

FARONICS

ANTI-EXECUTABLE™

ABSOLUTE Protection from
Unauthorized Executables



Faronics Anti-Executable Enterprise Sophos Enterprise

TECHNICAL WHITEPAPER

Last modified: September 9, 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

The process of updating virus definitions on workstations protected by Faronics Anti-Executable Enterprise involves three fundamental steps:

1. Deactivating Anti-Executable.
2. Updating the virus definitions.
3. Reactivating Anti-Executable.

This white paper provides technical information on how to perform these steps with Sophos Antivirus Enterprise.



Faronics Anti-Executable is not marketed as an antivirus product. However, Anti-Executable will protect workstations from any executable form virus. Many viruses come in an executable form, with Anti-Executable installed and activated, these viruses are never run, and therefore never become active.

Deactivating Anti-Executable

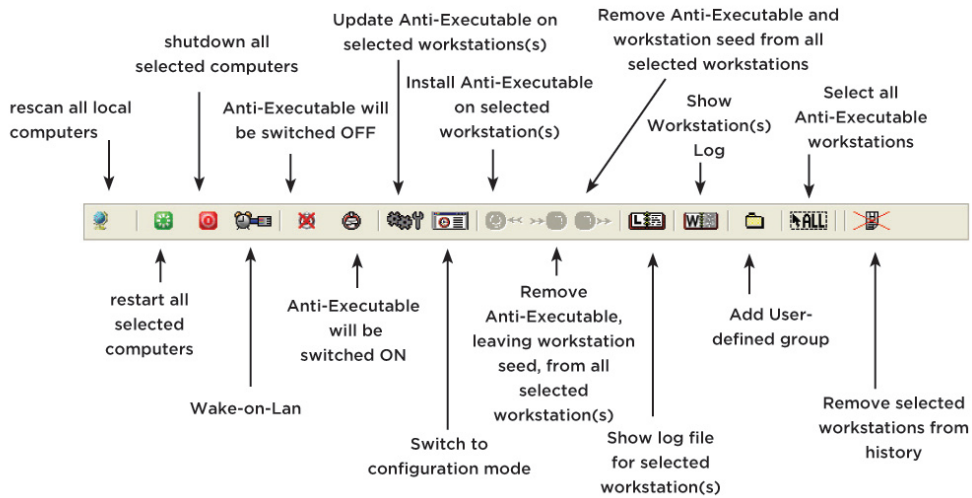
Faronics Anti-Executable protection must be deactivated before updating antivirus definitions. These definitions could include scan engine updates, so Faronics Anti-Executable must be deactivated in order for those updates to be reflected in the whitelist.


There are three ways to remotely deactivate Anti-Executable:

- By manually using the Anti-Executable Enterprise Console
- By setting up a Scheduled Maintenance Period
- By using the Command Line Control

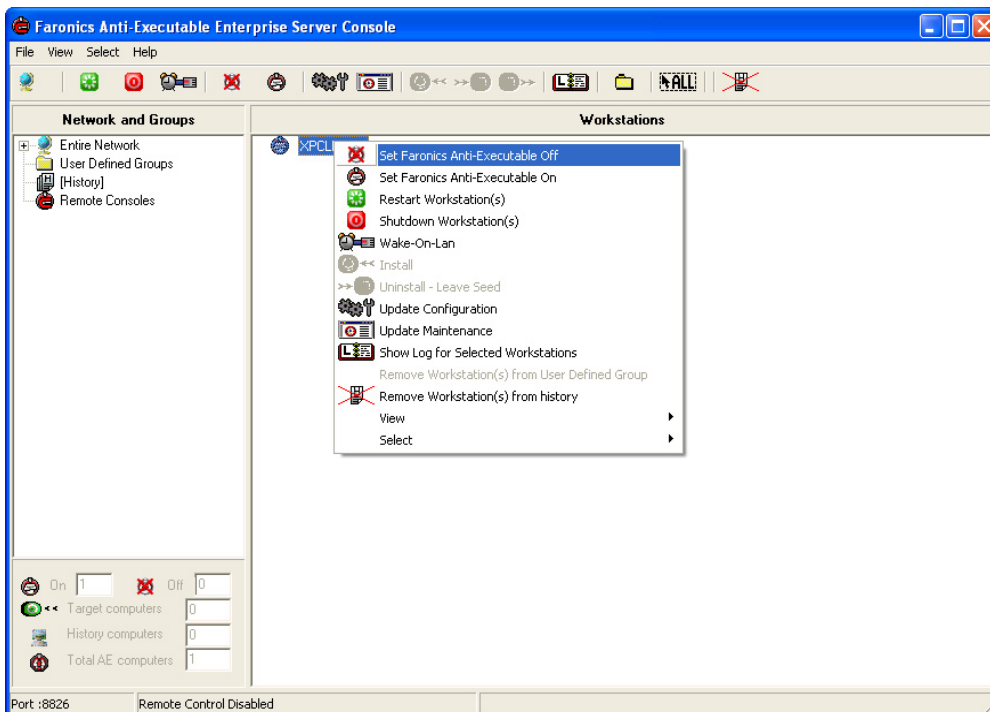
Manually Using the Anti-Executable Enterprise Console

