Faronics Anti-Executable™ Enterprise

ABSOLUTE Protection from Unauthorized Executables

User Guide

Faronics™
Intelligent Solutions for ABSOLUTE Control

www.faronics.com

Last modified: January 2023

Contents

Preface

Faronics Anti-Executable is a solution that ensures endpoint security by only permitting approved executables to run on a workstation or server.

Topics

Important Information

This section contains important information about Anti-Executable.

About Faronics

Faronics delivers software that helps manage, simplify, and secure multi-user computing environments. Our products ensure 100% workstation availability, and have freed IT personnel from tedious technical support and software issues. Fueled by a customer-centric focus, Faronics' technology innovations benefit educational institutions, healthcare facilities, libraries, government organizations and corporations.

Product Documentation

The following documents form the Faronics Anti-Executable technical 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 Feature History – This document lists the new features.
- Faronics Anti-Executable readme.txt – This document guides 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

Web: support.faronics.com

Email: support@faronics.com

Call Toll Free (North America): 1-800-943-6422

Call Local: 1-604-637-3333

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

Contact Information

Headquarters:

Faronics Corporation

609 Granville St., Suite 1400

Vancouver, BC V7Y 1G5, Canada

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)

Faronics Technologies USA Inc.

5506 Sunol Blvd, Suite 202

Pleasanton, CA, 94566, USA

Faronics EMEA

8, The Courtyard, Eastern Road

Bracknell, Berkshire

RG12 2XB, United Kingdom

Faronics Pte Ltd

160 Robinson Road

#05-05 SBF Center

Singapore 068914

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.
Anti-Executable Administrator	Anti-Executable Administrators have access to all Anti-Executable configuration options. They can manage Anti-Executable users, set Anti-Executable protection to Enabled or Disabled, and uninstall/upgrade Anti-Executable.
Anti-Executable 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	They can set Anti-Executable protection to *Enable* or *Disable*. Trusted Users cannot uninstall/upgrade Anti-Executable.
Central Control List	When Faronics Core is launched for the first time after installing Anti-Executable, you are prompted with a message to populate it. You can populate the Central Control List by adding the files and Publishers on the console computer. This Central Control List can then be applied to the workstations via a *Policy*. The Central Control List needs to be created only once, but can be applied multiple times to more than one workstation via a Policy.
Executable	Any file that can be launched by the operating system. The executable files managed by Anti-Executable have the extension *.scr*, *.jar*, *.bat*, *.com*, or *.exe*. Dynamic Link Library files with the extension *.dll* can be managed if configured in the Setup tab.
Execution Control List	An Execution Control list defines how Anti-Executable must manage a file or Publisher. The Execution Control List defines whether the file must be Allowed or Blocked.
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.

Term	Definition
Faronics Core Agent	The software installed on workstations to enable communication with Faronics Core Console.
JAR file	A JAR (Java Archive) is an archive file format contains many Java class files and associated metadata and resources (text, images and so on) into one file to distribute application software or libraries on the Java platform.
Maintenance Mode	When in Maintenance Mode, new executable files added or modified are automatically added to the Local Control List.
Policy	A policy is a group of Anti-Executable settings. Multiple policies can be created and applied to workstations via Faronics Core. You can create a New Policy, edit an existing Policy or delete a policy.
Protection	When set to *Enabled*, this setting indicates that Anti-Executable is protecting a computer based on the Central Control List and Local Control List. When set to Disabled, any executable can be launched on the computer.
Publisher	A Publisher is the creator of a file. A Publisher validates the file by digitally signing it. Anti-Executable uses the Publisher name, product filename, and version details to identify the files created by a Publisher.
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, and prevent the Alert from being displayed.
Temporary Execution Mode	Temporary Execution Mode allows users to run any executable without any action from Anti-Executable for a specified period. During this period, the user is allowed to run any executable without any restrictions. Blocked executables are not allowed to run.
Trusted Executable	A Trusted executable can launch other executables that themselves are unauthorized.
Unauthorized Executable	An Unauthorized executable is one that is not allowed to run.
Workstation	Any client or remote machine using the Operating System specified in the System Requirements.

Introduction

Anti-Executable ensures total endpoint productivity by only allowing approved applications to run on a computer or server. Any other program – whether they are unwanted, unlicensed, or simply unnecessary – are blocked from ever executing.

Topics

Anti-Executable Overview

About Anti-Executable

Faronics delivers software that helps manage, simplify, and secure multi-user computing environments. Our products ensure 100% workstation availability, and have freed IT personnel from tedious technical support and software issues. Fueled by a customer-centric focus, Faronics' technology innovations benefit educational institutions, healthcare facilities, libraries, government organizations and corporations.

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 bests suits your needs:

Edition	Use Anti-Executable to protect
Standard	A single standalone computer loaded with non-server operating system.
Server Standard	A single standalone computer loaded with server operating system.
Enterprise	Multiple computers loaded with non-server operating system.
Server Enterprise	Multiple computers loaded with server operating systems.

About Faronics Core Console

Faronics Core Console is an 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.

Faronics Core Console manages enterprise edition of Anti-Executable and Anti-Executable Server.

System Requirements

Console Requirements

Information on Faronics Core Console system requirements can be found in the Faronics Core Console user's guide available at www.faronics.com/library.

Workstation Requirements

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

- 32- and 64-bit editions of Windows 7, Windows 8.1, Windows 10, and Windows 11 up to version 22H2
- Windows Server 2008 R2, Windows Server 2012, Windows Server 2016, Windows Server 2019, and Windows Server 2022

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.

Anti-Executable Licensing works as follows:

The Core Server (a component of Faronics Core) automatically pushes the License Key to the workstations where Anti-Executable Client is installed (if the computers are offline, the License Key is applied once the computers are back online).

If the Faronics Anti-Executable License Key was entered while installing the Loadin, it is not necessary to enter it again in the Properties tab.

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

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.

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:

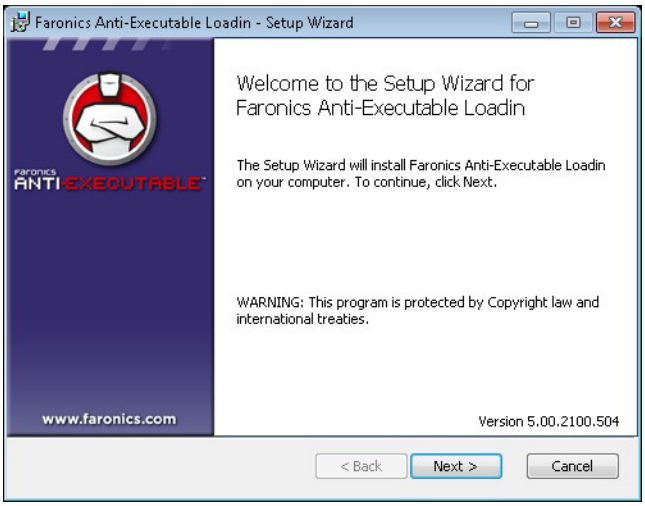
System	Install File
Windows (32-bit)	AEEnt_32-bit.msi
Windows (64-bit)	AEEnt_64-bit.msi
Windows Server (32-bit)	AESrvEnt_32-bit.msi
Windows Server (64-bit)	AESrvEnt_64-bit.msi

Installing Anti-Executable Loadin

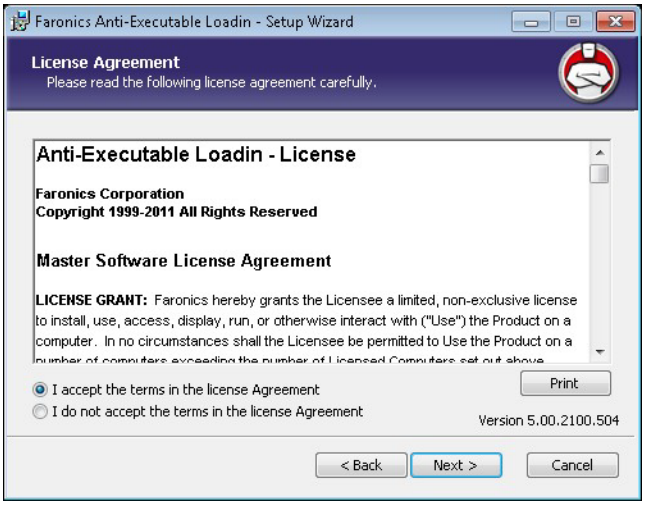
The Anti-Executable Loadin cannot be installed on a computer that does not have Faronics Core Console installed.

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

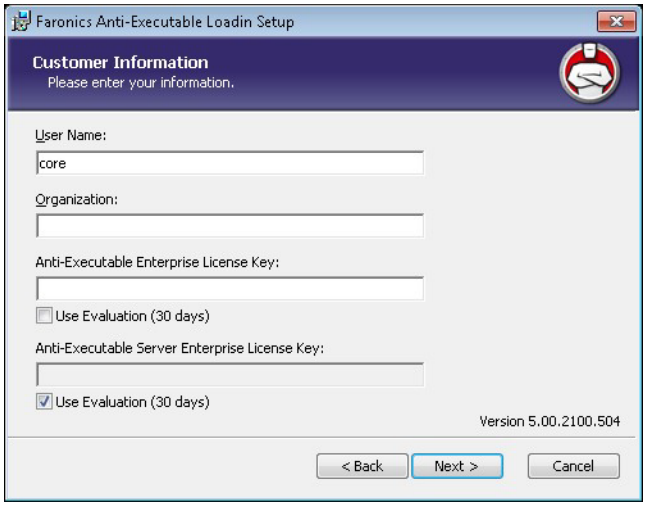
1. If Anti-Executable has been downloaded from the Internet, double-click the *Anti-Executable_Console_Loadin_Installer.exe* file to begin the installation process. Click *Next* to continue.



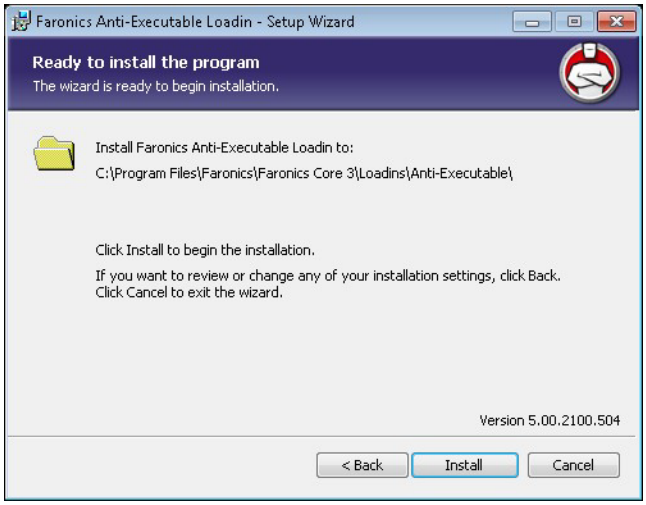
2. Read and accept the License Agreement. Click *Next* to continue.



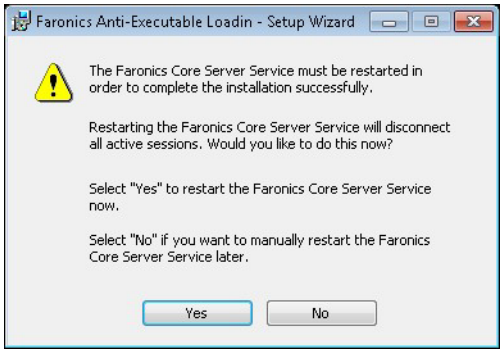
3. Enter the *User Name* and *Organization*. Specify the license key for *Anti-Executable Enterprise* or *Anti-Executable Server Enterprise*. Select *Use Evaluation* to install an evaluation version.



