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：2023 年 1 月

内容

序言

Faronics Anti-Executable 是通过仅允许被批准的可执行程序在工作站或服务器上运行，来确保终端安全性的解决方案。

主题

重要信息

本部分包含有关 Anti-Executable 的重要信息。

关于 Faronics

Faronics 致力于提供软件来帮助企业管理、简化多用户计算环境并确保其安全。我们的产品能够完全确保工作站的正常工作，并将 IT 人员从繁琐的技术支持和软件问题中解放出来。在以客户为中心的精神推动下，Faronics 取得的技术创新能够让教育机构、医疗机构、图书馆、政府部门以及企业获益。

产品文档

Faronics Anti-Executable 技术文档集包括以下文档：

- 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 功能历史记录 – 此文档列出了新增功能。
- Faronics Anti-Executable readme.txt – 此文档可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。

网址：support.faronics.com

电子邮件：support@faronics.com

免费电话（北美）：1-800-943-6422

本地电话：1-604-637-3333

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

总部：

Faronics Corporation
609 Granville St., Suite 1400
Vancouver, BC V7Y 1G5, Canada

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）

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

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 管理员可以指定警报中显示的消息和图片。
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 受信任的用户	他们可以将 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。
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。在 " 设置 " 选项卡中配置之后，扩展名为 .dll 的动态链接库文件也可受 Anti-Executable 管理。
执行控制列表	执行控制列表定义 Anti-Executable 必须如何管理文件或发行者。执行控制列表定义必须 " 允许 " 还是 " 阻止 " 文件。
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。
身份文件	身份文件数据库提供关于可执行文件的信息。身份文件详细信息包括制造商名称、应用程序类型、产品名称、产品版本、文件名和特殊代码。特殊代码是单字符字段，可以识别特殊的文件签名条目，如恶意代码签名或其他类型的特殊条目。特殊代码可以有值，如 M （恶意文件）、S （特殊文件），也可以留空 （普通文件）。
JAR (Java ARchive)	种存档文件格式，一个 JAR 文件中包含多个 Java 类文件以及关联的元数据和资源 （文本、图像等），能够在 Java 平台上分配应用软件或库。
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本地控制列表中。

术语	定义
保护	如果此设置设为*已启用*，表示 Anti-Executable 正在根据中央控制列表和本地控制列表对计算机实施保护。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。
发行者	发行者是文件的创建者，通过数字签名来验证文件。Anti-Executable 使用发行者名称、产品文件名和版本详细信息来标识发行者创建的文件。
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 图标以及阻止显示警报的选项。
临时执行模式	临时执行模式可让用户在指定时间内运行可执行程序，而无需从 Anti-Executable 执行任何操作。在此期间，用户可以运行任何可执行程序，不受任何限制。被阻止的可执行程序将不允许运行。
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。
未授权的可执行程序	未授权的可执行程序是不允许运行的可执行程序。

简介

Anti-Executable 只允许已获审批的应用程序在计算机或服务器上运行，因此确保了整体的终端生产率。所有其它多余的、未经许可的或者不需要的程序均会被拦截，无法执行。

主题

Anti-Executable 概述

关于 Anti-Executable

Faronics 致力于提供软件来帮助企业管理、简化多用户计算环境并确保其安全。我们的产品能够完全确保工作站的正常工作，并将 IT 人员从繁琐的技术支持和软件问题中解放出来。在以客户为中心的精神推动下，Faronics 取得的技术创新能够让教育机构、医疗机构、图书馆、政府部门以及企业获益。

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单个独立计算机。
服务器标准版	承载服务器操作系统的单个独立计算机。
企业版	承载非服务器操作系统的多个计算机。
服务器企业版	承载服务器操作系统的多个计算机。

系统要求

可在下列操作系统中安装 Anti-Executable：

- 32 位及 64 位版本的 Windows 7、Windows 8.1、Windows 10（最高 22H2 版）和 Windows 11（最高 22H2 版）。
- Windows Server 2008 R2、Windows Server 2012、Windows Server 2016、Windows Server 2019 和 Windows Server 2022。

