ESET Endpoint Antivirus

用户指南

单击此处显示此文档的联机版本

ESET Endpoint Antivirus 由 ESET, spol. s r.o. 开发

有关更多信息，请访问 www.eset.com。

客户服务：www.eset.com/support

修订日期 2022年m月4日

ESET Endpoint Antivirus9

ESET Endpoint Antivirus 9 代表了真正集成计算机安全的新方法。 最新版本的 ESET LiveGrid® 扫描引擎提高了速度和精确性，以保护您的计算机安全。 其结果是时刻监控会破坏您的计算机的攻击和恶意软件的智能系统。

ESET Endpoint Antivirus 9 是通过我们长期努力而诞生的一个完整安全解决方案，可提供最高防护，同时系统占用最少。基于人工智能的高级技术可主动消除病毒、间谍软件、木马、蠕虫、广告软件、Rootkit 和其他基于 Internet 攻击的渗透，而不会妨碍系统性能或中断您计算机的运行。

ESET Endpoint Antivirus 9 主要设计用于小型商业环境中的工作站。

在单独使用 ESET Endpoint Antivirus 一节中，可以找到分为多个章节和子章节以提供方向和上下文（包括下载、安装和激活）的帮助主题。

在企业环境中将 ESET Endpoint Antivirus 与 ESET PROTECT 结合使用，使您可以轻松地管理任意数量的客户端工作站、应用策略与规则、监控检测以及从任何联网计算机远程配置客户端。

常见问题章节中介绍了一些最常见的问题和难题。

功能和优点

重新设计的用户界面	此版本中的用户界面已基于可用性测试结果进行了大量重新设计和简化。 已仔细检查所有 GUI 用词和通知，并且该界面现在支持从右到左的语言，例如希伯来语和阿拉伯语。 在线帮助现在集成到 ESET Endpoint Antivirus 中，并提供动态更新支持内容。
病毒和间谍软件防护	主动检测和清除更多已知和未知病毒、蠕虫、木马和 Rootkit。即使是前所未见的恶意软件，高级启发式扫描也可对其进行标志，从而防止未知威胁并在恶意软件产生危害之前使其失效。Web 访问保护和网络钓鱼防护的功能是监视 Web 浏览器和远程服务器之间的通信（包括 SSL）。电子邮件客户端防护可控制通过 POP3(S) 和 IMAP(S) 协议接收的电子邮件通信。
定期更新	定期更新检测引擎（之前称为“病毒库”）和程序模块是确保计算机保持最高安全级别的最佳方法。
ESET LiveGrid®（云端信誉）	用户可以直接从 ESET Endpoint Antivirus 检查运行进程和文件的信誉。
远程管理	ESET PROTECT 使您可以在网络环境中从一个中心位置管理工作站、服务器和移动设备上的 ESET 产品。通过使用 ESET PROTECT Web 控制台（ESET PROTECT Web 控制台），您可以部署 ESET 解决方案、管理任务、强制执行安全策略、监控系统状态，以及快速应对远程计算机上出现的问题或威胁。
网络攻击防护	分析网络通信的内容并防止发生网络攻击。将阻止任何视为有害的通信。

Web 控制（仅限 ESET Endpoint Security）	Web 使您可以阻止可能包含潜在冒犯材料的网页。此外，雇主或系统管理员可以禁止访问 27 个以上的预先定义的网站类别和超过 140 个子类别。

此版本中的新功能?

ESET Endpoint Antivirus 9 已发布，可供下载

自动更新

- 确保您始终使用最新的产品版本
- 一种智能解决方案，可将对 ESET Endpoint Antivirus 的维护降低到最低程度
- 默认情况下启用，并使用“微程序组件更新”
- 它不会重新安装产品，并带有所有缺点，如在整个过程（包括配置传输）中从系统中注销
- 它下载的数据较少（差异更新）
- 它附带用户友好或完全可抑制的提醒，并与托管网络兼容

关联最终用户许可协议 (EULA) 修正

- 将在控制台或 ESET Endpoint Antivirus 用户界面中使用信息元素单独显示新的最终用户许可协议，与安装过程无关
- 简化了产品自动更新过程，并改进了您的用户体验，在每次 ESET 产品更新到较新版本时，您不再需要接受最终用户许可协议

本机 ARM64 内部版本

- 版本 9 提供 ARM64 内部版本

此版本包含各种错误修复和性能改进。

有关 ESET Endpoint Antivirus 中新功能的其他信息和屏幕截图，请阅读以下 ESET 知识库文章：

- ESET Endpoint Antivirus 9 中的新功能？

系统需求

若要使 ESET Endpoint Antivirus 无缝工作，系统应满足以下硬件和软件要求（默认产品设置）：

支持的处理器

Intel 或 AMD 处理器，32 位（x86）带有 SSE2 指令集）或 64 位 (x64)，1 GHz 或更高
基于 ARM64 的处理器，1GHz 或更高

操作系统

Microsoft® Windows® 11
Microsoft® Windows® 10
Microsoft® Windows® 8.1
Microsoft® Windows® 8
Microsoft® Windows® 7 SP1（带有最新 Windows 更新（至少带有 KB4474419 和 KB4490628）

