Faronics

ANTI-EXECUTABLE™

ENTERPRISE

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

1999–2023 Faronics Corporation。保留所有权利。Faronics、Deep Freeze、Deep Freeze Cloud、Faronics Deploy、Faronics Core Console、Faronics Anti-Executable、Faronics Anti-Virus、Faronics Device Filter、Faronics Data Igloo、Faronics Power Save、Faronics Insight、Faronics System Profiler 和 WINSelect 是 Faronics Corporation 的商标和 / 或注册商标。所有其他公司名称和产品名称均为其各自所有者的商标。

目录

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 11

Anti-Executable 概述 12
关于 Anti-Executable 12
Anti-Executable 版本 12
关于 Faronics Core Console 12
系统要求 13
控制台要求 13
工作站要求 13
Anti-Executable 许可证 14

安装 Anti-Executable 15

安装概述 16
安装 Anti-Executable 插件 17
在工作站上手动安装 Anti-Executable 20
通过 Faronics Core Console 在工作站上安装或升级 Anti-Executable 23

访问 Anti-Executable 25

概述 26
通过 Faronics Core Console 访问 Anti-Executable 27
Faronics Core Console 中的 Anti-Executable 列 27
通过 Faronics Core Console 执行 Anti-Executable 命令（插件菜单） 27
通过 Faronics Core Console 执行 Anti-Executable 命令（上下文菜单） 29
计划操作 30
在工作站上访问 Anti-Executable 企业版 31

使用 Anti-Executable 33

概述 34
创建中央控制列表 35
Anti-Executable 策略 38
配置 Anti-Executable 46
状态选项卡 47
检验产品信息 47
启用 Anti-Executable 保护 48
Anti-Executable 维护模式 48
从 Faronics Core Console 检索设置 49
执行控制列表选项卡 50
用户选项卡 51
添加 Anti-Executable 管理员或受信任的用户 51
删除 Anti-Executable 管理员或受信任的用户 52

启用 Anti-Executable 密码 52
临时执行模式选项卡 53
激活或禁止临时执行模式 54
设置选项卡 55
在 Anti-Executable 中设置事件记录 55
监视 DLL 执行 55
监视 JAR 执行 55
监视 VBScript 执行 56
监视 PowerShell 脚本执行 56
Anti-Executable 隐蔽功能 56
兼容性选项 56
自定义警报 57
通过 Faronics Core Console 创建 Anti-Executable 报告 58

命令行控制 59

命令行控制 60

卸载 Anti-Executable 63

在工作站上通过 Faronics Core Console 卸载 Anti-Executable 64
使用安装程序卸载 Anti-Executable 插件 65
卸载 Anti-Executable 插件（添加或删除程序） 67

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
技术支持
术语定义

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 插件	一个软件库，可扩展 Faronics Core Console 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	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。
中央控制列表	安装 Anti-Executable 后首次启动 Faronics Core 时，系统将通过一条消息提示您填充该列表。您可以通过添加控制台计算机上的文件和发行者来填充中央控制列表。然后可以将此中央控制列表通过*策略*应用于工作站。中央控制列表只需创建一次，但可以通过策略多次应用于多个工作站。
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。

术语	定义
Faronics Core Agent	工作站上安装的软件，用于启用与 Faronics Core Console 的通信。
JAR (Java Archive)	是一种存档文件格式，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。
策略	策略是一组 Anti-Executable 设置。可以创建多个策略并通过 Faronics Core 应用于工作站。您可以创建新策略、编辑现有策略或删除策略。
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。
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 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
系统要求
Anti-Executable 许可证

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。

关于 Faronics Core Console

Faronics Core Console 是用于管理多个 Faronics 产品的集成式框架。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。

Faronics Core Console 可管理企业版 Anti-Executable 和 Anti-Executable Server。

系统要求

控制台要求

有关 Faronics Core Console 系统要求的信息，请参阅 www.faronics.com/library 上提供的 Faronics Core Console 用户指南。

工作站要求

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 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。

Anti-Executable 许可证的工作原理如下：

Core Server （Faronics Core 的一个组件）自动将许可证密钥推送到安装了 Anti-Executable 客户端的工作站。如果计算机处于脱机状态，那么一旦其恢复联机，许可证密钥将立即应用。

如果在安装插件时已输入 Anti-Executable 许可证密钥，则无需在*属性*选项卡中再次输入。

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 插件

安装概述

必须安装 Anti-Executable 插件，才能通过 Faronics Core Console 执行 Anti-Executable 的特定任务。安装插件以后，便可通过 Faronics Core Console 在远程计算机上安装、配置、升级或卸载 Anti-Executable。

成功部署 Anti-Executable 后，Faronics Core Console 便可用于管理所有 Anti-Executable 任务和命令。

如果通过 Faronics Core Console 在远程计算机上安装，系统将自动选择合适的安装程序。但在手动安装前，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 （32 位）	AEEnt_32-bit.msi
Windows （64 位）	AEEnt_64-bit.msi
Windows Server （32 位）	AESrvEnt_32-bit.ms
Windows Server （64 位）	AESrvEnt_64-bit.ms

安装 Anti-Executable 插件

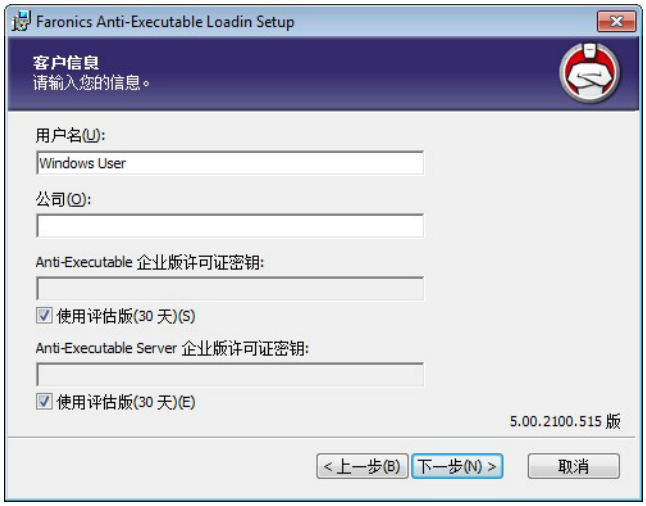
Anti-Executable 插件无法安装到没有安装 Faronics Core Console 的计算机中。

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：

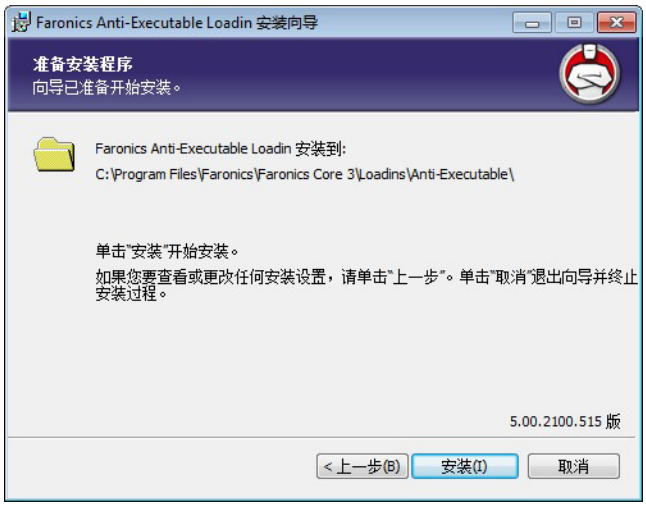
1. 如果是从 Internet 下载的 Anti-Executable，请双击 *Anti-Executable_Console_Loadin_Installer.exe* 文件开始安装过程。单击 *下一步* 继续。

2. 阅读并接受许可协议。单击 *下一步* 继续。

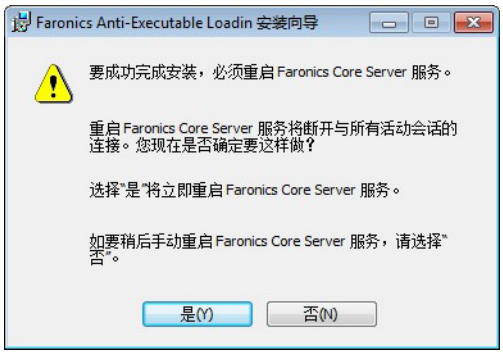
3. 输入*用户名*和*组织*。指定 *Anti-Executable Enterprise* 或 *Anti-Executable Server Enterprise* 的许可证密钥。选择*使用评估版*以安装评估版本。



4. 默认位置为 *C:\Program Files\Faronics\Faronics Core 3\Loadins\Anti-Executable*。单击*安装*继续。



5. 必须重启 Faronics Core Server 服务才能成功完成安装。单击*是*，重启 Faronics Core Server 服务。单击*否*则稍后再手动重启服务。



6. 单击*完成*结束安装。

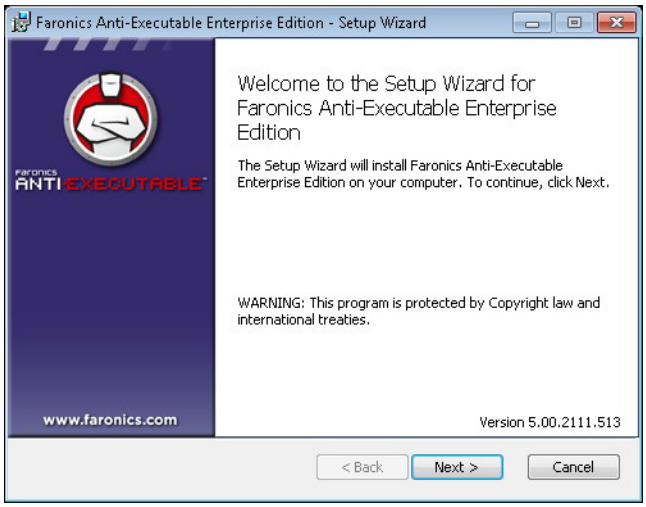
成功安装插件后，如果您选择了一个或多个工作站，Faronics Core Console 会在操作窗格中显示一个 Anti-Executable 特定功能列表。下面讲到的工作站列表中也会显示特定列。选择一个或多个工作站并采用右键单击式上下文菜单也可以使用 Anti-Executable 功能。

