Faronics

ANTI-EXECUTABLE™ STANDARD

User Guide

ABSOLUTE Protection from Unauthorized Executables

This page has been left blank intentionally.

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.

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:	7:00am to 5:00pm (PST)

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:	7:00am to 5:00pm (PST)
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

Last modified: May, 2009

This page has been left blank intentionally.

Contents

This page has been left blank intentionally.

Anti-Executable Overview

About Anti-Executable Standard

Anti-Executable protects machines by preventing unauthorized executables from running. Anti-Executable allows administrators to create a list of all the permissible applications on a machine. These White Lists can provide users the productivity tools required for their job, and protect them from distractions, such as chat programs and games, and Internet dangers, such as viruses and spyware.

Once Anti-Executable is installed, the administrative user must configure and apply an Active White List. Once the Protection setting has been set to *On*, authorized executables specified in the Active White List can be launched. Executables not in the Active White List cannot be opened by unspecified users (external users). A White List generated on one machine can be applied to another machine.

An attempted launch of an unauthorized executable displays an alert which is recorded in the Anti-Executable log file. Administrators can specify the content of the alert displayed.

Anti-Executable Editions

Faronics Anti-Executable has four different editons available. Depending on whether you want to install Faronics Anti-Executable on a server or a workstation running on a network , or on a standalone workstation, choose one of the following editions 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

System Requirements

Anti-Executable can be installed on 32- and 64-bit editions of Windows XP SP2 (or later), Windows Server 2003, Windows Server 2008 and Windows Vista.

Definition of Terms

Active White List	The list of executables, or folders containing executables, that are permitted by Anti-Executable to launch. Launching an executable not in the Active White List can only be accomplished by Anti-Executable Administrator and Trusted Users. There can be numerous White Lists but only one can be Active at any time.
Alert	The notification dialog that appears when an unauthorized executable is launched. Anti-Executable Administrators can specify the message and artwork displayed in the alerts.
Anti-Executable Administrator User	Administrator Users have access to all Anti-Executable configuration options. They can create and edit White Lists, manage Anti-Executable users, set Anti-Executable protection to *On* or *Off*, and uninstall Anti-Executable.
Anti-Executable Trusted User	Trusted Users can add applications to the Active White List, create and save new White Lists, and set Anti-Executable protection to *On* or *Off*. They cannot uninstall Anti-Executable.

Authorized Executable	An Executable that is in the Active White List and therefore can be launched.
Executable	Any file that can be launched by the operating system.
External User	Any user that is neither an Anti-Executable Administrator nor an Anti-Executable Trusted user. An external user can only run authorized executables. This restriction applies regardless of any user rights assigned by the operating system.
Protection	When set to *On*, this setting indicates that Anti-Executable is protecting a machine with an Active White List. When set to *Off*, any executable can be launched on the machine.
Stealth Mode	Anti-Executable provides no visual indication that it is installed on the system. The Anti-Executable icon is not shown in the Windows System Tray and alerts regarding unauthorized executables are not displayed.
Trusted Application	A Trusted Application 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 managed by Anti-Executable. Any application that has one of the following extensions: *.scr*, *.jar*, *.bat*, *.com*, or *.exe*.

Anti-Executable Licensing

Anti-Executable is available in both Full and Evaluation versions. A Full version requires a License Key while an Evaluation version can be operational for 30 days after installation. An expired Evaluation version will not protect a machine and must be uninstalled or upgraded to a Full version.

License information can be obtained by Anti-Executable Administrator and Trusted Users through the *Anti-Executable Status* tab. To upgrade from an Evaluation version to a Full version, enter a valid License Key and click *OK*.

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

Anti-Executable can only be installed when logged in as a user with Windows Administrator privileges.

Anti-Executable Install Files

Anti-Executable features installers for 32- and 64-bit versions of Windows Server 2003, Windows XP SP2, and Windows Vista. Before installing, verify the operating system version and choose the installer from the following list:

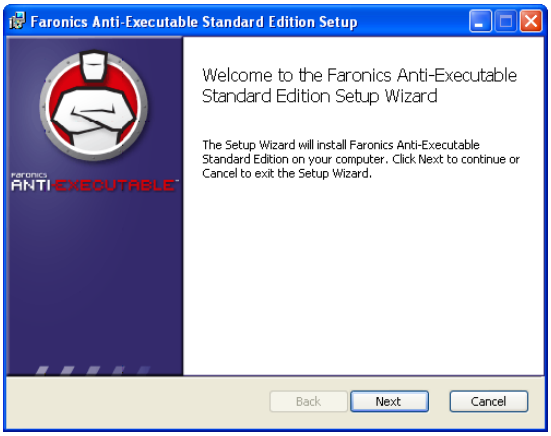
System	Install File
Windows XP/Vista 32-bit	*AEStd_32-bit.msi*
Windows XP/Vista 64-bit	*AEStd_64-bit.msi*
Windows Server 2003 32-bit	*AESrvStd_32-bit.msi*
Windows Server 2003 64-bit	*AESrvStd_64-bit.msi*

