

Faronics
ANTI-VIRUS™

可靠的威胁防护

用户指南

Faronics™
Intelligent Solutions for ABSOLUTE Control

www.faronics.com



最近修改日期：2015 年 9月

© 1999 - 2015 Faronics Corporation。保留所有权利。Faronics、Deep Freeze、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

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 11

Faronics Anti-Virus 概述 12
系统要求 13
Faronics Anti-Virus 要求 13
Faronics Core 要求 13
Deep Freeze 要求 13
Faronics Anti-Virus 许可证 14

安装 Faronics Anti-Virus 15

安装概述 16
安装 Faronics Core 16
安装 Faronics Anti-Virus 插件 17
通过 Faronics Core 在工作站上安装或升级 Faronics Anti-Virus 20
在工作站上手动安装 Faronics Anti-Virus 21

使用 Faronics Anti-Virus 25

Faronics Anti-Virus 概述 26
通过 Faronics Core 控制台管理 Faronics Anti-Virus 27
在工作站上部署 Faronics Anti-Virus 客户端 27
配置 Faronics Anti-Virus 27
刷新 Faronics Anti-Virus 28
Faronics Anti-Virus 策略 30
创建 Anti-Virus 策略 30
应用 Anti-Virus 策略 54
查看或修改 Anti-Virus 策略 55
重命名 Anti-Virus 策略 55
导入 Anti-Virus 策略 55
导出 Anti-Virus 策略 55
复制策略 57
删除 Anti-Virus 策略 57
通过 Faronics Core 控制台扫描 58
查看隔离的文件并对其进行操作 59
查看 Faronics Anti-Virus 日志 61
通过 Faronics Core 控制台更新 Faronics Anti-Virus 65
通过 Faronics Core 控制台计划 Faronics Anti-Virus 的操作 66
生成报告 67
全局报告 67
特定工作站报告 67

在工作站上使用 Faronics Anti-Virus 68
在工作站上启动 Faronics Anti-Virus 68
扫描工作站 70
通过右键单击扫描文件或文件夹 72
查看扫描历史记录 72
查看隔离的文件并对其进行操作 73
在工作站上更新 Anti-Virus 定义 74
通过系统任务栏管理工作站上的 Faronics Anti-Virus 75

命令行控制 77

命令行控制 78

卸载 Faronics Anti-Virus 79

卸载概述 80
通过 Faronics Core 控制台卸载 Faronics Ant-Virus 客户端 81
通过 " 添加或删除程序 " 卸载工作站上的 Faronics Anti-Virus 客户端 82
使用安装程序卸载 Faronics Anti-Virus 插件 83
通过 " 添加或删除程序 " 卸载 Faronics Anti-Virus 插件 85

序言

本用户指南介绍如何安装和使用 Faronics Anti-Virus。

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。 Faronics 坚持以市场为中心推动技术创新，其产品广泛应用于教育机构、医疗机构、图书馆、政府部门以及各个企业。

产品文档

以下文档构成了 Faronics Anti-Virus 文档集：

- *Faronics Anti-Virus 用户指南* — 此文档将指导您如何使用该产品。
- *Faronics Anti-Virus 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。

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：1-800-943-6422 或 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

- 网址：www.faronics.com
- 电子邮件：sales@faronics.com
- 电话：1-800-943-6422 或 1-604-637-3333
- 传真：1-800-943-6488 或 1-604-637-8188
- 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（加拿大和国际）
  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
主动保护	主动保护 (AP) 是一种实时检测恶意程序的方法。AP 在您工作或浏览 Internet 时安静地驻守在后台，一直监视执行（运行）的文件而不会对您的系统造成显著的压力。
广告程序	广告程序（也称为广告软件）通常基于环境或行为发起攻击，并跟踪浏览习惯，以此达到显示与用户相关的第三方广告的目的。广告可采用几种形式，包括在网页或部分 Windows 界面内嵌入弹出广告、隐藏式弹出广告、横幅或链接。有些广告程序的广告可能包含在应用程序本身或侧边栏、搜索栏和搜索结果内显示的文本广告。
电子邮件保护	电子邮件保护是一种幕后工具，它可保护您的计算机不受可能有害的入站和出站电子邮件消息侵害。只要您启用了电子邮件保护功能，您无需进行任何操作，系统会通过自动电子邮件扫描功能扫描所有附件有无恶意程序和病毒，保护您的计算机。
隔离区	隔离区是指 Faronics Anti-Virus 在计算机上用于存储恶意程序或无法杀毒的受感染文件的安全位置。如果将某一项目存放到该位置后，您的计算机或计算机上的文件无法正常操作，您可以查看风险详细信息以进行进一步研究，并将其从隔离区删除，还原到其在计算机中原来的位置。您还可以从隔离区中永久删除该风险。
流氓安全程序	流氓安全程序是来源未知或可疑，或者价值不明的软件。流氓安全程序通常采取在网站或垃圾邮件中插入警告的形式，声称您的计算机已感染病毒，并提供扫描和清除服务。切勿信任这些警告。信誉良好的防病毒或防间谍软件公司绝不会使用这种*通知*方式。流氓安全程序看上去就如同普通的防病毒或防恶意软件程序一样，但它会试图诱骗或纠缠您购买该程序。有些流氓安全程序就像*万灵丹*推销员，号称功能强大，实际毫无价值；而其他一些程序则可能对计算机造成实质危害，它们可能会安装恶意程序、甚或窃取您输入的信用信息导致身份盗用。此外，即使您已经知道这些警报是假的，您在关闭或删除它们时仍需加倍小心。
Rootkit	Rootkit 是可以隐藏文件和数据的存在，使其逃避检测，并可使攻击者在用户不知情的情况下控制计算机的软件。恶意程序（包括病毒、间谍软件、特洛伊木马和后门程序）常利用 Rootkit 将自己隐藏起来，以免被用户和恶意程序检测软件（例如，防病毒和防间谍软件应用程序）发现。某些广告程序的应用程序和 DRM（数字版权管理）程序也会利用 Rootkit 阻止用户删除不需要的软件。
防火墙	防火墙可以提供双向防护，同时限制入站和出站流量，从而保护您的网络免受非法入侵。
间谍软件	间谍软件会在您不知情的情况下将信息传送给第三方。它也称为跟踪软件、劫持软件、变脸软件、监控软件和盗窃软件。某些隐私权保护拥护者甚至将合法的访问控制、过滤、Internet 监控、密码恢复、安全保护和监视软件称为*间谍软件*，因为这些软件无需通知用户即可使用。

术语	定义
特洛伊木马	特洛伊木马采用虚假或欺骗性质的伪装手段，通常在未经用户完全了解和同意的情况下安装到计算机。换句话说，它对用户显示为完全无害的内容可能包含恶意代码，实际上是有害的。大多数特洛伊木马都表现出某种形式的恶意、敌意或有害的功能或行为。
病毒	计算机病毒是一段恶意代码，它能够自我复制并侵入其他程序或文件，在受感染的计算机内传播。病毒通常在用户执行受感染的文件或加载受感染的媒体，尤其是可移动媒体（例如，CD-ROM 或闪存驱动器）时进行传播。病毒还可以通过电子邮件中受感染的附件和文件进行传播。从进行骚扰、干扰，到造成危害和损坏，大多数病毒都具有*恶意攻击行为*；病毒可导致系统损坏、造成宝贵数据的丢失或被用于安装其他恶意程序。
蠕虫	蠕虫是一种恶意程序，它可以无需任何用户干预而进行自我传播。蠕虫与病毒的相似之处在于二者都可自我复制。不过，与病毒不同的是，蠕虫传播时不会附加到或感染其他程序和文件。蠕虫可通过连接至网络的、易受攻击的计算机上的安全漏洞跨计算机网络进行传播。蠕虫还可以通过使用电子邮件将本身的副本发送给用户通讯录中的所有人来传播。蠕虫可消耗大量的系统资源，导致计算机运行严重缓慢和不稳定。某些蠕虫可用于危害受感染的计算机和下载其他恶意软件。



简介

Faronics Anti-Virus 保护计算机不受安全风险攻击，并且不会因为慢速扫描时间和占用大量资源而降低计算机速度。采用下一代技术构建的 Faronics Anti-Virus 集强大的防病毒、防 Rootkit 和防间谍软件于一体，可保护您不受现今高度复杂的恶意软件侵害，同时与 *Faronics Deep Freeze* 和 *Faronics Anti-Executable* 无缝集成，构成完整的分层安全解决方案。

主题

Faronics Anti-Virus 概述

系统要求

Faronics Anti-Virus 许可证

Faronics Anti-Virus 概述

Faronics Anti-Virus 可保护工作站免受以下威胁：

- 广告程序
- 流氓安全程序
- Rootkit
- 间谍软件
- 特洛伊木马
- 蠕虫

Faronics Anti-Virus 可通过 Faronics Core 在多个工作站上进行部署。有关 Faronics Core 的信息，请参阅 Faronics Core 用户指南。最新的用户指南可在网站 http://www.faronics.com/library 上获得。

装有 Deep Freeze 时，可在托管工作站上更新 Anti-Virus 定义而无需*重启后 Thawed* 或在 *Maintenance Mode* 下重启。有关详细信息，请参阅 Deep Freeze Enterprise 用户指南。最新的用户指南可在网站 http://www.faronics.com/library 上获得。

系统要求

Faronics Anti-Virus 要求

Faronics Anti-Virus 插件要求如下：

- Faronics Core 3.7 或更高版本

工作站上的 Faronics Anti-Virus 客户端要求以下任意操作系统：

- Windows XP SP3 （32 位）或 Windows XP SP2 （64 位）
- Windows Vista SP2 （32 位或 64 位）
- Windows 7 （32 位或 64 位）
- Windows 8.1 （32 位或 64 位）
- Windows 10 （32 位或 64 位）
- Windows Server 2003 （32 位或 64 位）
- Windows Server 2008 R2 （64 位）
- Windows Server 2012 （64 位）

强烈建议所有组件都使用 Windows 管理员帐户进行安装。

Faronics Core 要求

有关 Faronics Core 系统要求的信息，请参阅 Faronics Core 用户指南。最新的用户指南可在网站 http://www.faronics.com/library 上获得。

Deep Freeze 要求

有关 Deep Freeze 系统要求的信息可在 Deep Freeze Enterprise 用户指南中找到。最新的用户指南可在网站 http://www.faronics.com/library 上获得。



要在 Deep Freeze 管理的工作站上运行 Faronics Anti-Virus，需要 Deep Freeze Enterprise 7.0 或更高版本。

Faronics Anti-Virus 许可证

Faronics Anti-Virus 许可证可通过 Faronics Core 控制台应用。要应用 Faronics Anti-Virus 许可证，请完成以下步骤：

1. 启动 Faronics Core 控制台。
2. 右键单击 *Core 服务器*并选择*属性*。
3. 单击 *Anti-Virus* 选项卡。 Anti-Virus 选项卡显示*版本*、*许可证密钥*（如果是许可版本）和*许可证过期*信息。
4. 单击*编辑*并在*许可证密钥*字段中输入*许可证密钥*。
5. 单击*应用*。单击*确定*。



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



如果 Faronics Anti-Virus 许可证密钥已过期，则无法下载病毒定义。

Faronics Anti-Virus 许可证的工作原理如下：

• Core 服务器（Faronics Core 的一个组件）自动将许可证密钥推送到安装了 Faronics Anti-Virus 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。

• 在工作站中，无法手动编辑许可证密钥。

安装 Faronics Anti-Virus

本章介绍如何安装 Faronics Anti-Virus。

主题

安装概述
安装 Faronics Anti-Virus 插件
通过 Faronics Core 在工作站上安装或升级 Faronics Anti-Virus
在工作站上手动安装 Faronics Anti-Virus

安装概述

Faronics Anti-Virus 包含两个组件：

- Faronics Anti-Virus 插件 - 在装有 Faronics Core 的计算机上安装。
- Faronics Anti-Virus 客户端 - 在将由 Faronics Anti-Virus 插件管理的工作站上进行部署。

Faronics Anti-Virus 的安装和配置包括以下步骤：

- 安装 Faronics Core 并生成 / 部署 Core Agent
- 安装 Faronics Anti-Virus 插件
- 部署 Faronics Anti-Virus 客户端

安装 Faronics Core

有关安装 Faronics Core 及生成和部署 Core Agent 的信息，请参阅 Faronics Core 用户指南。最新的用户指南可在网站 http://www.faronics.com/library 上获得。

安装 Faronics Anti-Virus 插件

要安装 Faronics Anti-Virus 插件，请完成以下步骤：

Anti-Virus 插件无法安装到没有安装 Faronics Core 控制台(或 Faronics Core 服务器)的计算机中。

1. 双击 *Anti-VirusLoadinInstaller.exe*。单击 *下一步*。



2. 阅读并接受许可协议。单击 *下一步*。



3. 输入*用户名*、*组织*和*许可证密钥*。或者，选择*使用评估版*复选框。 Faronics Anti-Virus 将在 30 天的评估期后过期。单击*下一步*。



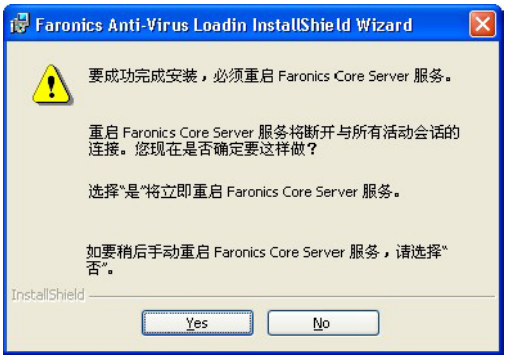
4. 默认位置为 *C:\Program Files\Faronics\Faronics Core 3\Loadins\Anti-Virus*。



5. 单击*安装*以安装 Faronics Anti-Virus 插件。



6. 此时将显示以下消息。单击*是*重启 Faronics Core 服务器服务。单击*否*在稍后手动重启 Faronics Core 服务器服务。



7. 单击*完成*结束安装。



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

Core Agent 是 Faronics Core 的一个组件，每个希望使用 Faronics Anti-Virus 管理的工作站都必须安装。有关安装 Core Agent 的详细信息，请参阅 Faronics Core 用户指南。最新的用户指南可在 http://www.faronics.com/library 上获得。

安装 Core Agent 后，即可在网络中检测到工作站，并可在 Core Console 中看到工作站。

要安装或升级 Faronics Anti-Virus，请选择一个或多个工作站：

1. 在右边窗格中单击 “ 配置工作站 ”，然后选择 *高级* > *安装 / 升级 Faronics Anti-Virus 客户端*。
2. 要安装另一个 Anti-Virus 程序，请选择以下选项：

- 安装 Faronics Anti-Virus Enterprise 工作站之前，请删除所有不兼容的 Anti-Virus 产品。
- 即使存在另一个 Anti-Virus 产品或无法将其删除，也要安装 Faronics Anti-Virus。



成功安装或升级后，工作站会重新启动。



如果安装了多个插件，可右键单击工作站，选择 *Anti-Virus*，访问 Faronics Anti-Virus 的右键上下文菜单，然后选择特定的操作。

在工作站上手动安装 Faronics Anti-Virus

在工作站上安装 Faronics Anti-Virus 客户端之前，从计算机上安装 Anti-Virus 插件的路径 *C:\Program Files\Faronics\Faronics Core 3\Loadins\Anti-Virus\Wks Installers* 复制相应的 *.msi* 文件到一个或多个工作站。

对将通过 Faronics Anti-Virus 进行保护的每个工作站重复此过程。

要在工作站上安装 Faronics Anti-Virus，请完成以下步骤：

1. 双击 *AntiVirus_Ent_32-bit.msi*（如为 32 位操作系统）和 *AntiVirus_Ent_64-bit.msi*（如为 64 位操作系统）。单击 *下一步*。



2. 要安装另一个 Anti-Virus 程序，请选择以下选项：

- 安装 Faronics Anti-Virus Enterprise 工作站之前，请删除所有不兼容的 Anti-Virus 产品。
- 即使存在另一个 Anti-Virus 产品或无法将其删除，也要安装 Faronics Anti-Virus。

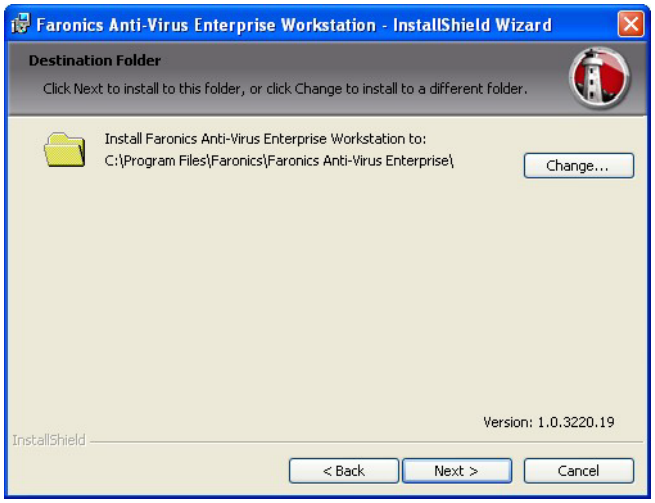
3. 阅读并接受许可协议。单击 *下一步*。



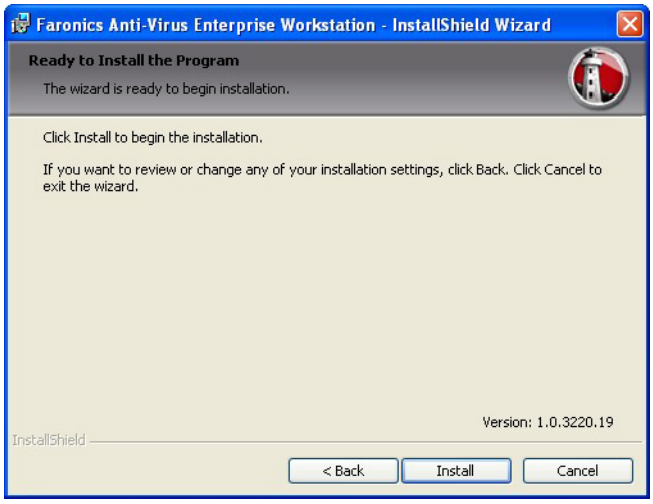
4. 输入*用户名*和*组织*。单击 *下一步*。



5. 默认位置为 *C:\Program Files\Faronics\Faronics Anti-Virus Enterprise*。单击*更改 ...* 以更改 Faronics Anti-Virus 的安装位置。单击 *下一步*。