在工作站上手动安装 Anti-Executable

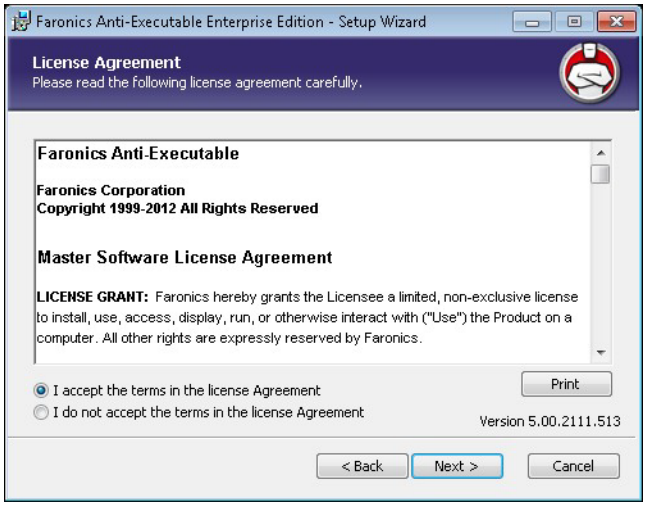
在工作站上安装 Anti-Executable 之前，从安装 Anti-Executable 插件的计算机上的路径 *C:\Program Files\Faronics\Faronics Core 3\Loadins\Anti-Executable\Workstation Installers* 复制相应的 *.msi* 文件到一个或多个工作站。

要在复制该文件后在工作站上手动安装 Anti-Executable，请完成以下步骤：

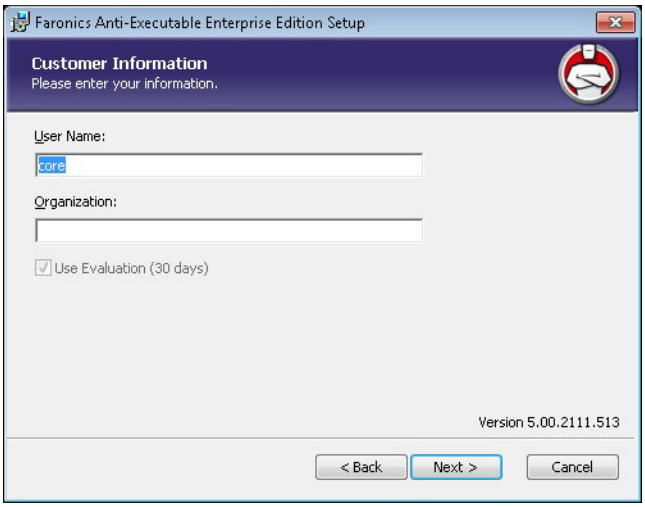
1. 双击 *.msi* 文件开始安装过程。单击 *下一步*继续。



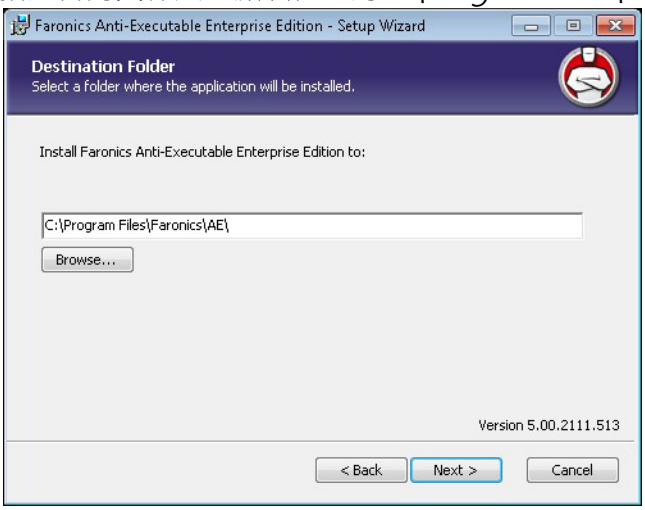
2. 接受许可协议。单击 *下一步*继续。



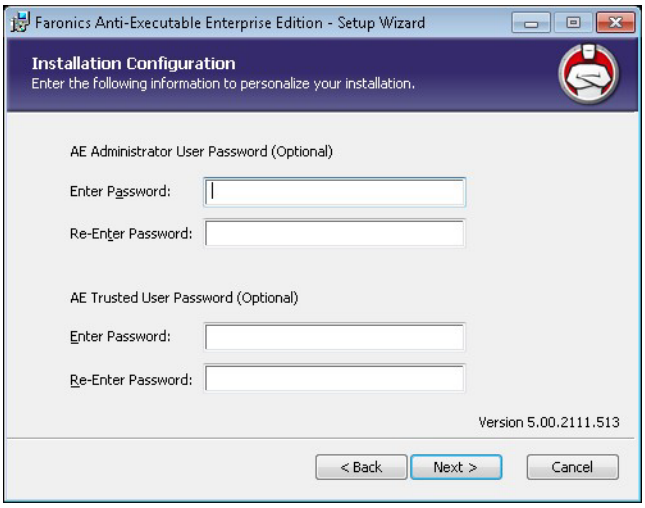
3. 指定*用户名*和*组织*。单击*下一步*继续。



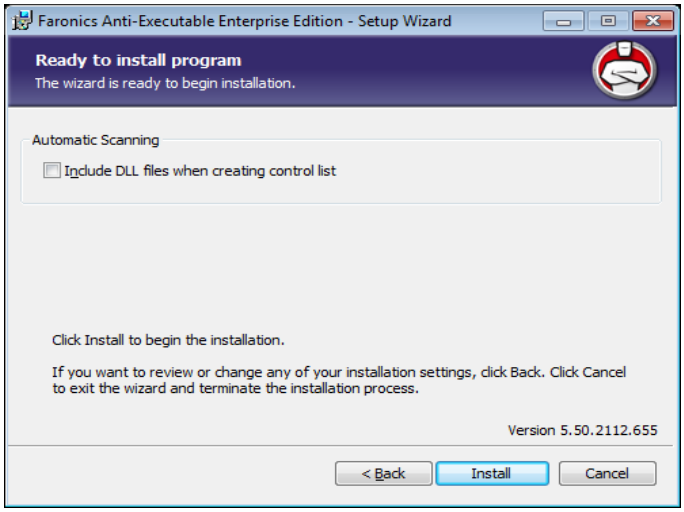
4. 指定*目的文件夹*。默认位置为 *C:\Program Files\Faronics\AE*。单击*下一步*继续。



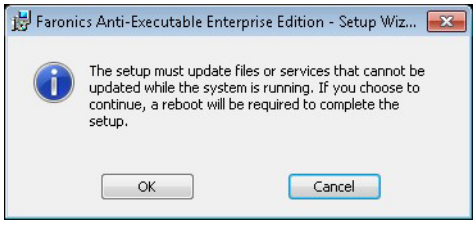
5. 指定 *AE 管理员用户密码*和 *AE 受信任的用户密码*。单击*下一步*继续。



6. 选择下列选项并单击*安装*。
   > 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。

通过 Faronics Core Console 在工作站上安装或升级 Anti-Executable

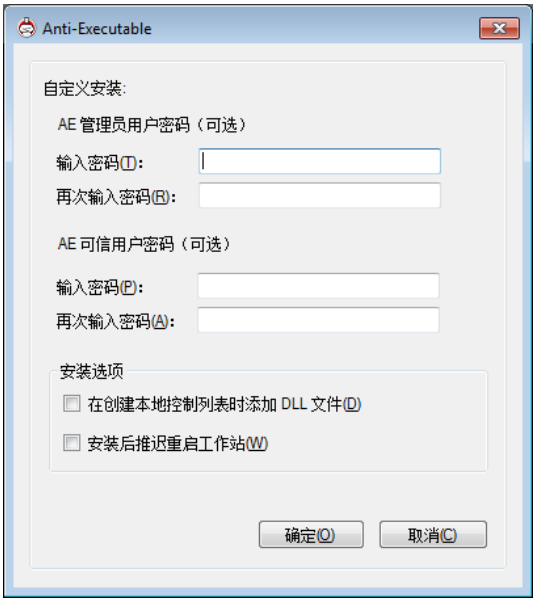
安装 Anti-Executable 插件会解压缩保护远程计算机所需的 Anti-Executable 安装文件（解压缩的具体文件取决于要安装的 Anti-Executable 版本）。

通过 Faronics Core Console 安装 Anti-Executable 之前，必须在每个工作台上安装 Faronics Core Agent。Faronics Core Agent 可实现 Faronics Core Console 和安装控制台的工作站之间的通信。有关部署 Faronics Core Agent 的过程的详细信息，请参阅 www.faronics.com/library 上提供的 *Faronics Core Console 用户指南*。

解压缩 Anti-Executable 文件的默认位置为 *C:\Program Files\Faronics\Faronics Core\Loadins\Anti-Executable\Workstation Installers*

要在一个或多个工作站上安装或升级 Anti-Executable，请完成以下步骤：

1. 从 Faronics Core Console 的列表中选择一个或多个工作站，然后选择 *操作窗格 > Anti-Executable > 安装 / 升级 Anti-Executable*，或者右键单击 Faronics Core Console 的列表中的工作站，然后选择 *Anti-Executable > 安装 / 升级 Anti-Executable*。
2. 指定工作站凭据，有如下两种选择：
   - 选择 *本地工作站帐户*，使用本地工作站帐户作为 Anti-Executable 的第一个用户。指定 *用户名*。单击 *确定*。
   - 选择 *域帐户*，使用域帐户作为 Anti-Executable 的第一个用户。指定 *域*、*用户名*。单击 *确定*。
3. 此时将显示 *自定义安装*对话框。指定 *AE 管理员密码*、*AE 受信任的用户密码*和 *许可证密钥*。选择以下显示的选项之一：
   - 在创建本地控制列表时包括 DLL 文件 – 扫描时包括 DLL（动态链接库）文件。
   - 安装后推迟重启工作站 – 安装后推迟重启。要使 Anti-Executable 正常工作，必须重启工作站。
4. 单击 *确定*以安装 Anti-Executable。Anti-Executable 将会安装，并且激活控制列表。


Anti-Executable
自定义安装:
AE 管理员用户密码（可选）
输入密码(T):
再次输入密码(R):
AE 可信用户密码（可选）
输入密码(P):
再次输入密码(A):
安装选项
在创建本地控制列表时添加 DLL 文件(D)
安装后推迟重启工作站(W)
确定(O)
取消(C)

访问 Anti-Executable

主题

概述
通过 Faronics Core Console 访问 Anti-Executable
在工作站上访问 Anti-Executable 企业版

概述

Anti-Executable Enterprise 可通过 Faronics Core Console 访问，也可从部署 Anti-Executable 的工作站上由已登录的授权用户直接访问。

通过 Faronics Core Console 访问 Anti-Executable

Anti-Executable 可通过 Faronics Core Console 进行访问，方法是从 Faronics Core Console 的工作站列表中选择单个工作站，然后打开*操作窗格 Anti-Executable > 配置 Anti-Executable 客户端*，或者右键单击列表中的某个工作站，然后选择*配置 Anti-Executable 客户端*。

