

FARONICS

ANTI-EXECUTABLE™

ABSOLUTE Protection from
Unauthorized Executables



**Faronics Anti-Executable Enterprise
Symantec Antivirus Corporate Edition**

TECHNICAL WHITEPAPER

Last modified: June 1, 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 approach these steps with Symantec Antivirus Corporate Edition.



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 therefore never become active.

Deactivating Anti-Executable

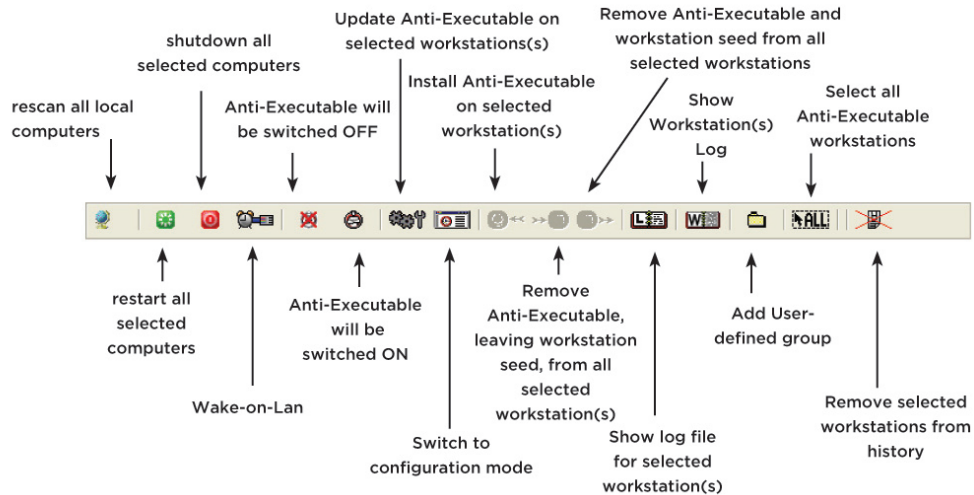
Faronics Anti-Executable protection must be deactivated before updating antivirus definitions. These definitions could include scan engine updates, so Faronics Anti-Executable must be deactivated in order for those updates to be reflected in the whitelist.


There are basically three ways to remotely deactivate Anti-Executable:

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

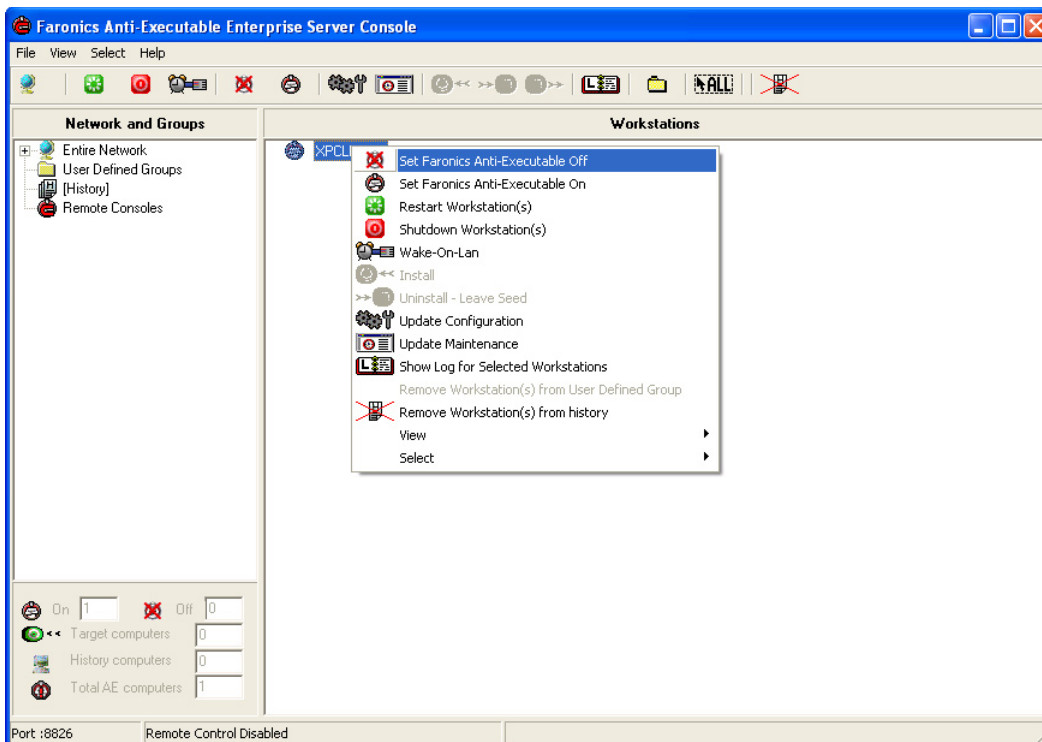
Manually Using the Anti-Executable Enterprise Console

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.

