote installation is exported to workstations in a logon script or in an e-mail. These two methods are very similar. They differ only in the way the file `nod32installer.exe` is sent to target workstations. To install the program, the **nod32installer.exe** needs to run on a client workstation.

- ▶ For “Export to logon script“, first select the name of your Package in the section ‘Installation location’ and then type in the path to this package in the ‘Folder’ text box, which will have the file `nod32installer.exe` placed inside it. This will automatically create the Share path in the next box.
- ▶ Note: The `nod32installer.exe` for this package, already exists in “C:\Program Files\ESET\RA\Server\packages\” folder. We do not recommend overwriting this `nod32installer` since it may affect another installation method. So, in this step, you should choose a folder for a secondary `nod32installer.exe` which will serve for the purpose of a logon script installation only. You may choose any name for this folder. It doesn’t even have to be a shared folder since a logon script uses proper share (“C\$” in the screenshot example). Whatever folder you choose, the ‘Share’ field will be filled automatically.
- ▶ In the Script location section, choose the current logon script directory and select the logon scripts that will be customized for the NOD32 logon script installation.
- ▶ Select the extension type of the logon script you want to use (all scripts are shown). For example: “script.bat“. To edit each logon script, use the Edit button and then save the result by clicking on the Save button in the editor.
- ▶ So as long as you have a login script directory on your server (these are normally created automatically but vary from one server to another) the following batch file will perform the installation correctly (.BAT):

**@echo off**

**IF NOT EXIST “C:\program files\eset\nod32.exe” \\servername\sharename\nod32installer.exe**

Note: This script, and the file “`nod32installer.exe`” need to be in a shared folder that EVERYONE has read-access to. Typically, there will be a special folder for logon scripts on Windows servers. This location varies under different versions of Windows (ie: NT4, 2000, 2003)

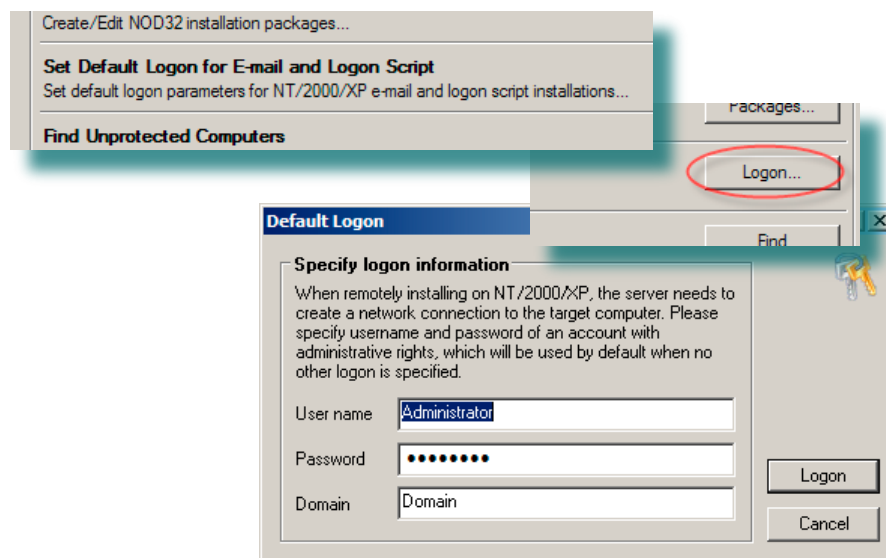
Replace `servername` and `sharename`, respectively with the names of the sever and share that have been set up.

- ▶ Choose the logonscript you want to affect and then hit the 'Export' button. A new line is added to the logon script which will make the installation happen. You may also see other lines of simple logon scripts which automatically map the server shared folder as drive X for clients.
- ▶ Close 'Export Installation to Logon Script' and wait until clients logon to install NOD32.

Please be sure that you set a default logon field properly (Applies to Install via Email also).

This may be any user which has administrator rights to a client computer. Of course the best (and logical) choice is the Domain Administrator account, since you ensure that you have administrative access to all computers in the domain. When administrating multiple domains/workgroups, we recommend to create an RA server for each domain/workgroup so that the server will keep the Default Logon, with administrative rights, to all clients of that particular server.

All corresponding files in the directory will be displayed according to the mask in the File(s) section (including logon scripts). Now also select files into which a line providing installation (or uninstallation) of NOD32 on remote workstations will be inserted. Click on the 'Edit' button to edit the file in the Configuration Editor. Click on the 'Save' button to confirm the changes made.

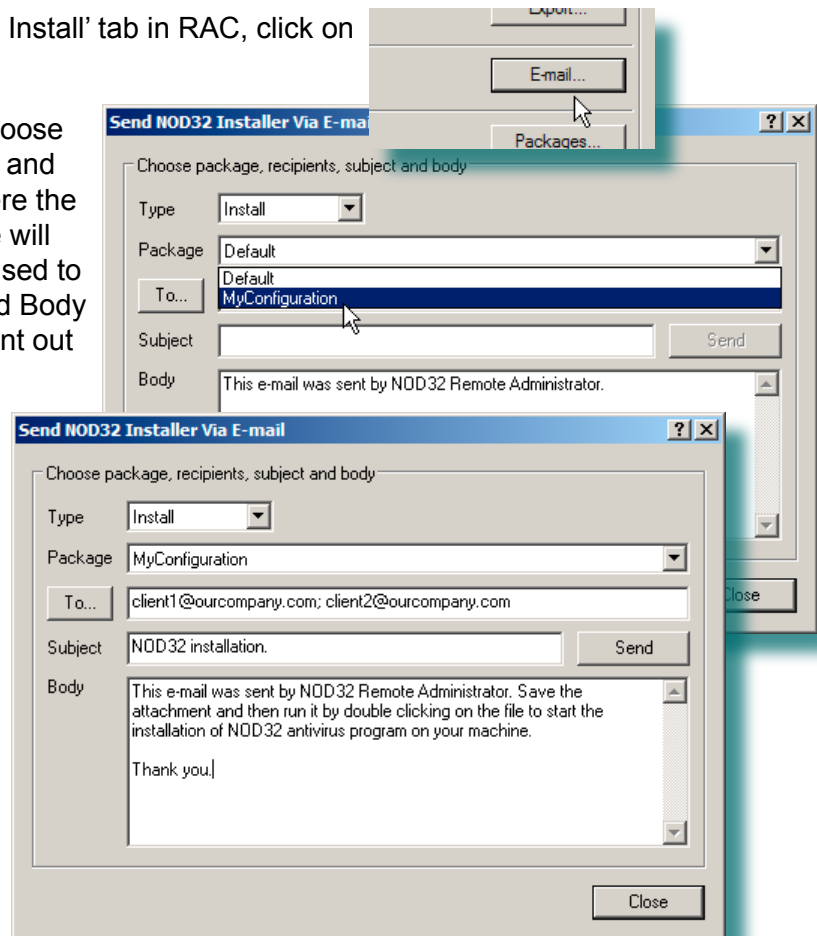




### 3. Send via E-mail

(for all workstation platforms including Win95/98/ME operating systems)

- ▶ Alternatively, 'Send via E-mail' naturally sends the file nod32installer.exe via e-mail. After the recipient(s) saves and runs the email attachment, either remote installation, or remote uninstallation, of NOD32 for Windows will start.
- ▶ While on the 'Remote Install' tab in RAC, click on the 'Email...' button.
- ▶ In the new window choose the required Package and select addresses where the nod32installer.exe file will be sent. It is also advised to define the Subject and Body of the e-mail being sent out to your clients.



- ▶ For the RA server to work properly, it is required to set the SMTP server address and sender e-mail address. In case this information is not available, the e-mail can be sent using the Microsoft Outlook application (Outlook Express is not supported).

## 4. Optional, manual installation

If you wish, you can choose your own installation method, outside of the console. Copy the file `nod32installer.exe` from RAS, in your corresponding package, onto a flash key/CD/floppy disk, and run the file on the client workstation. This will invoke a download from the server of the corresponding installation package.

`nod32installer.exe` is located in this directory on the server: **C:\Program Files\Eset\RA\Server\packages\{package\_name}\nod32installer.exe**

You can also create your own pre-configured installation. See page 78.

### Installing manually if there are any problems

If, for some reason, a push, logon script or email installation will not work, you could manually install on one or two machines to make sure they will connect to the server and appear in RAC clients panel as follows:

Download the Standard NOD32 single-user version, using the Username and Password you received with your administration license, and install onto your chosen workstation following the 'Typical' installation route and reboot the machine.

Open the **NOD32 Control Center** and go to the **Update > Setup** section. In the **Location** panel, press the **Servers...** button and then **Add...** In the new window enter your server's details like this: **http://myservername:8081** or **http://myserver'sIPaddress:8081** and click OK. The Username and Password text boxes should be rendered blank and click OK.

Now go to **NOD32 System Tools > NOD32 System Setup > Setup > Remote Administration** tab and check the box beside **Connect to Remote Administration Server**. Now enter the name or IP address only of your server in the text box. The default connection port should remain as 2222 but you can reduce the **Interval between connections to server (mins)** to **1** to speed things up in RAC. Click OK and Hide the NOD32 Control Center.

Now open RAC on your workstation and connect to RAS on your server. Within 1 minute the workstation you've just installed NOD32 onto will appear in the **Clients** pane, thus you will know that connections are successful between Client, Server and your administrator's workstation.

# Use of Tasks

## Creating Tasks for your workstations.

NOD32 Remote Administrator (RAS) enables the administrator to create tasks and apply them to remote client workstations running NOD32 for Windows.

Using the RA Console (RAC) you can create three types of tasks:

- ▶ “Configuration” – to make changes in configuration of remote client workstations.
- ▶ “On-Demand Scan” – to run an antivirus scan on remote client workstations.
- ▶ “Update Now” – to immediately update remote client workstations.

To run the planner wizard, press the key combination CTRL and N or from the toolbar: File ---> New Task...

