

Faronics

ANTI-EXECUTABLE™

ABSOLUTE Protection from
Unauthorized Executables



Faronics Anti-Executable - Integrating with ZENworks

TECHNICAL WHITEPAPER

Last modified: November, 2005

Faronics

Toll Free Tel: 800-943-6422

Toll Free Fax: 800-943-6488

International Tel: +1 604-637-3333

International Fax: +1 604-637-8188

www.faronics.com

©1999-2006 Faronics Corporation. All rights reserved.
Deep Freeze, Anti-Executable, and WINSelect are trademarks
and/or registered trademarks of Faronics Corporation.
All other company and product names are trademarks of their respective owners.

Introduction

This white paper provides some background information on integrating a ZENworks environment with Anti Executable. ZENworks gives a certain amount of desktop management control, and in combination with Anti Executable, users gain even more control, particularly in lab environments like schools and universities.

When using ZENworks, administrators are often concerned about how far to lock down computers in order to prevent students from corrupting systems and making them unusable for others. However, in most learning environments, administrators need computers to be open enough to provide hands-on experience necessary for student learning. Anti Executable, in combination with ZENworks, makes this possible.

Deploying Anti-Executable with ZENworks using the Silent Install Switch

Anti-Executable can be rapidly installed to many workstations over a network using Novell ZENworks using the Silent Install System provided by the Enterprise version of Anti-Executable. After the Silent Install is complete, the system immediately restarts. Any deployment utility that allows execution of a command line on a remote workstation can implement the Silent Install System.

The command line has the following options:

Syntax	Description
[/Install]	Install Anti-Executable using installation file
[/Uninstall]	Uninstall Anti-Executable
[/Uninstall /Seed]	Uninstall Anti-Executable and leave the workstation seed installed

Example Command Line: `AEWksinstall.exe /Install`

In the above example, the Anti-Executable installation program file is named *AEWksinstall.exe*. This command line installs Anti-Executable with the configuration settings as defined in the Configuration Administrator.

The Silent Install System does not work without the `[/Install]` or `[/Uninstall]` switch.

Anti-Executable must be deactivated before `[/Uninstall]` can be used.

Integrating Anti-Executable with ZENworks for Software or File Updates

To integrate Anti Executable into a ZENworks environment, a script is used to deactivate Anti-Executable. ZENworks is then used to deploy applications or registry changes. The script concludes with the instruction to reactivate Anti-Executable, with the settings updated.

This process can be performed remotely using Anti Executable's command line control (AEC), simple scripting, and ZENworks' application deployment.

Batch File Scripts

Using a batch file is the simplest way to use AEC without any additional scripting programs. Batch files are a capability of the DOS/Windows operating system.

The following batch file deactivates Anti-Executable:

```
REM Unprotect.bat
REM Test machine for De-activation of Anti Executable.
\\server\volume\directory\AEC.EXE ISON
if errorlevel 1 goto unprotect
exit
```

```

:unprotect
REM This section will deactivate Anti-Executable, if errorlevel above equals
REM '1' which is passed by the AEC command line utility.
\\server\volume\directory\AEC.EXE <password> OFF
REM ECHO %errorlevel%
REM You can debug AEC by using the above line, just remove the REM, which is
a remark command used to ignore statements in batch script, so that comments
can be made as done here.

```

The following batch file reactivates Anti-Executable:

```

REM Protect.bat
REM Test machine for activating Anti Executable.
\\server\volume\directory\AEC.EXE ISON
if errorlevel 1 goto activatedalready
REM Following line Protects machine if errorlevel is NOT equal to 1.
REM If errorlevel equals '1' then it skips the next line until it finds
REM : activatedalready, which is a batch script label. In this case an exit
REM command
\\server\volume\directory\AEC.EXE <password> ON
:activatedalready
Exit

```

Deactivating or reactivating Anti-Executable on command is easily done with these scripts. They can be especially useful in login scripts; when a user logs in, the log script deactivates or reactivates the software based upon the command in the script.

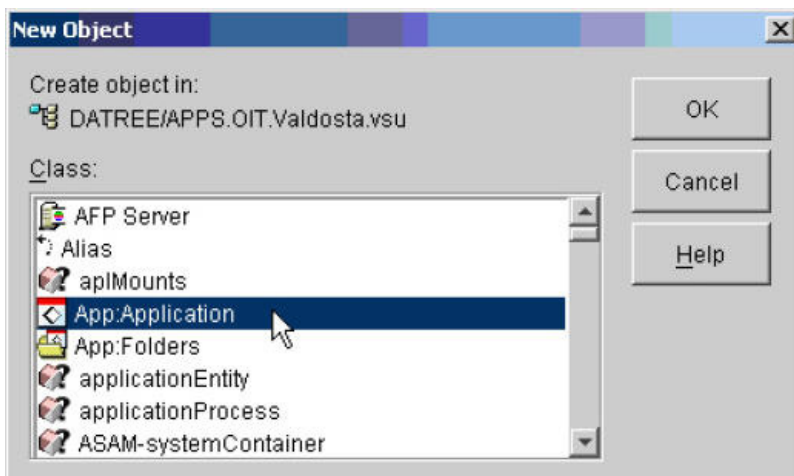
If there is a concern about the Anti-Executable password being viewable in clear text, freeware programs are available on the Internet to convert .BAT files into .COM files. These programs can encrypt the clear text file into unreadable machine code.