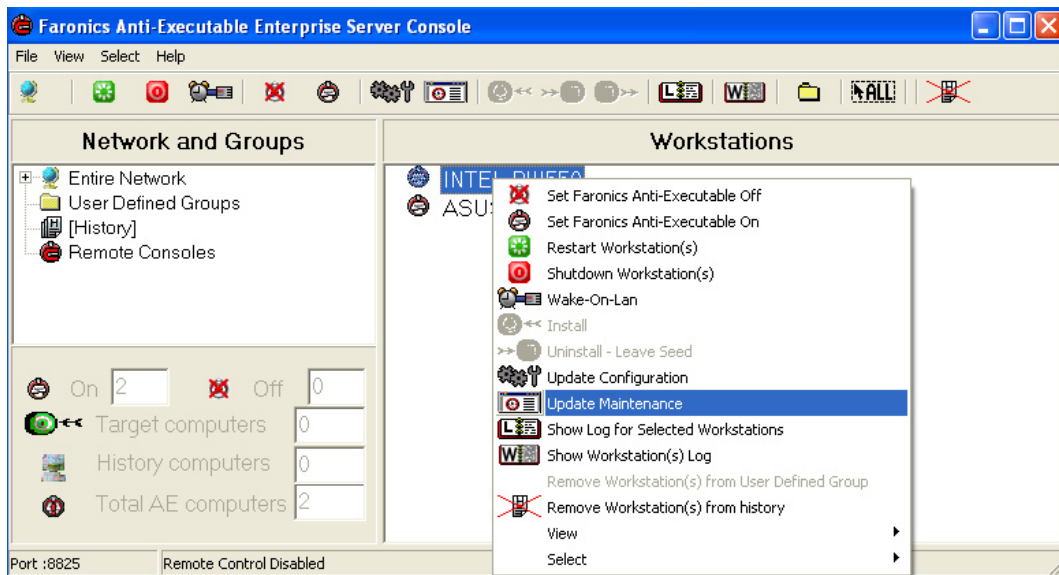


Setting up a Scheduled Maintenance Period

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 Period*.

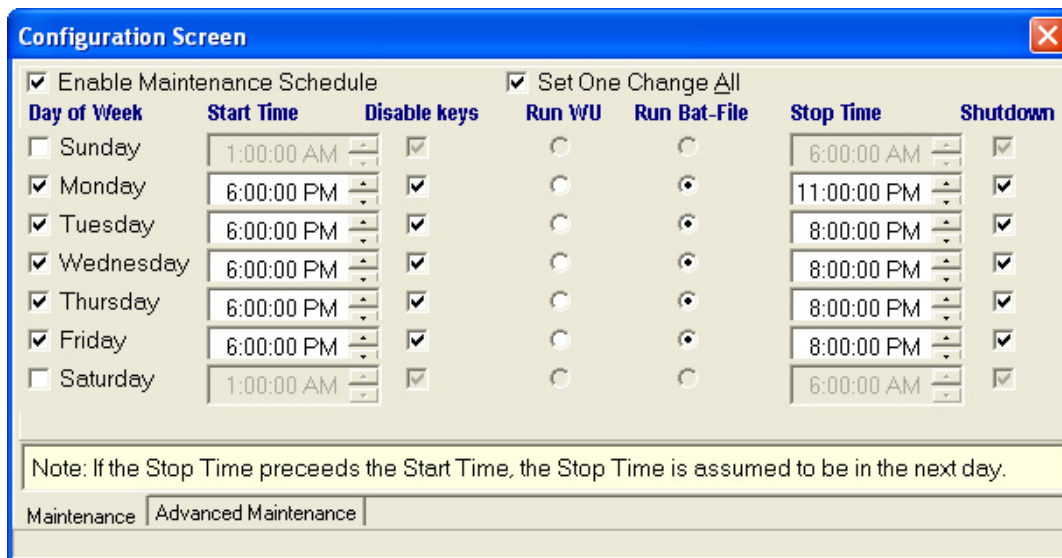


A red bar appears at the bottom of the screen.