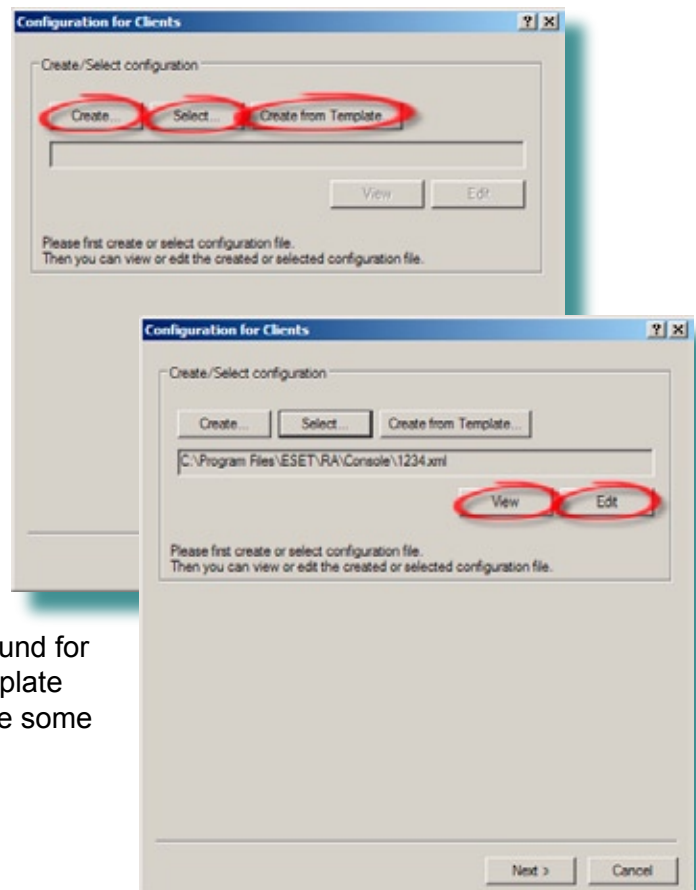
## Configuration task – changes in configuration

To apply a configuration task to client workstations, first you must create (clicking on the Create... button), or choose an already existing (the Select ... button) XML configuration file.

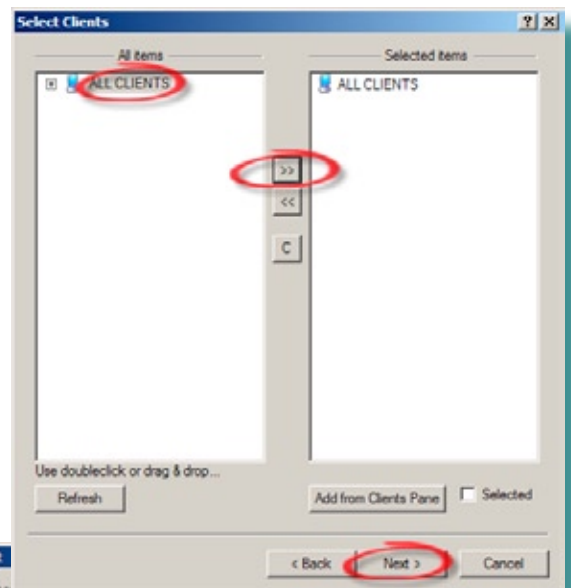
Configuration setup takes place in the NOD32 Configuration Editor – it is described in more detail in the chapter Configuration Editor (page 17).

The selected configuration can be viewed (the ‘View’ button), or changed (the ‘Edit’ button).

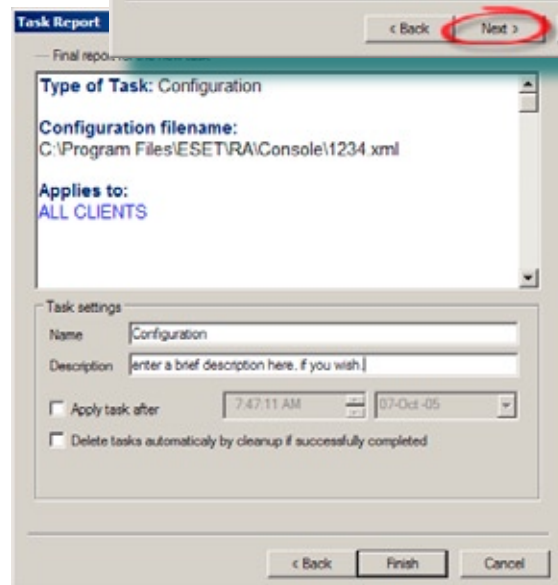
Use the ‘Create from Template...’ button to open an existing configuration and use it as a background for a new configuration. The original template will stay unchanged, even if you make some changes.



In the next step, choose workstations or groups, to which you want to assign the configuration (put them in the 'Selected items' section). Click on the 'Add from Clients Pane' to add currently displayed clients to the pane under 'Selected items'. Check the 'Selected' option to move only those clients which were highlighted in the left hand 'Clients' window. Alternatively, you can select some or all clients that are listed and click the >> button to add them to the list under 'Selected items' in the right hand panel.



In the final step, you can name the task, or add its description. This data serves only to help the administrator and for easier orientation. At the same time, you can delay the task (Apply task after), or provide its automatic deletion from the RA console after it has been successfully performed (Delete tasks automatically by cleanup if successfully completed).



## On-Demand Scan task

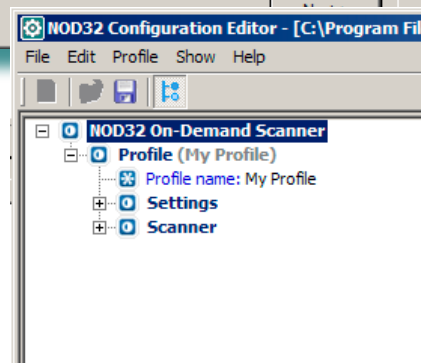
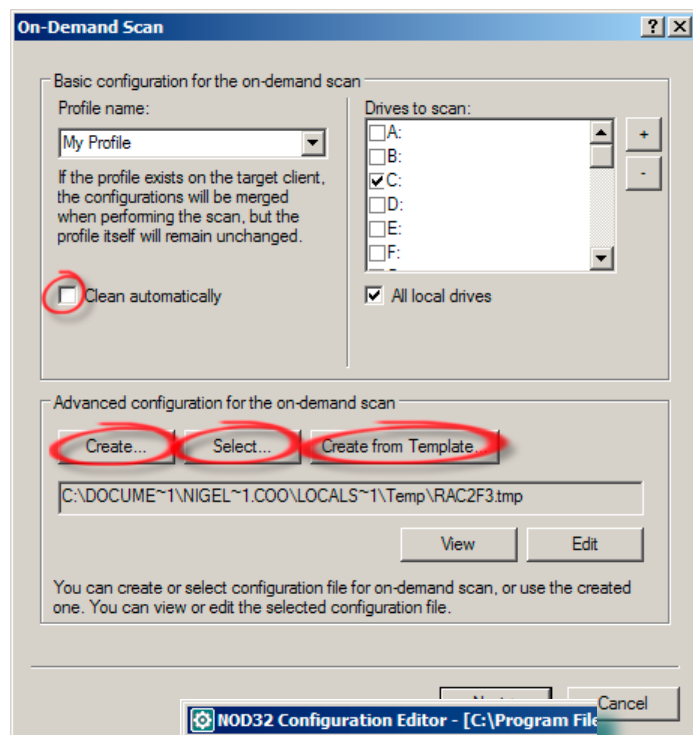
To apply this type of task, first create (clicking on the 'Create ...' button), or choose an already existing (the 'Select ...' button) XML configuration file with a specific scanner configuration (a standard, full configuration setup will not suffice), which will be applied on remote client computers to start antivirus scanning.

To setup the configuration file, open the NOD32 Configuration Editor – it is described in more detail in the chapter Configuration Editor (page 17). We recommend to focus on the color distinction of the small symbols in front of each attribute – they show, whether the attribute will be applied, or whether the original setting will not change. The selected configuration can be viewed (the 'View' button), or changed (the 'Edit' button).

Use the 'Create from Template...' button to open an existing scan configuration and use it as a background for a new configuration. The original template will stay unchanged even if you make some changes. In this mode - viewing, editing, creating - only the scanner settings are available to view.

In the upper section, choose a profile name from the 'Profile name' pull-down menu. If this profile is also found on the target workstation, the above mentioned configuration will be applied and will be added to the settings of the existing local configuration for this profile. ie: only items with a blue button will be recognised.

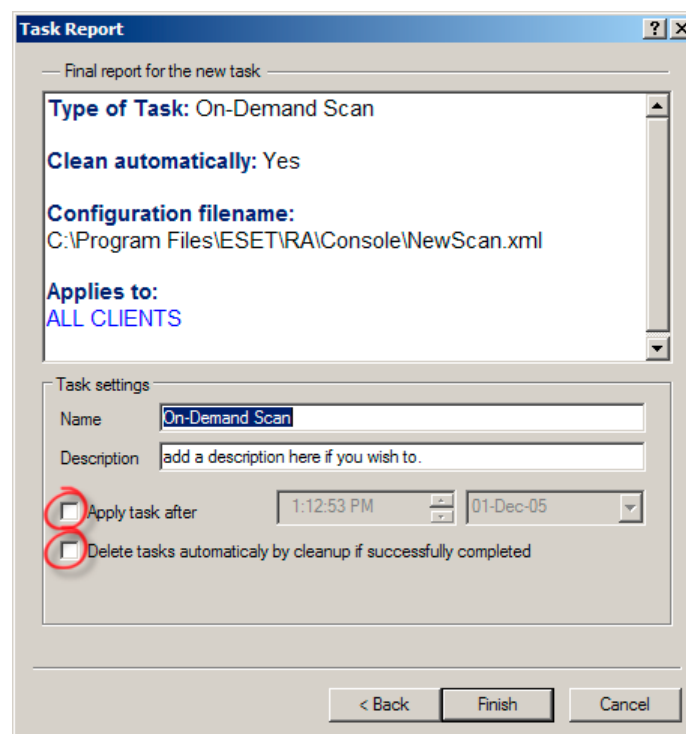
If you want to push a complete scanner configuration, regardless of previous target workstation configurations, then press the key combination CTRL + A or choose 'Mark all' from the menu 'Edit' during creation of the configuration. This will mark all settings with a blue button and will therefore all be picked up by the target workstations.



To run the On-Demand Scan task in cleaning mode (not in the default mode, where the scanner only creates a scanner log, and any reported infiltrations are left on the target client computer), check the 'Clean automatically' option. Then, if an alert is generated, the scanner will then take the action defined in your configuration automatically (NOD32 Configuration Editor ---> NOD32 On-Demand Scanner ---> Profile ---> Scanner ---> If an alert is generated/If cleaning cannot be performed).


In the next step, choose workstations or groups, to which you want to assign the scan configuration (put them in the 'Selected items' section). Click on the 'Add from Clients Pane' to add currently displayed clients to the pane under 'Selected items'. Check the 'Selected' option to move only those clients which were highlighted in the left hand 'Clients' window. Alternatively, you can select some or all clients that are listed and click the **>>** button to add them to the list under 'Selected items' in the right hand panel.

