



Faronics ANTI-VIRUS

ADVANCED System Integrity



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

序言
重要信息6
关于 Faronics
产品文档6
技术支持7
联系信息
术语定义
简介
Faronics Anti-Virus 概述
系统要求
Faronics Anti-Virus 要求13
Faronics Core 要求
Deep Freeze 要求
Faronics Anti-Virus 许可证
安装 Faronics Anti-Virus
安装概述
安装 Faronics Core16
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
在工作站上手动安装 Faronics Anti-Virus21
使用 Faronics Anti-Virus
Faronics Anti-Virus 概述
通过 Faronics Core 控制台管理 Faronics Anti-Virus 25
在工作站上部署 Faronics Anti-Virus 客户端
配置 Faronics Anti-Virus
刷新 Faronics Anti-Virus
Faronics Anti-Virus 策略
创建 Anti-Virus 策略
应用 Anti-Virus 策略
查看或修改 Anti-Virus 策略
重命名 Anti-Virus 策略
复制策略
删除 Anti-Virus 策略
导入 Anti-Virus 策略
导出 Anti-Virus 策略
通过 Faronics Core 控制台扫描 50
查看隔离的文件并对其进行操作 51
查看通过 Faronics Core 控制台更新 Faronics Anti-Virus



通过 Faronics Core 控制台计划 Faronics Anti-Virus 的操作	53
生成报告	54
全局报告	54
特定工作站报告	54
在工作站上使用 Faronics Anti-Virus	55
在工作站上启动 Faronics Anti-Virus	55
扫描工作站	
通过右键单击扫描文件或文件夹	57
查看扫描历史记录	58
查看隔离的文件并对其进行操作	
在工作站上更新 Anti-Virus 定义	60
通过系统任务栏管理工作站上的 Faronics Anti-Virus	61
命令行控制	63
命令行控制	64
卸载 Faronics Anti-Virus	65
卸载概述	
通过 Faronics Core 控制台卸载 Faronics Ant-Virus 客户端	67
通过"添加或删除程序"卸载工作站上的 Faronics Anti-Virus 客户端	68
使用安装程序卸载 Faronics Anti-Virus 插件	69
通过"添加或删除程序"卸载 Faronics Anti-Virus 插件	



序言

本用户指南介绍如何安装和使用 Faronics Anti-Virus。



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. 5506 Sunol Blvd, Suite 202 Pleasanton, CA, 94566 USA

Faronics Corporation (加拿大和国际) 609 Granville Street, Suite 620 Vancouver, BC V7Y 1G5 Canada

Faronics Corporation (欧洲) 8 The Courtyard, Eastern Road, Bracknell, Berkshire, RG12 2XB, United Kingdom





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。
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。
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 <i>通知</i> 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 <i>万灵丹</i> 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。



术语	定义
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。
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 <i>间谍软件</i> ,因为这 些软件无需通知用户即可使用。
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 <i>恶意攻击行为</i> ;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。

10 序言





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 7 (32 位或 64 位)
- Windows 8.1 (32 位或 64 位)
- Windows 10 (最高 22H2 版) (32 位或 64 位)
- Windows 11 (最高 22H2 版) (32 位或 64 位)
- Windows Server 2008 R2 (64 位)
- Windows Server 2012 (64 位)
- Windows Server 2016 (64 位)
- Windows Server 2019 (64 位)
- Windows Server 2022 (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。

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。



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。



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。

🔂 Faronics Anti-Virus	4 Loadin - InstallShield Wizard	×
客户信息 请输入您的信息。		
用户姓名(U):	AdminUser	
单位(<u>O</u>):	Faronics corporation	
		_
<u>许</u> 可证密钥:		
	厂 使用评估版 (30 天)(E)	
InstallShield	版本	4.0.2100.342
	<上一步(B) 下一步(N) >	取消

4. 默认的位置为 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 石在稍后手动重启 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:

- 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*。

😸 Faronics Anti-Virus - Instal	Shield Wizard
	Welcome to the InstallShield Wizard for Faronics Anti-Virus
	The InstallShield(R) Wizard will install Faronics Anti-Virus on your computer. To continue, dick Next.
	WARNIING: This program is protected by copyright law and international treaties.
www.faronics.com	Version: 4.0.2102.342
	< Back Next > Cancel