The Enterprise Console contains a toolbar at the top of the screen that allows quick access to the functions of the Console.



To deactivate Anti-Executable, select the workstation and click the *Anti-Executable Off* icon  on the toolbar.

Alternatively, right-click on the workstation and select the *Set Faronics Anti-Executable Off* option in the contextual menu, as shown below.



Setting Up a Scheduled Maintenance Period

There are two ways to set up a Scheduled Maintenance Period. The first is to set it up when configuring the Faronics Anti-Executable Enterprise installation files with the Configuration Administrator (best method for new deployments). The second way is to create or update the Maintenance Period using the Enterprise Console.

The following instructions elaborate on how to create/update the Maintenance Period with the Enterprise Console, assuming Anti-Executable is already deployed throughout the network.

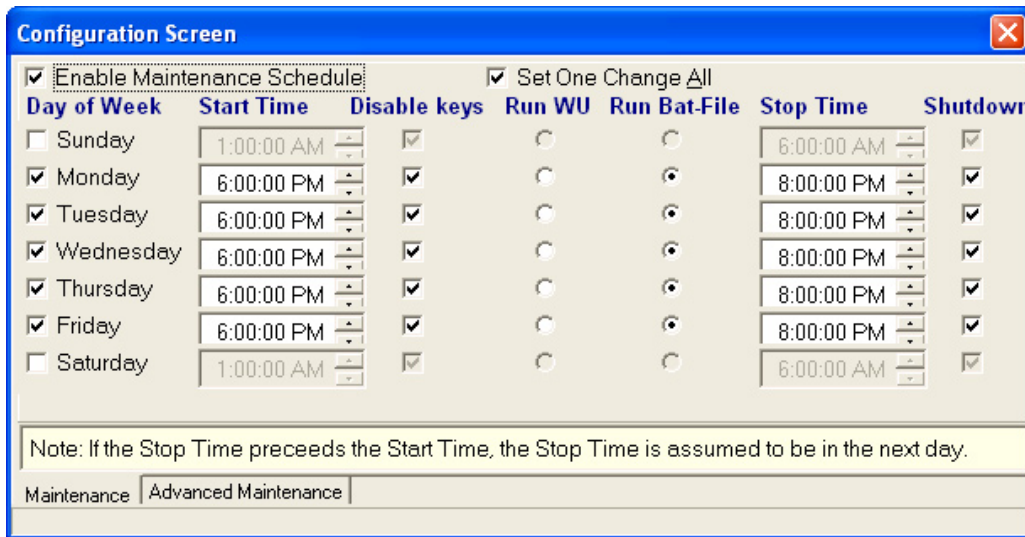
1. Open the Enterprise Console and right-click on any workstation.
Select *Update Maintenance*.



A red bar appears at the bottom of the screen.



2. Click *New*.
The Configuration screen appears, as shown. It only contains the *Maintenance* and *Advanced Maintenance* options.



3. Click on the *Maintenance* tab and place a check in the *Enable Maintenance Schedule* check box. Also place a check beside each day you want the Maintenance Schedule to run.
4. Set the Maintenance start time for each day in the *Start Time* column and the end time in the *Stop Time* column.
5. It is recommended that the *Disable keys* option is checked so the keyboard and mouse are disabled while the workstations are in Maintenance Mode.

Optional: check the *Shutdown* box so Anti-Executable shuts the workstations down at the end of the Maintenance Period.

6. Close the *Configuration* screen. A pop-up message appears requesting the administrator to select the workstations to send the new configuration to.

Select the workstations to be updated and click *Send*. This action updates all the selected workstations' configuration on the fly.

