



FARONICS
ANTI-EXECUTABLE[™]
ENTERPRISE

ABSOLUTE Protection from Unauthorized Executables

User Guide



FARONICS[™]
Intelligent Solutions for ABSOLUTE Control

www.faronics.com

Last modified: December, 2009

© 1999 - 2009 Faronics Corporation. All rights reserved. Faronics, Deep Freeze, Faronics Core Console, Faronics Anti-Executable, Faronics Device Filter, Faronics Power Save, Faronics Insight, Faronics System Profiler, and WINSelect are trademarks and/or registered trademarks of Faronics Corporation. All other company and product names are trademarks of their respective owners.

Contents

- Preface 5**
- Important Information 6
 - About Faronics 6
 - Product Documentation 6
- Technical Support 7
 - Contact Information. 7
- Definition of Terms 8

- Introduction 10**
- Anti-Executable Overview 11
 - About Anti-Executable 11
 - Anti-Executable Editions. 11
 - About Faronics Core Console. 11
- System Requirements 12
 - Console Requirements 12
 - Workstation Requirements 12
- Anti-Executable Licensing 13

- Installing Anti-Executable 15**
- Installation Overview. 16
- Installing Anti-Executable Loadin 17
- Installing Anti-Executable on a Workstation Manually 21
- Installing or Upgrading Anti-Executable on a Workstation via Faronics Core Console 25

- Accessing Anti-Executable 27**
- Overview 28
- Accessing Anti-Executable via Faronics Core Console. 29
 - Anti-Executable Columns in Faronics Core Console 29
 - Executing Anti-Executable Commands via Faronics Core Console 29
 - Scheduling Actions 31
- Accessing Anti-Executable Enterprise on a Workstation 32

- Using Anti-Executable 33**
- Overview 34
- Status Tab 35
 - Verifying Product Information 35
 - Enabling Anti-Executable Protection. 36
 - Anti-Executable Maintenance Mode 36
 - Exporting Anti-Executable Configurations 36
 - Retrieving settings from Faronics Core Console 37
- White List Tab. 38
 - White List Management through Faronics Core Console 38
 - Using The Anti-Executable White List Editor 39
 - Creating a New White List 40
 - Activating a White List 42
 - Adding Executables or Folders to an Existing White List Using the White List Editor 43

Adding Blocked Executables to the Active White List	44
Black List Tab	45
Black List Management through Faronics Core Console	45
Using The Anti-Executable Black List Editor	46
Creating a New Black List	47
Activating a Black List	49
Adding Executables or Folders to an Existing Black List Using the Black List Editor	49
Users Tab	50
Adding an Anti-Executable Administrator or Trusted User	50
Removing an Anti-Executable Administrator or Trusted User	51
Enabling Anti-Executable Passwords	52
Setup Tab	53
Setting Event Logging in Anti-Executable	53
Anti-Executable Stealth Functionality	53
Deep Freeze Maintenance Compatibility	54
Customizing Alerts	54
Creating an Anti-Executable Report through Faronics Core Console	55
Command Line Control	57
Command Line Control	58
Silent Install Commands	60
Uninstalling Anti-Executable	61
Uninstalling Using Faronics Core Console	62
Uninstalling on a Workstation using the Uninstall Wizard	63
Uninstalling the Anti-Executable Loadin	65

Preface

Anti-Executable protects computers by preventing unauthorized executables from running.

Topics

Important Information

Technical Support

Definition of Terms

Important Information

This section contains important information about your Faronics Product.

About Faronics

Faronics delivers market-leading solutions that help manage, simplify, and secure complex IT environments. Our products ensure 100% machine availability, and have dramatically impacted the day-to-day lives of thousands of information technology professionals. Fueled by a market-centric focus, Faronics' technology innovations benefit educational institutions, health care facilities, libraries, government organizations, and corporations.

Product Documentation

The following documents form the Faronics Anti-Executable documentation set:

- *Faronics Anti-Executable User Guide* — This document guides you how to use the product.
- *Faronics Anti-Executable Release Notes* — This document lists the new features, known issues and closed issues.
- *Faronics Anti-Executable readme.txt* — This document will guide you through the installation process.

Technical Support

Every effort has been made to design this software for ease of use and to be problem free. If problems are encountered, contact Technical Support

Email: support@faronics.com

Phone: 800-943-6422 or 604-637-3333

Hours: Monday to Friday 7:00am to 5:00pm (Pacific Time)

Contact Information

- Web: www.faronics.com
- Email: sales@faronics.com
- Phone: 800-943-6422 or 604-637-3333
- Fax: 800-943-6488 or 604-637-8188
- Hours: Monday to Friday 7:00am to 5:00pm (Pacific Time)
- Address: Faronics Technologies USA Inc.
2411 Old Crow Canyon Road, Suite 170
San Ramon, CA 94583
USA

Faronics Corporation
609 Granville Street, Suite 620
Vancouver, BC V7Y 1G5
Canada

Definition of Terms

Term	Definition
Alert	The notification dialog that appears when there is an attempt to launch an unauthorized executable. Anti-Executable Administrators can specify the message and image displayed in the alerts. For more information, refer to Exporting Anti-Executable Configurations .
Anti-Executable Administrator	Anti-Executable Administrators have access to all Anti-Executable configuration options. They can create and edit White Lists, Black Lists, manage Anti-Executable users, set Anti-Executable protection to Enabled or Disabled, and uninstall/upgrade Anti-Executable.
Anti-Executable Console Loadin	A software library that extends the functionality of Faronics Core Console allowing full control over the configuration and operation of Anti-Executable installed on remote workstations.
Anti-Executable Trusted User	Trusted Users have access to Status tab, White Lists tab and Black Lists tab. They can create and edit White Lists, Black Lists, and set Anti-Executable protection to <i>Enable</i> or <i>Disable</i> . Trusted Users cannot uninstall/upgrade Anti-Executable.
Authorized Executable	An Executable that is in the Active White List and therefore can be launched.
Black Folder	A folder, and its sub-folders, from which all executables are blocked.
Black List	A list of executables, or folders containing executables, that are blocked by Anti-Executable.
Executable	Any file that can be launched by the operating system. The executable files managed by Anti-Executable have the extension <i>.scr</i> , <i>.jar</i> , <i>.bat</i> , <i>.com</i> , or <i>.exe</i> .
External User	Any user that is neither an Anti-Executable Administrator nor an Anti-Executable Trusted user. An external user can run only authorized executables and has no control over Anti-Executable configuration. This restriction applies regardless of any user rights assigned by the operating system.
Faronics Core Agent	The software installed on workstations to enable communication with Faronics Core Console.
Maintenance Mode	When in Maintenance Mode, new executable files added or modified are automatically added to the Active White List.
Protection	When set to <i>Enabled</i> , this setting indicates that Anti-Executable is protecting a computer with an Active White List. When set to <i>Disabled</i> , any executable can be launched on the computer.

Term	Definition
Stealth Mode	Stealth Mode is a group of options that control visual indication of Anti-Executable's presence on a system. Stealth Mode provides the option to the Administrator to hide the Anti-Executable icon in the Windows system tray, prevent the Alert from being displayed and prevent the splash screen from being displayed.
Trusted Executable	A Trusted executable can launch other executables that themselves are unauthorized.
Unauthorized Executable	An Unauthorized executable is one that is not in the Active White List and can not be launched.
White Folder	A folder, and its sub-folders, from which any executable can be launched.
White List	A list of executables, or folders containing executables, that are allowed to run by Anti-Executable.
Workstation	Any client or remote machine using the Operating System specified in the System Requirements.

Introduction

Anti-Executable protects machines by preventing unauthorized executables from running.

Topics

[Anti-Executable Overview](#)

[System Requirements](#)

[Anti-Executable Licensing](#)

Anti-Executable Overview

About Anti-Executable

Anti-Executable prevents unauthorized executables from running, giving IT administrators total control over the computer. Any executable file that is not part of a list of files called the White List will not run. This White List is under the complete control of authorized users who can edit it, modify it, erase it, etc.

Nothing gets past Anti-Executable: attempts to rename the executable files, or run them from removable storage devices, or even from the network will be blocked, leaving your machines safe and saving you time, money, and effort.

Anti-Executable Editions

Faronics Anti-Executable has four different editions available. Whether you have servers or workstations, working standalone or as part of a network, Anti-Executable will provide you with the protection that you need. Choose the Anti-Executable edition that best suits your needs:

Edition	Use Anti-Executable to protect
Standard	Local computers loaded with non-server operating system
Server Standard	Local computers loaded with server operating systems
Enterprise	Remote computers loaded with non-server operating system*
Server Enterprise	Remote computers loaded with server operating systems*

*Enterprise versions allow to protect multiple computers from a central console called Faronics Core Console.

About Faronics Core Console

Faronics Core Console is a lightweight, high performance, secure, easy-to-learn, and integrated framework for the management of multiple Faronics products. It provides a consistent and reliable method of displaying, managing, installing, updating, and protecting workstations and servers from a single console, allowing your organization to increase efficiency with a complete management solution for Faronics products.

Enterprise Versions of Anti-Executable allow you to protect multiple workstations via Faronics Core Console.

System Requirements

Console Requirements

Information on Faronics Core Console system requirements can be found in the Faronics Core Console user's guide.

Workstation Requirements

Anti-Executable can be installed on the following operating systems:

- 32-bit edition of Windows XP SP3 and 64-bit edition of Windows XP SP2.
- 32- and 64-bit editions of Windows Server 2003, Windows Server 2008, Windows Vista, and Windows 7.

Anti-Executable Licensing

Anti-Executable is available in both Full and Evaluation versions. An Evaluation version can be downloaded for free from Faronics' web site (www.faronics.com) and it will be fully operational for 30 days after installation. An expired Evaluation version will not protect the machine and must be uninstalled or upgraded to a Full Version. A Full version requires a valid License Key in order to protect the machine.

License information can be entered multiple ways depending on the configuration:

- From the Console
- On an individual workstation
- Through the command line



Server editions of Anti-Executable cannot be installed on a non-Server Operating System. License Keys for Server editions of Anti-Executable cannot be used on non-Server editions.

Non-Server editions of Anti-Executable cannot be installed on a Server Operating System. License Keys for Non-Server editions of Anti-Executable cannot be used on Server editions.



Installing Anti-Executable

This chapter describes the installation process of Anti-Executable.

Topics

[Installation Overview](#)

[Installing Anti-Executable Loadin](#)

Installation Overview

The Anti-Executable Loadin must be installed to facilitate the execution of Anti-Executable specific tasks from Faronics Core Console. Once the Loadin has been installed, Anti-Executable can be installed, configured, upgraded or uninstalled on remote computers from Faronics Core Console.

Following a successful Anti-Executable deployment, Faronics Core Console can then be used to administer all Anti-Executable tasks and commands.

Anti-Executable features installers for 32- and 64-bit versions of Windows Server 2003, Windows Server 2008, Windows XP SP3, and Windows Vista.

If you are installing on a remote computer via Faronics Core Console, the appropriate installer is selected automatically. However, before installing manually, verify the operating system version and choose the installer from the following list:

System	Install File
Windows XP/Vista (32-bit)	AEEnt_32-bit.msi
Windows XP/Vista (64-bit)	AEEnt_64-bit.msi
Windows Server 2003 and Windows Server 2008 (32-bit)	AESrvEnt_32-bit.msi
Windows Server 2003 and Windows Server 2008 (64-bit)	AESrvEnt_64-bit.msi

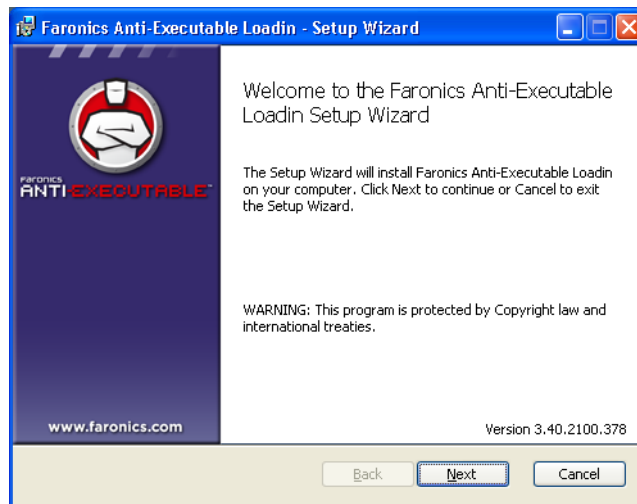
Installing Anti-Executable Loadin



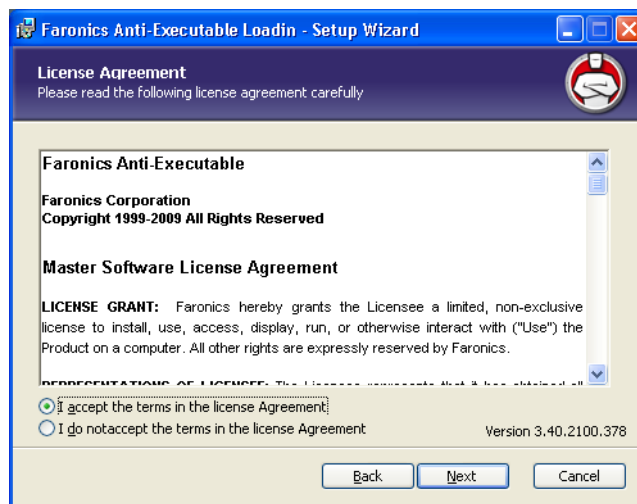
The Anti-Executable Loadin cannot be installed on a computer that does not have Faronics Core Console installed.

