



NOD 32

antivirus system

**ESET NOD32 Antivirus
for Novell Netware Server**
Installation

Copyright © Eset, spol. s r. o.
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, spol. s r. o. 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, spol. s r. o. Microsoft and Windows are registered trademarks of Microsoft Corporation.

Eset, spol. s r. o.
Aupark Tower, 16th Floor, Einsteinova 24,
851 01 Bratislava, Slovak Republic

<http://www.eset.sk/en>

Technical Support Worldwide:
<http://www.eset.com/support>
Technical Support for Europe:
<http://www.eset.eu/support>

REV.20090811-005

1. Introduction

This User Guide describes the usage of ESET NOD32 Antivirus for Novell Netware Server (or just ESET NOD32 Antivirus for Novell), namely:

- installation of the product,
- configuration of individual modules,
- updating of the product.

ESET NOD32 Antivirus for Novell consists of the following NLM modules:

- *AMON.NLM* – on-access scanner, which automatically scans files accessed from the network or locally, or files saved to the server.
- *NOD32.NLM* – on-demand scanner, which can be directed to scan certain groups of files on the disk (usually folders, volumes, or the whole hard disk). In this case, it is only a single action – after it is completed, the NOD32.NLM module is removed from memory.
- *NOD32UMC.NLM* - system utility for the creation, update and maintenance of the NOD32 modules storage mirror.
- *NOD32UP2.NLM* – module providing a virus signature database update for the modules *AMON.NLM* and *NOD32.NLM*.

2. Installation

Create a directory named, for example NOD32, on volume *SYS:* and copy files from the installation packages for the ESET NOD32 Antivirus for Novell into it. To download and compile NOD32 anti-virus modules in a comfortable way, you can use the *NOD32UPD.PL* script. Before the use, you need to configure the parameters. Read the script text part for details.

To launch the script, run this command:

```
PERL SYS:\WOD32\NOD32UPD.PL
```

It is recommended to enable automatic startup of *AMON.NLM* and *NOD32UPD.PL* at each server startup using system file *AUTOEXEC.NCF*.

Quick guide through the complete installation

Extract the installation package. eg: into volume *SYS:/NOD32*. Also, it is recommended to create file *AMON.CFG* and insert the following into it:

```
recipient=network_administrator_login
notify
clean
delete
log
```

Then load *AMON* - memory-resident monitor using the following command on the Novell system console:

```
LOAD SYS:/NOD32/AMON.NLM
```

With the above mentioned setting, *AMON* will send information about infiltrations to the user *network_administrator_login*, but also to a user, who manipulated with the infected file (parameter *notify*). At the same time, *AMON* will attempt to clean the infected file, and if it is not possible, the file will be deleted.

Next, it is required to provide updates for ESET NOD32 Antivirus for Novell. The mirror directory must be located on the same hard disk as the installation of ESET NOD32 Antivirus for Novell (let us assume it is located in *SYS:/PUBLIC/MIRROR*). The update process is composed of two stages. First, the so called pre-compiled modules are downloaded from the origin ESET server.

To download the modules, run this command on the console to set up and launch the *NOD32UMC.NLM* module:

```
LOAD SYS:\WOD32\WOD32UMC -a SYS:/NOD32/NOD32.
AUTH SYS:/PUBLIC/MIRROR/
```

where *NOD32.AUTH* contains authentication username and password acquired from the vendor.

Second part of the update process is the compilation of modules loadable by ESET NOD32 Antivirus Scanner.

To compile the modules, run this command on the console to set up and launch the NOD32UP2.NLM module:

```
LOAD SYS:/NOD32/NOD32UP2.NLM SYS:/PUBLIC/MIRROR/
-update -period=60
```

Now ESET NOD32 Antivirus for Novell will be updated from the mirror directory `SYS:/PUBLIC/MIRROR` every hour (parameter `-period=60`).

It is recommended to enable automatic startup of AMON.NLM and NOD32UP2.NLM at each server startup using system file `AUTOEXEC.NCF`.

3. Modules

AMON.NLM

To load AMON, use the following command on the system console:

```
LOAD SYS:/NOD32/AMON
```

To unload AMON from memory, use the following command:

```
UNLOAD AMON
```

AMON.CFG

If there is present the file AMON.CFG in the directory with the module AMON.NLM, configuration from AMON.CFG will be transferred to AMON at its startup.