Faronics Core Console 中的 Anti-Executable 列

以下与 Anti-Executable 有关的列显示在*结果*窗格中：

- 隐蔽 – 此列指定 Anti-Executable 是否以隐蔽模式运行。
- 保护 – 此列指定以下值之一：
  - 启用 – 如果设置为*启用*，表示 Anti-Executable 正在根据本地执行列表对工作站实施保护。
  - 禁用 – 如果设置为*禁用*，则工作站上的任何可执行程序均可启动。
  - 维护模式 – 处于维护模式时，添加或修改的新可执行文件将在选中*启用*时自动添加到本地执行列表中。如果选择*禁用*，Anti-Executable 将不会记录所做的更改。
  - 临时执行模式 – 如果设置为*临时执行模式*，则工作站上的任何可执行程序均可启动。
- 策略名称 – 应用于工作站的策略的名称。
- 版本 – 此列指定 Anti-Executable 版本。
- 事件报告 – 此列指定是否已启用或禁用事件报告。
- 许可证类型 – 此列指定这是评估版还是正式版。
- 鼠标 / 键盘 – 此列指定是否已启用或禁用一个或多个选定工作站的鼠标和键盘。

有关工作站列表中的其他列的详细信息，请参阅 www.faronics.com/library 上提供的 Faronics Core Console 用户指南。

通过 Faronics Core Console 执行 Anti-Executable 命令（插件菜单）

Anti-Executable 命令可通过 Anti-Executable 插件的右键单击上下文菜单访问。

*插件*菜单提供以下命令。

管理中央控制列表

该命令用于管理中央控制列表。中央控制列表是文件和发行者的存储库。中央控制列表可通过策略应用于一个或多个工作站。

新建策略

策略是一组设置。该命令用于创建新策略。策略可应用于一个或多个工作站。策略可定义中央控制列表中的项目是*被允许*还是*被阻止*。

保护

要快速*启用*或*禁用* Anti-Executable 保护，请选择一个或多个工作站并在*操作*窗格中单击*保护 > 启用* 或 *> 禁用*。

维护模式

将 Anti-Executable 设置为在维护模式下运行。在此期间将允许运行任何可执行程序。维护模式用于安装新应用程序和应用程序升级。

键盘和鼠标

禁用或启用一个或多个工作站的键盘和鼠标设备的方法是：单击*键盘 / 鼠标*，然后选择*禁用*或*启用*。

管理 AE 用户

选择此选项可管理 Anti-Executable 用户。

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。选择一个工作站，然后选择*临时执行模式*，再选择 *5*、*15*、*30*、*45*、*60* 或者*自定义*。选择一个工作站，然后选择*临时执行模式 > 禁用*以禁用临时执行模式。

启动本地控制列表扫描

通过扫描工作站上的文件，启动控制列表扫描。这将创建文件和发行者本地列表。添加到控制列表中的所有文件和发行者默认*被允许*。

重新分配策略

重新分配当前应用于工作站的策略。

配置 Anti-Executable 客户端

选择此选项可配置工作站上的 Anti-Executable 客户端。

安装 / 升级 Anti-Executable 客户端

选择此选项可安装或升级 Anti-Executable 客户端。

卸载 Anti-Executable 客户端

选择此选项可卸载 Anti-Executable。

通过 Faronics Core Console 执行 Anti-Executable 命令（上下文菜单）

Anti-Executable 命令可通过右键单击上下文菜单访问。

Anti-Executable 命令也可通过 Faronics Core Console 窗口右侧的 Faronics Core Console 操作窗格访问。选择列表中的工作站后，这些任务即会在操作窗格中列出。

保护

要快速*启用*或*禁用* Anti-Executable 保护，请选择一个或多个工作站并在*操作*窗格中单击*保护 > 启用* 或 *> 禁用*。

维护模式

将 Anti-Executable 设置为在维护模式下运行。

键盘和鼠标

禁用或启用一个或多个工作站的键盘和鼠标设备的方法是：单击*键盘 / 鼠标*，然后选择*禁用*或*启用*。

管理 AE 用户

选择此选项可管理 Anti-Executable 用户。

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。选择一个工作站，然后选择*临时执行模式*，再选择 *5*、*15*、*30*、*45*、*60* 或者*自定义*。选择一个工作站，然后选择*临时执行模式 > 禁用*以禁用临时执行模式。

启动本地控制列表扫描

通过扫描工作站上的文件，启动控制列表扫描。您还可以将文件或发行者添加到策略中。

重新分配策略

重新分配当前应用于工作站的策略。

配置 Anti-Executable 客户端

选择此选项可配置工作站上的 Anti-Executable 客户端。

安装 / 升级 Anti-Executable 客户端

选择此选项可安装或升级 Anti-Executable 客户端。

卸载 Anti-Executable 客户端

选择此选项可卸载 Anti-Executable。

计划操作

Anti-Executable 和 Faronics Core Console 事件可进行计划，以按照管理员期望的日期和时间，在一个或多个工作站上发生。单击一个或多个工作站，并选择 *计划操作*。此时将出现一个子菜单，其中包含以下可用操作列表：

由 Faronics Core Console 控制的操作：

- 关
- 重启
- 唤醒

由 Faronics Anti-Executable 控制的操作

- 保护（启用或禁用）
- 维护模式
- 警报（启用或禁用）
- 临时执行模式
- 启动控制列表扫描
- 安装 / 升级 Anti-Executable
- 卸载 Anti-Executable

选择一个操作后，系统将显示 *计划*菜单，管理员可通过该菜单指定操作发生的频率（一次、每日、每周或每月）。您可以根据频率选择特定时间、天、日期或月份。

在工作站上访问 Anti-Executable 企业版

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
状态选项卡
执行控制列表选项卡
用户选项卡
临时执行模式选项卡
设置选项卡
通过 Faronics Core Console 创建 Anti-Executable 报告

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：

- 中央控制列表 – 中央控制列表是文件和发行者的存储库。安装 Anti-Executable 后首次启动 Faronics Core 时，系统将通过一条消息提示您填充中央控制列表。您可以通过添加控制台计算机、网络上的远程计算机或 UNC 路径上的文件和发行者来填充中央控制列表。

  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。
- 策略 – 策略是一组 Anti-Executable 设置。可以创建多个策略并通过 Faronics Core 应用于工作站。您可以创建新策略、编辑现有策略或删除策略。策略可定义中央控制列表中的项目是*被允许*还是*被阻止*。
- 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。
- 文件和发行者本地列表 – 在工作站上首次安装 Anti-Executable 时，将有一个选项用来扫描工作站并创建*被允许*的所有文件和发行者的列表。该列表驻留在工作站上，无法通过 Faronics Core 查看或编辑。每个工作站都有自己的本地文件和发行者列表。

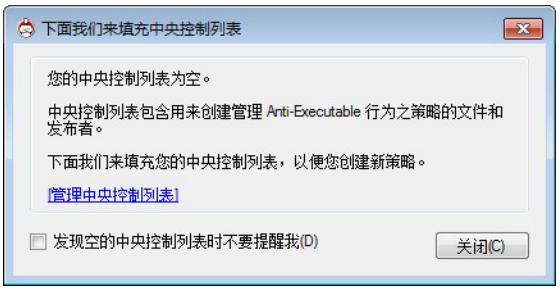
确保保持很小的中央控制列表。如果中央控制列表过大，将设置应用于多个工作站可能需要很长时间。

创建中央控制列表

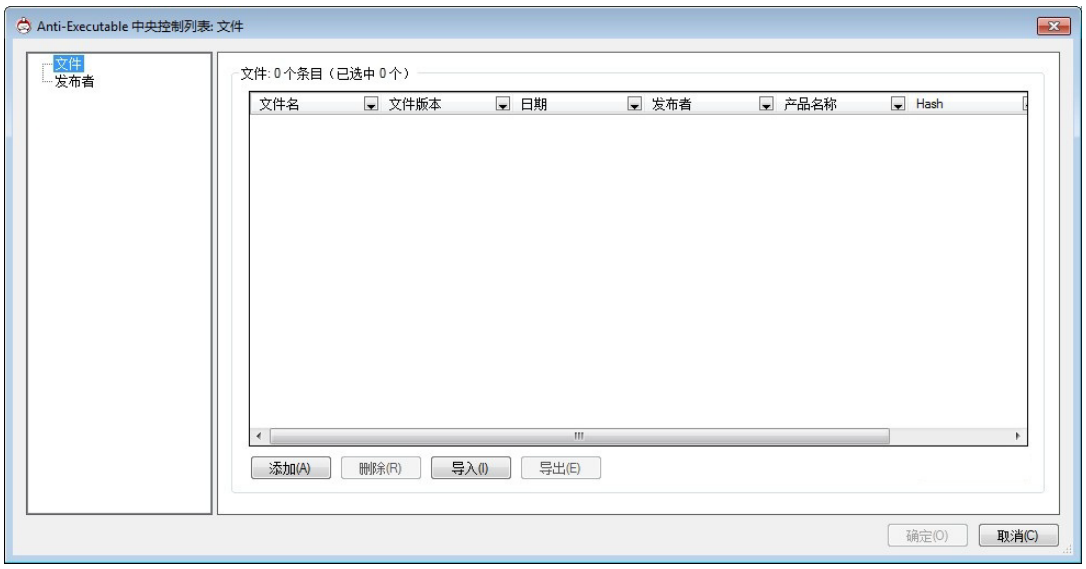
安装 Anti-Executable 后首次启动 Faronics Core 时，系统将通过一条消息提示您中央控制列表为空。

完成下列步骤以填充中央控制列表：

1. 在首次安装 Anti-Executable 后启动 Faronics Core 时，单击首次出现的对话框中的 *管理中央控制列表*。或者右键单击 Anti-Executable 插件并选择 *管理中央控制列表*。