6. 单击*安装*安装 Faronics Anti-Virus。



7. 单击*完成*结束安装。



在工作站上安装 Anti-Virus 客户端后建议您立即重启计算机。



使用 Faronics Anti-Virus

本章说明如何使用 Faronics Anti-Virus。

主题

Faronics Anti-Virus 概述
通过 Faronics Core 控制台管理 Faronics Anti-Virus
Faronics Anti-Virus 策略
通过 Faronics Core 控制台扫描
查看隔离的文件并对其进行操作
通过 Faronics Core 控制台更新 Faronics Anti-Virus
生成报告
在工作站上使用 Faronics Anti-Virus
通过系统任务栏管理工作站上的 Faronics Anti-Virus

Faronics Anti-Virus 概述

Faronics Anti-Virus 可通过以下方式使用：

通过 Faronics Core 控制台管理 Faronics Anti-Virus：

- 安装 Faronics Anti-Virus 插件（有关详细信息，请参阅*安装 Faronics Anti-Virus 插件*）
- 在工作站上部署 Faronics Anti-Virus 客户端
- 创建、编辑、删除和应用 Anti-Virus 策略
- 通过 Faronics Core 控制台扫描工作站
- 查看隔离的文件并对其进行操作
- 通过 Faronics Core 控制台更新 Anti-Virus 定义
- 生成报告

在工作站上使用 Faronics Anti-Virus

- 在工作站上启动 Faronics Anti-Virus
- 扫描工作站
- 在工作站上更新 Anti-Virus 定义。

通过 Faronics Core 控制台管理 Faronics Anti-Virus

一旦安装 Faronics Anti-Virus 插件后，即可通过 Faronics Core 控制台管理工作站。有关通过 Faronics Core 控制台管理 Faronics Anti-Virus 的各方面内容将在后面的章节中说明。

在工作站上部署 Faronics Anti-Virus 客户端

要在工作站上部署 Faronics Anti-Virus 客户端，请完成以下步骤：

1. 启动 Faronics Core 控制台。
2. 在 “ 控制台树 ” 窗格中，依次转至 *Faronics Core 控制台* >*[Core 服务器名称]*> *工作站* > *托管工作站*。
3. 右键单击一个或多个工作站，然后依次选择 *配置工作站* > *高级* > *安装 / 升级 Anti-Virus 客户端*。

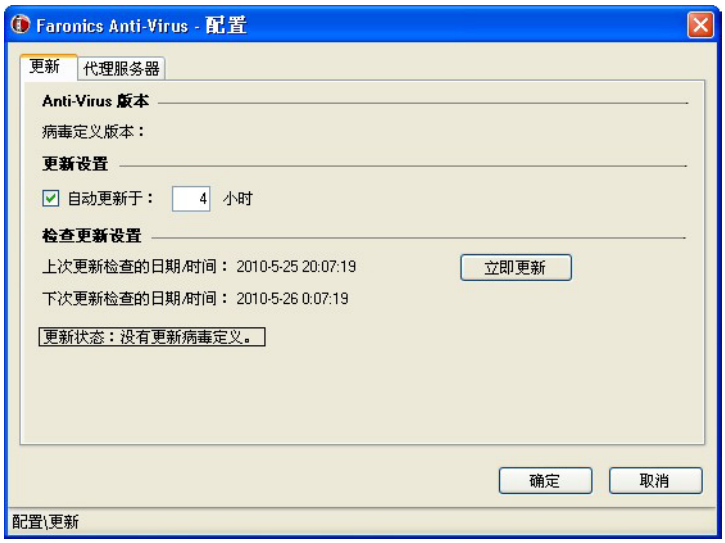
此时将在工作站上安装 Faronics Anti-Virus 客户端。

成功部署后，工作站拥有默认策略和最新的病毒定义。

配置 Faronics Anti-Virus

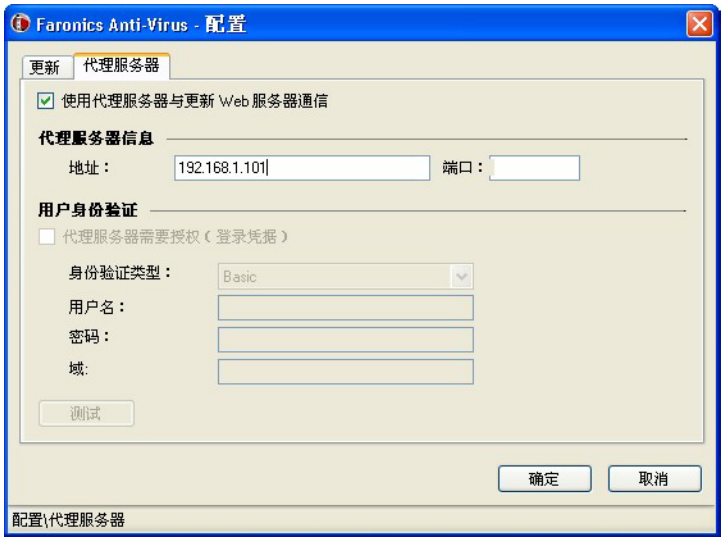
要配置 Faronics Anti-Virus，请完成以下步骤：

1. 启动 Faronics Core 控制台。
2. 在 “ 控制台树 ” 窗格中，依次转至 *Faronics Core 控制台* >*[Core 服务器名称]*> *工作站* > *托管工作站* >*Anti-Virus*。
3. 右键单击 Anti-Virus，然后选择*配置 Anti-Virus*。
4. 此时将显示 “ 配置 Faronics Anti-Virus” 对话框，其中包含 “ 更新 ” 选项卡。
5. “ 更新 ” 选项卡会显示扫描引擎版本和病毒定义版本。请指定以下选项：



- *自动更新频率（按小时计）* - 选中该复选框以自动更新病毒定义。
- *小时* - 指定介于 1 到 72 小时之间的值。
- *立即更新* - 单击此按钮以更新 Anti-Virus 定义。

6. 单击 “ 代理服务器 ” 选项卡并指定以下选项的值：



7. 选择 “ 使用代理服务器与更新 Web 服务器通信 ”，然后指定以下信息：

- *地址* - 指定 IP 地址或 URL。
- *端口* - 指定端口。

8. 选择代理服务器与更新 Web 服务器通信的用户，然后指定以下设置：

- *身份验证类型*
- *用户名*
- *密码*
- *域*

9. 单击*测试*以测试连接。单击测试以测试连接。单击确定以保存代理设置。

刷新 Faronics Anti-Virus

要从运行 Faronics Anti-Virus 的一个工作站检索设置，请完成以下步骤：

1. 启动 Faronics Core 控制台。
2. 在 “ 控制台树 ” 窗格中，依次转至 *Faronics Core 控制台 >[Core 服务器名称]> 工作站 > 托管工作站*。
3. 右键单击一个工作站，然后选择*刷新 Anti-Virus*。
4. 此时将刷新 Faronics Anti-Virus 并更新以下各列：

- 策略名称
- 状态

- % 扫描已完成
- 定义版本
- 上次更新的日期
- 上次扫描的日期
- 上次检测到威胁的日期
- 版本

Faronics Anti-Virus 策略

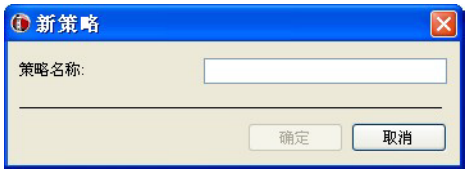
Anti-Virus 策略包含所有与 Faronics Anti-Virus 在工作站上运行方式相关的配置设置。策略包含程序进行的操作、计划、代理服务器、错误报告以及工作站上用户可执行的功能。以下各节说明如何创建和应用 Anti-Virus 策略。

Faronics Anti-Virus 包含一个*默认*策略。该默认策略包含管理 Faronics Anti-Virus 的最佳配置设置。

创建 Anti-Virus 策略

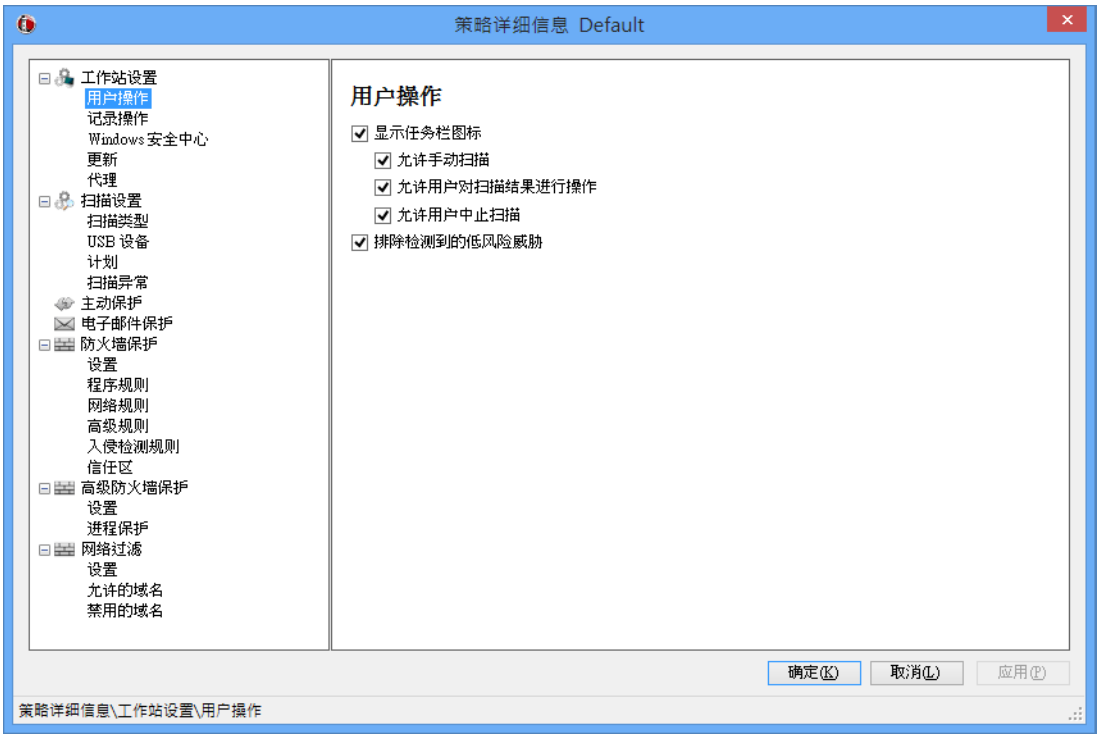
要新建一个 Anti-Virus 策略，请完成以下步骤：

1. 启动 Faronics Core 控制台。
2. 在*控制台树窗格*中，依次转至 *Faronics Core 控制台* >*[Core 服务器名称]*> *工作站* > *托管工作站* >*Anti-Virus*。
3. 右键单击 *Anti-Virus*，然后选择*新建策略*。
4. 在*新建策略*对话框中指定策略的名称。单击*确定*。新策略将在 *Anti-Virus* 节点策略下创建。例如，您可以将新策略命名为 *New Policy 1*。



5. 右键单击 *New Policy 1*，然后选择*策略详细信息*。此时将显示*策略详细信息*对话框。
6. 指定*工作站设置*节点中的设置：

- *工作站设置*节点 > *用户操作*窗格



— *显示任务栏图标* - 选中该复选框以在工作站的任务栏中显示 Faronics Anti-Virus 图标。如果没有选中此复选框，则 Faronics Anti-Virus 将对用户隐藏。

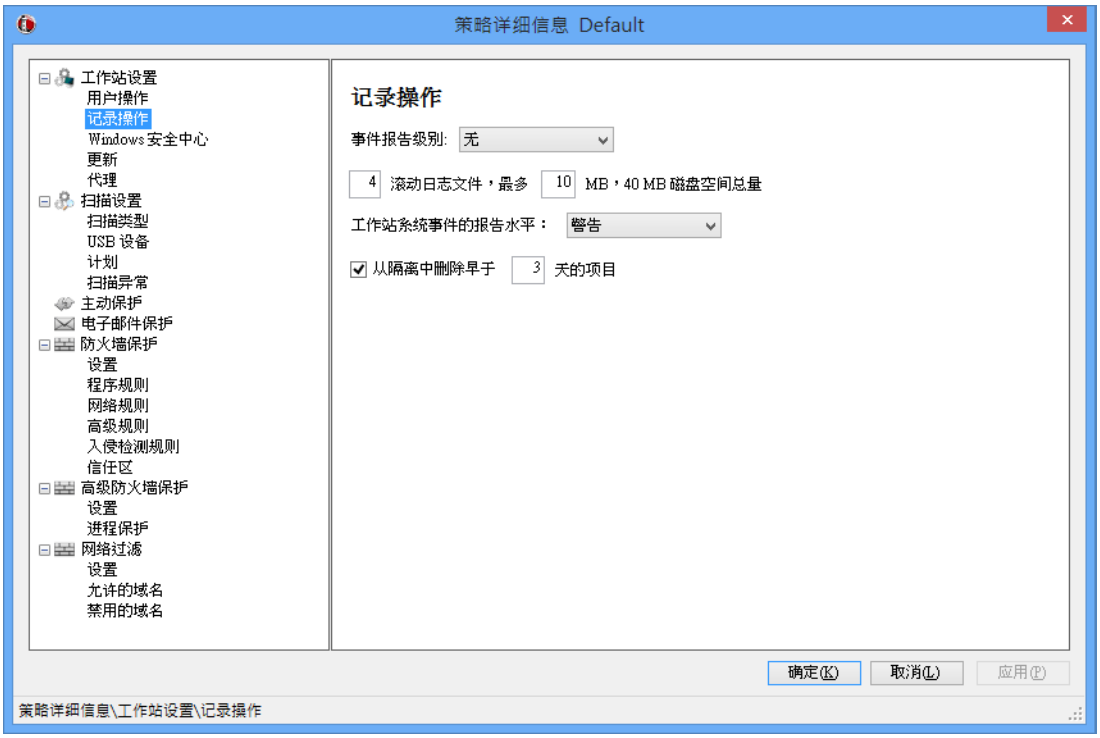
— *允许手动扫描* - 选中该复选框以允许用户手动启动工作站的 Faronics Anti-Virus 扫描。

— *允许用户对扫描结果进行操作* - 选中该复选框以允许工作站用户对扫描结果进行操作。

— *允许用户中止本地启动扫描* - 选中该复选框可让用户中止在工作站本地启动的扫描。

— *排除检测到的低风险威胁* - 选中该复选框以排除检测到的低风险威胁。低风险威胁是指不会对系统产生不良影响的威胁（例如，Cookie）。

- *工作站设置节点 > 记录操作*



— *日志记录级别* - 选择日志记录级别。选择*无*不记录日志。选择*错误*记录错误消息。选择*跟踪*以进行跟踪。选择*详细*以详细记录。

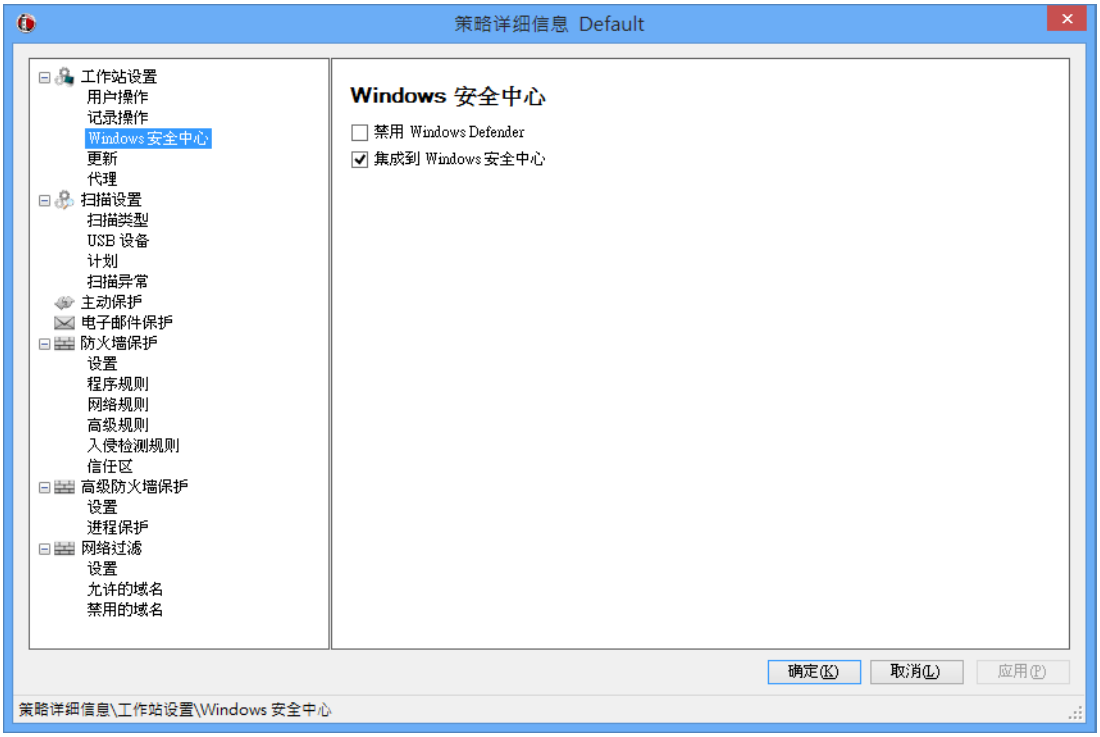
— *日志记录文件数* - 指定日志记录文件的数目。日志记录信息按顺序存储到文件。例如，如果指定了 3 个文件 A、B 和 C，则 Faronics Anti-Virus 首先将错误日志写入到文件 A。如果文件 A 已满，则开始写入到文件 B，最后写入到文件 C。一旦文件 C 已满，将删除文件 A 中的数据，并写入新的日志记录数据。