Windows XP 和 Windows Vista 不再受支持。

请始终尝试保持操作系统为最新版本。

其他

- 满足安装在计算机上的操作系统和其他软件的系统要求
- 0.3 GB 的可用系统内存（请参阅注释 1）
- 1 GB 的可用磁盘空间（请参阅注释 2）
- 最小显示器分辨率 1024x768
- 产品更新的 Internet 连接或到源的局域网连接（请参阅注释 3）
- 在单个设备上同时运行的两个病毒防护程序不可避免地会导致系统资源冲突，例如减慢系统运行速度使其不可操作

尽管可以在不满足这些要求的系统上安装和运行产品，但我们建议先基于性能要求完成可用性测试。

(1) 如果内存未在严重被感染的计算机上使用，或者当要将巨大的数据列表（例如 URL 白名单）导入产品中时，该产品可能使用更多内存。
(2) 下载安装程序、安装产品和在程序数据中保留安装程序包副本以及用于支持回滚功能的产品更新备份所需的磁盘空间。该产品在不同的设置下（例如当存储更多产品更新备份版本、保留内存转储或大量日志记录时）或被感染的计算机上（例如由于隔离功能）可能使用更多磁盘空间。我们建议保留足够的可用磁盘空间以支持操作系统更新并用于 ESET 产品更新。
(3) 尽管不建议这样做，但可从可移动磁盘手动更新该产品。

受支持语言

可以使用以下语言安装和下载 ESET Endpoint Antivirus。

语言	语言代码	LCID
英语(美国)	en-US	1033
阿拉伯语(埃及)	ar-EG	3073
保加利亚语	bg-BG	1026
简体中文	zh-CN	2052
繁体中文	zh-TW	1028
克罗地亚语	hr-HR	1050
捷克语	cs-CZ	1029
爱沙尼亚语	et-EE	1061
芬兰语	fi-FI	1035
法语(法国)	fr-FR	1036
法语(加拿大)	fr-CA	3084
德语(德国)	de-DE	1031
希腊语	el-GR	1032
*希伯来语	he-IL	1037
匈牙利语	hu-HU	1038
*印尼语	id-ID	1057
意大利语	it-IT	1040
日语	ja-JP	1041
哈萨克语	kk-KZ	1087
朝鲜语	ko-KR	1042
*拉脱维亚语	lv-LV	1062
立陶宛语	lt-LT	1063
Nederlands	nl-NL	1043
挪威语	nn-NO	1044
波兰语	pl-PL	1045
葡萄牙语(巴西)	pt-BR	1046
罗马尼亚语	ro-RO	1048
俄语	ru-RU	1049
西班牙语(智利)	es-CL	13322
西班牙语(西班牙)	es-ES	3082
瑞典语(瑞典)	sv-SE	1053
斯洛伐克语	sk-SK	1051
斯洛维尼亚语	sl-SI	1060
泰语	th-TH	1054
土耳其语	tr-TR	1055
乌克兰语(乌克兰)	uk-UA	1058
*越南语	vi-VN	1066

* ESET Endpoint Antivirus 以此语言提供，但联机用户指南不以此语言提供（重定向到英语版

本）。

要更改此联机用户指南的语言，请参阅语言选择框（右上角）.

预防

使用计算机（尤其是浏览 Internet时，请记住，世界上没有任何病毒防护系统可以完全消除检测和远程攻击的风险。要提供最大防护和便利，正确使用病毒防护解决方案和遵守一些有用规则非常重要：

定期更新

根据 ESET LiveGrid® 的统计数据，全球每天都会产生数以千计的新的独特渗透，它们绕过现有安全措施，以损害其他用户利益为代价给渗透者带来收益ESET 病毒实验室的专家每天分析这些威胁，准备并发布更新，以不断提高用户的保护级别。要确保这些更新的最大有效性，在系统上适当配置这些更新就显得非常重要。有关如何配置更新的更多信息，请参见更新设置章节。

下载安全补丁

恶意软件的作者通常利用各种系统漏洞，以提高恶意代码的传播效果。出于这种考虑，软件公司密切关注其应用程序中出现的任何漏洞，并且定期发布可消除潜在威胁的安全更新的原因。安全更新发布后需立即下载，这非常重要Microsoft Windows 和 Web 浏览器（例如Internet Explorer程序是安全更新定期发布的两个程序示例。

备份重要数据

恶意软件作者通常不关心用户需求，恶意程序的活动常常导致操作系统故障和重要数据丢失。定期将重要和敏感数据备份到外部存储器（例如 DVD 或外部硬盘驱动器）就显得非常重要。这将使得发生系统故障时恢复数据更加简单快速。

定期扫描计算机、查找病毒

实时文件系统防护模块可处理更多已知和未知的病毒、蠕虫、木马和 Rootkit这意味着每次您访问或打开文件时，将对其进行扫描以查找恶意软件活动。我们建议您每月至少运行一次计算机全面扫描，这是因为恶意软件病毒库不断变化并且检测引擎每天会自行更新。