Anti-Executable can be installed using the Setup Wizard. To install Anti-Executable, complete the following steps:

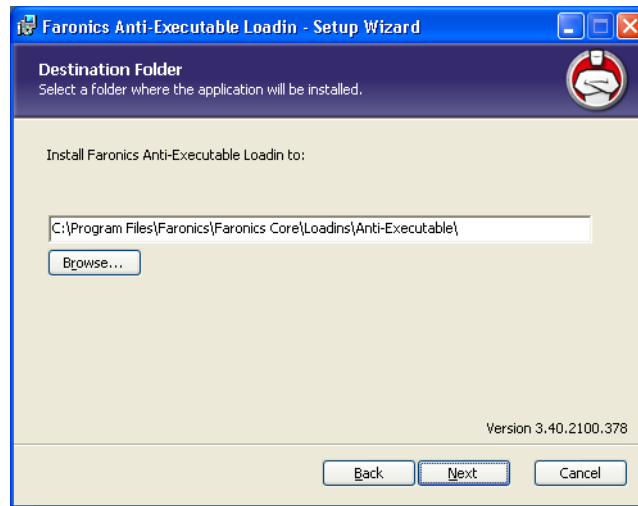
1. Insert the CD-ROM from the Media Package into the CD-ROM drive. If Anti-Executable has been downloaded via the Internet, double-click the *Anti-Executable_Console_Loadin_Installer.exe* file to begin the installation process. Click *Next* to continue.



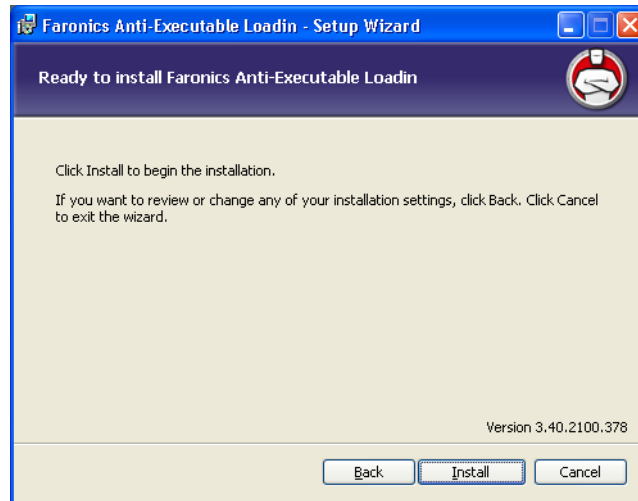
2. Read and accept the License Agreement. Click *Next* to continue.



3. Specify the install location. The default is `C:\Program Files\Faronics\Faronics Core\Loadins\Anti-Executable`. Click *Next* to continue.



4. Click *Install* to begin the installation.

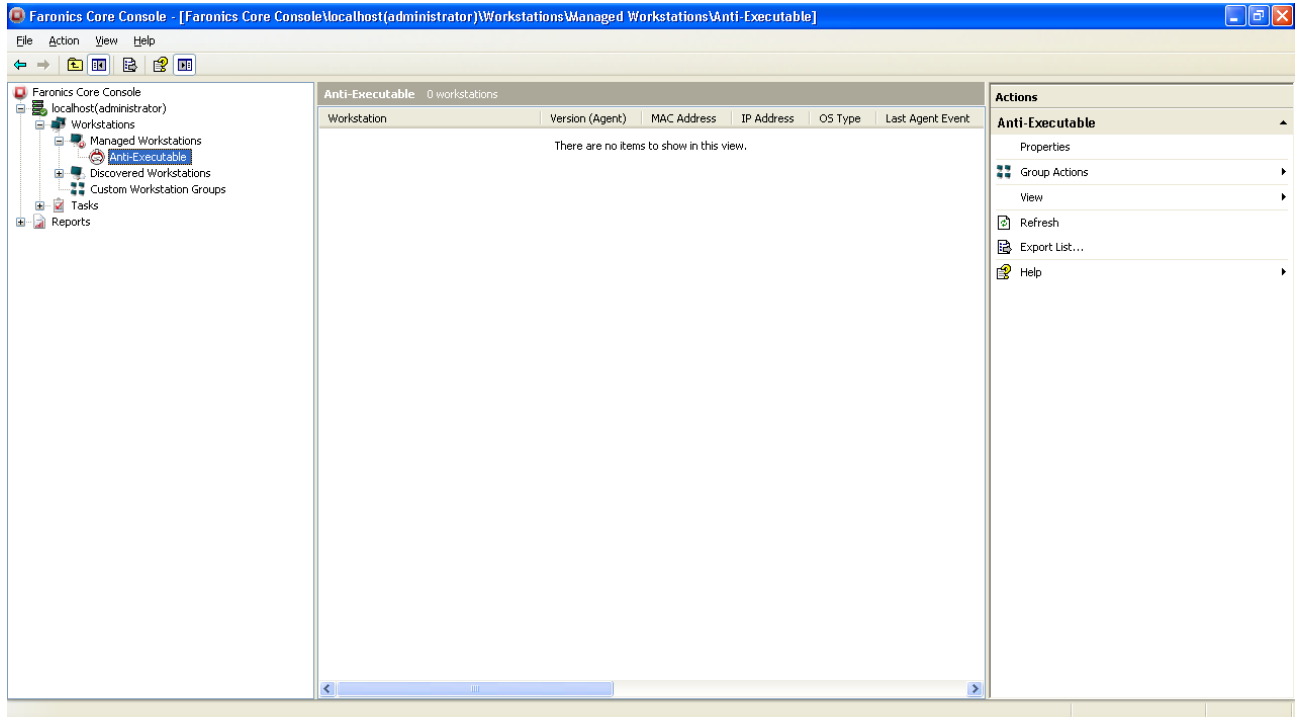


5. Click *Finish* to complete the installation.



If Faronics Core Console was running when Anti-Executable was being installed, an immediate Faronics Core Console restart is recommended following installation.

Once the Loadin has been successfully installed, Faronics Core Console displays a list of Anti-Executable specific features in the Actions pane when one or more workstations have been selected. There are also specific columns displayed in the workstation list as illustrated below. Anti-Executable features are also available by selecting one or more workstations and using the right-click contextual menu.



The Faronics Core Console screen is divided into three main parts:

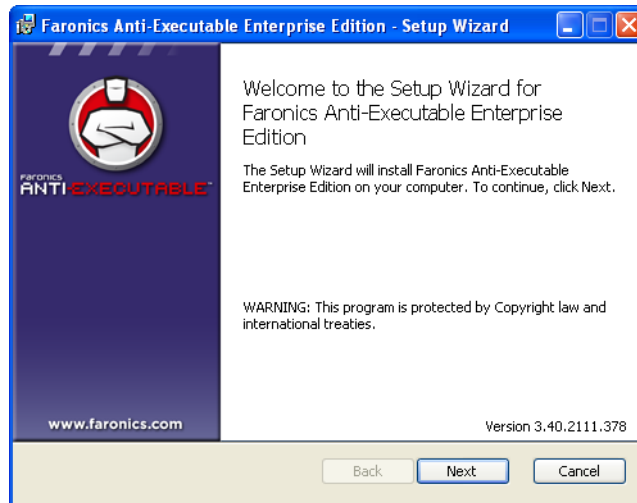
- *Console Tree Pane* — Display Faronics Core Console properties, workstations and groups, scheduled tasks, and generated reports.
- *Workstations List* — The list of all workstations that have reported to Faronics Core Console. This list also displays columns regarding workstation-specific information.
- *Actions Pane* — Users can click the Actions Pane to open a menu containing Anti-Executable tasks as well as scheduling options.

Installing Anti-Executable on a Workstation Manually

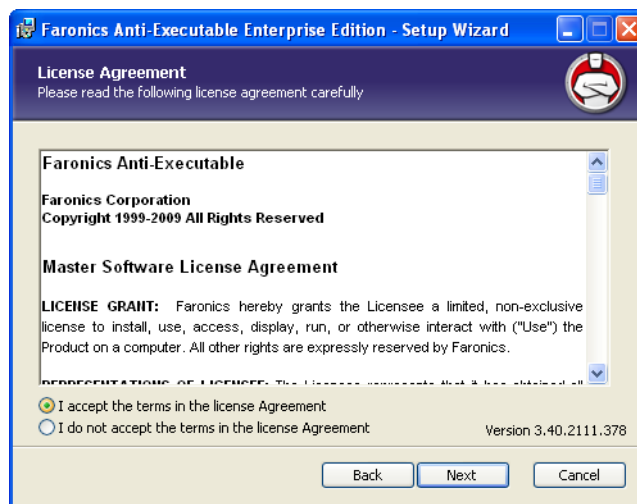
Before installing Anti-Executable on a workstation, copy appropriate *.msi* file from the path *C:\Program Files\Faronics\Faronics Core\Loadins\Anti-Executable\Workstation Installers* on the computer where the Anti-Executable Loadin is installed to one or more workstations.

To install Anti-Executable manually on a workstation after copying the file, complete the following steps:

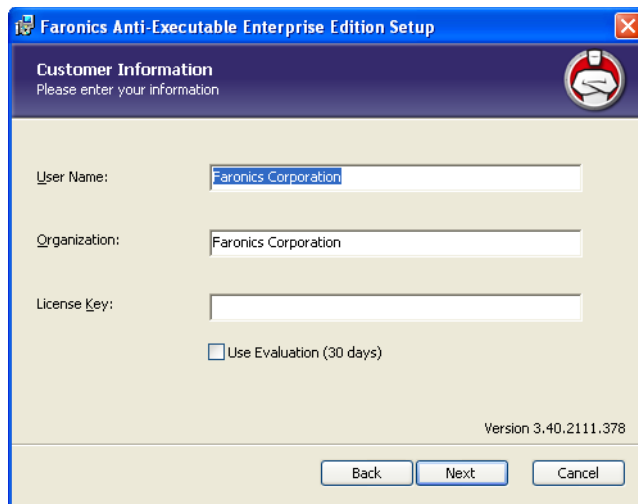
1. Double-click the *.msi* file to begin the installation process. Click *Next* to continue.



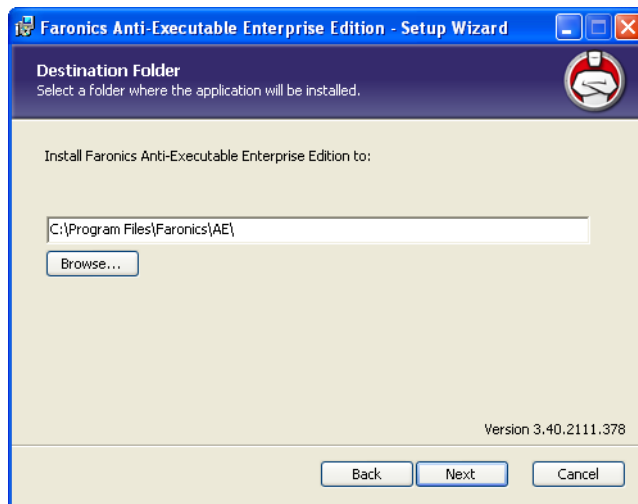
2. Read and accept the License Agreement. Click *Next* to continue.