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。

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

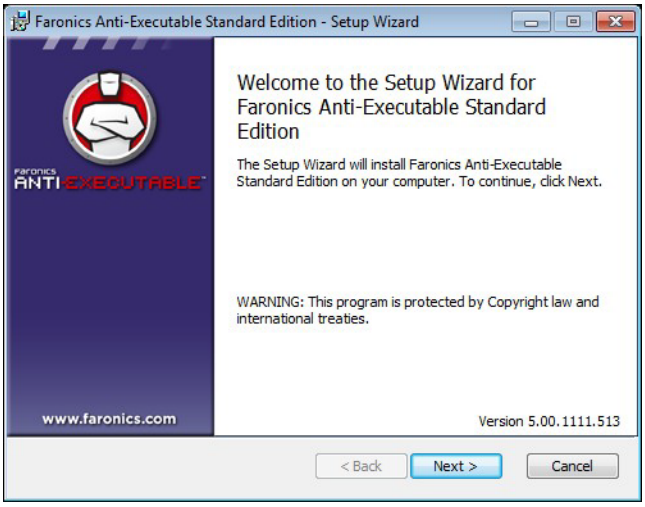
Anti-Executable 针对 Windows Server 2008 R2、Windows Server 2012、Windows Server 2016、Windows Server 2019 、Windows Server 2022 和 32 位和 64 位版本的 Windows 7、Windows 8.1、Windows 10 （最高 22H2 版）和 Windows 11 （最高 22H2 版）提供了不同的安装程序。

系统	安装文件
Windows 非服务器 （32 位）	AEStd_32-bit.msi
Windows 非服务器 （64 位）	AEStd_64-bit.msi
Windows Server （32 位）	AESrvStd_32-bit.msi
Windows Server （64 位）	AESrvStd_64-bit.msi