Installing Using the Setup Wizard

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

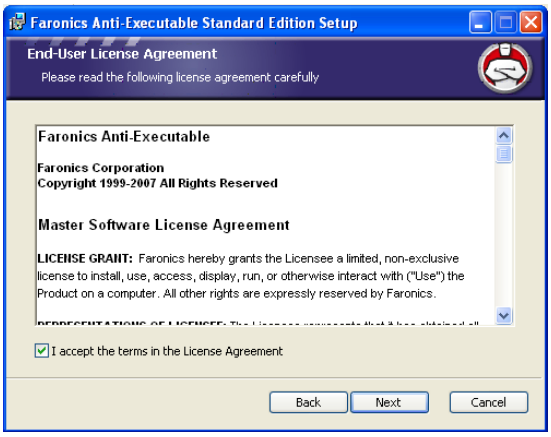
1. Insert the CD-ROM from the Media Package into the CD-ROM drive.

   If Anti-Executable has been downloaded via the Internet, double-click the *.msi* file to begin the installation process.



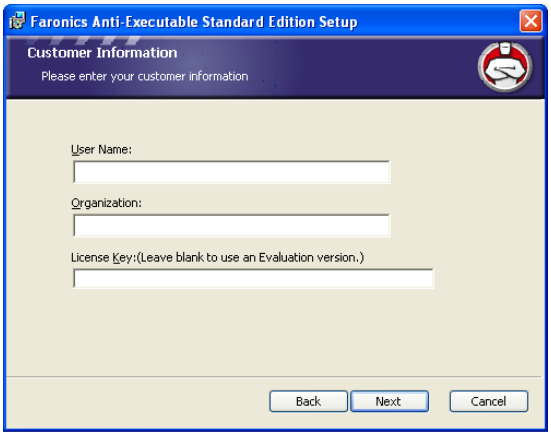
   Click *Next* to continue.

2. Read and accept the License Agreement.



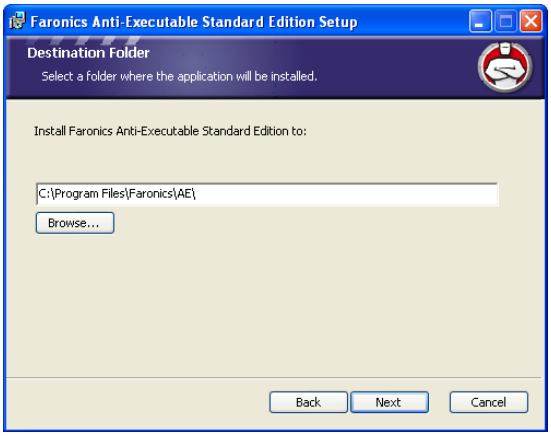
Click *Next* to continue.

3. Enter the *User Name* and *Organization*. If a valid License Key is not entered, Anti-Executable is installed as an Evaluation version and is valid for a limited time. An Evaluation version can be converted to a Full shipping version at any time by entering a License Key.



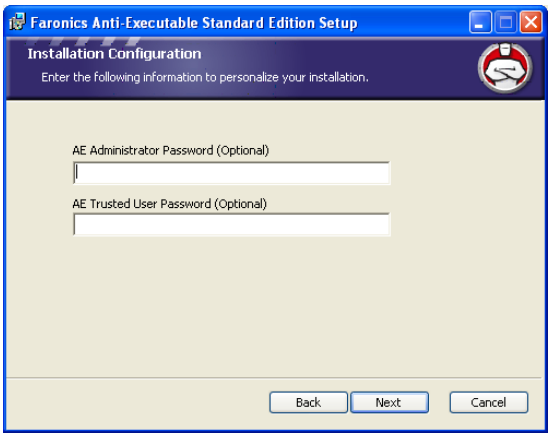
Click *Next* to continue.

4. Specify the install location. The default is *C:\Program Files\Faronics\AE*.



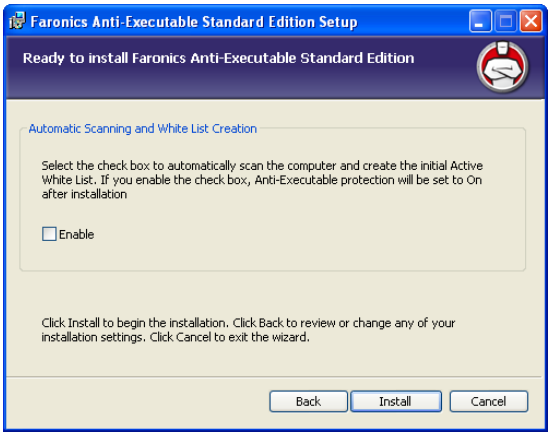
Click *Next* to continue.

5. OPTIONAL: Specify the Anti-Executable Administrator and Trusted User passwords. These passwords can also be set in the Anti-Executable Users tab following installation.