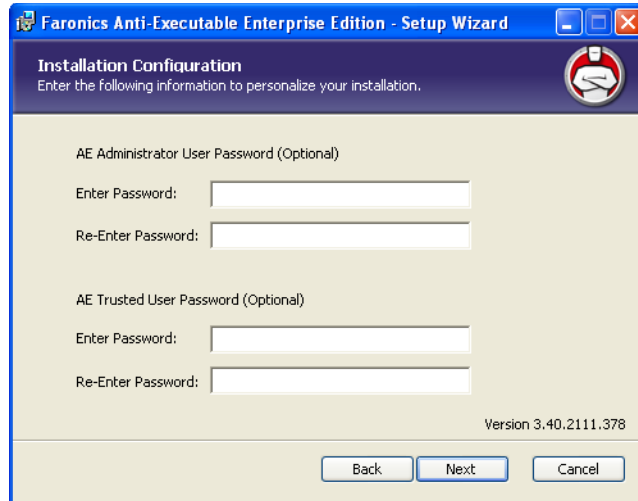
3. Enter the *User Name* and *Organization*. If *Use Evaluation* is selected, Anti-Executable is installed as an Evaluation version and is valid for 30 days. An Evaluation version can be converted to a Full shipping version at any time by entering a License Key. Click *Next* to continue.



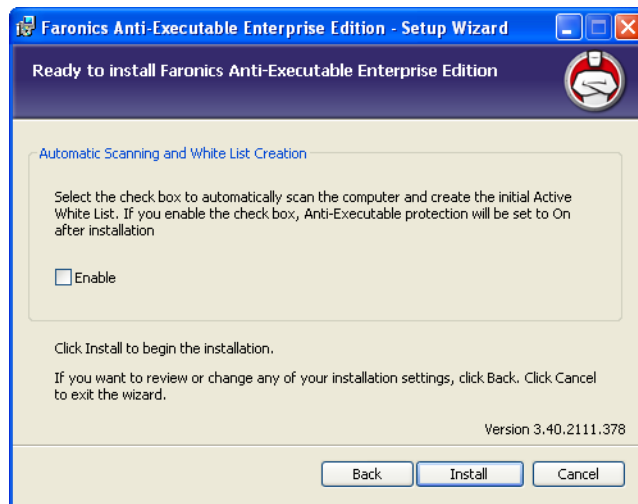
4. Specify the install location. The default is `C:\Program Files\Faronics\AE`. Click *Next* to continue.



5. This step is optional. Specify the Anti-Executable Administrator and Trusted User passwords. These passwords can also be set in the Anti-Executable Users tab following installation. Click *Next* to continue.



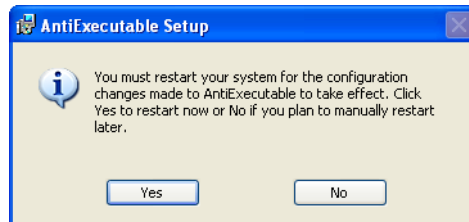
6. The *Automatic Scanning and White List Creation* dialog is displayed. Select *Enable* if you want Anti-Executable to automatically scan all non-removable drives on the computer and create a White List. Click *Install* to install Anti-Executable.



7. Click *Finish* to complete the installation.



8. Following a successful installation a restart is required. Click *Yes* to restart immediately or *No* to restart later.



An immediate restart is recommended following installation.

If the *Enable* check box is selected in the *Automatic Scanning and White List Creation* dialog, Protection is enabled and there is an Active White List when the computer restarts.

If the *Enable* check box is not selected in the *Automatic Scanning and White List Creation* dialog, Protection is disabled and there is no Active White List when the computer restarts.

Installing or Upgrading Anti-Executable on a Workstation via Faronics Core Console

Installing the Anti-Executable Loadin unbundles the Anti-Executable install files required to protect remote computers (the exact files that are unbundled will depend on the edition of Anti-Executable that is being installed).

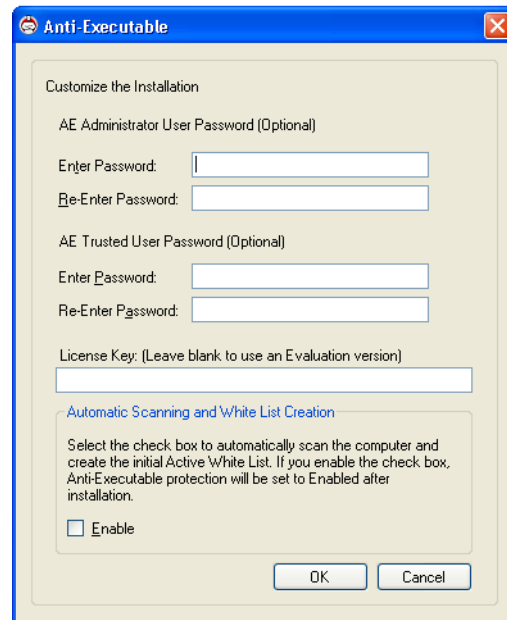


Prior to installing Anti-Executable via Faronics Core Console, the Faronics Core Agent must be installed on each workstation. The Faronics Core Agent enables communication between Faronics Core Console and the workstations on which it is installed. For more information on the process to deploy Faronics Core Agent, refer to the *Faronics Core Console User Guide*.

The default location where the Anti-Executable files are unbundled is *C:\Program Files\Faronics\Faronics Core\Loadins\Anti-Executable\Workstation Installers*

To install or upgrade Anti-Executable on one or more workstations, complete the following steps:

1. Select one or more workstation from the list in Faronics Core Console and select *Actions pane > Configure Workstation > Advanced > Install/Upgrade Anti-Executable*, or right-click on a workstation from the list in Faronics Core Console and select *Configure Workstation > Advanced > Install/Upgrade Anti-Executable*.
2. Specify the Workstation Credentials. There are two options:
 - Select *Local Workstation Account* to use the local workstation account to install/upgrade Anti-Executable. Specify the *User Name* and *Password*. Click *OK*.
 - Select *Domain Account* to use the domain account to install/upgrade Anti-Executable. Specify the *Domain*, *User Name* and *Password*. Click *OK*.
3. The *Customize the Installation* dialog is displayed. Specify the *AE Administrator Password*, *AE Trusted User Password* and *License Key*. To install in Evaluation mode, leave the *License Key* field blank. Select *Enable* in the *Automatic Scanning and White List Creation* pane if you want Anti-Executable to automatically scan all non-removable drives on the remote computer and create a White List. Click *OK*.



The screenshot shows the 'Anti-Executable' installation dialog box. It has a blue title bar with the text 'Anti-Executable' and a close button. The main area is titled 'Customize the Installation' and contains the following fields and options:

- AE Administrator User Password (Optional):** Two text boxes labeled 'Enter Password:' and 'Re-Enter Password:'.
- AE Trusted User Password (Optional):** Two text boxes labeled 'Enter Password:' and 'Re-Enter Password:'.
- License Key: (Leave blank to use an Evaluation version):** A single text box.
- Automatic Scanning and White List Creation:** A section with a blue header. Below it is a paragraph: 'Select the check box to automatically scan the computer and create the initial Active White List. If you enable the check box, Anti-Executable protection will be set to Enabled after installation.' Below this paragraph is a checkbox labeled 'Enable'.

At the bottom right of the dialog are 'OK' and 'Cancel' buttons.



An immediate restart is recommended following installation.

If the *Enable* check box is selected in the *Automatic Scanning and White List Creation* dialog, Protection is enabled and there is an Active White List when the computer restarts.

If the *Enable* check box is not selected in the *Automatic Scanning and White List Creation* dialog, Protection is disabled and there is no Active White List when the computer restarts.

Accessing Anti-Executable

Topics

Overview

Accessing Anti-Executable via Faronics Core Console

Accessing Anti-Executable Enterprise on a Workstation

Overview

Anti-Executable Enterprise can be accessed through Faronics Core Console or directly from the workstation where it is deployed.

The account used by Faronics Core Console to communicate with a workstation must be a Windows administrator account that is valid on that workstation. Communication from Faronics Core Console to the workstation occurs under the context of that account. This account becomes the first Anti-Executable Administrator following installation from Faronics Core Console. Additional Anti-Executable Administrators allowed to access Faronics Core Console must be added to the workstation's Anti-Executable users list to manage one or more workstations.



If the account used to communicate with a workstation through Faronics Core Console is changed, ensure the new account has Anti-Executable Administrator or Trusted User rights on the workstation.

Accessing Anti-Executable via Faronics Core Console

Anti-Executable can be accessed through Faronics Core Console by selecting one or more workstation(s) from the Workstations list in Faronics Core Console and opening the *Actions pane* > *Configure Anti-Executable*, or right-clicking on a workstation from the list and selecting *Configure Anti-Executable*.

Multiple workstations can be selected at one time. Hold down the *Shift* key to select a contiguous range of workstations or *CTRL* to select any number of non-contiguous workstations. Changes made will be applied to all selected workstations.



Workstation status can only be retrieved on an individual basis.

Anti-Executable Columns in Faronics Core Console

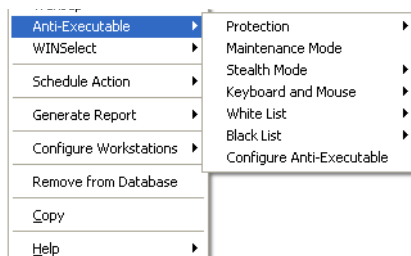
The following columns related to Anti-Executable are displayed in the *Results* pane:

- **Stealth** — This column specifies if Anti-Executable is running in Stealth Mode.
- **Protection** — This column specifies one of the following values:
 - *Enable* — When set to *Enable*, it indicates that Anti-Executable is protecting a workstation with an Active White List.
 - *Disable* — When set to *Disable*, any executable can be launched on the workstation.
 - *Maintenance Mode* — When in Maintenance Mode, new executable files added or modified are automatically added to the Active White List when *Enable* is selected. If *Disable* is selected, the changes are not recorded by Anti-Executable.
- **Version** — This column specifies the Anti-Executable version.
- **Logging** — This column specifies if the Log to Event Viewer option has been enabled or disabled.
- **License Type** — This column specifies if this is an Evaluation or a Full version.
- **Mouse/Keyboard** — This column specifies if the mouse and keyboard of one or more selected workstations are enabled or disabled.

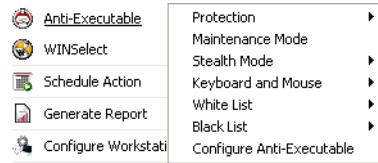
For information on the other columns in the Workstation list, refer to Faronics Core Console documentation.

Executing Anti-Executable Commands via Faronics Core Console

Anti-Executable commands can be accessed via the right-click context menu.



Anti-Executable commands can also be accessed via Faronics Core Console Actions pane located on the right side of the Faronics Core Console window. The Actions pane lists these tasks once a workstation has been selected from the list.



Protection

To quickly *Enable* or *Disable* Anti-Executable protection, select one or more workstations and click on *Protection > Enable* or *Disable* in the *Actions* pane.

Maintenance Mode

Set Anti-Executable to run in Maintenance Mode.

Stealth Mode

Configure Anti-Executable to run in Stealth Mode on one or more selected workstations.

Keyboard and Mouse

Disable or enable keyboard and mouse devices on an individual workstation or multiple workstations by clicking on *Keyboard/Mouse* and selecting *Disable* or *Enable*.

White List

A White List can be made Active on one or more workstations. Select a workstation and select *White List > Apply*. The user will be prompted with a dialog allowing them to select a White List.

Black List

A Black List can be made Active on one or more workstations. Select a workstation and select *Black List > Apply*. The user will be prompted with a dialog allowing them to select a Black List.

Configure Anti-Executable

Select this option to configure Anti-Executable.

Scheduling Actions

Anti-Executable and Faronics Core Console events can be scheduled to occur on one or more workstations at a date and time convenient to the administrator. Click on one or more workstations and select Schedule Action. The sub-menus which appear contain the following list of available actions:

Actions controlled by Faronics Core Console:

- Shutdown
- Restart
- Wake up

Actions controlled by Faronics Anti-Executable

- Protection (Enable or Disable)
- Maintenance Mode
- Black List (Apply)
- White List (Apply)
- Alerts (Enable or Disable)
- Logging (Enable or Disable)

Selecting an action displays a *Schedule* menu that allows the administrator to specify the frequency (one-time, daily, weekly or monthly). Based on the frequency, you can select the specific time, day, date, or month.

Accessing Anti-Executable Enterprise on a Workstation

Anti-Executable is accessed directly on a workstation by holding down the *Shift* key and double-clicking on the Anti-Executable icon in the Windows System Tray. The *Ctrl + Alt + Shift + F10* hotkey sequence can be used as well.

If you are an Administrator, you will have access to the Status, White List, Black List, User, and Setup tabs. If you are a Trusted User, you will have access only to the Status, White List, and Black List tabs.