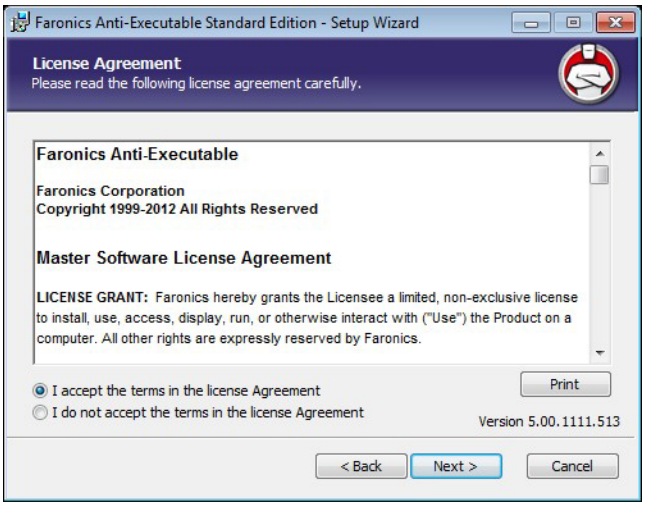
安装 Anti-Executable 标准版

要安装 Anti-Executable 标准版，请完成以下步骤：

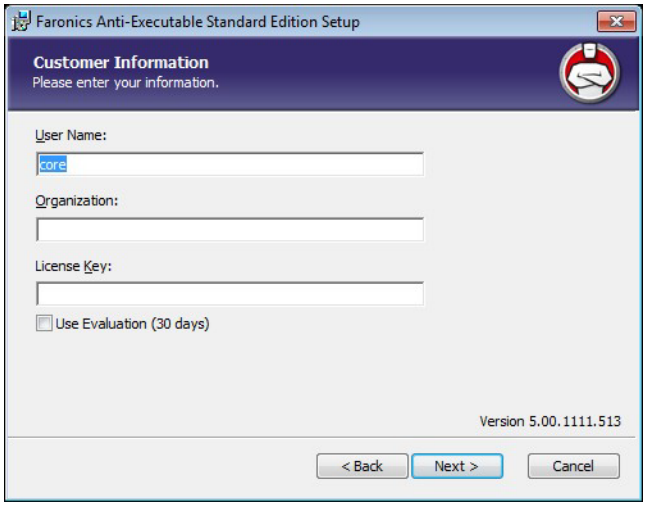
1. 双击 *.msi* 文件开始安装过程。单击 *下一步*继续。



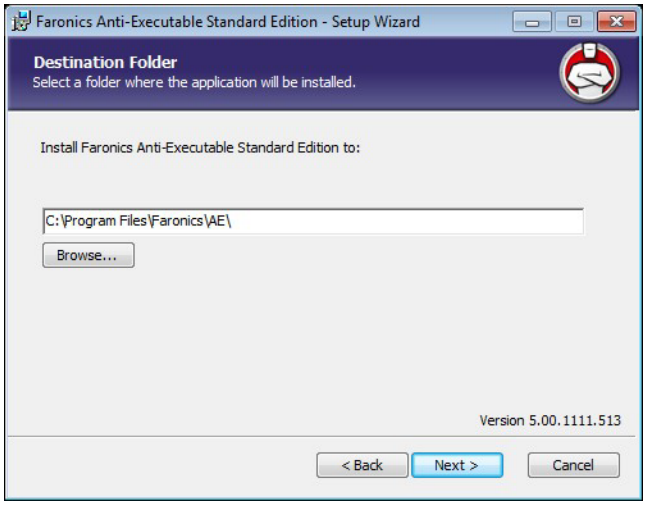
2. 接受许可协议。单击 *下一步*继续。



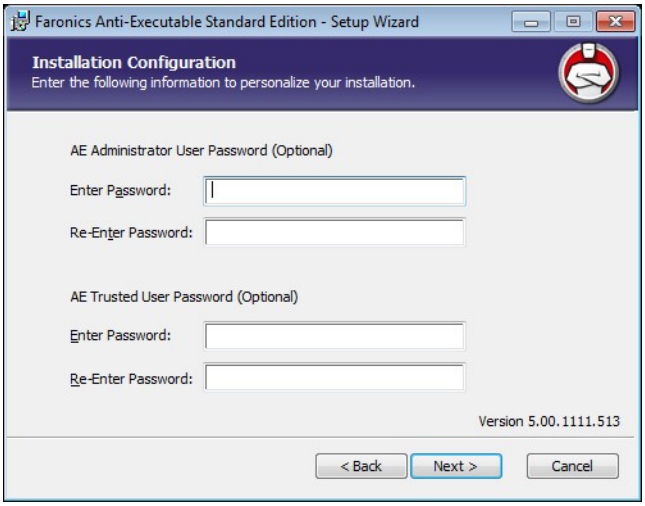
3. 指定*用户名*和*组织*。单击 *下一步*继续。



4. 指定*目的文件夹*。默认位置为 *C:\Program Files\Faronics\AE*。单击 *下一步*继续。

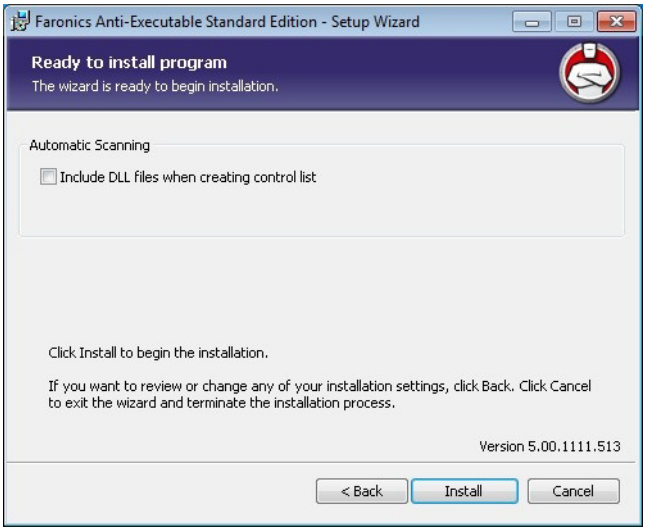


5. 指定 *AE 管理员用户密码*和 *AE 受信任的用户密码*。单击 *下一步*继续。

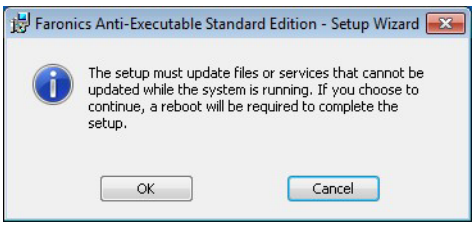


6. 选择下列选项并单击*安装*。Anti-Executable 将扫描计算机并创建包含所有文件和发行者列表的控制列表。

   > *创建控制列表时包括 DLL* – 如果想要包括 DLL，请选择此选项。



7. 单击*确定*以重启计算机。单击*取消*以稍后重启计算机。



8. 单击*完成*结束安装。

访问 Anti-Executable 标准版

Anti-Executable 可通过双击 Windows 系统任务栏中的 Anti-Executable 图标直接在工作站上进行访问。您也可以使用 Ctrl+Alt+Shift+F10 热键序列。

如果您是管理员，将可以访问 " 状态 "、" 执行控制列表 " 和 " 用户 " 选项卡。如果您是受信任的用户，将只可以访问 " 状态 " 和 " 执行控制列表 " 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