遵循基本安全规则

这是所有规则中最有用和最有效的一条 – 始终保持谨慎。现在许多渗透需要用户干预才能执行和传播。如果您打开新文件时比较谨慎，可为自己节省清除渗透所需的大量时间和精力。下面是一些实用指南：

- 不访问带有多个弹出窗口和闪烁广告的可疑网站。
- 谨慎安装免费软件、代码包等。只使用安全的程序，只访问安全的 Internet 网站。
- 谨慎打开电子邮件附件，尤其是批量发送的邮件和来自陌生发件人的邮件。

- 不要使用管理员帐户执行计算机的日常工作。

帮助页面

欢迎使用 ESET Endpoint Antivirus 帮助文件。此处提供的信息将使您熟悉本产品，并帮助您使计算机更安全。

入门

在开始使用 ESET Endpoint Antivirus 前，请注意我们的产品可由通过 ESET PROTECT 连接的用户或其自身使用。我们还建议您熟悉使用计算机时可能遇到的各种检测类型和远程攻击。

请参阅新功能以了解此版本的 ESET Endpoint Antivirus 中引入的功能。我们还准备了一份指南，帮助您设置和自定义 ESET Endpoint Antivirus 的基本设置。

如何使用 ESET Endpoint Antivirus 帮助页面

为了提供方向指导和上下文，帮助主题分为多个章节和子章节。您可以通过浏览帮助页面的目录结构找到相关信息。

若要了解有关程序中任意窗口的详细信息，请按 **F1**。将显示与当前查看的窗口相关的帮助页面。

您可以通过关键字或者键入字词或短语来搜索帮助页面。这两种方法的区别在于，关键字可能与文本中不包含该特定关键字的帮助页面在逻辑上相关。按字词和短语搜索将搜索所有页面的内容，并仅显示包含所搜索字词或短语的页面。

为了保持一致和帮助避免混淆，本指南中使用的术语均基于 ESET Endpoint Antivirus 参数名称。我们还使用了一组统一的符号来强调特别有用或非常重要的主题。

注释只是一个简短的意见。 尽管您可以忽略它，但注释可以提供有价值的信息，例如特定功能或指向某些相关主题的链接。

此信息需要您的注意，我们鼓励您不要跳过此内容。 它通常提供非关键的重要信息。

这是需要额外关注和谨慎使用的信息。 警告专门用于防止您犯潜在有害的错误。 请阅读并了解警告中包含的文本，因为它引用了高度敏感的系统设置或某些高风险的内容。

这是一个用例或实用示例，旨在帮助您了解如何使用某个功能或特性。

约定	含义
粗体类型	界面项目的名称，例如框和选项按钮。
斜体类型	您提供的信息的占位符。例如，文件名或路径表示您键入实际路径或文件名。
`Courier New`	代码示例或命令。
超链接	支持快速轻松地访问交叉引用的主题或外部Web位置。超链接以蓝色突出显示，可能带有下划线。
%ProgramFiles%	存储安装在 Windows 上的程序的 Windows 系统目录。

联机帮助是帮助内容的主要来源。 当您有正常的 Internet 连接时，将自动显示联机帮助的最新

版本。

远程管理端点的文档

可以从一个中心位置远程管理网络环境中客户端工作站、服务器和移动设备上的 ESET 业务产品以及 ESET Endpoint Antivirus。管理 10 个以上客户端工作站的系统管理员可以考虑部署一个 ESET 远程管理工具，以便从一个中心位置部署 ESET 解决方案、管理任务、强制执行安全策略、监控系统状态以及快速响应远程计算机上出现的问题或威胁。

ESET 远程管理工具

ESET Endpoint Antivirus可以通过 ESET PROTECT 或 ESET Cloud Administrator 远程管理 。

- ESET PROTECT 介绍
- ESET PROTECT Cloud 介绍

第三方远程管理工具

- 远程监控和管理 RMM

最佳做法

- 将安装有 ESET Endpoint Antivirus 的所有端点连接到 ESET PROTECT
- 保护已连接客户端计算机上的“高级设置”设置，以阻止未经授权的修改
- 应用建议策略，以强制执行可用的安全功能
- 最小化用户界面 – 减少或限制与 ESET Endpoint Antivirus 进行用户交互

操作指南

- 如何使用覆盖模式
- 如何使用 GPO 或 SCCM 部署 ESET Endpoint Antivirus

ESET PROTECT 介绍

ESET PROTECT 让您可以从一个中心位置管理网络环境中工作站、服务器和移动设备上的 ESET 产品。

通过使用 ESET PROTECT Web 控制台，可以部署 ESET 解决方案、管理任务、强制执行安全策略、监控系统状态以及快速响应远程计算机上出现的问题或检测。另请参阅 ESET PROTECT 架构和基础结构元素概述、ESET PROTECT Web 控制台快速入门和支持的桌面设置环境。