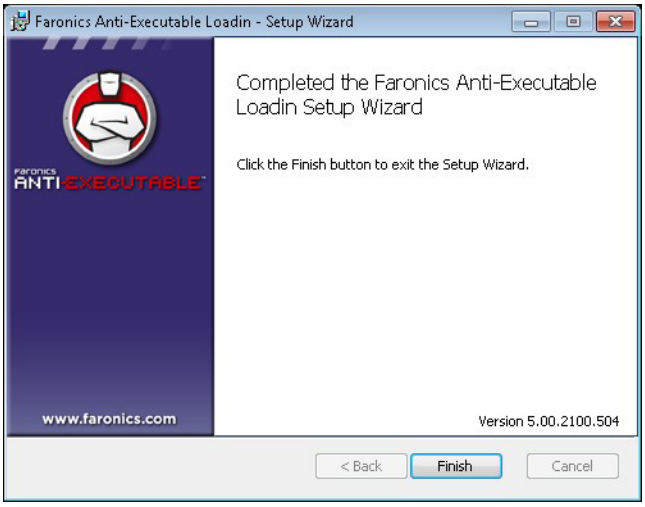
4. The default is *C:\Program Files\Faronics\Faronics Core 3\Loadins\Anti-Executable*. Click *Install* to continue.



5. The Faronics Core Server Service must be restarted to complete the installation successfully. Click *Yes* to restart the Faronics Core Server Service. Click *No* to restart the service manually later.



6. Click *Finish* to complete the installation.



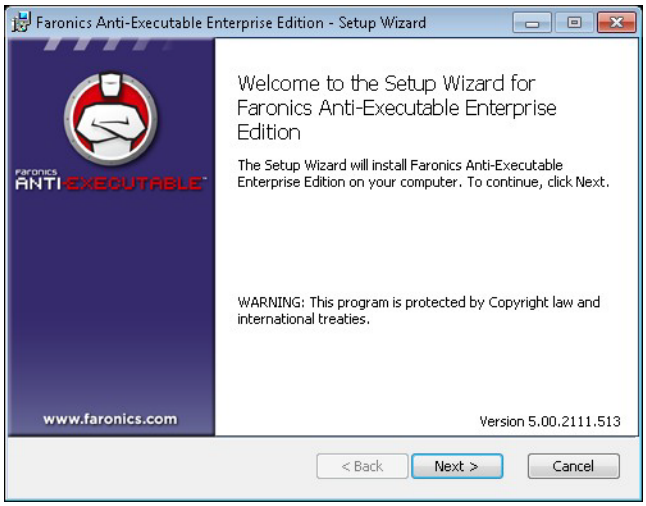
Once the Loadin has been successfully installed, Faronics Core Console displays a list of Anti-Executable specific features in the Actions pane when one or more workstations have been selected. There are also specific columns displayed in the workstation list as illustrated below. Anti-Executable features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

Installing Anti-Executable on a Workstation Manually

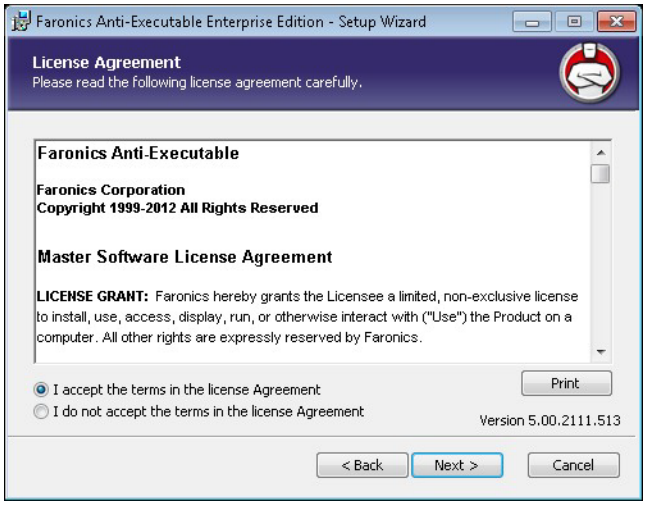
Before installing Anti-Executable on a workstation, copy appropriate *.msi* file from the path *C:\Program Files\Faronics\Faronics Core 3\Loadins\Anti-Executable\Workstation Installers* on the computer where the Anti-Executable Loadin is installed to one or more workstations.

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

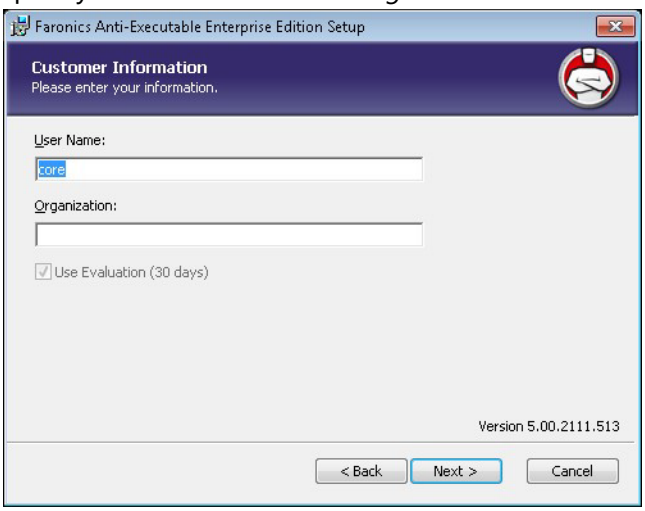
1. Double-click the *.msi* file to begin the installation process. Click *Next* to continue.



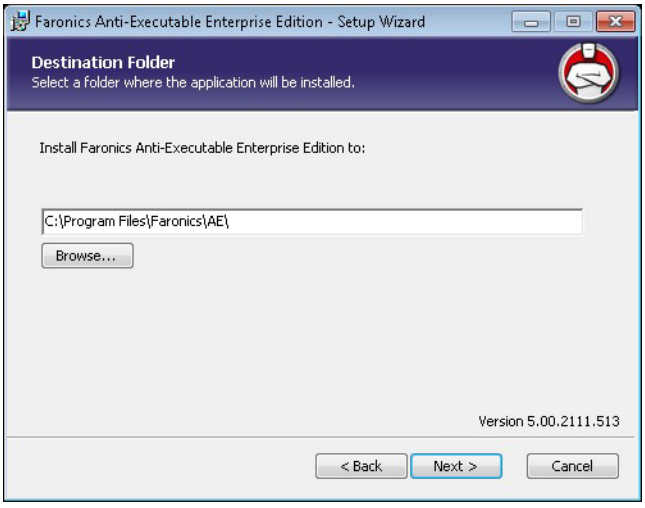
2. Accept the License Agreement. Click *Next* to continue.



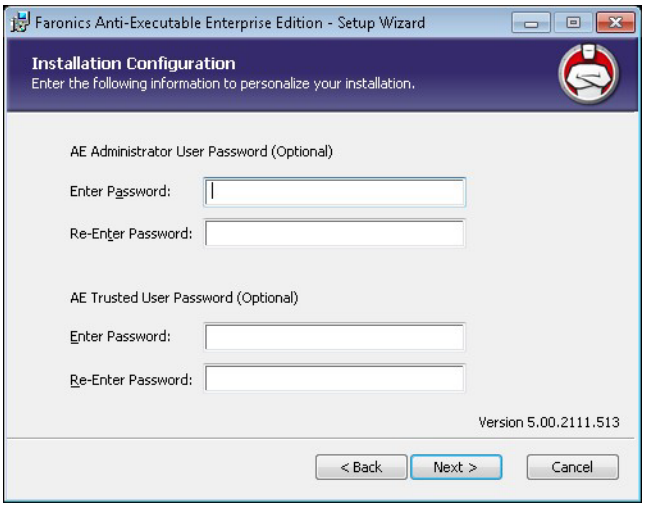
3. Specify the *User Name* and *Organization*. Click *Next* to continue.



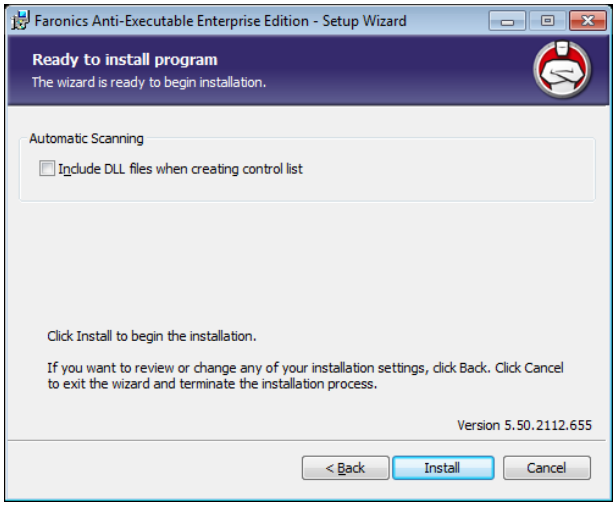
4. Specify the *Destination Folder*. The default location is *C:\Program Files\Faronics\AE*. Click *Next* to continue.



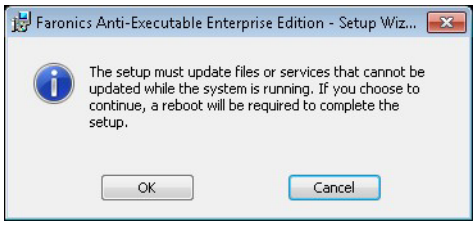
5. Specify the *AE Administrator User Password* and the *AE Trusted User Password*. Click *Next* to continue.



6. Select the following options and Click *Install*.
   > Include DLLs while creating the control list – Select this option if you want DLLs to be included.



7. Click *OK* to restart the computer. Click *Cancel* to restart the computer later.



8. Click *Finish* to complete the installation.

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

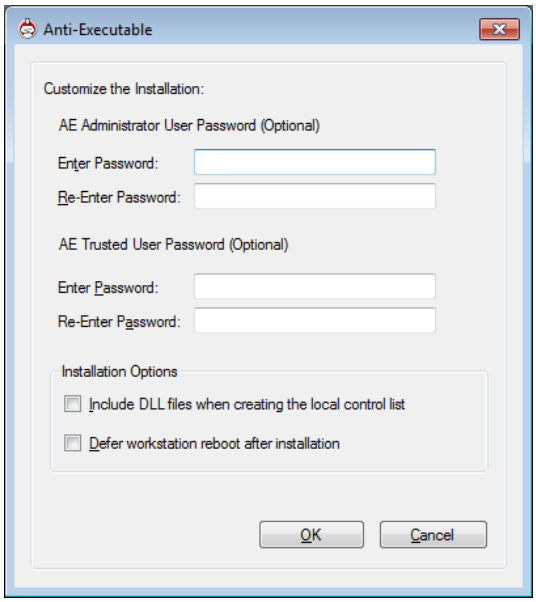
Installing the Anti-Executable Loadin unbundles the Anti-Executable install files required to protect remote computers (the exact files that are unbundled will depend on the edition of Anti-Executable that is being installed).

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* available at www.faronics.com/library.

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* > *Anti-Executable*> *Install/Upgrade Anti-Executable*, or right-click on a workstation from the list in Faronics Core Console and select *Anti-Executable*> *Install/Upgrade Anti-Executable*.
2. Specify the Workstation Credentials. There are two options:
   - > Select *Local Workstation Account* to use the local workstation account as the first user of Anti-Executable. Specify the *User Name*. Click *OK*.
   - > Select *Domain Account* to use the domain account as the first user of Anti-Executable. Specify the *Domain*, *User Name*. Click *OK*.
3. The *Customize the Installation* dialog is displayed. Specify the *AE Administrator Password*, *AE Trusted User Password* and *License Key*. Select one of the following displayed options:
   - > Include DLL files when creating the local control list – To include DLL (Dynamic Link Library) files while scanning.
   - > Defer workstation reboot after installation – To defer reboot after installation. A reboot is required for Anti-Executable to work properly.
4. Click *OK* to install Anti-Executable. Anti-Executable is installed and the Control List is activated.


Anti-Executable
Customize the Installation:
AE Administrator User Password (Optional)
Enter Password:
Re-Enter Password:
AE Trusted User Password (Optional)
Enter Password:
Re-Enter Password:
Installation Options
Include DLL files when creating the local control list
Defer workstation reboot after installation
OK
Cancel

Accessing Anti-Executable

Topics

Overview

Anti-Executable Enterprise can be accessed through Faronics Core Console or directly from the workstation where it is deployed by an authorized user who is logged on.