— *文件大小* - 选择每个文件的大小（以 MB 为单位）。

— *工作站系统事件报告级别* - 选择“无”、“错误”、“警告”或“信息”。

— *从隔离区中删除早于以下时间的项目* - 指定项目在隔离区中保留的天数。默认为 3 天。

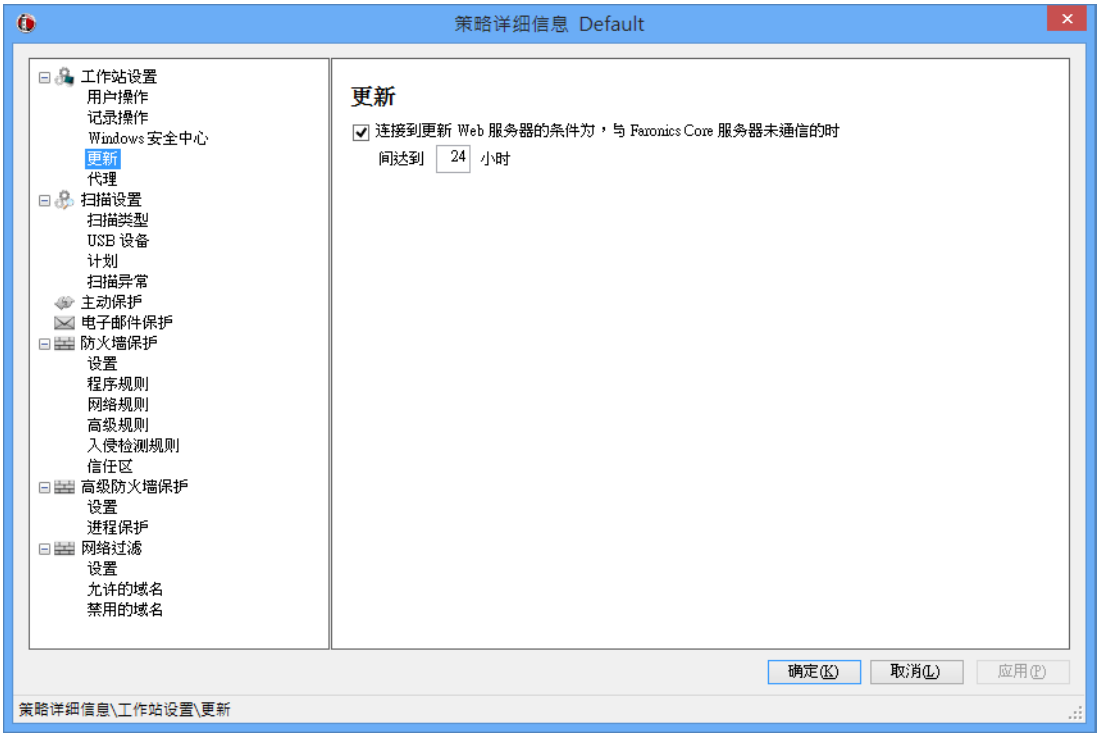
- *工作站设置*节点 >*Windows 安全中心*窗格



— *禁用 Windows Defender* - 选中该复选框以禁用 Windows Defender。这可避免 Faronics Anti-Virus 与 Windows Defender 之间可能的冲突。运行多个防病毒或防间谍软件程序时，一个程序可能会将其它程序误认作病毒或间谍软件，从而产生冲突。此外，运行多个防病毒或防间谍软件程序可能会增加处理器的工作负荷和内存占用率。不过，如果您希望运行 Windows Defender，您可以选择不禁用它。

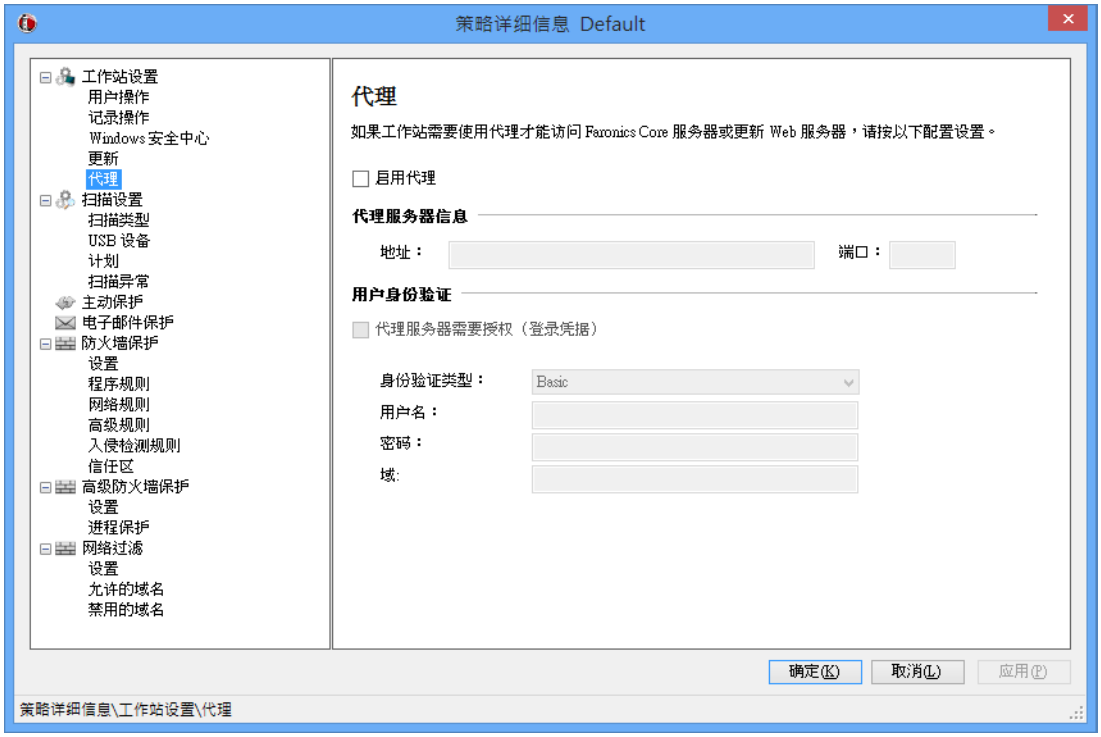
— *集成到 Windows 安全中心* - 选中该复选框以将 Faronics Anti-Virus 集成到 Windows 安全中心。 Windows 安全中心将通过系统任务栏通知您 Faronics Anti-Virus 是否处于活动状态。

- 工作站设置节点 > 更新窗格
  - *如果 x 小时内未与 Faronics Core 服务器通信，连接到更新 Web 服务器*：选中该复选框以连接到更新 Web 服务器并下载病毒定义（如果工作站与 Faronics Core Server 失去连接）。如果您没有选中此复选框，则工作站与 Faronics Core Server 失去连接时不会更新病毒定义。
- 工作站设置节点 > 代理窗格



- *启用代理* - 如果工作站需要代理访问 Faronics Core Server 或更新 Web 服务器，则选中该复选框。指定*地址*和*端口*。
- *代理服务器需要授权（登录凭据）* - 如果服务器需要身份验证，请指定以下字段的值：
- *身份验证类型* - 选择身份验证类型。
  - *用户名* - 指定用户名。
  - *密码* - 指定密码。
  - *域* - 指定域。

7. 指定*扫描*节点中的设置：



- *扫描*节点 > *扫描设置*窗格 - 选择以下各项用于快速扫描、深度系统扫描和自定义扫描：

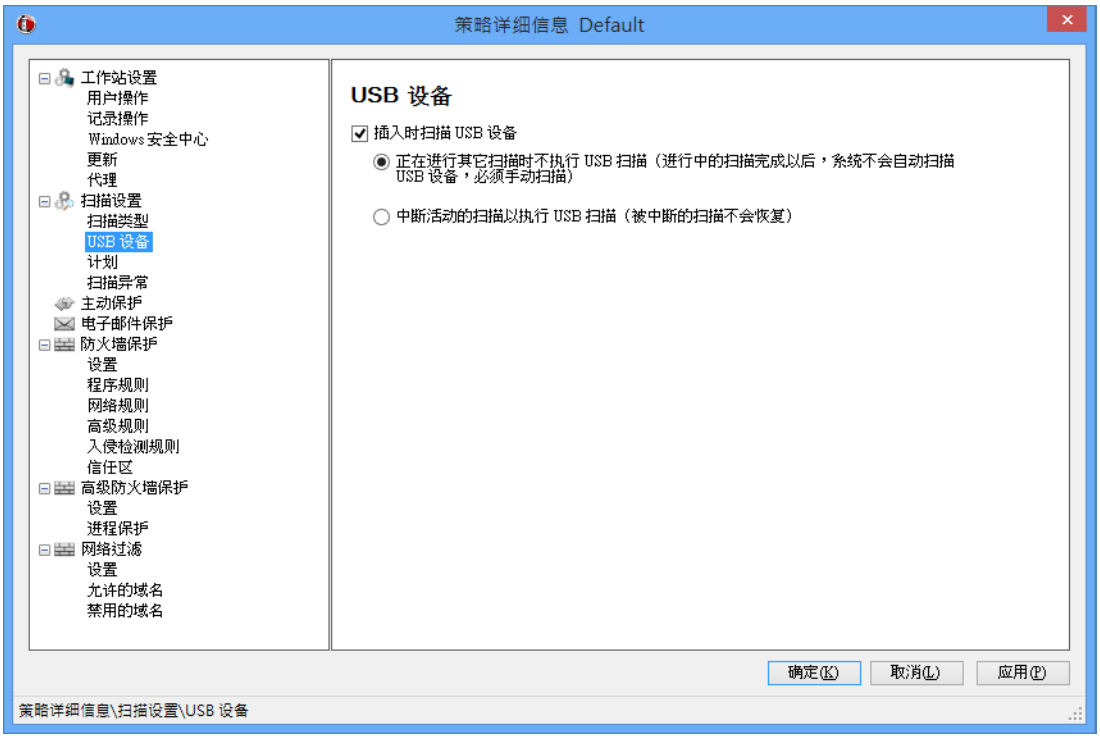
Faronics Anti-Virus 提供三种类型的扫描：

- *快速扫描* - 扫描计算机中容易受影响的区域。快速扫描比深度系统扫描持续时间短，使用的内存更少。
- *深度系统扫描* - 对计算机的所有区域进行全面扫描。这类扫描所花的时间取决于您的硬盘驱动器大小。
- *自定义扫描* - 基于*策略详细信息*对话框中所做的选择进行扫描。

为每种类型的扫描选择以下选项（视扫描类型的不同，某些选项可能会灰显，无法使用）：

- *启用 Rootkit 检测* - 检测计算机是否感染 Rootkit。
- *扫描压缩包* - 扫描 zip 文件中的内容。选中该选项，在扫描时扫描压缩文件（例如，.RAR 和 .ZIP 文件）。当发现 .RAR 文件内包含受感染的文件时，将隔离该 .RAR 文件。如果发现 .ZIP 文件内包含受感染的文件，则受感染的文件会被隔离，并替换为一个说明该文件受到感染而已被隔离的 .TXT 文件。
- *优先级较低的扫描* - 选择以较低的优先级运行 Faronics Anti-Virus，以便您能够继续使用其他程序而不会降低性能。对在计算机正常使用期间发生的计划扫描，最好选择此选项。
- *排除可移动驱动器（例如，USB）* - 从扫描进程中排除可移动驱动器。此时将不会扫描任何外部硬盘、 USB 驱动器等。
- *扫描 Cookie* - 扫描工作站上保存的 Cookie。
- *扫描注册表* - 扫描注册表。

- *扫描正在运行的进程* - 扫描所有正在运行的进程。
- 扫描节点 > USB 设备窗格 - 指定以下设置：

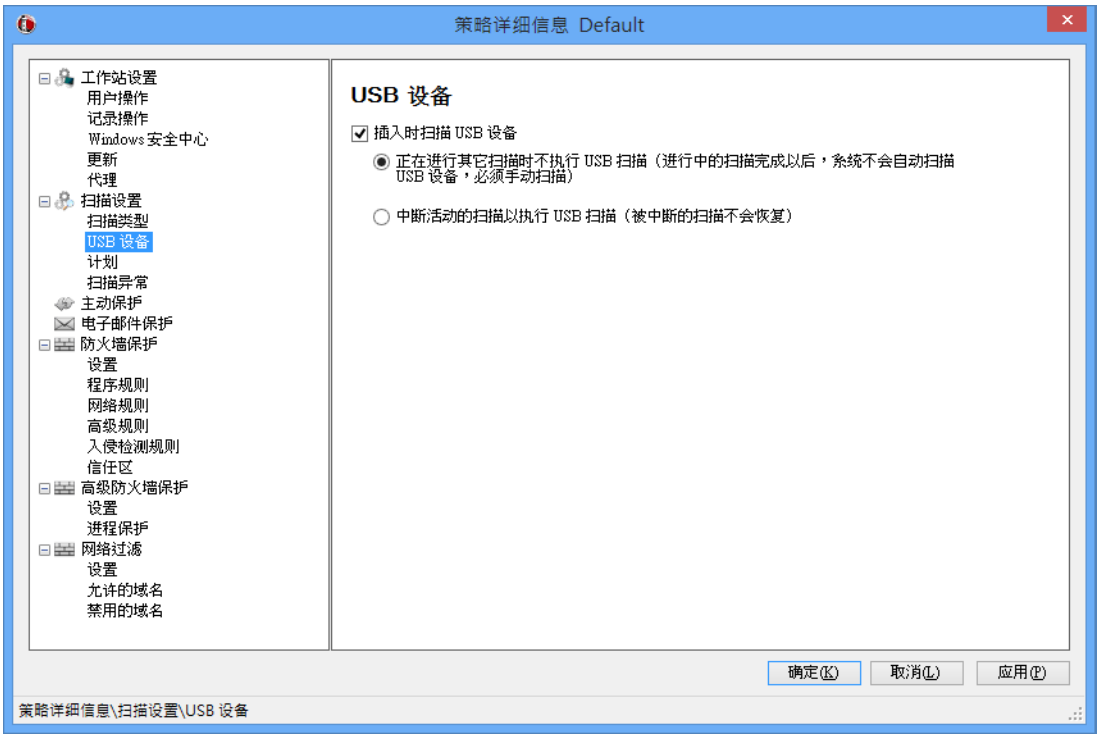


- *插入时扫描 USB 驱动器* - 选中该复选框以在插入时扫描 USB 驱动器，并选择以下选项之一：
  - *正在进行其它扫描时不执行 USB 扫描* – 选择此选项可确保活动的扫描不会因 USB 驱动器的插入而中断。活动的扫描完成后，必须手动扫描 USB 驱动器。
  - *中断活动的扫描以执行 USB 扫描* - 选择此选项可在 USB 驱动器插入时，中断活动的扫描以执行 USB 扫描。活动的扫描一旦中断，将无法自动恢复，必须手动重启。



如果*工作站设置*选项卡 > *用户操作*窗格中的*允许手动扫描*复选框已选中，则系统会自动扫描 USB 设备。如果*允许手动扫描*复选框未选中，则系统不会自动扫描 USB 设备。

- *扫描*节点 > *计划*窗格 - 指定以下设置：



快速扫描：

- *启用快速扫描* - 选中该复选框以启用 “ 快速扫描 ”。
- *启动* - 指定开始时间。
- *停止* - 指定结束时间。*启动*时间与*停止*时间之间间隔不得超过 *23.59* 小时。如果所有文件在*停止*时间以前扫描完毕，则扫描结束。如果扫描在*停止*时间尚未完成，则会在*停止*时间中止扫描。或者，选择*扫描完成时*以确保扫描完成。
- *天* - 选择计划执行快速扫描的日期。

深度扫描：

- *启用深度扫描* - 选中该复选框以启用深度扫描。
- *启动* - 指定开始时间。
- *停止* - 指定结束时间。*启动*时间与*停止*时间之间间隔不得超过 *23.59* 小时。如果所有文件在*停止*时间以前扫描完毕，则扫描结束。如果扫描在*停止*时间尚未完成，则会在*停止*时间中止扫描。或者，选择*扫描完成时*以确保扫描完成。
- *天* - 选择计划执行深度扫描的日期。

选项：

- *以 x 分钟为单位随机安排计划扫描开始时间* - 指定分钟数。随机安排计划扫描开始时间以减少对网络流量的影响。 Faronics Anti-Virus 将在扫描开始时向 Faronics Core 报告。如果同时开始对多个系统进行扫描，可能会影响网络流量。

启动时未执行的扫描选项：如果计划扫描期间工作站没有*开启*，选择以下任何一项扫描执行方式：

- *不执行快速扫描* - 如果您不想在启动时执行快速扫描，请选择此选项。
- *大约启动 x 分钟后执行快速扫描* - 指定 Faronics Anti-Virus 应在启动多少分钟后执行快速扫描。
- *提示用户执行快速扫描* - 选择此选项以提示用户执行快速扫描。