Using the batch file script with ZENworks script files can also be used within ZENworks to do many useful things. To use scripts in ZENworks, two application objects must be made: one to activate or reactivate Anti-Executable, and the other deactivate Anti-Executable.

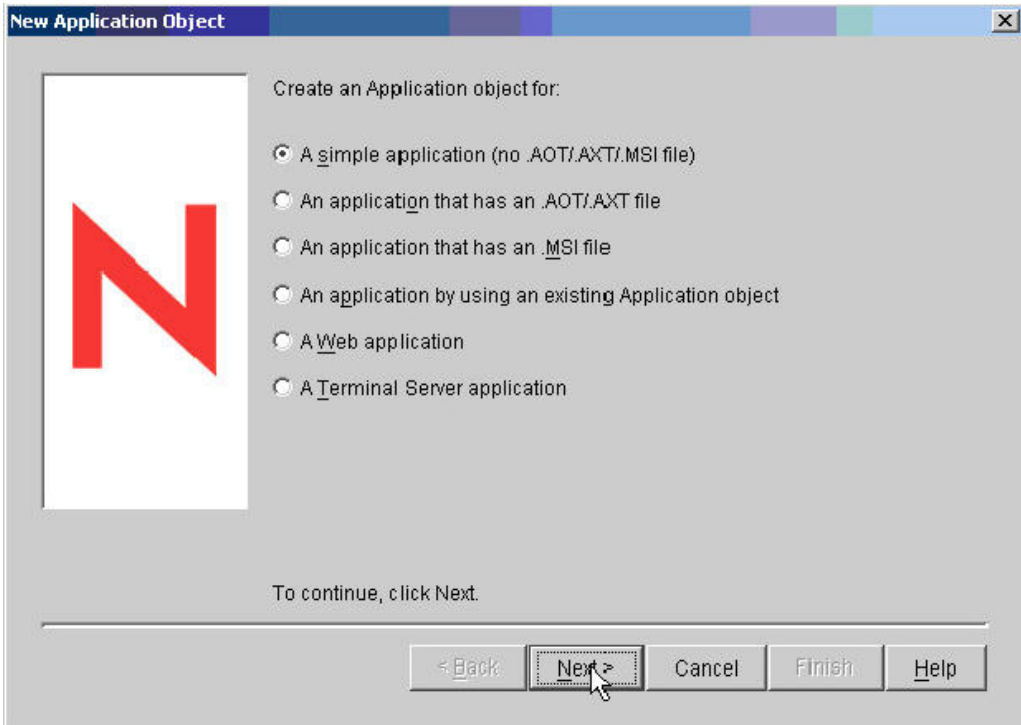
Activating Anti-Executable

The following instructions detail how to create an application object to activate or reactivate Anti-Executable.

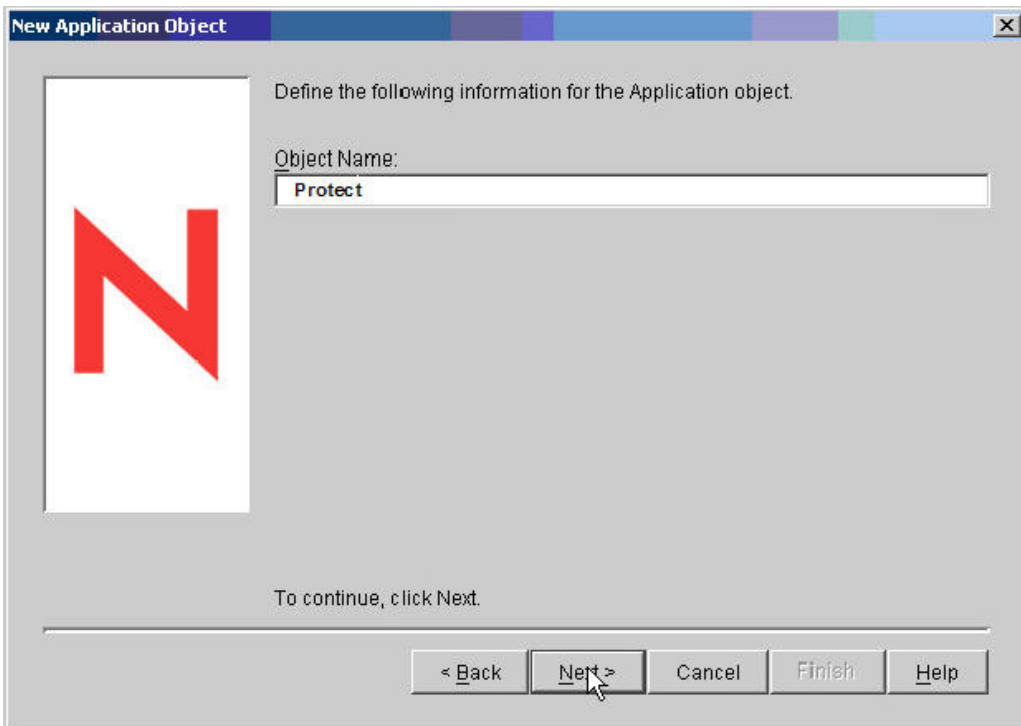
1. Create a new Application Object within ZENworks.



