NeoExec for Active Directory Setup Guide

Version 1.1

NeoValens S.A.
66, Rue de Luxembourg
L-4221 Esch-sur-Alzette
Luxembourg

Email: support@neovalens.com
Web: www.neovalens.com

Published on: September 2004

Contents

Introduction

This document explains how to install NeoExec for Active Directory (NeoExec/AD) on your computer.

NeoExec/AD is an innovative solution that allows you to manage your desktops and servers in a more secure manner. There exists a number of applications that require elevated privileges to run and, without NeoExec, the only solution available was to grant such privileges to the user. NeoExec on the other hand allows you to set the privileges on a per-application basis thereby helping in creating a more secure, manageable environment.

Privileged Applications Vs Privileged Accounts

Members of the local Administrators group have privileges that allow them to perform any action on a computer. Users are often made members of the Administrators group because some applications require elevated privileges to run. The problem is twofold: users often abuse of those privileges to install new applications and/or to modify the configuration of their computer and, possibly even more important, users with elevated privileges are more vulnerable to viruses and trojans. Most malware requires elevated privileges to be installed and to replicate, and members of the local Administrators group are the primary target.

The principle of *least privilege* states that users should be granted the most restrictive set of privileges needed for the performance of authorized tasks. Application of this principle limits the damage that can result from accident, error, or unauthorized use of an information system (IS).

NeoExec helps in applying the least privilege principle by restricting elevated privileges to selected applications.

NeoExec/AD components

NeoExec/AD consists of two components:

- NeoExec/AD MMC Snap-In.
- NeoExec/AD kernel driver and group policy extension

The NeoExec/AD MMC console allows you to define the NeoExec policies, that is, the list of Privileged Applications and their parameters. The MMC console plugs-in the Group Policy mechanism of Windows.

The MMC console can be used to define policies at the Site, Organizational Unit and Domain level. You can either install the NeoExec/AD MMC console on one or more Domain Controller or Windows 2000/XP workstations with the Administration Pack installed. Either way, the NeoExec node, named "Application Execution Policies", will appear in the Group Policy editor as a new node of the Computer Configuration node. The NeoExec/AD policies will automatically be deployed to the client computers by means of the built-in GPO deployment mechanism.

The MMC console can also be used to define local policies and it appears as a node of the local Group Policy snap-in (gpedit.msc). Such snap-in can be invoked from the NeoExec/AD shortcut menu or from the Run window by typing "gpedit.msc". You only need to install the NeoExec/AD MMC console on the computers for which you want to define local policies, typically computers not part of a domain.

The NeoExec/AD kernel driver reads the policies from the registry and applies them as users execute Privileged Applications. When an end user launches a privileged application NeoExec modifies the process token on the fly adding the groups that you have set in the policies, thereby allowing the user to run the application as if he/she was a member of such group.

New for NeoExec/AD

- MMC administrative console integrates into Windows 2000/2003 Group Policy management
- Automatic policy distribution by means of Group Policy objects
- Wizard based interface
- Simplified "command lines" management for built-in MMC snap-ins and Control Panel applets
- Ability to select a group other than Administrators (*Privileged Group*)
- Ability to restrict execution of Privileged Applications to selected users by means of ACLs (*Authorized Users*).

New for v1.1

- You can now have more than one Privileged Group. This allows you to mix both well-known groups such as Administrators and Power Users with both local and domain groups as required. Having more than one group allows you to create per-application ACLs based on such groups.
- You can now remove one or more groups from the process token. This allows you to remove sensitive groups when executing critical applications. This is especially useful when users with elevated privileges need to access the internet as NeoExec can revoke privileges of your choice for selected applications (such as Internet Explorer and Outlook for instance).
- You can now set per-process operating system privileges. Some processes require a number of privileges in order to work. Up to now such privileges would have been granted to the user but it is now finally possible to grant them on a per-application basis. By default, NeoExec will use
- Support for Windows Server 2003

Systems Requirements summary

Operating System	Kernel Driver	MMC Console
Windows 2000, any service pack	☑	☑
Windows XP, any service pack	☑	☑
Windows Server 2003	☑	☑

Setting up NeoExec/AD is straightforward and consist in setting up the NeoExec® for Active Directory MMC Console on your computer and deploying the NeoExec for Active Directory kernel driver on the computers you want to execute privileged applications.

Warning: NeoExec/AD is not an upgrade of NeoExec Professional but rather a brand new product. Do no install NeoExec/AD over NeoExec Professional.

Installing NeoExec® for Active Directory MMC SnapIn

This section explains how to install and uninstall the NeoExec® MMC SnapIn.