8. 指定*扫描*节点 > *扫描例外*窗格中的设置：

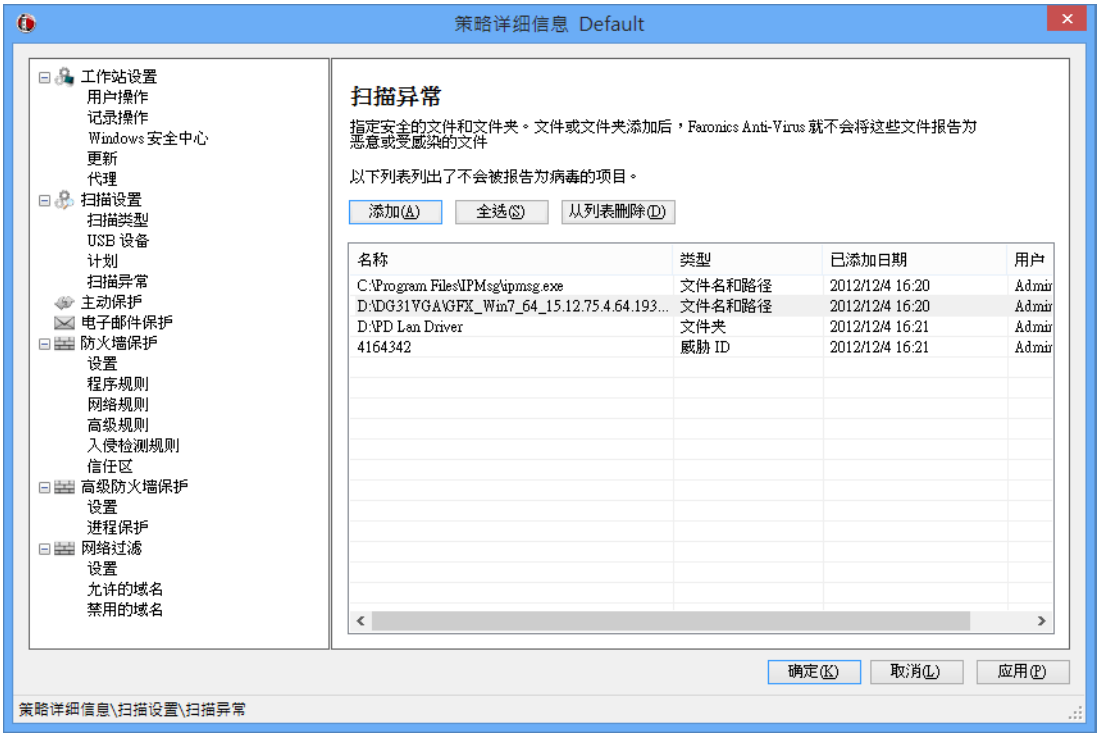
   已经确认安全和没有感染的文件夹或文件可以添加到 “ 扫描例外 ” 选项卡中。添加到 “ 扫描例外 ” 选项卡的文件夹或文件将始终被 Faronics Anti-Virus 扫描。但 Faronics Anti-Virus 不会将这些文件报告为恶意或被感染。此功能很实用，因为管理员确认安全的文件和文件夹不会被报告为恶意。

   a. 单击*添加*。

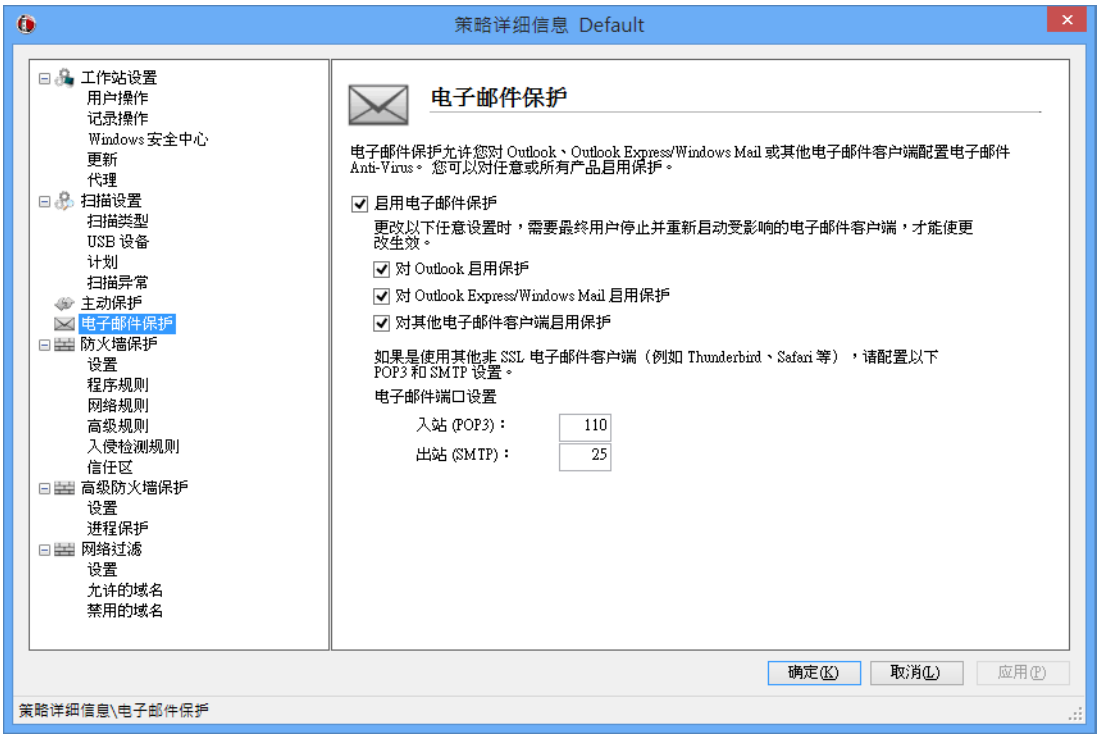


   b. 在*添加*对话框中，选择*文件完整路径*、*仅文件名*或*整个文件夹*。单击 “ 浏览 ” 以选择文件或文件夹，然后单击*确定*。

   c. *文件完整路径*将添加到 “ 扫描例外 ” 窗格中。

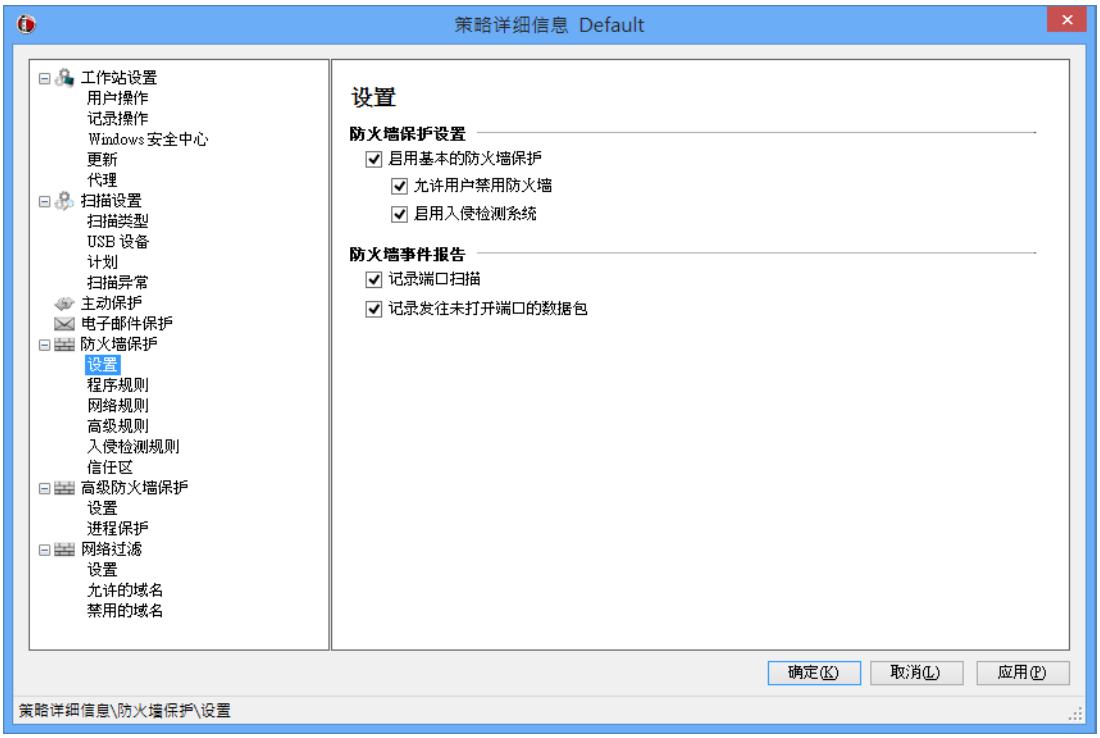

策略详细信息 Default
工作站设置
用户操作
记录操作
Windows 安全中心
更新
代理
扫描设置
扫描类型
USB 设备
计划
扫描异常
主动保护
电子邮件保护
防火墙保护
设置
程序规则
网络规则
高级规则
入侵检测规则
信任区
高级防火墙保护
设置
进程保护
网络过滤
设置
允许的域名
禁用的域名
扫描异常
指定安全的文件和文件夹。文件或文件夹添加后，Faronics Anti-Virus 就不会将这些文件报告为恶意或受感染的文件
以下列表列出了不会被报告为病毒的项目。
添加(A)
全选(S)
从列表删除(D)
名称
类型
已添加日期
用户
C:\Program Files\IPMsg\ipmsg.exe
文件名和路径
2012/12/4 16:20
Admir
D:\DG31VGAVGFX_Win7_64_15.12.75.4.64.193...
文件名和路径
2012/12/4 16:20
Admir
D:\PD Lan Driver
文件夹
2012/12/4 16:21
Admir
4164342
威胁 ID
2012/12/4 16:21
Admir
确定(K)
取消(L)
应用(P)
策略详细信息\扫描设置\扫描异常

9. 指定*主动保护*窗格中的设置：



- *启用主动保护* - 选择此选项以启用实时保护。主动保护是指 Faronics Anti-Virus 在后台进行实时扫描，不会对系统性能产生任何影响。如果有实时从 Internet 感染病毒的风险，请选择此选项。
- *允许用户关闭主动保护* - 选择此选项以允许用户关闭主动保护。如果用户安装或使用了可能被误认为病毒的软件（例如，在 Microsoft Office 中运行的高级宏或复杂的批处理文件），请选择此选项。
- *显示主动保护警报* - 选中此选项后，在主动保护期间检测到威胁时会显示警报。如果不希望显示警报，请不要选中此复选框。

10. 指定*电子邮件保护*窗格中的设置：

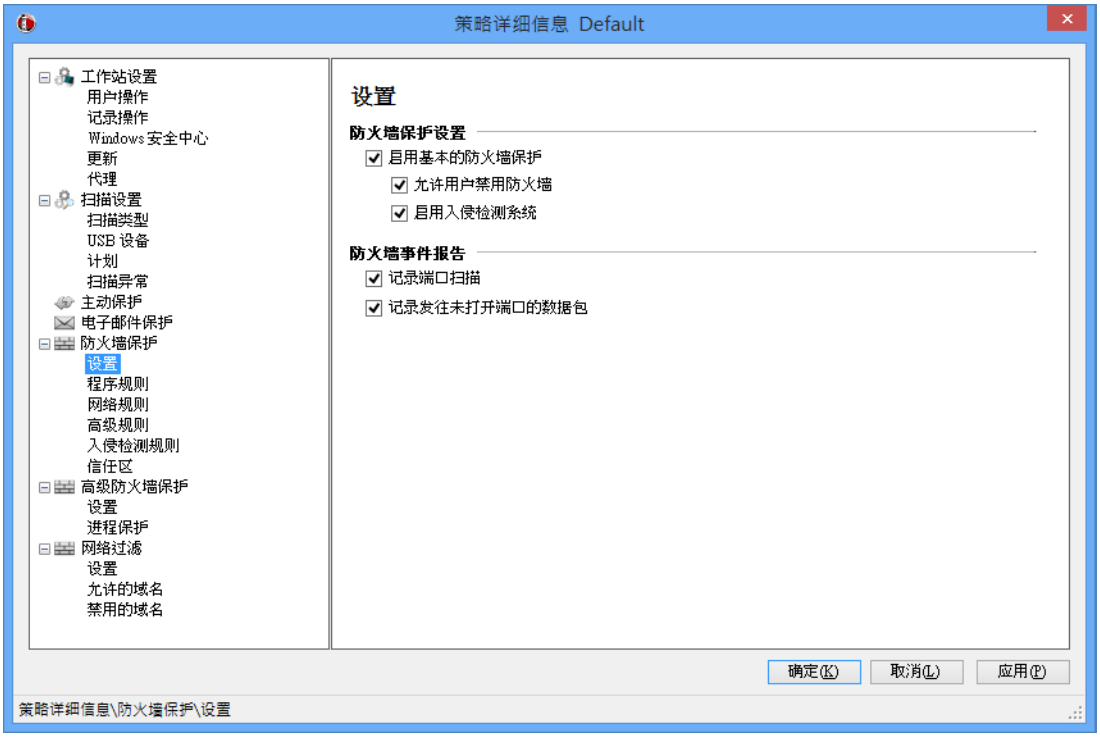


- *启用电子邮件保护* - 选中该复选框以启用电子邮件保护。如果选择*启用电子邮件保护*，则会启用以下选项。
  - 启用 Outlook 保护 - 选中该复选框以启用对 Outlook 的保护。 Faronics Anti-Virus 将扫描 Outlook 所接收和发送的全部电子邮件。
  - 启用 Outlook Express/Windows Mail 保护 - 选中该复选框以启用对 Outlook Express/Windows Mail 的保护。 Faronics Anti-Virus 将扫描 Outlook Express/Windows Mail 所接收和发送的全部电子邮件。
  - *启用其他电子邮件客户端保护* - 指定电子邮件入站端口 (POP3) 和出站端口 (SMTP) 设置。Faronics Anti-Virus 将扫描使用*入站*和*出站*设置的电子邮件程序中的所有邮件。

11. 指定*防火墙保护*节点中的设置：

防火墙保护节点可提供双向防护，同时限制入站和出站流量。您可以通过创建自定义规则来保护网络。不仅可以*允许*或*阻止*通信，还可将防火墙设置为*提示*。

- *防火墙节点* > *设置*窗格



防火墙保护设置：

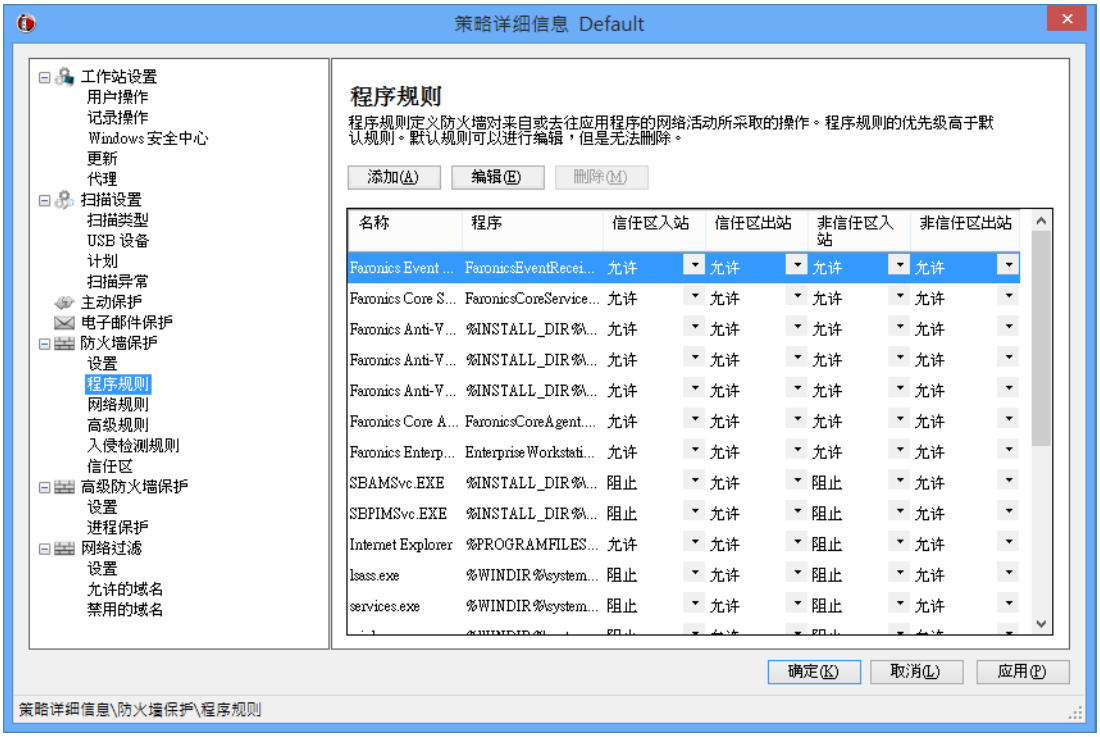
- *启用基本防火墙保护* - 选中此复选框可启用防火墙保护。
- *允许用户禁用防火墙* - 如果选中了*启用基本防火墙保护*复选框，则会启用此选项。选中此选项可允许用户禁用工作站的防火墙。

防火墙事件报告：

- *记录发往未打开端口的数据包* - 选中此复选框可记录发往未打开端口的数据包。这一数据可用于分析网络中对未打开端口的通信尝试。
- *记录端口扫描* - 选中此复选框可记录网络中对所有扫描端口的通信尝试。端口扫描数据将存储在日志文件中。