Controlling Anti-Executable Through the Command Line Control - AEC

The Anti-Executable *Command Line Control (AEC)* offers network administrators increased flexibility in managing workstation protected by Faronics Anti-Executable. AEC works in combination with third-party enterprise management tools and/or central management solutions. This combination allows administrators to update workstations on the fly and on demand.

It is important to note that AEC is not a stand-alone application. AEC integrates seamlessly with any solution that can run script files, including standard run-once login scripts.

The AEC executable is installed in same directory as the Configuration Administrator:

C:\Program Files\Faronics\Faronics Anti-Executable Enterprise\AEC.exe

AEC commands require a password with command line rights. One Time Passwords cannot be used.

AEC Options

| Syntax | Description |
|---------------------------------|---|
| AEC password ON | Turn Anti-Executable on |
| AEC password LOW | Set Anti-Executable security to Low* |
| AEC password HIGH | Set Anti-Executable security to High |
| AEC password OFF | Turn Anti-Executable off |
| AEC password CFG=[path] cfg.fzx | Replaces Anti-Executable configuration information. Works when Anti-Executable is On or Off.* |
| AEC ISON | Queries workstation if Anti-Executable is On. Returns 0 if Off. Returns 1 if on. |

* The *Low* security level is not available on Win 9x/Me machines

Example Batch File

Below is a sample batch file that can be modified for use with any antivirus software that supports updating through a command line.

```
@ECHO OFF
\\SERVER\SHARE\FOLDER\AEC.EXE ISON
IF ERRORLEVEL 1 GOTO PROTECTED
IF ERRORLEVEL 0 GOTO UNPROTECTED
ECHO Errors were encountered running the command line control on this
workstation.
:PROTECTED
\\SERVER\SHARE\FOLDER\AEC.EXE password OFF
GOTO END
:UNPROTECTED
REM *****
REM *Insert the command to update the antivirus software here. *
REM *****
\\SERVER\SHARE\FOLDER\AEC.EXE password ON
GOTO END
:END
```

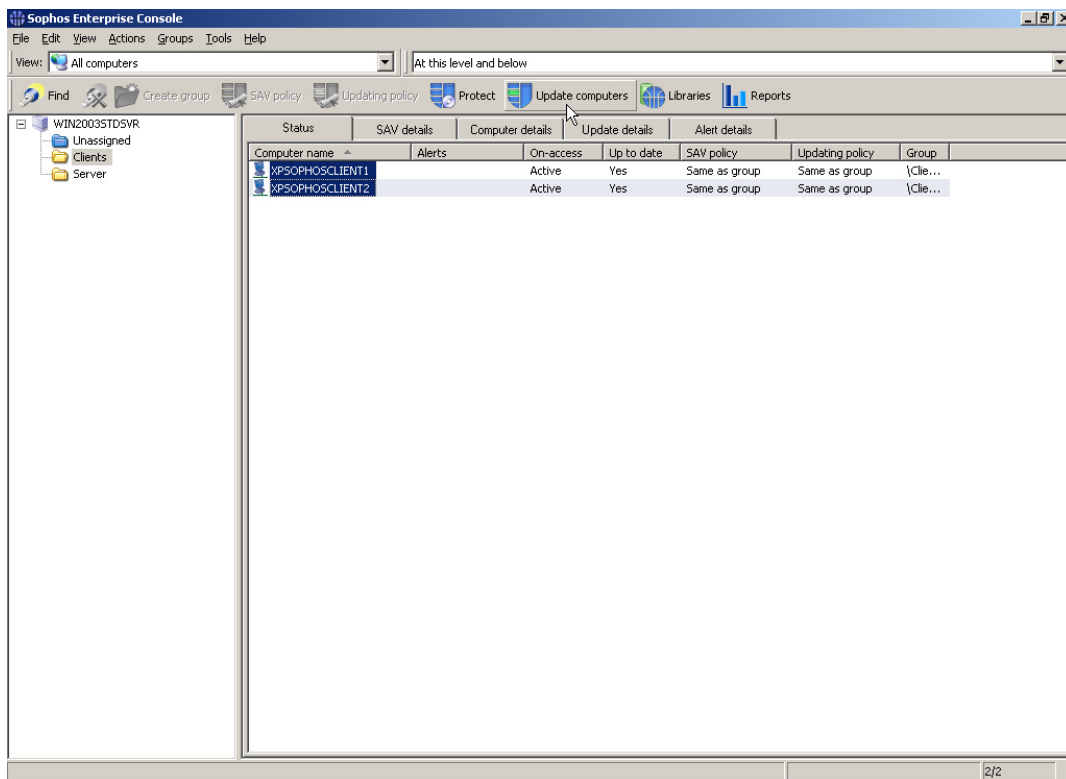
Updating the Virus Definitions

This document provides four different ways to approach virus signature file updates for Sophos Antivirus clients.