ESET PROTECT 由以下组件组成：

- ESET PROTECT 服务器 - ESET PROTECT 服务器既可以安装在 Windows 服务器上，也可以安装在 Linux 服务器上，还可以以虚拟设备的形式出现。它可处理与服务器代理的通信，还可以收集应用程序数据以及将这些数据存储在数据库中。

- ESET PROTECT Web 控制台 - ESET PROTECT Web 控制台是让您可以管理环境中客户端计算机的主界面。它将显示您网络中客户端状态的概述，并让您可以将 ESET 解决方案远程部署到不受托管的计算机。在安装 ESET PROTECT 服务器后，可以使用 Web 浏览器访问 Web 控制台。如果选择使 Web 服务器可通过 Internet 进行访问，可以通过 Internet 连接从任何地点或设备使用 ESET PROTECT。

- ESET Management 服务器代理 - ESET Management 服务器代理有助于增强 ESET PROTECT 服务器和客户端计算机之间的通信。必须在客户端计算机上安装服务器代理，才能在该计算机和 ESET PROTECT 服务器之间建立通信。因为它位于客户端计算机上，并且可以存储多个安全方案，因此使用 ESET Management 服务器代理可显著缩短对新检测的反应时间。通过使用 ESET PROTECT Web 控制台，可以将 ESET Management 服务器代理部署到由 Active Directory 或 ESET RD Sensor 识别的不受托管的计算机上。还可以根据需要在客户端计算机上手动安装 ESET Management 服务器代理。

- Rogue Detection Sensor - ESET PROTECT Rogue Detection (RD) Sensor 可检测您网络上是否存在未托管的计算机，并将其信息发送到 ESET PROTECT 服务器。这使您能够轻松地将新客户端计算机添加到您的安全网络中。RD Sensor 会记住已发现的计算机，并且不会再次发送相同的信息。

- Apache HTTP 代理 – 是可与 ESET PROTECT 结合使用的服务，用于：

  o将更新分发到客户端计算机以及将安装程序包分发到 ESET Management 服务器代理。

  o将通信从 ESET Management 服务器代理转发到 ESET PROTECT 服务器。

- 移动设备连接器 – 是一个可用于 ESET PROTECT 的移动设备管理的组件，允许您管理移动设备。Android 和 iOS 以及管理适用于 Android 的 ESET Endpoint Security。

- ESET PROTECT 虚拟设备 - ESET PROTECT VA 适用于想要在虚拟环境中运行 ESET PROTECT 的用户。

- ESET PROTECT 虚拟服务器代理主机 - ESET PROTECT 的组件，可虚拟化服务器代理实体，以允许管理无服务器代理的虚拟机。该解决方案支持自动化、动态组使用和与物理计算机上的 ESET Management 服务器代理相同级别的任务管理。虚拟服务器代理可收集虚拟机的信息，并将它发送到 ESET PROTECT 服务器。

- 镜像工具 – 镜像工具对脱机模块更新而言不可或缺。如果客户端计算机没有 Internet 连接，即可使用镜像工具从 ESET 更新服务器下载更新文件，然后将其存储在本地。

- ESET Remote Deployment Tool – 此工具可用于部署在 <%PRODUCT%> Web 控制台中创建的一体式程序包。它是通过网络在计算机上分发 ESET Management 服务器代理与 ESET 产品的一种便捷方式。

- ESET Business Account - ESET 商业版产品的新许可门户，允许用户管理许可证。有关激活产品的说明，请参阅本文档的 ESET Business Account 部分；有关使用 ESET Business Account 的详细信息，请参阅 ESET Business Account 用户指南。如果用户已经有一个 ESET 发布的用户名和密码，并希望将其转换为许可证密钥，请参阅转换旧许可证凭据部分。

- ESET Inspect – 一个全面的端点检测和响应系统，包括的功能如：事件检测、事件管理和响应、数据收集、攻击检测指示、异常检测、行为检测、策略违反。

使用 ESET PROTECT Web 控制台，可以部署 ESET 解决方案、管理任务、强制执行安全策略、监控系统状态以及快速响应远程计算机上出现的问题或威胁。

有关详细信息，请参阅 ESET PROTECT 联机用户指南。

ESET PROTECT Cloud 介绍

ESET PROTECT Cloud 让您可以在网络环境中从一个中心位置管理工作站和服务器上的 ESET 产品，而无需 ESET PROTECT 之类的物理或虚拟服务器。通过使用 ESET PROTECT Cloud Web 控制台，可以部署 ESET 解决方案、管理任务、强制执行安全策略、监控系统状态，以及快速响应远程计算机上出现的问题或威胁。

- 在 ESET PROTECT Cloud 联机用户指南中阅读有关此内容的更多信息

受密码保护的设置

若要最大限度地保护系统安全，需要正确配置 ESET Endpoint Antivirus。任何未经授权的更改或设置都可能导致客户端安全和保护级别降低。若要限制用户访问“高级设置”，管理员可以使用密码保护设置。

