FARONICS

ANTI-EXECUTABLE™ STANDARD

彻底防御未授权的可执行程序

用户指南

FARONICS™
Intelligent Solutions for ABSOLUTE Control

www.faronics.com

最近修改日期：2010 年 6 月

目录

序言 5

重要信息 6

关于 Faronics 6

产品文档 6

技术支持 7

联系信息 7

术语定义 8

简介 10

Anti-Executable 概述 11

关于 Anti-Executable 11

Anti-Executable 版本 11

关于 Faronics Core 控制台 11

系统要求 12

Anti-Executable 许可证 13

安装 Anti-Executable 15

安装概述 16

安装 Anti-Executable 17

使用 Anti-Executable 21

访问 Anti-Executable 22

使用 Anti-Executable 22

状态选项卡 23

检验产品信息 23

启用 Anti-Executable 保护 24

Anti-Executable 维护模式 24

导出 Anti-Executable 配置 24

导入 Anti-Executable 配置 24

白名单选项卡 25

使用白名单编辑器 26

创建新的白名单 26

激活白名单 30

在白名单编辑器中添加或删除列 30

将发行者或文件 / 文件夹添加到现有的白名单 31

使用白名单编辑器将可执行程序或文件夹添加至现有白名单 32

向活动白名单中添加可执行程序 33

黑名单选项卡 34

使用黑名单编辑器 35

创建新的黑名单 36

激活黑名单 38
在黑名单编辑器中添加或删除列 38
将发行者或文件 / 文件夹添加到现有的黑名单 39
使用黑名单编辑器将可执行程序或文件夹添加至现有黑名单. 41
用户选项卡. 42
添加 Anti-Executable 管理员或受信任的用户 42
删除 Anti-Executable 管理员或受信任的用户 44
启用 Anti-Executable 密码 45
设置选项卡. 46
在 Anti-Executable 中设置事件记录. 46
Anti-Executable 隐蔽功能. 46
Deep Freeze 维护兼容性. 46
自定义警报 47

卸载 Anti-Executable 49

使用安装向导进行卸载. 50

序言

Anti-Executable 可防止未授权可执行程序的运行，从而对计算机提供保护。

主题

重要信息
技术支持
术语定义

重要信息

本部分包含有关 Faronics 产品的重要信息。

关于 **Faronics**

Faronics 致力于提供各种业内领先的解决方案，帮助企业管理、简化复杂的 IT 环境并确保其安全。我们的产品能够完全确保机器的正常工作，并使成千上万的信息技术人员的日常工作得到了重大改善。在以市场为中心的理念推动下，Faronics 取得的技术创新让教育机构、医疗机构、图书馆、政府部门及企业都从中受益。

产品文档

以下文档构成了 Faronics Anti-Executable 文档集：

- *Faronics Anti-Executable* 用户指南 — 此文档将指导您如何使用该产品。
- *Faronics Anti-Executable* 发布声明 — 此文档列出了最新功能、已知问题和已解决的问题。
- *Faronics Anti-Executable readme.txt* — 此文档将指导您完成安装过程。

技术支持

在设计本软件时，我们竭尽所能确保其易于使用并尽量不出问题。如果遇到问题，请与技术支持部联系。

电子邮件：support@faronics.com

电话：800-943-6422 或 604-637-3333

工作时间：星期一至星期五上午 7:00 至下午 5:00（太平洋时间）

联系信息

- 网址：www.faronics.com
- 电子邮件：sales@faronics.com
- 电话：800-943-6422 或 604-637-3333
- 传真：800-943-6488 或 604-637-8188
- 工作时间：星期一至星期五上午 7:00 至下午 5:00（太平洋时间）
- 地址：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

  Faronics Corporation（欧洲）
  Siena Court
  The Broadway Maidenhead
  Berkshire, SL6 1NJ UK

术语定义

术语	定义
警报	通知对话框，出现在试图启动未授权的可执行程序时。Anti-Executable 管理员可以拟定警报中显示的消息和图片。有关详细信息，请参阅导出 *Anti-Executable* 配置。
Anti-Executable 管理员	Anti-Executable 管理员可以访问 Anti-Executable 的所有配置选项。他们可以创建和编辑白名单、黑名单，管理 Anti-Executable 用户，将 Anti-Executable 保护设置为 “ 已启用 ” 或 “ 已禁用 ”，以及卸载 / 升级 Anti-Executable。
Anti-Executable 控制台插件	一个软件库，可扩展 Faronics Core 控制台的功能，从而允许全面控制远程工作站上安装的 Anti-Executable 的配置和操作。
Anti-Executable 受信任的用户	受信任的用户可以访问 “ 状态 ” 选项卡、“ 白名单 ” 选项卡和 “ 黑名单 ” 选项卡。他们可以创建和编辑白名单、黑名单，将 Anti-Executable 保护设置为启用或禁用。受信任的用户无法卸载 / 升级 Anti-Executable。
授权的可执行程序	活动白名单中的可执行程序，可以启动。
黑名单文件夹	一个文件夹及其子文件夹，其中的所有可执行程序均被阻止。
黑名单	可执行程序列表，或包含可执行程序的文件夹，其内容被 Anti-Executable 阻止。
可执行程序	可由操作系统启动的文件。受 Anti-Executable 管理的可执行文件的扩展名为 *.scr*、*.jar*、*.bat*、*.com* 或 *.exe*。
外部用户	既不是 Anti-Executable 管理员，也不是 Anti-Executable 受信任用户的用户。 外部用户只能运行授权的可执行程序，不能控制 Anti-Executable 配置。无论操作系统为外部用户分配了怎样的用户权限，此限制仍然适用。
Faronics Core 代理	工作站上安装的软件，用于启用与 Faronics Core 控制台的通信。
维护模式	在 “ 维护模式 ” 下，新增或修改后的可执行文件将自动添加到活动白名单中。
保护	如果此设置设置为已启用，表示 Anti-Executable 正在根据活动白名单对计算机实施保护。如果设置为 “ 已禁用 ”，则计算机上的任何可执行程序均可启动。
隐蔽模式	“ 隐蔽模式 ” 是一组选项，用于控制 Anti-Executable 在系统上的标示。“ 隐蔽模式 ” 为管理员提供在 Windows 系统任务栏中隐藏 Anti-Executable 图标的选项，阻止显示警报和启动画面屏幕。
受信任的可执行程序	受信任的可执行程序可以启动其它未被授权的可执行程序。

术语	定义
未授权的可执行程序	未授权的可执行程序是指活动白名单中未包含而无法启动的程序。
白名单文件夹	一个文件夹及其子文件夹，其中的所有可执行程序均可启动。
白名单	可执行程序列表，或包含可执行程序的文件夹，允许 Anti-Executable 运行。
工作站	任何使用系统要求中指定的操作系统的客户端或远程计算机。

简介

Anti-Executable 可防止未授权可执行程序的运行，从而对计算机提供保护。

主题

Anti-Executable 概述

系统要求

Anti-Executable 许可证

Anti-Executable 概述

关于 Anti-Executable

Anti-Executable 可防止未授权的可执行程序运行，使 IT 管理员可完全控制计算机。不属于称为“白名单”的文件列表的任何可执行文件不会运行。此白名单处于授权用户的全面控制之下，他们可以对其进行编辑、修改、擦除等操作。

没有什么能通过 Anti-Executable：重命名可执行文件，或从可移动存储设备运行可执行文件，甚或从网络运行可执行文件的企图都将被阻止，从而保护您的计算机，节约您的时间、金钱和精力。

Anti-Executable 版本

Faronics Anti-Executable 有四个不同的可用版本。无论您拥有服务器还是工作站，单独工作还是在网络上工作，Anti-Executable 都将为您提供您所需的保护。选择最符合您需求的 Anti-Executable 版本：

版本	使用 **Anti-Executable** 实施保护
标准版	承载非服务器操作系统的本地计算机
服务器标准版	承载服务器操作系统的本地计算机
企业版	承载非服务器操作系统的远程计算机 *
服务器企业版	承载服务器操作系统的远程计算机 *

* 企业版允许通过称为 Faronics Core 控制台的中央控制台保护多台计算机。

关于 Faronics Core 控制台

Faronics Core 控制台是一种轻量级、高性能、安全、易用的集成式框架，用于管理多个 Faronics 产品。它通过单个控制台提供一致且可靠的方式来显示、管理、安装、更新和保护工作站和服务器，为组织提供了一个全面的管理解决方案来管理 Faronics 产品，从而提升效率。

Anti-Executable 企业版允许您通过 Faronics Core 控制台保护多个工作站。

系统要求

可在下列操作系统中安装 Anti-Executable：

—32 位版本的 Windows XP SP3 及 64 位版本的 Windows XP SP2。

—32 位及 64 位版本的 Windows Server 2003、Windows Server 2008、Windows Vista 及 Windows 7。

Anti-Executable 许可证

Anti-Executable 有正式版和评估版。评估版可从 Faronics 的网站 (www.faronics.com) 免费下载，安装后可完全运行 30 天。评估版过期后不会对计算机实施任何保护，必须卸载或升级为正式版。正式版需要有效的许可证密钥才能保护计算机。

Anti-Executable 管理员可通过 Anti-Executable 的 “ 状态 ” 选项卡获取许可证信息。要从评估版升级为正式版，请输入有效的许可证密钥并单击确定。

服务器版 Anti-Executable 不能安装在非服务器操作系统中。服务器版 Anti-Executable 的许可证密钥不可用于非服务器版。

非服务器版 Anti-Executable 不能安装在服务器操作系统中。非服务器版 Anti-Executable 的许可证密钥不可用于服务器版。

安装 Anti-Executable

本章描述 Anti-Executable 的安装过程。

主题

安装概述

安装 ***Anti-Executable***

安装概述

Anti-Executable 针对 32 位和 64 位版的 Windows Server 2003、Windows Server 2008、Windows XP SP3、Windows Vista 和 Windows 7 提供了不同的安装程序。