2. 阅读并接受许可协议。单击下一步。

😸 Faronics Anti-Virus - InstallShield Wizard	x
License Agreement Please read the following license agreement carefully.	
Faronics Anti-Virus - License Faronics Corporation	^
Copyright 2004 - 2017 All Rights Reserved Master Software License Agreement	
LICENSE GRANT: Faronics hereby grants Licensee a limited, non-exclusive license to install, use, access, display, run, or otherwise interact with (collectively, "Use") the Products on the number of computers or classrooms set out across from the heading 'Number of Licenses'	Ŧ
I accept the terms in the license agreement Print I do not accept the terms in the license agreement	
Version: 4.0.2102.342 InstallShield	2



3. 单击*安装*安装 Faronics Anti-Virus。

😸 Faronics Anti-Virus - InstallShield Wizard	x
Ready to Install the Program The wizard is ready to begin installation.	
Click Install to begin the installation.	
If you want to review or change any of your installation settings, click Back. Click Cancel exit the wizard.	to
Version: 4.0.2102.	342
< Back Sinstal Cance	el

4. 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 查看通过 Faronics Core 控制台更新 Faronics Anti-Virus 通过 Faronics Core 控制台计划 Faronics Anti-Virus 的操作 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
- 启用/禁用防火墙
- 查看扫描历史记录
- 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
- 启用/禁用主动保护
- 查看日志

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。
- 启用/禁用主动保护
- 启用/禁用防火墙
- 查看扫描历史记录
- 已隔离



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:

() Faronics Anti-Virus - 配置	×
更新 代理服务器	
病毒定义版本	.
Anti-Virus 防病毒(32位): 95350 (2017/1/9 14:40:47)	
Anti-Virus 防病毒(64 位): 65199 (2017/1/9 14:41:19)	
更新设置 ————————————————————————————————————	.
▶ 自动更新于: 2 小时	
检查更新设置	.
上次更新检查的日期/时间: 2017/1/9 14:52:40 立即更新	
下次更新检查的日期/时间: 2017/1/9 16:52:40	
更新状态:正在检查并下载更新	
确定(O) 取消	(N)
配置、更新	

- > 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:

(Faronics Anti-Viru	5-配置	×
	更新 代理服务器		
	☑ 使用代理服务器	导与更新 Web 服务器通信	
	代理服务器信息		
	地址:	127.13.1.45 端口: 1268	
	用户身份验证 —		
	☑ 代理服务器需	₽授权(登录凭据)	
	身份验证类型	Basic	
	用户名:		
	密码:		
	域:		
	测试		
		确定(O) 取消(N)	
đ	2置\代理服务器		

- 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。

如果您正在使用旧版 Anti-Virus · 请完成以下步骤以迁移至新版 Anti-Virus :



- 1. 从托管工作站中卸载旧版 Anti-Virus。
- 2. 配置新版 Anti-Virus 策略。
- 3. 在托管工作站中安装新版 Anti-Virus。



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 Console。
- 2. 在*控制台树窗格*中, 依次转至 Faronics Core 控制台 > [Core 服务器名称]> 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。

🌘 新策略	<u>></u>	4
策略名称:	ļ	1
	· 補定 取消	

- 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。



• 用户操作窗格

後新聞 新聞 新		×
 □ ▲ 工作均估设置 用户操作 记录操作 说录操作 Windows 安全中心 更新 代理 ○ 和描英型 USB 设备 计划 扫描美常 清理操作 ④ 医防火墙(保护 设置 程序规则 网络规则 高级规则 信任区 	 	
等略详细信良\丁作誌设置\用户操作	确定(K) 取消(L) 应用(P)	

- > 显示任务栏图标 选中此复选框可在工作站的任务栏中显示 Faronics Anti-Virus 防病毒图标。如果没有选中此复选框,则 Faronics Anti-Virus 防病毒将对用户隐藏。
 - ~ 允许手动扫描 选中此复选框可允许用户手动启动工作站的 Faronics Anti-Virus 防病毒扫描。
 - ~ 允许用户对扫描结果进行操作 选中此复选框可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。



• 记录操作窗格

🚯 策略详细信息 Default	<u>></u>	1
 □ ▲ 工作站设置 用户操作 记述操作 记述操作 记述操作 》 和描设置 扫描设置 扫描设置 扫描读型 USB设备 计划 扫描异常 清理操作 ● ● 立切保护 已 ■ 防火墙保护 设置 程序规则 网络规则 信任区 	 記录操作 事件报告级别: 无 ■ 承动日志文件,最多 10 MB,40 MB 磁盘空间总量 	
策略详细信息\工作站设置\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 防病毒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)。



• Windows 安全中心窗格

🚯 策略详细信息 Default		×
□ ① 工作おお设置 用户操作 记录操作 ● ● 更新 代理 □ ● 扫描设置 扫描读型 USB 设备 计划 扫描异常 清理操作 ● ● □ ● ● ● ○ <td>Windows 安全中心 ☑ 集成到 Windows 安全中心</td> <td></td>	Windows 安全中心 ☑ 集成到 Windows 安全中心	
策略详细信息\工作站设置\Windows 安全中心	 	:

> 集成到 Windows 安全中心 – 选中此复选框可将 Faronics Anti-Virus 防病毒集成到 Windows 安全中心。Windows 安全中心将通过系统任务栏通知您 Faronics Anti-Virus 防病毒是否处于活动状态。

•



 □ ▲ 工作站设置 用户操作 记录操作 Windows安全中心 更新 代理 	更新 ▼如果没有遠冻企业控制台运信在过去,连接到web服务器更新 20	4 🔹 小时
 代理 ○ 2 扫描设置 扫描类型 USB 设备 计划 扫描异常 清理操作 查式》保护 设置 段大塘(保护 设置 程序规则 网络规则 高级规则 信任区 	Anti-Virus 防病毒定义更新 ⑦ 使用 Anti-Virus 防病毒定义中途 ● 服务器 IP 192.168.6.242 ● 服务器名称 3月日 7724	
医略详细信息\工作站设置\Windows 安全	 بەن	确定(K) 取消(L) 应用

> 如果在过去 X 小时内未与 Faronics Core Server 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。

• *代理窗*格

▲ \$P\$ \$P\$ \$P\$ \$P\$ \$P\$ \$P\$ \$P\$ \$P\$ \$P\$ \$P	
	A
□ 工作站设置 用户操作 记录操作 吸射 更新 ● 扫描设置 扫描送型 USB 设备 计划 扫描异常 清理操作 主动保护 ● ■ おん/増保护 设置 程序规则 岡崎規則 高級规则 高級規則 信任区	代理 如果工作站需要使用代理才能访问 Faronics Core 服务器或更新 Web 服务器, 请按以下配置设置。 □ 启用代理 代理服务器信息 地址: 端口: 用户身份验证 「代理服务器需要授权(登录凭据) 身份验证类型: Basic 夏台 「 城: 「
	确定(K) 取消(L) 应用(P)

- > 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。
- > 代理服务器信息 指定 地址和 端口。
- > 用户身份验证

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*扫描设置*。

策略详细信息 Default ① □					X
□ □ 3 工作站设置 用户操作 记录操作	扫描类型				
Windows 安全中心 再新		快速	深度系统	自定义	
代理	启用 Rootkit 检测		V		
□ □ 参 扫描设置 扫描类型	在存档内扫描				
USB 设备	排除可移动驱动器				
日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日本の日	扫描注册表	\checkmark	×		
清理操作 小 注 注 : : : : : : : : : : : : : : : : :	扫描正在运行的进程	\checkmark	\checkmark		
日 藍 防火墙保护					
2011	Max archive file size limit:	100 🛨 🕴	MB		
网络规则 高级规则			恢复默	试值(G)	
信任区					
			确定(K)	取消(L)	应用(P)

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,在扫描时扫描存档文件(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。指定文件大小限制。
- > 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。



• USB 设备窗格

🕼 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 □ ● □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	 USB 设备 ● 正在进行其它扫描时不执行 USB 扫描(进行中的扫描完成以后,系统不会自动扫描 USB 设备,必须手动扫描) ● 中断活动的扫描以执行 USB 扫描(被中断的扫描不会恢复) ■ 取消进程对话中的 USB 扫描
策略详细信息\扫描设置\USB 设备	稍定他 取消止 应用P

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:

- > 正在进行其他扫描时不执行 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。
- > 抑制进行中的 USB 扫描对话 选择该选项可隐藏反病毒程序正在扫描所插入的 USB 驱动器的指示;无反病毒程序界面打开·系统托盘图标将不显示工具提示框来 表明扫描正在进行中。如发现病毒·用户将在扫描结束后收到通知;如未检测到病 毒·用户将不会收到扫描通知。

注意,如果插入时扫描 USB 驱动器选项未选择,该选项将被忽略。



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。



*计划*窗格 • 🕼 策略详细信息 Default × 🗆 🖂 工作站设置 计划 用户操作 记录操作 快速扫描 Windows 安全中心 更新 ☑ 启用快速扫描 代理 启动 8:00 🕴 停止 🖲 扫描完成时 🗆 👶 扫描设置 扫描类型 O 9:00 USB 设备 计划 □ 星期六 🗹 星期五 🗹 星期四 🗹 星期三 🗹 星期二 🔽 星期一 🗆 星期日 扫描异常 清理操作 深度扫描 🐠 主动保护 □ ஊ 防火墙保护 □ 启用深度扫描 设置 停止 🖲 扫描完成时 启动 1:00 * * 程序规则 • 3:00 ÷ 网络规则 高级规则 信任区 □ 星期六 🖸 星期五 🗹 星期四 🔽 星期三 🔽 星期二 🔽 星期日 选项 以 2 分钟为单位随机安排计划扫描开始时间 启动时未执行的扫描选项 ◎ 不执行快速扫描 大约启动 5 (5-60)分钟后执行快速扫描 ○ 提示用户执行快速扫描 确定(K) 取消(L) 策略详细信息\扫描设置\计划