The following screen appears:

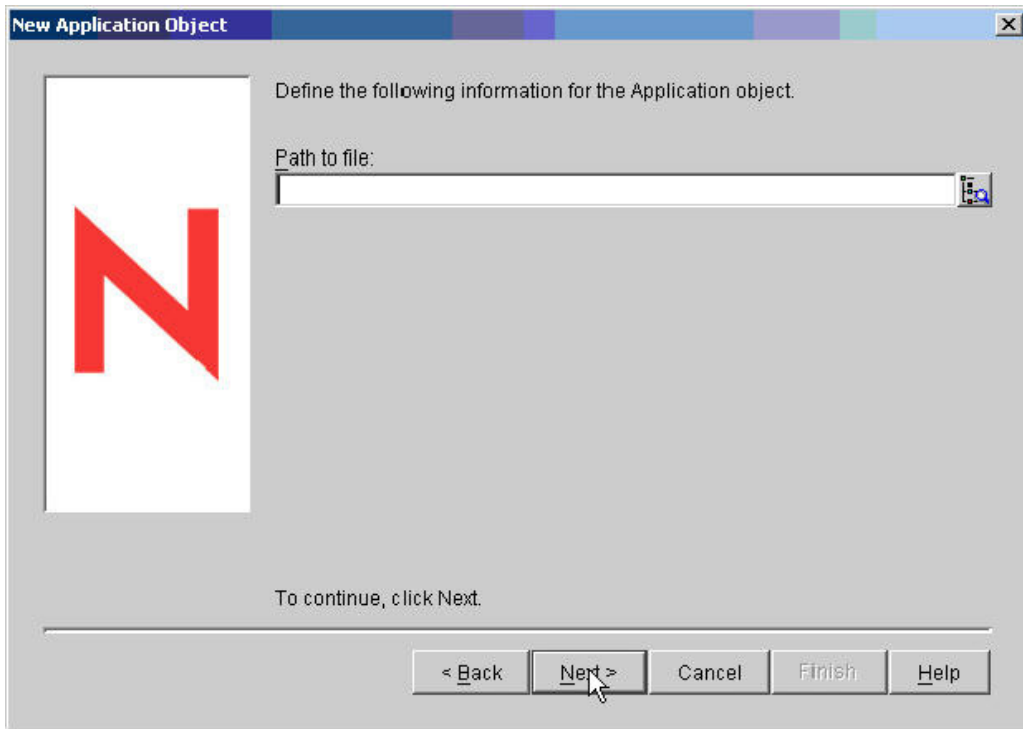


2. Click *Next* to create the simple application.



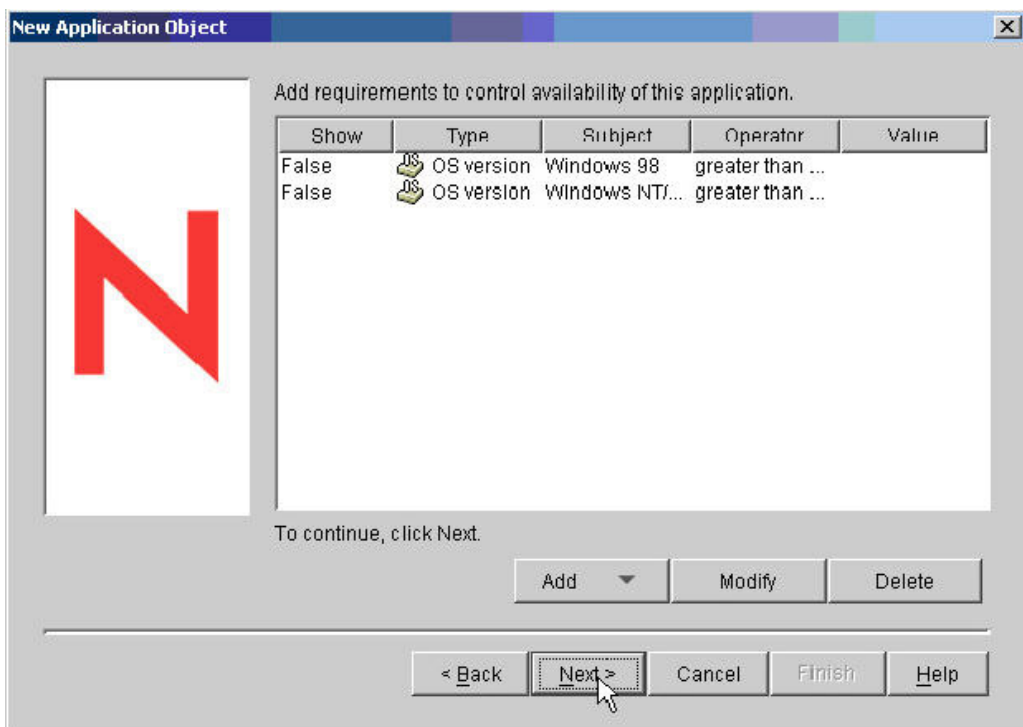
3. Give the application a name, and click *Next*.