- *防火墙保护*节点 > *程序规则*窗格

程序规则定义防火墙对来自或去往应用程序的网络活动所采取的操作。程序规则的优先级高于默认规则。默认规则可以进行编辑，但是无法删除。



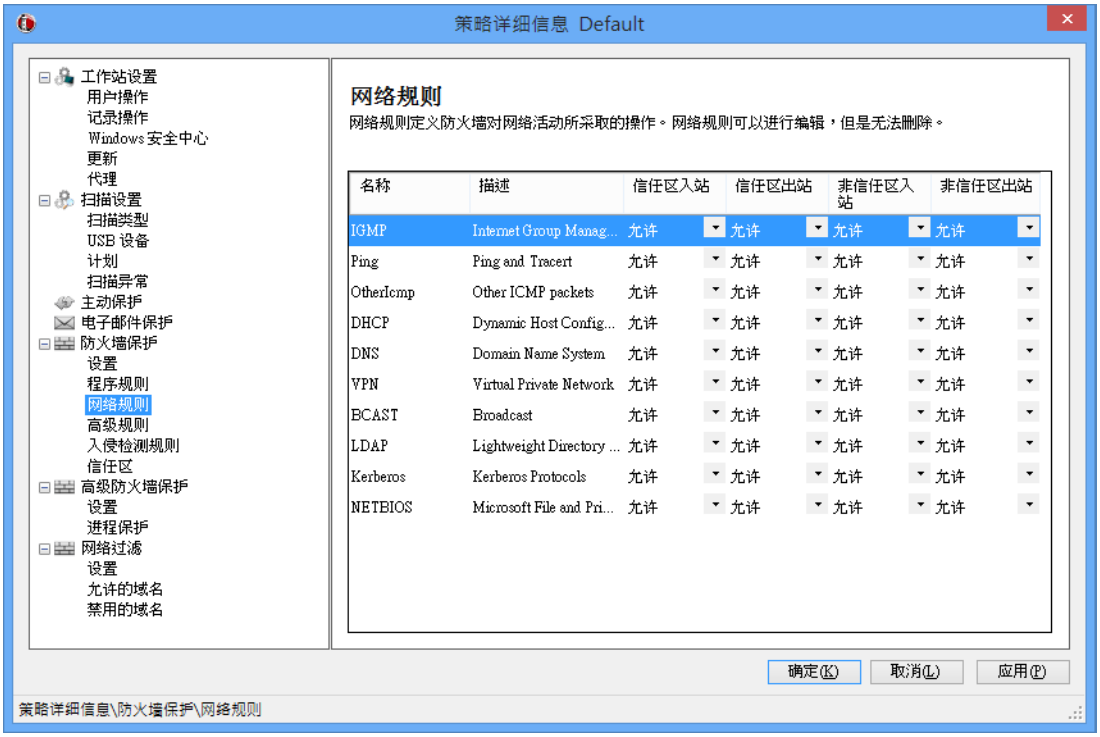
单击*添加*以添加新程序规则。指定或选择选项，然后单击*确定*。将显示以下参数：



- *名称* - 规则的名称。
- *程序* - 程序的名称，包括完整路径和扩展名。
- 信任区入站 - 对去往信任区程序的入站通信应执行的操作（*允许*、*阻止*或*提示*）。
- 信任区出站 - 对来自信任区程序的出站通信应执行的操作（*允许*、*阻止*或*提示*）。
- 非信任区入站 - 对去往非信任区程序的入站通信应执行的操作（*允许*、*阻止*或*提示*）。
- 非信任区出站 - 对来自非信任区程序的出站通信应执行的操作（*允许*、*阻止*或*提示*）。

- *防火墙保护*节点 > *网络规则*窗格

网络规则定义防火墙对网络活动所采取的操作。这类规则可以进行编辑，但是无法删除。



将显示以下参数：

- *名称* - 协议的名称。
- *说明* - 协议的说明。
- 信任区入站 - 对去往信任区协议的入站通信应执行的操作（*允许*、*阻止*或*提示*）。
- 信任区出站 - 对来自信任区协议的出站通信应执行的操作（*允许*、*阻止*或*提示*）。
- 非信任区入站 - 对去往非信任区协议的入站通信应执行的操作（*允许*、*阻止*或*提示*）。
- 非信任区出站 - 对来自非信任区协议的出站通信应执行的操作（*允许*、*阻止*或*提示*）。

- *防火墙保护*节点 > *高级规则*窗格

高级规则定义防火墙针对指定的应用程序、端口或协议所采取的操作。其中可能包括单个协议、本地或远程端口以及流量方向，或者是它们的组合。您可以添加、编辑或删除高级规则。



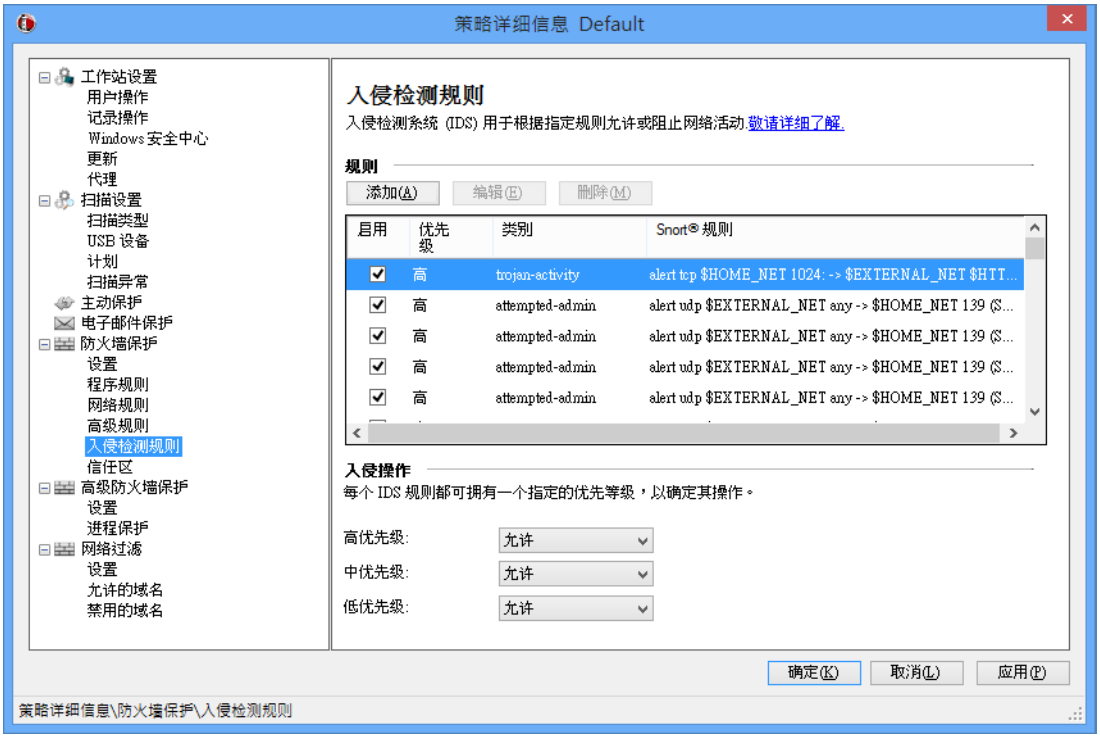
单击*添加*以添加新高级规则。指定或选择选项，然后单击*确定*。在“高级规则”窗格中将显示下列参数：



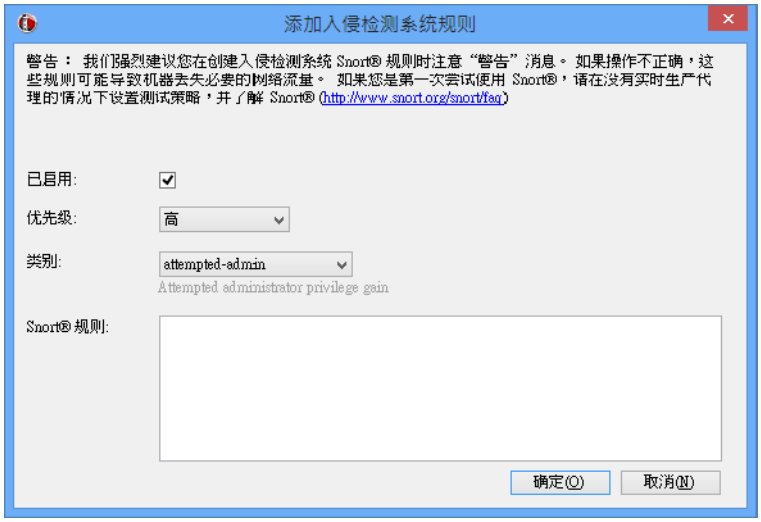
- *名称* - 规则的名称。
- *程序* - 程序的名称和路径。
- *操作* - 防火墙对来自指定的应用程序、端口或协议的通信所采取的操作。（*允许*、*阻止*或*提示*）。
- *方向* - 通信的方向（*双向*、*入站*、*出站*）。
- *协议* - 协议的名称。
- *本地端口* - 本地端口的详细信息。
- *远程端口* - 远程端口的详细信息。

- *防火墙保护*节点 > *入侵检测规则*窗格

入侵检测系统(IDS)用于根据指定的入侵检测规则允许或阻止网络活动。请在“入侵检测规则”窗格为该屏幕上每个分类为“高”、“中”或“低”优先级的规则指定操作(“允许”或“阻止”)。对于现有规则，可单击*编辑*进行修改或单击*删除*予以删除。



单击*添加*可添加新的入侵检测规则。请指定或选择选项，然后单击*确定*。单击*添加*后，即会显示下列参数：



— *启用*-选择是否启用该规则。

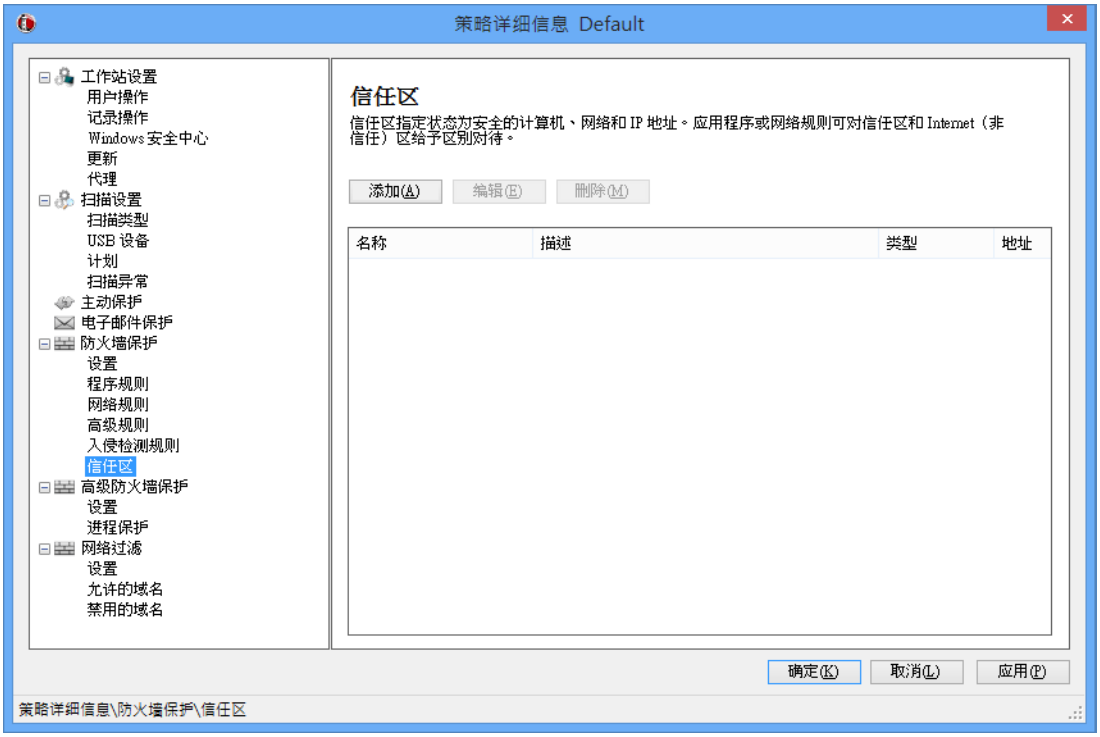
— *优先级*-选择规则的优先级为*高*、*中*或*低*。

— *类别*-选择规则的类别（例如*bad-unknown*、*attempted-admin*、*attempted-dos*或*attempted-recon*）。