快速扫描:

- > 启用快速扫描 选中此复选框可启用 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 选择执行已排程快速扫描的日期。

深度扫描:

- > 启用深度扫描 选中此复选框可启用深度扫描。
- > 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 选择执行已排程深度扫描的日期。


选项:

> 以x分钟为单位随机排程扫描开始时间 – 指定分钟数。随机排程扫描开始时间以减 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:如果排程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 防病毒应在启动多少分 钟后执行快速扫描。
- > 提示用户执行快速扫描 选择此选项可提示用户执行快速扫描。



• 扫描例外窗格

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*选项卡的文件将始终被 Faronics Anti-Virus 防病毒扫描。但是·Faronics Anti-Virus 防病毒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将不会被报告为恶意。

A. 单击*添加*。

 □● 工作站设置 用户博作 记录操作 Windows 安全中心 更新 (七環) (七環) (日本)设置 「日本(公置) (日本)设置 USB 设备 	扫描异常 指定受合的文件和文件表。文件或文件表述 意式受感染的文件 以下列表列出了不会被报告为病毒的项目。 添加(A) 全地(S) 从列民冊	动后,Faronics Ant , 涂(D)	i-Virus 就不会将这些文(+报告为恶
计划	名称	类型	已添加日期	用户
	C:\Users\AdminUser\Desktop\FC_4.10.21 C:\Users\AdminUser\Desktop\FC_4.10.21	文件名和路径 文件类	2017/1/9 15:16 2017/1/9 15:16	FaronicsCor FaronicsCor

B. 在*添加*对话框中,选择*文件完整路径、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*。

🚺 添加	加扫描例外
允许	文件完整路径 ▼
	C:\Users\Administrator\Desktop\Faronics 刻宽(图)
	确定 (近) 取消

C. 文件完整路径将添加到扫描例外窗格中。

 □ ▲ 工作お役置 田戸株作 记泉株作 Windows 安全中心 更新 代理 ○ ● 扫描決型 订相能关型 USB 设备 	扫描异常 指定安全的文件和文件夫。文件或文件夫 意或愛感染的文件 以下列表列出了不会納退告対病毒的项目。 添加(A) 全銭(5) 人列表冊	动后,Faronics Ant 论(D)	i-Virus 就不会将这些文的	并报告为恶
计划	名称	类型	已添加日期	用户
対曲テ市	C:\Users\AdminUser\Desktop\FC_4.10.21	文件名和路径	2017/1/9 15:16	FaronicsCor
/育理(木)ド	Anti-Virus_Ent_32-bit.msi	文件名	2017/1/9 15:16	FaronicsCor
日誌 防火墻保护 设置 程序规则 网络规则 高级规则 合权互互			2017/1/3 13.16	



• *清理操作*窗格

🜘 策略详细信息 Default			×
□ ▲ 工作均估设置 用户操作 记录操作 U动操作 更新 代理 ○ 2 扫描设置 扫描设置 日抽设置 日抽算常 通道操作 ● ●	 清理操作 对受感染的文件进行的默认操作 ○ 清理/隔离 检查到威胁后,尝试对文件杀毒,如果不成功则将其隔离。 ○ 清理/删除 检查到威胁后,尝试对文件杀毒,如果不成功则将其删除。 ☑ 从隔离中删除早于 3 天的项目 		
笙般祥如信自\扫描设架\法神操作		确定(K) 取消(L) 应用(P)	

- > 清理 / 隔离 检查到威胁后,尝试对文件杀毒,如果不成功则将其隔离。
- > 清理 / 删除 检查到威胁后,尝试对文件杀毒,如果不成功则将其删除。
- > 删除隔离区中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。



8. 指定*主动保护*窗格中的设置。

🚯 策略详细信息 Default		x
□	 ▶ 主动保护 ▶ 主动保护 ▶ 建动保护 ▶ 建动保护 ▶ 建成生产结晶、、 (1) ▶ 建成生产结晶、 (1) ▶ 建成生产结晶、 (1) ▶ 建成生产结晶、 (1) ▶ 通用主动保护 ▶ ● 常用主动保护 ▶ ● ● 第二 ▶ ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●	
策略详细信息\主动保护	In some (c. 4) International Control (c. 1)	