Syntax of the file AMON.CFG is as follows (each line may contain one of the following switches one switch per line):

onread+ (default setting)

Files will be tested in a moment when a command to open/read is detected.

The opposite switch is: **onread-**

onwrite+ (default setting)

Files are tested at the moment when a command to create/modify is detected.

The opposite switch is: **onwrite-**

onrename+ (default setting)

Files are tested at the moment when a command to rename is detected.

The opposite switch is: **onrename-**

all (default setting)

All files are tested. Otherwise, if the parameter **all** is used, only extensions defined by the Eset Company are tested.

notify

When an infiltration is detected, AMON sends a message to the user who attempted to access the infected file (using the *NetWare Message PopUp Service*).

recipient=user1, user2 ...

When an infiltration is detected, AMON sends a message to all users in the list. It is possible to list more users – in this case, use commas to delimit them – see the example above.

Other parameters:

pattern

log

logappend

logrewrite

clean

rename

delete

heur

heursafe

heurstd

heurdeep

These switches are identical to those used in module NOD32.NLM. They are described below (when entering parameters, always omit the hyphen).

NOD32.NLM

To run the NOD32 diagnostic scan or clean, enter the command as follows:

```
LOAD SYS:/NOD32/NOD32 [parameters] [path list]
```

If *[path list]* is not entered, NOD32 will automatically scan whole disk.

Parameters:

-help, -h, -?

Displays list of parameters with descriptions.

-subdir+ (default setting)

Enables testing of subdirectories.

The opposite switch is: *-subdir-*

-pack+

Enables testing of internally compressed files.

The opposite switch is: *-pack-* (default setting)

-arch+

Enables testing of archives (ZIP, RAR, ARJ...).

The opposite switch is: *-arch-* (default setting)

-pattern+ (default setting – recommended)

Enables testing using virus signatures.

The opposite switch is: *-pattern-*

-heur+ (default setting – recommended)

Enables detection using a heuristics method.

The opposite switch is: *-heur-*

There are three levels of heuristics analysis sensitivity:

-heursafe

-heurstd (default setting – recommended)

-heurdeep

Actions to take after an infiltration is found can be modified with the following parameters. The parameters can be suitably combined with each other. For example, parameters *-clean -delete* provide that an infected file, which cannot be cleaned, will be deleted. In case of the module AMON.NLM, not using any of the three following parameters will result only in blocking access to infected files.

-clean

Automatically cleans infected files.

-rename

Renames infected files.

-delete

Deletes infected files.

-prompt (not available for AMON.NLM)

Displays a dialog window individually on every infected file.

-log+ (default setting)

Enables logging to file (file NOD32.LOG, or AMON.LOG).

The opposite switch is: *-log-*

Log maintenance:

-logappend (default setting)

New information is attached to the end of existing log file.

-logrewrite

Logfile will be deleted with each module's startup.

-log=<filename>

Use this parameter to create your own log file.

Other parameters:

-list+

Enables listing of all scanned objects.

The opposite switch is: *-list-* (default setting)

Configuration – a practical example:

LOAD SYS:/NOD32/NOD32 -pack+ -arch+ -clean -delete

(Control of the whole disk including internally compressed files and archives. In case an infiltration is found, a file will be cleaned or deleted.)

NOD32UMC.NLM

(NOD32 internet Update Mirror Creator) module is a system utility for the creation, update and maintenance of the NOD32 modules storage mirror. After user authentication against NOD32 server which can be passed to NOD32UMC via NOD32 server authentication options the NOD32UMC utility will download into the MIRROR directory all the NOD32 engine category modules necessary to run any of the NOD32 application. Download of NOD32 component category modules (resp. download of classes of NOD32 component category modules - see subsection Tips for details) is optional and can be specified via command line by using string PLATFORM(S) or passed to NOD32UMC from external file (see section Other options for details). After proper download of all specified modules NOD32UMC will create control file MIRROR/update.ver which contains all the version information related to downloaded modules. This can be used later in the process of further mirrors creation. NOD32UMC supports download of the update modules via proxy server. Read sections Using proxy and Proxy authentication options of this manual for further information.

The syntax is as follows:

```
LOAD SYS:\NOD32\NOD32UMC AUTHENTICATION-OP-
TIONS [OTHER-OPTIONS] MIRROR [PLATFORM(S)]
```

where the following options are supported.