Accessing Anti-Executable via Faronics Core Console

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

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 a Local Execution 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 Local Execution List when *Enable* is selected. If *Disable* is selected, the changes are not recorded by Anti-Executable.
  - > Temporary Execution Mode – When set to *Temporary Execution Mode*, any executable can be launched on the workstation.
- Policy Name – Name of the policy applied on the workstation.
- Version – This column specifies the Anti-Executable version.
- Logging – This column specifies if logging 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 user guide available at www.faronics.com/library.

Executing Anti-Executable Commands via Faronics Core Console (Loadin-menu)

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

The following commands are available in the Loadin menu.

Manage Central Control List

This command is used to manage a Central Control List. A Central Control List is a repository of files and Publishers. The Central Control List can be applied to one or more workstations through a Policy.

New Policy

A Policy is a group of settings. This command is used to create a new policy. A policy can be applied to one or more workstations. Whether items in the Central Control List are Allowed or Blocked is defined in the Policy.

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. During this period, any executable will be allowed to run. The Maintenance Mode is used for installing new applications and application upgrades.

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*.

Manage AE Users

Select this option to manage Anti-Executable users.

Temporary Execution Mode

Temporary Execution Mode allows users to run any executable without any action from Anti-Executable for a specified period. Select a workstation and select *Temporary Execution Mode* and select *5, 15, 30, 45, 60 or Custom*. Select a workstation and select *Temporary Executing Mode* > *Disable* to disable Temporary Execution Mode.

Initiate a Local Control List Scan

Initiate a Control List scan by scanning for files on the workstation. This creates a local list of files and Publishers. All the files and Publishers added in the Control List are *Allowed* by default.

Reassign Policy

Reassign the policy currently applied on the workstation.

Configure Anti-Executable Client

Select this option to configure Anti-Executable Client on the workstation.

Install/Upgrade Anti-Executable Client

Select this option to install or upgrade the Anti-Executable Client.

Uninstall Anti-Executable Client

Select this option to uninstall Anti-Executable.

Executing Anti-Executable Commands via Faronics Core Console (Context-menu)

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.

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*.

Manage AE Users

Select this option to manage Anti-Executable users.

Temporary Execution Mode

Temporary Execution Mode allows users to run any executable without any action from Anti-Executable for a specified period. Select a workstation and select *Temporary Execution Mode* and select *5, 15, 30, 45, 60 or Custom.* Select a workstation and select *Temporary Executing Mode* > *Disable* to disable Temporary Execution Mode.

Initiate a Local Control List Scan

Initiate a Control List scan by scanning for files on the workstation. You can also add the files or Publishers to a policy.

Reassign Policy

Reassign the policy currently applied on the workstation.

Configure Anti-Executable Client

Select this option to configure Anti-Executable Client on the workstation.

Install/Upgrade Anti-Executable Client

Select this option to install or upgrade the Anti-Executable Client.

Uninstall Anti-Executable Client

Select this option to uninstall 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
- Alerts (Enable or Disable)
- Temporary Execution Mode
- Initiating a Control List Scan
- Install/Upgrade Anti-Executable
- Uninstall Anti-Executable

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 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, Execution Control List, and User tabs. If you are a Trusted User, you will have access only to the Status, and Execution Control 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

Anti-Executable provides multiple Control Lists for enhanced protection. The following components are available:

- Central Control List – A Central Control List is a repository of files and Publishers. When Faronics Core is launched for the first time after installing Anti-Executable, you are prompted with a message to populate the Central Control List. You can populate the Central Control List by adding the files and Publishers on the console computer, remote computer on the network or a UNC path.

  Anti-Executable is pre-populated with a list of commonly-known Publishers. This list is updated as needed.
- Policy – A policy is a group of Anti-Executable settings. Multiple policies can be created and applied to workstations via Faronics Core. You can create a New Policy, edit an existing Policy or delete a Policy. Whether items in the Central Control List are Allowed or Blocked is defined in the Policy.
- Execution Control List – An Execution Control list defines how Anti-Executable must manage a file or Publisher. The Execution Control List defines whether the file or Publisher must be Allowed or Blocked.
- Local List of Files and Publishers – When Anti-Executable is installed for the first time on the workstation, there is an option to scan the workstation and create a list of all files and Publishers that are *Allowed*. This list resides on the workstation and cannot be viewed or edited from Faronics Core. Each workstation has its own Local List of Files and Publishers.

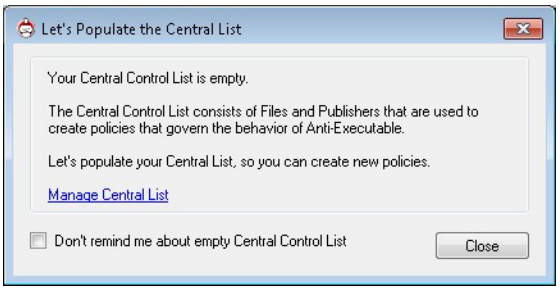
Make sure the Central Control List is kept very small. If the Central Control List is very large, it might take a long time for the settings to be applied to multiple workstations.

Create a Central Control List

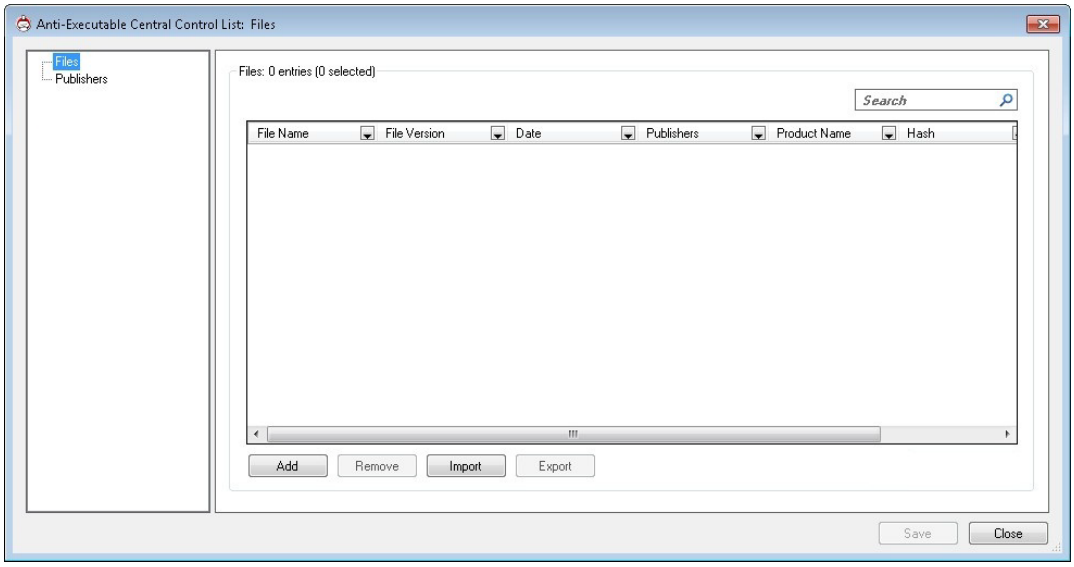
When Faronics Core is launched for the first time after installing Anti-Executable, you are prompted with a message that the Control List is empty.

Complete the following steps to populate a Central Control List:

1. Click *Manage Central Control List* in the dialog that appears for the first time when Faronics Core is launched after installing Anti-Executable for the first time. Alternatively, right-click the Anti-Executable Loadin and select *Manage Central Control List*.

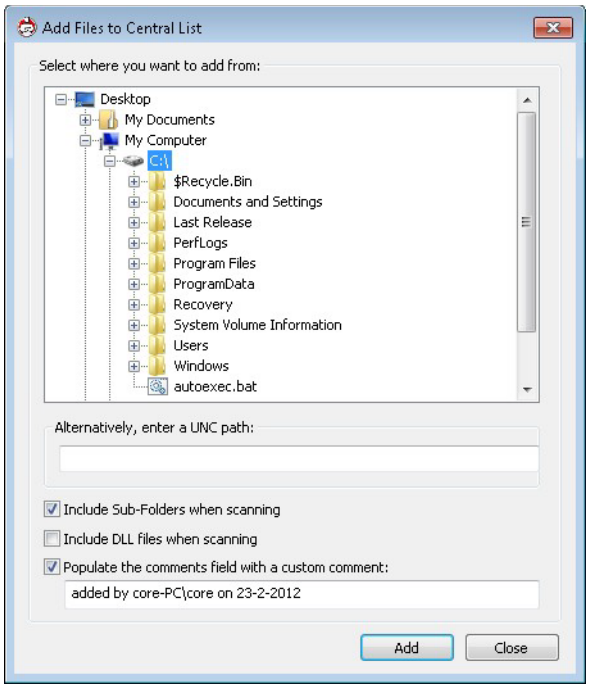


2. The Anti-Executable Central Control list screen is displayed.



3. In the File node, click *Add*. The *Add files to Central Control List* dialog is displayed.

4. Browse to select the folder/drive on the console computer. Select the following options and click *Add*:

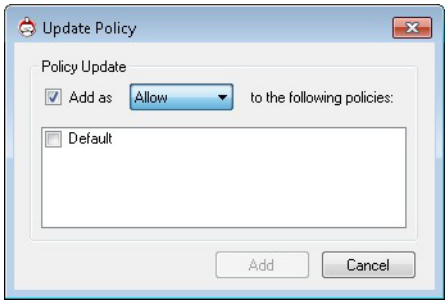


> Include sub-folders when scanning – Select this option to include all the sub-folders when scanning the selected drive/folder.

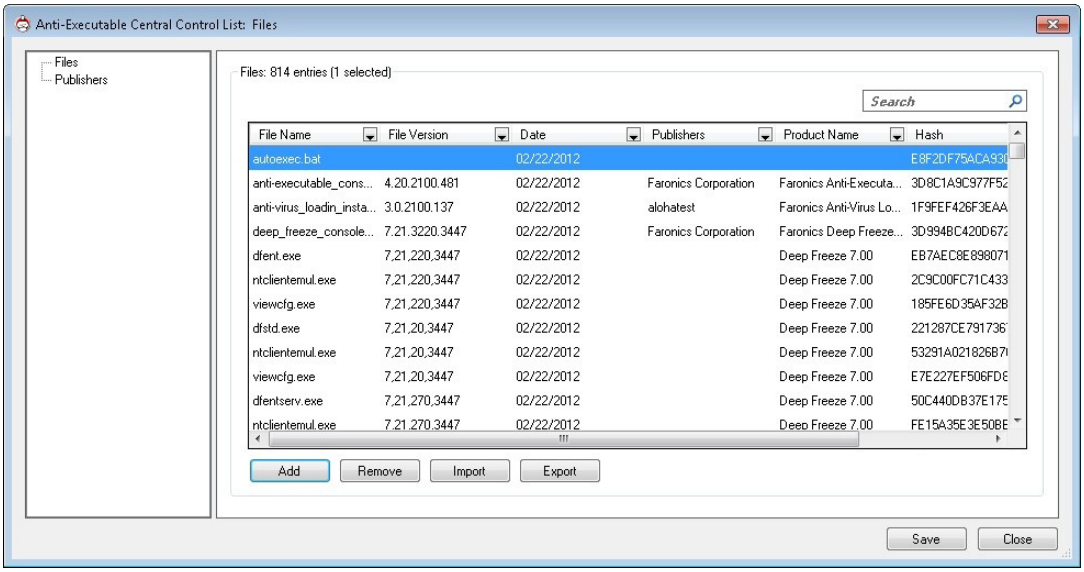
> Include DLL files when scanning – To include DLL (Dynamic Link Library) files while scanning.

> Populate the comments field with a custom comment – Select this option and edit the comment if required. These comments are visible in the Central List.