External users are not permitted to access Anti-Executable. Anti-Executable Administrator and Trusted Users must enter the appropriate passwords to access Anti-Executable if those passwords have been set.

Using Anti-Executable

This chapter describes the procedure to configure and use Anti-Executable.

Topics

[Overview](#)

[Status Tab](#)

[White List Tab](#)

[Adding Blocked Executables to the Active White List](#)

[Black List Tab](#)

[Users Tab](#)

[Setup Tab](#)

[Creating an Anti-Executable Report through Faronics Core Console](#)

Overview

Following installation, Anti-Executable must be configured. Anti-Executable Administrators can access all the following tabs:

- *Status* — Displays the version of Anti-Executable installed, whether newer versions of Anti-Executable are available and allows user to import and export configurations, and set Anti-Executable Protection to *Enable*, *Disable* or *Maintenance Mode*.
- *White Lists* — Used to create, edit, and apply White Lists.
- *Black Lists*— Used to create, edit, and apply Black Lists.
- *Users* — Used to add Administrators, Trusted users and their passwords.
- *Setup* — Used to configure Stealth Mode, manage logging, alert messages, and enable Anti-Executable compatibility with Deep Freeze.

Anti-Executable Trusted Users have access only to the Status, White Lists, and Black Lists tabs.

The Windows administrator user account that performed the installation is the first Anti-Executable Administrator.

Status Tab

The Status tab allows Anti-Executable Administrators and Trusted Users to configure various settings, set protection to *Enable*, *Disable*, or *Maintenance Mode*, and import or export previously saved configurations. When a single workstation is selected in Faronics Core Console and *Configure Anti-Executable* is selected, the workstation configuration is retrieved automatically.



Verifying Product Information

The About pane displays the version of Anti-Executable installed. If newer versions are available, *New version is available* is displayed. Click *Update* for more information.

If an Evaluation version of Anti-Executable has been installed, the *Valid until* field displays the date when Anti-Executable expires. Anti-Executable displays a notification about the current status of the License in the windows system tray.

Once the evaluation period expires, Anti-Executable will no longer protect a machine. The following expired icon is displayed in the system tray when Anti-Executable expires.



To convert an Evaluation version of Anti-Executable to a Full version, click *Edit* and enter a valid License Key in the *License Key* field. License Keys can be obtained by contacting Faronics.

Enabling Anti-Executable Protection

Following installation, Anti-Executable is enabled by default only if *Enable* was selected in the *Automatic Scanning and White List Creation* dialog during installation. Otherwise, Anti-Executable cannot protect the machine. Administrators or Trusted users must select *Enable* for White List protection to take place.



If Protection has been set to *Enable* and the Active White List is empty, only basic system executables (e.g. boot-up, login) can be launched. Only Anti-Executable Administrator and Trusted Users can manage White Lists.

Use the *Remind Me after every* check box to have Anti-Executable provide reminders on a workstation to enable Protection if Protection is disabled.

Anti-Executable Maintenance Mode

Select *Maintenance Mode* and click *Apply* to run Anti-Executable in Maintenance Mode. When in Maintenance Mode, new executable files added or modified are automatically added to the Active White List. To exit Maintenance Mode, select *Enable* or *Disable*.

If *Enable* is selected, the changes are recorded by Anti-Executable. If *Disable* is selected, the changes are not recorded by Anti-Executable.



The *Disable Keyboard and Mouse* check box is available only while accessing Anti-Executable via Faronics Core Console. This is to ensure that a computer that has its keyboard and mouse disabled can still be managed remotely via Faronics Core Console.



Adequate time required for Windows Updates must be provided while running in Maintenance Mode.



If the computer is running in Maintenance Mode, and the Protection is disabled, the changes made to the workstation during Maintenance Mode are not added to the Active White List.

Exporting Anti-Executable Configurations

Anti-Executable Administrators can save multiple configurations which can be applied to other workstations. If a White List has been set as Active, it is also included in the configuration export.

To save an Anti-Executable configuration file, click *Export* in the *Status* tab after making selections. The configuration file is saved in a proprietary format (*.aecfg*) to prevent tampering. To open a previously defined configuration file (*.aecfg*), click *Import* and browse to a configuration file.



Saving a configuration to XML only allows for viewing of the configuration settings. XML configuration files cannot be applied to other workstations.

Any changes made to the Anti-Executable settings will not take effect until you click *Apply*.

Retrieving settings from Faronics Core Console

The *Status* pane retrieves and displays all the settings of a single workstation. When a single workstation is selected and Anti-Executable is launched via Faronics Core Console, the workstation settings are retrieved automatically.



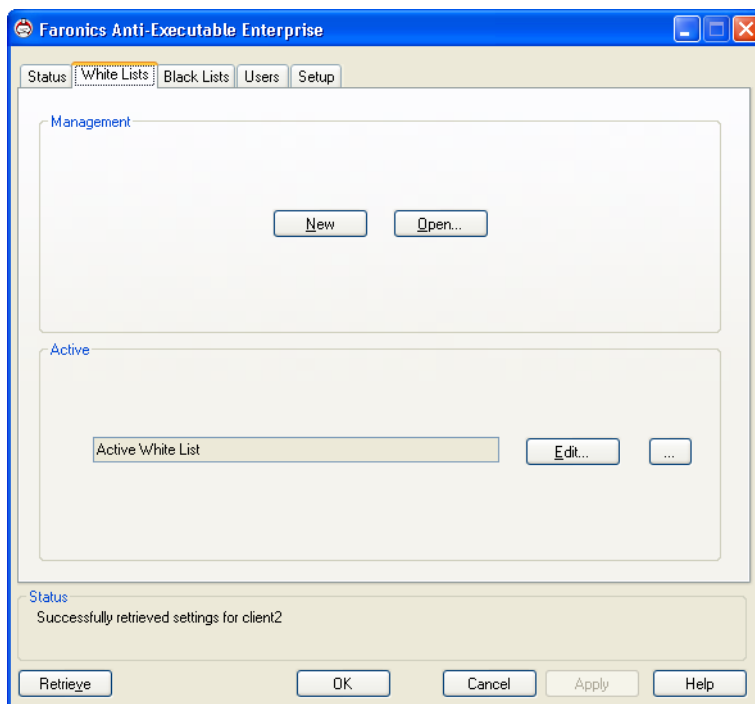
The status can only be retrieved when a single workstation is selected.

White List Tab

Anti-Executable allows the launch of any executable on the Active White List when Protection is set to *Enable*. Also included are White Folders—folders and their sub-folders from which any executable can be launched.

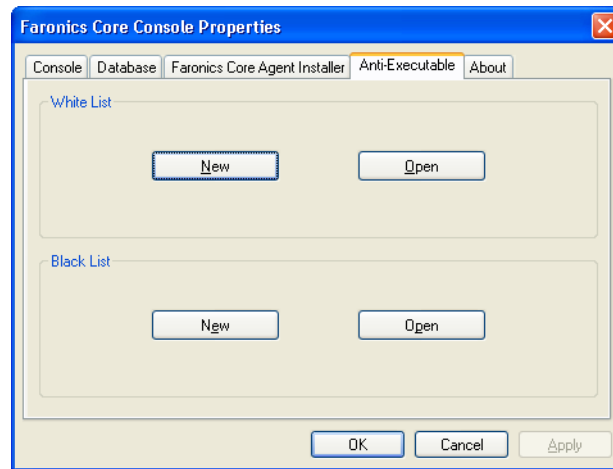
There can only be one White List active at a time on a workstation. Refer to the section titled [Creating a New White List](#) for information on creating the first White List.

Executables installed on a remote workstation cannot be added to the Active White List unless the remote workstation is visible through the file browser in the Anti-Executable Scan dialog. White Lists can be applied and deployed to workstations via Faronics Core Console or manually on each workstation.



White List Management through Faronics Core Console

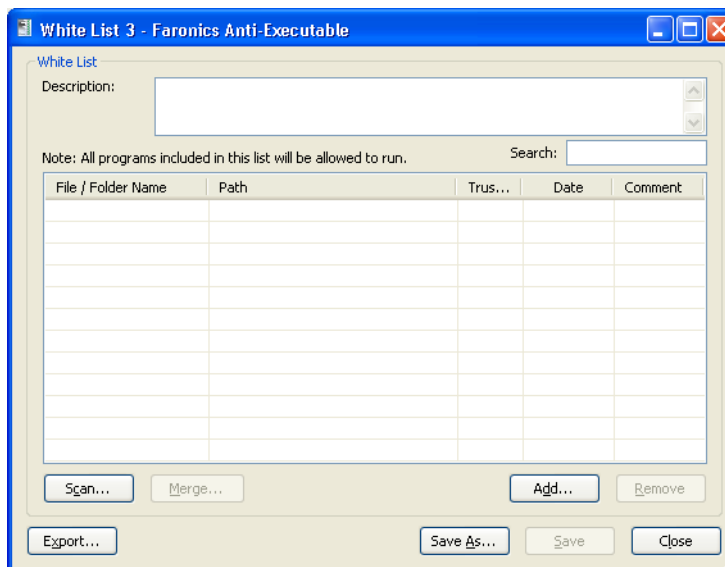
To configure Anti-Executable White Lists through Faronics Core Console, click *Properties* in the *Actions* pane on the right. Or, right-click *Faronics Core Console* in the left pane and select *Properties* from the contextual menu. To access the *Properties* option, the user must be in the top level node.



The *White List* tab can also be used to open or create White Lists. For more information consult the [Using The Anti-Executable White List Editor](#) section of this guide.

Using The Anti-Executable White List Editor

The White List Editor is opened by clicking on the *White List* tab and selecting *New*, *Open*, or *Edit*. The White List Editor also appears when an individual White List file is opened in Windows Explorer.



- *New* — Opens the White List Editor and creates a new White List.
- *Open* — Opens an existing White List for editing.
- *Edit* — Opens the White List editor to add or remove executables and/or folders to the Active White List.

Creating a New White List

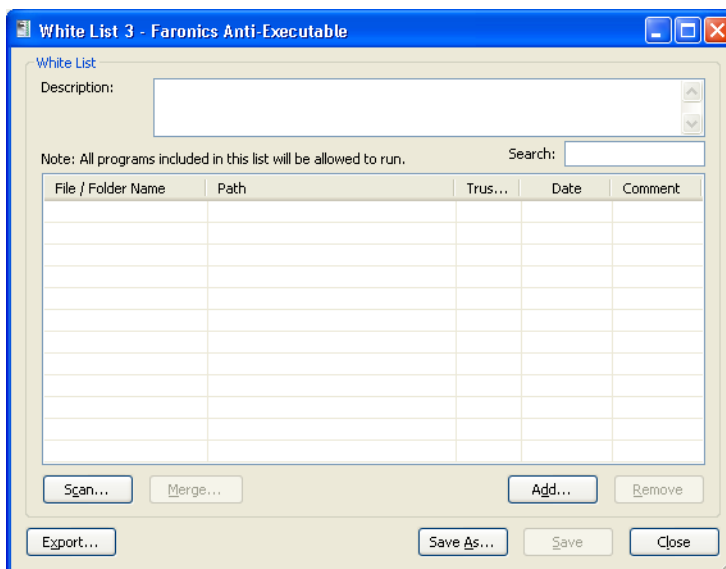
Only Anti-Executable Administrators and Trusted Users can access the White List editor on a workstation.



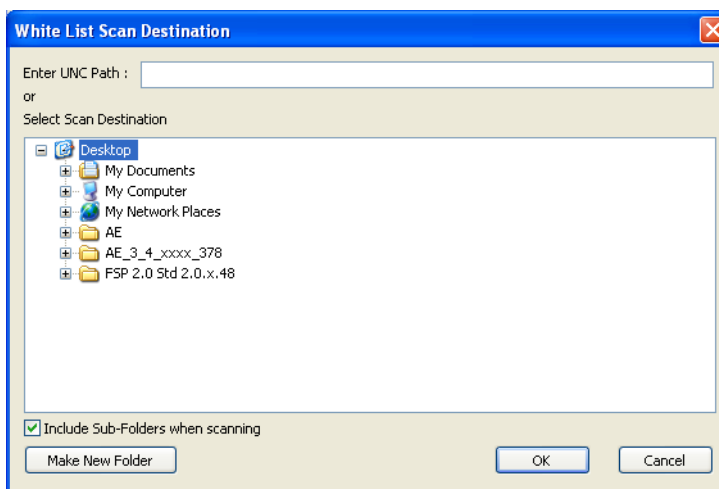
It is recommended to use a clean computer to create a White List. A clean computer is a system that has the Operating System and all the required applications installed for day-to-day operations. Creating a White List before the computer is handed over to the user will ensure that the White List contains only the files required for the computer to work properly.