— *Snort规则*-指定snort规则。有关Snort规则的详细信息，请访问www.snort.org/snort/faq。

- *防火墙保护*节点 > *信任区*窗格

信任区指定受信任的计算机、网络和IP地址。程序和网络规则可对信任区和Internet（非信任）区给予区别对待。

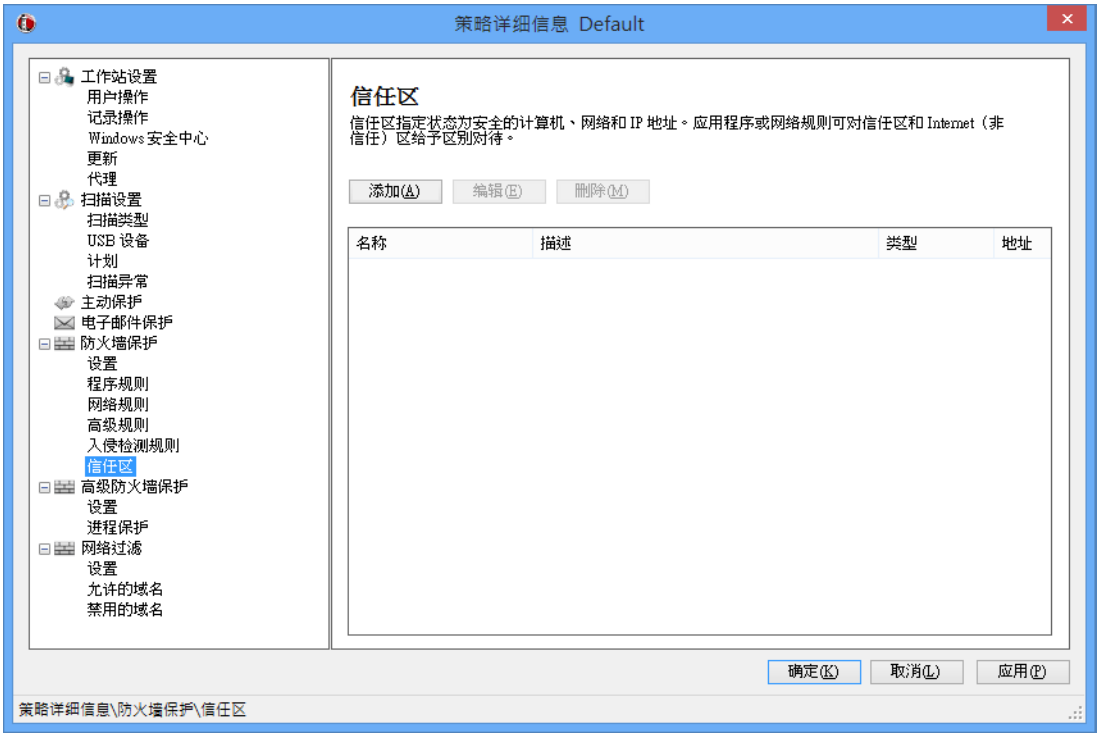


单击*添加*可添加新的信任区。请指定或选择选项，然后单击*确定*。此时将显示以下参数：

- *名称*-信任区的名称。
- *说明*-信任区的说明。
- *类型*-信任区的类型（*IP 地址*、*地址范围*或*网络*）。

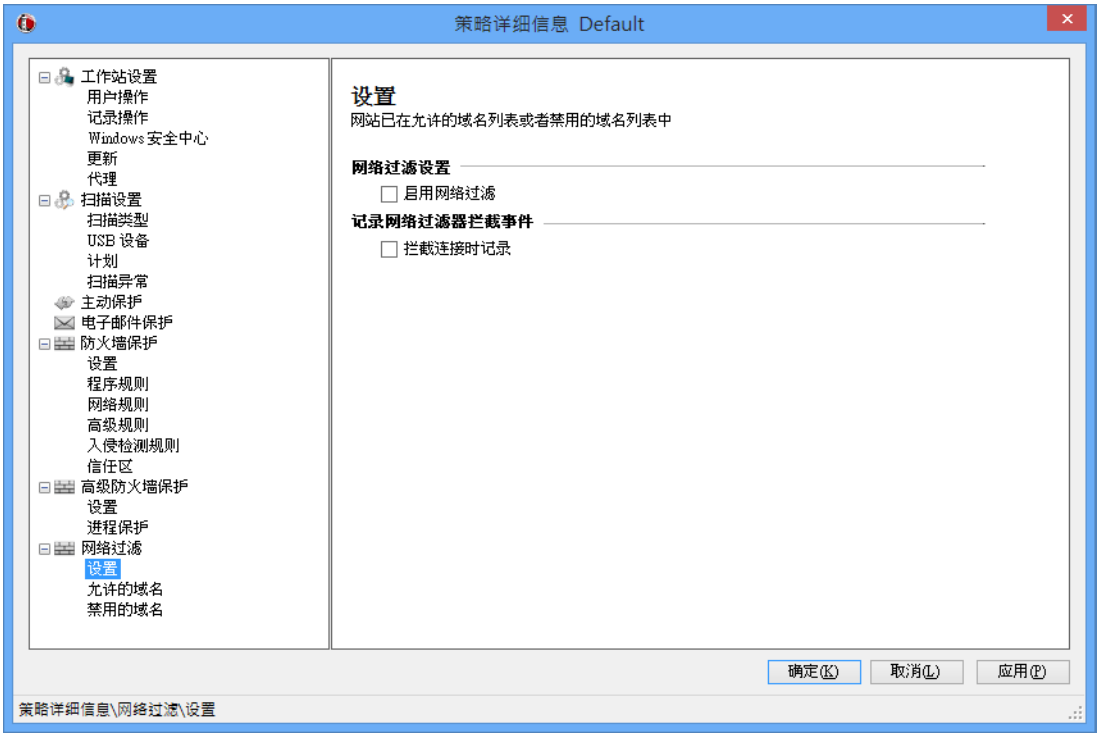
- *高级防火墙保护*节点 > *设置*窗格

“设置”窗格用于启用或禁用进程保护及启动保护。



- *网络过滤*节点 > *设置*窗格

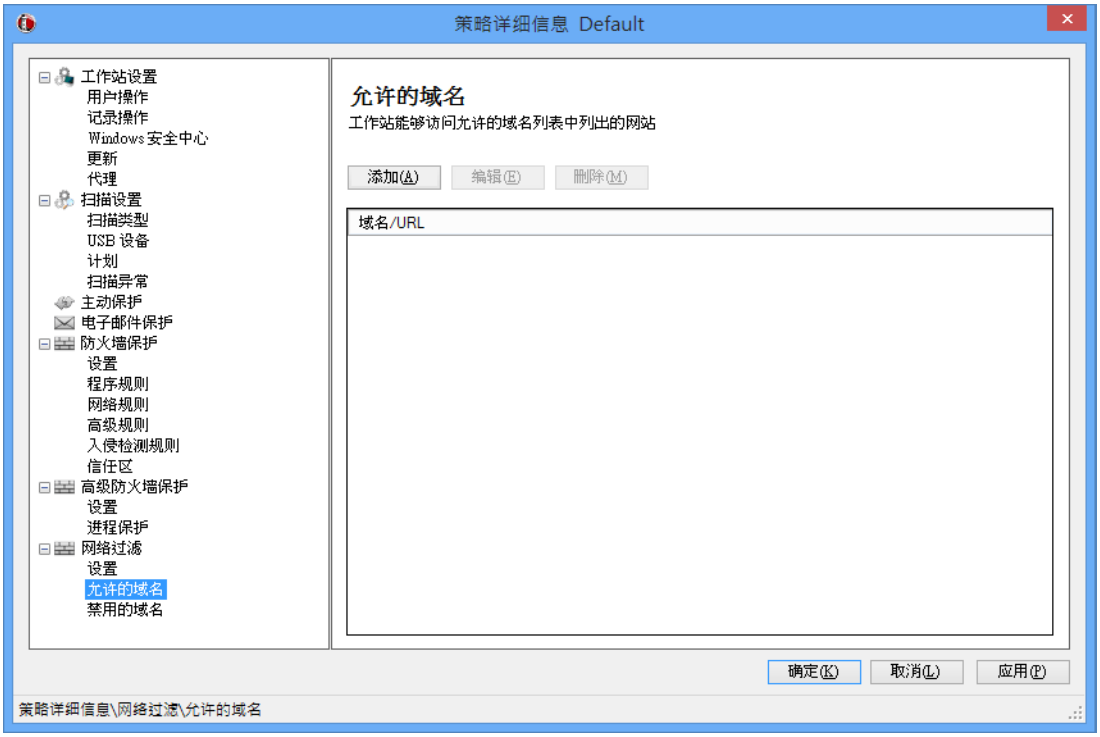
网络过滤功能可阻止某些类型的信息在您的浏览器上显示。您可以通过此窗格为网络过滤指定默认配置。



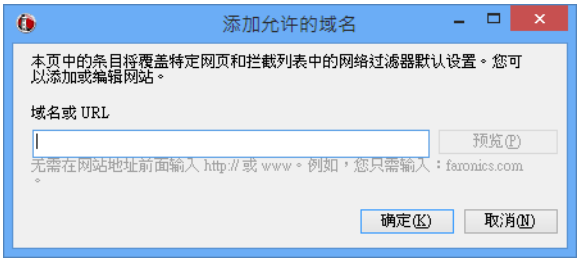
- 选择*启用网络过滤*以启用此功能。
- 选择*拦截连接时记录*，确保 Faronics Anti-Virus 执行的操作都记录在日志文件中。

- *网站过滤*节点 > *允许的域名*窗格

“ 允许的域名 ” 会覆盖默认网络过滤设置以及添加到 “ 拦截的广告 ” 列表中的网站。

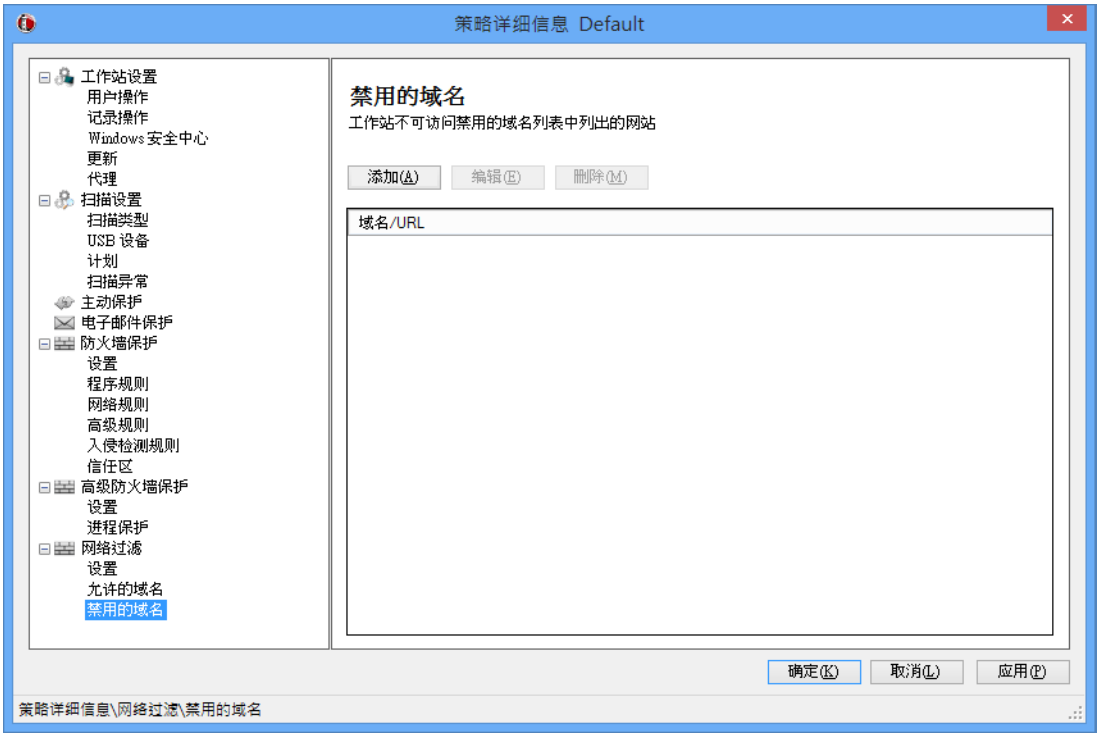


单击*添加*以添加新允许的域名。请指定或选择选项，然后单击*确定*。此时将显示以下参数：



- 域名或 URL - 指定要允许的域名或 URL。单击 “ 预览 ” 以预览域名或 URL。
- *网络过滤*节点 > *拦截的域名*窗格

指定必须在网络上拦截的域名。



单击*添加*以添加新拦截的域名。请指定或选择选项，然后单击*确定*。此时将显示以下参数：



- 域名或 URL - 指定要允许的域名或 URL。单击 “ 预览 ” 以预览域名或 URL。

12. 单击*确定*。此时新策略 *New Policy 1* 将在 *Anti-Virus* 节点下显示。

应用 Anti-Virus 策略

一旦创建 Anti-Virus 策略后，可通过 Faronics Core 控制台将其应用至一个或多个工作站。要应用策略，请完成以下步骤：

1. 选择一个或多个工作站。右键单击并选择*重新分配策略*。
2. 此时将显示*为工作站重新分配策略*对话框。从*分配策略*下拉列表中选择策略，然后单击*确定*。
3. 该策略将应用至所选工作站。

查看或修改 Anti-Virus 策略

一旦创建 Anti-Virus 策略后，可查看或修改该策略。要查看或修改策略，请完成以下步骤：

1. 启动 Faronics Core 控制台。
2. 在*控制台树窗格*中，依次转至 *Faronics Core 控制台 >[Core 服务器]> 托管工作站 > Anti-Virus>[策略名称]*。
3. 右键单击该策略，然后选择*策略详细信息*。
4. 要编辑该策略，请在选项卡中修改设置，如*创建 Anti-Virus 策略中所述。*
5. 单击*确定*以应用更改。
6. 对策略所做的更改将自动应用至策略所管理的工作站。

重命名 Anti-Virus 策略

一旦创建 Anti-Virus 策略后，可重命名该策略。要重命名策略，请完成以下步骤：

1. 启动 Faronics Core 控制台。
2. 在*控制台树窗格*中，依次转至 *Faronics Core 控制台 >[Core 服务器]> 托管工作站 > Anti-Virus>[策略名称]*。
3. 右键单击该策略，然后选择*重命名策略*。此时将显示*重命名策略*对话框。
4. 输入*新的策略名*，然后单击*确定*。

导入 Anti-Virus 策略

预配置的 Anti-Virus 策略可以导入到现有策略中。此功能可以节省时间，因为无需重新配置整个策略。

要导入现有策略，请完成以下步骤：

1. 启动 Faronics Core Console。
2. 在控制台树窗格中，依次转至 Faronics Core Console>[Core Server]> 托管工作站 >Anti-Virus>[策略名称]。
3. 右键单击该策略，然后选择导入策略。单击是覆盖现有策略中的当前设置。
4. 浏览并选择要导入的策略。只能导入之前以 XML 格式导出的策略。
5. 选择之前导出的策略，然后单击打开。该策略将会导入。

导出 Anti-Virus 策略

预配置的 Anti-Virus 策略可导出以供重复使用。此功能可以节省时间，因为无需重新配置整个策略。

要导出现有策略，请完成以下步骤：

1. 启动 Faronics Core Console。
2. 在控制台树窗格中，依次转至 Faronics Core Console>[Core Server]> 托管工作站 >Anti-Virus>[策略名称]。
3. 右键单击该策略，然后选择导出策略。

4. 浏览以选择位置。
5. 指定文件名并单击保存。该策略将以 XML 格式导出。

复制策略

可将现有的策略轻松复制到新策略。或者，可将现有策略中的数据复制到其他现有策略。

要复制策略，请完成以下步骤：

1. 启动 Faronics Core 控制台。
2. 在*控制台树窗格*中，依次转至 *Faronics Core 控制台 >[Core 服务器]> 托管工作站 > Anti-Virus>[策略名称]*。
3. 右键单击该策略，然后选择*复制策略*。此时将显示*复制策略*对话框。
4. 从下拉列表中选择*目标策略*，或单击*新建*将数据复制到新策略。为新策略指定名称。
5. 单击*立即复制策略数据*。

数据将复制到现有策略，或将使用在步骤 3 中所选现有策略创建一个新策略。

删除 Anti-Virus 策略

要删除现有策略，请完成以下步骤：

1. 启动 Faronics Core 控制台。
2. 在*控制台树窗格*中，依次转至 *Faronics Core 控制台 >[Core 服务器]> 托管工作站 > Anti-Virus>[策略名称]*。
3. 右键单击该策略，然后选择*删除策略*。此时将显示*删除策略*对话框。
4. 单击*是*删除策略。



删除分配给工作站的策略时，会以默认策略取代该策略。默认策略无法删除。

通过 Faronics Core 控制台扫描

扫描可以通过在 Anti-Virus 策略中制定计划，或通过 Faronics Core 控制台计划任务的方式手动执行。要通过 Faronics Core 控制台手动扫描工作站，请完成以下步骤：

1. 启动 Faronics Core 控制台。
2. 转至*工作站列表*窗格。
3. 右键单击一个或多个工作站，然后选择*扫描*。

- 对快速扫描，选择*扫描* > *快速*。
- 对深度扫描，选择*扫描* > *深度*。
- 要中止正在进行的扫描，请选择*扫描* > *中止*。
- 要暂停正在进行的扫描，请选择*扫描* > *暂停*。
- 要恢复已暂停的扫描，请选择*扫描* > *恢复*。

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。



通过 Anti-Virus 策略设置的“计划任务”始终优先于通过 Faronics Core 控制台设置的“计划操作”执行。

此时将在 Faronics Core 控制台的*工作站列表*窗格中显示扫描进度（*% 扫描已完成*）。

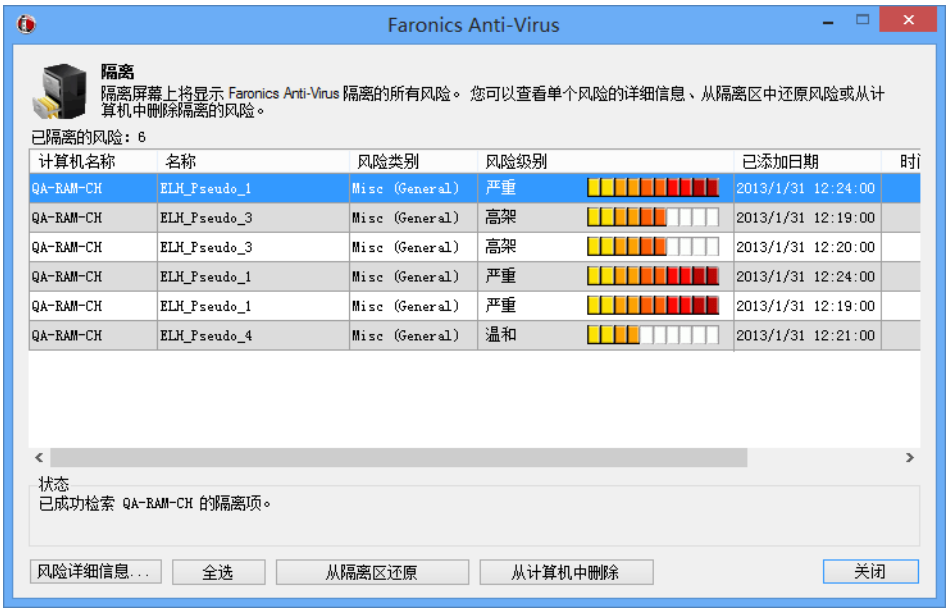


如果安装了多个插件，可通过右键单击工作站，选择 *Faronics Anti-Virus* 访问 Faronics Anti-Virus 的右键上下文菜单，然后选择特定的操作。

查看隔离的文件并对其进行操作

要查看通过 Faronics Anti-Virus 隔离的文件，请完成以下步骤：

1. 启动 Faronics Core Console。
2. 转至*工作站列表*窗格。
3. 选择工作站。
4. 右键单击该工作站，然后选择*查看隔离区*。此时将显示隔离文件的列表。



5. 将显示每个受感染文件的以下信息：

- 风险名称
- 风险类别
- 文件名
- 原位置
- 风险级别
- 已添加日期
- 时间 （天）
- 隔离执行者

6. 选择以下操作：

- *详细信息* - 选择一个文件，然后单击*详细信息*以查看受感染文件的详细信息。执行此操作系统也会显示建议的操作。
- *全选* - 选择所有文件。
- *从计算机中删除* - 从计算机中删除选定的文件。

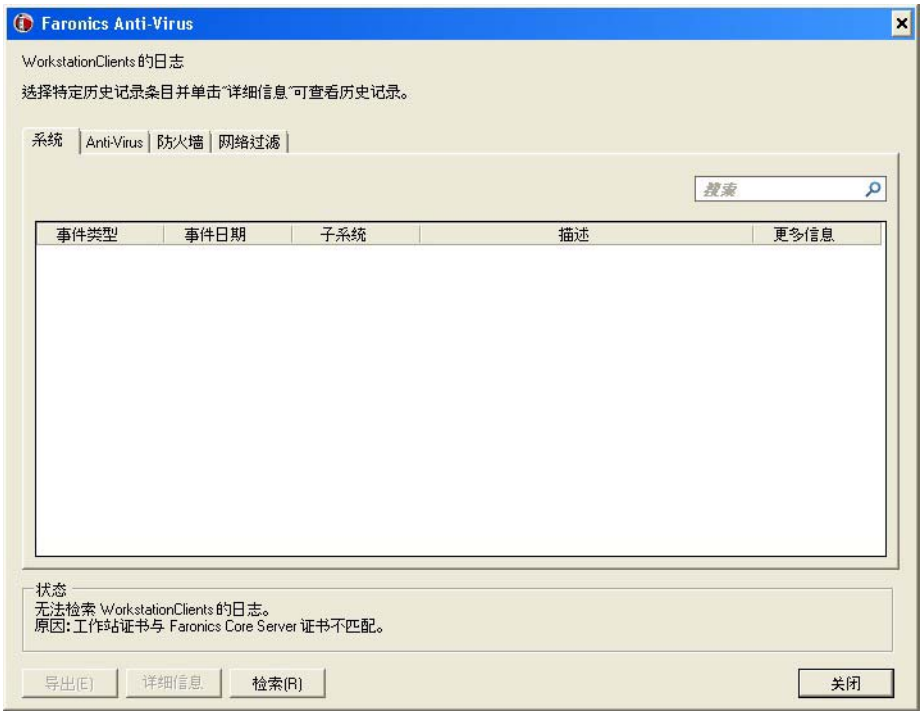
- *从隔离区还原* - 从计算机中还原选定的文件。
- *关闭* - 关闭对话框。