System Requirements

Windows 2000 Professional, any service pack

Windows XP Professional, any service pack

Windows Server 2003, any service pack

Installation

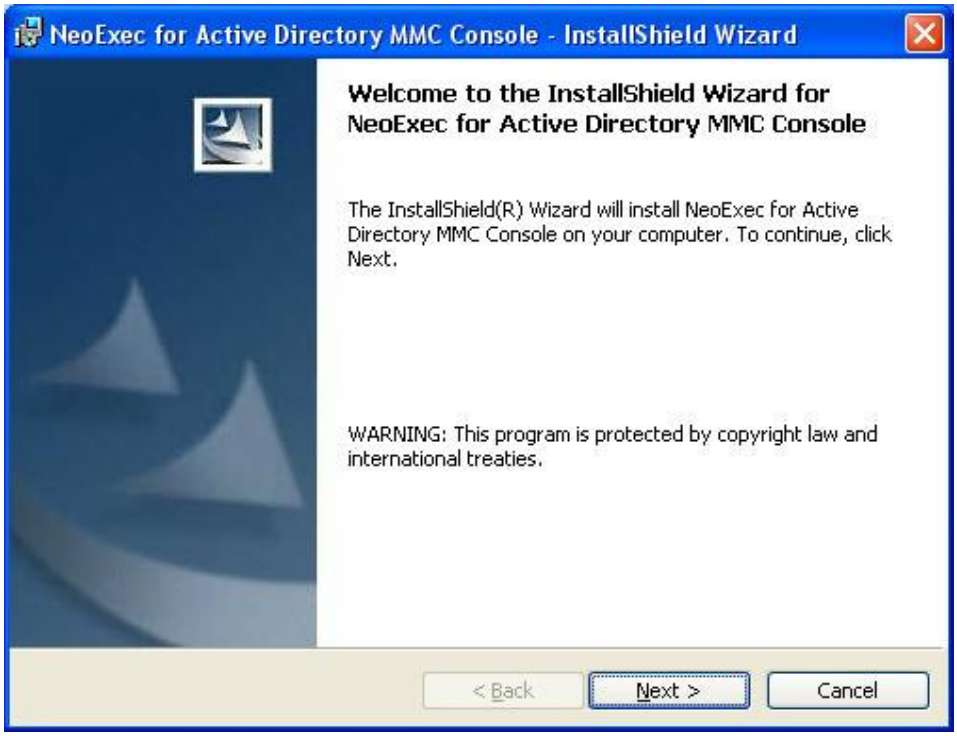
Step 1

Log on with administrative privileges and close all programs running on the computer.

Step 2

To begin the installation navigate to where the NeoExec® Administrative Console setup files are located.

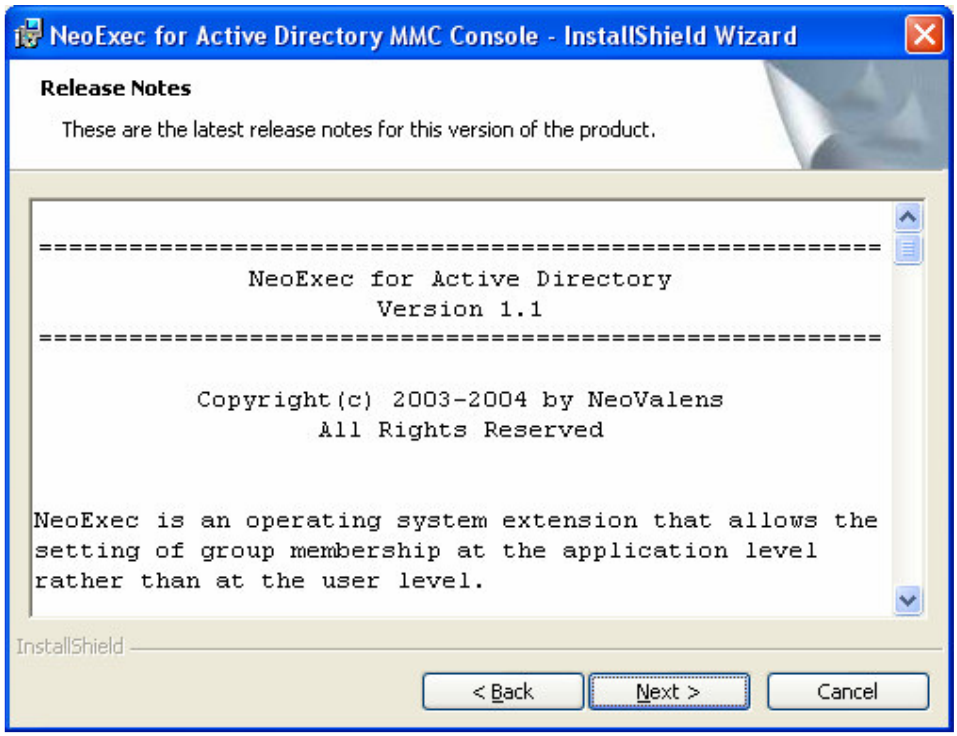
Double click on *NeoExec for Active Directory MMC Console.msi* to launch the installer. A series of screens will be displayed, beginning with the welcome dialog.



Click "Next" to continue.

Step 3

The Release Notes are displayed.



Read the Release Notes thoroughly. They may contain updated information which didn't make it into this guide. Use the scroll bars to read all of the text, and then click on *Next* to continue.