To create a new White List complete the following steps:

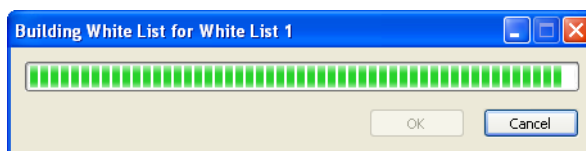
1. Launch Anti-Executable.
 - To launch Anti-Executable via Faronics Core Console, select a workstation, right-click and select *Anti-Executable > Configure Anti-Executable*. Click the *White List* tab after the workstation status has been retrieved.
 - To launch Anti-Executable on the workstation, *Shift+ double-click* the Anti-Executable icon in the System Tray. You can also use the *Ctrl+Alt+Shift+F10* hotkey. Specify the Administrator password to logon to Anti-Executable. Click the *White List* tab.
2. Click *New*. The White List editor appears:



3. To determine the available applications, click *Scan*, select a drive or directory.
 - Use *Ctrl+Click* or *Shift+Click* to select multiple drives or directories to scan the workstation locally.
 - Click *My Network Places*, browse and select a remote workstation for remote scanning.

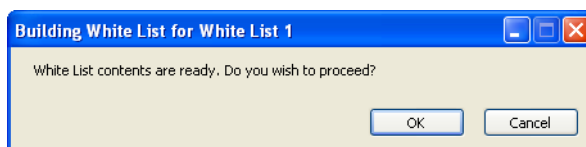


4. Click *OK*. The *Building White List for...* dialog appears to show the progress:



The *Scan* feature searches the selected location, and its sub-directories, for any executable files. (Files containing the extensions: *.scr*, *.jar*, *.bat*, *.com*, or *.exe*.) The duration of the scan depends on the location's size and number of executables found within.

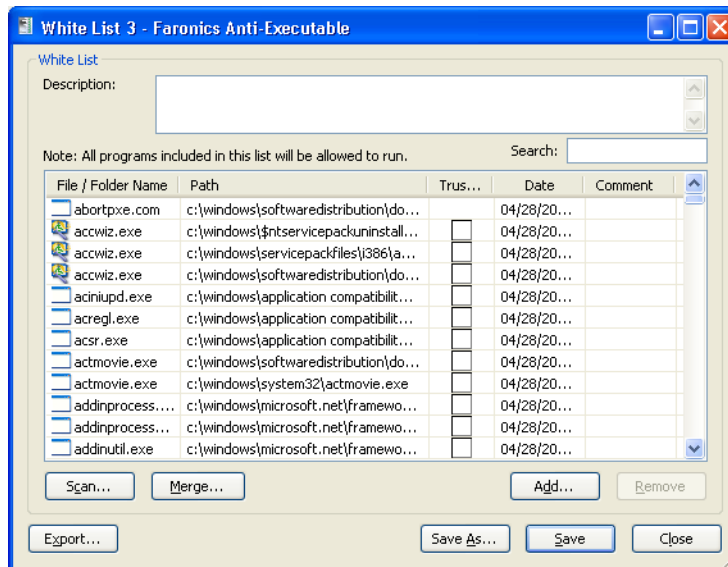
5. Once the scan has finished, Anti-Executable checks if you want to proceed. Click *OK*.



6. A populated White List appears. Folders and executables can be added on an individual basis. Click *Add* and select the folders or executables to be added to the new White List. If a folder is added, the executables within that folder, and its sub-folders, are permitted to launch.
 - To remove a folder or executable, select it and click *Remove*. This does not remove the folder or executable from the system.
 - To merge the folders or executables with an existing White List, click *Merge*. The *Open* dialog appears. Select an existing White List and click *Open*. The contents of the existing White List are merged with the scanned list of files or executables. Click *Save* to save the

White List with the same name. Click *Save As* to save the merged White List with a different name.

- To search for a particular folder or executable, enter one or more characters from the folder name or executable name in the *Search* field. The list is filtered based on the characters entered.
- To sort the executables added by date, click the title of the *Date* column.



7. Define whether an application is *Trusted* by clicking in the *Trusted* column. A selection indicates that an application is *Trusted* and can launch other executables that themselves are unauthorized.
8. Specify any comments for any applications by clicking the *Comment* column. A text prompt appears allowing for any additional information to be entered. A description can also be added for the entire list in the space provided at the top of the *White List* editor.
9. Click *Save* to save the White List. Click *Save As* to save under a different name. White Lists are saved in a proprietary format with the extension *.awl*. Click *Export* to export a White List to XML or CSV format. White Lists in XML or CSV format can be opened and edited through Windows Explorer but can not be set as the Active White List.



For more information about an executable, right-click the executable and select *Google Search*. The default browser is launched and the name of the executable is searched on www.google.com.

Activating a White List

After a White List has been created, it can be set as the Active White List by clicking the (browse) button in the Active White List section of the White List tab. The browse button launches an *Open* dialog. Browse to the White List and click *Open*.

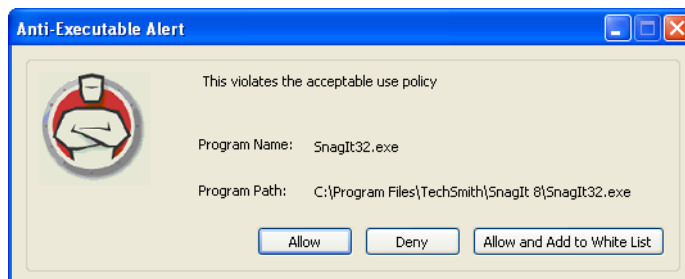
Adding Executables or Folders to an Existing White List Using the White List Editor

In addition to populating a new White List, the Scan feature allows executables from a specific location to be added to an existing White List. This location can be local, external, or on a network.

- Click *Scan* to launch the *White List Scan Destination* dialog. This will search the selected location for any executables. Once the scan has finished, the results can be merged into the White List.
- Individual folders and executables can be added by clicking *Add*.
- To open a previously created White List, click *Open* and browse to the White List file. Make any changes necessary with *Add*, *Remove*, *Scan*, or *Merge* buttons. These buttons add and remove executables and folders from the White List. They do not modify actual files or folders on the machine.
- Click the *White List Only* button to delete the executables from the Black List and ensure that they are a part of only the White List.
- Multiple White Lists can be opened and edited at the same time. Only one White List can be set as an Active White List at a time.

Adding Blocked Executables to the Active White List

Executables can be added to the active White List by launching them. If the workstation is in the protected state and an unauthorized executable is launched, the Anti-Executable Administrator or Trusted User is prompted with options to *Allow*, *Deny*, or *Allow and Add to White List*.



- *Allow*—Permits the executable to launch but does not add it to the Active White List. The next time the executable is launched, it will be blocked again.
- *Deny*—The executable is not added to the Active White List and remains an unauthorized executable. It is not permitted to launch.
- *Allow and Add to White List*—The executable is allowed to launch. It is also added to the Active White List, making it an authorized executable.

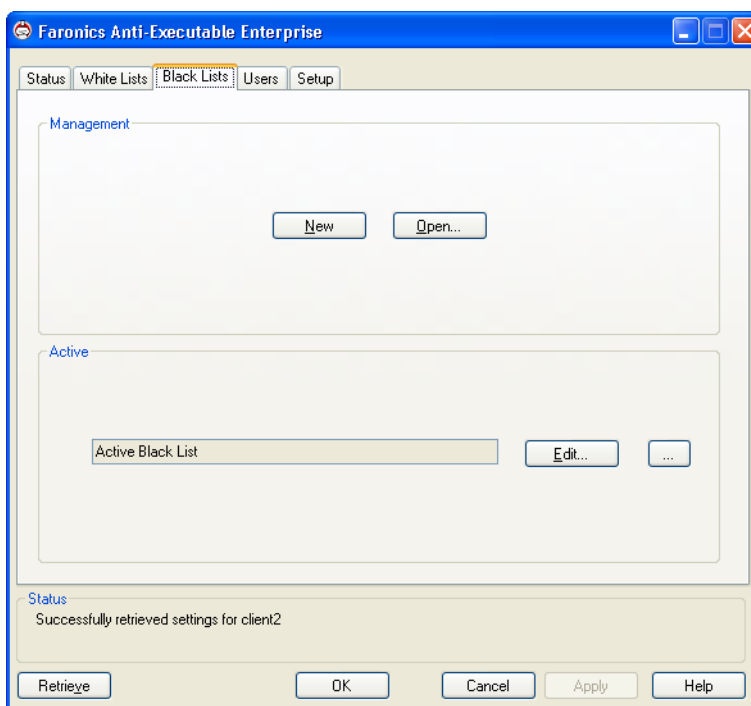
External users do not have the necessary permissions to *Allow*, *Deny*, or *Allow and Add to White List*. External users attempting to launch executables not in the Active White List are notified that the executable has been blocked. Refer to the section on [Customizing Alerts](#) for more information.

Black List Tab

Anti-Executable allows the blocking of any executable on the Active Black List when Protection is set to *Enable*. Also included are Black Folders—folders and their sub-folders from which any executable is blocked.

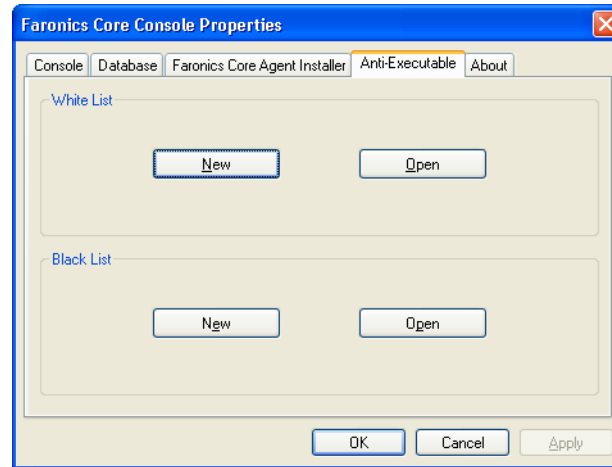
There can only be one Black List active at a time on a workstation. Consult the section titled [Creating a New Black List](#) for information on creating the first Black List.

Executables installed on a remote workstation can not be added unless the remote workstation is visible through the file browser in the Anti-Executable Scan feature. Black Lists can be applied and deployed to workstations via Faronics Core Console or manually on each workstation.



Black List Management through Faronics Core Console

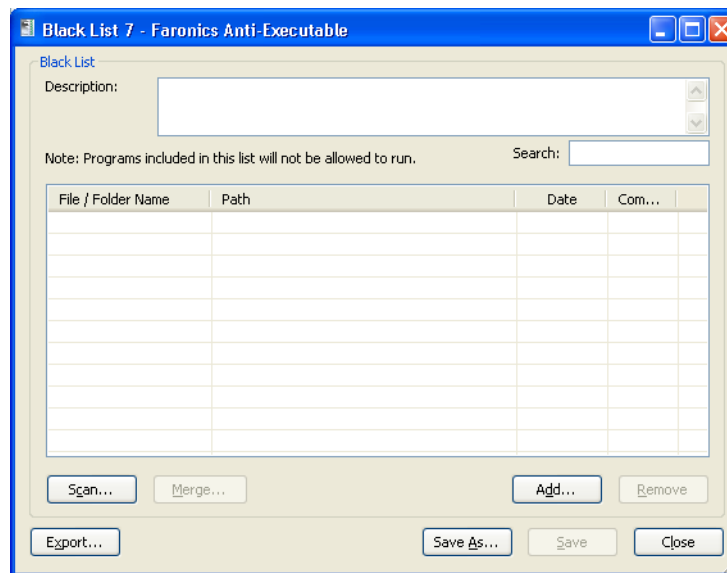
To configure Anti-Executable Black Lists through Faronics Core Console, click *Properties* in the *Actions* pane on the right side of Faronics Core Console. Or, right-click *Faronics Core Console* in the left pane and select *Properties* from the contextual menu. To access the *Properties* option, the user must be in the top level node.



The *Black List* tab can also be used to open or create Black Lists. For more information consult the [Using The Anti-Executable Black List Editor](#) section of this guide.

Using The Anti-Executable Black List Editor

The Black List Editor is opened by clicking on the *Black List* tab and selecting *New*, *Open*, or *Edit*. The Black List Editor also appears when an individual Black List file is opened in Windows Explorer.