- 启用主动保护 选择此选项可启用实时保护。主动保护是指 Faronics Anti-Virus 防病 毒在后台进行实时扫描,不会对系统性能产生任何影响。如果存在实时从 Internet 感 染病毒的风险,请选择此选项。
 - > 允许用户关闭主动保护 选择此选项可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 选择此选项可在主动保护期间检测到威胁时显示警报。如果不希望显示警报,请不要选中此复选框。



9. 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。您可*允许*或*阻止*通信。

• 设置窗格

🜒 策略详细信息 Default		×
 □ <li< th=""><th>设置 防火增保护设置 ◎ 鳥用基本的防火増保护 ◎ 允许用户禁用防火増 □ 鳥用防火増日志记录</th><th></th></li<>	设置 防火增保护设置 ◎ 鳥用基本的防火増保护 ◎ 允许用户禁用防火増 □ 鳥用防火増日志记录	
	确定(K) 取消(L) 应用(P)]
策略详细信息\防火墙保护\设置		

防火墙保护设置

- > 启用基本的防火墙保护 选中此复选框可启用防火墙保护。防火墙保护可阻止黑客 或恶意软件通过 Internet 或网络获取对您计算机的访问权限。
 - ~ 允许用户禁用防火墙 选择此选项可允许用户在计算机上禁用防火墙。
 - ~ 启用防火墙日志记录 选择此选项可将防火墙有关的所有操作进行日志记录。



• 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。

 □ 3. 工作お设置 用户操作 记录操作 吸引(1) · · · · · · · · · · · · · · · · · · ·	程序规则 程序规则定义防 规则。默认规则同 添加(A)	火墙对来自或去往应料 丁以进行编辑,但是无 编辑(E)	月程/序的网络活 法删除。 :(M)	动所采取的操	ff。程序规则的	的优先级高于默计	il
다 고파 곳포 USB 设备	名称	程序	信任区入站	信任区出站	非信任区2	非信任区出	站 🔺
计划	Faronics Event	%PROGRAMFILES	允许 🔹	允许	 ▲ ★ 允许 	▼ 允许	•
清理操作	Faronics Core	%PROGRAMFILES	允许 •	允许	▼ 允许	▼ 允许	-
→ ◆ 主动保护 □ ■ Stubie(215	Faronics Anti-Vi	%INSTALL_DIR%\	允许 🔹	允许	▼ 允许	▼ 允许	•
· · · · · · · · · · · · · · · · · · ·	Faronics Anti-Vi	%INSTALL_DIR%\	允许 🔹	允许	▼ 允许	▼ 允许	•
程序规则	Faronics Anti-Vi	%INSTALL_DIR%\	允许 🔹	允许	▼ 允许	▼ 允许	-
网络规则 高级规则	Faronics Core	%PROGRAMFILES	允许 🔹	允许	▼ 允许	▼ 允许	-
信任区	Faronics Enterp	%PROGRAMFILES	允许 🔹	允许	▼ 允许	▼ 允许	-
	Internet Explorer	%PROGRAMFILES	允许 🔹	允许	▼ β且止	▼ 允许	-
	lsass.exe	%WINDIR%\system	№日止 ▼	允许	▼ 阻止	▼ 允许	-
	services.exe	%WINDIR%\system	ß∄⊥ட் ▼	允许	▼ 月上	▼ 允许	-
	winlogon.exe	%WINDIR%\system	ß∄⊥ட்	允许	▼ B且⊥E	▼ 允许	-
	svchost.exe	%WINDIR%\system	ß∄⊥£ ▼	允许	▼ 允许	▼ 允许	-
	Deep Freeze S	%PROGRAMFILES	允许 🔹	允许	▼ 允许	▼ 允许	-
	Deep Freeze A	%PROGRAMFILES	允许 🔹	允许	▼ 允许	▼ 允许	-
	Deep Freeze C	%PROGRAMFILES	允许 🔹	允许	▼ 允许	▼ 允许	
	L			;	确定(K)	取消(L)	应用(P)

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*。此时将显示以下 参数:

(1) 添加規則		×
程序规则可为特定程序授予权限。程序规 置。	1则的优先级高于"任何其它应)	用程序 规则设
名称:		
程序:		
示例: c:\path\program.exe		浏览(R)
%ProgramFiles%\browser\browse	r.exe	
信任区入站:	允许	
信任区出站:	允许	
非信任区入站:	允许	
非信任区出站:	允许 💌	
<u>什么是区?</u>	,确定(0)	取(jij(N)