Step 4

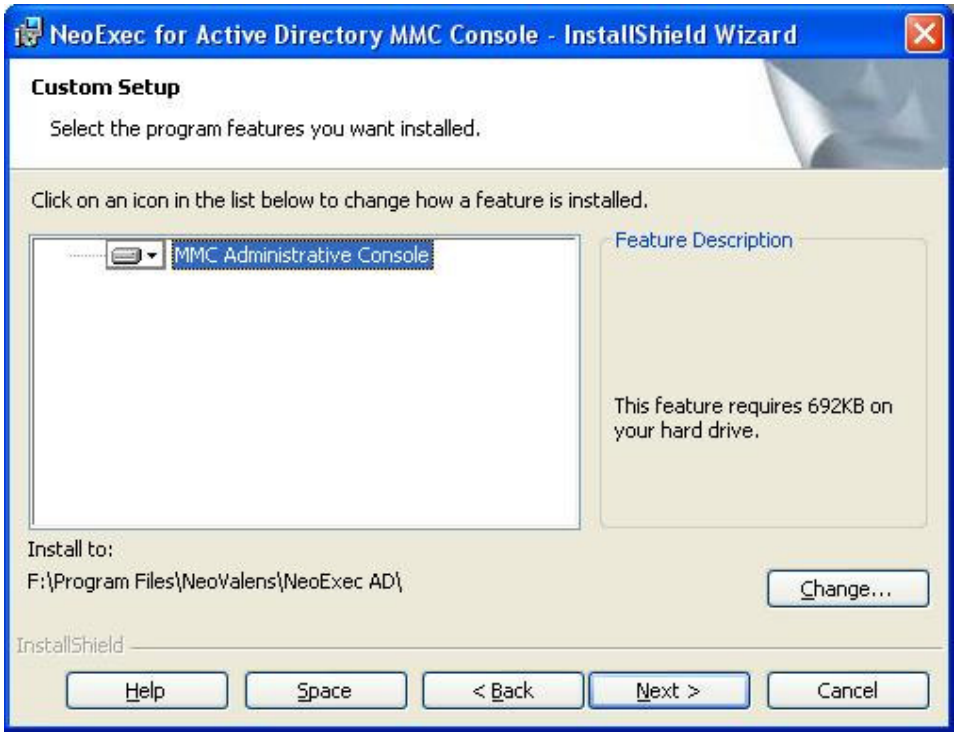
The License Agreement is displayed.

Copyright and international treaties protect the NeoExec® software. Read the license agreement carefully, and providing you agree with its terms, click on "I accept the terms in the license agreement". Click *Next* to continue.

If you do not agree with the terms, click on "I do not accept the terms in the license agreement". Setup will terminate without installing the NeoExec® for Active Directory MMC Console.

Step 5

The next screen shows the features available.



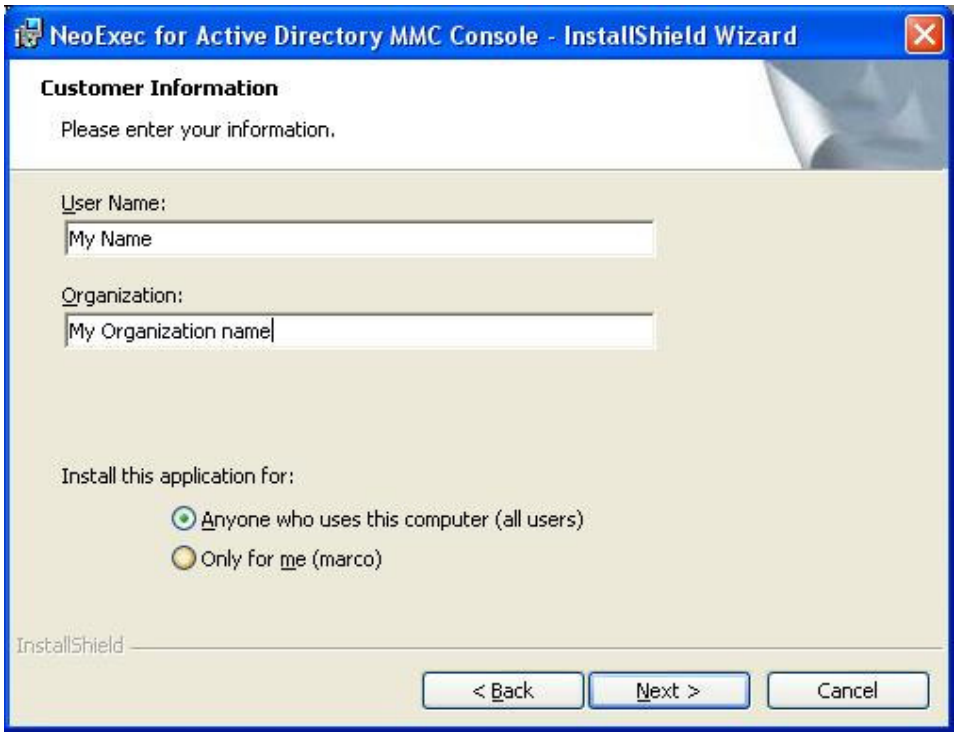
In this step you need to specify where to install the the NeoExec® for Active Directory Console. The default destination path is *\Program Files\NeoValens\NeoExec AD*.