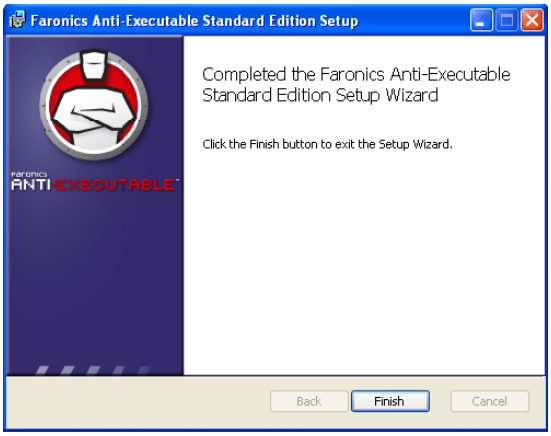


Click *Next* to continue.

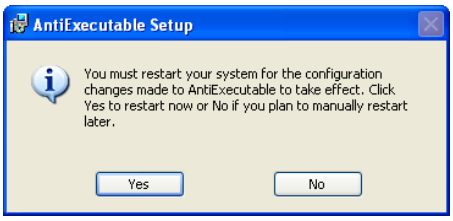
6. The *Automatic Scanning and White List Creation* dialog is displayed. Select *Enable* if you want Anti-Executable to automatically scan all non-removable drives on the computer and create a White List. Click *Install* to begin the installation.



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.

Accessing Anti-Executable

Anti-Executable is accessed by holding down the *Shift* key and double-clicking the Anti-Executable icon in the Windows System Tray. If the icon is not present, the *Ctrl* + *Alt* + *Shift* + *F10* hotkey sequence can be used.

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. For more information on passwords consult the section titled Enabling Anti-Executable Passwords.

Using Anti-Executable

Following installation, Anti-Executable must be configured.

Anti-Executable Administrator Users have access to the following tabs:

- *Status*—Update to newer versions of Anti-Executable, import and export configurations, and set Anti-Executable Protection to *Enable* or *Disable*. Anti-Executable can also be run in Maintenance Mode.
- *White Lists*—Create, edit, and apply White Lists.
- *Users*—Add Users and edit Administrator and Trusted User passwords.
- *Notifications*—Set Event Logging for Anti-Executable and configure Alert content.

Anti-Executable Trusted Users have access to the following tabs:

- *Status*—Update to newer versions of Anti-Executable, import and export configurations, and set Anti-Executable Protection to *Enable* or *Disable*. Anti-Executable can also be run in Maintenance Mode.
- *White Lists*—Create, edit, and apply White Lists.

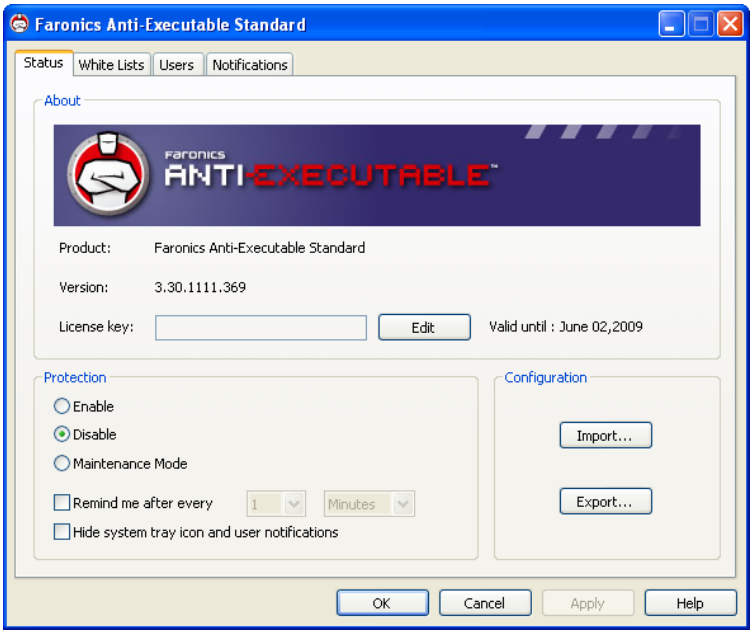
Accessing Anti-Executable via the System Tray (workstation only):

- *Enable Protection/Disable Protection*— Right-click the Anti-Executable icon and select *Enable Protection* or *Disable Protection* as required.

The Windows administrative user account that performed the installation is the first Anti-Executable Administrator. The first time the application is run, the machine is not protected and does not have an Active White List.

The Anti-Executable Status Tab

The first tab shown is the *Status* tab. *Status* allows Anti-Executable Administrators and Trusted Users to configure settings, set protection to *On* or *Off*, and import or export previously saved configurations.



Following installation a White List has not been applied to the system. It is recommended that a White List be created immediately following installation. For more information on configuring White Lists consult the White Lists section of this guide.

Verifying Product Information

In the *About* frame, Anti-Executable Administrators can get information on newer versions of Anti-Executable as they become available by clicking *Update*.

If an Evaluation version of Anti-Executable has been installed, the *Valid Until* field displays the remaining days until Anti-Executable expires. Once the evaluation period expires, Anti-Executable will no longer protect a machine.

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

Enabling Anti-Executable Protection

Following installation Anti-Executable is not enabled by default: therefore Anti-Executable cannot protect the machine. Administrators must toggle the *Protection* radio button to *On* for White List protection to take place.

If Protection has been set to On 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* check box to have Anti Executable provide reminders to enable Protection if Protection is set to *Disable* or, if the computer is running in Maintenance Mode.