The following screen appears:

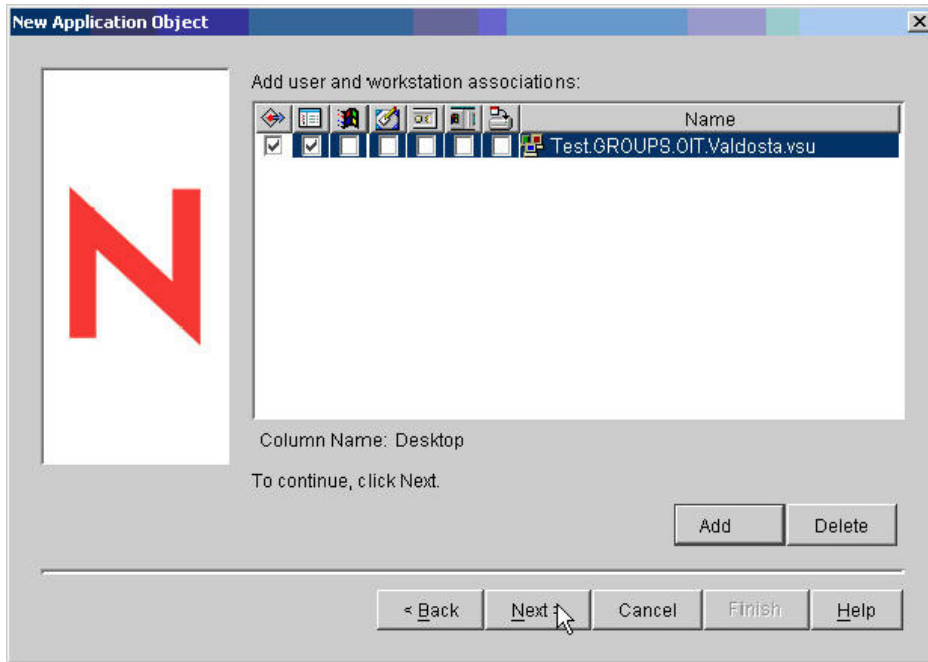


4. The above dialog asks for a *Path to file*; leave this field blank and click *Next*.

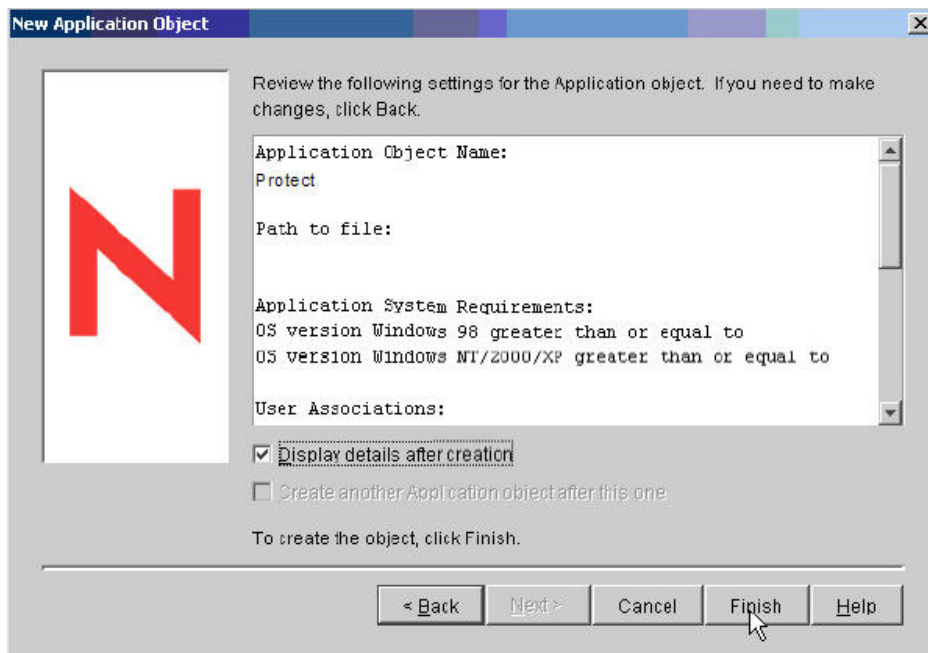
The screen to select application requirements appears:



5. Click *Next* to accept the default settings. Click *Add* to learn more about other options.

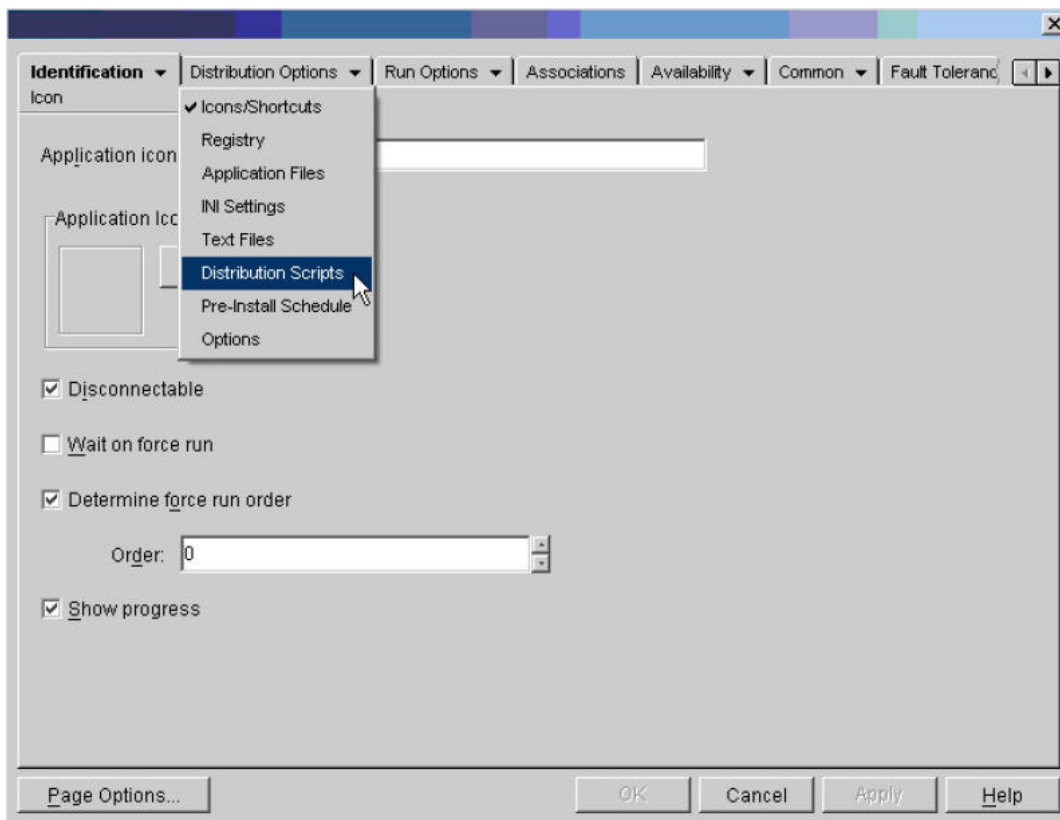


6. The above screen allows administrators to associate the application with a user or a group of users.
Check the first box, which indicates the use of the *Force Run* option when deactivating or reactivating Anti-Executable. *Force Run* means the application is forced to run when a user logs in or the application is refreshed.
The second box is checked by default, and indicates that the application is listed in Application Explorer.
7. Click *Next* to see the final summary screen.



8. Check *Display details after creation* and click *Finish*.

The properties dialog for the new application appears:

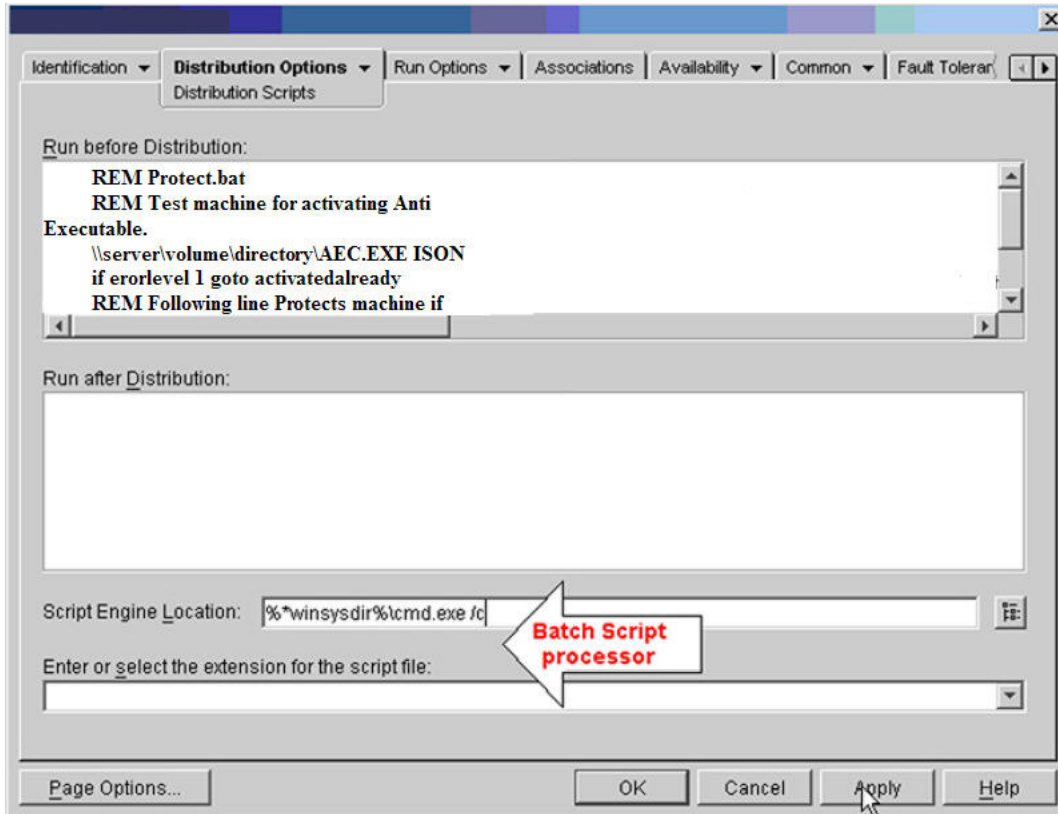


Configuring the Application Properties

Now that the object has been created, a number of configuration options are available.

Distribution Options Tab

The *Path to file* field was left blank in the process of creating the application because the newer versions of ZENworks allows Distribution scripts to be run, which allows a pre-script to be run before running an actual program. When Distribution Scripts are used with Anti Executable, the batch file script is copied into the *Run before Distribution* window, as shown in the following screen;



The above script is the same one used in the batch file.

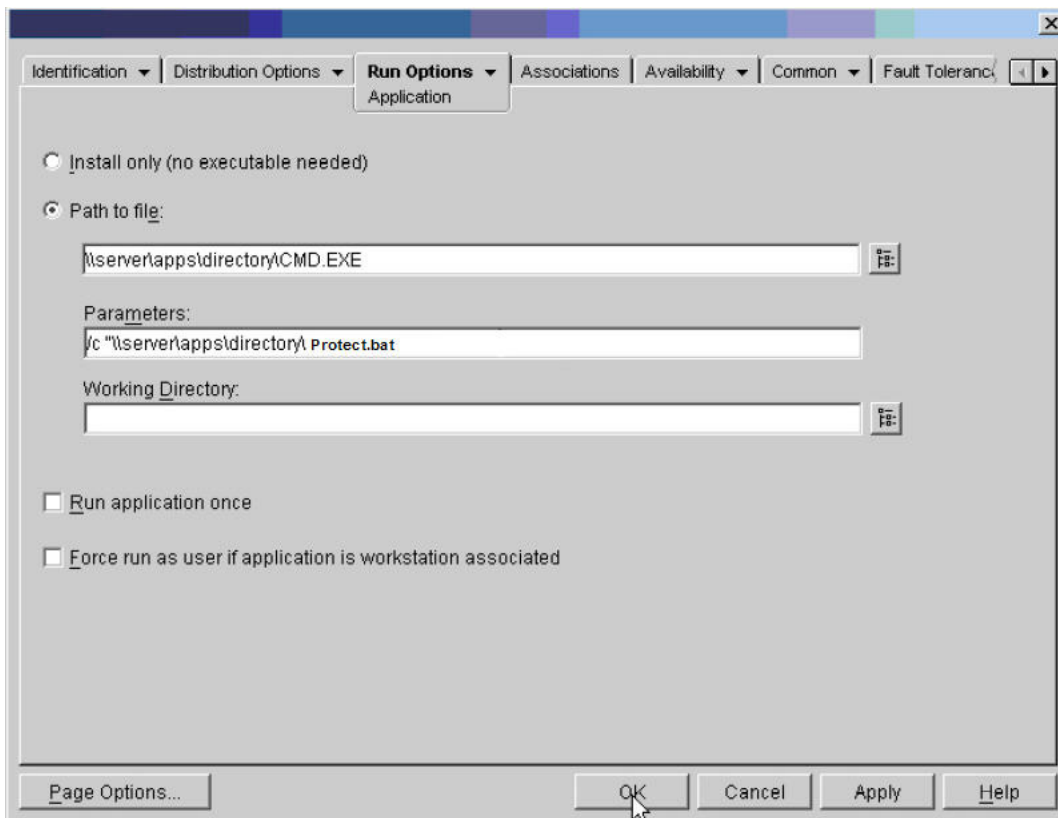
The text in the *Script Engine Location* is necessary for ZENworks to execute the script. This information tells ZENworks to use the Operating System to run the script commands above. The `%*winsysdir%` variable is one of many that can be used with ZENworks. The variable tells ZENworks to look in the operating system's system directory to find and launch the `cmd.exe` command. The `/c` parameter is necessary for ZENworks to spawn a new command environment and execute the above code successfully.