And finally name the task, or add a description to it. These features serve only for easier orientation for the administrator, who can thus later quickly identify tasks. At the same time, you can 'Apply task after' and choose a time and date, or delete it from the 'Tasks' tab of the RA console after it has been completed (Delete tasks automatically by cleanup if successfully completed).



## Update Now task

First, define the name of current Update profile that will be applied on remote workstations. If you do not use update profiles for update, you do not need to choose any profile, you can skip to the next step.

Next, choose workstations or groups, to which you want to assign the configuration (put them in the 'Selected items' section). Click on the 'Add from Clients Pane' to add currently displayed clients to the pane under 'Selected items'. Check the 'Selected' option to move only those clients which were highlighted in the left hand 'Clients' window. Alternatively, you can select some or all clients that are listed and click the  button to add them to the list under 'Selected items' in the right hand panel.

And finally name the task, or add a description to it. These features serve only for easier orientation for the administrator, who can thus later quickly identify tasks. At the same time, you can 'Apply task after' and choose a time and date, or delete it from the 'Tasks' tab of the RA console after it has been completed (Delete tasks automatically by cleanup if successfully completed).



# More detailed information

## Remote install in detail

In this chapter you can find more detailed information about the remote install process.

In the case of a Push installation, the following operations take place:

1. RAS contacts a remote workstation and attempts to authorize the connection by the username and password created and entered by the administrator from the RAC (the password cannot be left blank, or the connection will not work).
2. If successful, the RAS connects to the workstation using share ADMIN\$ and starts copying the file nod32installer.exe belonging to the installation package.
3. The file nod32installer.exe is started as a service and executed.
4. After that, nod32installer.exe contacts the RA server on port 2224 (TCP) and starts downloading the corresponding installation package.
5. When the download finishes successfully, the installation of the package starts, together with predefined attributes (configurations, command line parameters, etc...)

In the case of the variant “Export to logon script“, or “Send via E-mail“, the process starts with the running of the file nod32installer.exe (either manual – by user, or automatic, eg: from logon script). Then these operations take place:

1. The file nod32installer.exe is started as a service and executed.
2. After that, nod32installer.exe contacts the RAS on port 2224 (TCP) and starts downloading the corresponding installation package.
3. If there is also a Windows NT based operating system (ie: Windows 2000/XP, etc.), the RAS provides logon information – an account (username / password), that will be used for the installation .
4. When the download finishes successfully, the installation of the package starts, together with predefined attributes (configurations, command line parameters, etc...)

*NB: Username / password, or administrator account on that workstation must be defined in the RAC. To define it, click on the “Logon” button in the “Remote Install” (Set Default Logon for E-mail and Logon Script).*

## The file nod32installer.exe

The file nod32installer.exe is an installer that will prepare NOD32 for remote install.

After executing, it is installed as a service. It will also perform the following tasks:

- ◆ Check whether NOD32 for Windows is already installed on workstations. If yes, it will not attempt to install it again.
- ◆ Run installation of NOD32 under an administrator account. All data is sent from RAC, or the file nod32installer.exe receives them from RAS.
- ◆ Uninstall NOD32 from workstations.

Each new package created in the RAC has its own nod32installer.exe. Internal information in this file is related to the package and RAS.

Address of RA in the files nod32installer.exe is usually defined during the expert installation of the NOD32 Remote Administrator Server product. In case this address was not specified, the file is given a default name – ie: the name of the machine where RAS is being installed.

The file nod32installer.exe can be installed with the following parameters (without slash “/”):

- ▶ **MODE =**  
defines whether it is installation of NOD32 for Windows (value: 1), or uninstall (value: 0)
- ▶ **SERVER =**  
name or IP address of RAS, from which the NOD32 installation package will be downloaded.
- ▶ **PORT =**  
port to which a request for sending NOD32 installation packages will be sent.

Since nod32installer.exe runs in a totally silent mode, and no information about problems with installation is displayed, the installer creates a log that is saved in the file C:\nod32installer.log. It contains information about the most important operations.

At the same time, nod32installer.exe creates a key, HKEY\_LOCAL\_MACHINE\Software\Eset\NOD32 Remote Installer, in the Windows registry. This will prevent repeated installation of the same package, if previous installation was successful.

## Main features and settings in the RA Console

### The Clients window - upper panel

#### Server Name

Shows the name(s) of available servers that RAC is connected to.

#### Clients

Shows the number of clients connected to the particularv server.

#### Oldest Version

Shows the oldest version of the virus signature database installed on client workstation(s).

#### Least Recent Connected

Shows the oldest connection period of client workstation(s).

### The Clients window - lower panel

#### Client Name

Shows the name of the client machine.

#### Primary Server

Shows the name of the server with RAS running, to which the client is connected via their NOD32 Control Center. If it shows another server other than the one which the administrator is currently connected to, then it is as a result of replication.

#### Version

Shows the current version of the virus signature database on the client workstation. If there is an older version on the workstation, the data field is shown in red (default), but it does not inevitably mean there is a problem (eg: in case the workstation has been shut down for a week – it can be indicated in Last Connected).

#### Last Connected

Shows the time since the last connection of NOD32 on the workstation, to the RAS server. According to the settings of the console, 'time' is either Absolute (eg: 12:56:13), Relative (eg: 20 seconds ago) or Regional, according to the regional settings of the server.

#### Last Virus Alert

Shows infiltrations detected by the AMON, IMON, DMON and EMON modules on the chosen client workstation. Once alerts have been checked by the administrator, they can be removed from the list. Right-click on the client and select the Clear "Last Virus Alert" Text option. You can switch to the Alert Log window by double-clicking on the client under the Last Virus Alert column. This will then show details in the new window of virus alerts only appertaining to that client.

### Last Event

Shows any recent events appertaining to this client. Once events have been checked by the administrator, they can be removed from the list. Right-click on the client and select the Clear “Last Event” Text option. You can switch to the Event Log window by double-clicking on the client under the Last Event column. This will then show details in the new window of recent events only appertaining to that client.

### AMON

Shows the status of the AMON module on the client workstation.

### Configuration

Shows if the configuration on the client is ready and indicates the time elapsed since the client connected to RAS.

### OS

Shows the operating system of the client machine.

### IP

Shows the last known IP address of the client workstation.

### Mobile User

If the Mobile User option is turned on, then the workstation will be updated as soon as the machine connects to the RAS (see interval defined by the NOD32 Control Center settings). This attribute can be enabled by the Set ‘Mobile User’ flag option using the right mouse button context menu. It’s recommended to use the Mobile User setting if you connect to the network with a notebook computer. The NOD32 Antivirus System update is performed immediately afterwards.

### New

Indicates clients newly added to the client list. This action simultaneously sets a small red ‘star’ on the PC icon under the Client Name column. By default, the flag is disabled when a new client connects to RAS.

### Comment

It serves for inserting the administrator’s comments (eg: an alternative name of the client workstation). Double-click on the client’s name and in the new window, on the General tab, you can add your brief remarks.

## Context menu options

Right-click on a client to bring up a menu that enables applying of other features to effectively filter events. Most options are self-explanatory, but here are the others:

### Select by 'Client A'

Only records containing the thread 'Client A' in the same attribute (column), where the context menu has been brought up will be selected. The thread Client A will be automatically replaced by the value from the cell, where the context menu has been brought up.

### New Task (more details are found on page 43)

- ◆ Configuration Task - enables a modified configuration to be applied to the client. In fact, as many other clients as required may be included in this task at the appropriate window.
- ◆ On-Demand Scan - enables a NOD32 scan of the client machine. In fact, as many other clients as required may be included in this task at the appropriate window.
- ◆ Update Now - by default, the client will check for virus signature updates every hour. This task will force the client to check for updates (see interval defined by the NOD32 Control Center settings). In fact, as many other clients as required may be included in this task at the appropriate window.

### Add to Group...

This allows you to create 'groups' of clients within your network so, for example, different configuration settings can be pushed to specific groups.

### Request Configuration

If the client is not currently connected to RAS, ie: the machine is switched off, selecting this option will show the configuration is requested in the Clients window in RAC, so that when the client workstation is running again, the message will change to Ready and you can right-click on the client and choose Configuration...

### Configuration...

This will bring up a window called Client Properties and the Configuration tab. You can retrieve a configuration from a remote client workstation to View it or keep the parameters by clicking on Save As... The latter may be useful if the client's configuration is worth keeping and then pushing to other clients in the network or group. Having saved it by giving the configuration a new name, the Configuration Editor will open (in case there are one or two amendments to be made), then go to File > Save and close the Configuration Editor. You will then be returned to the Client Properties window where you can choose New Task. In the next window, choose Select and locate your newly saved configuration, click Next, select the clients you wish to apply the configuration to, click Next, review the task details and click Finish. Within 5 minutes (default) the clients will pick up the new configuration.

### Properties

This will bring up a window called Client Properties and the General tab where you can get an overview of the client's details.

## Practical Examples:

We want only those workstations with some virus event to be displayed: Click the right mouse button in the Clients tab on any of the Last Virus Alert empty cells and choose Select by ' ' from the context menu. Now, in the context menu, select the Hide Selected feature.

We want to display virus events only from the workstations John and Mary: In the Alert Log tab, click the right mouse button on any cell with the text 'John' in the Client Name column. In the context menu, choose Select by 'John'. Now press and hold the CTRL key and, in a similar way, (with the right mouse button and by selecting Select by 'Mary') select 'Mary'. Click the right mouse button and choose Hide Unselected from the context menu. Release the CTRL key. At the same time, together with the left mouse button, you can use the CTRL key to select/unselect chosen items, as well as the SHIFT key to select/unselect a group of items.

## The other windows

### Alert Log

Contains information about infiltrations detected by AMON, IMON, EMON and other modules. Double-click the left mouse button to gain more information about the alert. The displayed information can be filtered too by right-clicking on any column (Module, Object, Virus, etc.) and choose Select by 'xxxx' from the context menu. Now, in the context menu, select Hide Unselected.

---

### Event log

Contains information about an event other than virus alerts. The displayed information can be filtered too by right-clicking on the Event column and choose Select by 'xxxx' from the context menu. Now, in the context menu, select Hide Unselected. Double-click the left mouse button to gain more information about the event.

---

### Scan Log

Contains reports that were performed by the NOD32 on-demand scanner, which was planned in the Tasks tab, or invoked directly on the client computer. Double-click on the client to gain more detailed information about the performed scan, or request for the details if servers in your network are replicated.

