



NOD32

antivirus system

**NOD32 for MS Windows
File 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.
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.sk/en/support>

Last revised on 11th August 2009

1. Introduction

MS Windows Server uses the same installation package as NOD32 for Windows – the workstations version. To provide smooth operation of the server, it is required to set up specific program options during the installation. The procedure is described in this document.

2. Recommended setup overview

- During the installation, choose the **EXPERT** option. During the Expert installation, forbid the activation of the **IMON** module. The module could cause problems on the network communication level, and, with a view to the “philosophy” of the module, it would be of almost no use anyway. It is also recommended to disable the **EMON** and **DMON** modules during the installation process.

After the installation is complete and the server is restarted, we recommend setting up the individual modules as described below:

AMON

- In the *Exclusions* tab, we recommend setting up exclusions for folders that shall not be controlled, or for those, which, if controlled, could slow down the whole system (e.g.: exclude folders, where eventual database server, or mail server store their data). Simultaneously, exclusions at the *Extension* level can be set up in the *Detection* tab. The **TMP** and **EML** extensions are typical examples of exclusion.
- In the *Actions* tab, it is suitable to select the option *Clean automatically* to avoid displaying alert windows if an eventual infiltration is found.

DMON, EMON, IMON

- If these modules are already installed, we recom-

end stopping them (using the *Quit* button in each module) – the icons in front of the modules in the *NOD32 Control Center* must be greyed out. We expressly recommend that at least the **IMON** module be quit-
ted.

3. Update

- We recommend downloading updates regularly every hour (it is the default setting for NOD32).
- In the *Setup of Automatic Update* tab, click on *Change* and set up the way you want NOD32 to behave in case Eset launches a new program component update of NOD32¹. Please consider that each program component update requires reboot of the server, and if the server is not rebooted, NOD32 is not able to download any other updates (including virus signature database updates). Incorrect setting may have impact on not only on security of the server itself, but also on security of workstations (if the server distributes updates via LAN using the *Mirror* feature). We recommend setting up the server to *Perform program component upgrade only if necessary for proper virus signature database functioning* and *Offer computer restart if necessary*. It is not required to install each program component update, since it doesn't have any influence on the quality of detection. If you leave the option *Notify before program component upgrade*, NOD32 will download a program component upgrade only with administrator's approval. Without the confirmation, the NOD32 antivirus system will not download any program upgrade.

¹ Program component upgrades bring new features to NOD32, or simply correct and improve a current version. Program component updates do not have any influence on the quality of detection. The NOD32 antivirus system “engine” updates, including the heuristic analysis module, support of archive files, etc., are a part of common virus database updates.