1) Manually Updating Virus Definitions

1. Using the Anti-Executable Enterprise Console, turn the Anti-Executable protection off. The change in workstation status is reflected in the console.
2. Start the *Sophos Enterprise Console*. A list of your client machines appears. If the machines need to be updated, the *Up to date* column shows the value *No*.
3. Highlight the client machines to be updated and click *Update Computers*, as shown.

The clients are now updated with the latest file definitions.



2) Scheduling Updates to Occur Automatically (Sophos AutoUpdate)

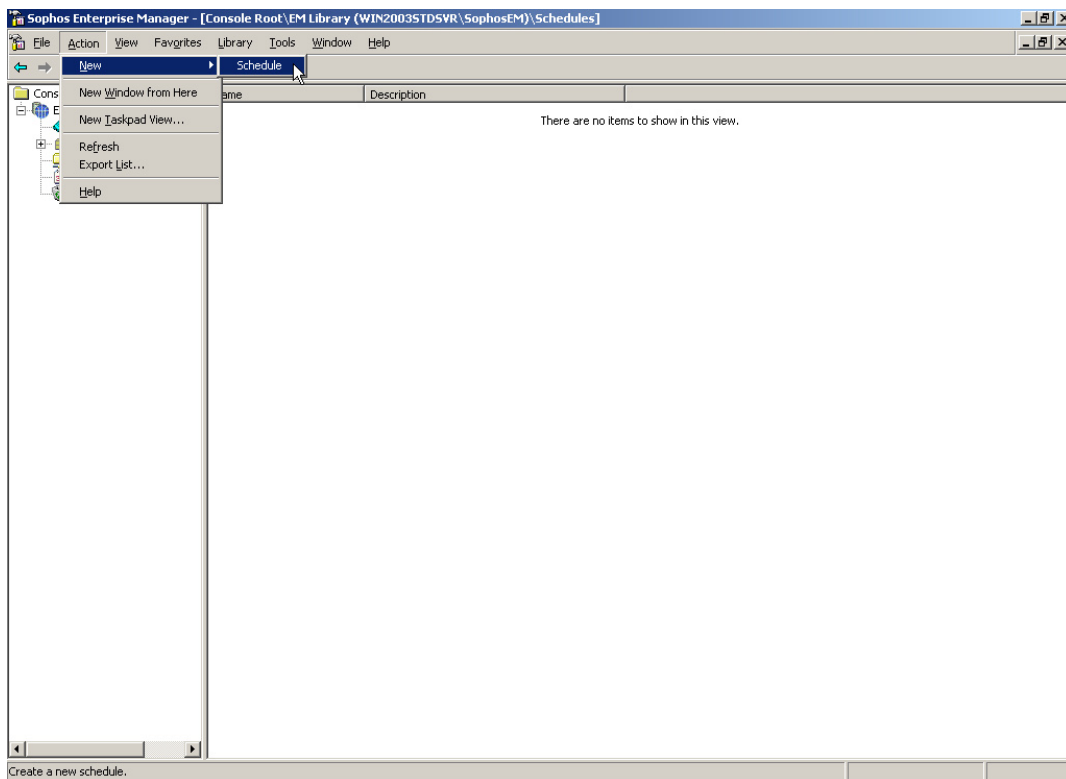
Automatically updating the definitions on client machines must happen during an Anti-Executable maintenance period.

Using Sophos Antivirus Enterprise, the definition updates are first downloaded to the server. The clients can be scheduled to check the server for updates every set number of minutes.

If there is an update on the server, it is downloaded to the clients. By scheduling the server update during the client maintenance period, the clients are able to update the definition files while Anti-Executable is deactivated.

This can be accomplished using the following steps:

1. Open the *Sophos Enterprise Manager*.
2. Select *Action->New->Schedule* as shown.



- In the *Schedule Wizard* dialog that appears, click *Next*.

In the following screen of the wizard, enter a name and description for the scheduled download.