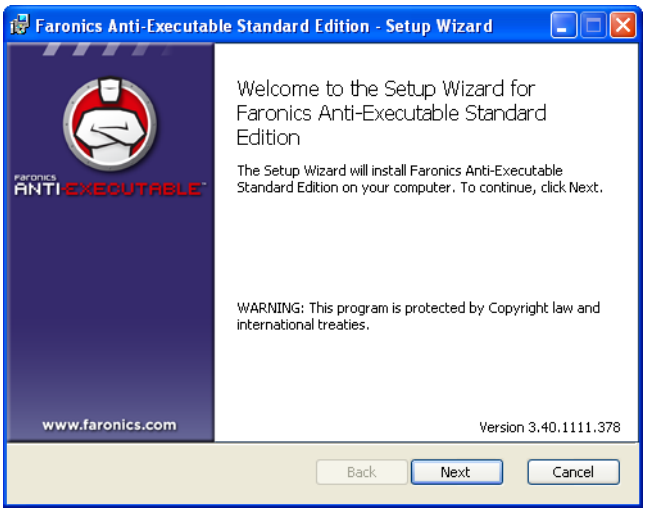
安装前，请检查操作系统版本并根据下表选择安装程序：

系统	安装文件
Windows XP/Vista（32 位）	AEStd_32-bit.msi
Windows XP/Vista（64 位）	AEStd_64-bit.msi
Windows Server 2003 和 Windows Server 2008（32 位）	AESrvStd_32-bit.msi
Windows Server 2003 和 Windows Server 2008（64 位）	AESrvStd_64-bit.msi

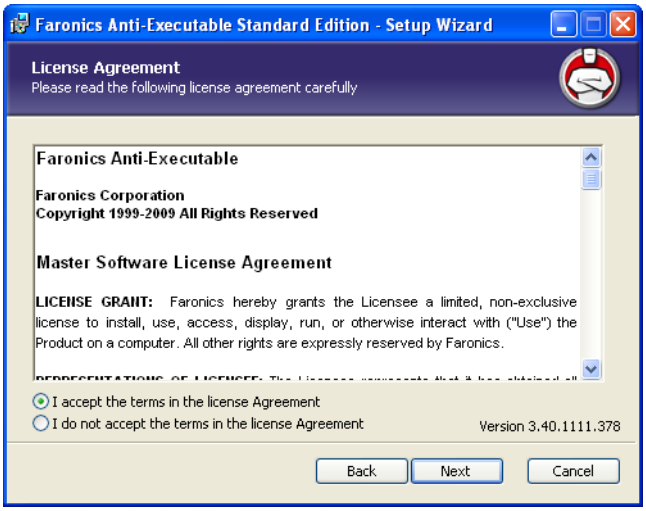
安装 **Anti-Executable**

Anti-Executable 可通过安装向导进行安装。要安装 Anti-Executable，请完成以下步骤：

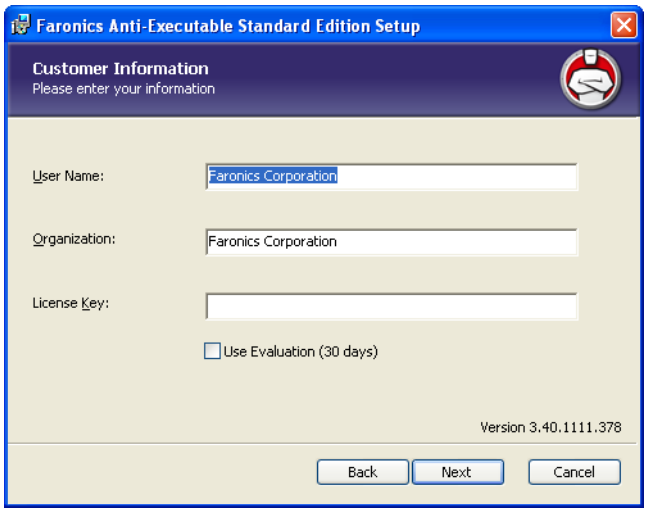
1. 如果已通过 Internet 下载 Anti-Executable，请双击 *AEStd_32-bit_en.msi*（适用于 32 位操作系统）或 *AEStd_64-bit_en.msi*（适用于 64 位操作系统）开始安装过程。单击下一步继续。



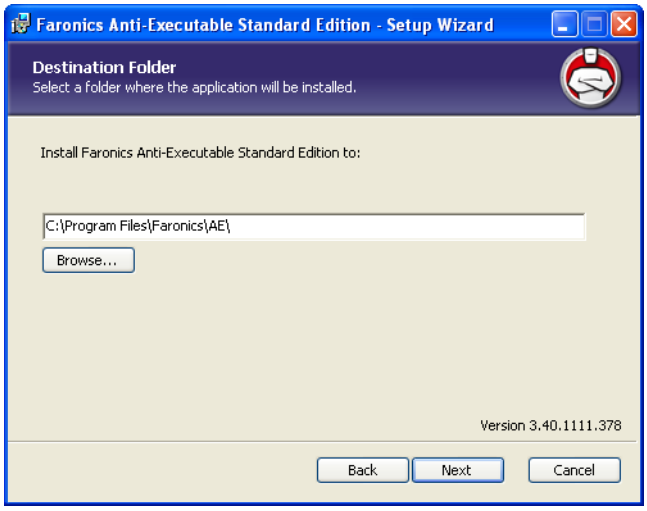
2. 阅读并接受许可协议。单击下一步继续。



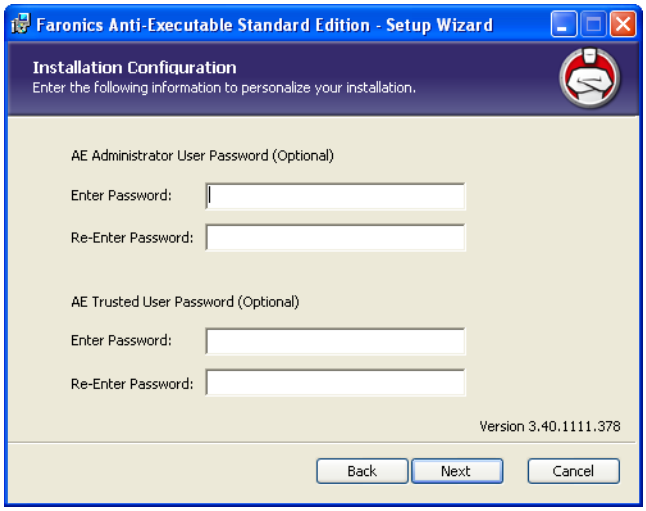
3. 输入用户名和组织。如果选择使用评估版，Anti-Executable 将作为评估版安装，有效期为 30 天。只要输入许可证密钥，评估版可随时转换成正式版。单击下一步继续。



4. 指定安装位置。默认位置为 *C:\Program Files\Faronics\AE*。单击下一步继续。



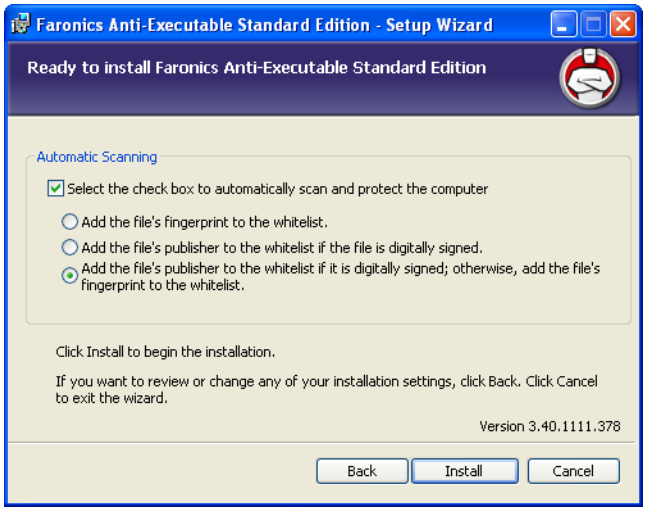
5. 此步骤为可选步骤。指定 Anti-Executable 管理员和受信任用户的密码。安装后，也可以在 Anti-Executable 用户选项卡中设置这些密码。单击下一步继续。



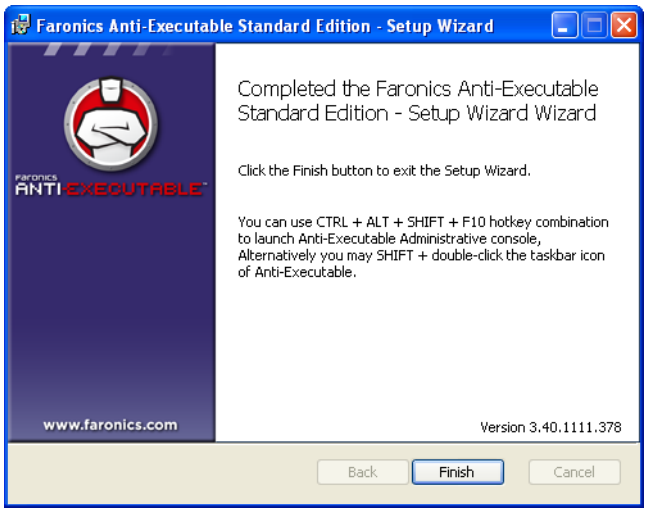
6. 此时将显示自动扫描对话框。如果您希望 Anti-Executable 自动扫描计算机上所有不可移除的驱动器并创建白名单，请选中此复选框。选择以下显示的选项之一：

- 将文件的指纹添加到白名单 – 将文件的唯一标识符添加到白名单。其指纹已加入白名单的所有文件都可以运行。
- 如果文件已有数字签名，则将文件发行者添加到白名单 – 将文件的发行者添加到白名单。所有经白名单中的发行者数字签名的文件都可以运行。
- 如果文件已有数字签名，则将文件发行者添加到白名单。否则，添加文件的指纹 – 如果文件已有数字签名，则添加文件的发行者；如果没有数字签名，则添加文件的指纹。

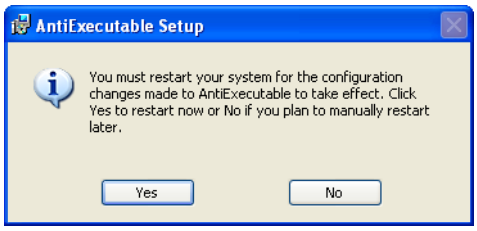
单击安装以安装 Anti-Executable。 Anti-Executable 将会安装，并且白名单激活。