查看 Faronics Anti-Virus 日志

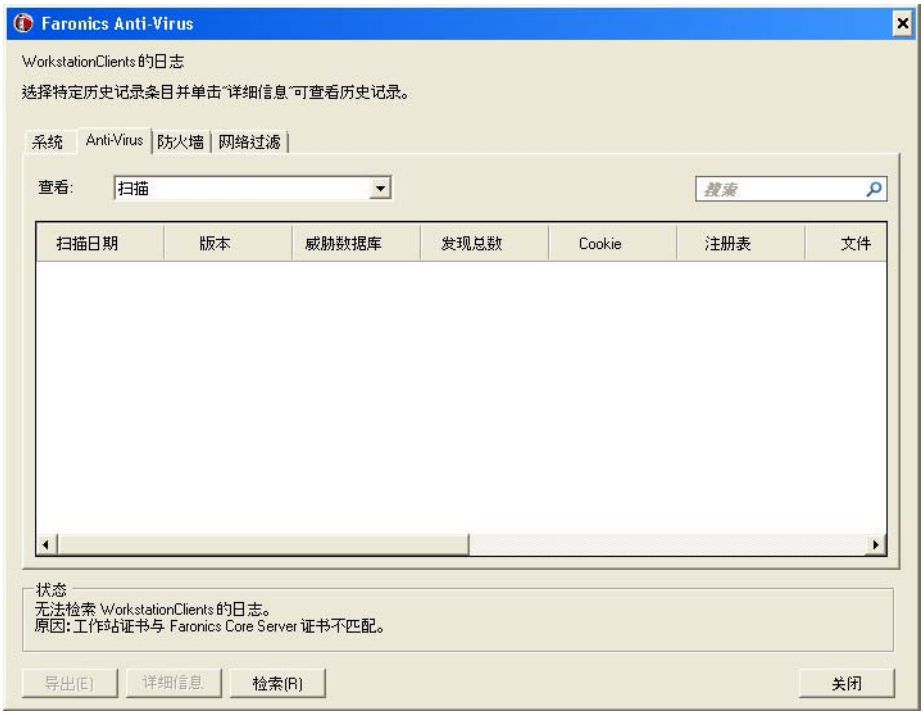
要查看日志，请完成以下步骤：

1. 启动 Faronics Core Console。
2. 转至*工作站列表*窗格。
3. 选择工作站。
4. 右键单击该工作站，然后选择*查看日志*。随即出现带有以下选项卡的日志窗口：

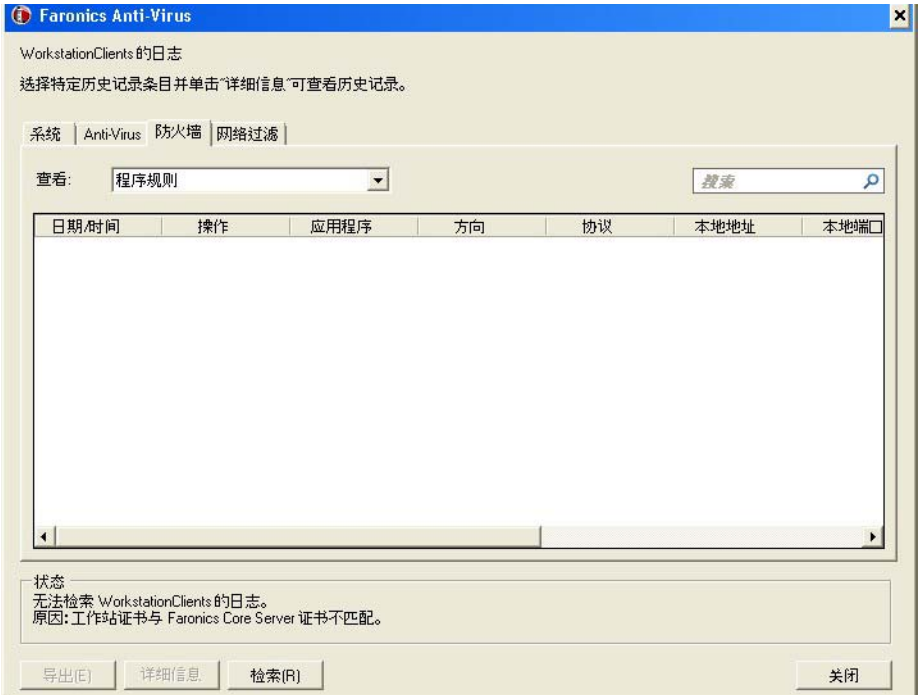
- 系统选项卡 - 显示系统事件。



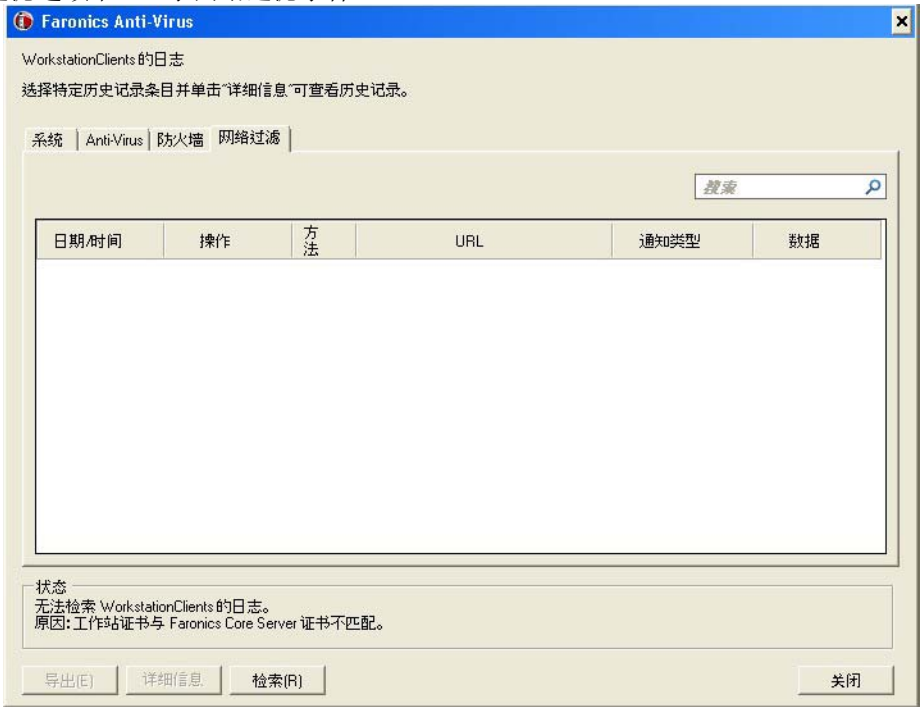
- Anti-Virus 选项卡 - 显示 Anti-Virus 事件。从下拉菜单中选择下列选项以查看选定结果：
  - 扫描
  - 主动保护
  - 电子邮件保护



- 防火墙选项卡 - 显示防火墙事件。从搜索字段中搜索指定事件。从下拉菜单中选择下列选项以查看选定结果：
  - 程序规则
  - 网络规则
  - 高级规则
  - 入侵检测系统
  - 进程保护
  - 适配器
  - 未打开端口数据包



- 网络过滤选项卡 - 显示网络过滤事件。



5. 选择每个选项卡中的以下操作之一：

- *导出* - 以 .txt 或者 .csv 格式导出日志。
- *详细信息* - 查看日志条目的详细信息。
- *检索* - 从工作站检索日志。
- *关闭* - 关闭对话框。



此选项仅当只选择一个工作站时可用。

通过 Faronics Core 控制台更新 Faronics Anti-Virus

Faronics Anti-Virus 定义可通过 Faronics Core 控制台在工作站上进行更新。 Faronics Core 可充当托管工作站的 Anti-Virus 更新存储库。 Anti-Virus 更新将通过 Faronics Core 自动发送到远程工作站。此外， Faronics Core 管理员可以按以下步骤手动更新病毒定义。

要在工作站上更新 Faronics Anti-Virus，请完成以下步骤：

1. 启动 Faronics Core 控制台。
2. 转至*工作站列表*窗格。
3. 右键单击一个或多个工作站，然后选择*更新*。

- 选择*更新* > *完全更新* - 这将更新 Anti-Virus 定义。
- 选择*更新*>*强制执行完全更新* - 这将删除现有的 Anti-Virus 定义并更新最新的 Anti-Virus 定义。

通过 Faronics Core 控制台计划 Faronics Anti-Virus 的操作

可对 Faronics Anti-Virus 和 Faronics Core 控制台事件进行计划，使它们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，然后选择*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 控制台控制的操作：

- 关机
- 重新启动
- 唤醒

由 Faronics Anti-Virus 控制的操作：

- 主动保护 > 启用
- 主动保护 > 禁用
- 扫描 > 快速
- 扫描 > 深度
- 更新 > 完全更新
- 更新 > 强制执行完全更新
- 立即修复
- 安装 / 升级 Anti-Virus 客户端
- 卸载 Anti-Virus 客户端



通过 Anti-Virus 策略设置的“计划任务”始终优先于通过 Faronics Core 控制台设置的“计划操作”执行。

生成报告

Faronics Anti-Virus 可提供多份报告，以便监视每个工作站上的活动。报告分为两类：

- 全局报告 - 这些报告基于所有受 Faronics Anti-Virus 保护的工作站情况编制。
- 特定工作站报告 - 这些报告仅涉及选定的工作站。

全局报告

要生成全局报告，请完成以下步骤：

1. 启动 Faronics Core 控制台。
2. 在*控制台树*窗格中，依次转至 *Faronics Core 控制台 >[Core 服务器]> 托管工作站 > Anti-Virus*。
3. 在*操作*窗格中，单击*全局报告*。
4. 选择报告，然后在随后显示的对话框中输入日期范围。单击*确定*。系统会显示以下报告：

- *按检测结果数量分类威胁* - 按在由 Faronics Anti-Virus 管理的所有工作站上检测到的结果数量分类显示检测到的威胁。
- *威胁严重性摘要* - 显示威胁严重性摘要。
- *前 25 台感染病毒最严重的计算机* - 显示前 25 台感染病毒最严重的计算机。

5. 选定的报告将在*控制台树*窗格 > *报告*节点中显示。

特定工作站报告

要生成特定工作站报告，请完成以下步骤：

1. 启动 Faronics Core 控制台。
2. 在*控制台树*窗格中，依次转至 *Faronics Core 控制台 >[Core 服务器]> 托管工作站*。
3. 选择要生成该报告的工作站。
4. 右键单击该工作站，然后选择*报告*。
5. 选择报告，然后在随后显示的对话框中输入日期范围。单击*确定*。系统会显示以下报告：

- 工作站详细信息
- 上次扫描
- 扫描历史记录
- 主动保护历史记录
- 隔离区
- 电子邮件保护历史记录
- 系统事件消息

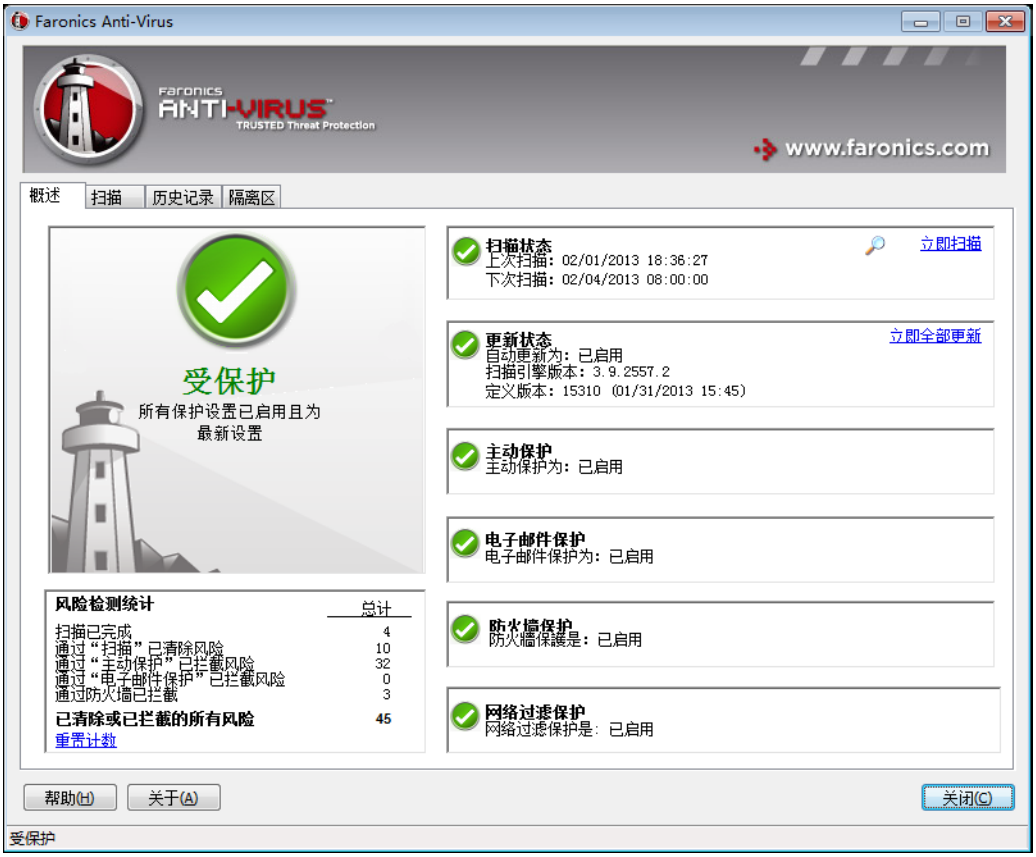
6. 选定的报告将在*控制台树*窗格 > *报告*节点中显示。

在工作站上使用 Faronics Anti-Virus

工作站上 Faronics Anti-Virus 中可用的功能完全取决于 Anti-Virus 策略中所选的设置。有关 Anti-Virus 策略的详细信息，请参阅 *Faronics Anti-Virus 策略*。

在工作站上启动 Faronics Anti-Virus

依次转至*开始* > *程序* >*Faronics*>*Anti-Virus Enterprise*>*Faronics Anti-Virus Enterprise*。或者，您可以双击系统任务栏中的 Faronics Anti-Virus 图标。



以下窗格将向用户显示重要信息：

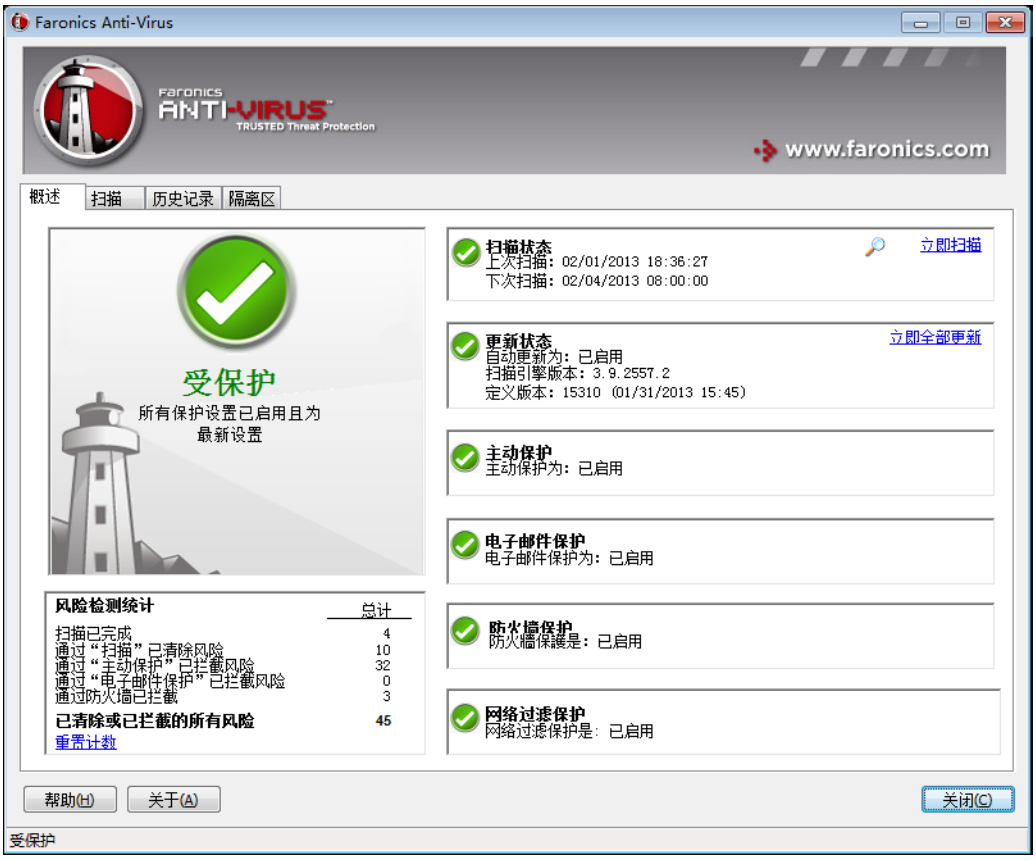
- 显示*受保护*或*不受保护*，告知计算机是否受到保护。如果显示“不受保护”，请单击*不受保护*标志下的*立即修复*按钮。
- *扫描状态*显示上次扫描的时间。要立即扫描，请单击*立即扫描*链接。
- *更新状态*显示上次更新的时间。要更新病毒定义，请单击*立即全部更新*链接。
- *主动保护*显示是否启用实时保护。
- *电子邮件保护*显示是否通过 Faronics Anti-Virus 保护电子邮件。
- “防火墙保护”显示工作站是否受到防火墙的保护。
- *网络过滤保护*显示工作站是否受 Faronics Anti-Virus 的网络过滤功能保护。