---

## Tasks

'Type' – type of task.

'Name' – name of task.

'Date To Deploy' – date and time of assigning to target client computers.

'Description' – note added by administrator to describe the task.

'Configuration' – information about accessibility to current configuration. Double-click on the task to get more detailed information, especially in the Details tab. In the Details tab you can find a list of client computers, which were assigned the task, and current state of the task. This attribute has one of these values:

- ◆ **Waiting** - A task is waiting for RA server to be sent to the target workstation. There can be one or two reasons for this – for example, the client workstation is shut down, or the NOD32 Control Center has made no contact to the RA server yet (by default it connects in 5 minute intervals).
- ◆ **Done** - Task has been assigned to the client computer – the target workstation. It does not necessarily mean that the task has been performed by the target workstation yet.
- ◆ **Pending** - Task is being performed.



## Reports

The Reports tab serves for creation of statistical information. Reports can be planned (for example once a week) or performed on demand (generated on administrator's command). Individual variants of reports can be selected in the menu Report/Type. Report/Style determines graphical layout of the resulting report (NOD32 Scheme is more graphically demanding). In the 'Filter' section you can choose which clients (Target clients), or viruses (Virus) will be included in the report.

Other details can be set by clicking on the 'Additional Settings' button. It applies mostly to data in the heading and in the types of the diagrams used. At the same time, you can filter the client computers according to states of chosen attributes, and you can also choose the format of the output file (HTML,CSV).

In the Interval tab you can define an interval, for which the report will be generated:

- ◆ **Current** - events that took place in a chosen time period – eg: if a report is created on Wednesday, and the interval is set to Current Week, then the events from Sunday, Monday, Tuesday, and Wednesday will be included.
- ◆ **Completed** - Only events that took place in a chosen, closed period will be included in the report. For example, the whole of the last, completed month -- or 2, 3 months, etc. -- a whole week, from Sunday to the following Saturday. If the parameter 'Add also the current period' is active, the period chosen above will also include events from the last closed period until the moment of creating.
- ◆ **From/To** - Use this setting to define a period for which the report will be generated.

### Example:

We want to create a report including events from the last calendar week, ie: from Sunday to the following Saturday. We want such a report to be generated on the following Monday (after Saturday). In the Reports/Interval tab, choose Completed and set 1 Weeks. Remove 'Add also the current period'. In the Reports/Scheduler tab, set Frequency to Weekly and choose Monday. There are further settings you can add, such as the exact time on Monday that the report is generated, where the report goes (save to report database, send by email to a specified recipient or save in a specified folder) and also specify an exact date range that the report will cover.

Click on the Scheduler tab to define and setup an automatic report in chosen time or intervals (Frequency section). Enter the time when the report will be generated to the 'Run at' time field, and in the 'and store the result to' section (press the 'Select Target...' button) specify how and where the report will be exported. The report will be saved to the report database (default - C:\Program Files\ESET\RA\Console\Reports - can be edited by going to RAC > Tools > Console Options... > Paths tab), but can be sent via e-mail to a chosen address, or exported to a folder. A report can be exported, for example, to a folder that is accessible via intranet. Then it can be shared by all employees.

To send generated reports via e-mail, you need to set the SMTP server and sender address (RAC > Tools > Server Options... > Other Settings tab) and enter the server's name (or IP address) plus the sending email address.

To define the time period when generating will be active, go to the Range section. You can define the date of the last report (End by), or the number of generated reports (End after).

To save the settings of a defined report to a template, click on the 'Save' or 'Save as...' buttons. When creating a new template, click on the 'Save as...' button and give the template a name. In the upper part of the console window, you can see names of templates that were already created. Beside the template names, there is information about time/intervals, when the reports will be generated according to the preset data.

Move back to the 'Options' tab and click on the 'Generate Now' button with the relevant template selected to generate a report at any moment, regardless of any preset schedule. This can also be done by right-clicking on your chosen template and choosing 'Generate Now' or going to the toolbar and selecting Actions > Generate Now. Already generated reports can be viewed in the 'Generated Reports>>' button.

With the context menu options you can perform other operations with reports. Favorite templates can be placed in the left window Favorites, and thus you can later immediately generate reports from favorite templates. To move a template to Favorites choose Add to Favorites in the context menu in the list of the scheduled templates.

Following is a list of report types:

- ◆ Top Viruses – list of the most frequently detected viruses
- ◆ Top Clients with most Alerts – list of the most "active" client workstations (by number of detected viruses)
- ◆ Alerts Progress – progress of virus events (number)
- ◆ Alerts Comparative Progress – progress of virus reports by chosen viruses (using filter) compared with the total number of viruses.
- ◆ Alerts By Module – number of virus alerts from the individual NOD32 modules.
- ◆ Alerts By Object – number of virus alerts according to the way they attempted to infiltrate (emails, files, boot sectors).
- ◆ Combined Top Clients/Top Viruses – combination of the above mentioned types.
- ◆ Combined Top Viruses/Alerts Progress – combination of the above mentioned types.
- ◆ Combined Top Viruses/Alerts Comparative Progress – combination of the above mentioned types.
- ◆ Clients Report, Alerts Report, Events Report, Scans Report, Tasks Report – typical reports that can be viewed in the tabs Clients, Alert Log, Event Log, Scan Log or Tasks tab.
- ◆ Comprehensive Report – summary of these types:
  - Combined Top Clients/Top Viruses, Combined Top Viruses/Alerts Comparative Progress and Specified Alerts Progress.

## Remote Install

This tab offers several variants of remote installation of the NOD32 Antivirus System on workstations and related features. More detailed information has already been covered on pages 33 to 42.

---

### RA Configuration of License keys (.LIC files)

NOD32 Remote Administration (or NOD32 Enterprise Edition package) is delivered with a license key – nod32.lic. After installation of RAS and RAC, the key must be copied into the folder C:\Program Files\Eset\RA\Server. The license key file must always have .lic extension. The license file contains information about the expiry date and the number of clients allowed to connect to NOD32 Remote Administrator. The license file in fact determines functionality of NOD32 Remote Administrator as a product. RAS reads information from the nod32.lic file when starting the nod32ra.exe service. If there are more license keys in the folder C:\Program Files\Eset\RA\Server, then RAS will choose the most appropriate (more detailed information can be found in the file nod32ra.log). If the license key has expired, NOD32 Remote Administrator will run in demo mode, ie: number of clients will be limited to two. If there are more clients than is defined in the license key (purchased), only a limited number of clients, corresponding with the defined number, will be displayed. Note: Should you have any problems with application of license keys, please look in the file C:\ProgramFiles\Eset\RA\Server\nod32ra.log where you can find the exact reason for the failure.

---

### RAC (Console) connection to RAS (Server) setup

More detailed information has already been covered on page 14.

Further setup details are found by going to Tools > Console Options Columns - Show/Hide -- Here you can define, what attributes should be displayed in individual console tabs.

#### Colors tab:

Here you can define what colors will be assigned for what events.

- ◆ Clients: Previous Version – color for previous virus signature database (compared with current)
- ◆ Clients: Older Version or N/A – color for older virus signature database (compared with current), or color for unknown database.
- ◆ Clients: Last Connected – color for client which was not connected for the longest time. You can also define the time interval for what constitutes the last connection.
- ◆ Clients: Last Virus Alert – color for last virus event.
- ◆ Clients: Last Event – color for last event – other than virus event.
- ◆ Clients: AMON Stopped – color assigned to client with AMON turned off.
- ◆ Event Log: Diagnostic – color for events classified as “Diagnostic”.
- ◆ Event Log: Warning – color for events classified as “Warning”.

**Paths tab:**

Here you can specify a directory to which the console will locally save reports downloaded from RAS. By default, it is C:\Program Files\ESET\RA\Console\Reports.

**Date/Time tab:**

Appearance of the date/time columns.

Time display format.

- ◆ Absolute – console will display absolute time (eg: 14:30:00).
- ◆ Relative – console will display relative time (eg: 2 weeks ago).
- ◆ Regional – console will display time according to regional settings (taken from the Windows settings).
  
- ◆ Recalculate UTC time to your local time (use local time) – Check this checkbox to recalculate to your local time. When you check this option, all time values will be shown and taken as UTC (Universal Time Coordinated, also known as GMT - Greenwich Mean Time) time values. This does not refer to reports scheduler - that is in the server's local time.

**Other settings tab:**

Filter settings - 'Auto Apply Changes' allows all settings in the filter pane, except the server & client names, to be applied automatically if changed.

Other settings:

Use automatic refresh – automatic data refresh in a current folder and in chosen interval.

Empty console recycle bins at application exit – click to remove items from internal recycle bin of the console after finishing working with it. You can select it in the Reports tab.

Show gridlines – click to separate all individual cells of all tabs by gridlines.

Use systray icon – console will be represented by a Windows system tray icon.

Show on taskbar when minimized - console will be represented by an icon/tab on the taskbar.

Use highlighted systray icon when problematic clients found – use this option, together with the Edit button to define events, which will trigger a change of the systray icon color. So if, for example, you minimize the RA console program, by the change of the icon color, you will see that a new problem has occurred.

## RAC server options setup

Further setup details are found by going to Tools > Server Options

### General

Shows general information about the server's name, the port that RAC is using to connect to RAS (default is 2223), the version of RAC/RAS that's installed, who NOD32 Remote Administrator is licensed to, the number of clients that may connect to RAS, the expiry date of the license, the current NOD32 virus signature database version installed on the server, the date & time currently observed by the server, the time zone and the uptime since the server has been running.

If you want to set a password when connecting RAC to RAS, or change an existing password, there is a 'Change Password...' button. By default, the password is blank.

When renewing your license, there is a 'Renew License' button, which will help you to locate the new nod32.lic file and upload it to the server without the need to have to restart the NOD32 Remote Administrator Server service manually.

### Database Maintenance

- Only keep the latest XX events for each client – enables archiving of last XX events by each client.
- Only keep the latest XX scan logs for each client – enables archiving of last XX scan logs by each client.
- Delete clients not connected for the last X months - this will completely delete clients who have not connected within the specified time interval.
- Delete alert logs older than X months.
- Delete event logs older than X months.
- Delete scan logs older than X months.
- Clean up scheduler - Clean up every XX minutes – sets the frequency of the above mentioned processes.
- Clean Up Now button – older records will be deleted (according to the settings).
- Compact & repair scheduler - when compacting the database, the server is in maintenance mode and does not serve any clients. This may take a few minutes. The scheduler's time is in the server's local time.
- Compact Now button - will invoke compacting regardless of the scheduler.