To change the location, click on *Change...* to browse the system. Navigate to the desired location and click *OK*, or click *Cancel* to return to the default destination path.

Click *Next* to continue with the installation.

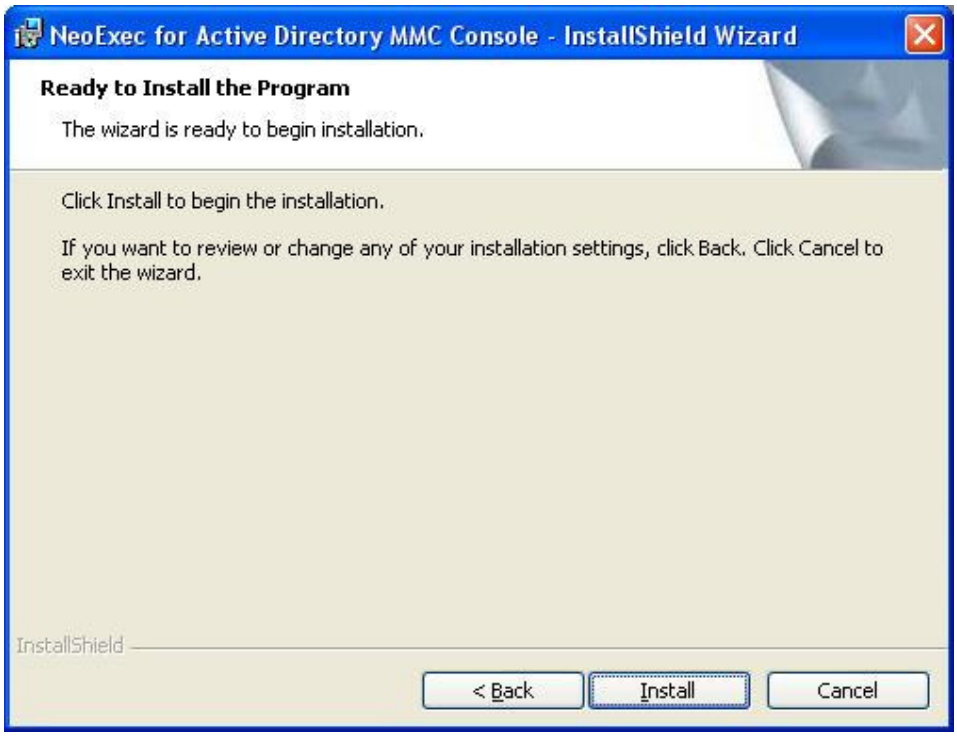
Step 6

In this step you need to decide who will see the shortcut to the NeoExec for Active Directory MMC Console snap-in. Users will require administrative privileges to manage NeoExec.



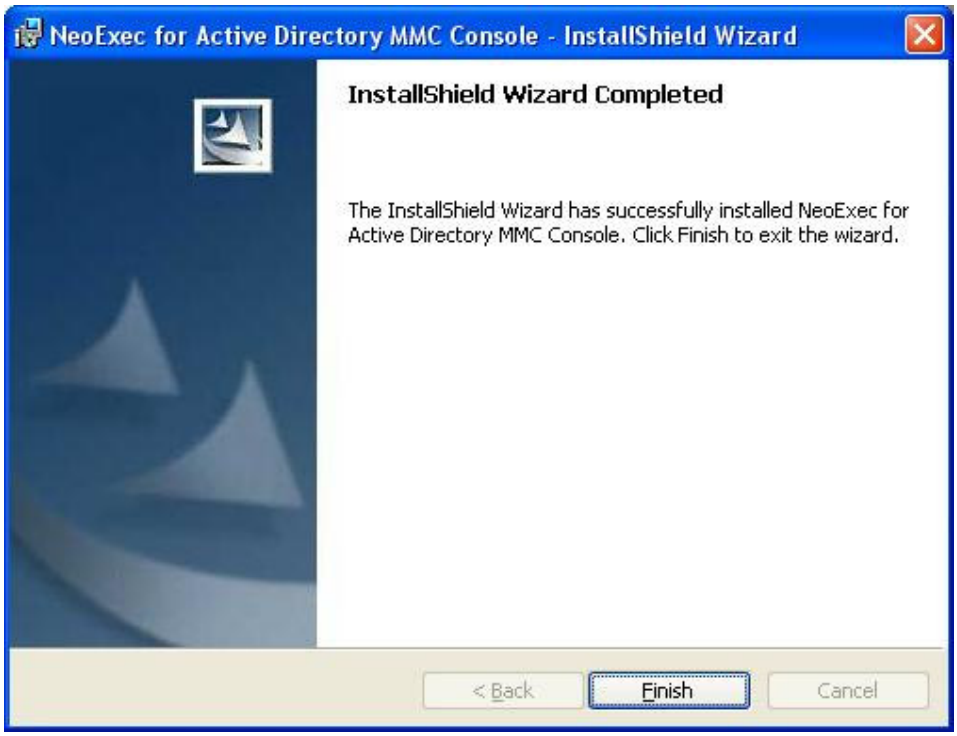
Step 7

You are now ready to begin installation. You can change any of the installation settings by clicking *Back*. Otherwise, click *Install* to begin installation.