本章描述配置和使用 Anti-Executable 的步骤。

主题

概述

Anti-Executable 提供多个控制列表以增强保护功能。可用的组件如下：

- 执行控制列表 – 执行控制列表定义 Anti-Executable 必须如何管理文件或发行者。执行控制列表定义必须"允许"还是"阻止"文件或发行者。

  Anti-Executable 预先填充了一个众所周知的发布者列表。此列表根据需要进行更新。
- 文件和发行者本地列表（控制列表） – 在工作站上首次安装 Anti-Executable 时，Anti-Executable 将扫描计算机并创建*被允许*的所有文件和发行者的列表。

配置 Anti-Executable

Anti-Executable 提供下列选项卡：

- 状态
- 执行控制列表
- 用户
- 临时执行模式
- 设置

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*。

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 或 Faronics 合作伙伴以获取许可证密钥。

启用 Anti-Executable 保护

安装后将默认启用 Anti-Executable。

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执行控制列表中。若要退出维护模式，请选择*启用*或*禁用*。

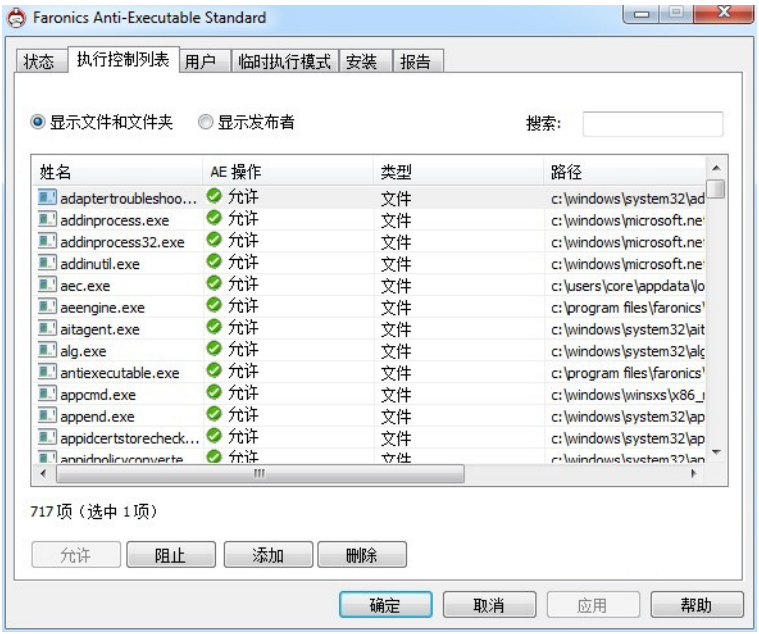
如果选择*启用*，Anti-Executable 将记录所做的更改。如果选择*禁用*，Anti-Executable 将不会记录所做的更改。

在以维护模式运行期间，必须为 Windows 更新提供充足的时间。

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执行控制列表中。

执行控制列表选项卡

" 执行控制列表 " 选项卡用于指定是否必须 " 允许 " 或 " 阻止 " 中央控制列表中的项目。



完成下列步骤以指定 Anti-Executable 行为：

1. 选择 " 显示文件和文件夹 " 或 " 显示发行者 "。
2. 如果选择 " 显示文件和文件夹 "，则将显示以下列：
   - 名称
   - AE 操作
   - 来源
   - 受信任
   - 类型
   - 路径
   - 添加日期
   - 备注
3. 单击*添加*，将文件或文件夹添加到中央控制列表和执行控制列表中。选择项目并单击*删除*，将其从执行控制列表中删除。选择项目并单击*允许*或*阻止*。单击*身份文件详细信息*以查看所选文件的身份文件详细信息。
4. 单击 " 应用 "。单击 " 确定 "。

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 – 可以管理中央控制列表、本地控制列表、执行控制列表、用户和设置，还可以卸载 Anti-Executable。
- 受信任的用户 – 可以配置 Anti-Executable 以及设置执行控制列表。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。