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, *Enable* or *Disable* Protection.

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

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

Anti-Executable Stealth Functionality

If Anti-Executable is running on a public machine, hide notifications and the Anti-Executable icon by checking the *Hide system tray and user notifications* check box. This prevents the Anti-Executable icon from being displayed in the System Tray. Alerts are also prevented from being displayed.

Exporting Anti-Executable Configurations

Anti-Executable Administrators can save multiple configurations which can be applied to other machines. 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 *Open* and browse to a configuration file.

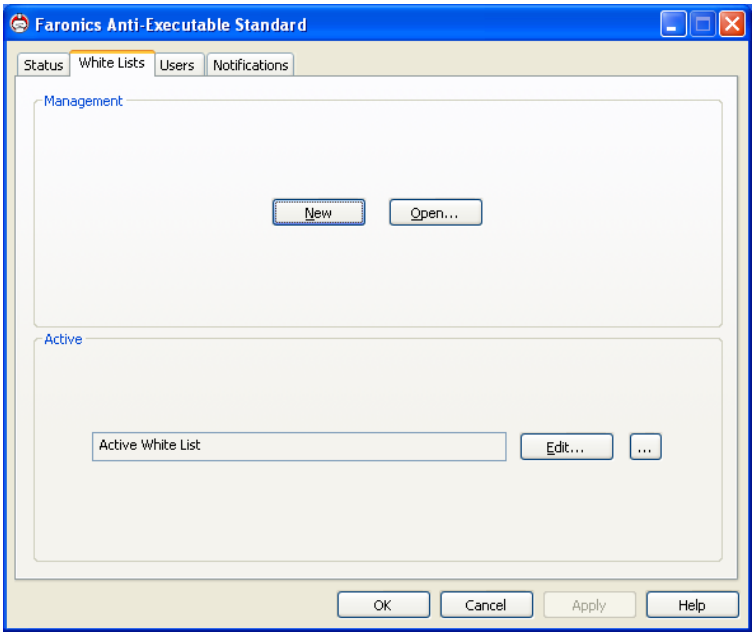
Saving a configuration to XML only allows for viewing of the configuration settings. XML configuration files cannot be applied to other machines.

Any changes made will not take affect until Apply is clicked.

The Anti-Executable White List Tab

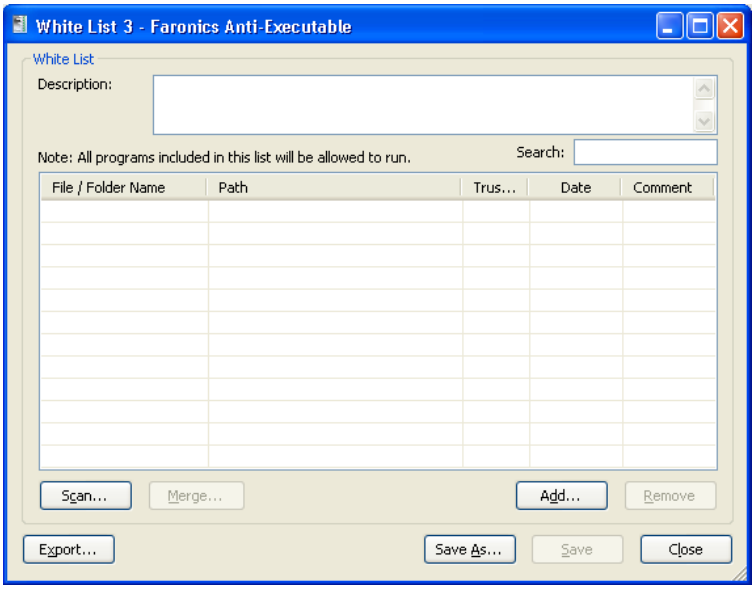
Anti-Executable allows the launch of any executable on the Active White List when Protection is set to *On*. Also included are White Folders—folders and their sub-folders from which any executable can be launched.

There can only be one White List active at a time. Consult the section titled Creating a New White List for information on creating the first White List.



Using The Anti-Executable White List Editor

The Anti-Executable 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.

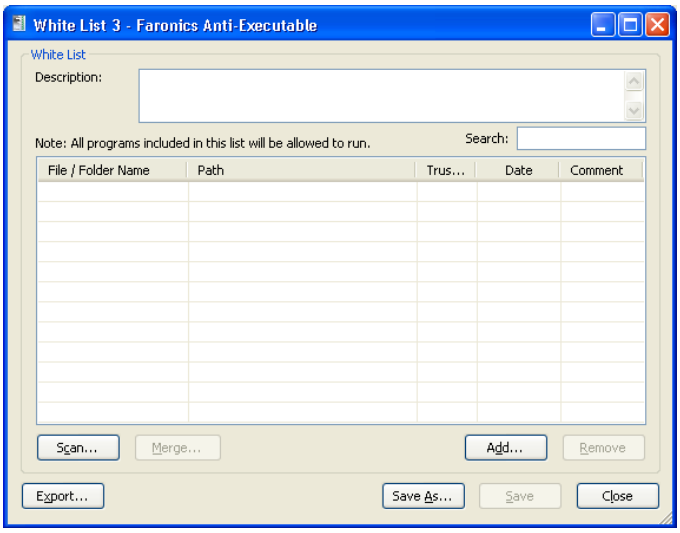


- *New*—Opens the White List Editor and allows Anti-Executable Administrators and Trusted Users to create a new White List.
- *Open*—Opens an existing White List for editing.
- *Edit*—Opens the White List editor to add or remove executables and/or folders to the Active White List.