Step 8

Finally once the installation is complete the following screen is displayed.



Click *Finish* to exit the installation program.

There is no need to reboot.

Shortcuts

Once the installation is successfully completed, you should be able to access the NeoExec® for Active Directory MMC Console from the *Start -> Programs -> NeoExec AD-> NeoExec AD MMC Console* shortcut. As NeoExec MMC console integrates with the Local Security Policies you can also access the snap-in by running "gpedit.msc" from the command line.

WARNING

There is a *known bug* in Windows XP that causes the previously-edited policies to remain in effect. This bug occurs when you use gpedit.msc to edit local policy settings. The bug and workaround are documented in the Microsoft Knowledge Base Article - 828538 on the Microsoft web site:

http://support.microsoft.com/default.aspx?scid=kb;en-us;828538

We suggest following Microsoft recommendations and installing the GPMC on the computers you plan to edit NeoExec/AD local policies.

GPMC

http://www.microsoft.com/downloads/details.aspx?FamilyId=0A6D4C24-8CBD-4B35-9272-DD3CBFC81887&displaylang=en

And also: Microsoft Knowledge Base Article - 326469

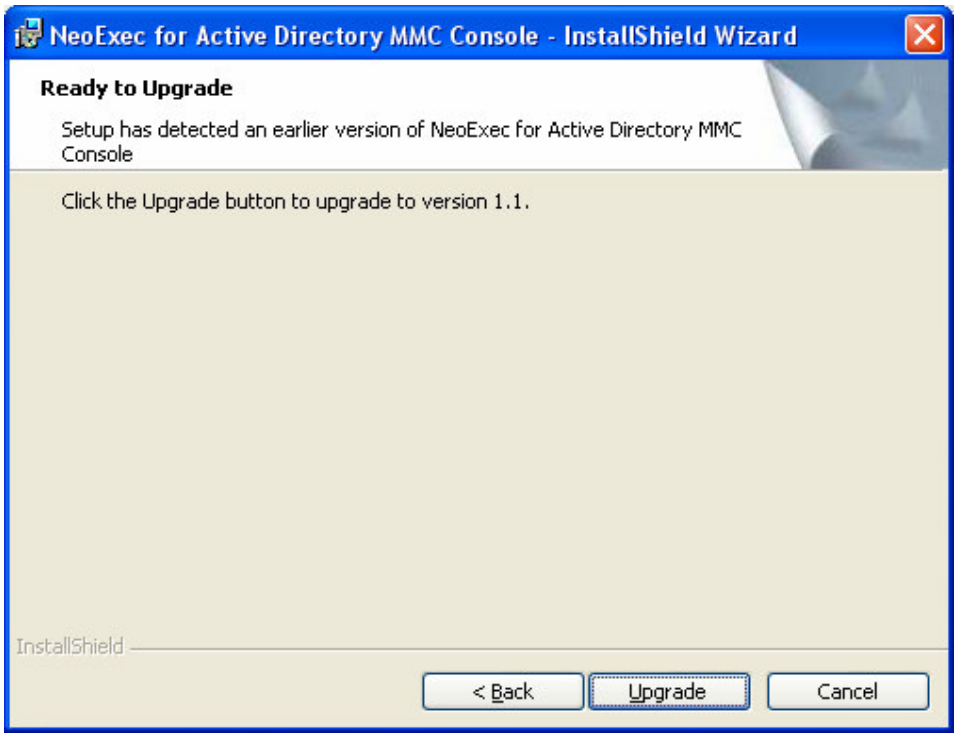
http://support.microsoft.com/default.aspx?kbid=326469

Upgrading from a previous version

Log on with administrative privileges and close all programs running on the computer.

To upgrade navigate to where the NeoExec® Administrative Console setup files are located.

Double click on *NeoExec for Active Directory MMC Console.msi* to launch the installer. The upgrade dialog will be shown.



Click on the *Upgrade* button to upgrade to v1.1. There is no need to reboot.

Uninstalling the NeoExec® MMC Console

At any time after installing NeoExec® MMC Console you can uninstall it from your computer. To uninstall NeoExec you must log on with administrative privileges.

To uninstall NeoExec® MMC Console go to *Start* -> *Settings* -> *Control Panel* and select *Add or Remove Programs*.

Select *NeoExec® for Active Directory MMC Console* and click *Change/Remove*.

A series of prompts will be displayed to confirm that you want to remove the application from your computer.

Click on *Yes* to uninstall.

Once this has completed the NeoExec® for Active Directory MMC Console has been removed from your computer.

There is no need to reboot.

Installing the NeoExec for Active Directory kernel driver

This section explains how to install and uninstall the NeoExec® for Active Directory kernel driver.