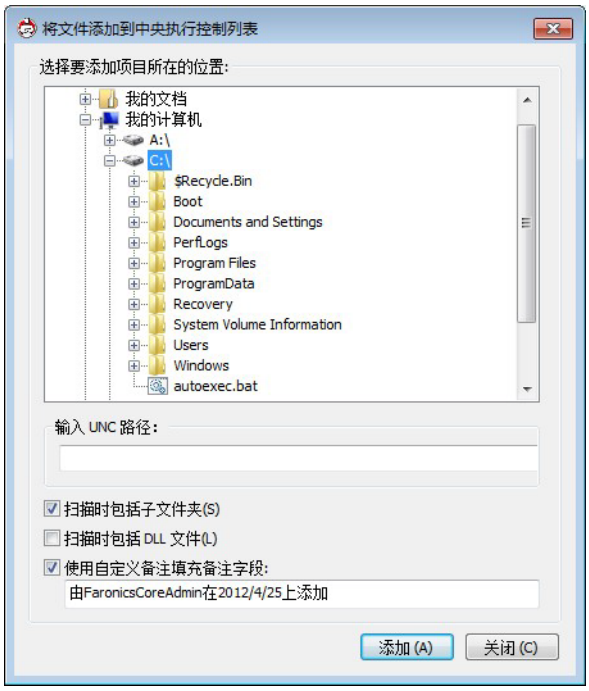


2. 此时将显示 *Anti-Executable 中央控制列表*屏幕。



3. 在 *文件节点*中单击 *添加*。此时将显示 *添加文件到中央控制列表*对话框。

4. 浏览以选择控制台计算机上的文件夹 / 驱动器。选择下列选项并单击*添加*：

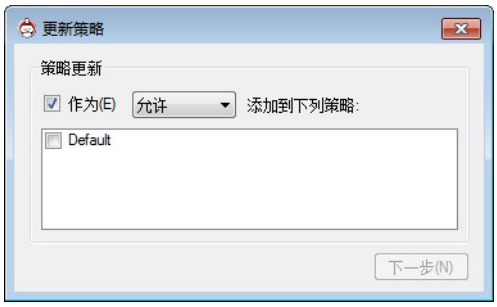


> 扫描时包括子文件夹 – 选择此选项可在扫描选定的驱动器 / 文件夹时包括所有子文件夹。

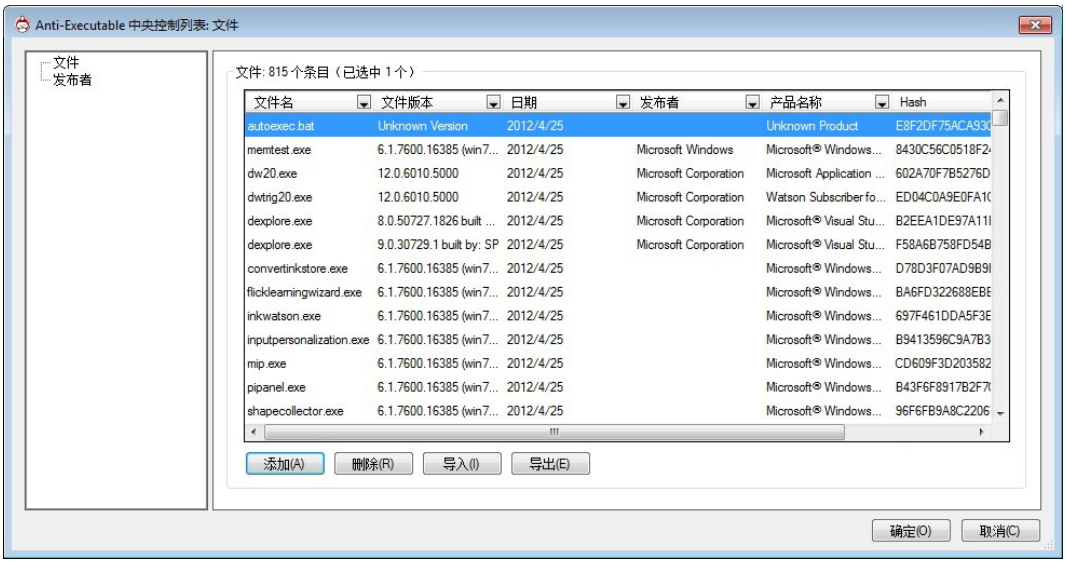
> 扫描时包括 DLL 文件 – 扫描时包括 DLL （动态链接库）文件。

> 使用自定义备注填充备注字段 – 选择此选项并编辑备注 （如果需要）。这些备注将显示在中央列表中。

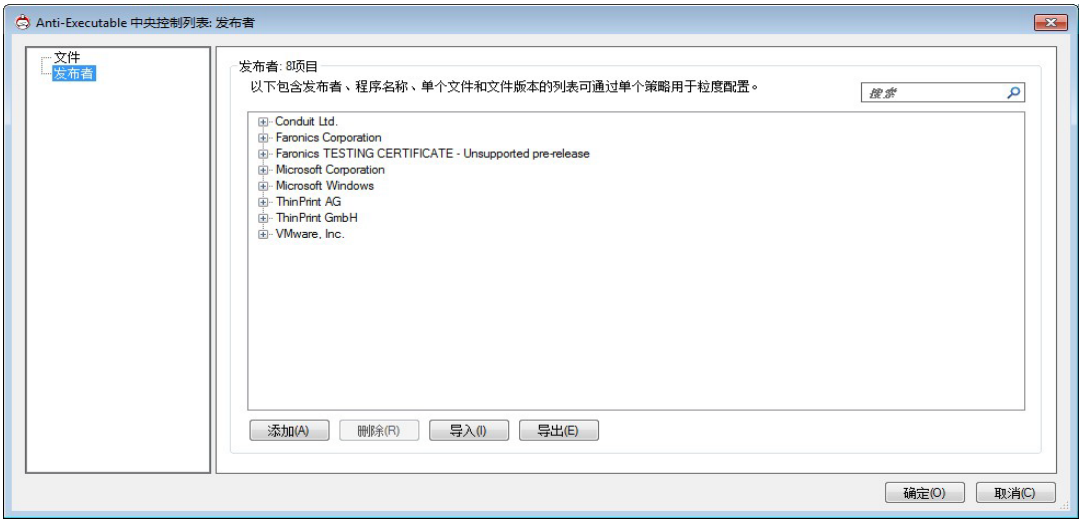
5. 将这些文件添加到*策略更新*对话框中的一个或多个策略。从下拉列表中选择*允许*或*阻止*，并选择要将这些文件添加到的策略。



6. 此时将显示已添加的文件。您可以选择*删除*以删除选定的文件，以及*导出*或*导入*文件列表。您可以根据列标题对文件排序，还可以从列标题动态搜索特定字符串。



7. 单击*发行者*。此时将自动添加并显示控制台计算机上的发行者列表。单击*添加*以添加发行者。单击*删除*以删除选定的发行者。单击*导入*以导入发行者列表。单击*导出*以导出发行者列表。