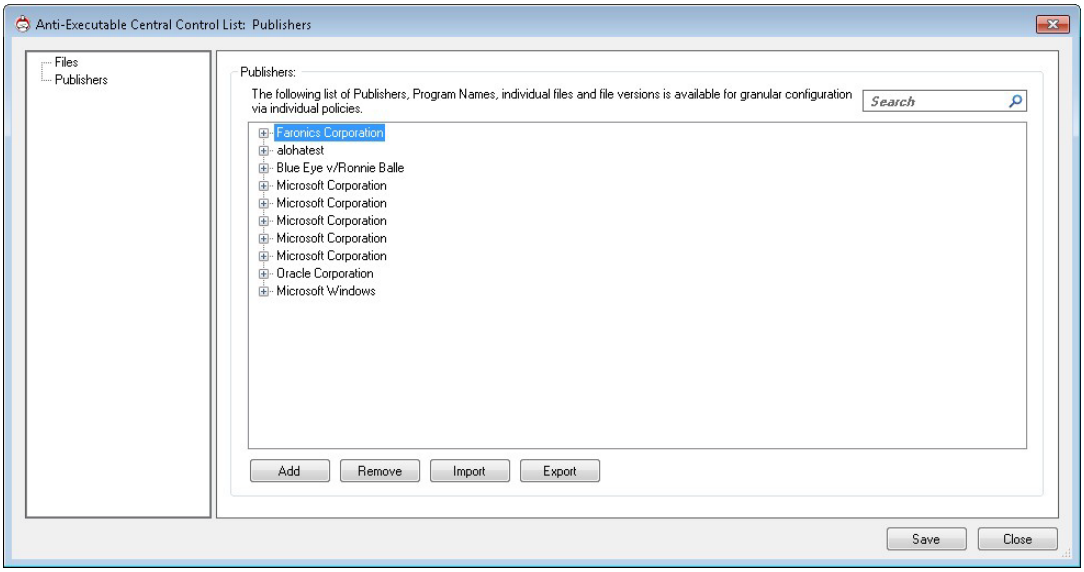
5. Add these files to one or more policy in the Policy Update dialog. Select Allow or Block from the drop-down and select policy to which these must be added.



6. The added files are displayed. You can select Remove to remove a selected file, Export or Import the list of files. You can sort the files based on the title of the column. You can also dynamically search for a specific string from the column header.



7. Click *Publishers*. The list of Publishers on the console computer is automatically added and is displayed. Click *Add* to add Publishers. Click *Remove* to remove the selected publisher. Click *Import* to import a list of Publishers. Click *Export* to export the list of Publishers.



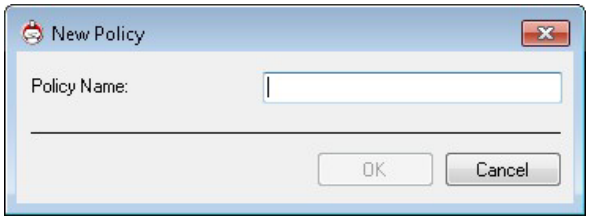
8. Click *OK*. The Central Control List is saved and can be applied to workstations via a policy.

Anti-Executable Policy

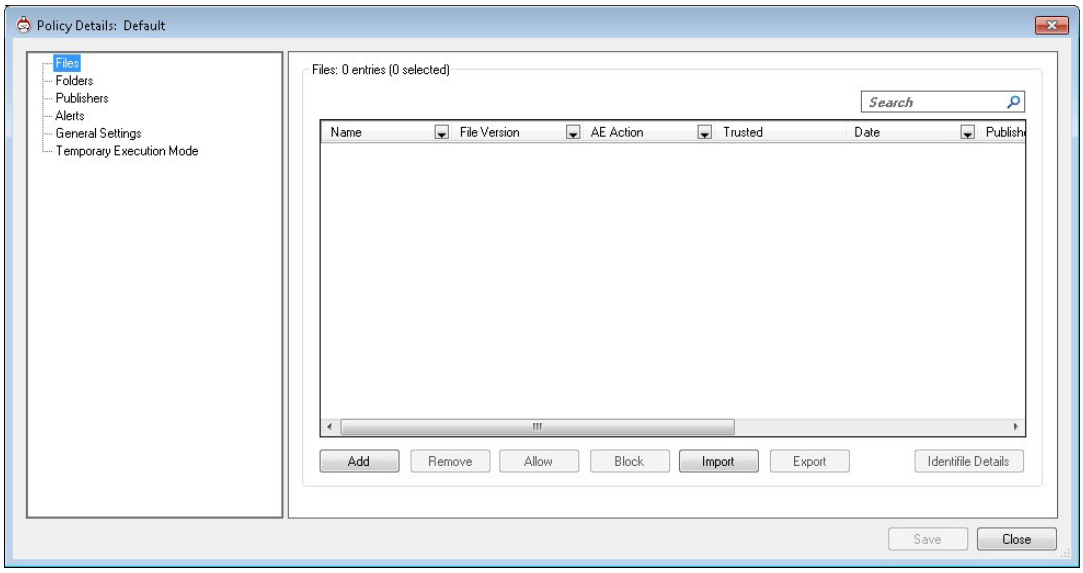
A Policy is a group of settings. An Anti-Executable Policy can be created and applied to multiple workstations. Multiple Policies can be created as per the requirement.

Complete the following steps to create an Anti-Executable Policy:

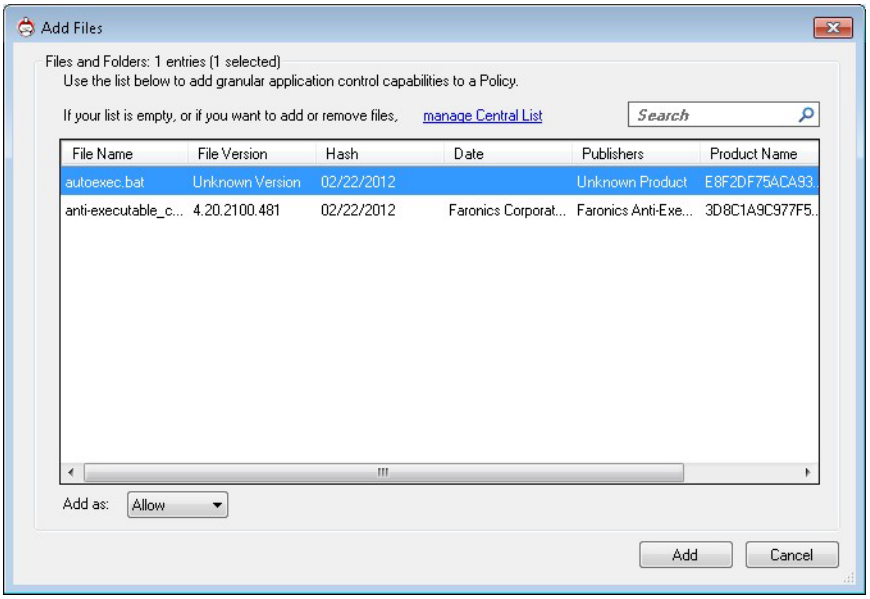
1. Right-click on the Anti-Executable Loadin and select New Policy.
2. The New Policy dialog is displayed. Specify the name of the policy and click *OK*.



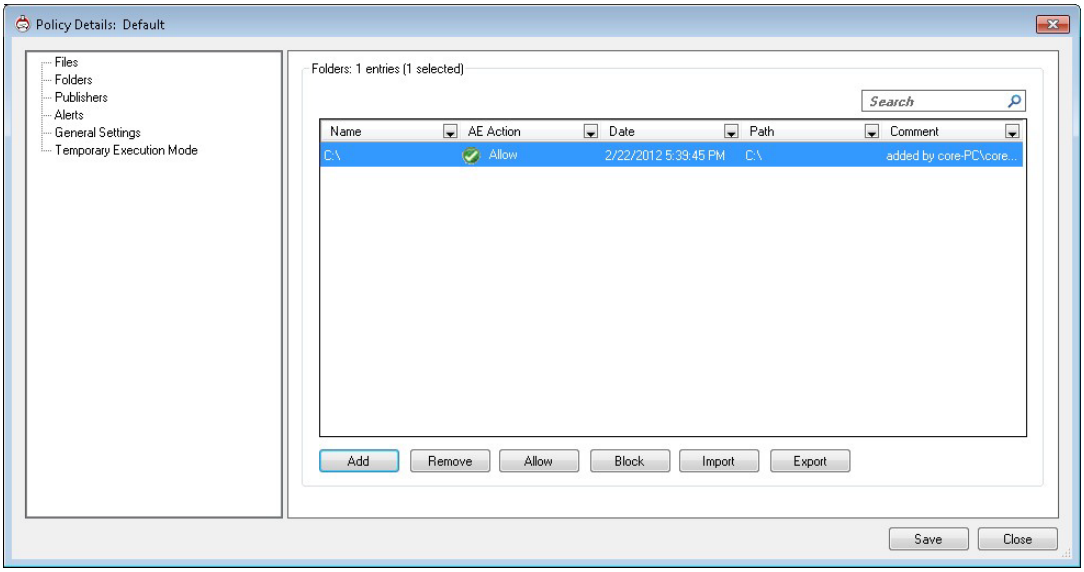
3. The Policy dialog is displayed with the File node.



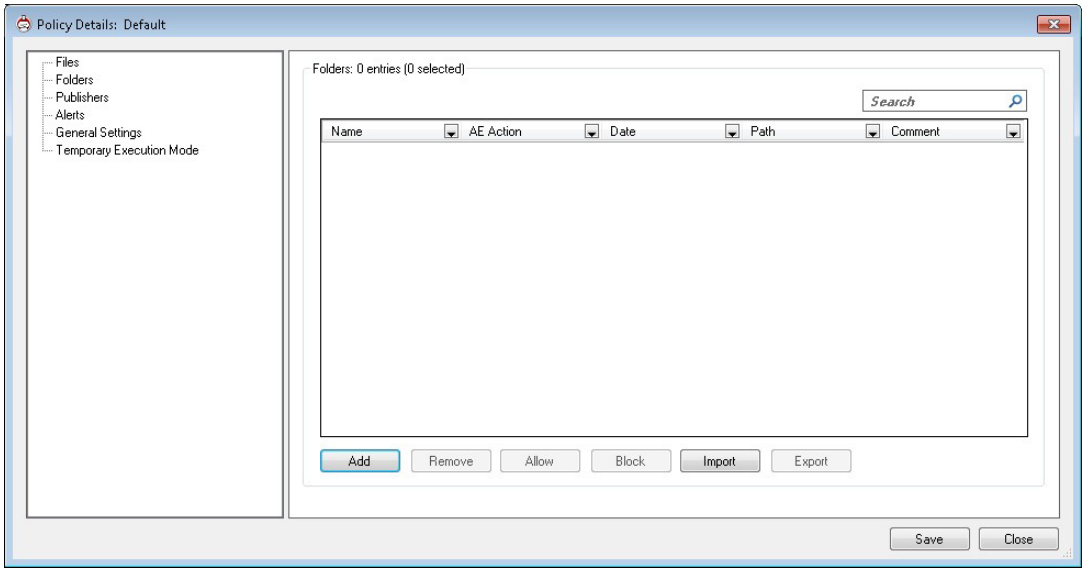
4. In the File node, click *Add*. The files added to the Central Control List are displayed. Select the files and select Allow or Block from the Add as drop-down and click *Add*.



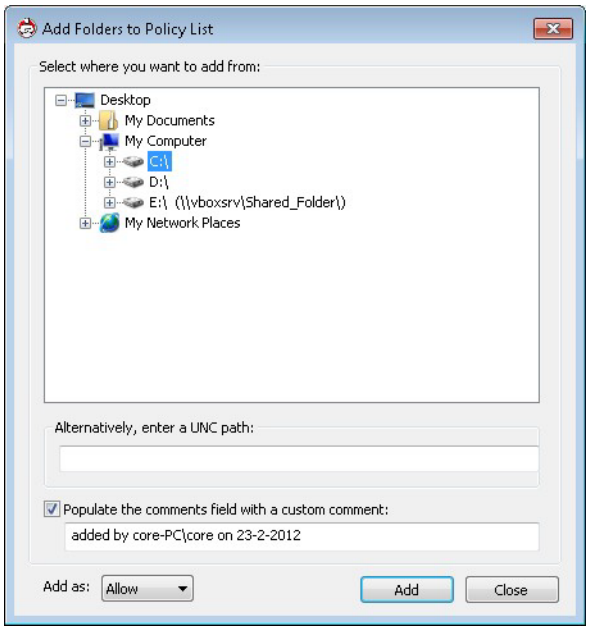
5. The files are added to the policy.