- *风险检测统计*显示 Faronics Anti-Virus 所执行操作的统计信息。单击*重置计数*可将计数清零。

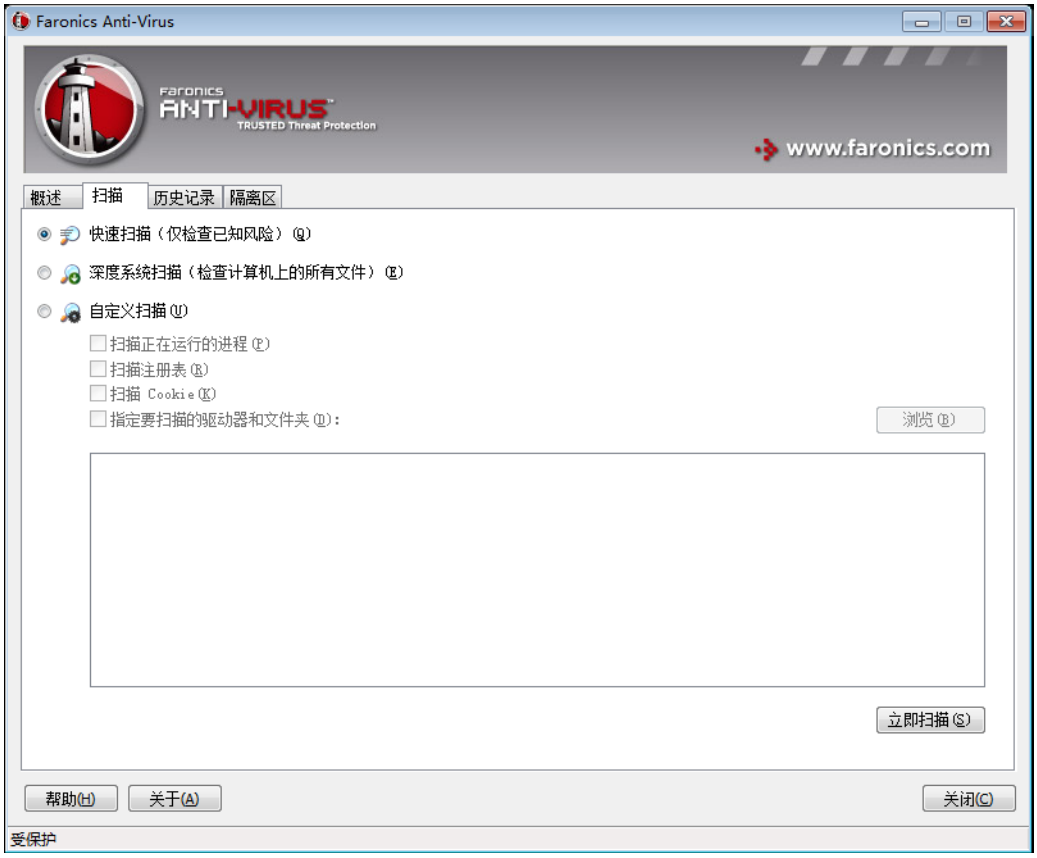
扫描工作站

要扫描工作站，请完成以下步骤：

1. 依次转至*开始* > *程序* > *Faronics*> *Anti-Virus Enterprise*> *Faronics Anti-Virus Enterprise*。或者，您可以双击系统任务栏中的 Faronics Anti-Virus 图标。



2. 在*扫描状态*窗格中，单击*立即扫描*。此时将显示*扫描*选项卡。或者，您还可以单击*扫描*选项卡。



3. 选择以下选项之一：

- *快速扫描* - 仅扫描已知的威胁。
- *深度系统扫描* - 详细扫描工作站上的所有文件。
- *自定义扫描*（选择以下各项之一）：
  - *扫描正在运行的进程* - 扫描工作站上正在运行的进程。
  - *扫描注册表* - 扫描注册表。
  - *扫描 Cookie* - 扫描工作站上存储的 Cookie。
  - *指定要扫描的驱动器和文件夹*：单击*浏览*并选择文件夹。

4. 单击*立即扫描*。旋转的图标表示正在进行扫描。扫描完成后将显示扫描结果。
5. 选择文件，系统将显示以下选项：

- 依次选择*更改清除操作* > *建议操作*以执行 Faronics Anti-Virus 建议的操作。
- 依次选择*更改清除操作* > *隔离 / 杀毒*以隔离该文件或对其杀毒。
- 依次选择*更改清除操作* > *删除*以删除该文件。
- 依次选择*更改清除操作* > *允许*以允许该文件。
- 单击*全选*以选择*扫描结果*中显示的所有文件。
- 单击*详细信息*以显示风险的详细信息。
- 单击*取消*以关闭该对话框而不进行任何操作。
- 单击*清除*以删除文件并关闭该对话框。

还可通过 Faronics Core 控制台进行操作。有关详细信息，请参阅*查看隔离的文件并对其进行操作。*

通过右键单击扫描文件或文件夹

您可以轻松扫描文件或文件夹(一个或多个)有无病毒。当工作站上安装了 Faronics Anti-Virus 时，右键单击菜单中会添加 “ 扫描病毒 ” 选项。

要扫描计算机上的文件或文件夹，请完成以下步骤：

1. 右键单击文件或文件夹。
2. 选择*扫描病毒*。

此时将执行扫描并显示结果。

查看扫描历史记录

要查看扫描历史记录，请完成以下步骤：

1. 依次转至*开始* > *程序* >*Faronics*>*Anti-Virus Enterprise*>*Faronics Anti-Virus Enterprise*。或者，您可以双击系统任务栏中的 Faronics Anti-Virus 图标。
2. 单击*历史记录*选项卡。



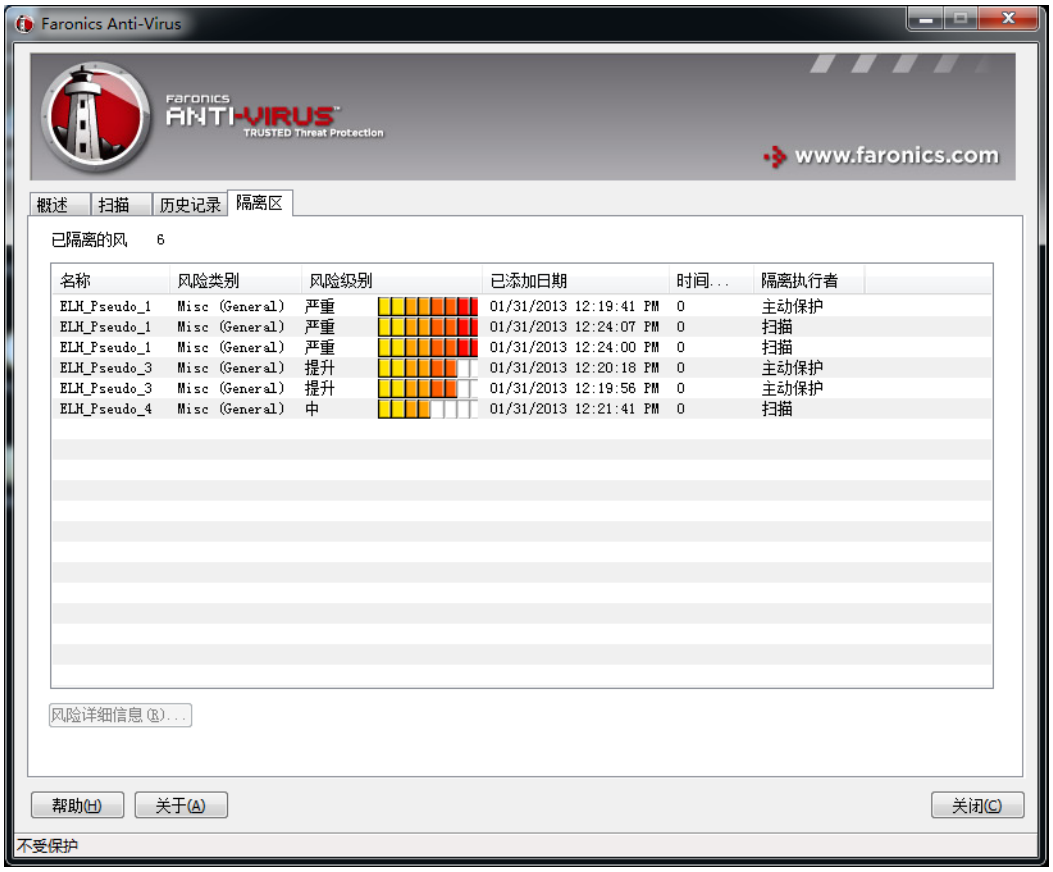
3. 选择以下操作：

- *仅显示发现有风险的扫描* - 选择此选项仅查看发现有风险的扫描。
- *详细信息* - 选择某个条目，然后单击详细信息以查看扫描的详细信息。

查看隔离的文件并对其进行操作

要查看隔离区，请完成以下步骤：

1. 依次转至*开始* > *程序* >*Faronics*>*Anti-Virus Enterprise*>*Faronics Anti-Virus Enterprise*。或者，您可以双击系统任务栏中的 Faronics Anti-Virus 图标。
2. 单击*隔离区*选项卡。



3. 单击*风险详细信息*。将显示每个受感染文件的以下信息：

- 名称
- 风险类别
- 风险级别
- 已添加日期
- 时间 （天）
- 隔离执行者

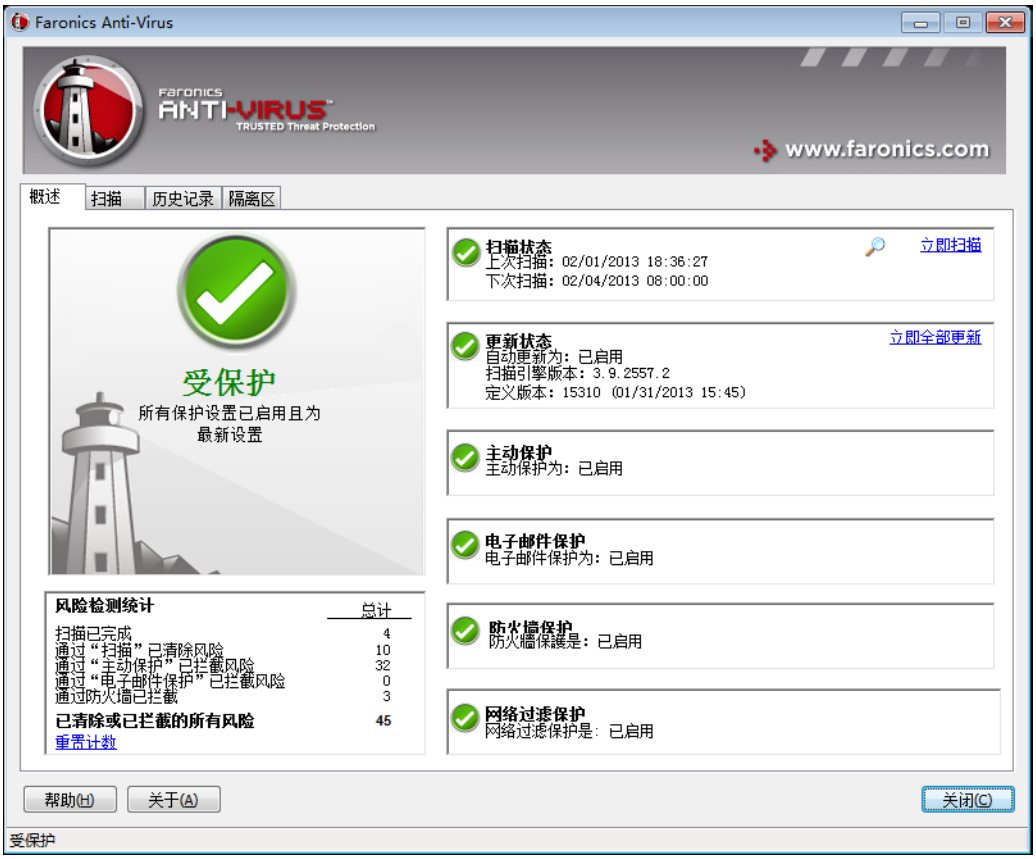
4. 选择以下操作：

详细信息 - 选择一个文件，然后单击*详细信息*以查看受感染文件的详细信息。执行此操作系统也会显示建议的操作。

在工作站上更新 Anti-Virus 定义

要在工作站上更新 Anti-Virus 定义，请完成以下步骤：

1. 依次转至*开始* > *程序* > *Faronics*> *Anti-Virus Enterprise*> *Faronics Anti-Virus Enterprise*。或者，您可以双击系统任务栏中的 Faronics Anti-Virus 图标。



2. 在*更新状态*窗格中，单击*立即全部更新*。此时将显示*立即全部更新*对话框。
3. 单击*安装更新*。此时将更新工作站上的病毒定义。

通过系统任务栏管理工作站上的 Faronics Anti-Virus

Faronics Anti-Virus 可在工作站上通过系统任务栏上的菜单进行管理。

右键单击系统任务栏中的 Faronics Anti-Virus 图标。系统将显示以下选项：

- 打开 Faronics Anti-Virus - 启动工作站上的 Faronics Anti-Virus。
- *主动保护*
  - *主动保护* > *启用主动保护* - 启用主动保护。
  - *主动保护* > *禁用主动保护* > *[选择选项]* - 选择要禁用主动保护的时间。可选择 5 分钟、15 分钟、 30 分钟、 1 小时、“ 直到计算机重启 ” 或 “ 永久 ”。仅当在 Anti-Virus 策略中选择了此选项时，此选项方会显示。
- *立即扫描* > *[选择选项]* - 可选择“取消扫描”、“暂停扫描”、“恢复扫描”、“快速扫描”或“深度扫描”。仅当在 Anti-Virus 策略中选择了此选项时，此选项方会显示。



要使用上述选项，必须先在 Anti-Virus 策略中指定该等选项。有关详细信息，请参阅*创建 Anti-Virus 策略*。



命令行控制

本章说明 Faronics Anti-Virus 可用的各种命令行控制。

主题

命令行控制

命令行控制

Faronics Anti-Virus 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实施控制，使网络管理员能够更灵活的管理 Faronics Anti-Virus 工作站。

要运行 Faronics Anti-Virus 的命令，请完成以下步骤：

1. 在工作站上，通过命令提示符依次转至 < *系统目录* >:*Program Files**Faronics**Faronics Anti-Virus Enterprise*。
2. 输入 `AVECLI\[ 命令 ]`

可用的命令如下：

命令	定义
`definitionversion`	显示病毒定义版本。
`scanengineversion`	显示扫描引擎版本。
`updatedefs`	更新并应用病毒定义。
`setlicense[key]`	应用授予的许可证密钥。
`scanquick`	开始快速扫描。
`scandeep`	开始深度扫描。

语法：

```
AVECLI\definitionversion
```

卸载 Faronics Anti-Virus

本章介绍如何卸载 Faronics Anti-Virus。

主题

卸载概述
通过 Faronics Core 控制台卸载 Faronics Ant-Virus 客户端
通过“添加或删除程序”卸载工作站上的 Faronics Anti-Virus 客户端
使用安装程序卸载 Faronics Anti-Virus 插件
通过“添加或删除程序”卸载 Faronics Anti-Virus 插件

卸载概述

Faronics Anti-Virus 插件在 Faronics Core 控制台（或 Faronics Core 服务器）系统中安装。Faronics Anti-Virus 客户端在工作站上安装。

可手动或通过 Faronics Core 控制台卸载工作站上的 Faronics Anti-Virus 客户端。一旦完成此操作后，即可卸载 Faronics Core 控制台（或 Faronics Core 服务器）系统中的 Faronics Anti-Virus 插件。

卸载步骤将在接下来的各节中说明。

通过 Faronics Core 控制台卸载 Faronics Ant-Virus 客户端

要通过 Faronics Core 控制台卸载 Faronics Ant-Virus 客户端，请完成以下步骤：

1. 启动 Faronics Core 控制台。
2. 在*控制台树窗格*中，依次转至 *Faronics Core 控制台 >[Core 服务器]> 托管工作站*。
3. 选择要卸载 Faronics Anti-Virus 客户端的工作站。
4. 右键单击并选择*配置工作站 > 高级 > 卸载 Anti-Virus 客户端*。

此时将从工作站上卸载 Faronics Anti-Virus 客户端。

通过“添加或删除程序”卸载工作站上的 Faronics Anti-Virus 客户端

要通过 Windows 中的*添加或删除程序*卸载 Faronics Anti-Virus，请完成以下步骤：

1. 依次单击*开始* > *控制面板* > *添加或删除程序*。
2. 选择 *Faronics Anti-Virus Enterprise 工作站*。
3. 单击*删除*。

此时将从工作站上卸载 Faronics Anti-Virus 客户端。

使用安装程序卸载 Faronics Anti-Virus 插件

要卸载 Faronics Anti-Virus 插件，请完成以下步骤：

1. 双击 *Anti-VirusLoadinInstaller.exe*。单击 *下一步*。



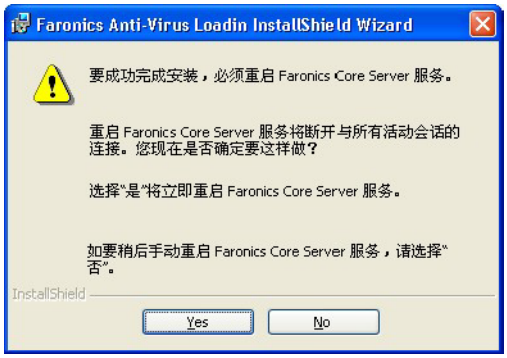
2. 选择*删除*。单击 *下一步*。



3. 单击*删除*。



4. 此时将显示以下消息。单击*是*重新启动 *Faronics Core Server* 服务，或单击*否*稍后再手动重启 *Faronics Core Server* 服务。



5. 此时将从您的计算机中删除 Faronics Anti-Virus 插件。单击*完成*结束卸载。



通过 “ 添加或删除程序 ” 卸载 Faronics Anti-Virus 插件

要通过 Windows 中的*添加或删除程序*卸载 Faronics Anti-Virus 插件，请完成以下步骤：

1. 依次单击*开始* > *控制面板* > *添加或删除程序*。
2. 选择 *Faronics Anti-Virus 插件*。
3. 单击*删除*。