### Logging

'Enable logging' – enables logging of the RAS activity to a chosen file (Log filename) and setting of verbosity of the information (Log verbosity):

1. Only critical errors of server as a whole.
2. As above plus includes errors in communication between server and clients (Sessions). This is the default installation level.
3. More detailed report of most of the activities; including time and date of all individual connections of console (connection/end of session).
4. Including NOD32 Installer connection reports.
5. Most detailed report (debug mode). We recommend using this when having problems in communication between clients and RAS, or when having problems with replication. Often you can find here the exact reason of any failure.

You can rotate logs when, by default, they reach 512MB in size and delete them when they are so many days old (default is 90 days). Plus there is a 'View' button to instantly view the most recent log details. Also, there are options to 'Log to OS application log' and a 'Database Debug Log'.

## Replication

### Replication "to" settings

Enable "to" replication – allows replication, as described in the chapter "Installation for a multi-site network" (page 70).

Replicate Up Now button – will perform an immediate replication to the chosen upper server.

Upper server – (IP or DNS) address of parent RAS, to which data will be copied from the child RAS. (screenshot)

Replicate every XX minutes – interval of replication.

Replicate alert log, event log and scan log plus client configuration details -- the check boxes enable defining of log types (alert, event, and scan), which can be replicated (transferred) to a parent server on the administrator's demand, and, in the right-hand section, whether it is to happen automatically (Automatically replicate alert or scan log details).

Automatic log replication does not inevitably have to be active – the administrator can ask for them from a child server.

### Replication "from" settings

Enable "from" replication – Check this option to define RAS child servers (their names) in the 'Allowed servers' dialog box, from which RAS will receive requests for replication. If you use more servers, please separate their names by commas. RAS can also be configured directly with the file nod32ra.ini. Replication takes place on TCP port 2846.

## Other settings

**SMTP settings** - enter the mail server's name (or IP address) plus the sending email address. These details should appear automatically when installing RAS and RAC.

**Allow new clients** – Clients are, by default, added to the list (the Clients tab in console) automatically at the moment when RAS registers the first attempt to establish connection from a new, so far unregistered client module of NOD32 Control Center. Checking this option enables automatic adding of new clients to the clients list. If you leave this option unchecked, automatic adding will not be enabled. This setting does not apply to new clients which were added to the clients list from 'child servers' by replication.

**Automatically reset "New" flag by new clients** – defines whether a newly added client will be marked by the attribute 'New' or not.

**Ports** - shows the correct, default port settings - 2223, RAC connects to RAS; 2222, NOD32 client connects to RAS; 2846, child servers replicate to this server on this port.



## How to use the console more effectively:

Press F5 to refresh RAC.

In a larger network, with more workstations, these features will come in handy: Selection of more records can be performed, for example, by pressing the CTRL key and left clicking on the selected items, or in a similar way, but with the SHIFT key. Press the key combination “CTRL” and “A” to select all workstations.

Groups - Individual clients can be placed in groups using the Edit > Groups feature from the console menu. Placing into groups can be used to filter or to create tasks, since the tasks can be applied to the whole group. The groups are independent of each server – they do not replicate.

Filter - Filter is used to display only records that are important for the administrator to know. Filter can be enabled by the option View > ‘Show/Hide Filter Pane’ in the console menu. To activate a filter, check the ‘Use Filter’ checkbox and click the Apply Changes button to start the filtering. In the first section – ‘Computer filter criteria’ - you can filter servers/clients in several ways:

- ◆ Only clients (whole word) – Only those clients whose name corresponds to a word thread you typed in will be included in the output.
- ◆ Only clients like – Only those clients whose name contains a thread you typed in will be included in the output.

In the next section, you can limit filtration by the Groups division.

- ◆ Clients in Groups – In this case, only clients belonging to defined groups will be selected.
- ◆ Clients in other Groups or N/A - Only clients belonging to other than chosen groups, or not belonging to any group will be included in output. If a client belongs to some of the chosen groups, but also in a group that was not selected, then this client will also be included in output.
- ◆ Clients in no Groups - In this case, individual clients will be selected.

The other filter settings differ depending on the active tab, but mostly it is only a variation of the time filter that can limit outputs only to records that were created in a certain time period.

Export Data from the tabs Clients, Alert Log, Event Log, Scan Log and Tasks can be (even after filters have been applied) exported to a file using the option Export... in the File menu. Or alternatively, by the option Export Selected... – only selected records will be exported. Data can be exported to different file extensions. We recommend exporting to an HTML or to a CSV file (the file can be edited, for example, in MS Excel after that), where individual attributes are separated by commas (comma delimited) or by semicolons (semicolon delimited).

### Print

Similarly, data from the tabs Clients, Alert Log, Event Log, Scan Log, Tasks can be printed. First of all, configure page setup in the menu File > Page Setup. In the section Mode you can choose, whether the page will be printed in mode WYSIWYG (“what you see is what you get”), or in grayscale. In the section Tables also choose whether eventual graphics will be printed (PC symbols, etc.) To set page headers and to browse and enable printing of a logo (eg: of the company) go to Headers and Footers. Click Preview to view the final appearance of the page (as well as with the option Print Preview in the menu File).

### Deleting unnecessary data

To effectively remove old and unnecessary data in the tabs Alert Log, Event Log, Scan Log, and Tasks, choose the Edit > Delete special... option. Click the ‘Specify Date’ button to define what data should be removed.

### Maintenance and backing up of NOD32 Remote Administrator Server

We recommend keeping the RAS database up to date and deleting old records in order not to overburden the system unnecessarily. It applies mostly to data in the “Alert Log” tab. To delete unnecessary data, use the feature described in “Deleting unnecessary data”.

### What is relevant to saving information

All data is saved in the file nod32ra.mdb, which is usually located in the folder C:\Program Files\Eset\RA\Server. It can be stored in case of server failure (when saving, please stop the NOD32 service – required). Details from individual logs (for example NOD32 on-demand scanner logs) are stored into the subdirectory Storage (C:\Program Files\ESET\RA\Server\storage). Also client configurations and reports in xml extensions can be found there.



# Possible problems & error codes

## Error messages

As with most reputable software, NOD32 Remote Administrator can return more detailed information about a problem that has occurred.

The error message is, in many cases, accompanied with its SC error code and GLE error code.

SC codes mostly contain only internal information for easier orientation in the problem code, GLE codes (Get Last Error) are more important for the user. These are classic “Win32 Error Codes” – a list of such codes can be found on this webpage:

[http://msdn.microsoft.com/library/default.asp?url=/library/en-us/debug/base/system\\_error\\_codes.asp](http://msdn.microsoft.com/library/default.asp?url=/library/en-us/debug/base/system_error_codes.asp)

### Following are some commonly found errors:

**Problem:**

During remote installation, the error “Could not set up IPC connection to target computer (SC error code 6, GLE error code 1326)”

The GLE error means that a wrong or unknown password for the account (under which remote installation was to take part) was entered.

---

**Problem:**

Quite often you can come across this message caused by the nod32installer.exe: “NOD32 Installer was told to quit by the server XYZ.”

It means that installation on the chosen client workstation was already performed (successful or not) and RA refuses to repeat it.

**Solution:**

This message keeps on occurring until the administrator deletes the message related to the workstation in the Remote Install tab from:

- ▶ the bottom of the ‘List of pending and failed installations’ panel or
- ▶ the ‘Successful Installs List’ tab.

You can right click on the specific client and select ‘Clear’.

---

**Problem:**

The error message “NOD32 Installer could not connect to server XYZ” means that RAS is not accessible to the file nod32installer.exe.

**Solution:**

It is recommended to check, whether XYZ can really be localized in the network (eg: by ‘pinging’ XYZ), or whether the communication is not blocked by a firewall.

**Problem:**

Especially with MS Windows XP, you can come across other, already mentioned, problems connected with the option 'Use simple file sharing'. In this case, the error 'Access denied' may appear when using the 'Get Info' option during the Push install process.

**Solution procedure:**

- ▶ Click on Start, and then on the icon My Computer
- ▶ From the toolbar, click on Tools and choose Folder Options
- ▶ In the View tab, uncheck the option 'Use simple file sharing'

*Note: Windows XP Home Edition does not support disabling of the Simple file sharing option. That is why it is not possible to install NOD32 remotely to this platform.*

---

**Problem:**

Windows XP Service Pack 2, contains a built-in firewall. The firewall, if turned on, blocks the NOD32 installation package sent to a workstation.

**Solution:**

To solve the problem, enable File and Printer Sharing in the Windows firewall.

**Solution procedure:**

- ▶ Click on Start, then click on the Control Panel icon
  - ▶ Select Windows Firewall
  - ▶ In the Exceptions tab check File and Printer Sharing
- 

**Problem:**

The user account that is being used to authorize access for the Windows XP workstation has no password.

**Solution:**

The Windows security rules do not allow remote install through a user not using a password.

**Solution procedure:**

To authorize access to the workstation where NOD32 is to be installed remotely, create a new user account with a password. Or assign a password to the existing user account.

**Problem:**

During remote installation, the error “Could not retrieve required information from target computer (RES error code 14, GLE error code 997)” may occur.

This problem occurs in some cases if an installation takes place from NOD32 Remote Administrator Server which is located on a Windows 2003 Server system, and NOD32 is installed on a Windows 2000 operating system.

**Solution:**

The system account, from which the NOD32 Remote Administrator service is started, does not have the right to install. To solve the problem, start the NOD32 RAS service from the Administrator’s user account.

**Solution procedure:**

- ▶ click on Start > Settings > Control Panel > Administrative Tools > Services
- ▶ right click on the NOD32 Remote Administrator service, and from the context menu choose Properties
- ▶ choose This Account from the Log On tab and insert “Administrator”
- ▶ click OK to close the window
- ▶ click right mouse button on the NOD32 Remote Administrator service and choose Restart from the context menu

After the installation succeeds, we recommend switching the NOD32 Remote Administrator service back to the default setting (local system account).

## Possible error messages produced by the NOD32 workstation

The following error messages can be produced directly by the installer, which is used with all Eset MS Windows based products (ie: the installer launched by the file SETUP.EXE, or after running the installation file downloaded from the Eset website).