管理员可以创建策略以密码保护连接的客户端计算机上 ESET Endpoint Antivirus 的“高级设置”设置。要创建新策略，请执行以下操作：

1. 在 ESET PROTECT Web 控制台或 ，在左侧主菜单中单击**策略**。

2. 单击**新建策略**。

3. 为新策略命名，并（可选）为它提供简短的说明。单击**继续**按钮。

4. 从产品列表中，选择 **ESET Endpoint for Windows**。

5. 在**设置**列表中单击**用户界面**，然后展开**访问设置**。

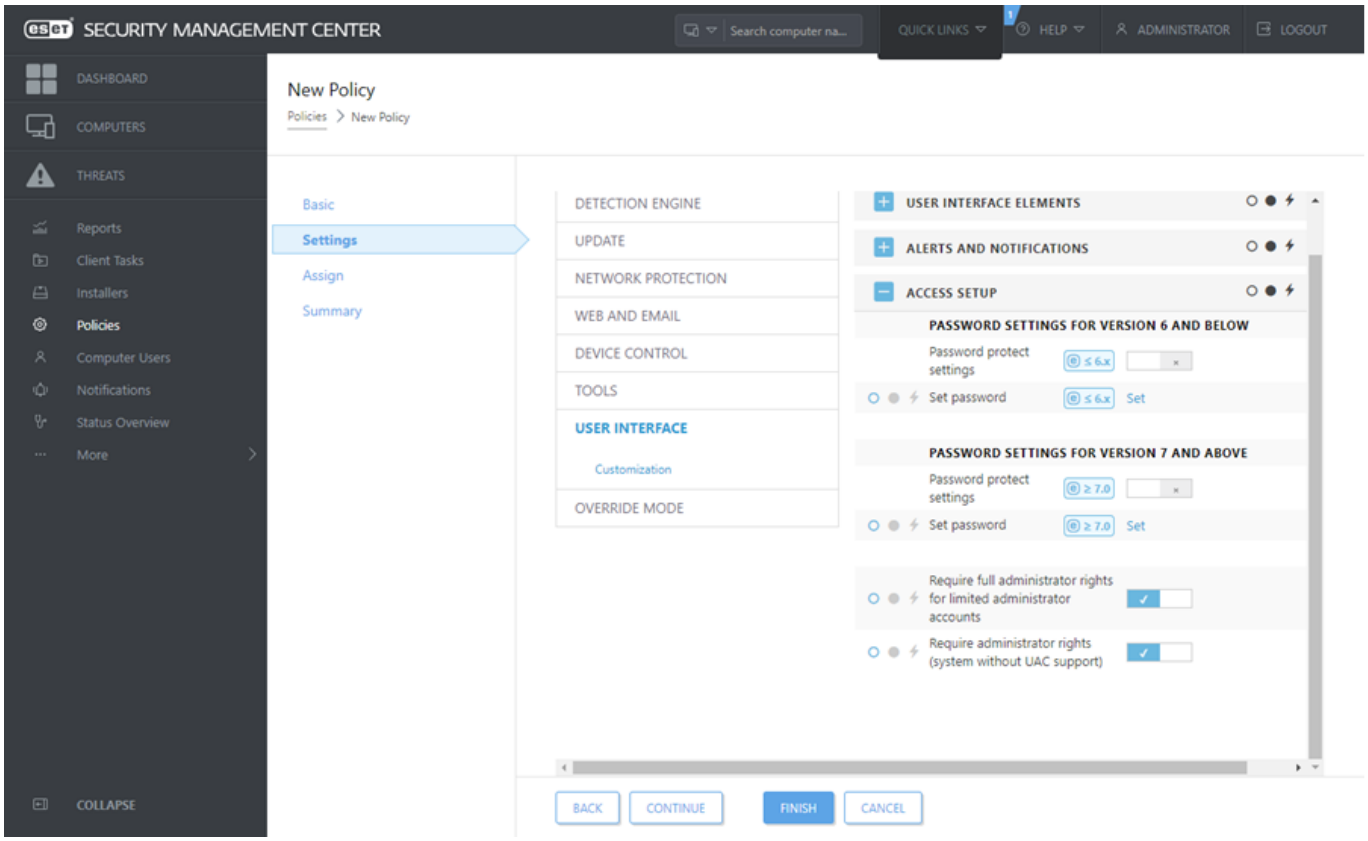
6. 根据 ESET Endpoint Antivirus 的版本，单击滑块以启用**以密码保护设置**。请注意，ESET Endpoint 产品版本 7 提供增强的防护。如果网络中同时具有版本 7 和版本 6 的 Endpoint 产品，建议您为每个版本使用不同密码创建两个单独的策略。

7. 在弹出窗口中，创建新密码，进行确认，然后单击**确定**。单击**继续**。

8. 将策略分配到客户端。单击**分配**，然后选择要以密码保护的计算机或计算机组。单击**确定**以确认。

9. 检查所有需要的客户端计算机是否都在目标列表中，然后单击**继续**。

10. 在汇总中检查这些策略设置，然后单击**完成**以保存新策略。



什么是策略

管理员可以使用 ESET PROTECT Web 控制台中的策略向在客户端计算机上运行的 ESET 产品推送特定配置。策略可以直接应用于个别计算机以及计算机组。还可以将多个策略分配到计算机或计算机组。