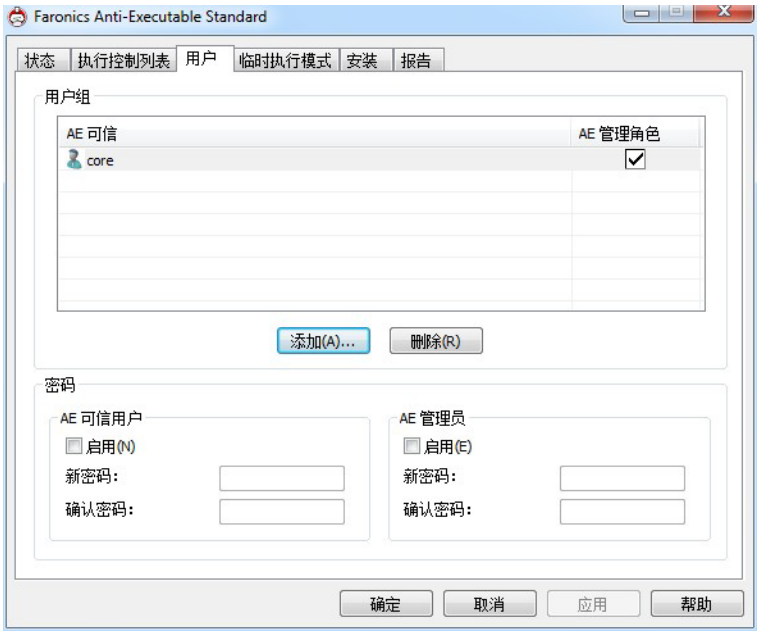
如果 Anti-Executable 管理员或受信任的用户尝试在已启用 Anti-Executable 的情况下打开未授权的应用程序，将显示 " 警报 " 对话框。

添加 Anti-Executable 管理员或受信任的用户

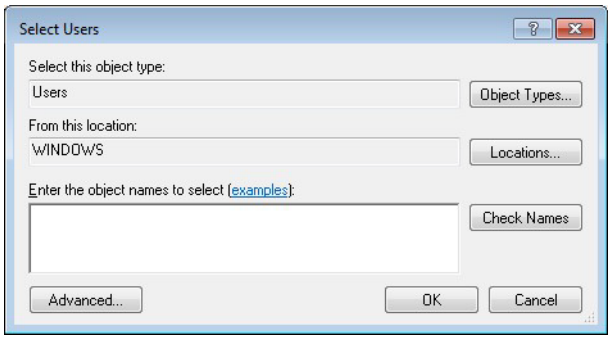
所有 Anti-Executable 用户均为现有 Windows 用户帐户。但是，并非所有 Windows 用户帐户都会自动成为管理员或受信任的用户。不是管理员或受信任用户的 Windows 用户帐户为外部用户。

要将用户添加至 Anti-Executable，请执行以下步骤：

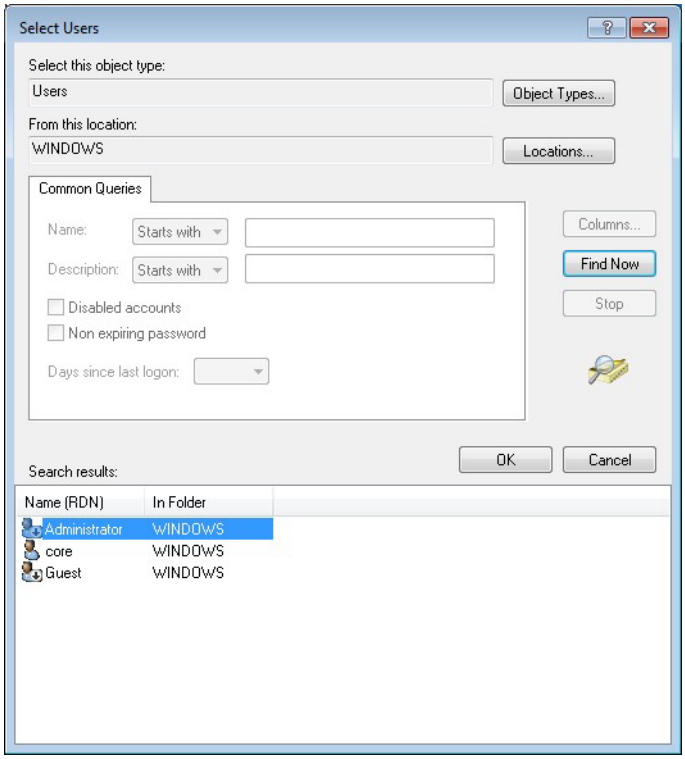
1. 单击 Anti-Executable 窗口顶部的*用户*选项卡。



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. 单击高级 > 立即查找以显示可用用户列表。Anti-Executable 管理员可添加域用户（或组）和本地用户 （或组）。单击用户或组以将其添加至 Anti-Executable 的列表中，然后单击 " 确定 "。