7. 单击完成结束安装。



8. 成功安装后需要重启。单击是立即重启，也可以单击否稍后重启。



建议安装后立即重启。

如果在自动扫描及白名单创建对话框中选中了启用复选框，则会启用保护功能，在计算机重启时将生成活动白名单。

如果在自动扫描及白名单创建对话框中未选中启用复选框，则会禁用保护功能，在计算机重启时不会生成活动白名单。

使用 Anti-Executable

本章描述访问、配置和使用 Anti-Executable 的步骤。

主题

访问 ***Anti-Executable***
状态选项卡
白名单选项卡
向活动白名单中添加可执行程序
黑名单选项卡
用户选项卡
设置选项卡

访问 **Anti-Executable**

Anti-Executable 可通过按住 Shift 键并双击 Windows 系统任务栏中的 Anti-Executable 图标进行访问。如果图标未显示，可使用 *Ctrl* + *Alt* + *Shift* + *F10* 热键序列。

如果您是管理员，将可以访问 “ 状态 ”、“ 白名单 ”、“ 黑名单 ”、“ 用户 ” 和 “ 设置 ” 选项卡。如果您是受信任的用户，将只可以访问 “ 状态 ”、“ 白名单 ”、“ 黑名单 ” 选项卡。

外部用户不允许访问 Anti-Executable。如果设置了密码，Anti-Executable 管理员和受信任的用户必须输入相应的密码才能访问 Anti-Executable。

使用 **Anti-Executable**

安装后，必须对 Anti-Executable 进行配置。Anti-Executable 管理员可访问以下所有选项卡：

- 状态 — 显示安装的 Anti-Executable 的版本，较新版本的 Anti-Executable 是否可用，允许用户导入和导出配置，以及将 Anti-Executable 保护设置为启用、禁用或维护模式。
- 白名单 — 用于创建、编辑和应用白名单。
- 黑名单 — 用于创建、编辑和应用黑名单。
- 用户 — 用于添加管理员、受信任的用户及其密码。
- 设置 — 用于配置 “ 隐蔽模式 ”，管理事件报告、警报消息以及启用 Anti-Executable 与 Deep Freeze 的兼容性。

执行安装的 Windows 管理员用户帐户会成为第一位 Anti-Executable 管理员。

状态选项卡

“状态”选项卡允许 Anti-Executable 管理员和受信任的用户配置各种设置，将保护设置为启用、禁用或维护模式以及导入或导出之前保存的配置。如果您在 Faronics Core 控制台中选择了一个工作站，并选择了配置 *Anti-Executable*，会自动检索工作站配置。

检验产品信息

“关于”窗格显示安装的 Anti-Executable 的版本。如果有新版本可用，系统将显示新版本已可用。单击更新可获取详细信息。

如果安装的是评估版 Anti-Executable，有效至字段将显示 Anti-Executable 到期的日期。Anti-Executable 在 Windows 系统任务栏中显示有关许可证当前状态的通知。

评估版到期后，Anti-Executable 不再对计算机实施保护。Anti-Executable 到期后，系统任务栏中将显示以下到期图标。

要将评估版的 Anti-Executable 转换为正式版，请单击编辑，然后在许可证密钥字段内输入有效的许可证密钥。您可以联系 Faronics 以获取许可证密钥。

启用 **Anti-Executable** 保护

安装后，仅当在安装期间在自动扫描及白名单创建对话框中选择了启用时，默认情况下才会启用 Anti-Executable。否则，Anti-Executable 不能对计算机实施保护。管理员或受信任的用户必须选择启用，白名单保护才生效。

如果 “ 保护 ” 被设置为启用，而活动白名单为空，则只可启动基本的系统可执行程序（如启动、登录）。只有 Anti-Executable 管理员和受信任的用户可以管理白名单。

选中提醒频率复选框，使得工作站上的 Anti Executable 在 “ 保护 ” 被禁用的情况下发出提醒。

Anti-Executable 维护模式

选择维护模式并单击应用可在维护模式下运行 Anti-Executable。在 “ 维护模式 ” 下，新增或修改后的可执行文件将自动添加到活动白名单中。若要退出维护模式，请选择启用或禁用。

如果选择启用，Anti-Executable 将记录所做的更改。如果选择禁用，Anti-Executable 将不会记录所做的更改。

如果计算机以维护模式运行，并禁用了保护功能，则在维护模式期间对工作站进行的更改不会添加到活动白名单中。

在以维护模式运行期间，必须为 Windows 更新提供充足的时间。

导出 **Anti-Executable** 配置

Anti-Executable 管理员可保存多个配置，以应用于其它计算机。如果白名单已被设置为 “ 活动 ”，则也会包含于导出的配置中。

要保存 Anti-Executable 配置文件，请在选择后单击状态选项卡中的导出。配置文件将以专有格式 (*.aecfg*) 进行保存以防止篡改。要打开之前定义的配置文件 (*.aecfg*)，请单击导入并浏览到配置文件。

如果以 XML 格式保存配置，则只允许查看配置的设置。XML 配置文件无法应用于其它计算机。

对 Anti-Executable 设置所做的任何更改将不会生效，直到您单击应用。

导入 **Anti-Executable** 配置

Anti-Executable 管理员和受信任的用户可以单击导入，以导入先前导出的 Anti-Executable 配置。在显示的导入选项对话框中选择一个或多个导入选项。以下选项可选，但即使不选择以下任何选项，导入过程也会成功：

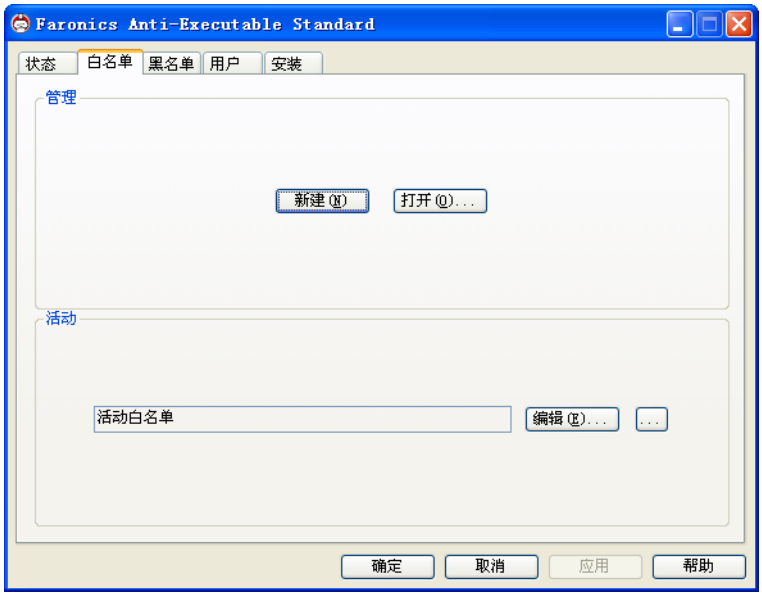
- 导入活动白名单和黑名单
- 导入警报图片
- 导入 Anti-Executable 用户

单击确定并浏览到配置文件 (.aecfg)。

白名单选项卡

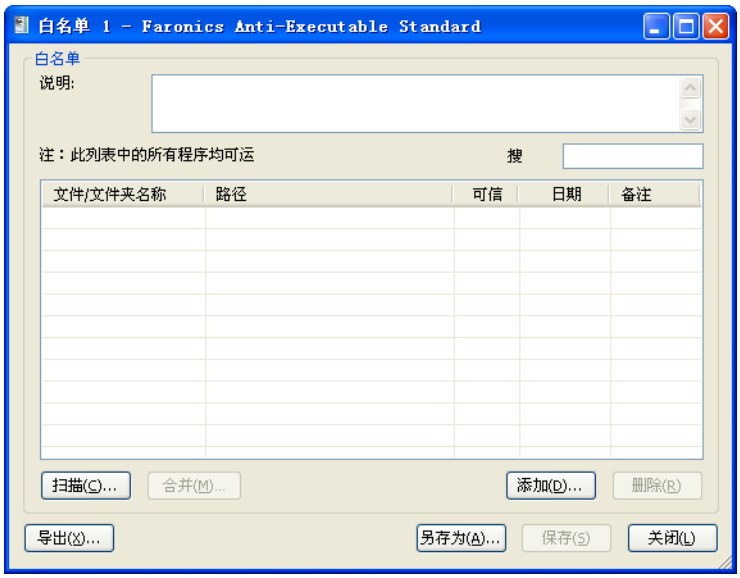
当 “ 保护 ” 设置为启用时，Anti-Executable 允许启动活动白名单中的任何可执行程序。另外，白名单文件夹（文件夹及其子文件夹）中的可执行程序也可启动。

一次只能有一个活动白名单。请参阅标题为创建新的白名单的部分以获取有关创建第一个白名单的信息。



使用白名单编辑器

单击白名单选项卡，选择新建、打开或编辑即可打开 Anti-Executable 的白名单编辑器。如果通过 Windows Explorer 打开一个白名单文件，也会出现白名单编辑器。



- 新建 — 打开白名单编辑器，允许 Anti-Executable 管理员和受信任的用户创建新的白名单。
- 打开 — 打开现有的白名单进行编辑。
- 编辑 — 打开白名单编辑器，将可执行程序和 / 或文件夹添加至活动白名单中，或从白名单中删除可执行程序和 / 或文件夹。