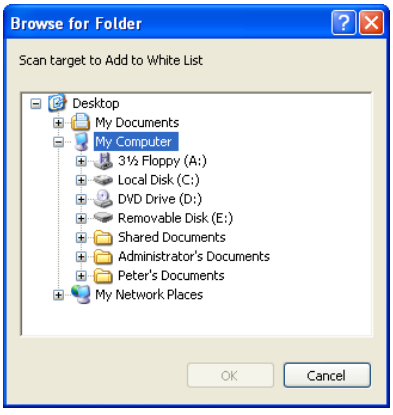
Creating a New White List

Only Anti-Executable Administrators and Trusted Users can access the White List editor. To create a new White List complete the following steps:

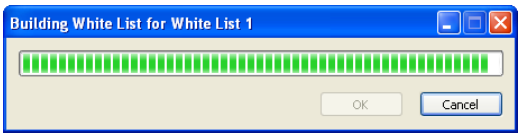
1. Click *New*. The White List editor appears:



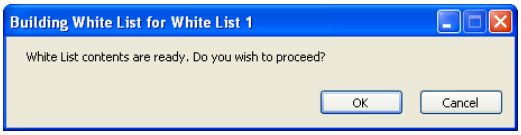
2. To determine the available applications, click *Scan*, select a drive or directory. Use *Ctrl+Click* or *Shift+Click* to select multiple drives or directories.



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 White List. Click *OK*.



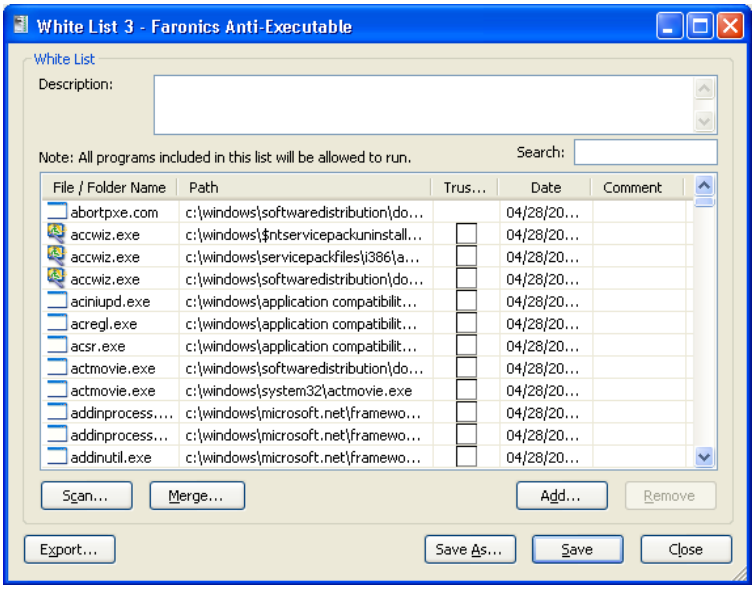
4. A populated White List appears. Folders and executables can be added on an individual basis. Click *Add* and select the folders or executables to be added to the new White List. If a folder is added, the executables within that folder, and its sub-folders, are permitted to launch.

   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.

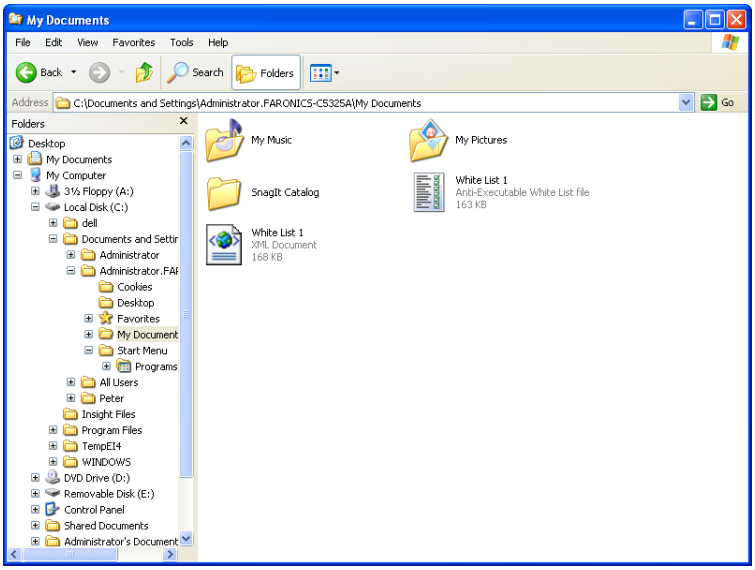
   To sort the executables added by date, click the title of the *Date* column.



5. Define whether an application is *Trusted* by clicking in the *Trusted* column. A check mark indicates that an application is Trusted and can launch other executables that themselves are unauthorized.