Any script can be used at this point in the process, depending on what the administrator wants to do.

NOTE: It is possible to run other more versatile and complex scripts, such as VBScript, by selecting the appropriate *Script Engine Location*.

Run Options Tab

Alternatively, instead of using the Distribution Options, the *Run Options* tab is a different route to take. Run Options, as shown in the following screen, tells ZENworks what programs to run and how to run them when ZENworks launches the application object.



In the above screen, the *Path to file* field is filled in. While this field can be filled in when the application object is created, it is not recommended. The necessary parameters may be forgotten in later stages of configuration. Also, this option does not need to be set if Distribution Scripts are going to be used. If Distribution Scripts are going to be used, select the *Install only* option.

According to the parameters in the dialog, the application is running the CMD.exe from the server. This can also be set to run locally using the `%*winsysdir%` variable. This tells ZENworks to run a command shell prompt and spawn a new command. The new command is running a batch file on the server that has the Protect script inside it.

CMD.EXE is the NT or greater version of COMMAND.COM used with 9x operating systems. Switch this if it is being run for 9x environments.

Batch Files versus Distribution Scripts

The difference between using the CMD.EXE and using Distribution Scripts depends on the administrator's preferred method, as well as the version of ZENworks being used. Older versions of ZENworks do not have the option of using Distribution Scripts.

The advantage of using Distribution Scripts is that batch files do not have to be run from the server. Everything is inside the application object. This means greater security because if users don't have access to the object, they can't read the script inside it. The only thing needed on the server is the AEC.exe program that is executed.

If a batch file is used, unless a program is used to convert it from batch to an executable, the clear-text batch file setting is on the server with the Anti-Executable password inside it. Distribution Scripts can also give much more flexibility when being used with more advanced scripting engines.

Defining Application Rights

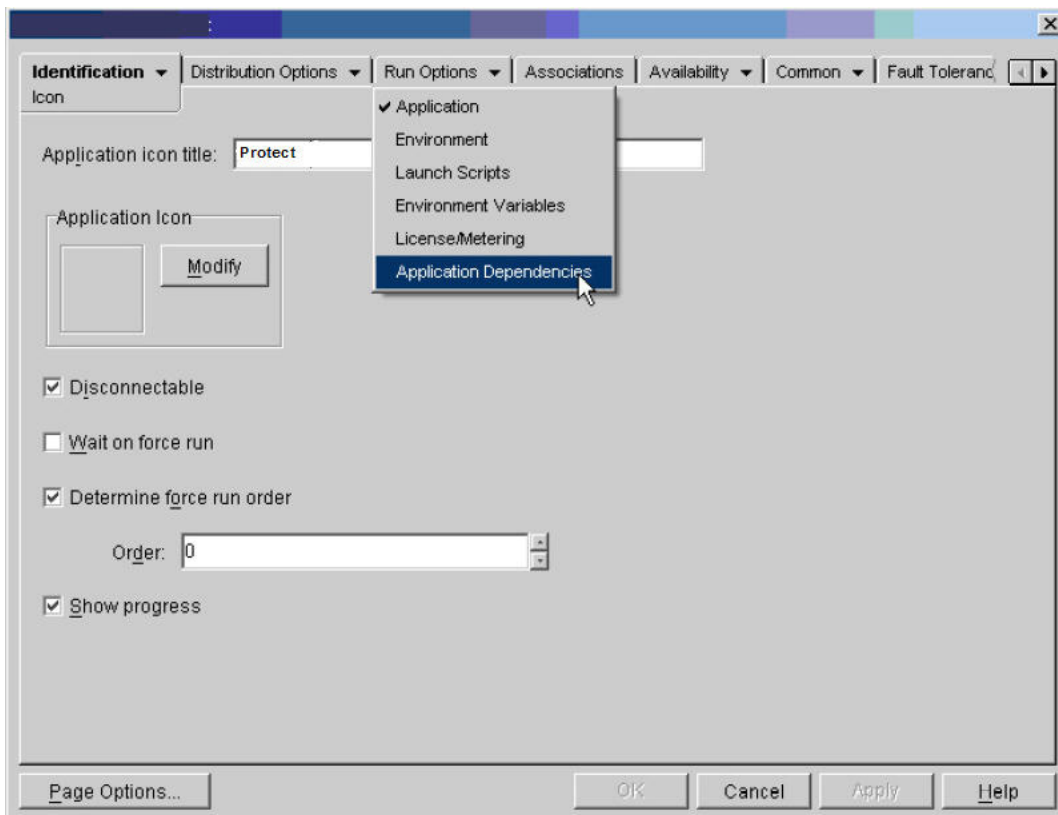
Once a method is chosen, using either the Standard Run Options or the more advanced method of Distribution Scripts, the rights for the application need to be defined.