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.

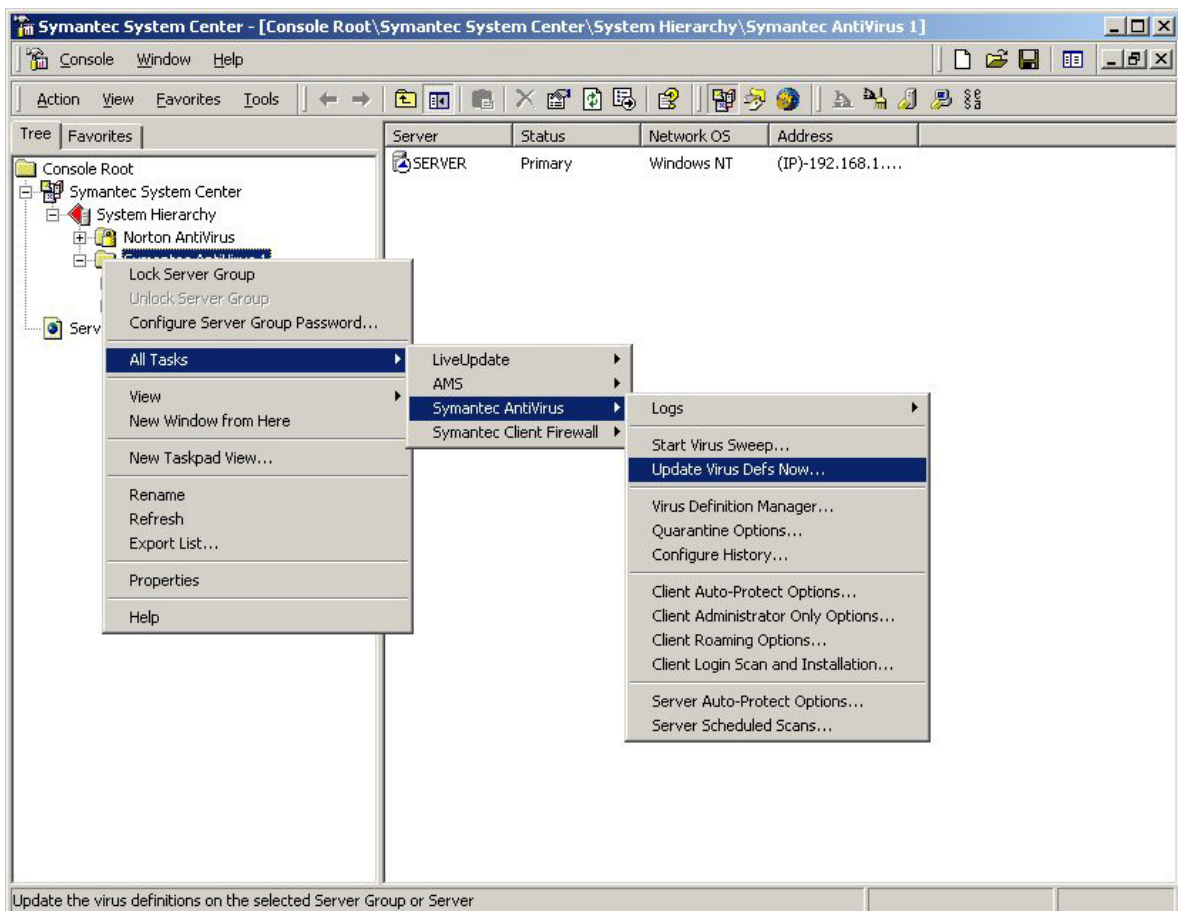
```
@ECHO OFF
\\SERVER\SHARE\FOLDER\AEC.EXE ISON
IF ERRORLEVEL 1 GOTO PROTECTED
IF ERRORLEVEL 0 GOTO UNPROTECTED
ECHO Errors where encountered running the command line control on this
workstation.
:PROTECTED
\\SERVER\SHARE\FOLDER\AEC.EXE password OFF
GOTO END
:UNPROTECTED
REM *****
REM *Insert the command 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 definitions updates for the Symantec Antivirus Corporate edition.

1) Manually Update the New Virus Definitions

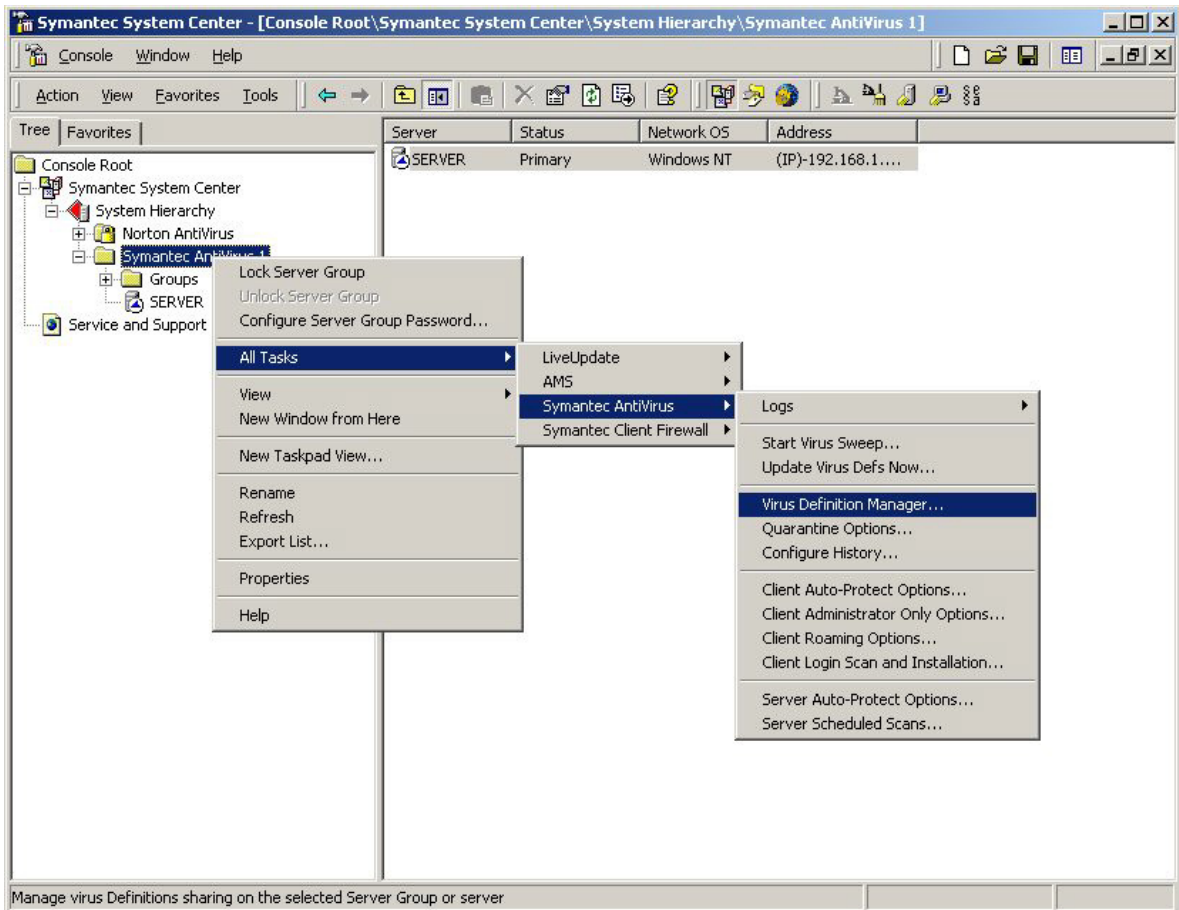
1. Using the Enterprise Console, deactivate Anti-Executable on the workstations. Once the computers are unprotected, open the *Symantec System Center Console* on your antivirus server.
2. Unlock the server group.
3. Right-click on the server group and select *All Tasks > Symantec Antivirus > Update Virus Defs Now*.