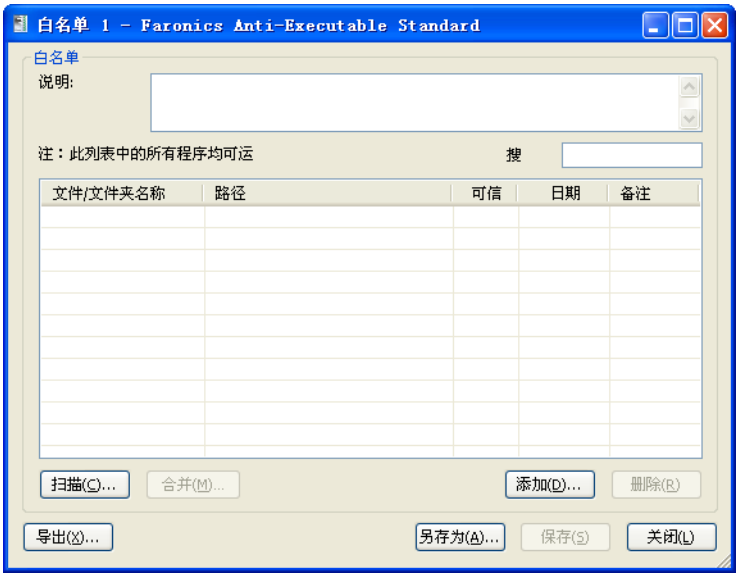
创建新的白名单

只有 Anti-Executable 管理员和受信任的用户可访问白名单编辑器。

建议使用干净的计算机创建白名单。干净的计算机是指为日常操作而安装了操作系统和所有必需应用程序的系统。在将计算机交给用户之前创建白名单可确保白名单仅包含计算机正常运行所需的文件。

要创建新的白名单，请完成以下步骤：

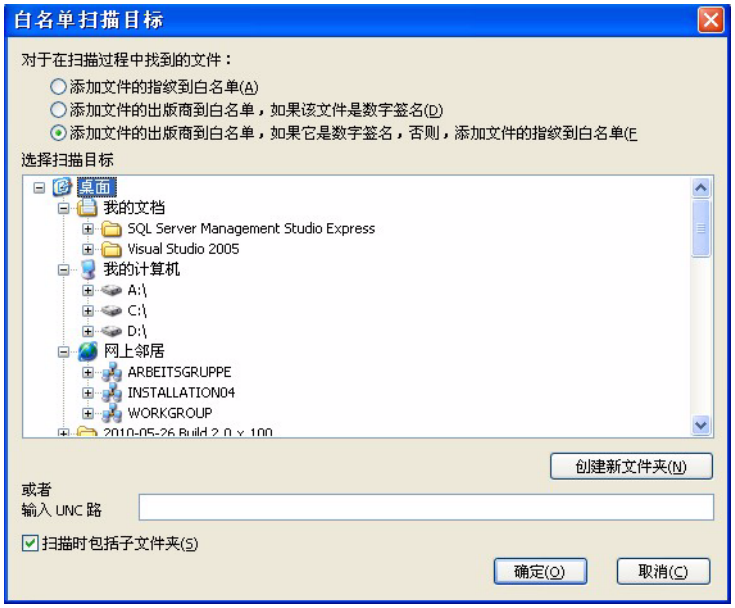
1. 按下 *Shift* 并双击系统任务栏中的 Anti-Executable 图标。或者，您也可以使用 *Ctrl+Alt+Shift+F10* 热键。指定登录 Anti-Executable 的管理员密码。单击白名单选项卡。单击新建。此时将显示白名单编辑器：



2. 要确定可用的应用程序，请单击扫描，然后选择驱动器或目录。
   - 使用 Ctrl + 单击或 Shift + 单击选择多个驱动器或目录以在本地扫描工作站。
   - 单击网上邻居，浏览并选择远程工作站进行远程扫描。
   - 也可以在输入 UNC 路径字段中输入 UNC 路径。

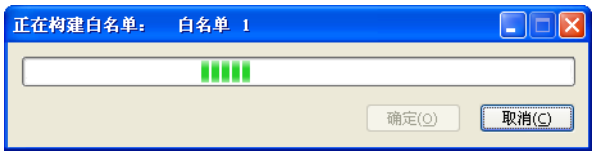
选择以下选项之一：

- 将文件的指纹添加到白名单 – 将文件的唯一标识符添加到白名单。其指纹已加入白名单的所有文件都可以运行。
- 如果文件已有数字签名，则将文件发行者添加到白名单 – 将文件的发行者添加到白名单。所有经白名单中的发行者数字签名的文件都可以运行。
- 如果文件已有数字签名，则将文件发行者添加到白名单。否则，添加文件的指纹 – 如果文件已有数字签名，则添加文件的发行者；如果没有数字签名，则添加文件的指纹。

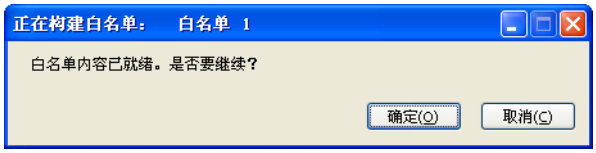


扫描功能会搜索选定位置及其子目录，查找任何可执行文件（包含扩展名为：*.scr*、*.jar*、*.bat*、*.com* 或 *.exe*. 的文件）。扫描时间取决于位置的存储容量和其中包含的可执行程序数量。

3. 单击确定。此时将出现正在构建白名单：对话框，其中显示进程：

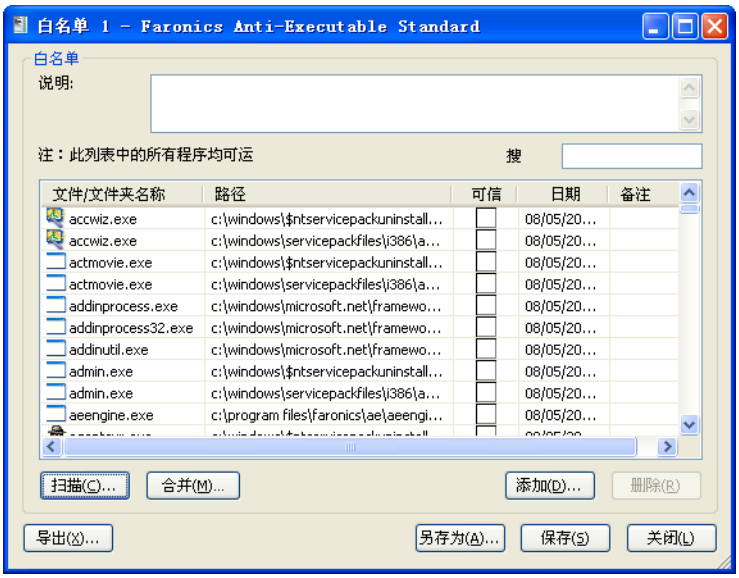


4. 完成扫描后，Anti-Executable 将确认您是否要继续。单击确定。



5. 此时将出现填写完好的白名单。可逐个添加文件夹和可执行程序，方法是单击添加并选择要添加至新的白名单中的文件夹或可执行程序。如果添加的是文件夹，则文件夹及其子文件夹中的可执行程序均允许启动。
   - 要删除文件夹或可执行程序，请将其选定并单击删除。此操作不会从系统中删除文件夹或可执行程序。
   - 要将文件夹或可执行程序与现有白名单相合并，请单击合并。此时将出现打开对话框。选择现有白名单并单击打开。现有的白名单内容将与扫描到的文件或可执行程序列表合并。单击保存以同名保存白名单。单击另存为使用其它名称保存合并后的白名单。
   - 要搜索特定文件夹或可执行程序，请在搜索字段中输入文件夹名称或可执行程序名称中的一个或多个字符。系统将根据输入的字符筛选出列表。

   若要按添加日期排列可执行程序，请单击日期列的标题。



6. 单击可信列可定义应用程序是否可信。选中此复选框表示应用程序受信任，可启动其它未授权的可执行程序。
7. 单击“备注”列填入对任何应用程序的所有注释。此时会出现文本提示，允许您输入其他信息。您还可以在白名单编辑器顶部的空格中添加对整个列表的说明。
8. 单击保存以保存白名单。单击另存为以其它名称保存。白名单将以专有格式保存，扩展名为 *.aewl*。单击导出以将白名单导出为 XML 或 CSV 格式。XML 或 CSV 格式的白名单可通过 Windows Explorer 打开和编辑但不能设置为活动白名单。

有关可执行程序的详细信息，右键单击可执行程序并选择 *Google* 搜索。将启动默认浏览器，并在 www.google.com 上搜索可执行程序的名称。

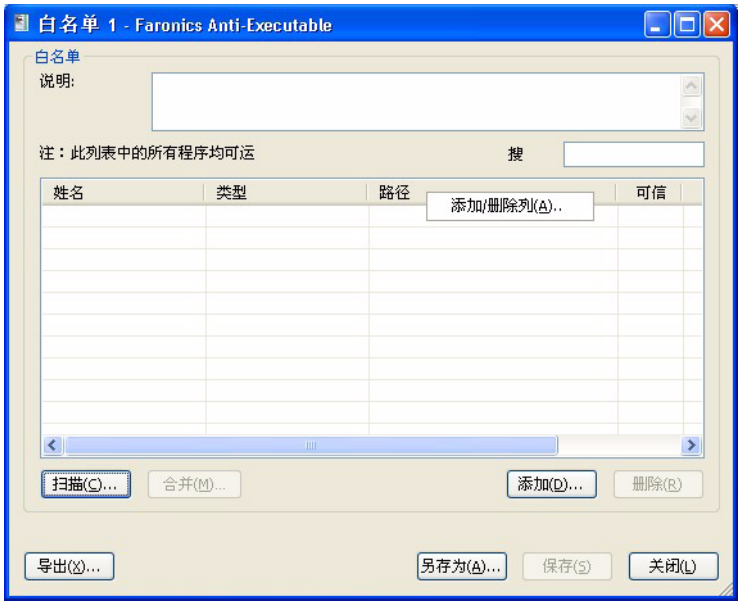
激活白名单

创建白名单后，单击白名单选项卡中活动白名单部分的浏览按钮可将其设置为活动白名单。浏览按钮可启动打开对话框。浏览至白名单并单击打开。

在白名单编辑器中添加或删除列

要添加或删除列，完成以下步骤：

1. 打开白名单编辑器。
2. 右键单击列标题并选择添加 / 删除列。



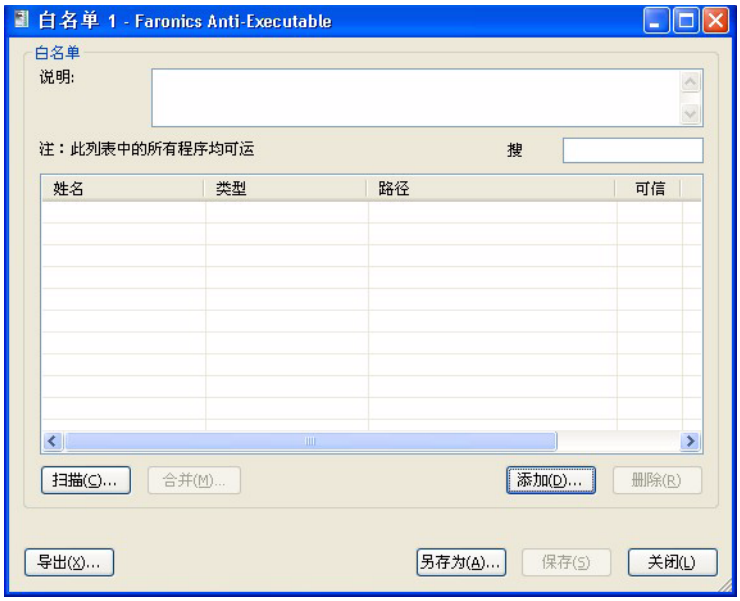
3.选择要添加的列。清除要删除的列的对应复选框。也可以单击上移或下移更改列的位置。以下列无法删除：名称、类型、路径、日期和备注。