8. 单击*确定*。中央控制列表即已保存，并可以通过策略应用于工作站。

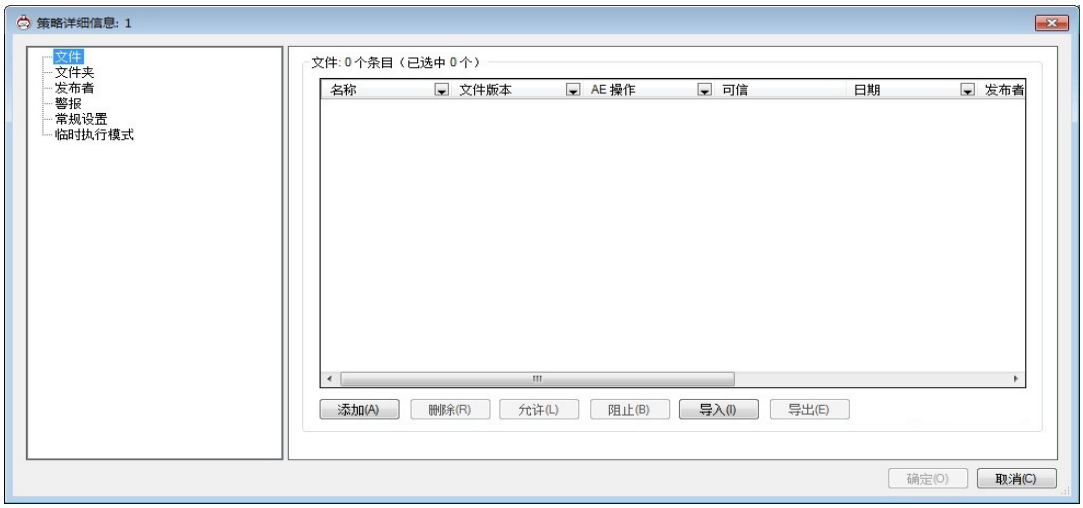
Anti-Executable 策略

策略是一组设置。可以创建一个 Anti-Executable 策略并应用于多个工作站。也可以根据需要创建多个策略。

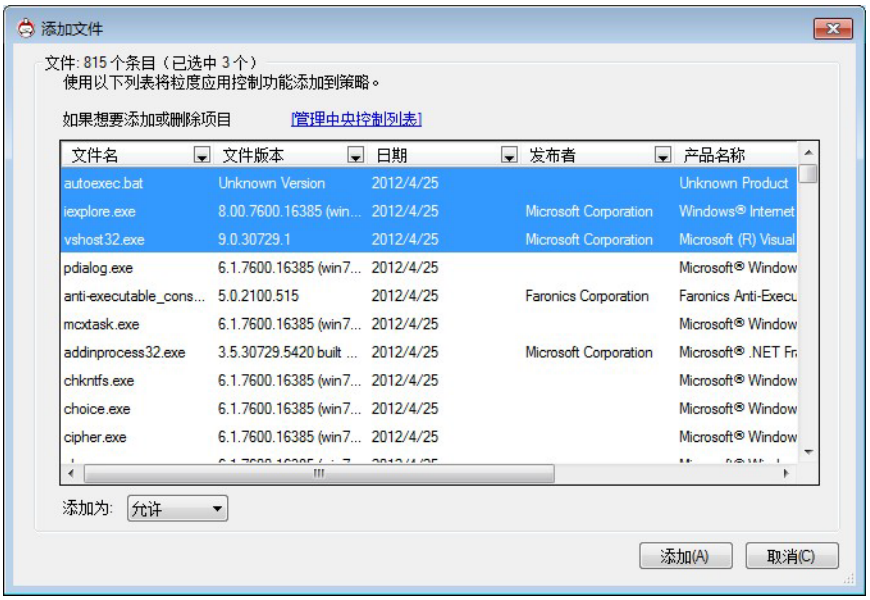
完成下列步骤以创建 Anti-Executable 策略：

1. 右键单击 Anti-Executable 插件，然后选择*新建策略*。
2. 此时将显示*新建策略*对话框。指定策略名称并单击*确定*。

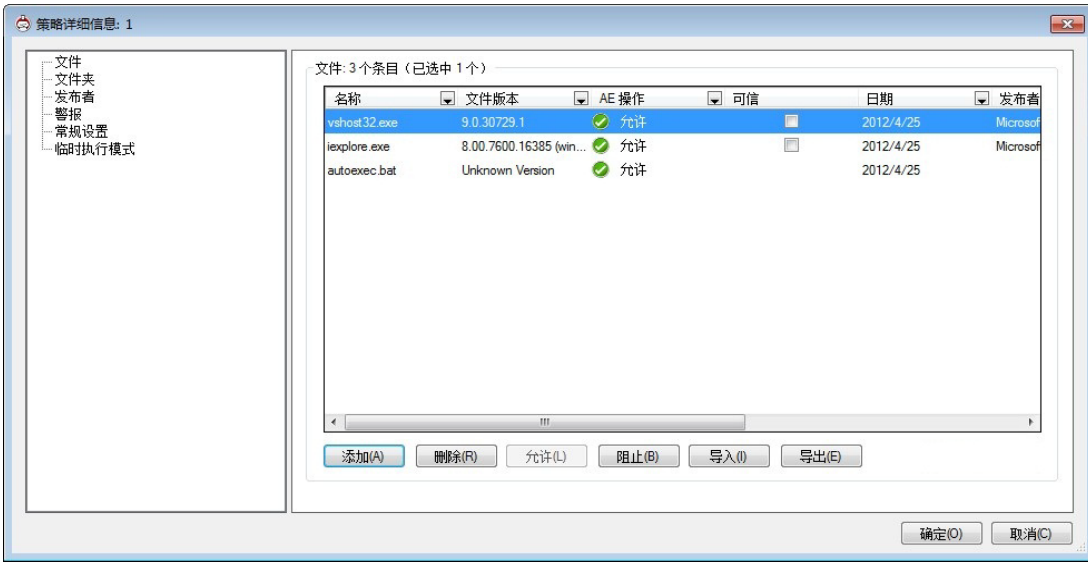
3. 此时将显示*策略*对话框及*文件*节点。



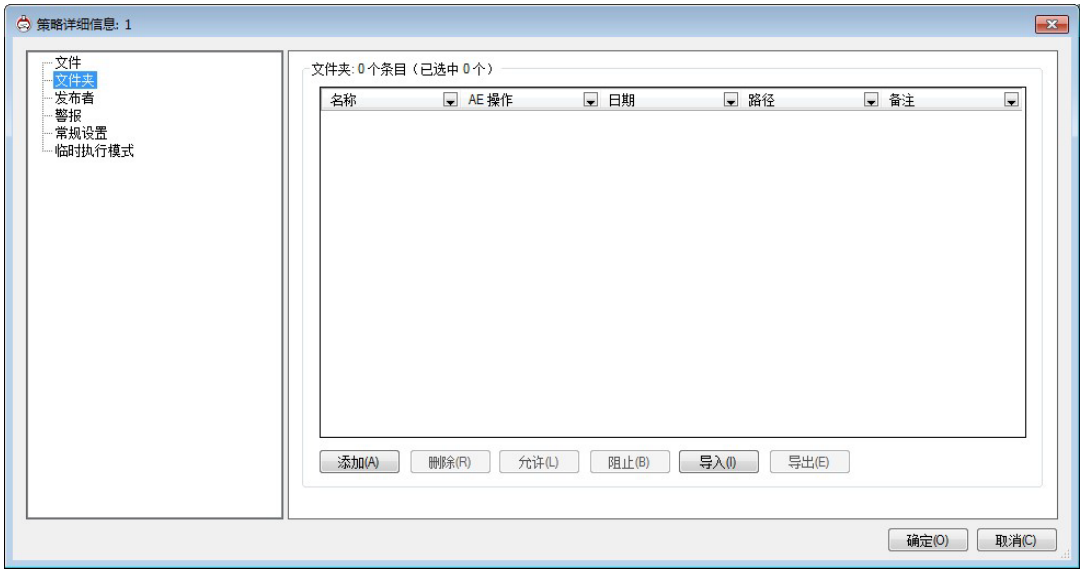
4. 在*文件节点*中单击*添加*。此时将显示已添加到中央控制列表的文件。选择文件并从*添加为*下拉列表中选择*允许*或*阻止*，然后单击*添加*。



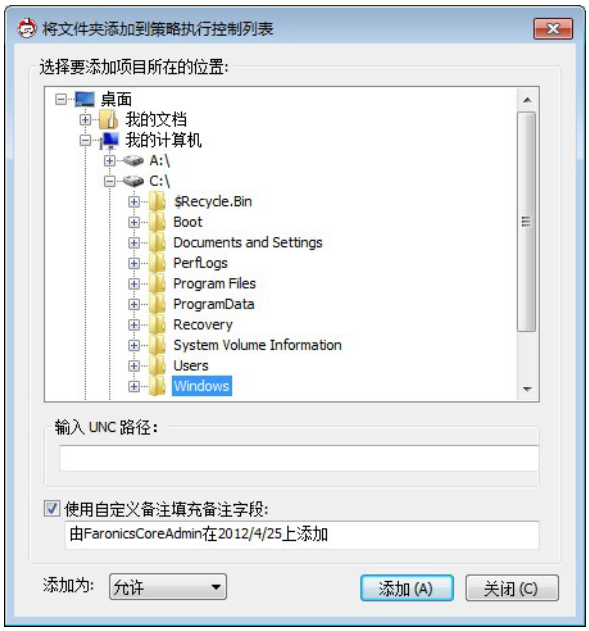
5. 文件即已添加到策略。



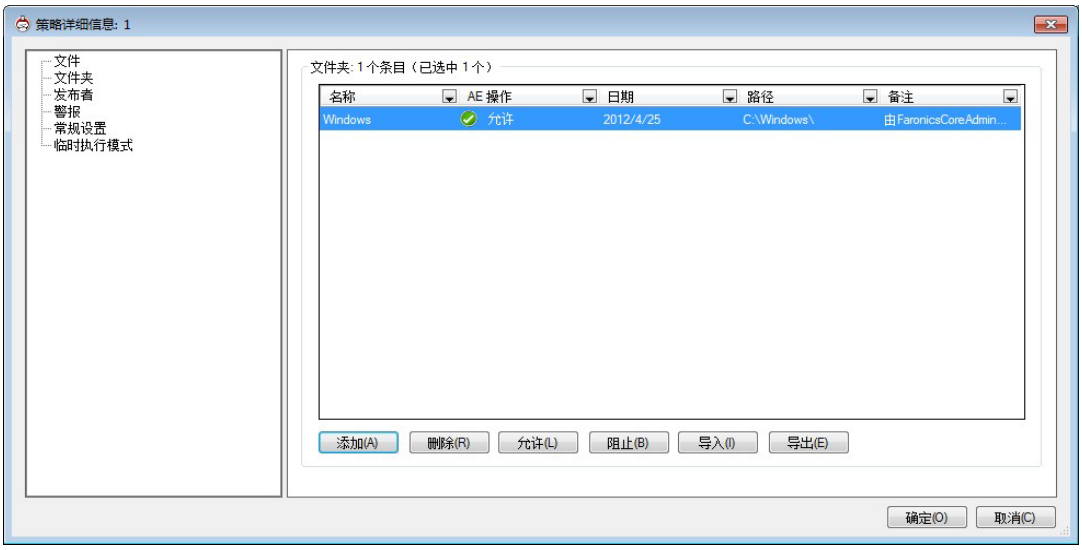
6. 单击*文件夹*节点，然后单击*添加*。



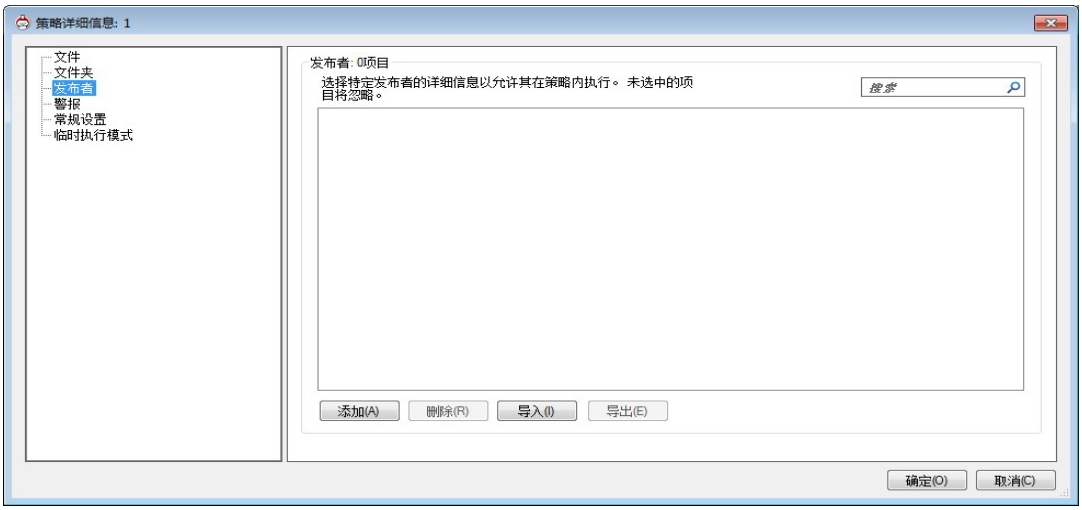
7. 浏览并在*添加文件夹到策略列表*对话框中选择文件夹。或者，您可以输入 UNC 路径。选择*使用自定义备注填充备注字段*并指定备注（可选）。单击*添加*。