The NeoExec® software uses Microsoft Windows Installer to install the NeoExec® for Active Directory driver on Windows 2000 professional and Windows XP Professional.

System Requirements

Windows 2000 Professional, any service pack

Windows XP Professional, any service pack

Windows Server 2003, any service pack

Installation

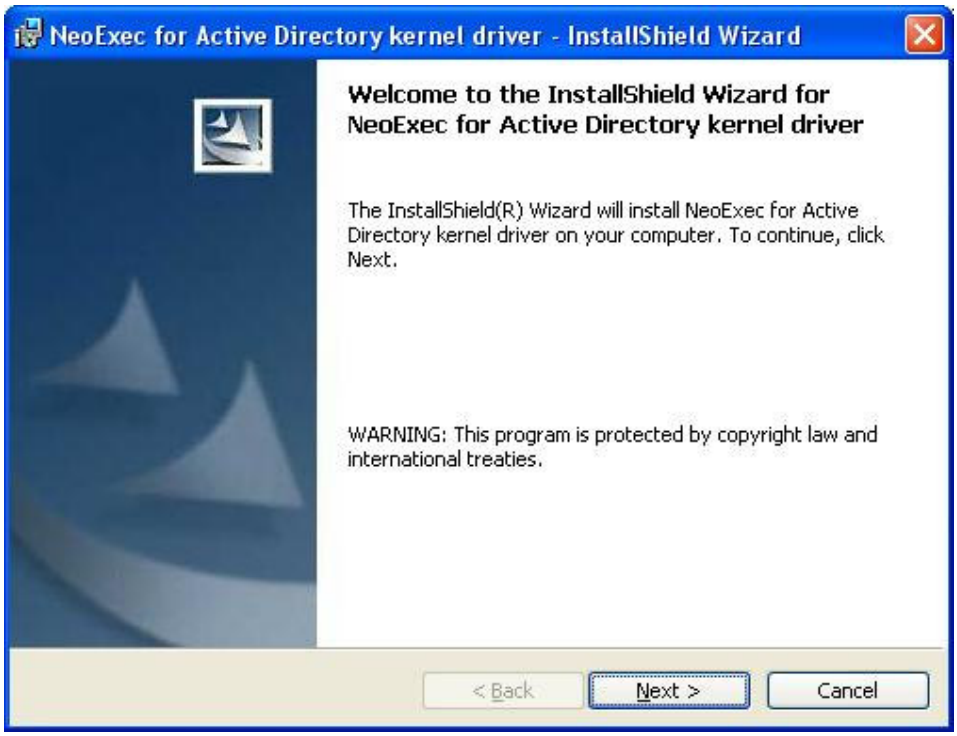
Step 1

Log on with administrative privileges and close all programs running on the computer.

Step 2

To begin the installation navigate to where the NeoExec® for Active Directory setup files are located.

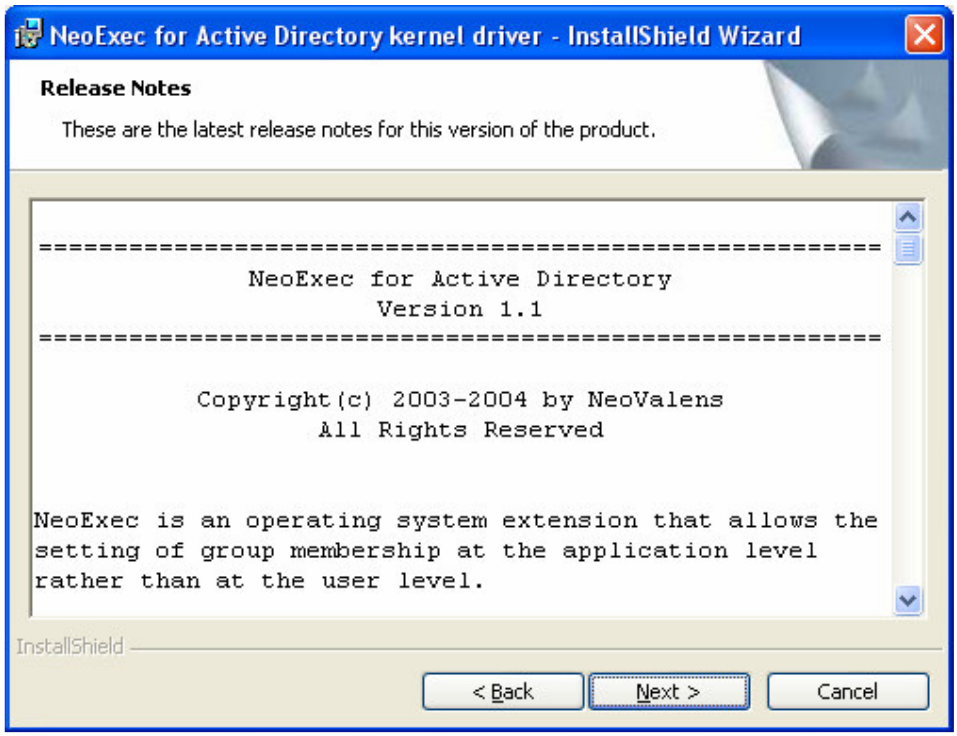
Double click on *NeoExec for Active Directory kernel driver.msi* to launch the installer. A series of screens will be displayed, beginning with the welcome dialog.