4. 单击确定。

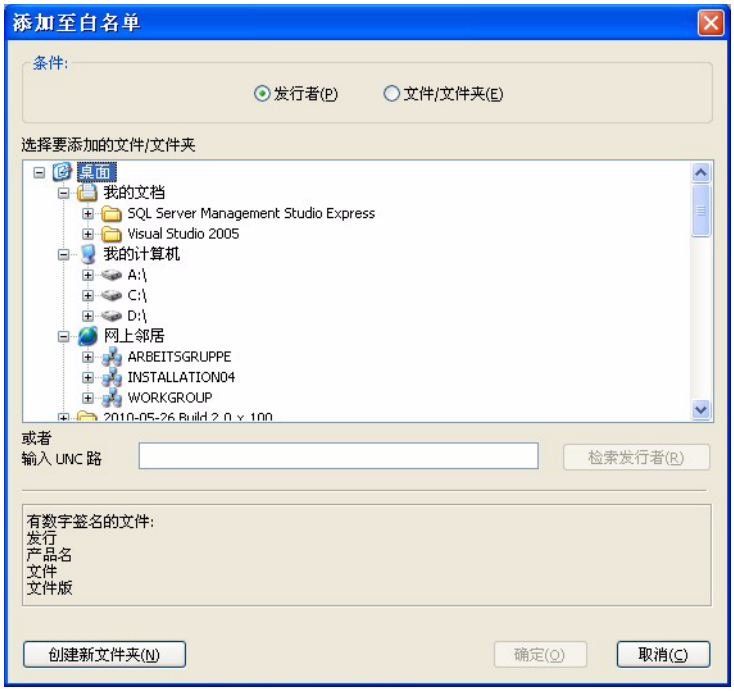
将发行者或文件 / 文件夹添加到现有的白名单

要添加或删除列，完成以下步骤：

1. 打开白名单编辑器。
2. 单击添加。



3. 此时将显示 " 添加到白名单 " 对话框。选择发行者或文件 / 文件夹。如果已选择发行者，浏览以选择要添加其发行者的文件。如果文件有数字签名，则显示发行者名称。或者，如果已选择文件 / 文件夹，请浏览以选择文件或文件夹。也可以在输入 UNC 路径字段中输入 UNC 路径。



4. 单击 “ 确定 ”。发行者或文件 / 文件夹即添加到白名单。

使用白名单编辑器将可执行程序或文件夹添加至现有白名单

除了填写新的白名单，扫描功能还允许将可执行程序从特定位置添加到现有白名单。此位置可以是本地、外部或网络位置。

- 单击扫描以启动白名单扫描目标对话框。这将搜索所有可执行程序的选定位置。完成扫描后，扫描结果可合并到白名单中。
- 单击添加可添加单个文件夹和可执行程序。
- 要打开之前创建的白名单，请单击打开并浏览到白名单文件。使用添加、删除、扫描或合并按钮进行任何必需的更改。这些按钮可在白名单中添加和删除可执行程序及文件夹。它们不会修改计算机上的实际文件或文件夹。
- 单击 “ 仅限白名单 ” 按钮可删除黑名单中的可执行程序并确保它们只出现于白名单中。
- 您可以同时打开和编辑多个白名单。一次仅可将一个白名单设置为活动白名单。

向活动白名单中添加可执行程序

可执行程序启动后，可添加到活动白名单中。如果机器处于被保护状态，此时启动未授权的可执行程序，Anti-Executable 管理员或受信任的用户会被提示选择允许、拒绝或允许并添加至白名单。

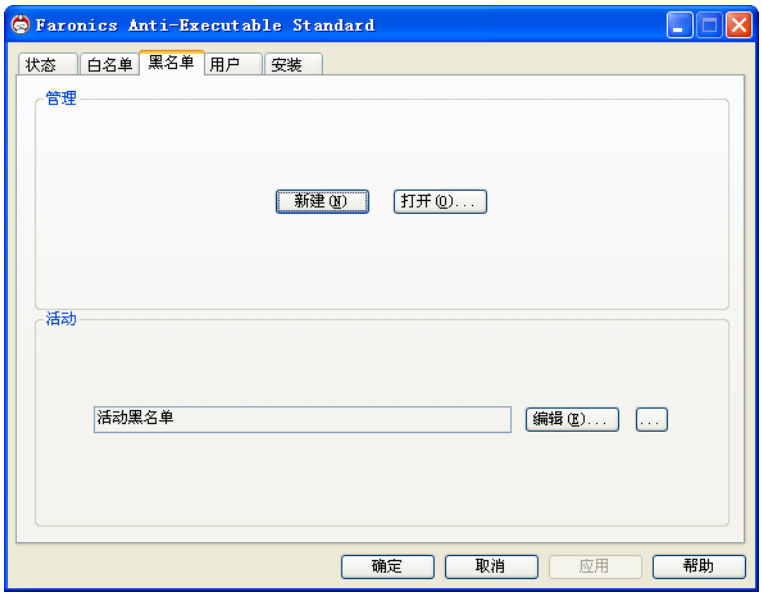
- 允许 — 允许启动可执行程序，但不将其添加至活动白名单。下次启动可执行程序时，将再次被阻止。
- 拒绝 — 可执行程序不会添加至活动白名单，且仍未被授权。因而不允许启动。
- 允许并添加至白名单 — 允许启动可执行程序。该程序还将被添加至活动白名单中，从而成为授权可执行程序。

外部用户没有必需的权限选择允许、拒绝或允许并添加至白名单。外部用户尝试启动活动白名单中未包含的可执行程序时，会收到该程序被阻止的通知。有关详细信息，请参阅自定义警报上的部分。

黑名单选项卡

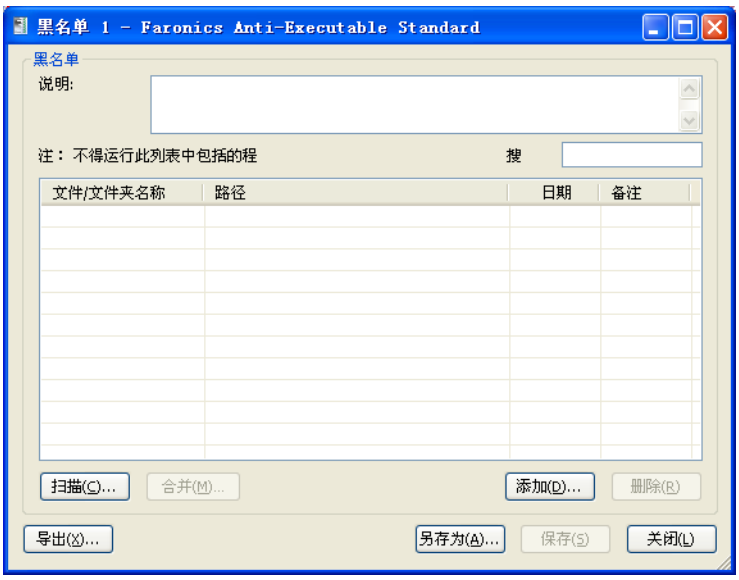
当“保护”设置为启用时，Anti-Executable 允许阻止活动黑名单中的任何可执行程序。另外，黑名单文件夹（文件夹及其子文件夹）中的所有可执行程序也被阻止。

一次只能有一个活动黑名单。请参阅标题为创建新的黑名单的部分以获取有关创建第一个黑名单的信息。



使用黑名单编辑器

单击黑名单选项卡，选择新建、打开或编辑即可打开 Anti-Executable 的黑名单编辑器。如果通过 Windows Explorer 打开一个黑名单文件，也会出现黑名单编辑器。



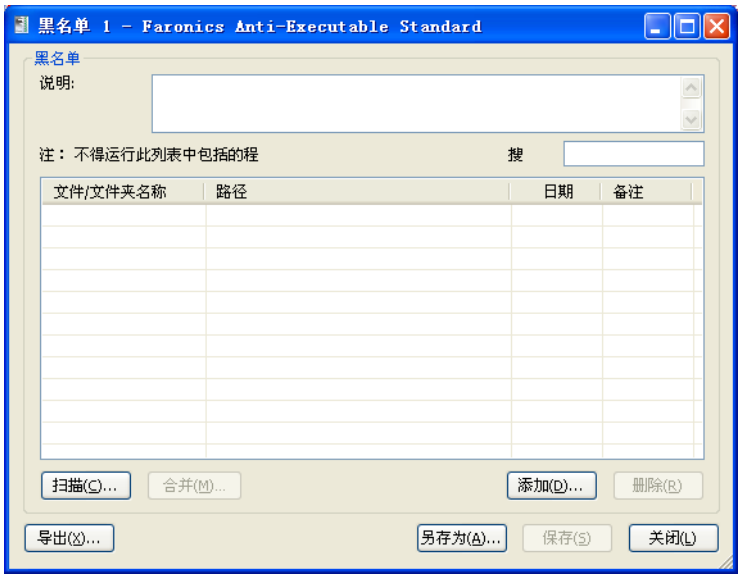
- 新建 — 打开黑名单编辑器，允许 Anti-Executable 管理员和受信任的用户创建新的黑名单。
- 打开 — 打开现有的黑名单进行编辑。
- 编辑 — 打开黑名单编辑器，将可执行程序和 / 或文件夹添加至活动黑名单中，或从黑名单中删除可执行程序和 / 或文件夹。