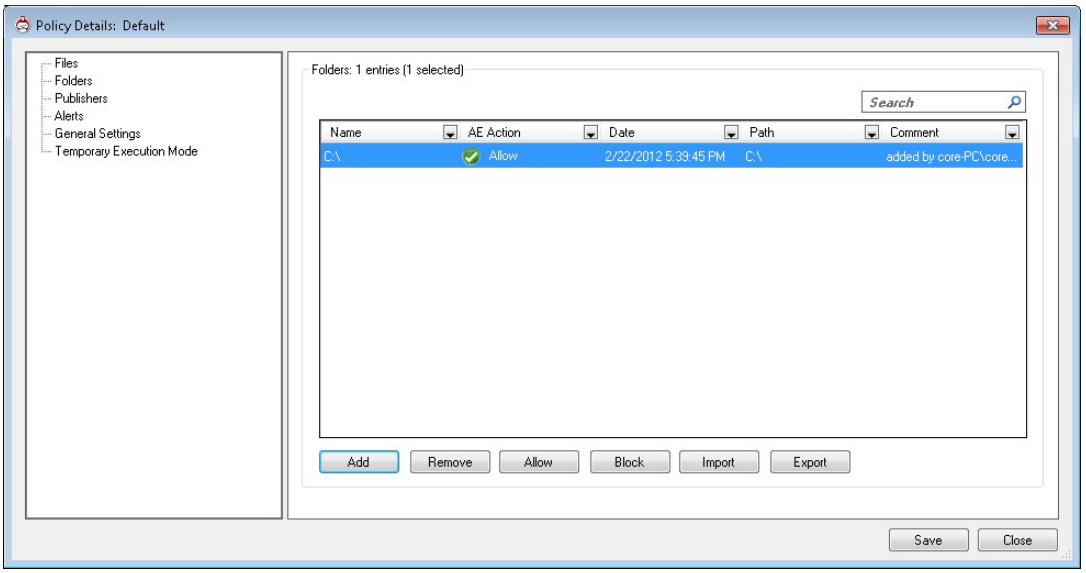
6. Click the *Folders* node and click *Add*.



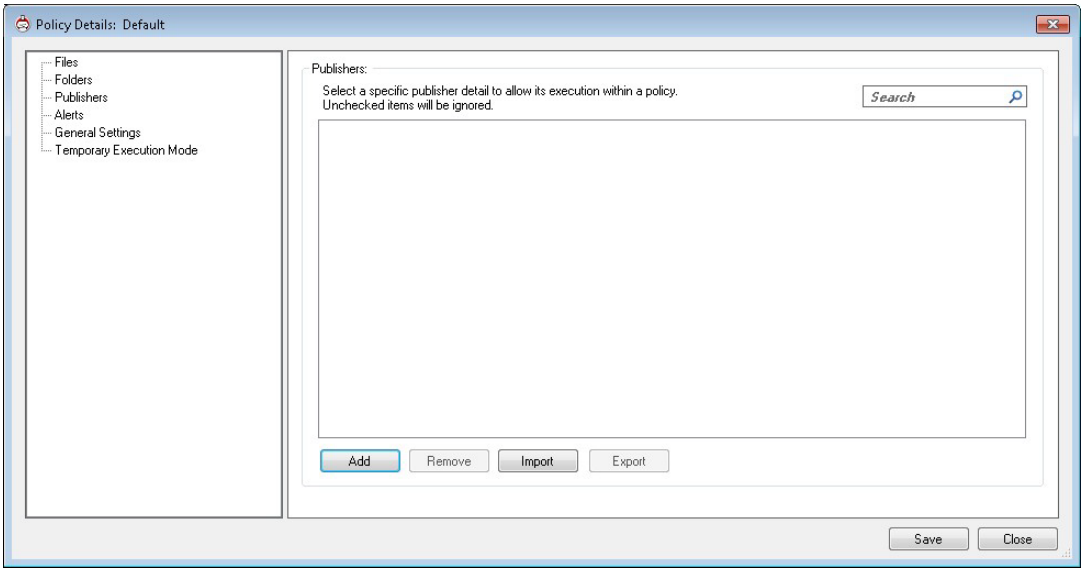
7. Browse to select the folder from the Add Folders to Policy List dialog. Alternatively, you can enter a UNC path. Select the Populate the comments field with a custom comment and specify a comment (optional). Click *Add*.



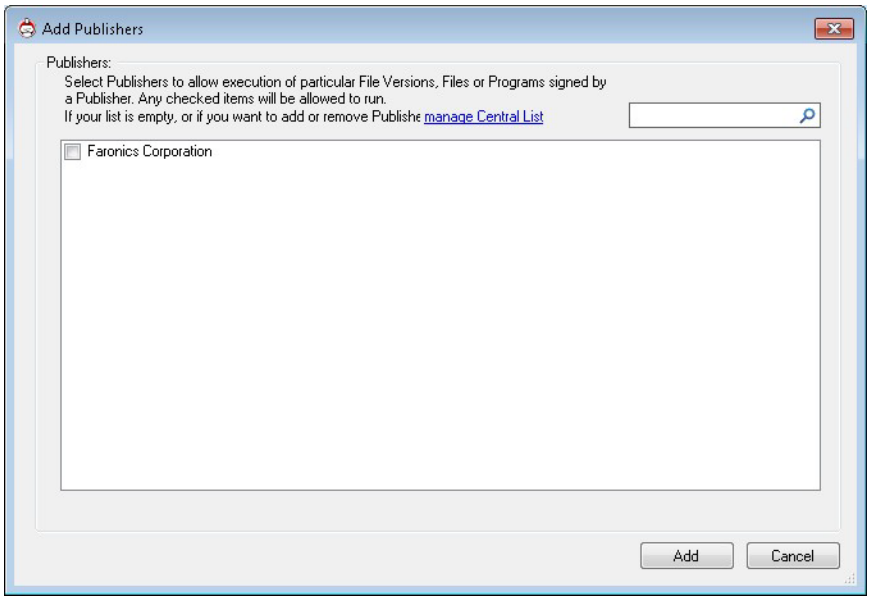
8. The folder/drive is added to the policy.



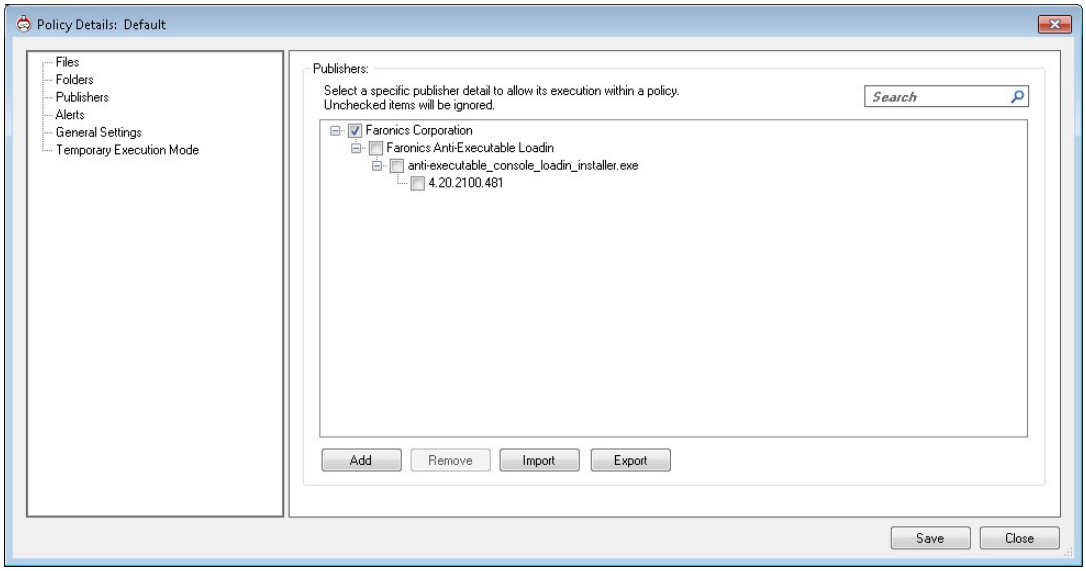
9. Click the *Publishers* node. Click *Add*.



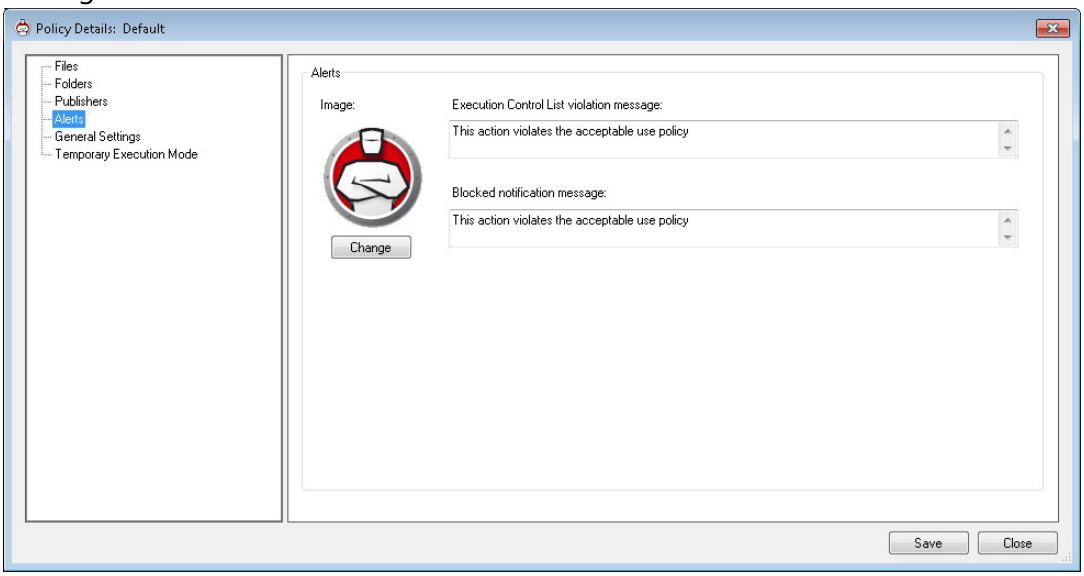
10. Select the Publishers that were added to the Central Control List and click *Add*.



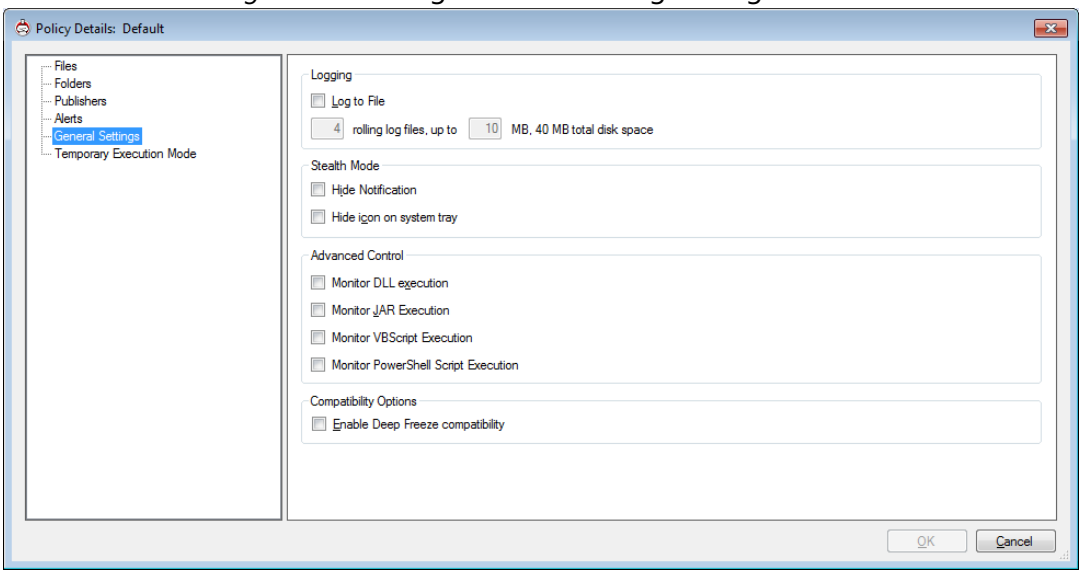
11. The Publishers are added. Select the top node of the Publisher to add all sub-nodes or just select the sub-node.