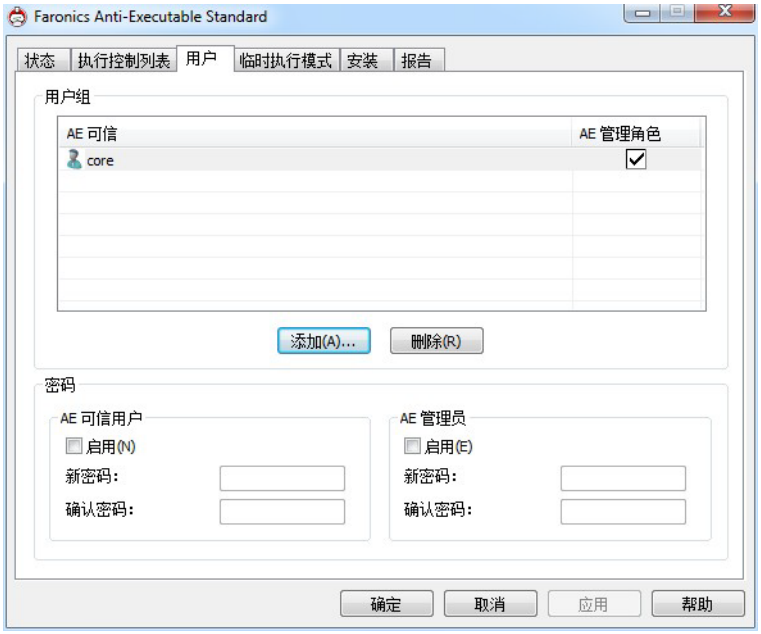
4. 默认情况下，每个被添加的用户均为 Anti-Executable 受信任的用户。如果要赋予新用户管理权限，请选中 *Anti-Executable 管理角色*复选框，以将其指定为 Anti-Executable 管理员。

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*。这不会删除用户的 Windows 用户帐户。此用户现在成为外部用户。

启用 Anti-Executable 密码

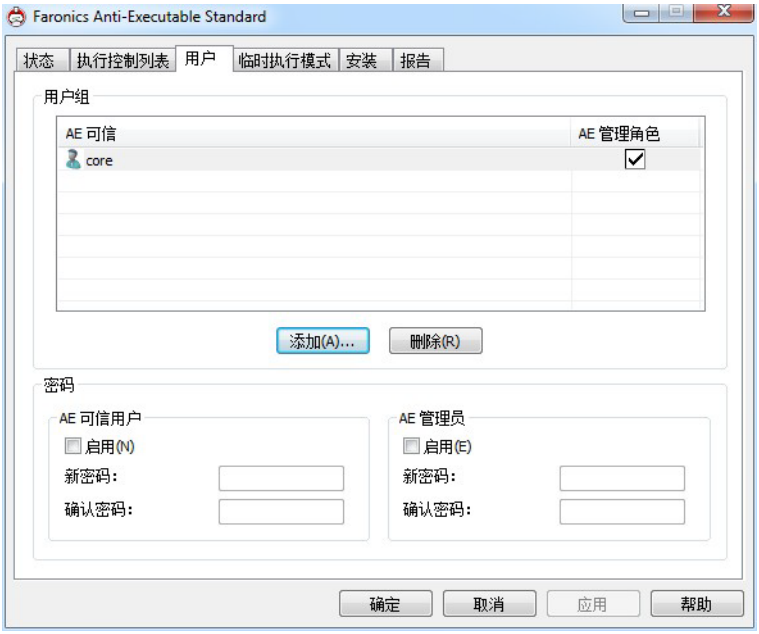
Anti-Executable 可以为每个用户组附加一个密码，作为一项额外的保护措施。密码只能应用于相关组的成员。要指定密码，请确保选中了*启用*复选框，然后在*新密码*和*确认密码*字段中输入密码。单击*应用*以保存更改。



临时执行模式选项卡

临时执行模式可让用户在指定时间内运行可执行程序，而无需从 Anti-Executable 执行任何操作。在此期间，用户可以运行任何可执行程序，不受任何限制。临时执行模式结束之后，Anti-Executable 会立即启用。" 临时执行模式 " 选项卡显示策略信息。不能在工作站上修改 " 临时执行模式 " 选项卡上的设置。