创建新的黑名单

只有 Anti-Executable 管理员和受信任的用户可访问黑名单编辑器。

要创建新的黑名单，请完成以下步骤：

1. 按下 *Shift* 并双击系统任务栏中的 Anti-Executable 图标。或者，您也可以使用 *Ctrl+Alt+Shift+F10* 热键。指定登录 Anti-Executable 的管理员密码。单击黑名单选项卡。单击新建。此时将显示黑名单编辑器：



2. 要确定可用的应用程序，请单击扫描，然后选择驱动器或目录。使用 *Ctrl* + 单击或 *Shift* + 单击选择多个驱动器或目录。或者，单击网上邻居，浏览并选择远程工作站。单击确定。

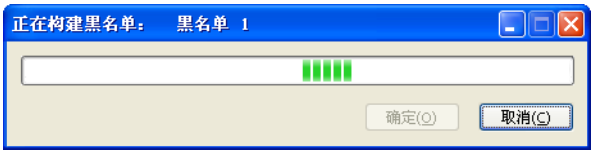
• 选择以下选项之一：

— 将文件的指纹添加到黑名单 – 将文件的唯一标识符添加到黑名单。其指纹已加入黑名单的所有文件都不可以运行。

— 如果文件已有数字签名，则将文件发行者添加到黑名单 – 将文件的发行者添加到黑名单。所有经黑名单中的发行者数字签名的文件都不可以运行。

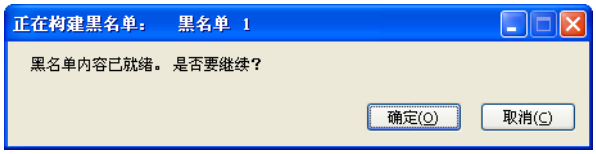
— 如果文件已有数字签名，则将文件发行者添加到黑名单。否则，添加文件的指纹 – 如果文件已有数字签名，则添加文件的发行者；如果没有数字签名，则添加文件的指纹。

此时将出现正在构建黑名单：对话框，其中显示进程：



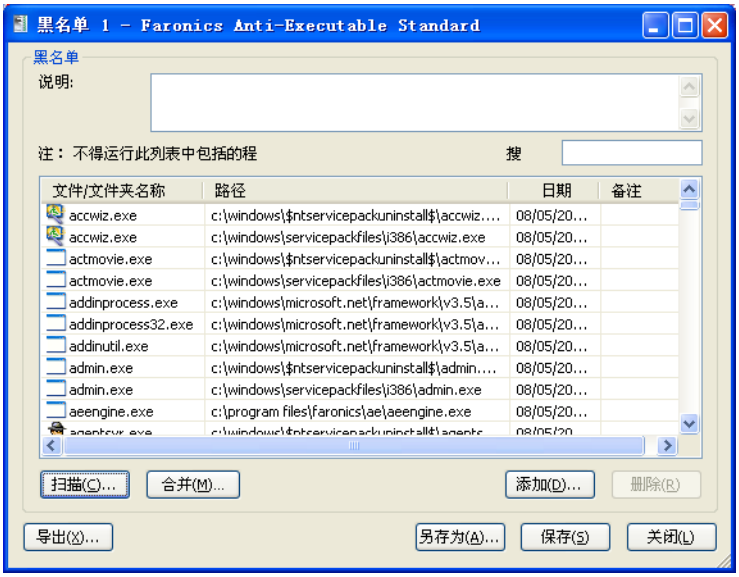
扫描功能会搜索选定位置及其子目录，查找任何可执行文件（包含扩展名为：*.scr*、*.jar*、*.bat*、*.com* 或 *.exe*. 的文件）。扫描时间取决于位置的存储容量和其中包含的可执行程序数量。

3. 扫描完成后，Anti-Executable 会提示您将结果合并到新的黑名单中。单击确定。



4. 此时将出现填写完好的黑名单。可逐个添加文件夹和可执行程序，方法是单击添加并选择要添加至新的黑名单中的文件夹或可执行程序。如果添加的是文件夹，则文件夹及其子文件夹中的可执行程序均被阻止。
   - 要删除文件夹或可执行程序，请将其选定并单击删除。此操作不会从系统中删除文件夹或可执行程序。
   - 要将文件夹或可执行程序与现有黑名单相合并，请单击合并。此时将出现打开对话框。选择现有黑名单并单击打开。现有的黑名单内容将与扫描到的文件或可执行程序列表合并。单击保存以同名保存黑名单。单击另存为使用其它名称保存合并后的黑名单。
   - 要搜索特定文件夹或可执行程序，请在搜索字段中输入文件夹名称或可执行程序名称中的一个或多个字符。系统将根据输入的字符筛选出列表。

   若要按添加日期排列可执行程序，请单击日期列的标题。



5. 单击备注列填入对任何应用程序的所有注释。此时会出现文本提示，允许您输入其他信息。您还可以在黑名单编辑器顶部的空格中添加对整个列表的说明。
6. 单击保存以保存黑名单。单击另存为以其它名称保存。黑名单将以专有格式保存，扩展名为 *.aebl*。单击导出以将黑名单导出为 XML 或 CSV 格式。XML 或 CSV 格式的黑名单可通过 Windows Explorer 打开和编辑但不能设置为活动黑名单。

有关可执行程序的详细信息，右键单击可执行程序并选择 *Google* 搜索。将启动默认浏览器，并在 www.google.com 上搜索可执行程序的名称。

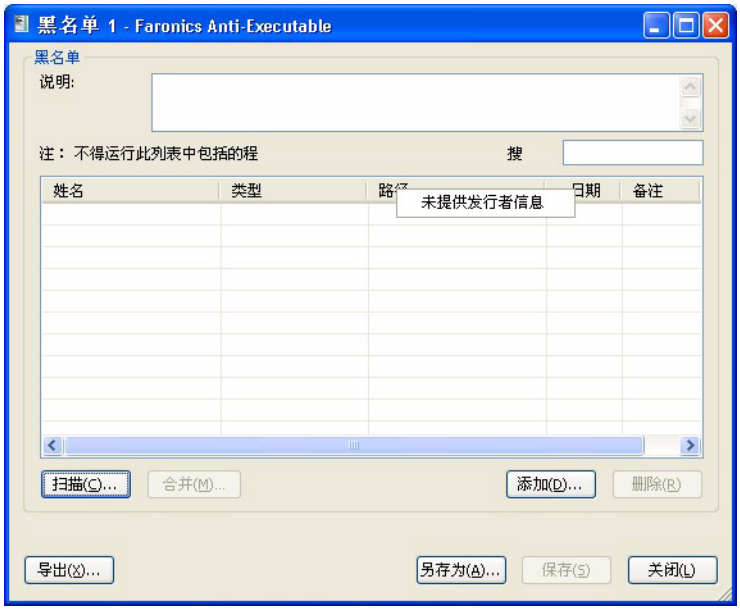
激活黑名单

创建黑名单后，单击黑名单选项卡中活动黑名单部分的浏览按钮可将其设置为活动黑名单。浏览按钮可启动打开对话框。浏览至黑名单并单击打开。

在黑名单编辑器中添加或删除列

要添加或删除列，完成以下步骤：

1. 打开黑名单编辑器。
2. 右键单击列标题并选择添加 / 删除列。



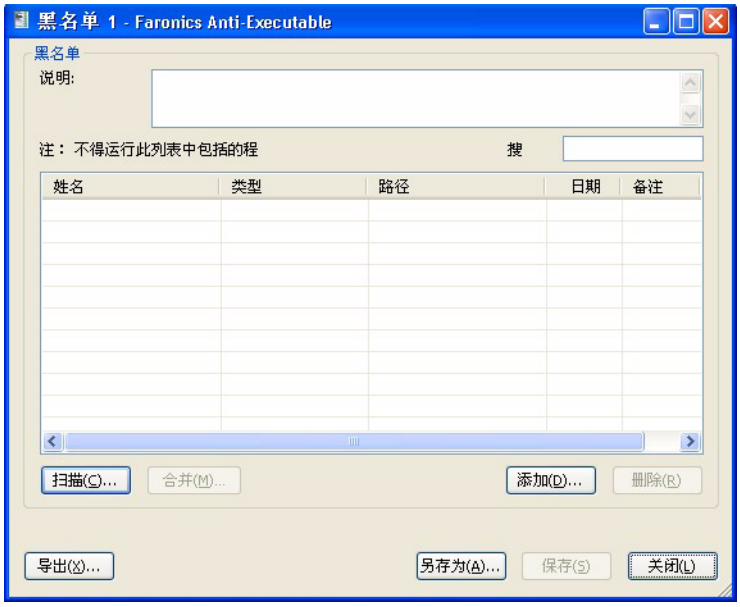
3. 选择要添加的列。清除要删除的列的对应复选框。也可以单击上移或下移更改列的位置。以下列无法删除：名称、类型、路径、日期和备注。