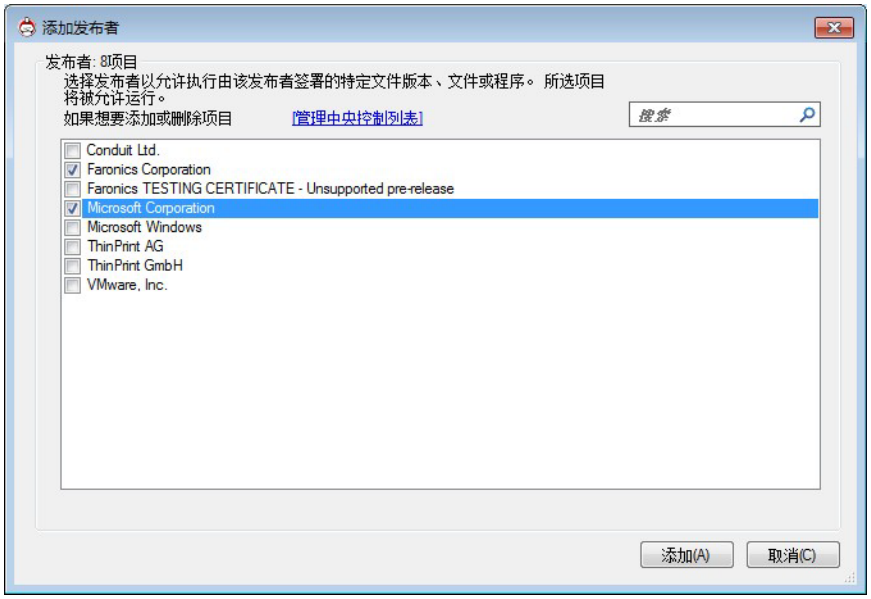
8. 文件夹 / 驱动器即已添加到策略。



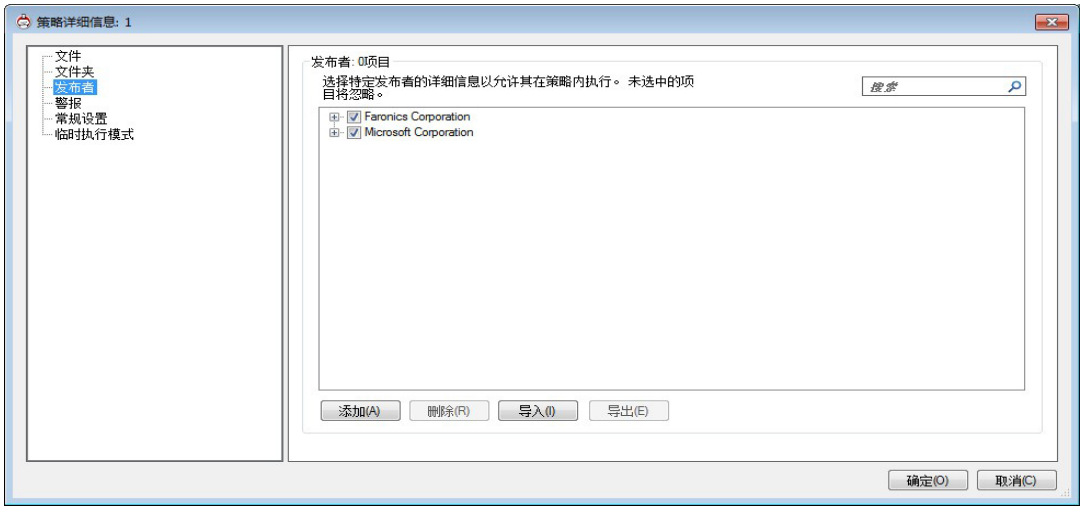
9. 单击*发行者*节点。单击*添加*。



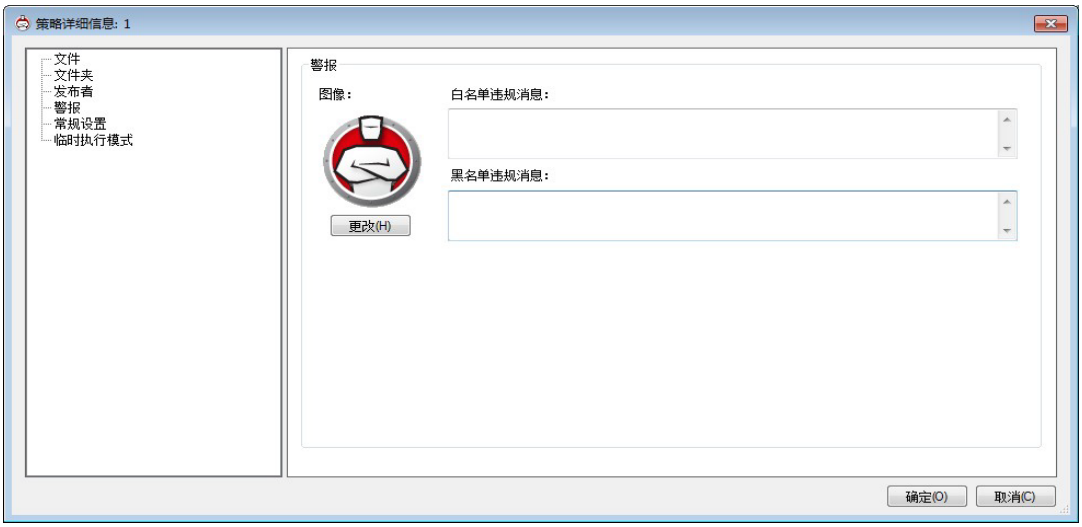
10. 选择已添加到中央控制列表的发行者，然后单击*添加*。



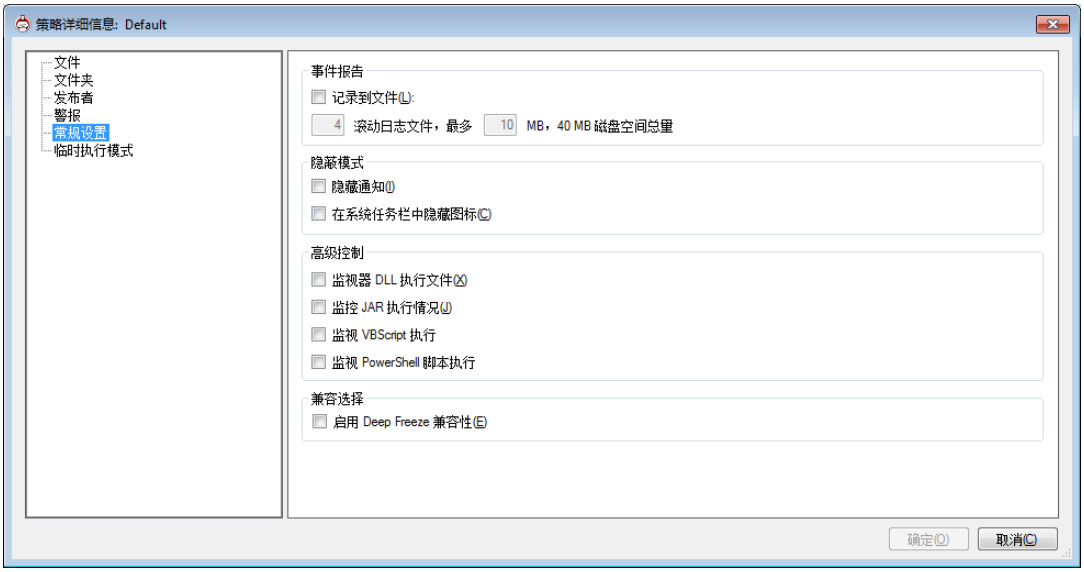
11. 发行者即已添加。选择*发行者*的顶部节点以添加所有子节点，或者选择子节点。



12. 单击*警报*节点。单击*更改*以更改向用户显示的图片。您还可以编辑*执行控制列表违规消息*和*被阻止的通知消息*。



13. 单击*常规设置*节点。配置下列设置：



- 事件报告 – 选择*记录到文件*以将事件记录到日志文件。在 Windows 7 中，日志文件位于 *C:\ProgramData\Faronics\Storage Space\AEE*。
- 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。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。

- 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
- 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。

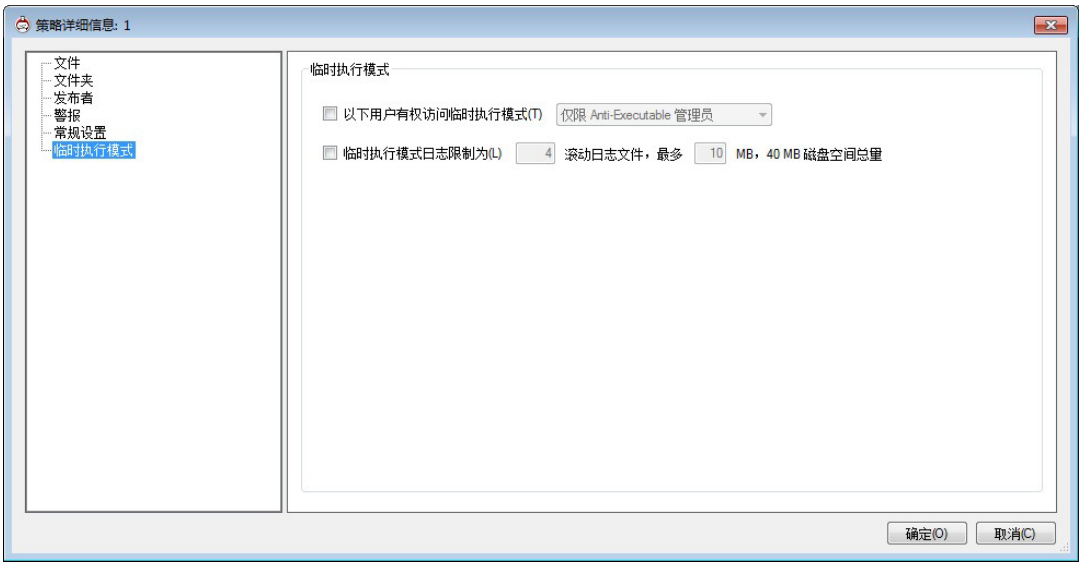
如果启用了 *Deep Freeze 兼容性*，但 Deep Freeze 处于*冻结*状态，则无法将 Anti-Executable 设为维护模式。原因在于重启计算机时对计算机所做的更改将丢失。

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。

14. 单击*临时执行模式*节点。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。



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 – 选中此复选框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 – 选中此复选框可在临时执行模式下创建日志文件。
  - 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。

15. 单击*确定*。该策略即已保存。

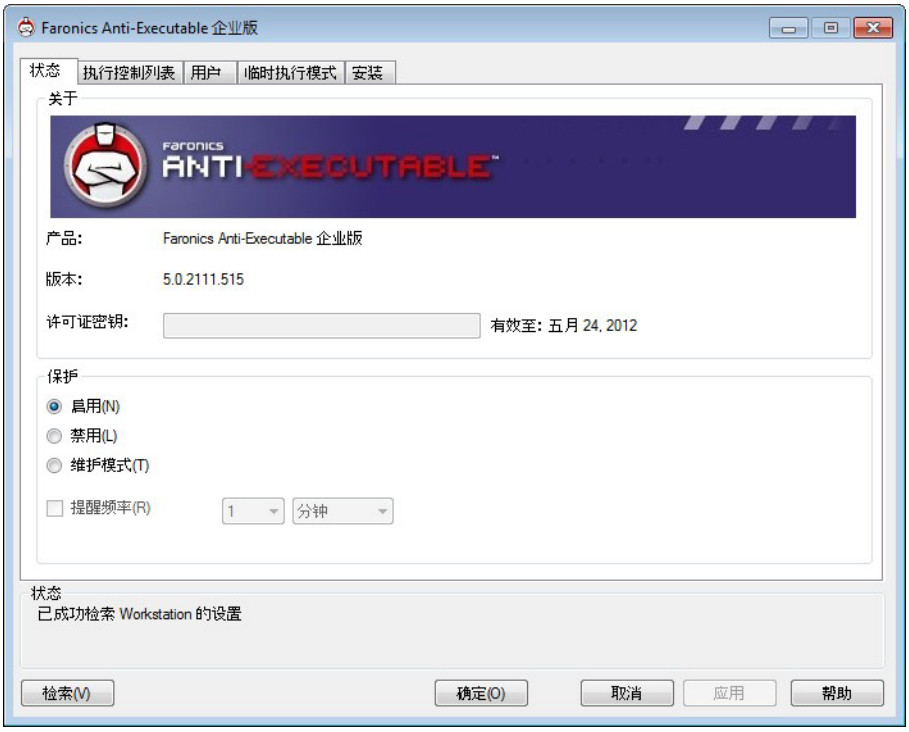
配置 Anti-Executable

右键单击单个工作站并选择*配置 Anti-Executable 客户端*。此时将从工作站检索 Anti-Executable 设置并显示下列选项卡：

- 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*。如果您在 Faronics Core Console 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。