Click *Next* to continue.

Step 3

The Release Notes are displayed.



Read the Release Notes thoroughly. They may contain updated information which didn't make it into this guide. Use the scroll bars to read all of the text, and then click on *Next* to continue.

Step 4

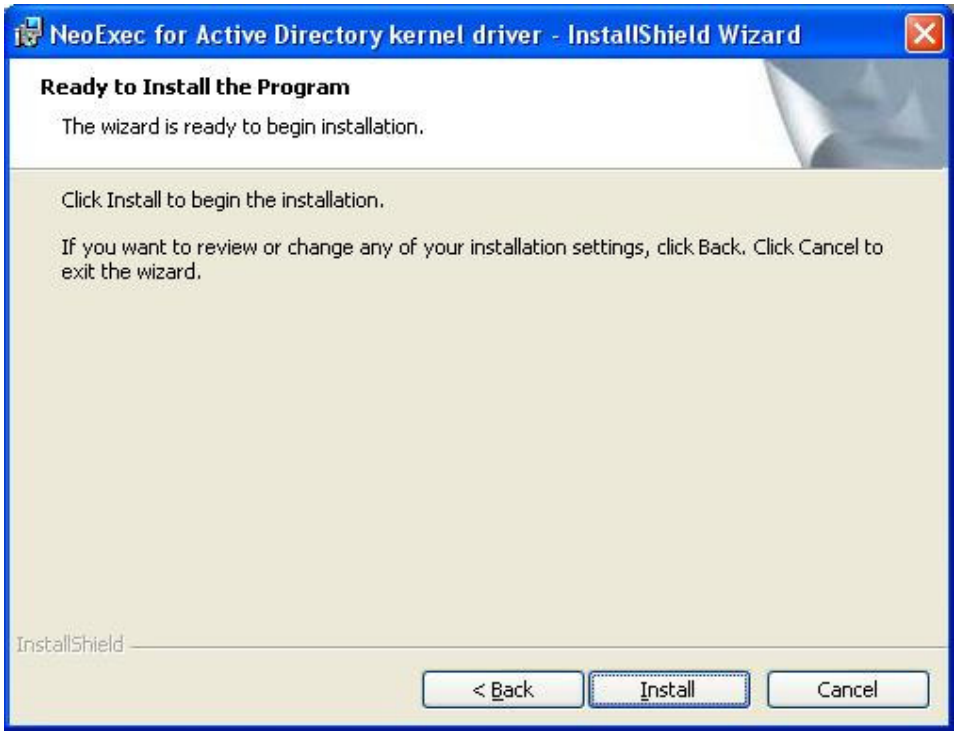
The License Agreement is displayed.

Copyright and international treaties protect the NeoExec® software. Read the license agreement carefully, and providing you agree with its terms, click on "I accept the terms in the license agreement". Click *Next* to continue.

If you do not agree with the terms, click on "I do not accept the terms in the license agreement". Setup will terminate without installing NeoExec® kernel driver.

Step 5

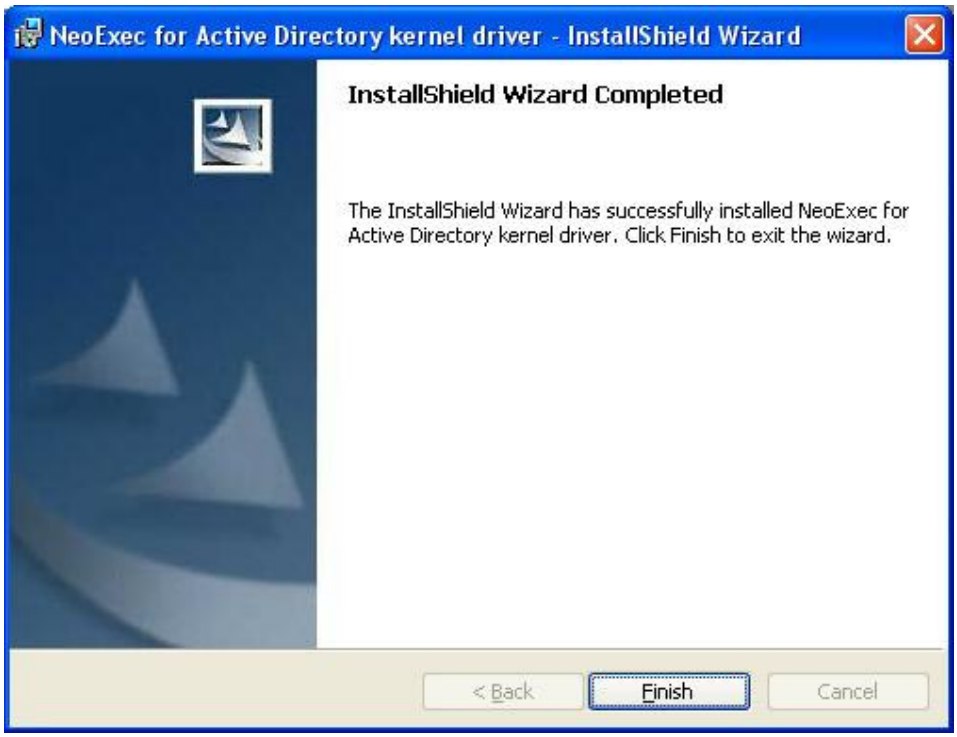
You are now ready to begin installation. You can change any of the installation settings by clicking *Back*. Otherwise, click *Install* to begin installation.