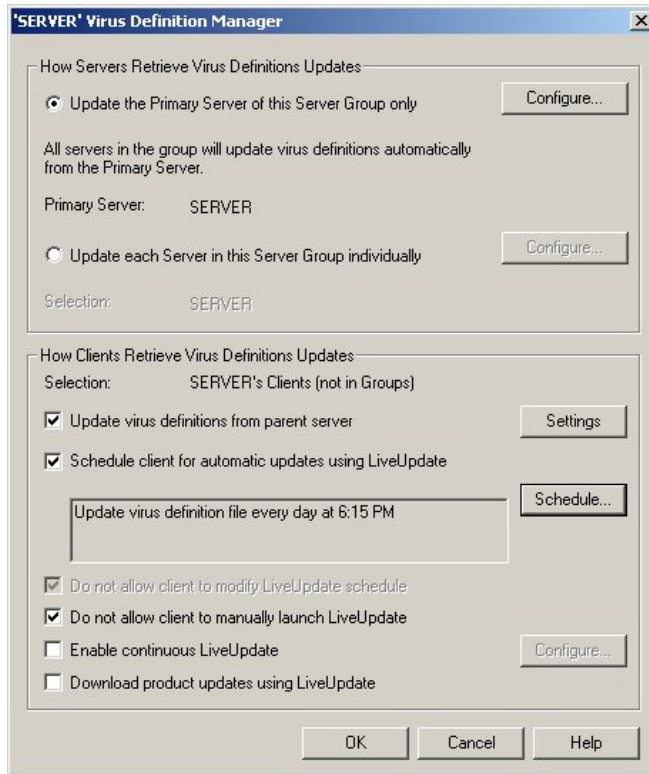
4. Follow the steps presented. The server and the workstations are updated with the latest definitions.

2) Scheduling the Virus Definitions Updates.

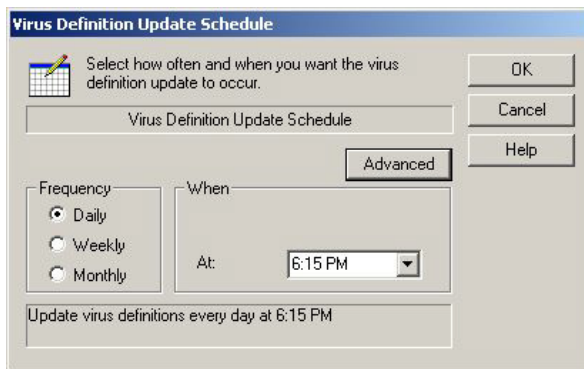
1. Using the Anti-Executable Enterprise Console, schedule a *Maintenance Period* as per instructions provided above.
2. Open the *Symantec System Center Console* on your antivirus server and Unlock the server group. Right-click on the server group and select *All Tasks > Symantec AntiVirus > Virus Definitions Manager*.



The Virus Definitions Manager opens, as shown below.



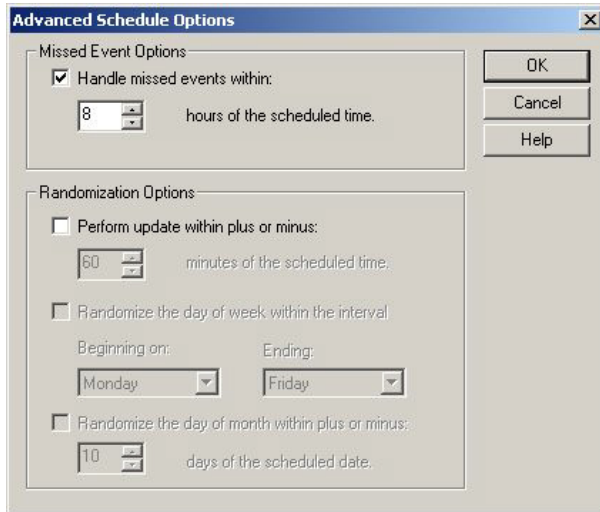
3. Click *Schedule*. Select how often and when you want to update the virus definitions.



In this example, Anti-Executable Enterprise is set to have a maintenance window Monday through Friday from 6:00 pm to 8:00 pm.

