

FARONICS

ANTI-EXECUTABLE™

ABSOLUTE Protection from
Unauthorized Executables



Faronics Anti-Executable - Best Practices

TECHNICAL WHITEPAPER

Last modified: December, 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 document was created to give administrators a set of guidelines to follow in order to ensure Anti-Executable is set up and deployed in the most ideal way. This document describes the best way to set up a client machine to use Anti-Executable. It also describes some different methods to administer Anti-Executable for patches and updates.

Implementation

This section explains recommended methods to initially configure your Anti-Executable environment and deploy it to your clients. This section also explains additional configuration settings recommended by Faronics to secure the machines.

Selecting a Customization Code

When configuring a customization code, it is good to use a combination of letters and numbers. It is also recommended to write this code down and store it in a safe place. Unlike a password, a customization code is not easy to change after deployment. Changing the customization code results in having to re-deploy the entire installation of Anti-Executable.

Installation Configuration

When creating a workstation install file, there are many settings that can be configured. A couple of these configuration settings are recommended when creating the install file:

It is recommended that you create a password for the workstation that can be used locally at the client machine. This allows the administrator to deactivate Anti-Executable on the client machine when changes need to be made. It also allows for the possibility that the client machine will not be seen in the Enterprise Console in which case this would be the only way to deactivate the client machine. If the Admin option is toggled, the user is able to modify all of the settings for the client machine, which can be quite useful.

It is also recommended that you set a password for the Command Line Control (CMD). This allows Anti-Executable to be deactivated through a script or batch file.

Installation Deployment

Any deployment solution can be used to push an image with Anti-Executable to your clients. Faronics does not recommend any specific deployment solutions. They should all work with an image that has Anti-Executable installed. In order to successfully deploy an image with Anti-Executable installed, Anti-Executable must be deactivated. This allows for additional drivers to install when the image is pushed to a new machine. For more information about deploying images with Anti-Executable, please refer to the white paper entitled: *Faronics Anti-Executable Enterprise - Master Images and Rapid Deployment* at the following location:

http://www.faronics.com/whitepapers/FAEEnt_RapidDeployment.pdf

Securing the System

The CMOS should be configured to prevent booting from the floppy drive or CD-ROM drive (i.e. set to boot to the hard drive) and the CMOS must be password protected. This is a normal precaution for most public access computers.

Managing the Whitelist

Before installing Anti-Executable, it is recommended that you remove any applications that are not wanted on the machine. During the install of Anti-Executable, a deep file scan is performed on the machine. All applications are then loaded into an encrypted whitelist. There is no way to access this whitelist. New applications are added to the whitelist by simply deactivating Anti-Executable, installing the application, and reactivating Anti-Executable. For more information, please refer to the white paper entitled, *Faronics Anti-Executable Enterprise - Updating Software Solutions* at the following location:

http://www.faronics.com/whitepapers/FAEEnt_UpdatingSoftwareSolutions.pdf

Installation Order With Other Faronics Products

In order to properly install an environment that contains both Deep Freeze and Anti-Executable, it is suggested that you install Deep Freeze first followed by Anti-Executable. This ensures that Deep Freeze is properly added to Anti-Executable's list of authorized executables.

Network Architecture

In a more complex networking environment, it is recommended to use the Server Service Manager. This allows multiple enterprise consoles to be used to administer the Anti-Executable deployment. The Server Service Manager allows packets sent from the clients to be contained to a certain physical area. This keeps the distance the packets need to travel to a minimum, and reduces the chance that the packet would not make it to the console.

A Remote Control Enabled (RCE) Console could be used in place of the Server Service Manager. However, many benefits of the Server Service Manager make it a more suitable choice over the RCE Console.

How the RCE Console or Server Service Manager is used is up to the administrator. There is no specific recommendation on how the Anti-Executable environment is configured. Each situation depends on the network topology. For more information on remote console management, please refer to the white paper entitled, *Faronics Anti-Executable Enterprise - Remote Console Management* at the following location:

http://www.faronics.com/whitepapers/FAEEnt_RemoteConsole.pdf

Network Based Applications

The Anti-Executable whitelist contains all of the authorized applications on the machine. This may lead to the question, "What about network applications?" Network based applications can run on a machine protected by Anti-Executable, depending on the security settings. If Anti-Executable is configured to run on the *High Security Setting* but the *Network Prevention* checkbox is not checked, the network based application will run. If the *Network Prevention* checkbox is checked, the folder running the network application will need to be added to the *Exempted Folders*.

For more information about the different settings available for Anti-Executable, please refer to the *Faronics Anti-Executable Enterprise User Guide* at the following location:

http://www.faronics.com/doc/FAEEnt_Manual.pdf

Maintenance

The following information provides recommendations for managing an Anti-Executable deployment.

To Patch or Not to Patch

This debate has gone on for quite some time. There is no specific recommendation whether to keep machines up to date or to never patch the machines. Both methods have their advantages. This may come down to the policy that has been implemented within the organization.

Antivirus Requirements

Anti-Executable prevents unauthorized applications from running. This whitelist technology is very efficient at blocking harmful malware. This leads to the question, "Do I need Antivirus protection if I have Anti-Executable?" Faronics does not suggest removing Antivirus tools. In today's computing world, it is better to have more protection than not enough.

Patch Management

Several methods can be used to update machines protected by Anti-Executable:

1. Use the Scheduled Maintenance feature to set up a period during which Anti-Executable is deactivated and updates can be sent to the workstations.

During the Scheduled Maintenance period, an option can be set to disable the keyboard and mouse at the workstation, allowing for updates to only take place via the network.

2. Use the Anti-Executable Command Line Control (AEC)

AEC can be integrated into your existing imaging or management solution or you can use run-once login scripts. AEC also has a query feature for you to check the status of the computers - whether Anti-Executable is On or Off - and then make decisions based on that status. These features combined offer you the ability to update your workstations "on demand". For more information about the Command Line Control, please refer to the white paper entitled, *Faronics Anti-Executable Enterprise - Remote Administration with Secure Command Line Control* at the following location:

http://www.faronics.com/whitepapers/FAEEnt_RemoteAdministration.pdf

3. Use the Enterprise Console to centrally toggle the Anti-Executable protection on workstations and make them available for updating.