Error	Meaning
101	administration rights required
102	no configuration file specified
103	lack of memory
104	old version of the Operating System
105	cannot create a temporary folder to extract the installation files
106	error extracting files
107	internal program error
108	attempting to overinstall with an older component
109	internal program error
110	internal program error
111	cannot create a file on the disk
112	internal program error
113	internal program error
114	SETUP.XML corrupt or missing
115	the current version not compatible with the old version (you need to uninstall the old version)
116	error writing to the operating system registry
117	upgrade required
118	attempting to overinstall with a different language version (uninstall the previous version first)
119	corrupt uninstall file
120	registering service error
121	component installation error
122	cannot install a certain component to the computer
123	attempting to install the trial version again error
124	wrong Operating System, the installer is intended for the Windows NT/2000/XP/2003 Operating System
125	wrong Operating System, the installer is intended for the Windows 95/98/ME Operating System

To find out the exact reason why the installation failed, run the install file (ie: the SETUP.EXE file) from a command prompt or using a File Manager with the /TEST parameter (ie: SETUP.EXE /TEST). The detailed description of the installation process will be saved in an **nsetup.log** file which can be located in the same directory as SETUP.EXE (ie: normally, C:\Program Files\Eset\Install)

# Installation

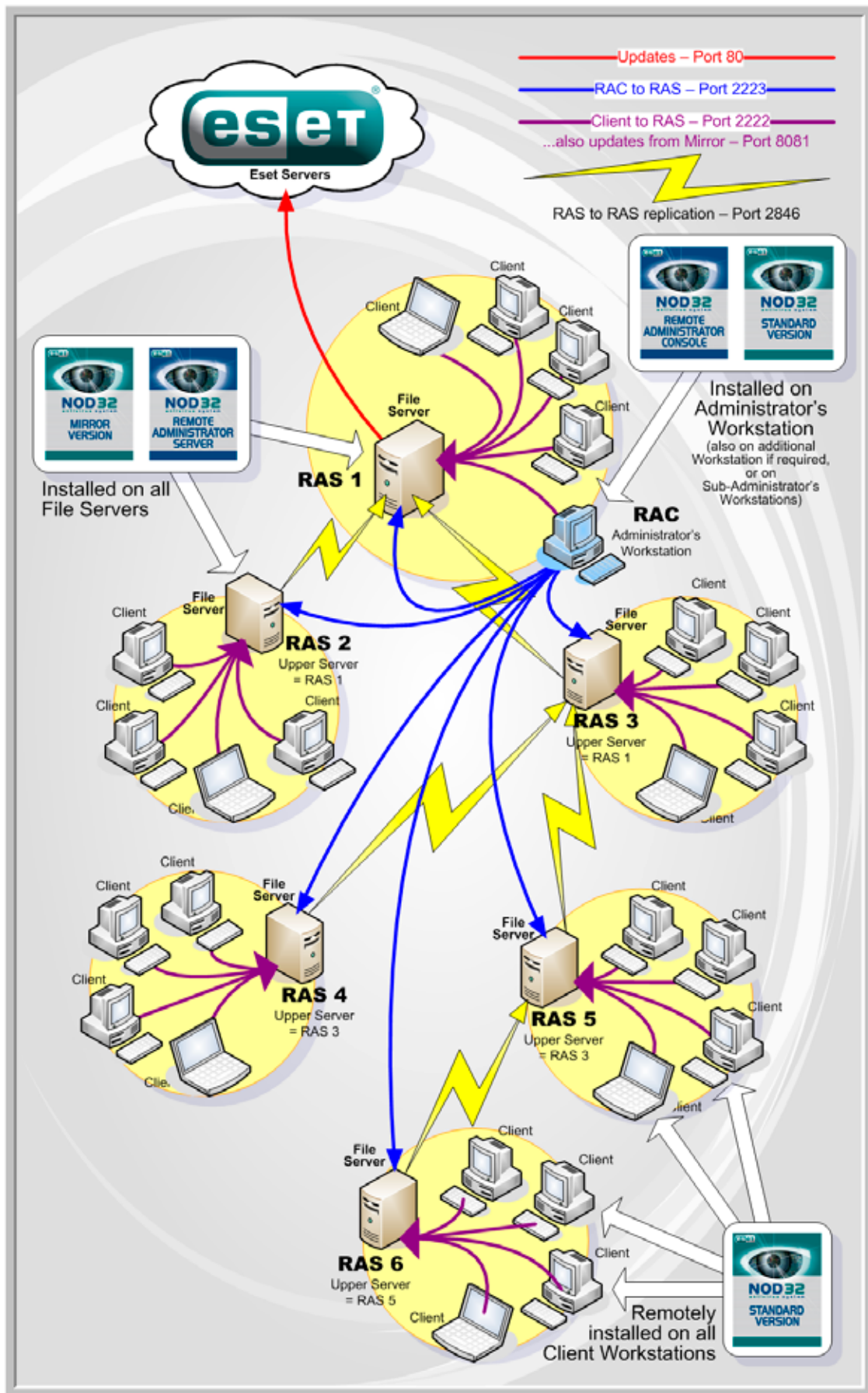
## for a multi-site network

## Installing NOD32 in a multi-site network

In large networks, you can install more RA servers for easier manipulation. The servers would create an imaginary structure. The burden connected with communication with client workstations and RAS can be distributed. This way you can also define sub-administrators who will control only a group of client workstations. All transfers between servers are encrypted.

A company department network is an example of a sub-network. It is recommended to install RAS for each department, controlling client computers only within its own network, as seen in the illustration on the following page.

If, from the point of view of replication, RAS 1 will be set as the main (root) server, then all the other servers are controlled by it. According to the figure, RAS 3 is superior to RAS 4, RAS 5, and RAS 6, as well as RAS 5 is superior to RAS 6 (superior = 'upper server' in the scheme).





Networks consisting of superior / inferior RAS servers allows the administrator to only control those client workstations that can be momentarily accessed by RAS (using RAC) and eventually can control clients connected to inferior RA server(s).

So if the administrator connects using RAC to RAS 3, he/she will be able to control client workstations connected to RAS 3, RAS 4, RAS 5, and RAS 6. If the administrator connects to RAS 5, he/she will be able to control RAS 5 and RAS 6. And if he/she connects to RAS 1, he/she will be able to control all workstations of course.

It leads to another idea – you can use more administrators to control only partial groups of client workstations (and which are connected to a certain RAS and to RA servers inferior to it).

What information will be retrieved from the client workstations connected to inferior RA servers is configured in the replication setup.

Replication is nothing other than a communication of RAS with superior RA servers. Its specific features are described in the chapter called 'More detailed information' on page 47, about the RA server setup.

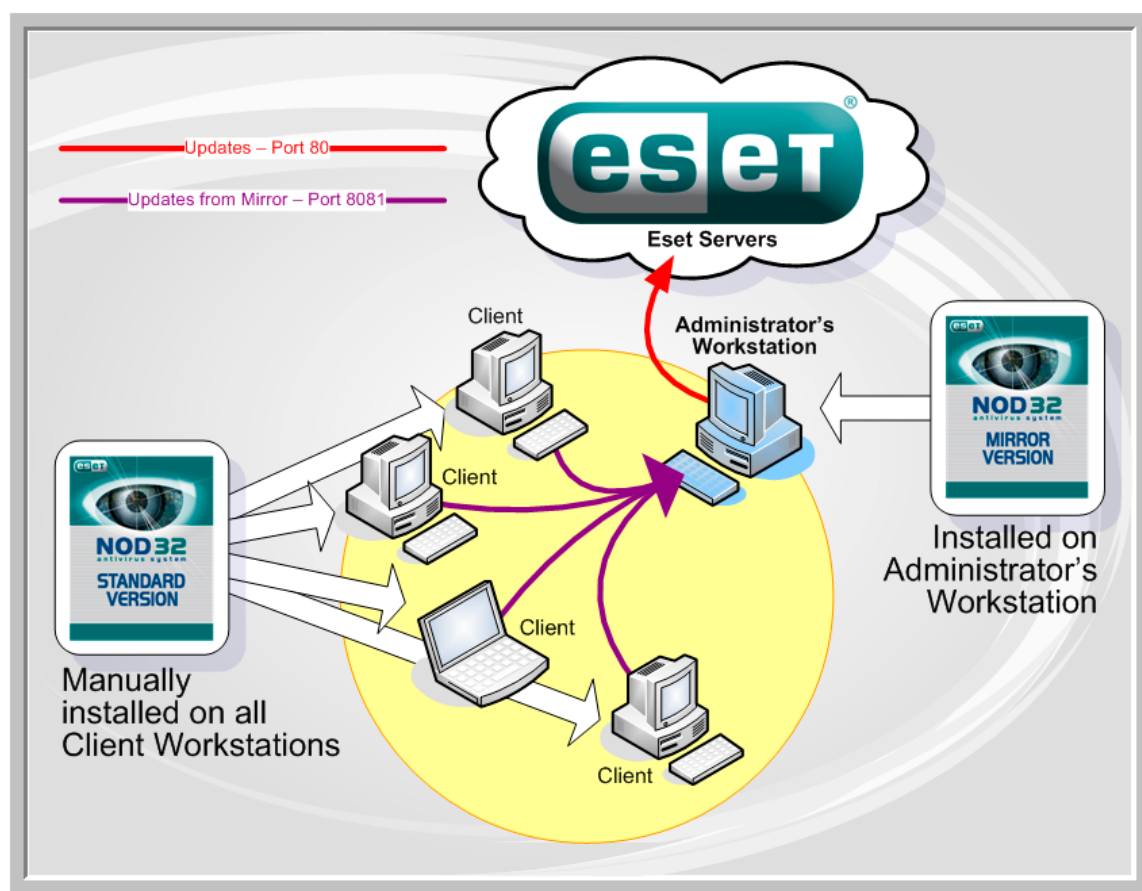
## Mirror servers replication

This is not directly connected to NOD32 Remote Administrator, but it is recommended to also replicate updates on local mirror servers. Updates from the server can be distributed not only to the target workstations, but also to inferior servers – they will send them to workstations they control, as per the illustration on page 72.