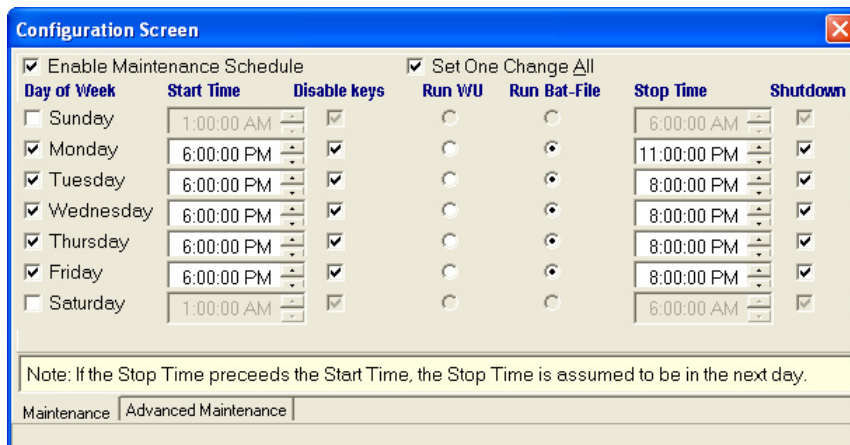
- Click *Advanced* to open the *Advanced Schedule Options*. Uncheck all the Randomization options to force the server to update the new definitions at the scheduled time.

For large networks, you can set up a wider maintenance window and randomize the updates.

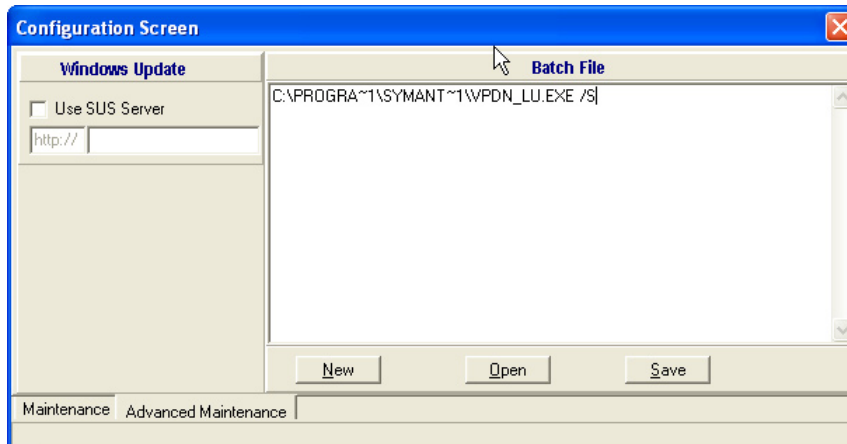


3) Configure Anti-Executable Enterprise to Run a Batch File that Updates the Virus Definitions

- Open the Anti-Executable Enterprise Console and follow the steps on p. 4 to set up a Scheduled Maintenance Period.
- Check on the *Run Bat* radio button to allow the workstations to run a batch file automatically during the Maintenance period.

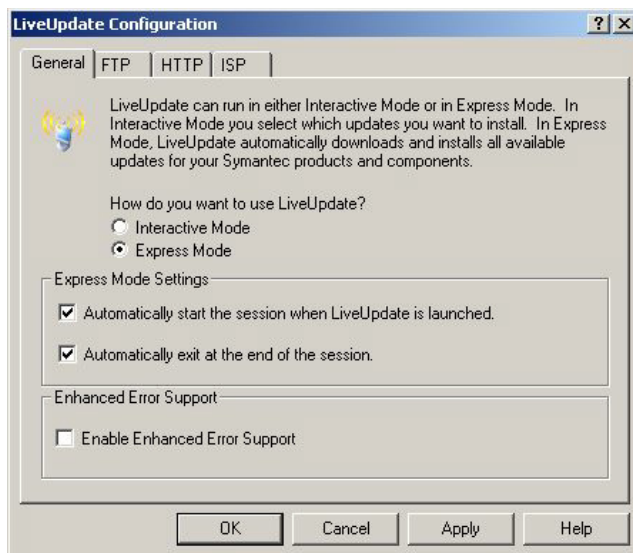


- Click on the *Advanced Maintenance* tab and enter the following line in the Batch File window:
C:\PROGRA~1\SYMANT~1\VPDN_LU.EXE /S



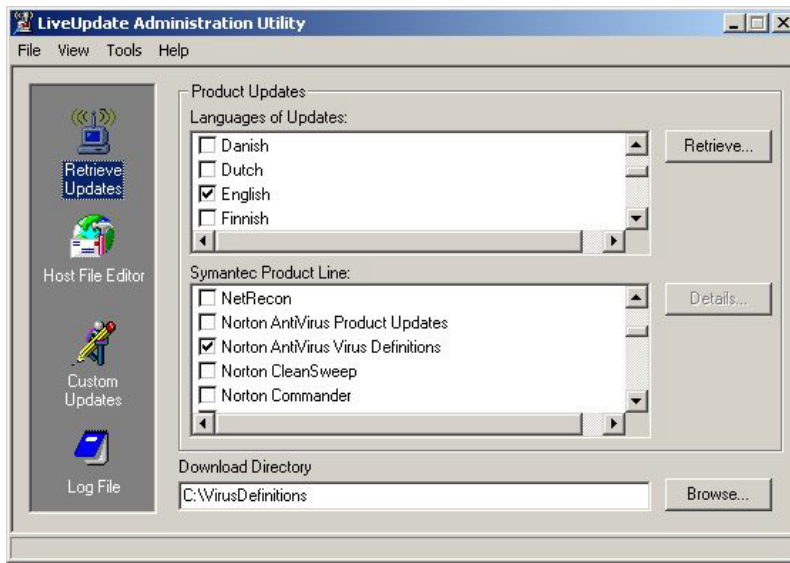