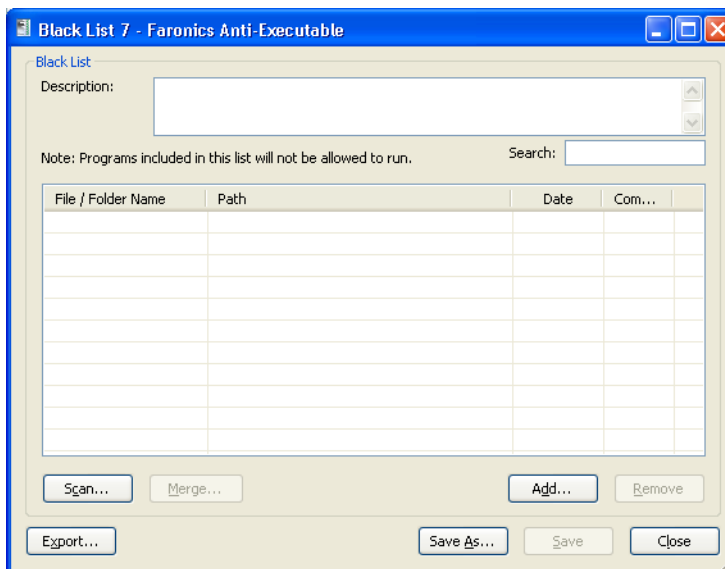


- *New* — Opens the Black List Editor and creates a new Black List.
- *Open* — Opens an existing Black List for editing.
- *Edit* — Opens the Black List editor to add or remove executables and/or folders to the Active Black List.

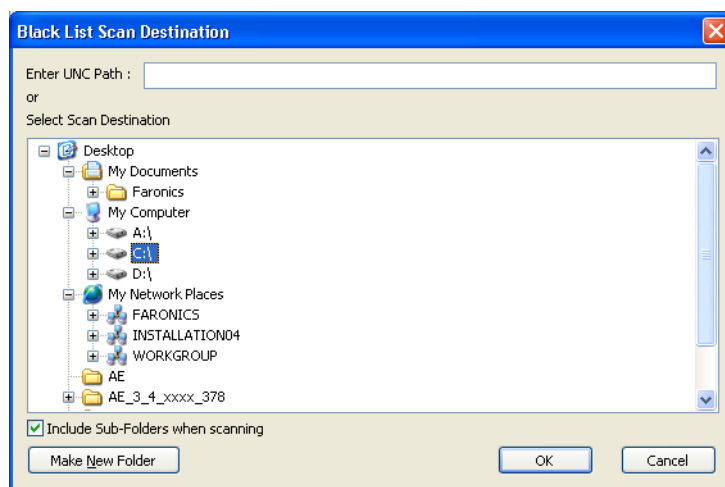
Creating a New Black List

To create a new Black List complete the following steps:

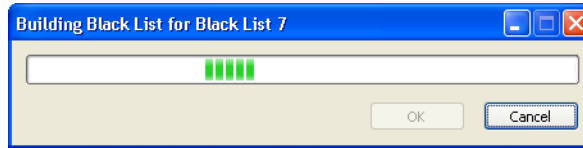
1. Launch Anti-Executable.
 - To launch Anti-Executable via Faronics Core Console, select one or more workstations, right-click and select *Anti-Executable > Configure Anti-Executable*. Click the *Black Lists* tab.
 - To launch Anti-Executable on the workstation, *Shift+ double-click* the Anti-Executable icon in the System Tray. Alternatively, you can use the *Ctrl+Alt+Shift+F10* hotkey. Specify the Administrator password to logon to Anti-Executable. Click the *Black Lists* tab.



2. To determine the available applications, click *Scan*, select a drive or directory. Use *Ctrl+Click* or *Shift+Click* to select multiple drives or directories. Alternatively, click *My Network Places*, browse and select a remote workstation. Click *OK*.

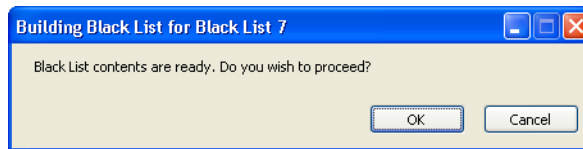


The *Building Black List for...* dialog appears to show the progress:

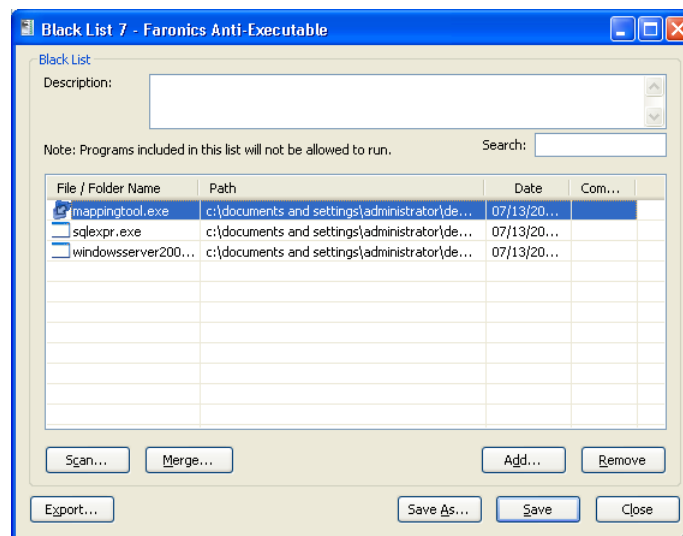


The *Scan* feature searches the selected location, and its sub-directories, for any executable files. (Files containing the extensions: *.scr*, *.jar*, *.bat*, *.com*, or *.exe*.) The duration of the scan depends on the location's size and number of executables found within.

3. Once the scan has finished, Anti-Executable asks to merge the results into the new Black List. Click *OK*.



4. A populated Black List appears. Folders and executables can be added on an individual basis. Click *Add* and select the folders or executables to be added to the new Black List. If a folder is added, the executables within that folder, and its sub-folders, are permitted to launch.
 - To remove a folder or executable, select it and click *Remove*. This does not remove the folder or executable from the system.
 - To merge the folders or executables with an existing Black List, click *Merge*. The *Open* dialog appears. Select an existing Black List and click *Open*. The contents of the existing Black List are merged with the scanned list of files or executables. Click *Save* to save the Black List with the same name. Click *Save As* to save the merged Black List with a different name.
 - To search for a particular folder or executable, enter one or more characters from the folder name or executable name in the *Search* field. The list is filtered based on the characters entered.
 - To sort the executables added by date, click the title of the *Date* column.



5. Specify any comments for any applications by clicking the *Comment* column. A text prompt appears allowing for any additional information to be entered. A description can also be added for the entire list in the space provided at the top of the *Black List* editor.
6. Click *Save* to save the Black List. Click *Save As* to save under a different name. Black Lists are saved in a proprietary format with the extension *.aobl*. Click *Export* to export a Black List to XML or CSV format. Black Lists in XML and CSV format can be opened and edited through Windows Explorer but can not be set as the Active Black List.



For more information about an executable, right-click the executable and select *Google Search*. The default browser is launched and the name of the executable is searched on www.google.com.

Activating a Black List

After a Black List has been created, it can be set as the Active Black List by clicking the (browse) button in the Active Black List section of the Black List tab. The browse button launches an *Open* dialog. Browse to the Black List and click *Open*.

Adding Executables or Folders to an Existing Black List Using the Black List Editor

In addition to populating a new Black List, the Scan feature allows executables from a specific location to be added to an existing Black List. This location can be local, external, or on a network.

- Click *Scan* to launch the *Black List Scan Destination* dialog. This will search the selected location for any executables. Once the scan has finished, the results can be merged into the Black List.
- Individual folders and executables can be added by clicking *Add*.
- To open a previously created Black List, click *Open* and browse to the Black List file. Make any changes necessary with *Add*, *Remove*, *Scan* or *Merge* buttons. These buttons add and remove executables and folders from the Black List. They do not modify actual files or folders on the machine.
- Click the *Black List Only* button to delete the executables from the White List and ensure that they are a part of only the Black List.
- Multiple Black Lists can be opened and edited at the same time. Only one Black List can be set as an Active Black List at a time.

Users Tab

Anti-Executable uses Windows user accounts to determine the features available to users. There are two types of Anti-Executable users:

- *Administrator User* — Can manage White Lists, Black Lists, Users, and Setup and can uninstall Anti-Executable.
- *Trusted User* — Can create, configure, and set the Active White List or the Active Black List. They are prohibited from uninstalling Anti-Executable and cannot manage Users or Setup.

By default, the Windows user account which performs the Anti-Executable installation becomes the first Anti-Executable Administrator User. This Administrator User can then add existing Windows users to Anti-Executable.

Any user not listed by Anti-Executable is an external user who is subject to the executable launch limitations specified by the contents of the Active White List.

If an Anti-Executable Administrator or Trusted User attempts to open an unauthorized application while Anti-Executable is enabled, they will be shown a dialog with an option to *Allow*, *Deny*, or *Allow and Add to White List*.

Adding an Anti-Executable Administrator or Trusted User

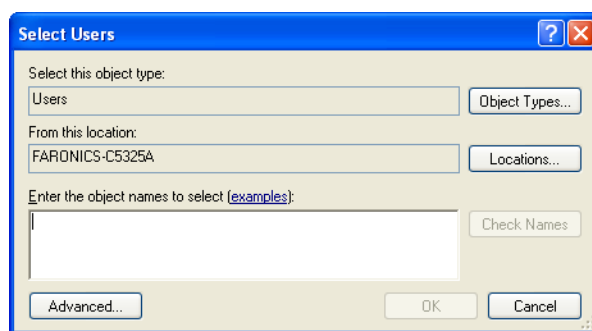
All Anti-Executable users are existing Windows user accounts. However, all Windows user accounts do not automatically become Administrators or Trusted users. Windows user accounts that are not Administrators or Trusted Users are External users.

To add a user to Anti-Executable, perform the following steps:

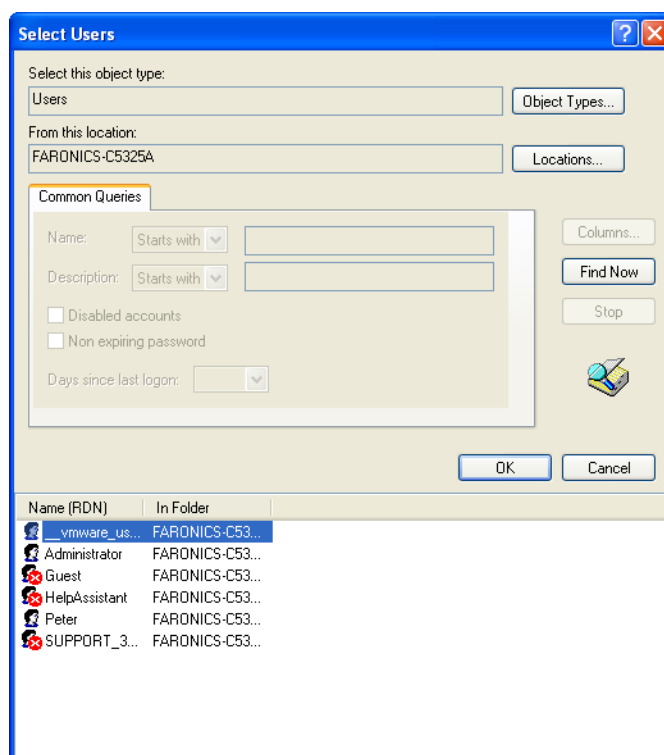
1. Click the *Users* tab at the top of the Anti-Executable window.



- Click *Add* to add a new user. Select the *User* icon from the list provided.



- If the list is empty, click *Advanced* > *Find Now* to display a list of available users. Domain administrators that have logged in as such can add other domain users. Click on a user name to add it to Anti-Executable's list and click *OK*.