以下选项在临时执行模式下可用：



- 以下用户有权访问临时执行模式 – 可让一组特定用户在其系统上激活临时执行模式。可以选择"所有用户"、"Anti-Executable 用户"或"仅 Anti-Executable 管理员"。
- 临时执行模式日志 – 在临时执行模式期间创建日志文件。
  - > 日志文件数 – 指定日志文件的数目（最多 10 个）。日志记录信息按顺序存储到文件。例如，如果指定了 3 个文件 A、B 和 C，则 Faronics Anti-Executable 首先将错误日志写入到文件 A。如果文件 A 已满，则开始写入到文件 B，最后写入到文件 C。一旦文件 C 已满，将删除文件 A 中的数据，并写入新的日志记录数据。
  - > 文件大小 – 选择每个文件的大小（以 MB 为单位）。最多可以有 10 个日志文件，每个文件最大为 10 MB，即所有文件合计最大为 100 MB。

激活或禁止临时执行模式

- 激活临时执行模式：右键单击系统任务栏中的 Anti-Executable 图标，然后选择 *临时执行模式 > x 分钟* (设置为 60 分钟、24 小时或 7 天)
- 禁止临时执行模式：右键单击系统任务栏中的 Anti-Executable 图标，然后选择 *临时执行模式 > 禁用*

临时执行模式激活之后，工作站的系统任务栏将显示以下图标：

在临时执行模式结束前的 3 分钟，一则消息将在工作站显示。

临时执行模式下禁用 Windows 自动更新。

设置选项卡

Anti-Executable 管理员可设置 " 事件报告 " 记录用户的各种操作、启用 " 隐蔽模式 " 的各种设置、设置 " 警报 " 以及启用 " 兼容性选项 "。

在 Anti-Executable 中设置事件记录

选择 *记录到文件*以将事件记录到日志文件。日志文件位于 *All Users/Documents* 目录下面。

监视 DLL 执行

选中 *监视 DLL 执行*复选框以监视 DLL。如果此复选框未选中，则即使已将 DLL 文件添加至执行控制列表，这些文件也不会被监视。

监视 JAR 执行

选中*监视 JAR 执行*复选框以监视 JAR 文件。如果此复选框未选中，则即使已将 JAR 文件添加至执行控制列表，这些文件也不会被监视。

监视 VBScript 执行

选择此选项可监视 VBScript 文件。如果此复选框未选中，则即使已将 VBScript 文件添加至控制列表，这些文件也不会被监视

监视 PowerShell 脚本执行

选择此选项可监视 PowerShell 脚本文件。如果此复选框未选中，则即使已将 PowerShell 文件添加至控制列表，这些文件也不会被监视

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 图标以及阻止显示警报的选项。

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。

兼容性选项

Anti-Executable 与 Deep Freeze 兼容。

Deep Freeze 兼容性

此功能仅当计算机上安装了 Deep Freeze 和 Anti-Executable 才适用。

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

如果选中*启用 Deep Freeze 兼容性*复选框，Anti-Executable 会在 Deep Freeze 进入维护模式时自动进入维护模式（在维护模式下，Deep Freeze 将会重启为 *Thawed* 状态）。

Deep-Freeze 和 Anti-Executable 同时设为维护模式后，添加至计算机的任何可执行程序不仅会被加至执行控制列表，而且会在 Deep Freeze 退出维护模式、重新冻结计算机后受其保护。

Deep Freeze 将会在 Anti-Executable 退出维护模式后不久退出维护模式。Anti-Executable 退出维护模式后，任何新的可执行文件或更新的可执行文件即会添加至执行控制列表。当 Deep Freeze 退出维护模式时，系统将*冻结*更新的执行控制列表并重启计算机。

如果启用了 *Deep Freeze 兼容性*，但 Deep Freeze 处于*冻结*状态，则无法将 Anti-Executable 设为维护模式。原因在于重启计算机时对计算机所做的更改将丢失。

如果禁用了 Anti-Executable，当 Deep Freeze 进入维护模式时，Anti-Executable 将继续处于禁用状态。

由 Deep Freeze 触发的维护期均优先于 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 " 窗格指定警报消息和图片，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：