The setup will copy the driver file *neoexec.sys* to the *\SystemRoot\System32\Drivers* directory. It will also create a directory called *Neo* under *\SystemRoot\System32* which will hold the NeoExec® license file.

Step 6

Once the installation is complete the following screen is displayed.



Click *Finish* to exit the installation program.

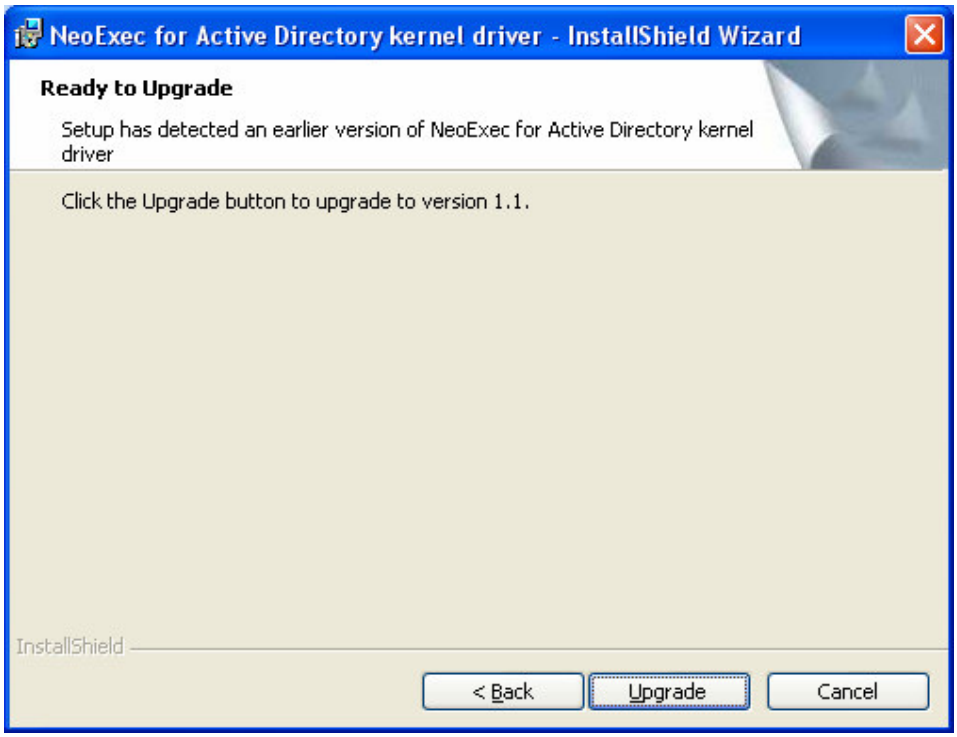
There is no need to reboot.

Upgrading from a previous version

Log on with administrative privileges and close all programs running on the computer.

To upgrade navigate to where the NeoExec® kernel driver setup files are located.

Double click on *NeoExec for Active Directory kernel driver.msi* to launch the installer. The upgrade dialog will be shown.



Click on the *Upgrade* button to upgrade to v1.1. The upgrade requires a reboot.

Uninstalling the NeoExec® for Active Directory kernel driver

At any time after installing the NeoExec® for Active Directory kernel driver you can uninstall it from your computer. To uninstall the NeoExec kernel driver you must log on with administrative privileges.

To uninstall the kernel driver go to *Start -> Settings -> Control Panel* and select *Add or Remove Programs*.

Select *NeoExec® for Active Directory kernel driver* and click *Change/Remove*.

A series of prompts will be displayed to confirm that you want to remove the application from your computer.

Click on *Yes* to uninstall.

Once this has completed, NeoExec® for Active Directory kernel driver has been removed from your computer.

The final screen informs you that you need to reboot your system in order for the uninstall to take effect. You can chose to do this now, or at a later date.

After the Installation

Once the setup has completed you need to define which applications will be run as a Privileged Application and this is done by means of the NeoExec® MMC Console.

For more information on creating configuration files refer to the NeoExec for Active Directory Administration Guide.

Trial mode

Without the license file, NeoExec® for Active Directory will start in Trial mode. NeoExec® for Active Directory can be used for evaluation purposes for up to thirty days, after which the product will be disabled unless a valid license file is supplied.