4. 单击确定。

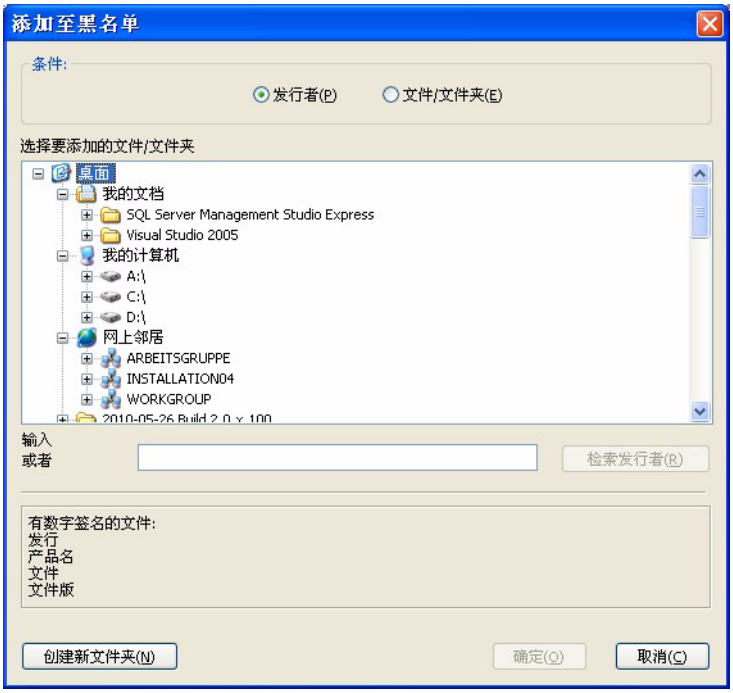
将发行者或文件 / 文件夹添加到现有的黑名单

要添加或删除列，完成以下步骤：

1. 打开黑名单编辑器。
2. 单击添加。



3. 此时将显示 “ 添加到黑名单 ” 对话框。选择发行者或文件 / 文件夹。如果已选择发行者，浏览以选择要添加其发行者的文件。如果文件有数字签名，则显示发行者名称。或者，如果已选择文件 / 文件夹，请浏览以选择文件或文件夹。也可以在输入 UNC 路径字段中输入 UNC 路径。



4. 单击确定。发行者或文件 / 文件夹即添加到黑名单。

使用黑名单编辑器将可执行程序或文件夹添加至现有黑名单

除了填写新的黑名单，扫描功能还允许将可执行程序从特定位置添加到现有黑名单。此位置可以是本地、外部或网络位置。

- 单击扫描以启动黑名单扫描目标对话框。这将搜索所有可执行程序的选定位置。完成扫描后，扫描结果可合并到黑名单中。
- 单击添加可添加单个文件夹和可执行程序。
- 要打开之前创建的黑名单，请单击打开并浏览到黑名单文件。使用添加、删除、扫描或合并按钮进行任何必需的更改。这些按钮可在黑名单中添加和删除可执行程序及文件夹。它们不会修改计算机上的实际文件或文件夹。
- 单击仅限黑名单按钮可删除白名单中的可执行程序并确保它们只是黑名单中的一部分。
- 可同时打开和编辑多个黑名单。一次仅可将一个黑名单设置为活动黑名单。

用户选项卡

Anti-Executable 使用 Windows 用户帐户来确定用户可用的功能。Anti-Executable 用户分为两种类型：

- 管理员用户 — 可以管理白名单、黑名单、用户和设置，还可以卸载 Anti-Executable。
- 受信任的用户 — 可以创建、配置和设置活动白名单或活动黑名单。它们不能卸载 Anti-Executable，也不能管理用户或设置。

默认情况下，执行 Anti-Executable 安装的 Windows 用户帐户是第一位 Anti-Executable 管理员用户。然后这位管理员用户就可以向 Anti-Executable 中添加现有的 Windows 用户。

Anti-Executable 未列出的用户均被视为外部用户，这些用户受到活动白名单内容中指定的可执行程序启动限制。

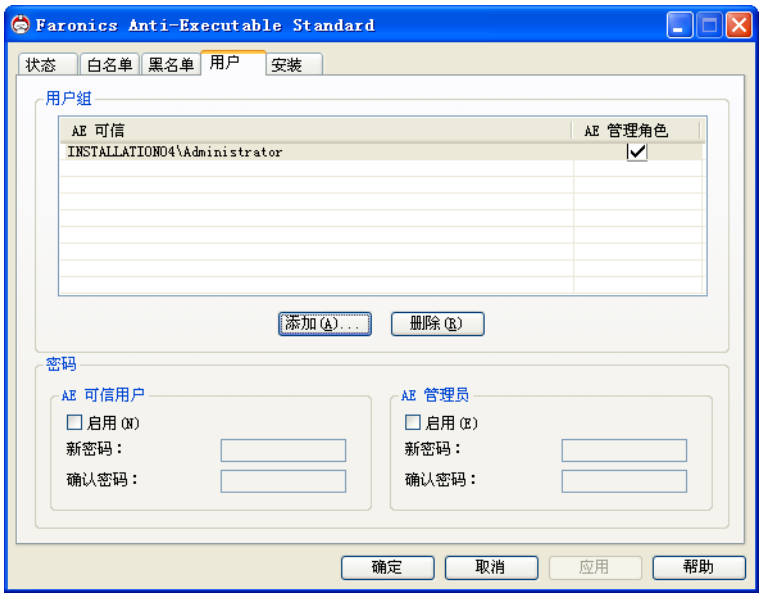
如果 Anti-Executable 管理员或受信任的用户在启用了 Anti-Executable 的情况下尝试打开未授权的应用程序，他们会看到一个对话框，提示选择允许、拒绝或允许并添加至白名单。

添加 **Anti-Executable** 管理员或受信任的用户

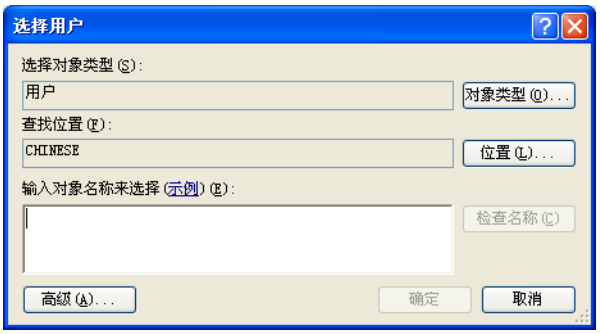
所有 Anti-Executable 用户均为现有 Windows 用户帐户。但是，所有 Windows 用户帐户不会自动成为管理员或受信任的用户。不是管理员或受信任用户的 Windows 用户帐户为外部用户。

要将用户添加至 Anti-Executable，请执行以下步骤：

1. 单击 Anti-Executable 窗口顶部的用户选项卡。

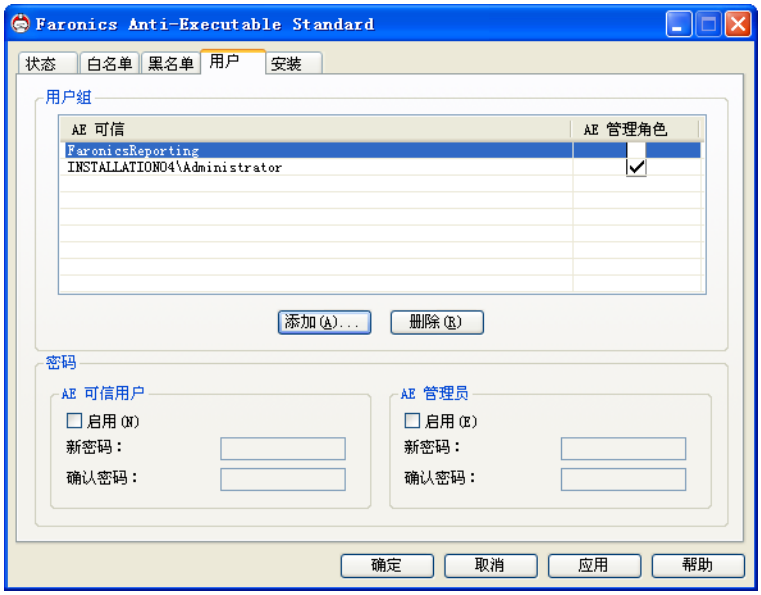


2. 单击添加以添加新用户。从提供的列表中选择“ 用户 ”图标。



3. 如果列表为空，请单击高级> 立即查找以显示可用用户列表。当前登录的域管理员可添加其他域用户。单击用户名以将其添加至 Anti-Executable 的列表中，然后单击确定。

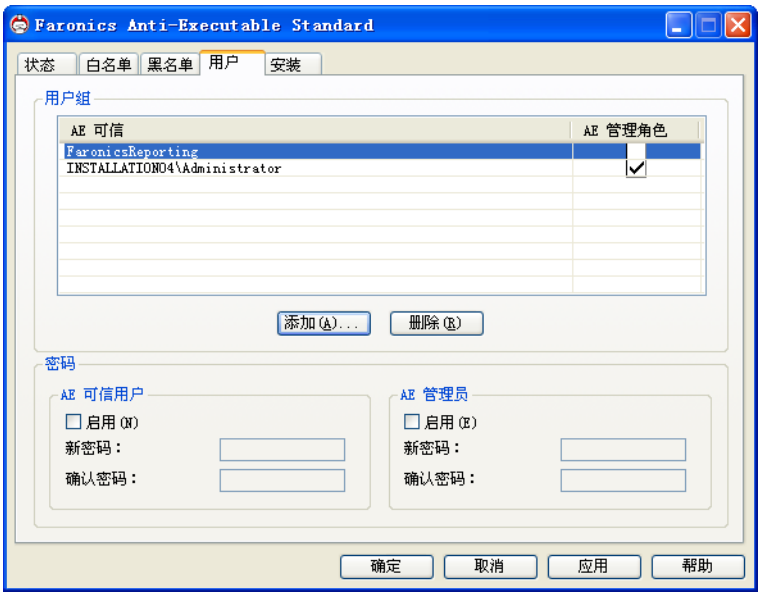
4. 默认情况下，每个被添加的用户均为 Anti-Executable 受信任的用户。如果要赋予新用户管理权限，请选中 *Anti-Executable* 管理角色复选框，以将其指定为 Anti-Executable 管理员。



5. 完成后单击应用。

删除 **Anti-Executable** 管理员或受信任的用户

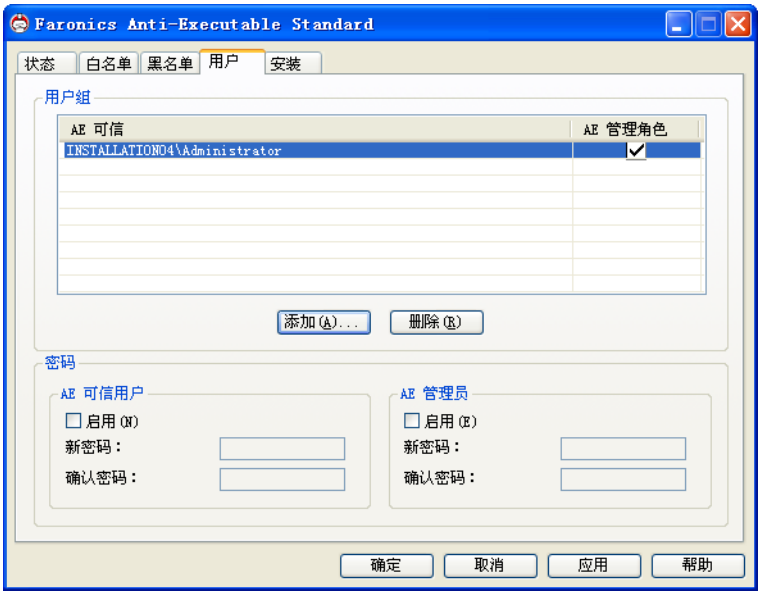
单击用户选项卡并选择要删除的用户。单击删除。此操作不会删除用户的 Windows 用户帐户；用户会立即变为外部用户。