用户必须具有以下权限，才能创建新策略：用于读取策略列表的**读取**权限、用于将策略分配到目标计算机的**使用**权限，以及用于创建、修改或编辑策略的**写入**权限。

将采用静态组排列的顺序来应用策略。但对于动态组来说，情况却并非如此，其中策略首先应用到子动态组。这使您可以将具有较大影响的策略应用到组树的顶部，并将更多特定策略应用到子组。通过使用标志，则具有对树中较高层级组的访问权限的 ESET Endpoint Antivirus 用户可以覆盖较低层级组的策略。在 ESET PROTECT 联机帮助中详细介绍了该算法。

建议您将更多一般策略（例如，更新服务器策略）分配到组树中较高层级的组。更多特定策略（例如，设备控制设置）应分配到组树中的较深层级。策略合并时，较低层级的策略通常会覆盖较高层级的策略的设置（除非使用策略标志另行定义）。

合并策略

应用到客户端的策略通常是多个策略合并到一个最终策略的结果。在合并策略时，一般规则是后面的策略始终替换由前面策略设定的设置。若要更改此行为，可以使用策略标志（可用于每个设置）。

在创建策略时，您会注意到某些设置具有可配置的其他规则（替换/附加/前置）。

- **替换** – 替换整个列表，添加新值并删除所有以前的值。
- **附加** – 项目将添加到当前应用列表的底部（必须是其他策略，本地列表始终被覆盖）。
- **前置** – 项目将添加到列表的顶部（本地列表被覆盖）。

ESET Endpoint Antivirus 支持以新方式合并本地设置和远程策略。如果设置为列表（例如，网站列表）并且远程策略与现有本地设置冲突，则远程策略会覆盖它。您可以通过选择不同的合并规则，来选择如何组合本地和远程列表：

- 合并远程策略的设置。
- 合并远程和本地策略 – 具有生成的远程策略的本地设置。

若要详细了解合并策略，请按照 ESET PROTECT 联机用户指南操作，并查看示例

标志的工作原理

应用到客户端计算机的策略通常是将多个策略合并到一个最终策略的结果。合并策略时，可以使用策略标志调整最终策略的预期行为（由于应用策略的顺序）。标志定义策略将如何处理特定设置。

对于每个设置，您可以选择以下标志之一：

不应用	策略不会设置具有此标志的任何设置。由于设置未由策略进行设定，因此可以由以后应用的其他策略更改。
应用(A)	具有**应用**标志的设置将应用于客户端计算机。但当合并策略时，它可以由以后应用的其他策略覆盖。将策略发送到包含标有此标志的设置的客户端计算机时，这些设置将更改客户端计算机的本地配置。由于此设置未强制执行，因此它仍可以由以后应用的其他策略更改。
强制	具有**强制执行**标志的设置具有优先级，无法由以后应用的任何策略覆盖（即使它还具有**强制执行**标志）。这可确保以后应用的其他策略不会在合并时更改此设置。将策略发送到包含标有此标志的设置的客户端计算机时，这些设置将更改客户端计算机的本地配置。

方案：*管理员*希望允许用户 *John* 在其家庭组中创建或编辑策略，并查看由*管理员*创建的所有策略，包括带有 强制执行标志的策略。*管理员*希望 *John* 可以查看所有策略，但无法编辑由*管理员*创建的现有策略。*John* 只可以在其家庭组 San Diego 中创建或编辑策略。
解决方案：*管理员*需遵循以下步骤：
创建自定义静态组和权限集
1. 创建一个名为 *San Diego* 的新静态组。
2. 创建名为 *Policy - All John*（包含静态组*全部*的访问权限和**策略**的**读取**权限）的新权限集。
3. 创建名为 *Policy John*（包含静态组 *San Diego* 的访问权限以及**组和计算机**和**策略**的功能访问**写入**权限）的新权限集。此权限集允许 *John* 在他的家庭组 *San Diego* 中创建或编辑策略。
4. 创建新用户 *John*，然后在**权限集**部分中选择 *Policy - All John* 和 *Policy John*。
创建策略
5. 创建新策略 *All- Enable Firewall*，展开**设置**部分，选择 **ESET Endpoint for Windows**，依次导航到**个人防火墙 > 基本**，然后通过 **强制执行**标志应用所有设置。展开**分配**部分，然后选择“静态组”*全部*。
6. 创建新策略 *John Group- Enable Firewall*，展开**设置**部分，选择 **ESET Endpoint for Windows**，依次导航到**个人防火墙 > 基本**，然后通过 **应用**标志应用所有设置。展开**分配**部分，然后选择“静态组”*San Diego*。
结果
由于 **强制执行**标志已应用于策略设置，则将首先应用由*管理员*创建的策略。已应用强制执行标志的设置具有优先级，无法由以后应用的其他策略覆盖。用户 *John* 创建的策略将在管理员创建的策略之后应用。
若要查看最终策略顺序，请依次导航到**更多 > 组 > San Diego**。选择计算机，然后选择**显示详细信息**。在**配置**部分中，单击**已应用的策略**。