12. Click the *Alerts* node. Click *Change* to change the image displayed to the users. You can also edit the Execution Control List violation message and Blocked notification message.



13. Click *General Settings* node. Configure the following settings:



- Logging – Select *Log to File* to log events to the log file. In Windows 7, the log file is located at *C:\ProgramData\Faronics\Storage Space\AEE*.
- Stealth Mode – 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. 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.
- Monitor DLL Execution – Select the *Monitor DLL Execution* checkbox to monitor DLLs. If this checkbox is not selected, the DLLs will not be monitored even if they have been added to the Control List.
- Monitor JAR Execution – Select the *Monitor JAR Execution* checkbox to monitor JAR files. If this checkbox is not selected, the JAR files will not be monitored even if they have been added to the Control List.
- Monitor VBScript Execution – Select the Monitor VBScript Execution checkbox to monitor VBScript files. If this checkbox is not selected, the VBScript files will not be monitored even if they have been added to the Execution Control List.
- Monitor PowerShell Execution – Select the Monitor PowerShell Execution checkbox to monitor PowerShell files. If this checkbox is not selected, the PowerShell files will not be monitored even if they have been added to the Execution Control List.
- Compatibility Options – Anti-Executable is compatible with Deep Freeze.
  - > Deep Freeze Compatibility – This feature is applicable only when Deep Freeze and Anti-Executable are installed on the computer. The Deep Freeze Compatibility feature allows the Administrator to synchronize the Maintenance Modes of Deep Freeze and Anti-Executable. By enabling the *Enable Deep Freeze Compatibility* checkbox, Anti-Executable will automatically enter Maintenance Mode when Deep Freeze enters Maintenance Mode (Deep Freeze reboots *Thawed* in 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 Execution Control 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 Execution Control List. When Deep Freeze exits its Maintenance Mode, it will reboot the computer *Frozen* with the updated Execution Control List.

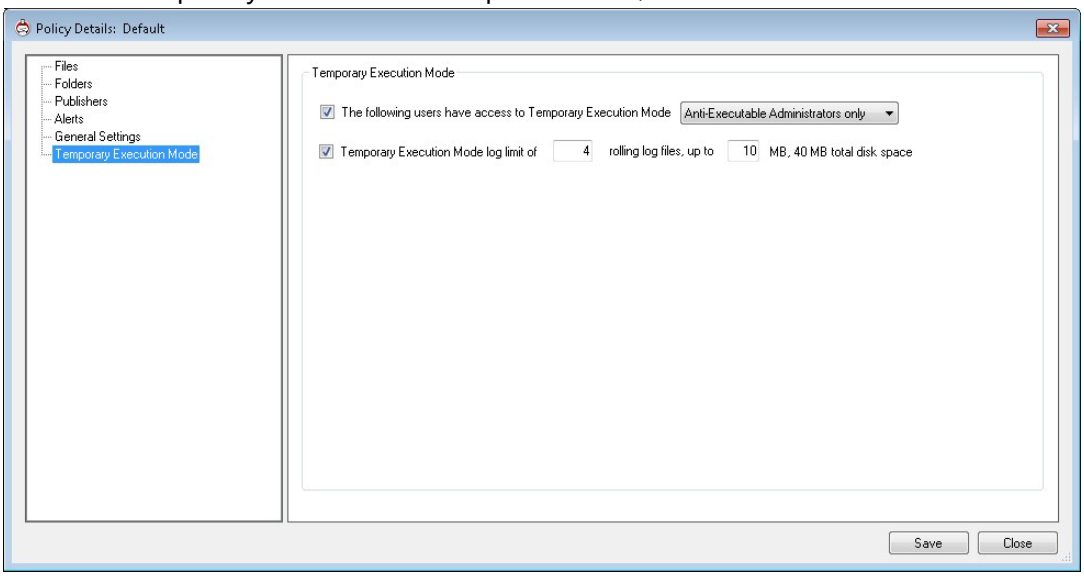
It is not possible to set Anti-Executable to Maintenance Mode if *Deep Freeze Compatibility* is enabled and Deep Freeze status is *Frozen*. This is because, changes made to the computer will be lost on reboot.

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.

14. Click the Temporary Execution Mode node. Temporary Execution Mode allows users to run any executable without any action from Anti-Executable for a specified period. During this period, the user is allowed to run any executable without any restrictions. Once the Temporary Execution Mode period ends, Anti-Executable is Enabled.



The following options are available for Temporary Execution Mode:

- The following users have access to Temporary Execution Mode – Select the checkbox to allow specific set of users to activate Temporary Execution Mode on their systems. Select All Users, Anti-Executable users or Anti-Executable Administrators only.
- Temporary Execution Mode log – Select the checkbox to create log files during Temporary Execution Mode.
  - > Number of log files – Specify the number of log files (up to a maximum of 10). The logging information is stored in the files serially. For example, if there are 3 files A,B and C, Faronics Anti-Executable first writes the error logs to file A. Once file A is full, it starts writing to file B and finally file C. Once file C is full, the data in file A is erased and new logging data is written to it.
  - > File size – Select the size of each file in MB. There can be a maximum of 10 log files of up to 10 MB each i.e. total 100 MB.

15. Click *OK*. The policy is saved.

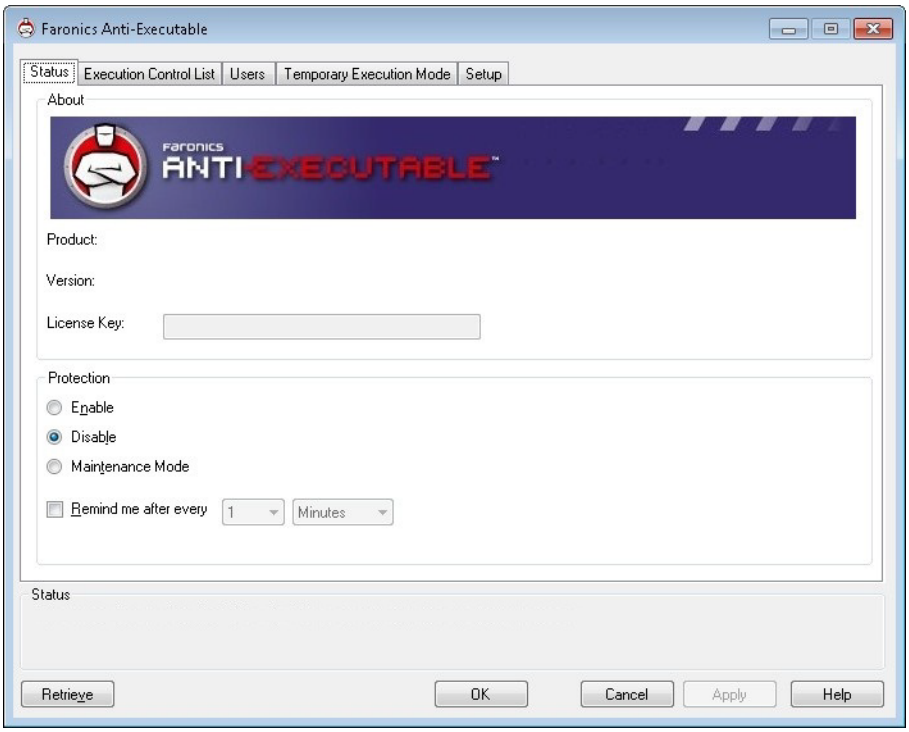
Configuring Anti-Executable

Right-click on a single workstation and select Configure Anti-Executable Client. Anti-Executable settings are retrieved from the workstation and the following tabs are available:

- Status
- Execution Control List
- Users
- Temporary Execution Mode
- Setup

Status Tab

The Status tab allows Anti-Executable Administrators and Trusted Users to configure various settings, set protection to *Enable*, *Disable,* or *Maintenance Mode*. 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.

License Keys can be obtained by contacting Faronics or Faronics Partners.

Enabling Anti-Executable Protection

Following installation, Anti-Executable is enabled by default.

Use the *Remind Me after every* checkbox 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 Execution Control 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.

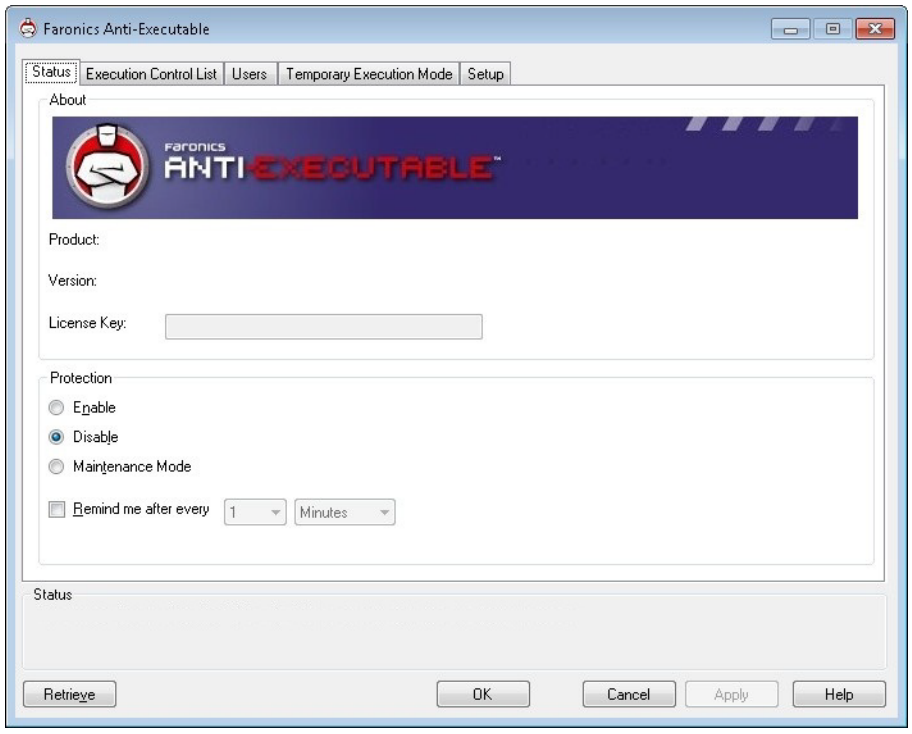
The *Disable Keyboard and Mouse* checkbox is available only while accessing Anti-Executable via Faronics Core Console. This is to ensure that a computer that has its keyboard and mouse disabled can still be managed remotely via Faronics Core Console.

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 Execution Control List.

Retrieving settings from Faronics Core Console

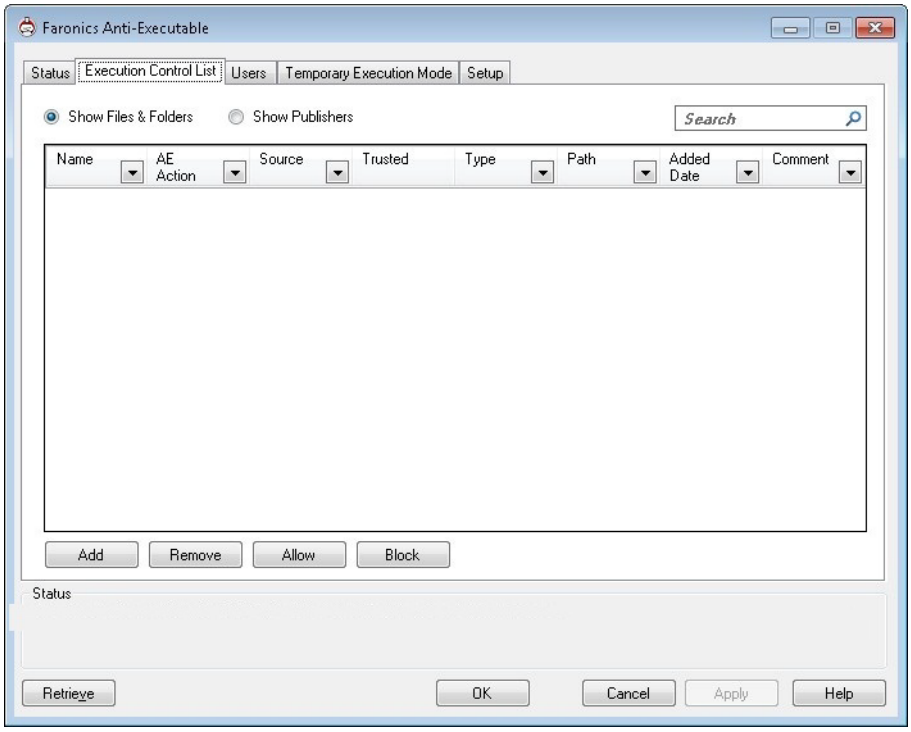
The *Status* pane retrieves and displays all the settings of a single workstation. When a single workstation is selected and Anti-Executable is launched via Faronics Core Console, the workstation settings are retrieved automatically.