- Specify the time to obtain the Sophos Update files from the Sophos Web site. This should correspond to the period that has been set up for the Anti-Executable Maintenance period.

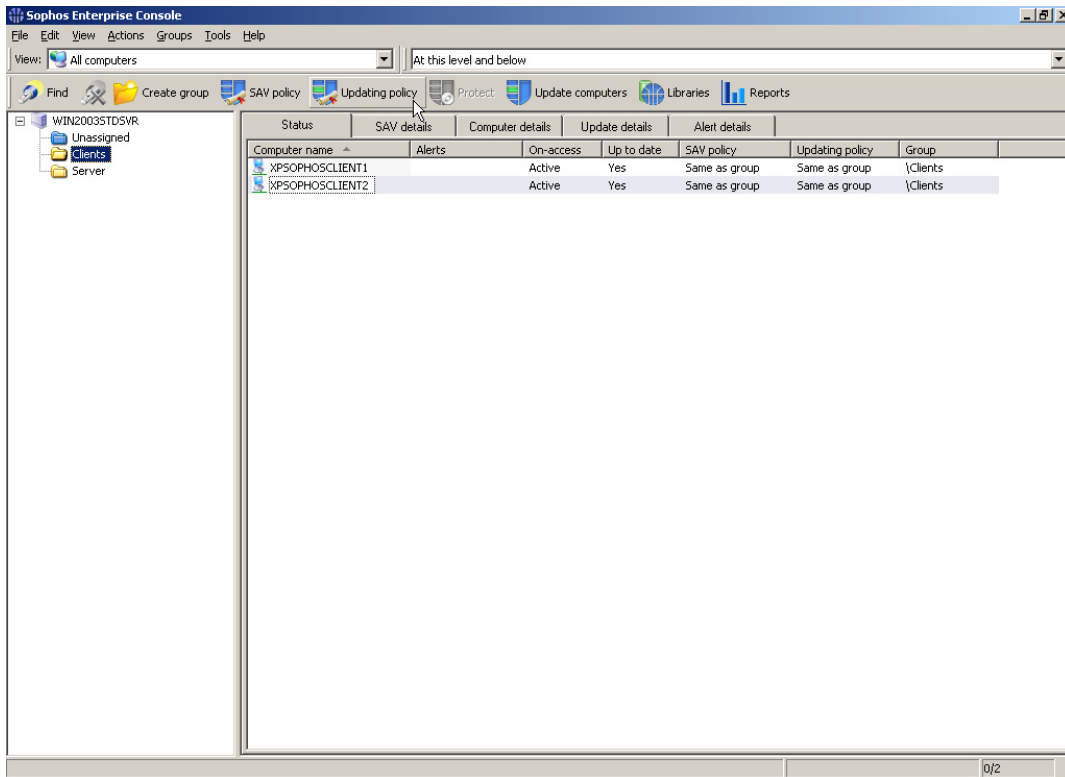
The Anti-Executable Maintenance period can be set using the steps outlined earlier in this document under the section titled, *Setting up a Scheduled Maintenance Period*.

In the following example, we have set up Sophos to download the updates between 8-9 pm. After these updates are downloaded, the *Up to date* column in the Sophos console reports *Yes* for each client. The updates must be downloaded while Anti-Executable is deactivated.

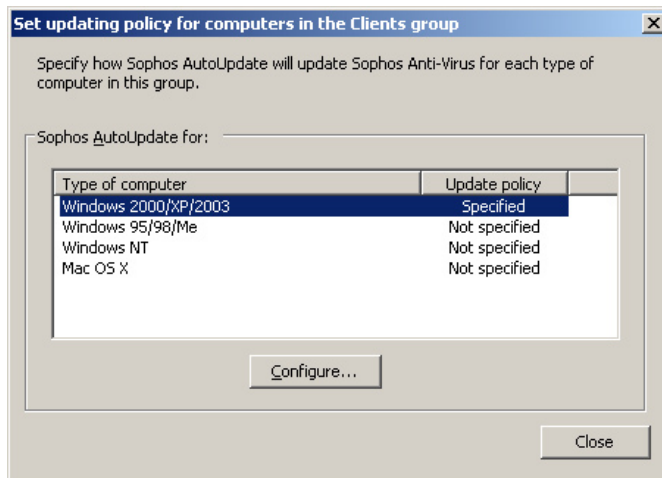
5. Click *Next* followed by *Finish* to complete the wizard. Your scheduled updates appear under your list of scheduled actions in the *Sophos Enterprise Manager*.