- 执行控制列表违规消息
- 被阻止的通知消息

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。

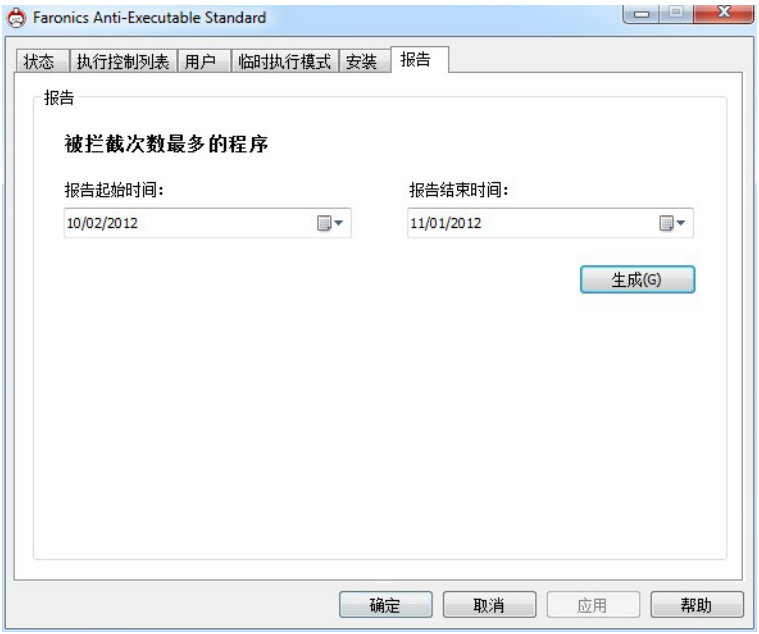
单击 " 更改 " 并浏览以选择位图图片文件。选定图片将与文本一起显示在警报对话框中。警报消息将显示以下信息：

- 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

如下所示为警报对话框范例：

" 报告 " 选项卡

通过 " 报告 " 选项卡，您可以生成选定时段被拦截次数最多的程序的报告。



要生成报告，请完成以下步骤：

1. 单击*报告*选项卡。
2. 为*报告起始时间*选择日期。
3. 为*报告结束时间*选择日期。
4. 单击*生成*。

此时浏览器将启动，报告将显示。

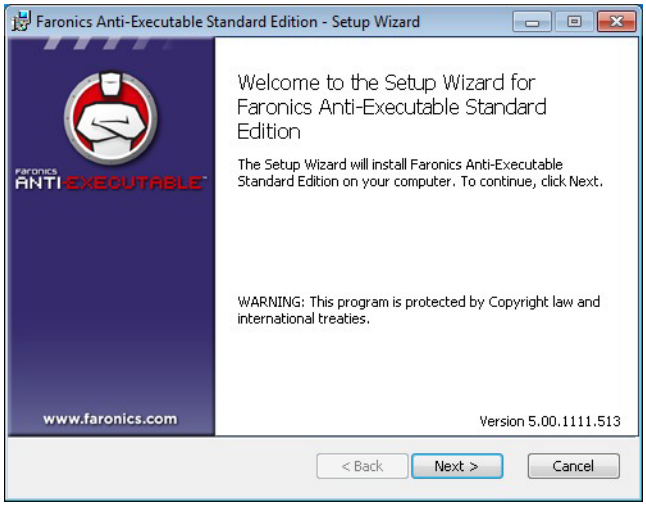
卸载 Anti-Executable

主题

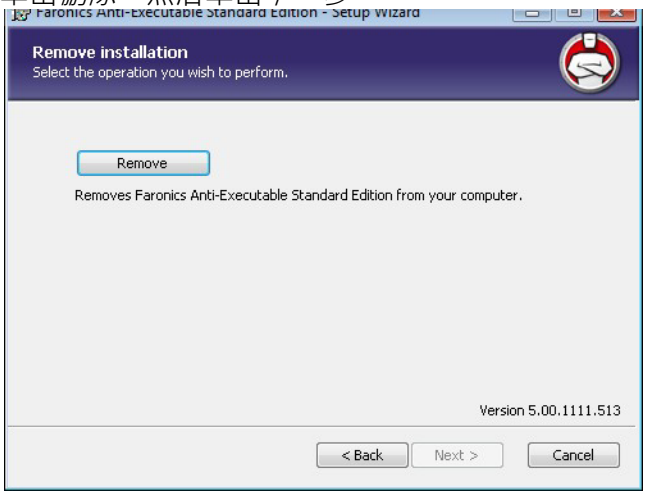
卸载 Anti-Executable 标准版

Anti-Executable 可通过双击 *.msi* 安装文件删除。此时将显示安装向导：

1. 单击 *下一步*开始卸载。



2. 单击 *删除*，然后单击 *下一步*。



3. 单击*删除*。


Faronics Anti-Executable Standard Edition - Setup Wizard
Ready to remove program
Click Remove to remove Faronics Anti-Executable Standard Edition from your computer. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.
Version 5.00.1111.513
< Back
Remove
Cancel

4. 单击*完成*。