# Installation


for a small office network

## Installing NOD32 in a small network



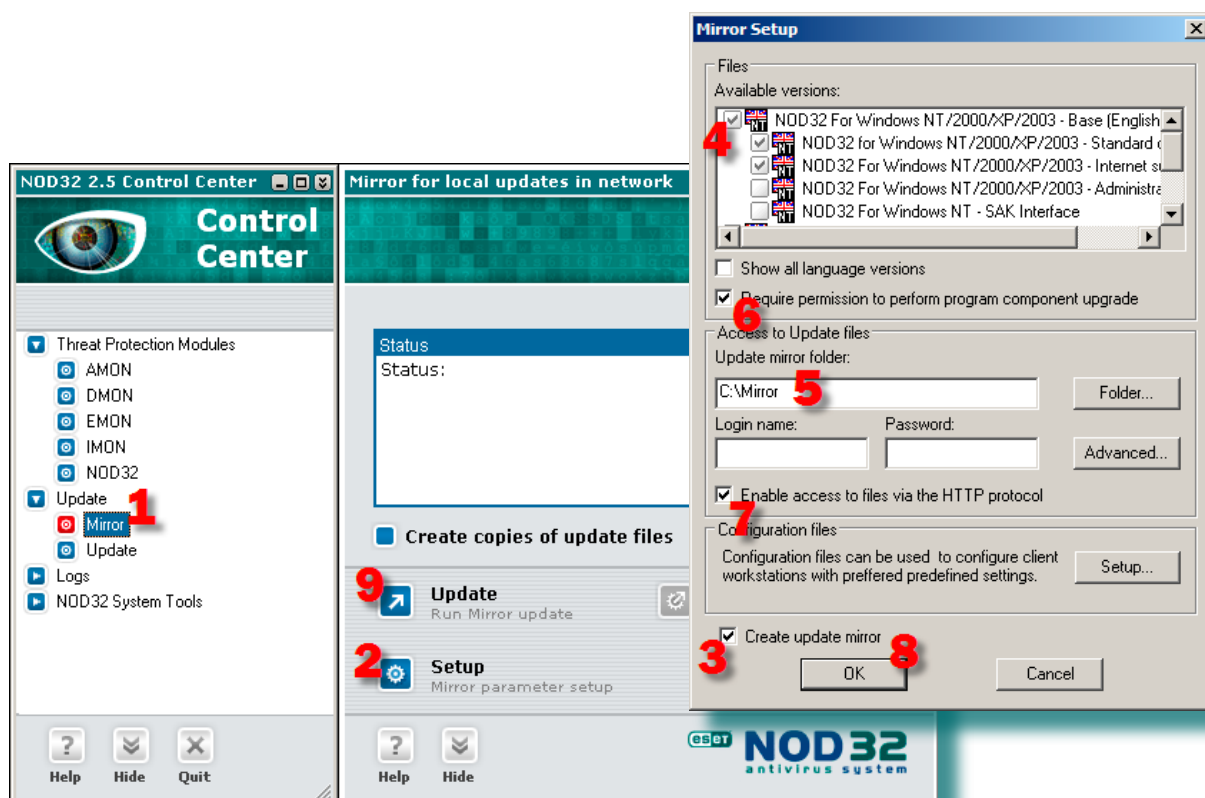
Here are the basic, recommended steps to take when setting up a Mirror for NOD32 in a small network of less than 10 workstations (for example):

- ▶ Using your Username and Password, download and install NOD32 LAN Update Server (Mirror) version onto the machine that will always be connected to the internet, at least through the working day, and will therefore receive the virus signature updates from Eset automatically. The correct version should either be for Windows 95/98/ME or Windows NT/2000/2003/XP. Check out this machine's operating system before you download.
- ▶ For Windows NT/2000/2003/XP/Vista, 32 or 64 bit: <http://www.eset.com/download/balance.php?dir=/download/win/v2ad/ndntenad.exe>
- ▶ For Windows 95/98/ME: <http://www.eset.com/download/balance.php?dir=/download/win/v2ad/nd98enad.exe>
- ▶ Its virus signature database will form the basis of a Mirror for the client workstations.
- ▶ For detailed instructions on downloading and installing NOD32 LAN Update Server (Mirror) version (which is the same as installing the Standard, single-user version) please click here: <http://download1.eset.com/manuals/StandardInstallGuide.pdf>

- ▶ Save the download and then run the installer by double-clicking it. It's recommended to follow a 'Typical' installation – you can alter your settings later if you wish. Whether from a CD or from a download, the installation instructions from this point are the same.
- ▶ Once installed and you have rebooted your PC, NOD32 will automatically update within one hour. However, you can press 'Update now' immediately. You should then create a Mirror on this machine. Click this icon once  in the system tray, which will open the Control Center.

The items 1 to 9 below are illustrated in the screenshot on the next page:

1. Click 'Mirror'
  2. Click 'Setup'
  3. Tick 'Create update mirror'
  4. Tick the 'Available versions' you require for your network. ie: WinNT machines and/or Win9x machines. All versions that will be running on the workstations should be checked.
  5. Setup a path to the Mirror on your server. You can choose to create this folder anywhere you wish, but it's recommended to keep the path reasonably short (ie: C:\Mirror or C:\NOD32\Mirror or C:\Program Files\Eset\Mirror)
  6. Tick 'Require permission to perform program component upgrade'. Besides the virus signatures database update, a license also includes program updates – program component upgrades, which require a restart of the operating system and bring a lot of new features and improvements to NOD32 (it is an upgrade to a completely new version, eg: from 2.0 to 2.5). Choose this to ensure that the program component upgrade will **not** be applied to a local update server immediately it is available on the servers of the Eset company. NOD32 on the workstations will remain in the current version, and the workstations will only accept virus signatures updates from the mirror. It is up to the user to consider this option, especially since before updating all workstations in the network, the new version may be tested in a detached network dedicated to testing.
  7. Tick 'Enable access to files via the HTTP protocol'
  8. Click 'OK'
  9. Click the 'Update' button to update your newly created Mirror, since there may be more components mirrored than are used by the local system.
- ▶ If you would prefer a Shared Folder Mirror path, when entering it, please use the UNC path. Let's assume that the shared folder is named NOD32NET and is located on the MAIN server. Then enter the path in this form: **\\MAIN\NOD32NET**



## Distributing a configuration

Using a local update server – Mirror – you can also distribute a configuration for NOD32, by which the workstations will be configured at the next attempt to update. In order to automatically distribute a configuration, set the update server on the workstations to **http://IP\_address\_of\_your\_server:8081** (if it is the version with an HTTP server) or to **\\MAIN\NOD32NET** (if it is the version with a shared folder).

Place the configuration XML file on the server. The configuration itself is created on the same PC where the mirror is created. Click on the Mirror button in the Update section in the NOD32 Control Center, and then click on the Setup button. In the Mirror Setup dialog window, click on **Setup** in **Configuration files**. After clicking on the Setup button, select **Add**, then **New** and create a new configuration file. Save the new configuration file anywhere on the local disk, EXCEPT for the folder that holds the Mirror.

After this is done, the application **NOD32 Configuration Editor** is launched (see page 17 for more details). After required changes are made, save them by clicking on the diskette in the upper part of the window. Then just close the window and click **OK** to return to the NOD32 Control Center.

Now, by clicking on the **Update** button in the Mirror for local updates section, the configuration file will be generated in the folder with the Mirror. The presence of the configuration file in the update folder / mirror will ensure, that the workstations will, besides downloading updates, apply this configuration also.

## Creating a common configuration

If you are manually installing NOD32 onto workstations, you can setup a configuration that the workstations in your network can all use, which could save a lot of time configuring each machine later:

- ▶ On your machine (assuming that is where NOD32 LAN Update Server [Mirror] version is installed), go Start > Programs > Eset > Configuration Editor.
- ▶ This will open a default configuration window which you can then adjust the settings to suit your needs.
- ▶ The most significant section is under **UpdateProfile(My Profile)\Settings** where the internet connection type must be selected and the update server must be specified, ie: the name or IP address of your machine (where the Mirror is). The Username and Password should remain blank as the clients are updating locally from your machine.
- ▶ More details about using the Configuration Editor can be found on page 17.
- ▶ More details about creating a secondary update profile for clients with laptops that are taken away from the office regularly, can be found on page 30.
- ▶ Save this configuration to your desktop as **nod32.xml**
- ▶ Next download from the Eset website, using your Username and Password, and save to **your** desktop, the version(s) of NOD32 that you will be installing on your client's PCs. Do not run the installer(s).
- ▶ Next, right click on the installer and choose 'Extract to...' or 'Extract files...' (will depend on the archiving program you use). Choose to save the contents to a new folder on your desktop. Name the folder 'NOD32 Install' or any special name you wish, but for this explanation, I'll use '**NOD32 Install**'.
- ▶ In that folder, **add** the **nod32.xml** file that you've just created.
- ▶ Now while inside the **NOD32 Install** folder, create a new text document (Notepad) and type the following text line into it:

**setup.exe /instmf /silentmode /forceold /reboot /showrestart /cfg=nod32.xml**

(Pay close attention to where the spaces are, or better still, copy and paste from this document). A full list of the installation command switch options are on the next page.

- ▶ Rename that text document to **setup.bat**
- ▶ Copy the **NOD32 Install** folder onto a CD, flash key or any removable media capable of storing this folder which will be around 9MB in size.
- ▶ Insert the CD or flash key on the first target PC, open the **NOD32 Install** folder and double click the batch file **setup.bat**
- ▶ This will only take a few seconds and the PC will reboot and start collecting updates from the Mirror on your machine automatically.
- ▶ Run the **setup.bat** file on each machine in your network.

For detailed installation instructions on a single PC, please refer to the Standard Installation Guide available for download from our website (<http://download1.eset.com/manuals/StandardInstallGuide.pdf>).