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

Execution Control List Tab

The Execution Control List tab allows you to specify whether the items in the Local Control List or Central Control List must be Allowed or Blocked.



Complete the following steps to specify the Anti-Executable behavior:

1. Select Show Files & Folders or Show Publishers.
2. If Show Files & Folders is selected, the following columns are displayed:
   - Name
   - AE Action
   - Source
   - Trusted
   - Type
   - Path
   - Added Date
   - Comment
3. Click *Add* to add Files or Folders to the Central Control List and Execution Control List. Select an item and click *Remove* to remove from the Execution Control List. Select an item and click *Allow* or *Block*.
4. Click *Apply*. Click *OK*.

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 Central Control List, Local Control List, Execution Control List, Users, and Setup and can uninstall Anti-Executable.
- Trusted User – Can configure Anti-Executable, and set the Execution Control 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.

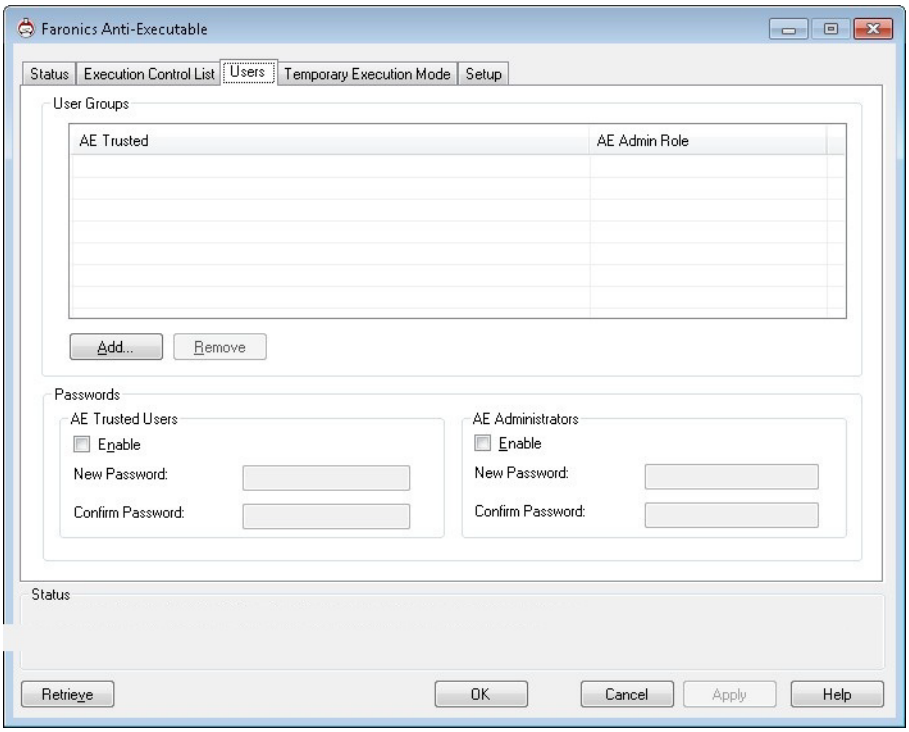
If an Anti-Executable Administrator or Trusted User attempts to open an unauthorized application while Anti-Executable is enabled, the Alert dialog will be displayed.

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.



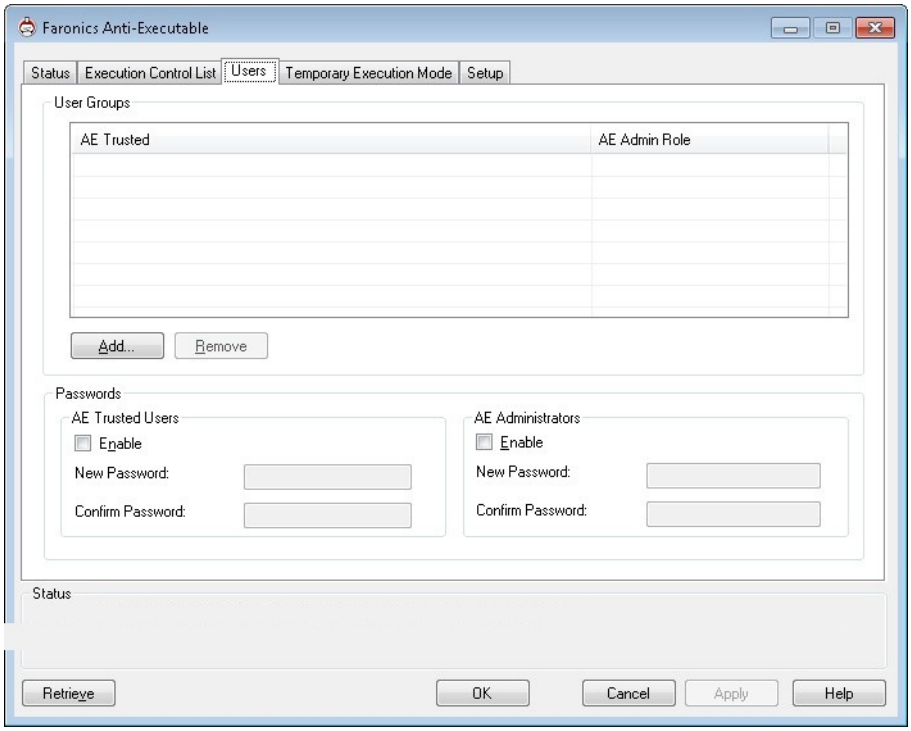
2. Click *Add* to add a new user. Select the *User* icon from the list provided.
3. Click *Advanced* > *Find Now* to display a list of available users. Anti-Executable administrators can add domain users (or groups) and local users (or groups). Click on a user or group to add it to Anti-Executable's 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* checkbox.

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

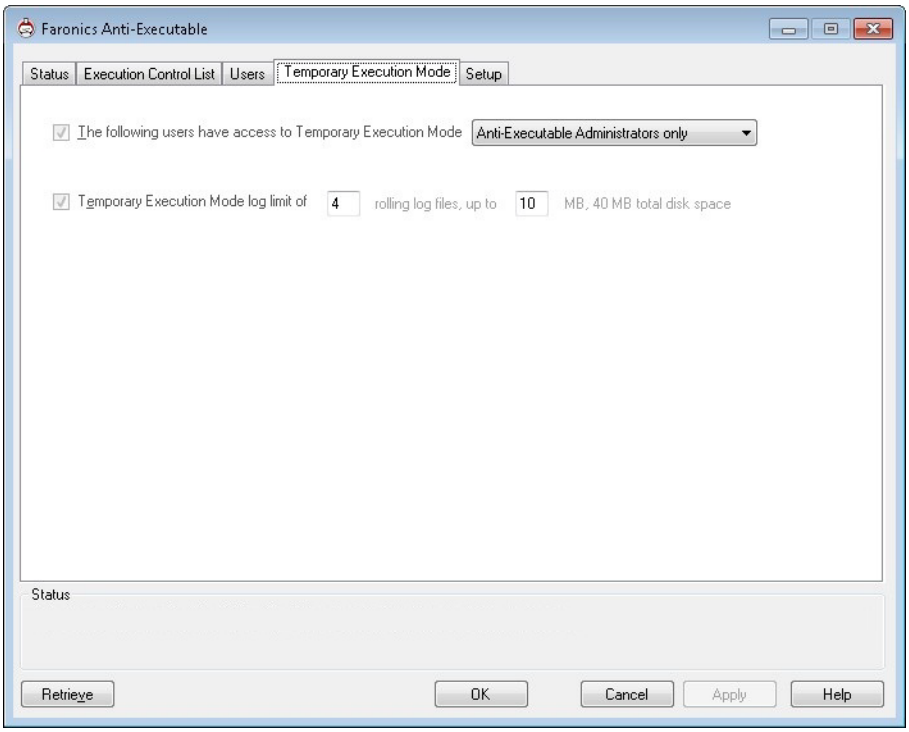
As an added layer of protection, Anti-Executable can attach a password to each user group. Passwords only apply to the members of the associated groups. To specify a password, ensure the *Enable* checkbox is selected and enter the password in the *New Password* and *Confirm Password* fields. Click *Apply*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



Temporary Execution Mode Tab

Temporary Execution Mode allows users to run any executable without any action from Anti-Executable for a specified period. During this period, the user is allowed to run any executable without any restrictions. Once the Temporary Execution Mode period ends, Anti-Executable is Enabled. The Temporary Execution Mode tab displays the information from the Policy. Settings on the Temporary Execution Mode tab cannot be modified on the workstation. Settings in the Temporary Execution Mode tab cannot be modified since they are part of a Policy.

The following options are available for Temporary Execution Mode:



- The following users have access to Temporary Execution Mode – To allow specific set of users to activate Temporary Execution Mode on their systems. Select All Users, Anti-Executable users or Anti-Executable Administrators only.
- Temporary Execution Mode log – To create log files during Temporary Execution Mode.
  - > Number of log files – Specify the number of log files (up to a maximum of 10). The logging information is stored in the files serially. For example, if there are 3 files A,B and C, Faronics Anti-Executable first writes the error logs to file A. Once file A is full, it starts writing to file B and finally file C. Once file C is full, the data in file A is erased and new logging data is written to it.
  - > File size – Select the size of each file in MB. There can be a maximum of 10 log files of up to 10 MB each i.e total 100 MB.

Activating or Deactivating Temporary Execution Mode

Temporary Execution Mode can be activated in the following ways:

From Faronics Core:

- Activating Temporary Execution Mode: Select one or more workstations and select *Anti-Executable* > *Temporary Execution Mode* > *x minutes* (select up to 60 minutes, 24 hours or 7 days)
- Deactivating Temporary Execution Mode: Select one or more workstations and select *Anti-Executable* > *Temporary Execution Mode* > *Disable*

From the workstation:

- Activating Temporary Execution Mode: Right-click on the Anti-Executable icon in the System Tray and select *Temporary Execution Mode* > *x minutes* (select up to 60 minutes, 24 hours or 7 days)
- Deactivating Temporary Execution Mode: Right-click on the Anti-Executable icon in the System Tray and select *Temporary Execution Mode* > *Disable*

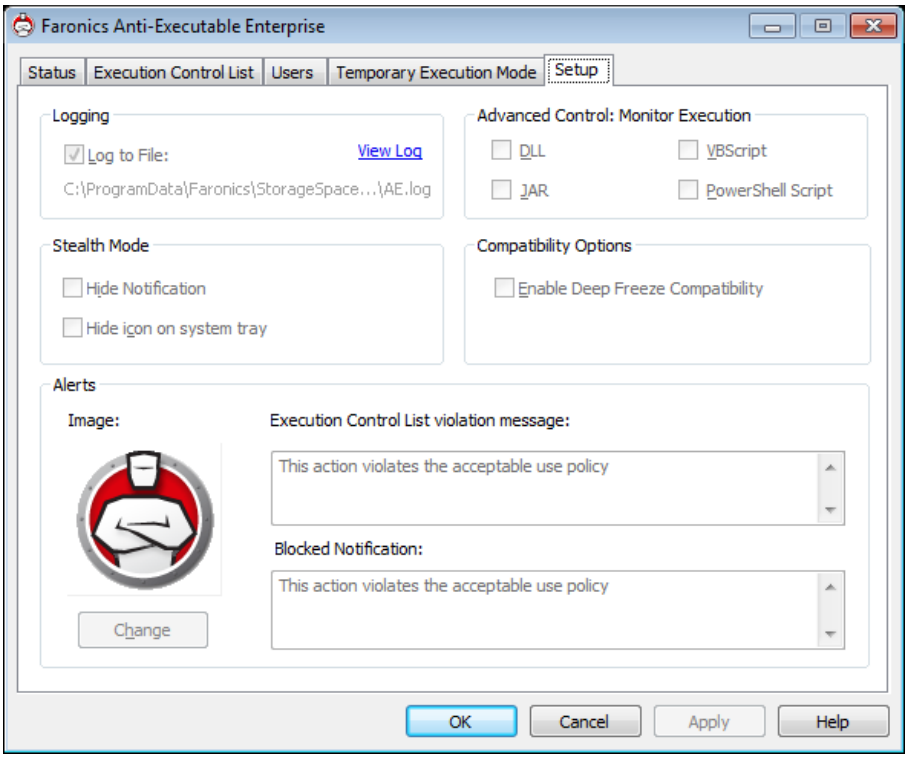
The following icon is displayed in the System Tray at the workstation when Temporary Execution Mode is activated:

A message appears at the workstation 3 minutes before the Temporary Execution Mode ends.