单独使用 ESET Endpoint Antivirus

本用户指南的这一部分和使用 ESET Endpoint Antivirus 部分旨在面向在没有 ESET PROTECT 或 ESET PROTECT Cloud 的情况下使用 ESET Endpoint Antivirus 的用户。ESET Endpoint Antivirus 的所有特性和功能均可完全访问，具体取决于用户的帐户权限。

安装方法

在客户端工作站上安装 ESET Endpoint Antivirus 版本 9.x 的方法有多种，除非通过 ESET PROTECT 或 ESET PROTECT Cloud 将 ESET Endpoint Antivirus 远程部署到客户端工作站。

- 安装或升级 ESET Endpoint Antivirus 到版本 6.6.x

方法	用途	下载链接
通过 ESET AV Remover 安装	在继续安装之前，ESET AV Remover 工具可帮助您删除之前安装在您系统上的几乎所有病毒防护软件。	下载 64 位 下载 32 位
***安装 (.exe)	不使用 ESET AV Remover 进行安装。	N/A

方法	用途	下载链接
安装 (.msi)	在商业环境中，.msi 安装程序是首选安装包。这主要是由于使用 ESET PROTECT 等各种工具的脱机和远程部署。	下载 64 位 下载 32 位
命令行安装	ESET Endpoint Antivirus 可以使用命令行进行本地安装，也可以使用 ESET PROTECT 中的客户端任务进行远程安装。	N/A
使用 GPO 或 SCCM 进行部署	使用 GPO 或 SCCM 等管理工具将 ESET Management Agent 和 ESET Endpoint Antivirus 部署到客户端工作站。	N/A
使用 RMM 工具部署	适用于远程管理和监控 (RMM) 工具的 ESET DEM 插件让您可以将 ESET Endpoint Antivirus 部署到客户端工作站。	N/A

ESET Endpoint Antivirus 以 30 多种语言提供。

通过 ESET AV Remover 安装

在继续执行安装过程之前，卸载计算机上的所有现有安全应用程序非常重要。选中**我想要使用 ESET AV Remover 卸载不受欢迎的病毒防护应用程序**旁边的复选框，以使 ESET AV Remover 扫描系统并删除任何受支持的安全应用程序。使该复选框保持取消选中状态，然后单击**继续**以在不运行 ESET AV Remover 的情况下安装 ESET Endpoint Antivirus。

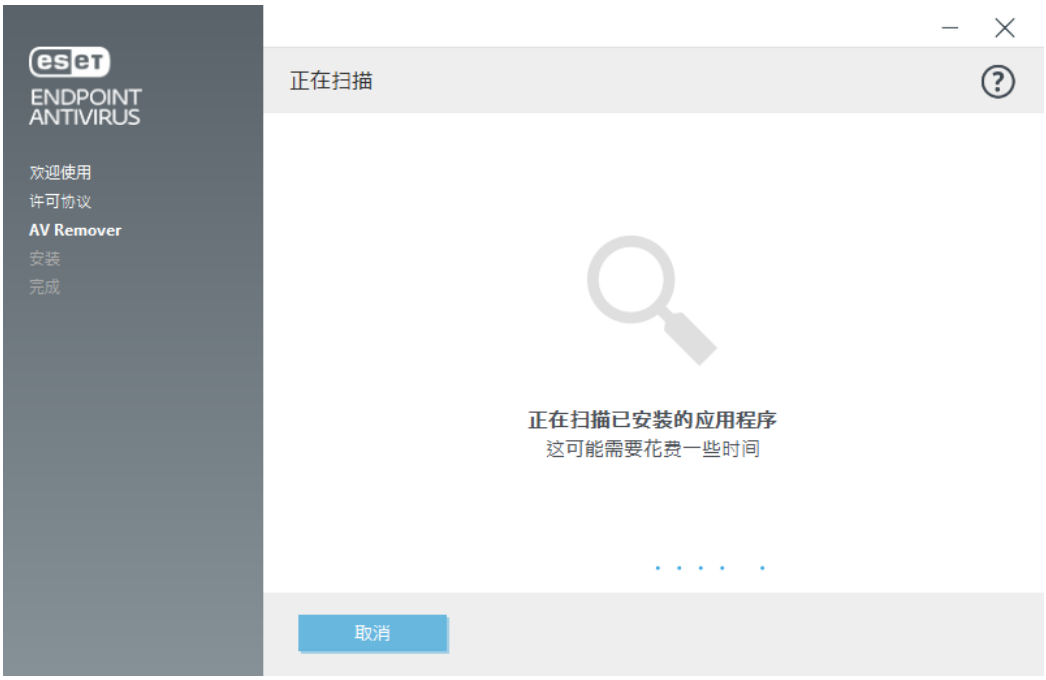
ESET AV Remover

ESET AV Remover 工具可帮助您删除之前安装在您的系统上的几乎所有病毒防护软件。按照下面的说明使用 ESET AV Remover 删除现有病毒防护程序：