## Installation command switches

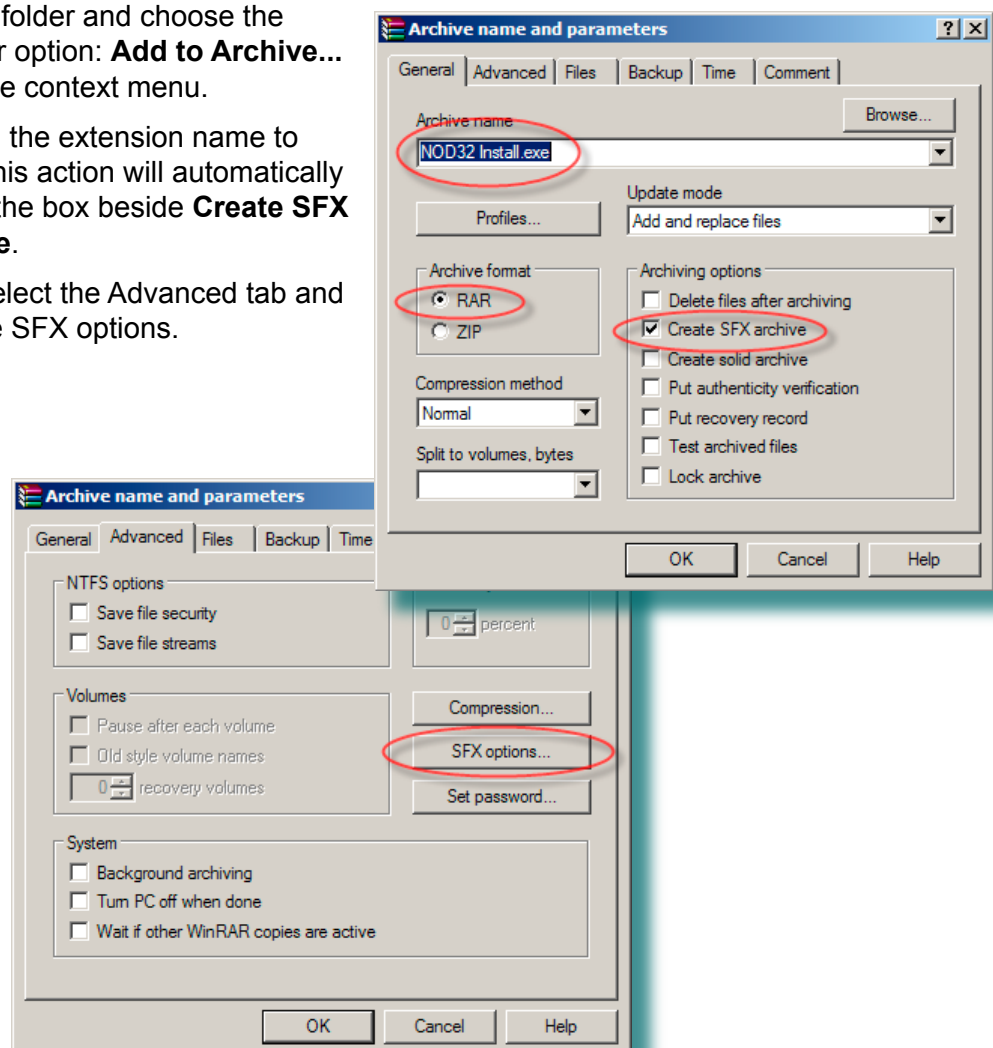
<b>/INSTMFC</b>	this parameter turns on installation of MFC libraries – if it is necessary – without asking. The MFC library must be located in the same directory as SETUP.EXE. The installation program will check whether there are newer libraries in the system (or none) and will proceed with the installation accordingly.
<b>/SILENTMODE</b>	a mode without dialog windows – silent installation.
<b>/REBOOT</b>	after a silent installation is complete, the PC is not restarted by default, even though it may be required. Using this parameter will switch the restart option on.
<b>/FORCEOLD</b>	will install an older version of NOD32 over an existing version, without providing a popup warning to the client (must be used in conjunction with /REBOOT).
<b>/CFG=</b>	switch with a configuration name (if this parameter is not present, NOD32.XML is used by default).
<b>/SETTINGS=</b>	name with obligatory SETUP.XML file (entered only if SETUP.XML is not present in the installation folder, or has a different name).
<b>/TEST</b>	installation creates NSETUP.LOG, where the process of installation is described in detail.
<b>/PWD=</b>	entering password for uninstall. This is important in case a current version of NOD32 is protected by a password, and the administrator intends to reinstall in silent mode.
<b>/NUP=</b>	if the value of this parameter is set (name of the file with component), the installation does not require SETUP.XML for the whole installation, but you can install only one component.
<b>/UNINSTALL</b>	uninstall of existing installation.

The switches with “=” require entering of a thread. It can be put into quote marks, but does not have to. Quote marks are obligatory only if the thread contains spaces.

## Creating a self-extracting installer

This will require an archive program like WinRAR which is capable of producing self-extracting installers:

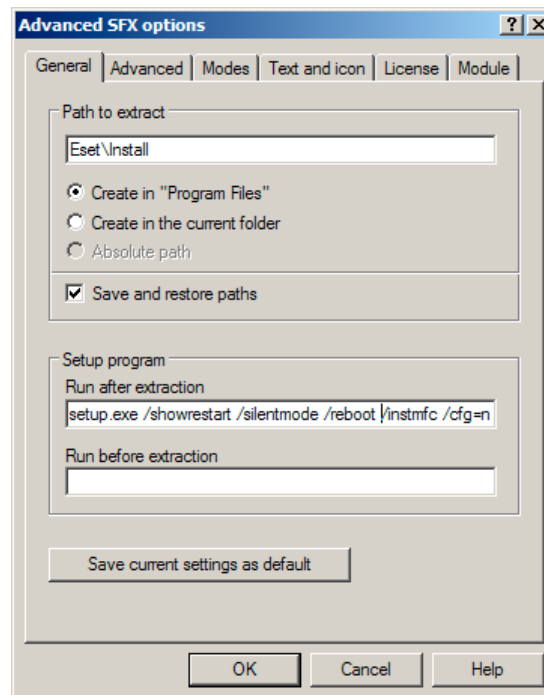
- ▶ Follow the steps as described on page 78 (“Creating a common configuration”) regarding downloading the standard NOD32 version(s) and creating your desired settings using the Configuration Editor.
- ▶ Save your configuration as **nod32.xml**
- ▶ Next download from the Eset website, using your Username and Password, and save to **your** desktop, the version(s) of NOD32 that you will be installing on your client’s PCs. Do not run the installer(s).
- ▶ Next, right click on the installer and choose ‘Extract to...’ or ‘Extract files...’ (will depend on the archiving program you use). Choose to save the contents to a new folder on your desktop. Name the folder ‘NOD32 Install’ or any special name you wish, but for this explanation, I’ll use ‘**NOD32 Install**’.
- ▶ In that folder, **add** the **nod32.xml** file that you’ve just created.
- ▶ Now right-click on the **NOD32 Install** folder and choose the WinRAR option: **Add to Archive...** from the context menu.
- ▶ Amend the extension name to **.exe** This action will automatically check the box beside **Create SFX archive**.
- ▶ Now select the Advanced tab and choose SFX options.



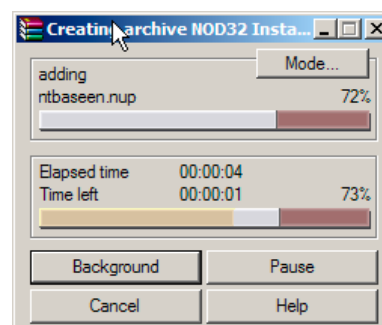


- ▶ In the **Run after extraction** text box, you can enter any additional command switches to be run after the installer is extracted. For example:

**setup.exe /instmfc /silentmode /forceold /reboot /showrestart /cfg=nod32.xml**



- ▶ Click OK, and OK again, and the installer will be created.
- ▶ Copy the **NOD32 Install.exe** onto a CD, flash key or any removable media capable of storing this folder which will be around 10MB in size.
- ▶ Insert the CD or flash key on the first target PC and double click the **NOD32 Install.exe**
- ▶ This will only take a few seconds and there will be a prompt to reboot. When the PC restarts, it will start collecting updates from the Mirror on your machine automatically.
- ▶ Run the **NOD32 Install.exe** on each machine in your network.



# Additional information

## Command Line Parameters

Here is a list of the Command Line parameters and their effects:

Many parameters are enabled or disabled with a plus (+) or minus (-) sign. For example, to enable the scanner self-check, use **/selfcheck+** , to disable it, use **/selfcheck-**

### General:

- ▶ **/help** Display the list of program switches
- ▶ **/selfcheck+ (-)** Self-test enable (disable)
- ▶ **/expire+ (-)** Enable (disable) the program expiration notice
- ▶ **/subdir+ (-)** Enable (disable) the sub-directories scanning
- ▶ **/sound+ (-)** Sound warning enable (disable)
- ▶ **/list+** Create the list of all tested objects in the Log
- ▶ **/list-** Include in the Log only the objects infected
- ▶ **/break+ (-)** Enable (disable) testing intermission
- ▶ **/scroll+ (-)** Enable (disable) Log scrolling
- ▶ **/quit+ (-)** Quit/do not quit the program after scanning

### Detection:

- ▶ **/pattern+ (-)** Enable (disable) testing using virus signatures
- ▶ **/heur+ (-)** Enable (disable) heuristic analysis
- ▶ **/scanfile+ (-)** Enable (disable) scanning of files
- ▶ **/scanboot+ (-)** Enable (disable) boot sector scanning
- ▶ **/scanmbr+ (-)** Enable (disable) master boot record (MBR) scanning
- ▶ **/scanmem+ (-)** Enable (disable) scanning memory
- ▶ **/arch+ (-)** Enable (disable) scanning archives (ZIP, ARJ and RAR)
- ▶ **/sfx + (-)** Enable (disable) scanning self-extracting archives
- ▶ **/pack+ (-)** Enable (disable) scanning runtime-packed files internally
- ▶ **/mailbox+ (-)** Enable (disable) scanning mailboxes
- ▶ **/adware** Enable detection of adware, spyware and riskware
- ▶ **/unsafe** Enable detection of potentially dangerous applications
- ▶ **/unwanted** Enable detection of potentially unwanted applications
- ▶ **/local** Scan all local non-removable media
- ▶ **/network** Scan all network disks
- ▶ **/ext=<LIST>** Add a new extension to the list of scanned files. (multiple entries are permitted, e.g., /ext=EXT1,EXT2)
- ▶ **/all** Scan all files

### Heuristic analysis:

- ▶ **/ah** Enable advanced heuristics
- ▶ **/heur+ (-)** Enable (disable) standard heuristics

**Log:**

- ▶ **/log+ (-)** Enable (disable) log file creation
- ▶ **/wrap+ (-)** Enable (disable) wrapping text in log
- ▶ **/logappend** Enable (disable) appending to log file
- ▶ **/logrewrite** Enable rewriting of the Log file
- ▶ **/logsize=N** Set Log file to a maximum size of N KB
- ▶ **/log=<FILENAME>** Set the Log file name (e.g.: /log=NOD.LOG)

**Cleaning:**

- ▶ **/cleanmode** Enables cleaning mode (the actions taken will depend on the action settings)
- ▶ **/clean** Clean infected objects (if applicable)
- ▶ **/prompt** Prompt for an action when a virus is detected
- ▶ **/rename** Rename infected files
- ▶ **/delete** Delete infected files
- ▶ **/quarantine** Copy infected file to quarantine before taking further action (clean/delete)

Note: If the switches: **/prompt**, **/rename** or **/delete** are used concurrently with the **/clean** switch, the corresponding action will be carried out only if the virus cannot be cleaned. The further along a parameter is listed, the higher priority it has. For instance, using the **/clean /delete /prompt** parameters will result in that the **/prompt** parameter will supersede the **/clean /delete** parameters.