NOD32 server authentication options

User authentication against NOD32 server can be done by using the following options:

```
-u
--username user
    Use username user for authentication.
-p
--password pass
    Use password pass for authentication.
-a
--authfile auth_file
    Read username and password from auth_file instead
    of command line. Check the NOD32.AUTH to see the
    format of the auth_file.
```

Proxy authentication options

User authentication against proxy server used as a mediator of communication between local client and NOD32 server can be done by using the following options:

```
--proxy-username proxy_user
    Use username proxy_user for authentication.
--proxy-password proxy_pass
    Use password proxy_pass for authentication.
--proxy-authfile proxy_auth_file
    Read username and password from proxy_auth_file
    instead of command line. Format of the proxy_auth_
    file is the same as the format of the auth_file.
```

Other options

```
-s
--server server
    Check and/or download updates from server server.
-f
--readfrom file
    Use file file to read the packages to be mirrored.
```

```
-q
--query
    Query for available update packages and exit.
-v
--query-verbose
    Verbose query for available update packages and
    exit.
-l
--log-level level
    Set module logging level to value defined by argu-
    ment level. Following values of argument level are
    supported:
        0 none
        1 error
        2 notice (default)
        5 debug
    See section Logging for details.
-c
--check
    Only check what needs to be downloaded and exit.
-r
--remove-obsolete
    Remove automatically all obsolete modules from the
    local mirror.
-h
--help
    List the command line options and exit.
```

Using proxy

It is possible to download update modules via http proxy server(HTTP/1.0 protocol is used for communication with proxy and/or NOD32 server).

This is invoked automatically in case http_proxy environment variable is defined. Note that both http_proxy and HTTP_PROXY are understood, http_proxy is checked for first. If neither http_proxy nor HTTP_PROXY is defined, NOD32UMC will be connecting directly.

Example: `http_proxy=proxy.mycompany.com:3128`

The system utility NOD32UMC supports basic authentication against proxy server. This is invoked automatically by defining at least one of the three command line op-

tions described in section Proxy authentication options of this manual.

Note that it is not recommended to define any of the proxy authentication options in case the proxy authentication is not required.

Logging

NOD32UMC utility provides logging with output to terminal. Several logging levels are provided. Description of individual levels is as follows:

none

No logging output.

error

Only error and warning messages.

notice

Brief information about the modules downloaded is logged.

debug

Debug information about the downloading process is logged.

Tips

1. Download of classes of component category modules. Using command line argument PLATFORMS it is possible to define so called component category modules for download. To query list of component category modules available use command line option -q, --query. Note that so called classes of component category modules can be specified by argument PLATFORMS as well. For instance when WIN98 string defined as an PLATFORMS argument, all component modules related with WIN98 platform will be downloaded. All strings common for multiple component modules can be used for this purpose.

Download - a practical example

```
LOAD SYS:/WOD32\NOD32UMC -a SYS:/NOD32/NOD32.  
AUTH SYS:/PUBLIC/MIRROR/
```

(NOD32.AUTH contains authentication username and password acquired from the vendor.)

NOD32UP2.NLM

To update the ESET NOD32 Antivirus Scanner modules properly, the mirror directory location must be the same as created by NOD32UMC.NLM utility.

The syntax is as follows:

```
LOAD SYS:/NOD32/NOD32UP2 mirror_directory [folder_with_NLM_modules] [parameters]
```

Only *mirror_directory*, or a path to the mirror folder is required. This folder will provide update files for the modules NOD32.NLM and AMON.NLM.

[*directory_with_NLM_modules*] is optional in case the file NOD32UP2.NLM is located in the directory together with files NOD32.NLM and AMON.NLM.

Possible parameters:

-update

Provides NOD32 updates (otherwise, available updates will be displayed only).

-period=n

This parameter triggers update attempts every n minutes. We recommend updating every hour (*-period=60*).

-show_retvals

Use of this parameter returns all possible return values with brief comments.

-help

Will list all parameters with brief comments.

Special parameters:

-no_signature

This parameter can be used to avoid error No. 107. The error means that update files have an invalid digital signature.

Update - a practical example:

```
LOAD SYS:/NOD32/NOD32UP2.NLM SYS:/PUBLIC/MIRROR/  
-update -period=60
```

(The modules AMON.NLM and NOD32.NLM will be updated every hour from the mirror directory: SYS:/PUBLIC/MIRROR/).

Tips

1. Use NOD32UPD.PL script for modules download.

Edit and run NOD32UPD.PL script to download and update NOD32 anti-virus modules in a comfortable way.

Read the script text part for details.