The update settings for the clients also need to be set up. This is explained in the following steps.

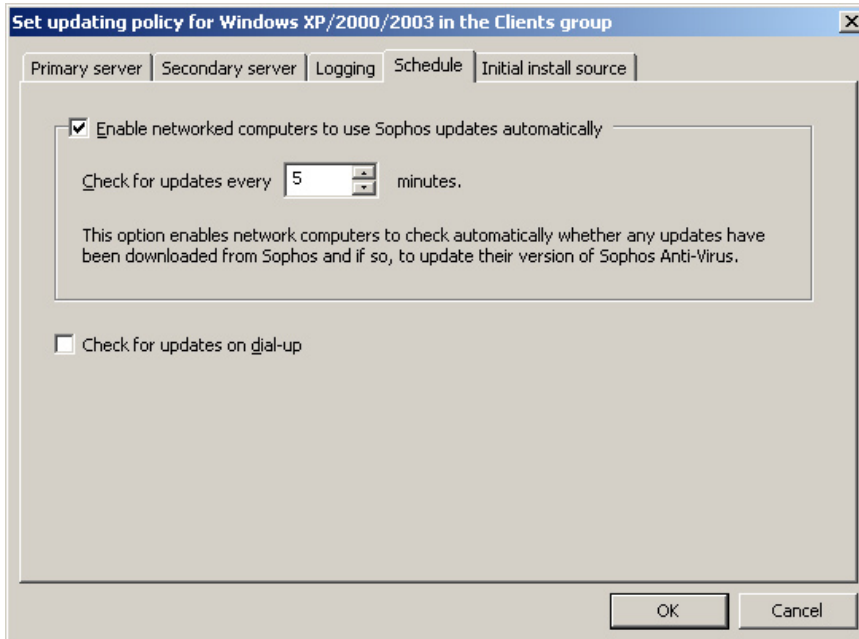
6. Open the *Sophos Enterprise Console*, if it is not already open.
7. Highlight the group that contains your client machines and select the *Updating Policy* button, as shown.



8. The following update policy dialog appears. Select the type of computers being used and click the *Configure* button.



9. Another dialog with several tabs appears, as shown. Select the *Schedule* tab.



10. Check the *Enable networked computers to use Sophos updates automatically* option.

Enter the number of minutes you would like the client machines to check for updates. In this example, the clients look to the Sophos server for updates every 5 minutes.

11. Click *OK*.

With this configuration, the clients will check for updates every 5 minutes. It is assumed the clients will be up-to-date until the Sophos server obtains new updates during the Anti-Executable maintenance period. It is essential that these updates occur during the Anti-Executable Maintenance period; otherwise the clients will attempt to update while Anti-Executable is activated.

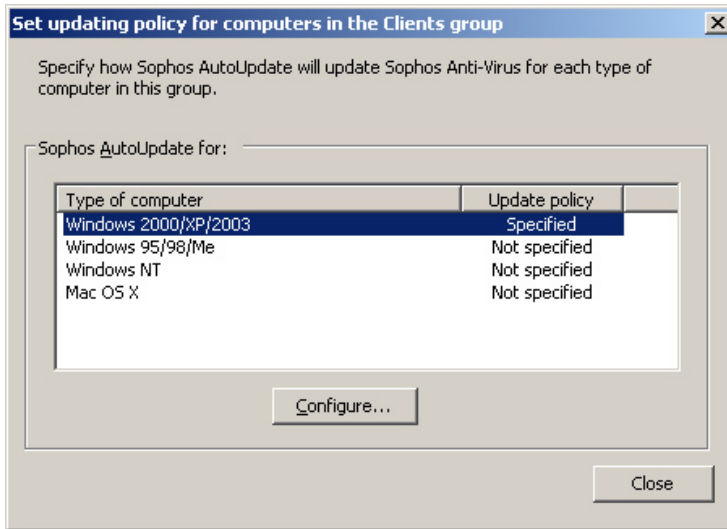
3) Configure Anti-Executable to Run a Batch File to Update the Virus Definitions