- > 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 (允许或阻止)。
- > 信任区出站 对来自信任区程序的出站通信应执行的操作 (允许或阻止)。
- > 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 (允许或阻止)。
- > 非信任区出站 对来自非信任区程序的入站通信应执行的操作 (允许或阻止)。



• 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。

エ作站设置 用户操作 ア ア プ ア プ ア プ マ プ マ プ マ プ マ プ マ プ マ プ マ プ マ プ マ プ マ プ マ ジ マ ジ マ ジ マ ジ マ ジ マ ジ マ ジ ジ マ ジ	 络規則 ^{路规则定义防火1}	啬对网络活动所采取的	操作。网络规	l Dij	可以进行编辑	뮵,	但是无法删除	除。		
代理 多 扫描设置	跡	描述	信任区入站	i	信任区出站		非信任区入 站		非信任区出	站
	MP I ng I herlcmp (Internet Group Manag Ping and Tracert Other ICMP packets	允许 允许 允许 <u>余</u> 许	- - -	允许 允许 允许 允许	• • •	 允许 允许 允许 ☆ 対 	• • •	允许 允许 允许 众 许	• • •
▼ 王初末护 Dr ■ 防火墙保护 DN 设置 VP 週路规则 BC 高级规则 LD 信任区 K	NS YN CAST DAP	Domain Name System Virtual Private Network Broadcast Lightweight Directory	允许 允许 允许 允许 允许 允许 允许	• • • • • •	んけ 允许 允许 允许 允许 允许 允许 允许	* * * *	允许 允许 允许 允许 允许 允许 允许	• • • •	允许 允许 允许 允许 允许 允许 允许 允许	* * * *
NE	TBIOS	Microsoft File and Prin	允许	•	允许	•	允许	•	允许	•
				_		_		_		



为以下选项选择网络规则:

名称	描述	信任区入站	信任区出站	非信任区入 站	非信任区入站
IGMP	Internet 组管理 协议	选择允许或阻 止	选择允许或阻 止	选择允许或 阻止	选择允许或阻 止
Ping	Ping 以及 Tracert	选择允许或阻 止	选择允许或阻 止	选择允许或 阻止	选择允许或阻 止
其他 ICMP	其他 ICMP 包	选择允许或阻 止	选择允许或阻 止	选择允许或 阻止	选择允许或阻 止
DHCP	动态主机配置协议	选择允许或阻 止	选择允许或阻 止	选择允许或 阻止	选择允许或阻 止
DNS	域名系统	选择允许或阻 止	选择允许或阻 止	选择允许或 阻止	选择允许或阻 止
VPN	虚拟专用网络	选择允许或阻 止	选择允许或阻 止	选择允许或 阻止	选择允许或阻 止
BCAST	发布	选择允许或阻 止	选择允许或阻 止	选择允许或 阻止	选择允许或阻 止
LDAP	轻量级目 录访问协议	选择允许或阻 止	选择允许或阻 止	选择允许或 阻止	选择允许或阻 止
Kerberos	Kerberos P 协议	选择允许或阻 止	选择允许或阻 止	选择允许或 阻止	选择允许或阻 止
NETBIOS	Microsoft 文件和 打印机共享	选择允许或阻 止	选择允许或阻 止	选择允许或 阻止	选择允许或阻 止



• 高级规则窗格

高级规则可以定义防火墙针对指定应用程序、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。

● 工作站设置 First设置 First设置 ● 引着设置 · 高级规则的处理顺序即为列出顺序。 ● 扫描设置 · 活动设置 1 描述设置 · 活动设置 1 描述设置 · 指描读型 USB 设备 · 指示 1 指数设置 · 福田() 1 活動完裕 · 福田() ● 芝 动作用 · 市市() · St 动保护 · 福田() · 日本 · 「「「」 · 「「」 · 「「」 · 「「」 · 「「」 · 「」 · 「「」 · 「」 · 「「」 · 「」 · 「」 · 「」 · 「」 · 「」 · 「」 · 「」 · 「」 · 「」 · 「」 · 「」 · 「」	④ 工作站设置 用户操作 记录操作	高级规则	ſ					
代理 Table Participa Participa 扫描決型 USB 设备 计划 古描字常 透程 计划 扫描异常 道理操作 方向 协议 本地端 「書理操作 方向 协议 不地端 通信	Windows 安全中心 更新	添力n(A)	2理顺序即为列出 编辑(F)		后 F(I)	6TEM	1	
日期示予 清理操作 ③ 至初保护 设置 程序規则 网络规则 高强规则 信任区	代理 分 扫描设置 扫描设置 日描类型 USB设备 计划	名称 FaronicsSA	程序	操作 允许	 方向 ▼ 两者 	bù 协议 ▼ UDP	」 本地端 口 7726	」远程 「端□ 任何端□
	11冊F市 清理操作 ● 主动保护 ■ 防火増保护 设置 程序規則							
	网络规则 高级规则 信任区							
The second s						****	Testilas	