6. 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.
7. Click *Apply* to save and apply the updated White List. Click *Save As* to save under a different name. White Lists are saved in a proprietary format.

   Click *Export* to export a White List to XML format. XML White Lists can be opened through Windows Explorer but cannot be set as the Active White List.

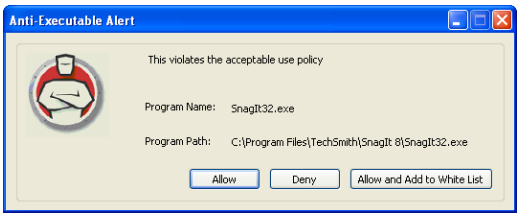


Activating a White List

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 to the Active White List

Executables can be added to the active White List by launching them. If the machine 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 by an Anti-Executable Administrator or Trusted User the *Allow*, *Deny*, or *Allow and Add to White List* dialog appears.
- *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. Consult the section on Alerts for more information.

The Anti-Executable Users Tab

Only Anti-Executable Administrators are able to access the Users tab.

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

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

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.

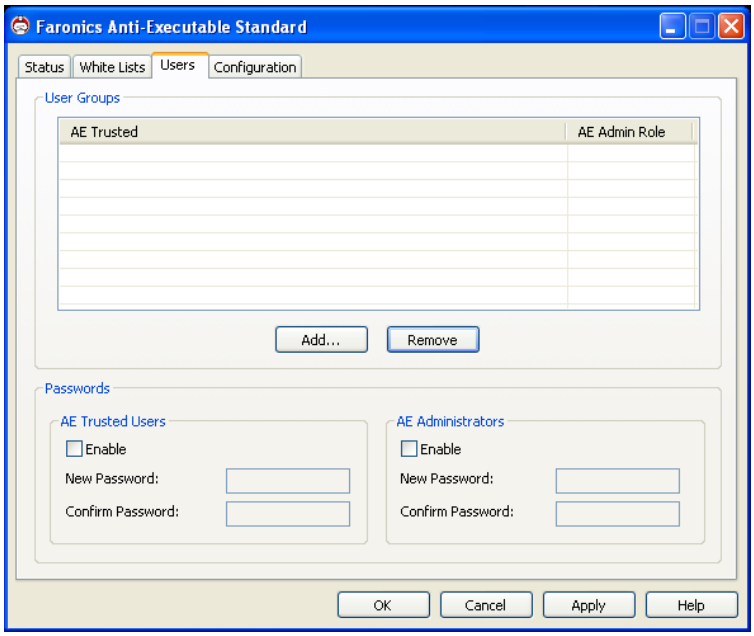
If an Anti-Executable Administrator or Trusted User attempts to open an unauthorized application while Anti-Executable is enabled, they will be shown a dialog with an option to *Allow*, *Deny*, or *Allow and Add to White List*.

If an external user attempts to open an unauthorized executable while Anti-Executable is *On* and *Hide Alerts is* disabled, the alert dialog is displayed and the executable is prevented from launching.

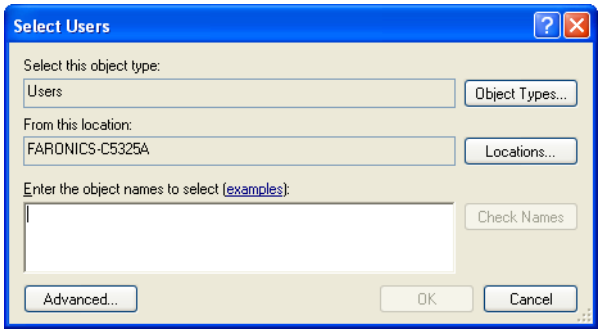
Adding an Anti-Executable Administrator or Trusted User

All Anti-Executable users are existing Windows user accounts. To add a user to Anti-Executable, perform the following steps:

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

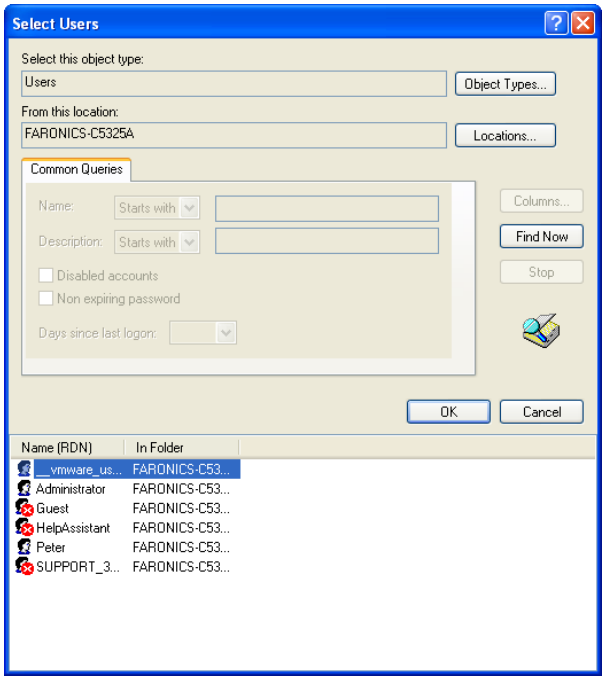


2. Click *Add* to add a new user. Select the User icon from the list provided.

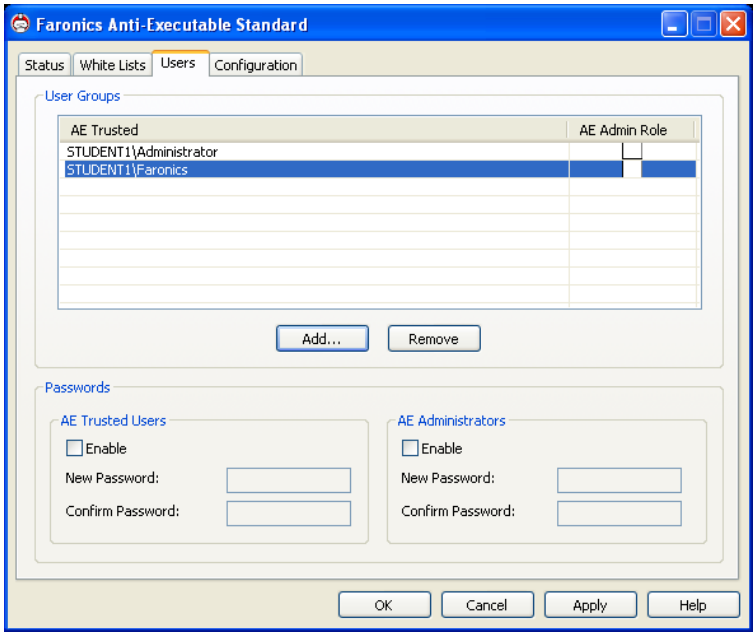


3. If the list is empty, click *Advanced* > *Find Now* to display a list of available users. Domain administrators that have logged in as such can add other domain users.

   Click on a user name to add it to Anti-Executable's list and click *OK*.



4. 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.



5. Click *Apply* when finished.

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

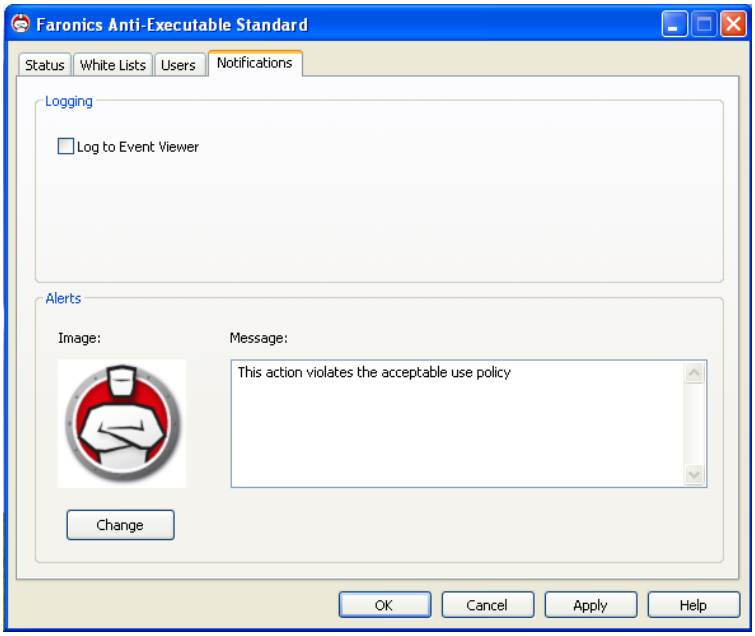
As an added layer of protection, Anti-Executable can attach a password to each user group. Passwords only apply to the members of the associated groups. To specify a password, ensure the *Enable* check box is checked and enter the password in the *New Password* and *Confirm Password* fields.

Click *Apply* to save any changes.

The Anti-Executable Notifications Tab

Anti-Executable records actions and events occurring on each machine.

An Anti-Executable Administrator can specify the content of the Alert messages displayed when a user attempts to open an unauthorized executable. Both settings can be configured on the *Notifications* tab.



Setting Event Logging in Anti-Executable

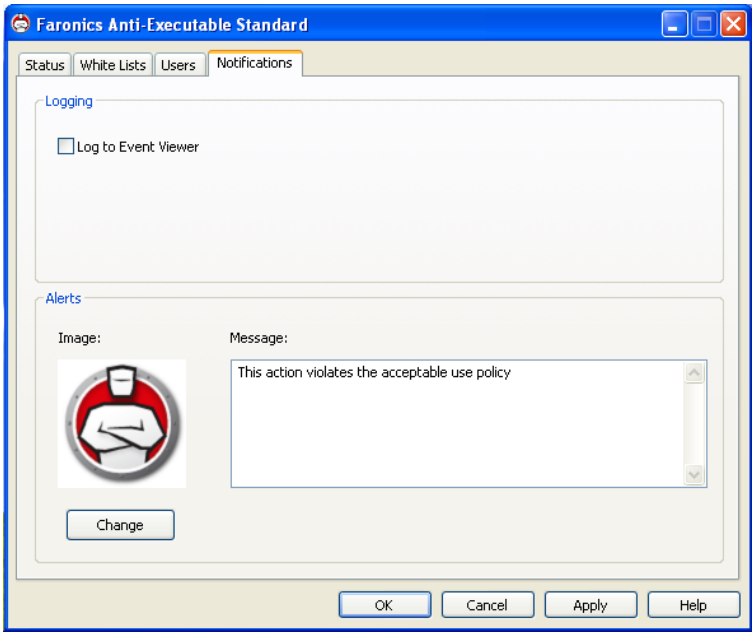
Select Log to Event Viewer to log events to the Event Viewer. To view the logged events, complete the following steps:

1. Go to *Start>Control Panel>Administrative Tools>Event Viewer*.
2. Click *Anti-Executable* in the left pane.
3. The events are displayed in the right pane.