Turn Off Client Update Schedule

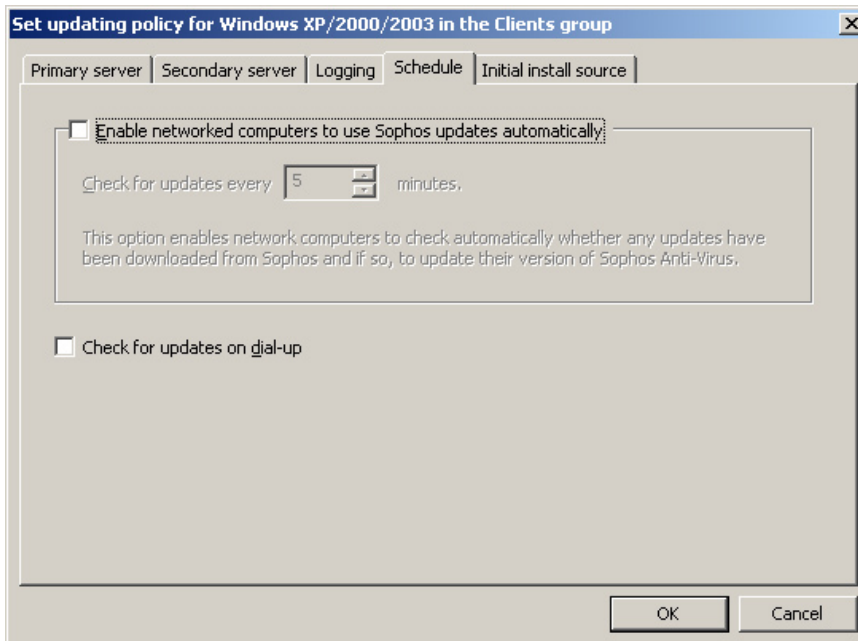
Using this method, turn off scheduled updates in the client update policy and call the update through the use of a script file. The script can be called using a batch file that is run when the Anti-Executable Maintenance period is active. When this script file is run, the client attempts to download the new virus definitions from the server.

1. Using the *Sophos Enterprise Console*, select the group of clients whose update policies are to be modified, and click *Updating Policy*. The updating policy dialog appears.

2. Select the type of computers being used and click *Configure*.



3. Another dialog with several tabs appears.
Select the *Schedule* tab.



4. Uncheck the *Enable networked computers to use Sophos updates automatically* option.
The clients will no longer look to the Sophos server for updates.

Create the Script File

The script file can be created using many different editors. In this case, Notepad is used.

1. Open Notepad and enter the following text:

```
dim obj
set obj = CreateObject("ActiveLinkClient.ClientUpdate.1")
obj.UpdateNow 1,1
```

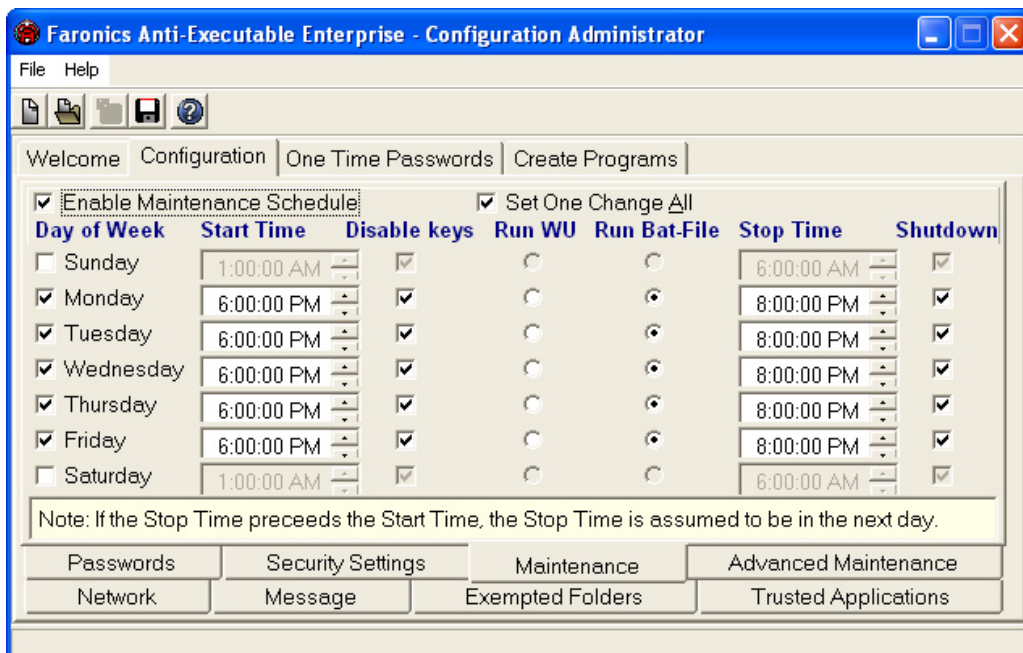
2. Save the Notepad file as *Schedule.vbs*. Do not save the file with the .TXT extension.