Automatic Windows Updates will be disabled during Temporary Execution Mode.

Setup Tab

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



Setting Event Logging in Anti-Executable

Select *Log to File* to log events to the log file. In Windows 7, the log file is located at *C:\ProgramData\Faronics\Storage Space\AEE*.

Monitor DLL Execution

Select the *Monitor DLL Execution* checkbox to monitor DLLs. If this checkbox is not selected, the DLLs will not be monitored even if they have been added to the Execution Control List.

Monitor JAR Execution

Select the *Monitor JAR Execution* checkbox to monitor JAR files. If this checkbox is not selected, the JAR files will not be monitored even if they have been added to the Execution Control List.

Monitor VBScript Execution

Select the *Monitor VBScript Execution* checkbox to monitor VBScript files. If this checkbox is not selected, the VBScript files will not be monitored even if they have been added to the Execution Control List.

Monitor PowerShell Execution

Select the *Monitor PowerShell Execution* checkbox to monitor PowerShell files. If this checkbox is not selected, the PowerShell files will not be monitored even if they have been added to the Execution Control List.

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 and prevent the Alert 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.

Compatibility Options

Anti-Executable is compatible with Deep Freeze.

Deep Freeze Compatibility

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

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

By enabling the *Enable Deep Freeze Compatibility* checkbox, Anti-Executable will automatically enter Maintenance Mode when Deep Freeze enters Maintenance Mode (Deep Freeze reboots *Thawed* in 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 Execution Control 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 Execution Control List. When Deep Freeze exits its Maintenance Mode, it will reboot the computer *Frozen* with the updated Execution Control List.

It is not possible to set Anti-Executable to Maintenance Mode if *Deep Freeze 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:

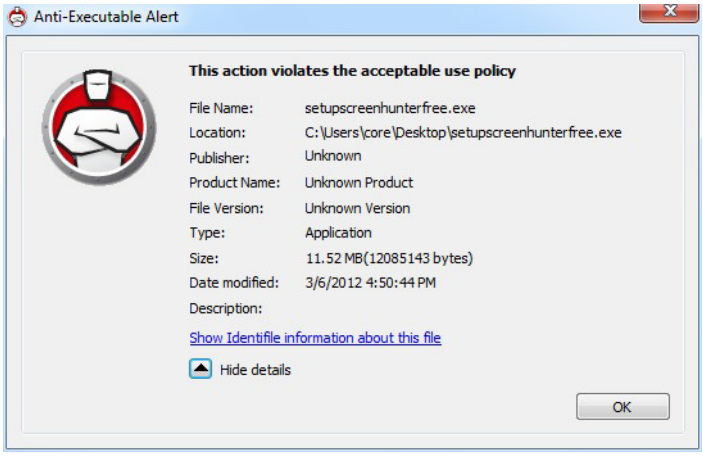
- Execution Control List violation message
- Blocked notification message

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

A sample alert dialog is displayed below:

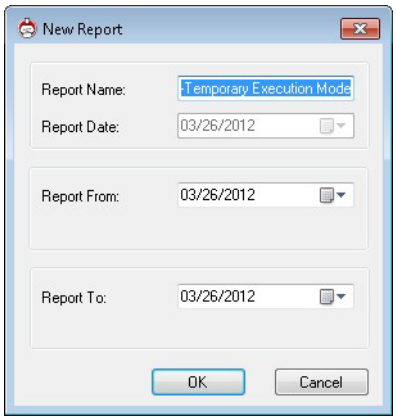


Creating an Anti-Executable Report through Faronics Core Console

Anti-Executable provides the following reports:

- Activity Report – Detailed report for each workstation.
- Temporary Execution Mode Report – Detailed report for all executables launched during Temporary Execution Mode.
- Most Blocked Programs
- Most Violated Machines
- Global Report: Additions to the Central Control List – Files
- Global Report: Additions to the Central Control List – Publishers
- Global Report: Additions to the Local Execution List

To view a report, right-click the workstation(s) and select *Generate Report* > *[Select the Report]*. The following dialog appears:



- Anti-Executable Report displays the following information:
  - > Time Stamp
  - > Machine Info
  - > User Info
  - > Event ID
  - > Description
- Temporary Execution Mode report displays the following information:
  - > Time Stamp
  - > File Name
  - > Hash

Command Line Control

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

Topics

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.

Function	Command
Display Protection Status	`[path]AEC status [/pw=<password>]`
Enable Anti-Executable	`[path]AEC Protect On [/pw=<password>]`
Disable Anit-Executable	`[path]AEC Protect Off [/force] [/pw=<password>]` The switch */force* must be used if Anti-Executable is in Maintenance Mode.
Anti-Executable version	`[path]AEC version /PW=<password>` Note that Command Line Interface does not display the License Key (if it exists), while the User Interface does.
Enable Maintenance Mode	`[path]AEC Maintenance [/duration=<n>] [/lock] /PW=<password>` Using the command without any switch enables Maintenance Mode. Using the switch `/duration=<n>` enables Maintenance Mode for `n` minutes. The `/lock` switch disables the keyboard and mouse. The switch `/lock` must be used with the switch `/duration=<n>`.

Function	Command
Change Anti-Executable password	`[path]AEC changePassword <AEAdmin/AETrustedUser> /NEWPW=<New Password> [/pw=<Password>]` Changing a password, if one exists, requires the old password.
Add a folder or file to local control list as *Allow*	`[path]AEC allow <file or folder name and path> [/pw=<password>]`
Add a folder or file to local control list as *Block*	`[path]AEC block <file or folder name and path> [/pw=<password>]`
Display the current local control list	`[path] AEC displaylcl [/allowed] [/blocked] [/xml] [/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 Protect On [/pw=<password>]`

In the above example, [path] is the path to the Anti-Executable command line interface file (`AEC.exe`).

Uninstalling Anti-Executable

Topics

Uninstalling Anti-Executable on the Workstation via 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 *Anti-Executable* > *Uninstall Anti-Executable*.

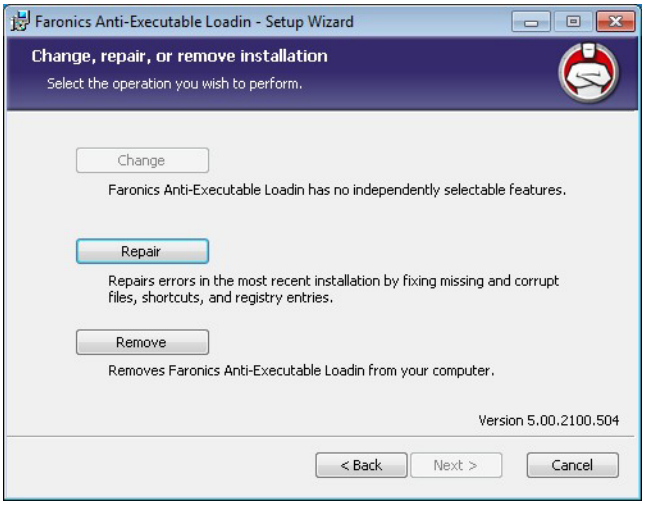
After Anti-Executable has been uninstalled from the selected workstations, Faronics Core Console will reboot them to complete the uninstall process.

Uninstalling Anti-Executable Loadin using (Installer)

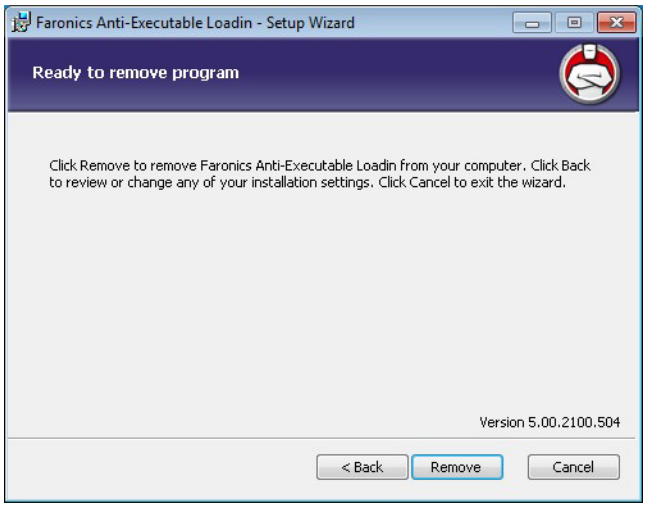
Anti-Executable can be removed by double-clicking on *Anti-Executable_Console_Loadin_Installer.exe*. The Setup Wizard is displayed:

1. Click *Next* to begin the uninstall.

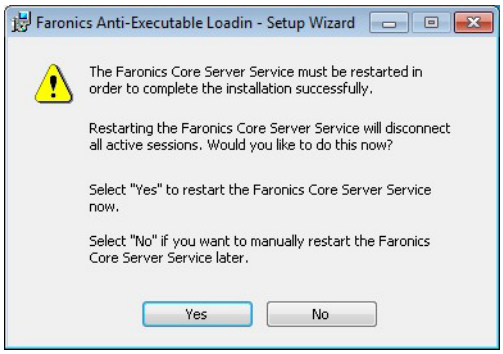
2. Click *Remove* followed by Next.



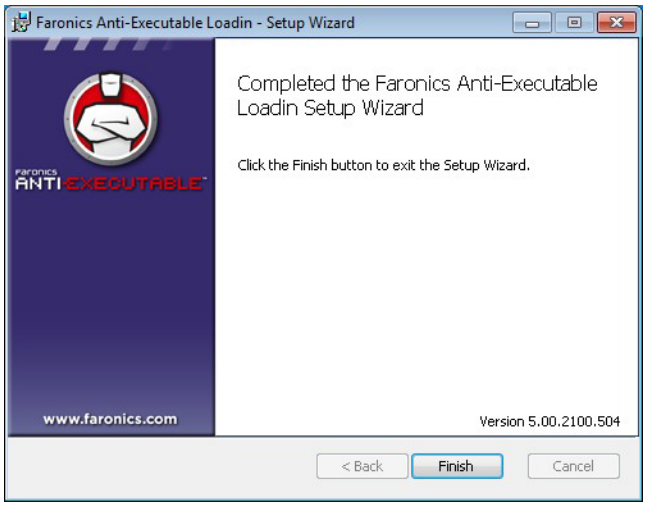
3. Click *Remove*.



4. Click *Yes* to restart the Faronics Core Server Service. Click *No* to restart the Faronics Core Server Service later.



5. Click *Finish*.



Uninstalling Anti-Executable Loadin (Add or Remove Programs)

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.