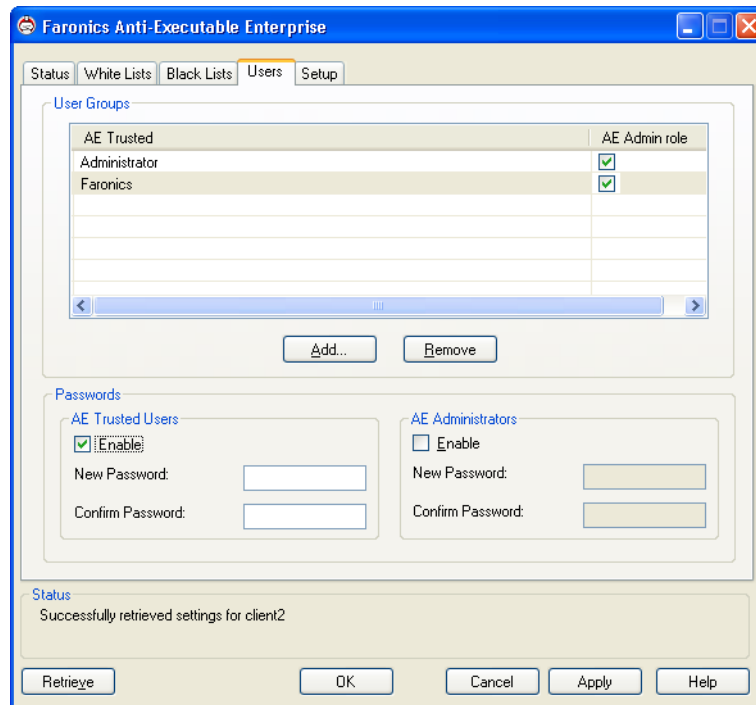
- By default, each added user is an Anti-Executable Trusted User. If the new user is to be given administrative rights, specify them as an Anti-Executable Administrator by checking the *Anti-Executable Admin Role* check box.

Removing an Anti-Executable Administrator or Trusted User

Click on the *Users* tab and select the user to be removed. Click *Remove*. This does not remove the user's Windows user account. The user has now become an external user.

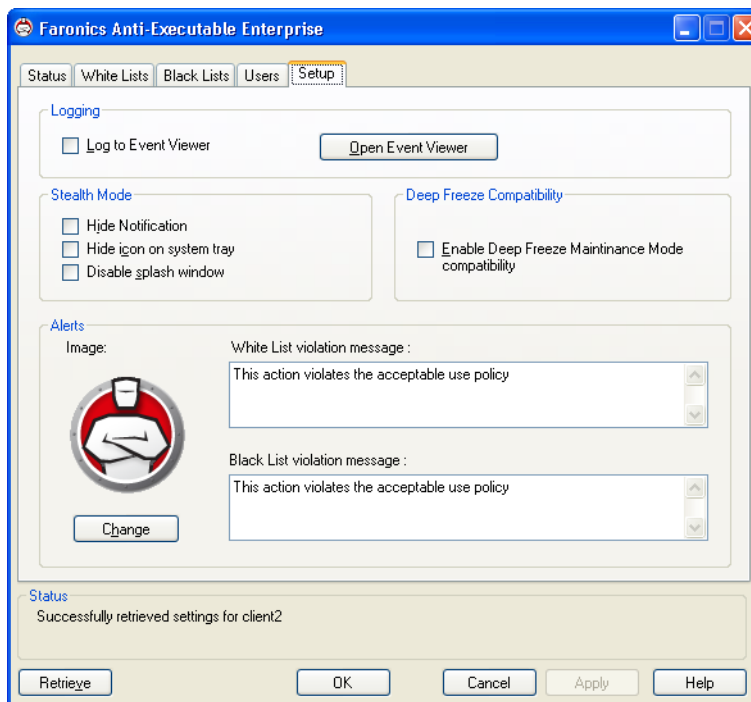
Enabling Anti-Executable Passwords

As an added layer of protection, Anti-Executable can attach a password to each user group. Passwords only apply to the members of the associated groups. To specify a password, ensure the *Enable* check box is selected and enter the password in the *New Password* and *Confirm Password* fields. Click *Apply* to save any changes.



Setup Tab

The Anti-Executable Administrator can setup Logging to log various user actions, apply various settings for Stealth Mode, set up Alerts and enable Deep Freeze Compatibility.



Setting Event Logging in Anti-Executable

Select *Log to Event Viewer* to log events to the Event Viewer. To view the logged events, click *Open Event Viewer*.

Anti-Executable Stealth Functionality

Stealth Mode is a group of options that control visual indication of Anti-Executable's presence on a system. Stealth Mode gives the option to the Administrator to hide the Anti-Executable icon in the Windows system tray, prevent the Alert from being displayed and prevent the splash screen from being displayed.

When Anti-Executable is not visible in the system tray, Administrators and Trusted users can launch Anti-Executable through the *Ctrl + Alt + Shift + F10* hotkey.

Stealth functionality has the following options:

- *Hide Notification* — prevents the Alert from being displayed.
- *Hide icon on system tray* — hides the Anti-Executable icon in the system tray.
- *Disable splash windows* — disables the Anti-Executable splash window that is displayed before Anti-Executable is launched.

Deep Freeze Maintenance Compatibility



This feature is applicable only when Faronics Deep Freeze and Faronics Anti-Executable are installed on the computer.

The Deep Freeze Maintenance Mode Compatibility feature allows the Administrator to synchronize the Maintenance Modes of Deep Freeze and Anti-Executable.

By enabling the *Enable Deep Freeze Maintenance Mode Compatibility* check box, Anti-Executable will automatically enter Maintenance Mode when Deep Freeze enters Maintenance Mode.

By setting both Deep-Freeze and Anti-Executable to be in Maintenance Mode at the same time, any executable that is added to the computer, will not only be added to the Active White List, but will be retained by Deep Freeze once it freezes back the computer after the Maintenance Mode ends.

Anti-Executable will stay in Maintenance Mode until shortly before the Maintenance Mode of Deep Freeze ends. Once Anti-Executable exits Maintenance Mode, it will add any new or updated executable files to the Active White List. When Deep Freeze exits its Maintenance Mode, it will reboot the computer *Frozen* with the updated White List.



It is not possible to set Anti-Executable to Maintenance Mode if *Deep Freeze Maintenance Mode Compatibility* is enabled and Deep Freeze status is *Frozen*. This is because, changes made to the computer will be lost on reboot.

If Anti-Executable is disabled, and Deep Freeze enters Maintenance Mode, Anti-Executable will continue to be disabled.

Maintenance periods triggered by Deep Freeze will take precedence over any other Maintenance periods scheduled on Anti-Executable.

For more information on Deep Freeze, visit <http://www.faronics.com/deepfreeze>.

Customizing Alerts

Anti-Executable Administrators can use the Alerts pane to specify the message and an image that appears whenever a user attempts to run an unauthorized executable. The following messages can be set:

- *White List violation message* — displayed when a White List is violated.
- *Black List violation message* — displayed when a Black List is violated.

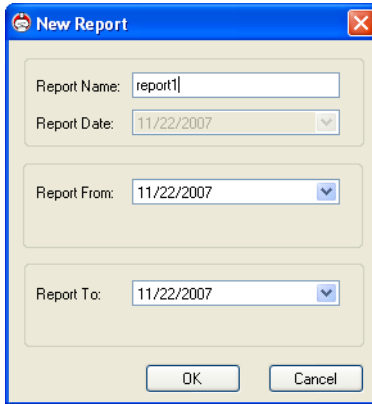
Enter a message or use the default message provided. This text will be displayed in all alert dialogs whenever a user attempts to run an unauthorized executable.

Choose a bitmap image by clicking Change and browsing to a file. The selected image will accompany the text in the alert dialog. Alert messages display the following information:

- Executable location
- Executable name
- Default or customized image
- Default or customized message

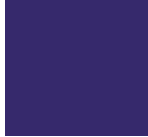
Creating an Anti-Executable Report through Faronics Core Console

To view the log for one or more selected workstations, right-click the workstation(s) and select *Generate Report > Anti-Executable Report*. The following dialog appears:



A sample report is displayed below:

	Time Stamp	Machine Info	User Info	Event Id	Description
1	15:45:05 04/24/09	client2	SYSTEM	ConfigChange	Configuration changed.
2	15:57:44 04/24/09	client2	SYSTEM	ConfigChange	Configuration changed.
3	15:57:45 04/24/09	client2	SYSTEM	ConfigChange	Protection enabled.
4	16:04:37 04/24/09	client2	SYSTEM	ConfigChange	Configuration changed.
5	16:05:01 04/24/09	client2	SYSTEM	ConfigChange	Configuration changed.
6	16:06:56 04/24/09	client2	SYSTEM	ConfigChange	Maintenance mode enabled.
7	16:06:56 04/24/09	client2	SYSTEM	ConfigChange	Keyboard and mouse disabled.
8	16:09:56 04/24/09	client2	SYSTEM	ConfigChange	Keyboard and mouse enabled.
9	16:09:56 04/24/09	client2	SYSTEM	ConfigChange	Protection enabled.
10	16:32:32 04/24/09	client2	SYSTEM	WhiteListChange	Active white list changed.
11	16:33:45 04/24/09	client2	CLIENT2\Administrator	Violation	(C:\WINDOWS\system32\calc.exe)
12	16:48:47 04/24/09	client2	SYSTEM	ConfigChange	Configuration changed.
13	16:54:36 04/24/09	client2	SYSTEM	ConfigChange	Configuration changed.
14	10:15:24 04/27/09	client2	SYSTEM	ConfigChange	Configuration changed.
15	10:15:34 04/27/09	client2	SYSTEM	ConfigChange	Configuration changed.
16	10:16:25 04/27/09	client2	SYSTEM	ConfigChange	Configuration changed.
17	10:17:41 04/27/09	client2	SYSTEM	ConfigChange	Configuration changed.
18	10:18:00 04/27/09	client2	CLIENT2\Administrator	Violation	(C:\WINDOWS\system32\calc.exe)
19	10:18:09 04/27/09	client2	SYSTEM	ConfigChange	Configuration changed.
20	10:20:43 04/27/09	client2	SYSTEM	ConfigChange	Configuration changed.
21	10:21:09 04/27/09	client2	SYSTEM	ConfigChange	Configuration changed.
22	10:21:49 04/27/09	client2	SYSTEM	ConfigChange	Configuration changed.
23	10:21:55 04/27/09	client2	SYSTEM	ConfigChange	Configuration changed.
24	10:35:56 04/27/09	client2	SYSTEM	ConfigChange	Configuration changed.
25	10:35:57 04/27/09	client2	SYSTEM	ConfigChange	Protection enabled.
26	10:39:12 04/27/09	client2	SYSTEM	ConfigChange	Maintenance mode enabled.
27	10:39:12 04/27/09	client2	SYSTEM	ConfigChange	Keyboard and mouse disabled.
28	10:42:12 04/27/09	client2	SYSTEM	ConfigChange	Keyboard and mouse enabled.
29	10:42:12 04/27/09	client2	SYSTEM	ConfigChange	Protection enabled.
30	10:50:15 04/27/09	client2	SYSTEM	ConfigChange	Configuration changed.
31	10:50:26 04/27/09	client2	SYSTEM	ConfigChange	Configuration changed.
32	10:50:51 04/27/09	client2	SYSTEM	ConfigChange	Configuration changed.
33	10:52:18 04/27/09	client2	SYSTEM	ConfigChange	Configuration changed.
34	10:53:03 04/27/09	client2	SYSTEM	ConfigChange	Configuration changed.
35	11:07:29 04/27/09	client2	SYSTEM	ConfigChange	Configuration changed.



Command Line Control

This chapter explains the various Command Line Controls available for Anti-Executable.

Topics

Command Line Control

Command Line Control

Anti-Executable Command Line Control offers network administrators increased flexibility in managing Anti-Executable workstations by allowing for control of Anti-Executable via third-party management tools and/or central management solutions. The following commands are available:



Use the `/PW=<password>` switch to execute the command on computers where a password has been set. Specify the password for the Administrator or the Trusted User as applicable.



The switch in [] is optional. White Lists have the extension `.aewl`. Black Lists have the extension `.aebL`.