When saved successfully, the file icon should appear as follows: 

Set Up Anti-Executable Maintenance to Run the Script

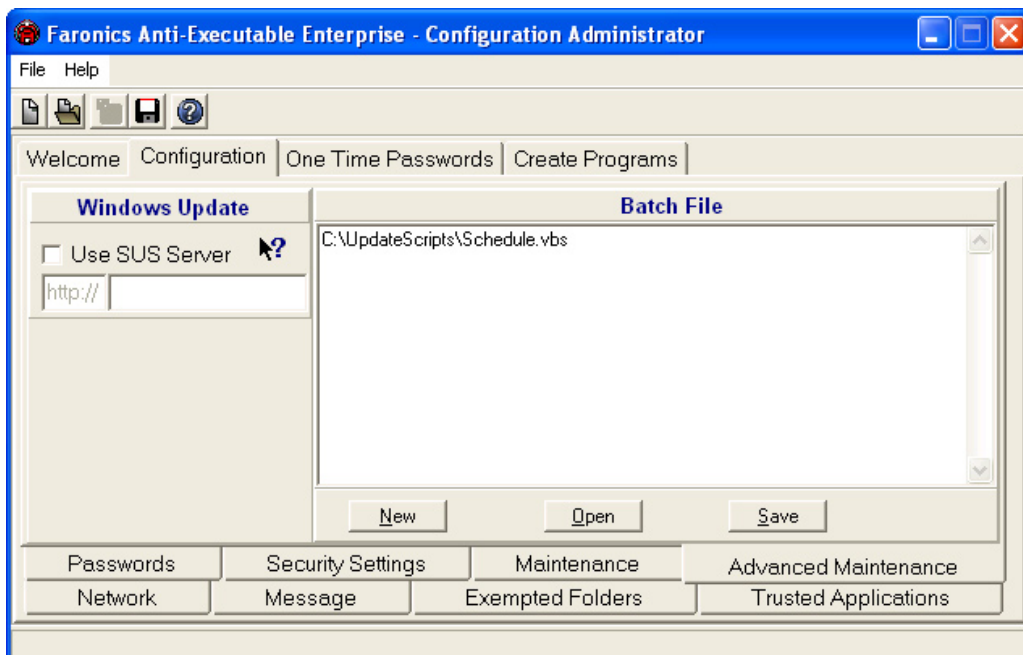
The created script file must now be set up to run during the Anti-Executable Maintenance period. This is done in the *Advanced Maintenance* tab of the Anti-Executable Configuration Administrator.

1. Open the *Anti-Executable Enterprise Server Console* and follow the steps described on page four to set up a Scheduled Maintenance period.
2. Check the *Run Bat File* radio button to allow the workstations to run a batch file automatically during the maintenance period.



3. On the *Advanced Maintenance* tab, type the path and filename of the script in the Batch File editor.

In the following example, the script file path is: C:\UpdateScripts\Schedule.vbs



At this point, the workstations need to be updated with these new settings. Please refer to the Anti-Executable Enterprise user guide with regards to performing a configuration update.

4) Updating Virus Definitions Via a Batch File in a Third-Party Desktop Management Solution

Virus definitions can be also updated running a batch file from a Desktop Management software such as Novell ZenWorks, Altiris, Microsoft SMS, BigFix, etc. Using a batch file, we can call the SCHEDULE.VBS created earlier.

To do this, add a task that runs the following batch file:

```
@ECHO OFF
\\SERVER\SHARE\FOLDER\AEC.EXE ISON
IF ERRORLEVEL 1 GOTO PROTECTED
IF ERRORLEVEL 0 GOTO UNPROTECTED
ECHO Errors were encountered running the command line control on this
workstation.
:PROTECTED
\\SERVER\SHARE\FOLDER\AEC.EXE password OFF
GOTO END
:UNPROTECTED
REM *****
\\SERVER\SHARE\FOLDER\SCHEDULE.VBS
REM *****
\\SERVER\SHARE\FOLDER\AEC.EXE password ON
GOTO END
:END
```