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。

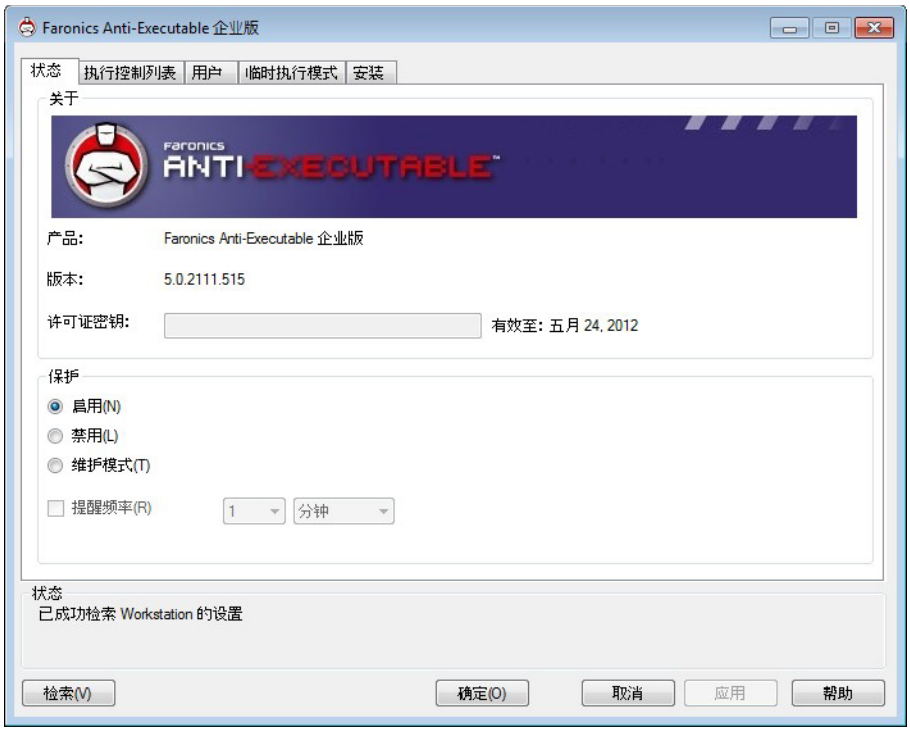
*禁用键盘和鼠标*复选框仅在通过 Faronics Core Console 访问 Anti-Executable 时才可用。这用于确保已禁用键盘和鼠标的计算机仍可通过 Faronics Core Console 远程管理。

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。

从 Faronics Core Console 检索设置

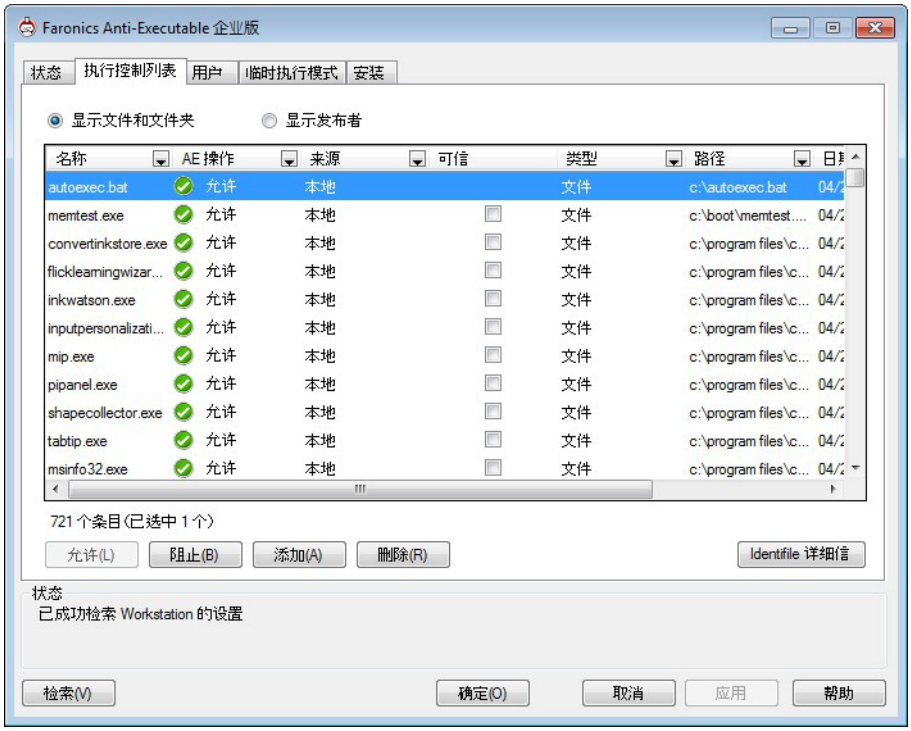
*状态*窗格检索并显示单个工作站的所有设置。选择一个工作站并通过 Faronics Core Console 启动 Anti-Executable 后，将自动检索工作站设置。



只有在选定了工作站的情况下才能检索状态。

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*本地控制列表或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。

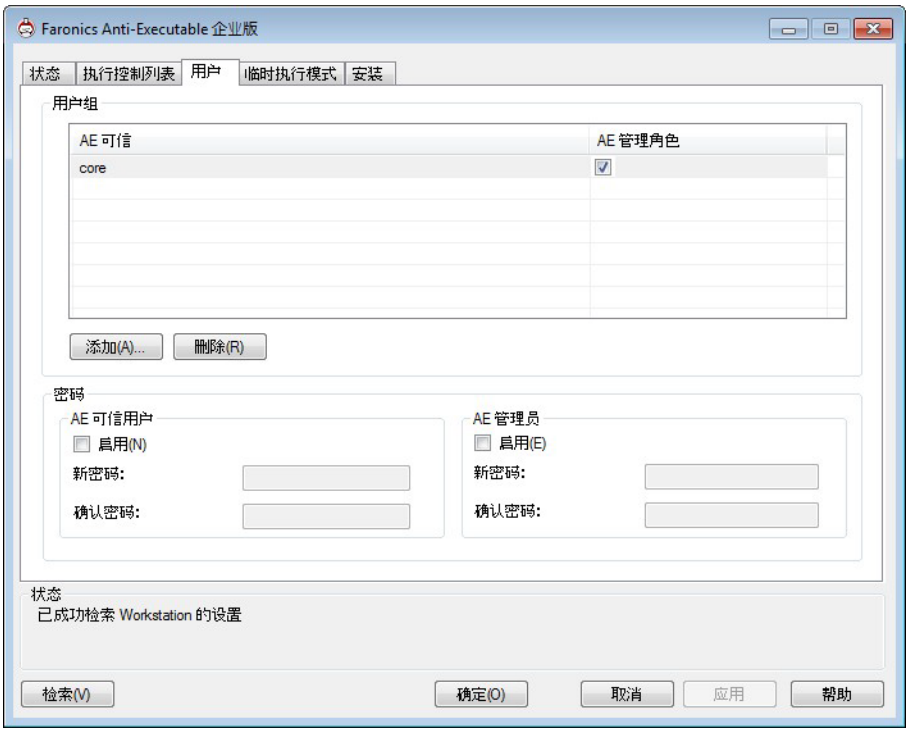
如果 Anti-Executable 管理员或受信任的用户尝试在已启用 Anti-Executable 的情况下打开未授权的应用程序，将显示*警报*对话框。

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。



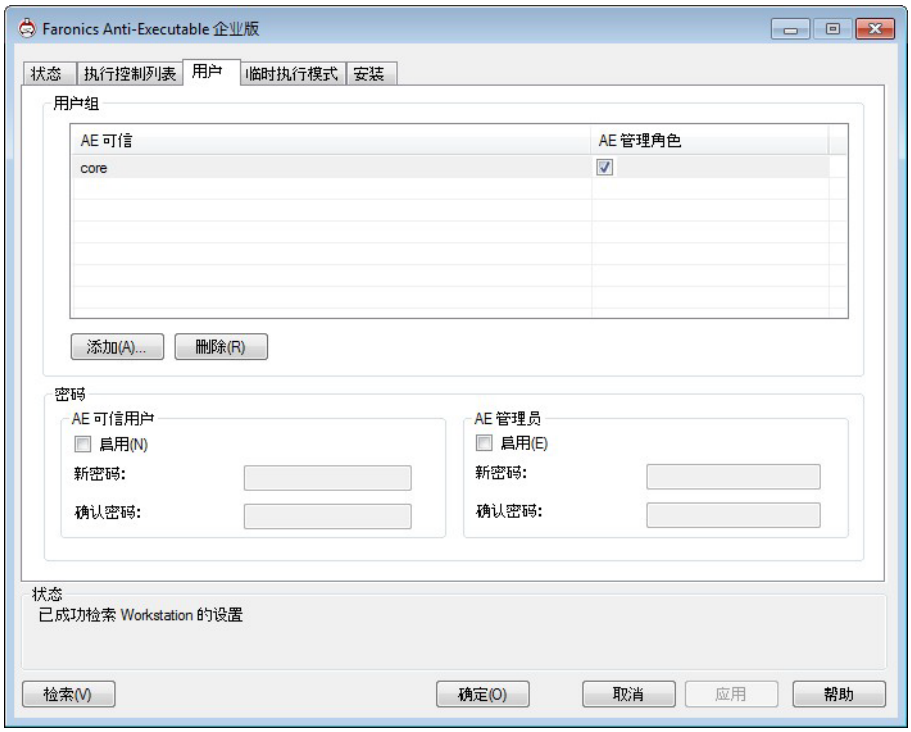
2. 单击*添加*以添加新用户。从提供的列表中选择*用户*图标。
3. 单击高级 > 立即查找以显示可用用户列表。Anti-Executable 管理员可添加域用户（或组）和本地用户 （或组）。单击用户或组以将其添加至 Anti-Executable 的列表中，然后单击确定。
4. 默认情况下，每个被添加的用户均为 Anti-Executable 受信任的用户。如果要赋予新用户管理权限，请选中 *Anti-Executable 管理角色*复选框，以将其指定为 Anti-Executable 管理员。