The easiest way to do this is by giving the application object rights to the AEC program on the server. With an older version of ZENworks, the rights need to be given to a user or a group of users. If rights are assigned through the application object, the user or workstation has those rights as long as it is associated with that application object, regardless of run-once statements, etc.

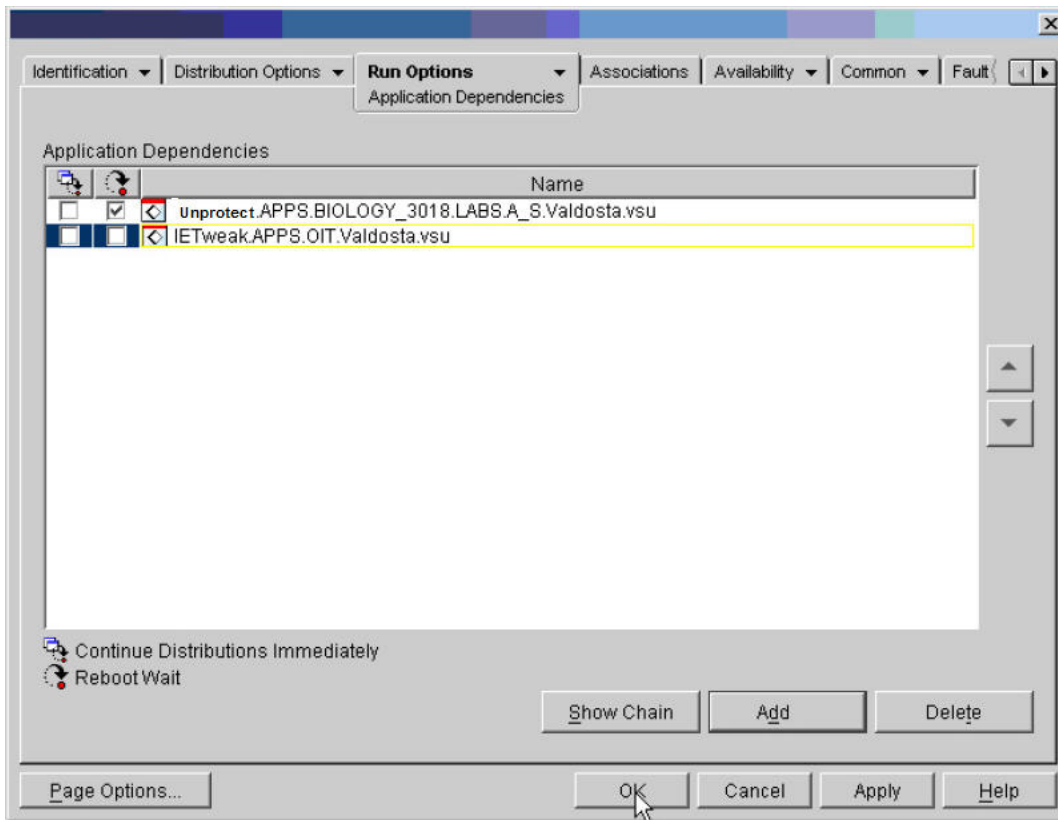
Application Deployment Example

The following example explains how to install an application in a lab where Anti Executable is activated.

1. Create the application to install. The example is a browser tweak called IETweak.
After the application is created, edit the Protect application.



2. Select *Application Dependencies* from the *Run Options* menu, as shown in the following screen.



3. Add the Unprotect application, created in the same manner as the Protect application.
4. Add the application to be installed.

This is an example of how ZENworks and Anti Executable can coexist peacefully. There are limitless combinations of options available in ZENworks.

The following are more advanced options:

- Schedule application deployments using these scripts and wake-on LAN features available in ZENworks
- Do hands-off deployment without users logging in to workstations
- Shut-down machines when deployment is done
- Using the new Enterprise version of Anti Executable, you can:
 - a) See which machines have Anti-Executable activated or deactivated
 - b) Shutdown/Restart machines manually from a central location

There are truly limitless options available when using ZENworks and Anti Executable in combination. Together they give flexibility, versatility, and stability in desktop management facilities.