This command calls LiveUpdate, which downloads the virus definitions from the server. For this method to work properly, the LiveUpdate configuration had to be set in the *Express Mode* in every workstation.

4. Open the workstation *Control Panel* and double click on *Symantec LiveUpdate*. The *LiveUpdate Configuration* window appears.
5. Select *Express Mode* and enable both Express Mode settings so the workstation automatically starts the session when LiveUpdate is launched, and exits at the end of the session.

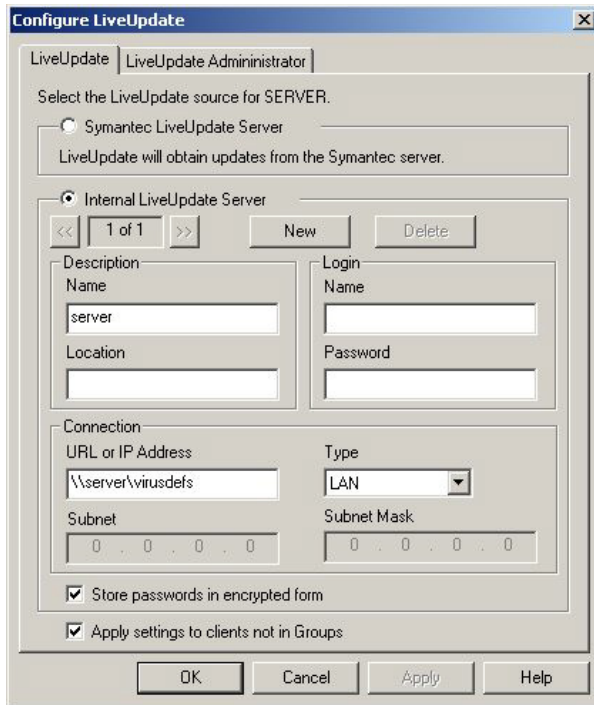


Setting up the LiveUpdate Server

1. Go to *Start > Programs > LiveUpdate Administration Utility > LiveUpdate Administration Utility*.
2. Select the language and the Product Line (in this case, *Norton Antivirus Virus Definitions*) and click *Retrieve*.
3. Make sure that the *Download Directory* is shared so all the workstations have access to it.



4. After the *LiveUpdate Administration Utility* is done downloading the virus definitions, open the Symantec System Center Console and unlock your group.
5. Right-click on the server group and select *All Tasks > LiveUpdate > Configure*. The *Configure LiveUpdate* window appears.



6. Select the *Internal LiveUpdate Server* option.
Enter the server name and the virus definitions folder.
7. Now the workstations are fully configured to receive and keep the latest virus definitions daily.

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.

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 where encountered running the command line control on this
workstation.
:PROTECTED
\\SERVER\SHARE\FOLDER\AEC.EXE password OFF
GOTO END
:UNPROTECTED
REM *****
REM * C:\PROGRA~1\SYMANT~1\VPDN_LU.EXE /S *
REM *****
\\SERVER\SHARE\FOLDER\AEC.EXE password ON
GOTO END
:END
```