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

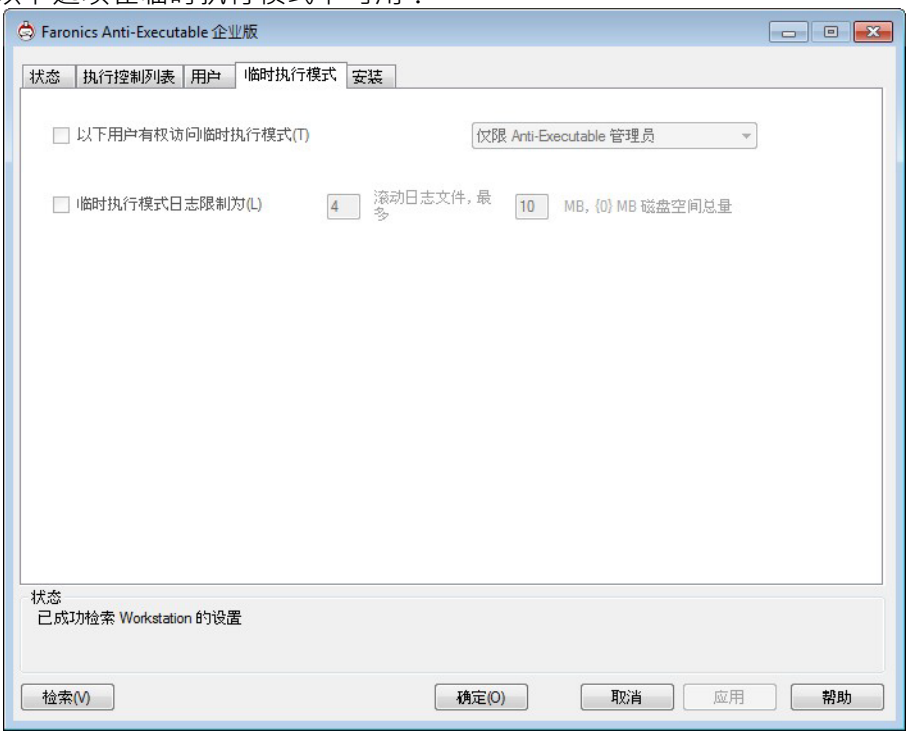
Anti-Executable 可以为每个用户组附加一个密码，作为一项额外的保护措施。密码只能应用于相关组的成员。要指定密码，请确保选中了*启用*复选框，然后在*新密码*和*确认密码*字段中输入密码。单击*应用*以保存更改。



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。不能修改*临时执行模式*选项卡中的设置，因此它们是策略的组成部分。

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

临时执行模式可通过以下方式激活：

从 Faronics Core：

- 激活临时执行模式：选择一个或多个工作站，然后选择 *Anti-Executable > 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：选择一个或多个工作站，然后选择 *Anti-Executable > 临时执行模式 > 禁用*

从工作站：

- 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*

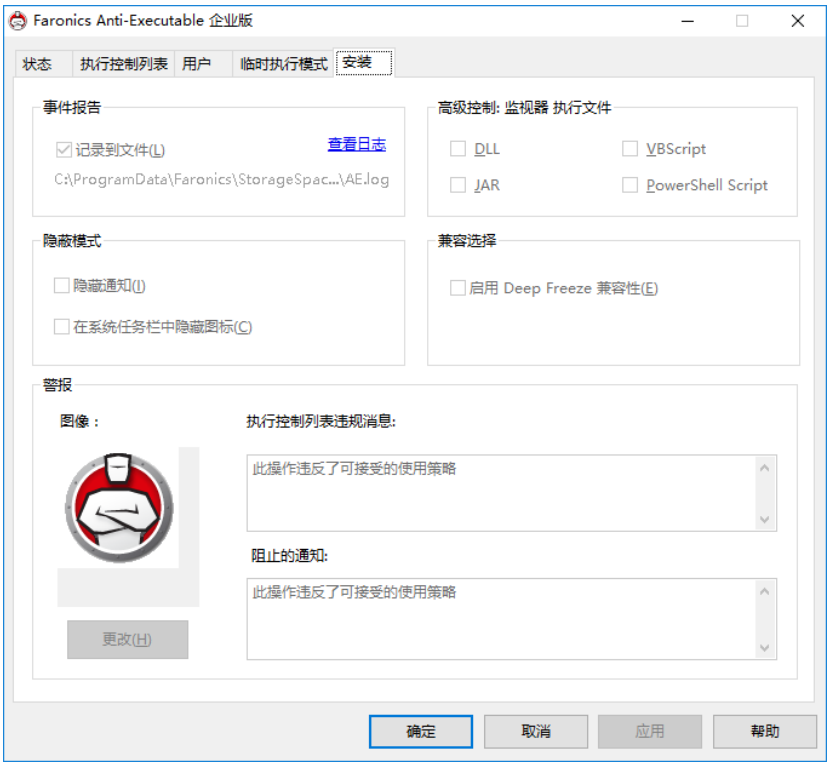
临时执行模式激活之后，工作站的系统任务栏将显示以下图标：

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。在 Windows 7 中，日志文件位于 *C:\ProgramData\Faronics\Storage Space\AEE*。

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

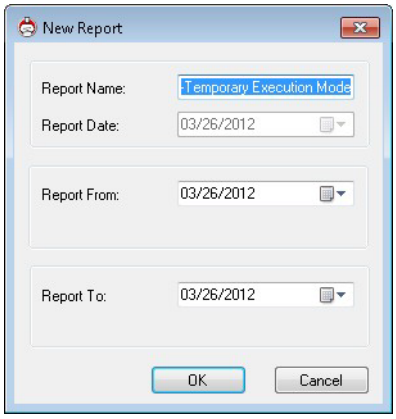
如下所示为警报对话框范例：

通过 Faronics Core Console 创建 Anti-Executable 报告

Anti-Executable 可提供以下报告：

- 活动报告 – 每个工作站的详细报告。
- 临时执行模式报告 – 临时执行模式期间启动的所有可执行程序的详细报告。
- 被拦截次数最多的程序
- 违规次数最多的计算机
- 全局报告：中央控制列表添加项 – 文件
- 全局报告：中央控制列表添加项 – 发行者
- 全局报告：本地执行列表添加项

要查看报告，请右键单击工作站并选择*生成报告 > [选择报告]*.：



- Anti-Executable 报告显示下列信息：
  - > 时间戳
  - > 机器信息
  - > 用户信息
  - > 事件 ID
  - > 描述
- 临时执行模式报告显示下列信息：
  - > 时间戳
  - > 文件名
  - > Hash

命令行控制

本章说明 Anti-Executable 可用的各种命令行控制。

主题

命令行控制

命令行控制

Anti-Executable 命令行控制允许通过第三方管理工具和 / 或中央管理解决方案对 Anti-Executable 实施控制，从而为网络管理员提供更高的 Anti-Executable 工作站管理灵活性。可用的命令如下：

使用 `/PW=<password>` 开关在已设置密码的计算机上执行命令。为管理员或信任的用户指定适用的密码。

`[ ]` 内的开关可选。

功能	命令
显示保护状态	[path]AEC status [/pw=<password>]
启用 Anti-Executable	[path]AEC Protect On [/pw=<password>]
禁用 Anti-Executable	[path]AEC Protect Off [/force] [/pw=<password>] 如果 Anti-Executable 处于维护模式，则必须使用开关 */force* 。
Anti-Executable 版本	[path]AEC version /PW=<password> 请注意，命令行界面不会显示许可证密钥（如果有），而用户界面会显示。
启用维护模式	[path]AEC Maintenance [/duration=<n>] [/lock] /PW=<password> 使用此命令时若不带任何开关，将启用维护模式。使用开关 `/duration=<n>` 可将维护模式启用 n 分钟。使用 `/lock` 开关将禁用键盘和鼠标。开关 `/lock` 必须与开关 `/duration=<n>` 一起使用。

功能	命令
更改 Anti-Executable 密码	[path]AEC changePassword <AEAdmin/AETrustedUser> /NEWPW=<New Password> [/pw=<Password>] 如果设定了密码，要更改密码，需要提供旧密码。
将文件夹或文件作为*允许*项添加到本地控制列表	[path]AEC allow <file or folder name and path> [/pw=<password>]
将文件夹或文件作为*阻止*项添加到本地控制列表	[path]AEC block <file or folder name and path> [/pw=<password>]
显示当前本地控制列表	[path] AEC displaylcl [/allowed] [/blocked] [/xml] [/pw=Password]
更新许可证密钥	[path]AEC updateLicense <License Key> /PW=<password>

说明

< 必须由用户输入 >

[用户可以选择输入]

[path]：被引用文件在磁盘上的存储位置

命令行示例

[path]AEC Protect On [/pw=<password>]

在上例中，[path] 是找到 Anti-Executable 命令行界面文件 (`AEC.exe`) 的路径。

卸载 Anti-Executable

主题

在工作站上通过 Faronics Core Console 卸载 Anti-Executable
使用安装程序卸载 Anti-Executable 插件

在工作站上通过 Faronics Core Console 卸载 Anti-Executable

Anti-Executable 可使用 Faronics Core Console 从一个或多个工作站中删除。要卸载 Anti-Executable，请执行以下步骤：

1. 打开 Faronics Core Console。
2. 单击 Faronics Core Console 左侧窗格中的*工作站*图标。
3. 右键单击*工作站列表*中要删除 Anti-Executable 的工作站。
4. 单击 *Anti-Executable > 卸载 Anti-Executable*。

从选定的工作站中卸载 Anti-Executable 后，Faronics Core Console 将重启工作站以完成卸载过程。

使用安装程序卸载 Anti-Executable 插件

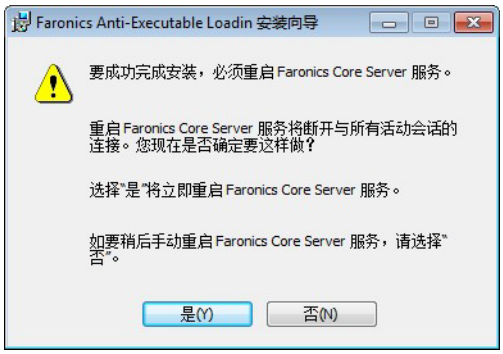
Anti-Executable 可以通过双击 *Anti-Executable_Console_Loadin_Installer.exe* 删除。此时将显示安装向导：

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*。

4. 单击*是*重启 Faronics Core Server 服务。单击*否*，稍后重启 Faronics Core Server 服务。



5. 单击*完成*。

卸载 Anti-Executable 插件（添加或删除程序）

Anti-Executable 插件可通过*添加/删除*程序卸载。为此，请单击*开始 > 控制面板 > 添加/删除程序 > Anti-Executable 插件 > 删除*。卸载 Anti-Executable 插件将删除 Faronics Core Console 中的所有 Anti-Executable 管理功能。此操作不会删除个别工作站上的 Anti-Executable 安装。