启用 **Anti-Executable** 密码

Anti-Executable 可以为每个用户组附加一个密码，作为一项额外的保护措施。密码只能应用于相关组的成员。

要指定密码，请确保选中启用复选框。在新密码和确认密码字段中输入密码。单击应用以保存更改。



设置选项卡

Anti-Executable 管理员可设置 “ 事件报告 ” 以记录用户的各种操作，应用 “ 隐蔽模式 ” 的各种设置，设置 “ 警报 ” 以及启用 “Deep Freeze 兼容性 ”。

在 **Anti-Executable** 中设置事件记录

选择记录到文件以将事件记录到事件查看器。日志文件保存在工作站的 S:/AEE/AE.log 目录下。

Anti-Executable 隐蔽功能

“ 隐蔽模式 ” 是一组选项，用于控制 Anti-Executable 在系统上的标示。“ 隐蔽模式 ” 为管理员提供在 Windows 系统任务栏中隐藏 Anti-Executable 图标的选项，阻止显示警报和启动画面屏幕。

当 Anti-Executable 在系统任务栏中不可见时，管理员和受信任的用户可通过 *Ctrl* + *Alt* + *Shift* + *F10* 热键启动 *Anti-Executable*。

隐蔽功能具有以下选项：

- 隐藏通知 — 阻止显示警报。
- 隐藏系统任务栏中的图标 — 隐藏系统任务栏中的 Anti-Executable 图标。
- 禁用启动画面窗口 — 禁用启动 Anti-Executable 前显示的 Anti-Executable 启动画面窗口。

Deep Freeze 维护兼容性

此功能仅当在计算机上安装 Faronics Deep Freeze 和 Faronics Anti-Executable 时才适用。

“Deep Freeze 维护模式兼容性 ” 功能允许管理员同步 Deep Freeze 和 Anti-Executable 的维护模式。

通过启用启用 *Deep Freeze* 维护模式兼容性复选框，当 Deep Freeze 进入维护模式时，Anti-Executable 将自动进入维护模式。

通过同时将 Deep-Freeze 和 Anti-Executable 设置为维护模式，添加至计算机的任何可执行程序不仅将被添加至活动白名单，而且将被 Deep Freeze 在维护模式结束后重新冻结计算机后保留。

Anti-Executable 将保持维护模式，直到 Deep Freeze 维护模式结束前不久。一旦 Anti-Executable 退出维护模式，系统即会将任何新的可执行文件或更新的可执行文件添加至活动白名单。当 Deep Freeze 退出维护模式时，系统将冻结更新的白名单并重启计算机。

如果启用了 “Deep Freeze 维护模式兼容性 ” 并且 Deep Freeze 处于 “ 冻结 ” 状态，则无法将 Anti-Executable 设为维护模式。

如果 Anti-Executable 被禁用，而 Deep Freeze 进入维护模式，Anti-Executable 将继续处于禁用状态。

由 Deep Freeze 触发的维护期将优先于 Anti-Executable 上计划的任何其它维护期。

有关 Deep Freeze 的详细信息，请访问 http://www.faronics.com/deepfreeze。

自定义警报

Anti-Executable 管理员可以使用 “ 警报 ” 窗格拟定警报消息和图片，这些内容将在用户尝试运行未授权的可执行程序时出现。可设置以下消息：

- 白名单违规消息 — 当白名单违规时显示。
- 黑名单违规消息 — 当黑名单违规时显示。

输入一条消息或使用提供的默认消息。此文本将在用户尝试运行未授权的可执行程序时在所有警报对话框中显示。单击更改并浏览以选择位图图片文件。选定图片将与文本一起显示在警报对话框中。警报消息将显示以下信息：

- 可执行程序位置
- 可执行程序名称
- 默认或自定义的图片
- 默认或自定义的消息

卸载 Anti-Executable

本章说明卸载 Anti-Executable 的步骤。

主题

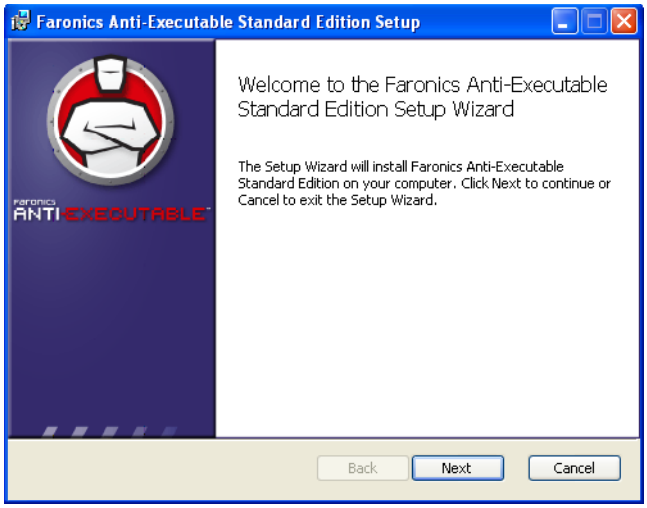
使用安装向导进行卸载

使用安装向导进行卸载

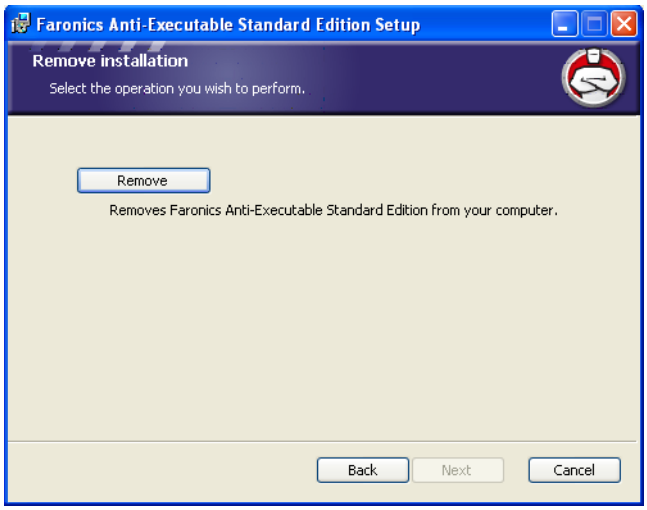
Anti-Executable 仅可由具有 Anti-Executable 管理员权限的登录用户卸载，卸载时的 Anti-Executable 的 “ 保护 ” 必须设置为禁用。

完成以下步骤以删除 Anti-Executable：

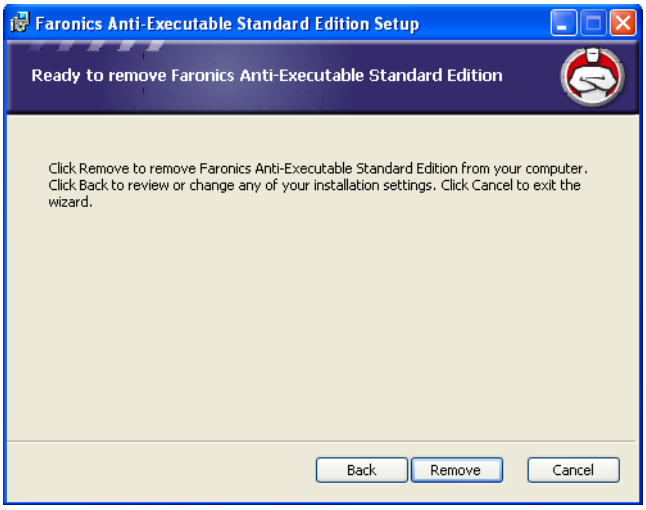
1. 双击用于安装 Anti-Executable 的 *.msi* 文件。此时将显示安装向导。



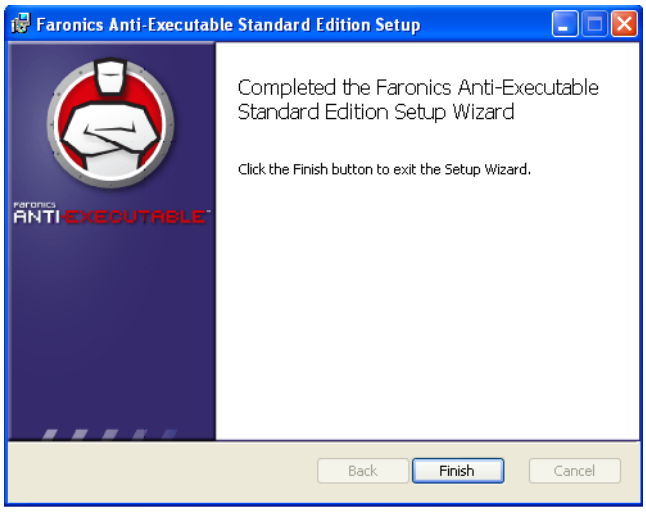
2. 单击删除，然后单击下一步。



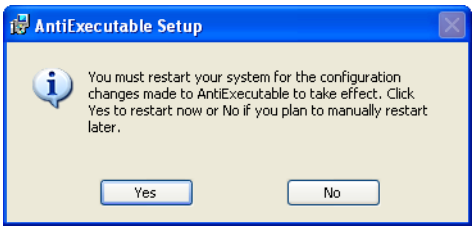
3. 单击删除。



4. 单击完成结束卸载。



5. 成功卸载后，需要重启。单击是立即重启，也可以单击否稍后重启。



建议卸载后立即重启。