Function	Command
Add a folder or file to a White List or Black List	<code>[path]AEC AddToList <List path and name.aebl or .aewl> <file or folder name and path> /PW=<password></code>
Add a folder or file to Active Black List	<code>[path]AEC AddToActiveBlackList <file or folder name and path> /PW=<password></code>
Add a folder or file to Active White List	<code>[path]AEC AddToActiveWhiteList <file or folder name and path> /PW=<password></code>
Anti-Executable version	<code>[path]AEC version /PW=<password></code> Note that Command Line Interface does not display the License Key (if it exists), while the User Interface does.
Apply Black List	<code>[path]AEC applyBlackList <Black List path and name.aebl> /PW=<password></code>
Apply White List	<code>[path]AEC applyWhiteList <White List path and name.aewl> /PW=<password></code>
Change Anti-Executable password	<code>[path]AEC changePassword <AEAdmin AETrustedUser> /PW=<password></code> Changing a password, if one exists, requires the old password.
Disable Anti-Executable	<code>[path]AEC protect off [/force] /PW=<password></code> The switch <code>/force</code> must be used if Anti-Executable is in Maintenance Mode.
Disable Deep Freeze Compatibility	<code>[path]AEC DFCompatibility /disable /PW=<password></code>

Function	Command
Display Black List	<pre>[path] AEC displayBlackList [/xml] [Black List path and name.aebl] /PW=<password></pre> <p>If <i>/xml</i> switch is not specified, the Black List will be displayed in tabular form. If Black List name is not specified, the active Black List will be displayed.</p>
Display White List	<pre>[path] AEC displayWhiteList [/xml] [White List path and name.aewl] /PW=<password></pre> <p>If <i>/xml</i> switch is not specified, the White List will be displayed in tabular form. If White List name is not specified, the active White List will be displayed.</p>
Enable Anti-Executable	<pre>[path]AEC protect on /PW=<password></pre>
Enable Deep Freeze Compatibility	<pre>[path]AEC DFCompatibility /enable /PW=<password></pre>
Enable Maintenance Mode	<pre>[path]AEC Maintenance [/duration=n] [/lock] /PW=<password></pre> <p>Using the command without any switch enables Maintenance Mode. Using the switch <i>/duration=n</i> enables Maintenance Mode for <i>n</i> minutes. The <i>/lock</i> switch disables the keyboard and mouse. The switch <i>/lock</i> must be used with the switch <i>/duration=n</i>.</p>
Export Black List	<pre>[path] AEC exportBlackList </active Source black list path and name.aebl> <Destination File path and name.xml Destination File path and name.csv> /PW=<password></pre>
Export Configuration	<pre>[path]AEC exportConfiguration <Config file path and name.xml> /PW=<password></pre> <p>or</p> <pre>[path]AEC exportConfiguration <Config file path and name.aecfg>/PW=<password></pre>
Export White List	<pre>[path] AEC exportWhiteList </active Source white list path and name.aewl> <Destination File path and name.xml Destination File path and name.csv> /PW=<password></pre>
Generate Black List	<pre>[path] AEC generateBlackList <New Black List path and name.aebl> <Directory from which to start> [/apply] /PW=<password></pre>
Generate Black List and exclude Sub-Folders	<pre>[path]AEC generateBlackList <New Black List path and name.aebl> <Directory from which to start> /NoSub [/apply]/PW=<password></pre>

Function	Command
Generate Black List and include executables in Black List Only	[path]AEC generateBlackList <New Black List path and name.aebl> <Directory from which to start> [/NoSub] /BlackListOnly /apply /PW=<password>
Generate Black List and scan Multiple Destinations	[path]AEC generateBlackList <New Black List path and name.aebl> <folderlist.txt> [/NoSub] [/BlackListOnly] [/apply] /PW=<password> <i>folderlist.txt</i> contains a set of folders and/or drives where Anti-Executable will scan to create the list. For example: C:\Program Files C:\Commonly Used Files D:\ The switch /apply must be used with the switch /BlackListOnly.
Generate Black List and select <i>My Computer</i> as scanning destination	[path]AEC generateBlackList <New Black List path and name.aebl> <"My Computer"> [/apply] /PW=<password>
Generate White List	[path] AEC generateWhiteList <New White List path and name.aewl> <Directory from which to start> [/apply]/PW=<password>
Generate White List and exclude Sub-Folders	[path]AEC generateWhiteList <New White List path and name.aewl> <Directory from which to start> </NoSub> [/apply] /PW=<password>
Generate White List and include executables in White List Only	[path]AEC generateWhiteList <New White List path and name.aewl> <Directory from which to start> [/NoSub] /WhiteListOnly /apply /PW=<password>
Generate White List and scan Multiple Destinations	[path]AEC generateWhiteList <New White List path and name.aewl> <folderlist.txt> [/NoSub] [/WhiteListOnly] [/apply] /PW=<password> <i>folderlist.txt</i> contains a set of folders and/or drives where Anti-Executable will scan to create the list. For example: C:\Program Files C:\Commonly Used Files D:\ The switch /apply must be used with the switch /WhiteListOnly.
Generate White List and select <i>My Computer</i> as scanning destination	[path]AEC generateWhiteList <New White List path and name.aewl> <"My Computer"> [/apply] /PW=<password>

Function	Command
Import Configuration	[path]AEC importConfiguration <Config file path and name.aecfg> /PW=<password>
List Commands	[path]AEC help
Merge two White Lists /Black Lists and apply	[path]AEC merge list1 list2 /apply /PW=<password> where <i>list1</i> and <i>list2</i> are the Black List or White List.
Merge two White Lists /Black Lists and save	[path]AEC merge list1 list2 <New list path and new list name> /save /PW=<password> where <i>list1</i> and <i>list2</i> are the Black List or White List.
Merge two White Lists /Black Lists, save and apply	[path]AEC merge list1 list2 <New list path and new list name> /save /apply /PW=<password> where <i>list1</i> and <i>list2</i> are the Black List or White List.
Merge White List /Black List with the current White List / Black List and apply	[path]AEC merge list /apply /PW=<password> where <i>list</i> is the Black List or White List.
Protection Status	[path]AEC status /PW=<password>
Update License Key	[path]AEC updateLicense <License Key> /PW=<password>

Legend

<mandatory user input>

[optional user input]

[path]: location where the file being referred to is stored on disk

Example Command Line

```
[path]AEC generateWhiteList engineeringLab.aewl C:\ /PW=<password>
```

```
[path]AEC applyWhiteList engineeringLab.aewl /PW=<password>
```

In the above example, [path] is the path to the Anti-Executable command line interface file (AEC.exe). *GenerateWhiteList* is the Anti-Executable command that creates a White List that in this case is called *engineeringLab.aewl*. The *.aewl* file extension is used for White List. The switch *C:* at the end of the command indicates that the White List will contain all the executable files currently present on the C drive. The second command makes the White List *engineeringLab* the active White List. In both cases, the password for the administrator is specified as <password>.

Silent Install Commands

Function	Command
Silent install (default)	<code>msiexec /q /i [path] <Product MSI></code>
Silent install (Scan fixed drives)	<code>msiexec /q /i [path]<Product MSI> ISSCANENABLED="1"</code>
Silent install (set passwords)	<code>msiexec /q /i [path] <Product MSI> AEADMINPSW=[password] TRUSTEDUSRPSW=[password]</code>
Silent install (set product key /Full version install)	<code>msiexec /q /i [path] <Product MSI> AEPRODUCTKEY=[License key]</code>
Silent uninstall	<code>msiexec /q /x [path] <Product MSI></code>

Uninstalling Anti-Executable

Topics

[Uninstalling Using Faronics Core Console](#)

[Uninstalling on a Workstation using the Uninstall Wizard](#)

Uninstalling Using Faronics Core Console

Anti-Executable can be removed from one or more workstations using Faronics Core Console. To uninstall Anti-Executable perform the following steps:

1. Open Faronics Core Console.
2. Click on the *Workstations* icon in the left pane of Faronics Core Console.
3. Right-click on the workstation(s) in the *Workstation List* from which Anti-Executable will be removed.
4. Click on *Configure Workstations > Advanced > Anti-Executable > Uninstall Anti-Executable*.



After Anti-Executable has been uninstalled from the selected workstations, Faronics Core Console will reboot them to complete the uninstall process.

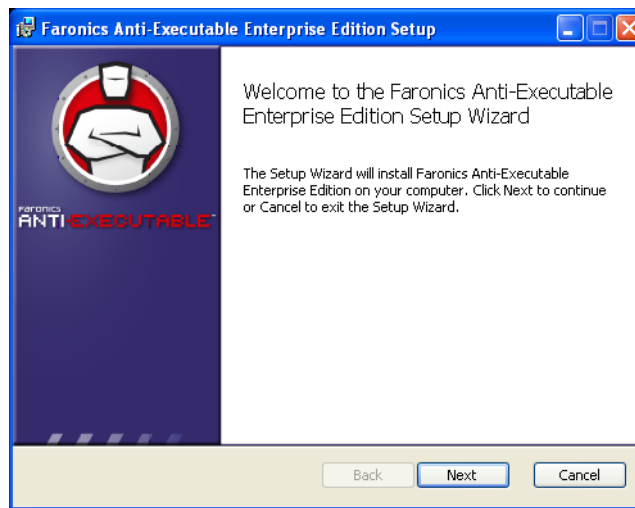
Uninstalling on a Workstation using the Uninstall Wizard



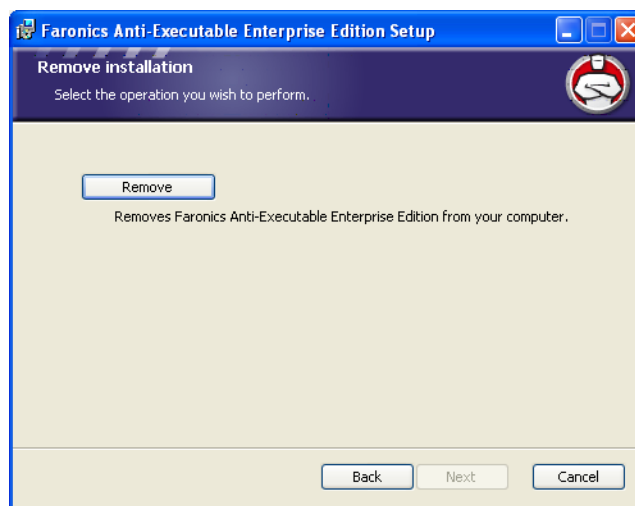
Anti-Executable can only be uninstalled by an Anti-Executable Administrator when Protection is set to *Disabled*.

Anti-Executable can be removed by double-clicking on the *.msi* file used to install Anti-Executable. The Setup Wizard appears:

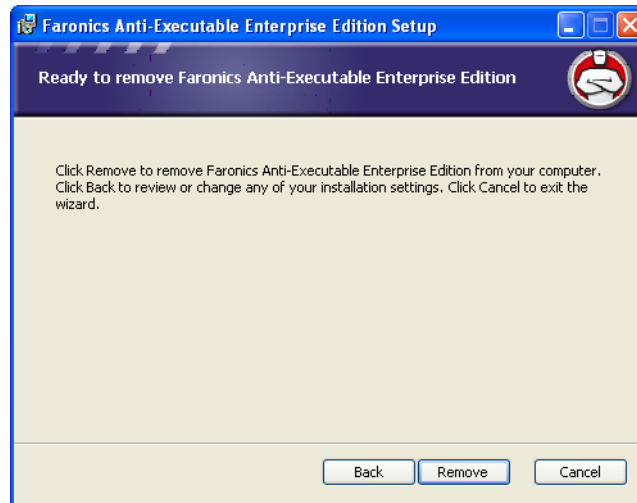
1. Click *Next* to begin the uninstall.



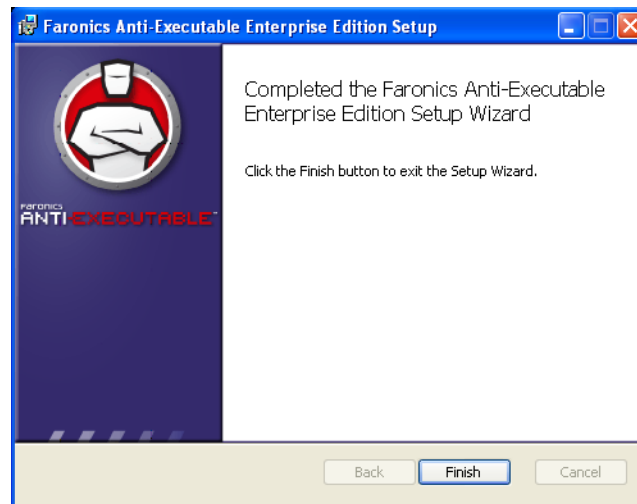
2. Click *Remove* followed by *Next*.



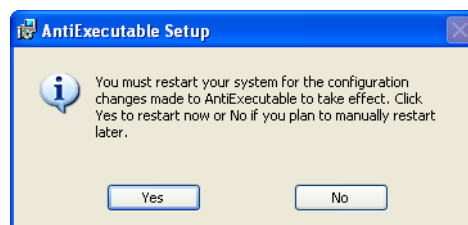
3. Click *Remove*.



4. Click *Finish* to complete the uninstall.



5. Following a successful uninstall, a workstation restart is required. Click *Yes* to restart immediately or *No* to restart later.



An immediate workstation restart is recommended following uninstall.

Uninstalling the Anti-Executable Loadin

The Anti-Executable Loadin can be uninstalled through *Add/Remove* programs. To do so click on *Start > Control Panel > Add/Remove Programs > Anti-Executable Loadin > Remove*.

Uninstalling the Anti-Executable Loadin will remove all Anti-Executable management capabilities from Faronics Core Console. It will not remove Anti-Executable installations from the individual workstations.