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:

🜔 添加高级規則		×
高级规则定义的 地或远程端口以	防火墻针对指定的应用程序、端□或 从及流量方向,或者是它们的组合。)	协议所采取的操作。其中可能包括单个协议、本 数可以添加、编辑或删除高级规则。
名称:		
, 程序(留空则应	用于所有程序):	
		浏览(R)
示例: c:\pa %Prog	th\program.exe ramFiles%\browser\browser.exe	
操作:	允许	
方向:	两者	
协议类型:	TCP	添加(A)
		冊JF条(M)
本地端口:	所有端口	
	元例: 80, 443, 5000-5010	
远程峭□∶	所有端口	
	示例: 80, 443, 5000-5010	· 确定(0) 取消(N)

- > 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 (*允许或阻止*)。
- > 方向 通信的方向 (*双向、入站*或出站)。
- > 协议类型 协议的类型 (ICMP、IGMP、TCP、UDP) 和名称。
- > 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。



• *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。

□ 「「作坊设置 用申特作 记录操作 Windows 安全中心 更新 代理 日本描述型 信任区 信任区常定代态为安全的计算机、网络和 IP 地址。应用程序或网络规则可为信任区和 Internet (非信 包区结子区别对待。 □ 伊福设置 日本描述型 本加(A) 常服(E) □ 日福设置 常服(A) □ 日福设置 常服(A) □ 日福设置 常服(A) □ 日福设置 常服(A) ○ 日福(A) 常服(A) □ 日福(A) 常服(A) ○ 日福(A) 常服(A) ○ 日本(A) 日本(A) ○ 日本(🚯 策略详细信息 Default				X
USB 设备 注射 计划 扫描异常 清理操作 注意 ● 主动保护 送置 程序规则 网络规则 高级规则 高级规则 「言王区 () ////////////////////////////////////	 ○ ▲ 工作時設置 用户操作 记录操作 Windows 安全中心 更新 代理 ○ 和描设置 扫描设置 扫描设置 	信任区 信任区指定状态为安全的计算机、网络和 IP 地址。应用程序或网络规则 任)区给予区别对待。 添加(A) 编辑(E) 删除(M)	可对信任区和	Internet(非信	
	030 度留 计划 扫描异常 清理操作 ● 註詞保护 设置 程序规则 网络规则 高级规则 『言王区	名称 描述	<u> </u>	地址	
		确定	(K) 取消	斯(L) 应用(P))

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

🌘 添加信任区	X			
—————————————————————————————————————				
名称:				
l				
描述:				
地址类型:	IP 地址 ▼			
IP 地址:	· · ·			
	确定(0) 取消(N)			

- > 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 地址或 网络)。

10.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 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 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 *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。



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 Console。
- 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

要刪除现有策略,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。

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。



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。
 - > 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。

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。



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。



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。

Faronics A	Anti-Virus						
Sin	高离 高离屏幕上 几中删除隔	将显示 Faronics Anti- 离的风险。	Virus 🛱	鹤的所有风险。您可	「以查看单个风险的	〕详细信息、从隔离区中还原风	风险或从计算
已隔离的风	险:1						
计算机名称	F I	名称		已添加日期	时间(天)	文件路径	
WIN-QEEM	BO25F0L	EICAR-Test-File (not a	i virus)	2017/1/9 15:37:00	0	C:\Users\AdminUser\Desktop\	EICAR.txt
己成功检索	k WIN-QEI	EM8025FOL 的隔离项	1.				
全选		从隔离区还原	从	计算机中删除			关闭

- 5. 将显示每个受感染文件的以下信息:
 - > 风险名称
 - > 文件名
 - > 原位置
 - > 已添加日期
 - > 时间(天)
- 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。