If Protection has been set to On 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.

Customizing Alerts

Anti-Executable Administrators can use the *Alerts* pane to specify the message and image that appears whenever a user attempts to run an unauthorized executable.



Enter a message in the *Message* field or use the default message provided at install time. This text will be displayed in all alert dialogs.

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

When Anti-Executable has been set to Stealth Mode, Alert messages are not displayed, regardless of which Anti-Executable user type is logged in.

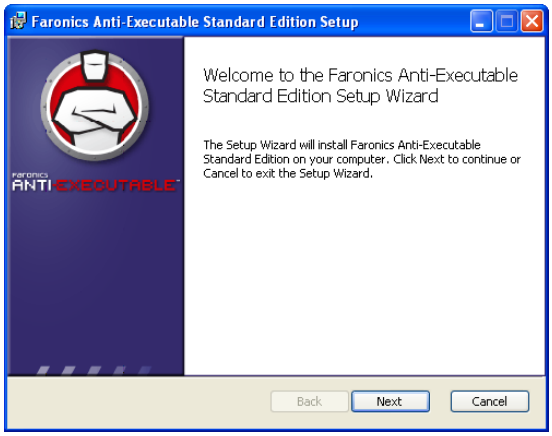
Uninstalling Anti-Executable

Anti-Executable can only be uninstalled when logged in as a user with Anti-Executable Administrator privileges and Anti-Executable Protection is set to Off.

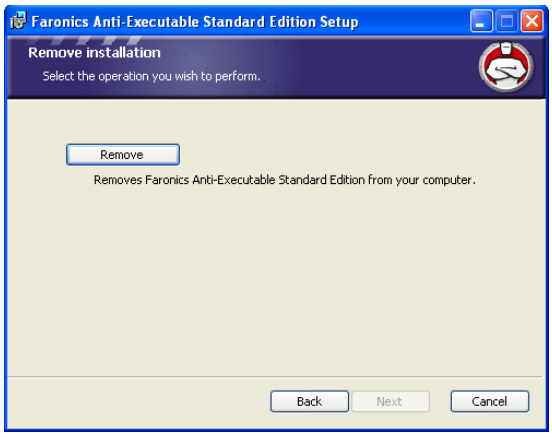
Uninstalling Using the Setup Wizard

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

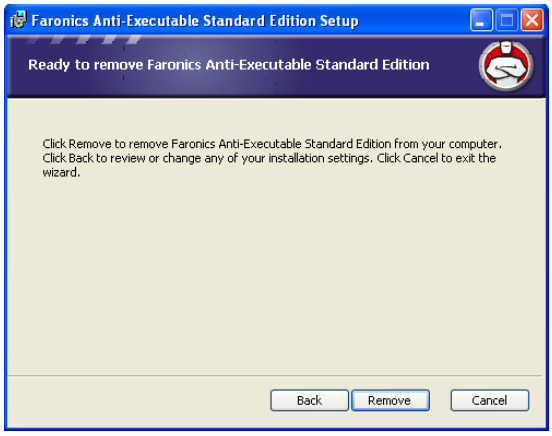
1. Click *Next* to begin the uninstall.



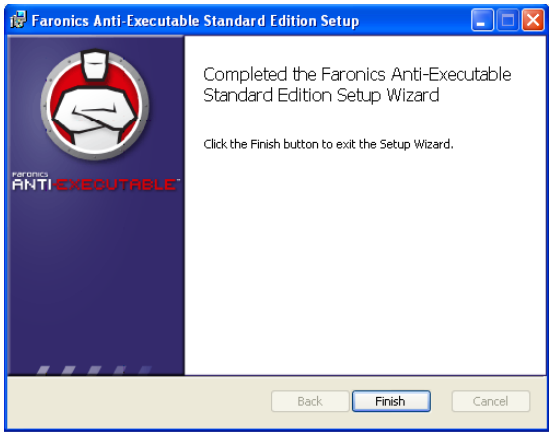
2. Click *Remove* followed by *Next*.



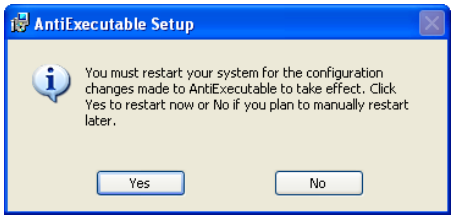
3. Click *Remove*.



4. Click *Finish* to complete the uninstall.



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



An immediate restart is recommended following uninstall.