Faronics ANTI-VIRUS TRUSTED Threat Protection 報送()	扫描(5) 历史记录(H)	_ × 隔离(0)
受保护 所有保护设置被启用并且是最新的	主动保护 _{已启用}	臣王 防火墙保护 _{已启用}
风险检测统计 扫描已完成: 1 通过"扫描"已清除风险: 0 通过"主动保护"已拦截风险: 0 通过防火墙已拦截: 216 已清除或已拦截的所有风险: 216 重置计数(8)	更新状态 自动更新已启用 扫描引擎: v3.0.5.370 定义: v105130 2019/1/8 10:39:36 立即更新(U)	日描状态 上次扫描: 2019/1/8 13:12:25 下次扫描: 2019/1/9 8:00:00 立即扫描(い)
		www.faronics.com (j)

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。
- 防火墙保护显示工作站是否受到防火墙的保护。
- 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 •

Faronics ANTI-VIRUS TRUSTED Threat Protection 被途()	扫描(S) 历史记录(H)	_ × 「福离(Q)
受保护 所有保护设置被启用并且是最新的	主 动保护 _{已启用}	防火 靖保 护 _{己高用}
知险检测统计 扫描已完成: 1 通过"扫描"已清除风险: 0 通过"主动保护"已拦截风险: 0 通过防火墙已拦截: 216 已清除或已拦截的所有风险: 216 重置计数(P)	更新状态 自动更新已启用 扫描引擎: v3.0.5.370 定义: v105130 2019/1/8 10:39:36 立即更新(U)	月描状态 上次扫描: 2019/1/8 13:12:25 下次扫描: 2019/1/9 8:00:00 立即扫描(N)

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。

正在扫描文件 Faronics Anti-Virus 当前正在扫描您的计算机。扫描期间可以查看其他 Faronics Anti-Virus 功能。	
检测到的风险: 0 风险 包含 0 疑似点 经过的时间: 00:00:05 大约剩余 8 分钟	10 0
风险名称 风险类别 风险疑似点	
	^
(c). 上口 55	



- 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。

		概述①	扫描(5)	历史)	, (H)	X 隔离(Q) (2显示发现有风险的扫描(W)
开始日期/时间	持续时间(分钟秒)扫描类	型 运行类型		所有风险	风险已清除	 定义版本
2019/1/8 13:03:52	08:32 快速	手动		0	0	105130
详细信息(<u>D</u>)						

- 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。

	IRUS STED Threat Protection	歡述①	扫描(5)	历史记录(1)	_ × 隔离(Q) 已隔离的风险: 1
名称	已添加日期		时间 (天)	文件路径	
EICAR-Test-File (not a virus)	2019/1/8 13:49:47		0	UNC\vboxsrv\Shared\EICAR\e	icar.com.txt
还原(<u>R</u>) 删除(<u>D</u>)					
					www.faronics.com (j)

- 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
 - > 已添加日期
 - > 时间(天)
 - > 隔离执行者



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 ·

Faronics ANTI-VIEUS TRUSTED Threat Protection 数述@	扫描(5) 历史记录(1)	_ ×) 隔离()
受保护 所有保护设置被启用并且是最新的	() 主动保护 _{已启用}	萨尔 防火 墙保护 已启用
风险检测统计 扫描已完成: 1 通过"扫描"已清除风险: 0 通过"主动保护"已拦截风险: 0 通过防火墙已拦截: 216 已清除或已拦截的所有风险: 216 重置计数(8)	更新状态 自动更新已启用 扫描引擎: v3.0.5.370 定义: v105130 2019/1/8 10:39:36 立即更新(U)	人 扫描状态 上次扫描: 2019/1/8 13:12:25 下次扫描: 2019/1/9 8:00:00 立即扫描(N)

2. 在 更新状态窗格中,单击 立即更新。此时将显示 立即更新对话框。



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。
- 防火墙保护 > 启用或禁用。



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 " 添加或刪除程序 " 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。

🙀 Faronics Anti-	/irus 4 Loadin InstallShield Wizard
程序维护 修改、修复或删释	^{余程序。}
○ 修改(M)	更改要安装的程序功能。此选项可显示"自定义选择"对话框,在其 中您可以更改安装功能的方式。
○ 修复(P)	修复程序中的错误。通过此选项您可修复缺少或损坏的文件、快捷 方式和注册表项。
◎ 删除(R)	从计算机中删除 Faronics Anti-Virus 4 Loadin。 版本 4.0.2100.346
InstallShield ———	<上一步(B) 下一步(N) > 取消

3. 单击*删除*。

🚏 Faronics Anti-Virus 4 Loadin InstallShield Wizard
删除程序 您已经选择从采统中删除此程序。
单击"删除"从计算机中删除 Faronics Anti-Virus 4 Loadin 。删除后此程序将不能再使 用。
要查看或更改任何设置, 诸单击"上一步"。
版本 4.0.2100.346
<上一步(B) 删除(R) 取消

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*。