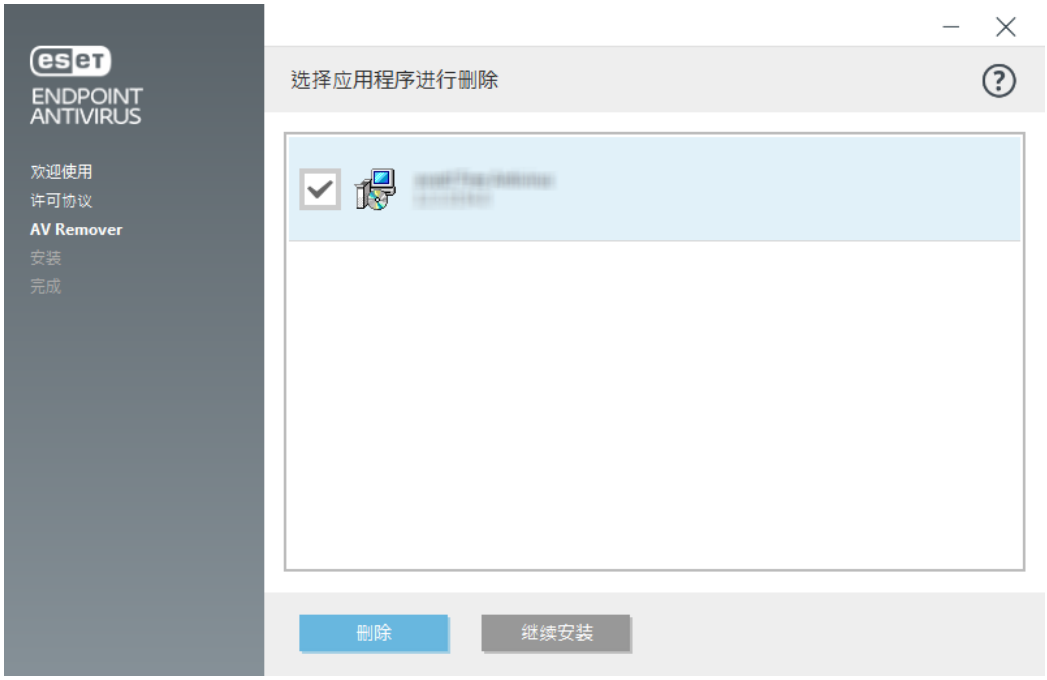
1. 若要查看 ESET AV Remover 可以删除的病毒防护软件的列表，请访问 ESET 知识库文章。

2. 阅读最终用户许可协议并单击**接受**，以确认接受。单击**拒绝**将在不删除计算机上的现有安全应用程序的情况下继续安装 ESET Endpoint Antivirus。

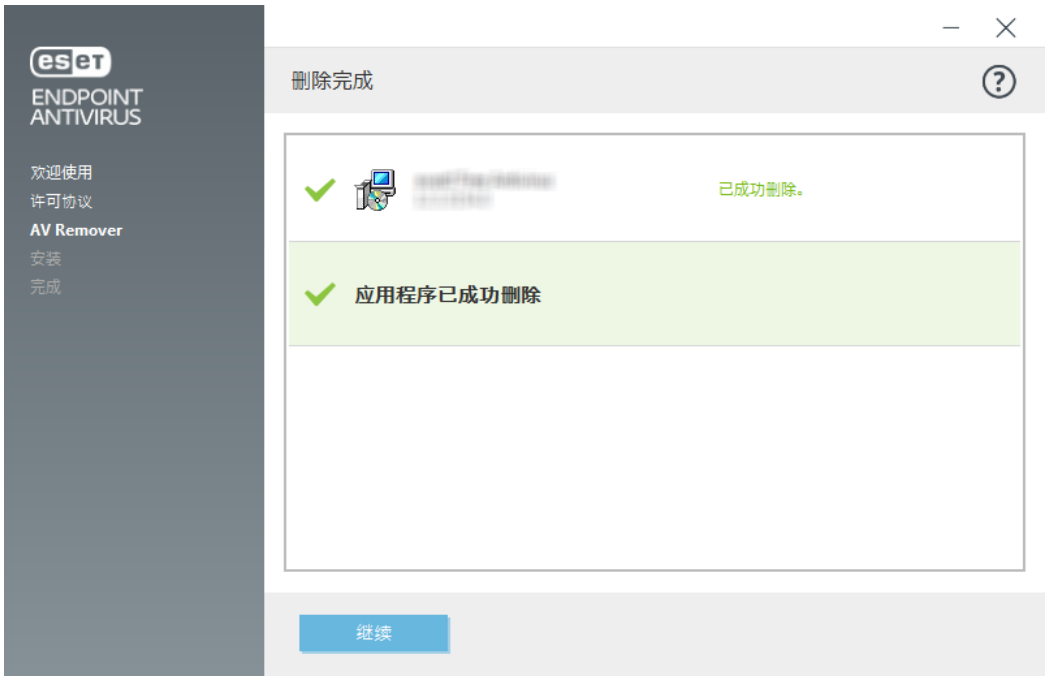
3. ESET AV Remover 将开始在系统中搜索病毒防护软件。



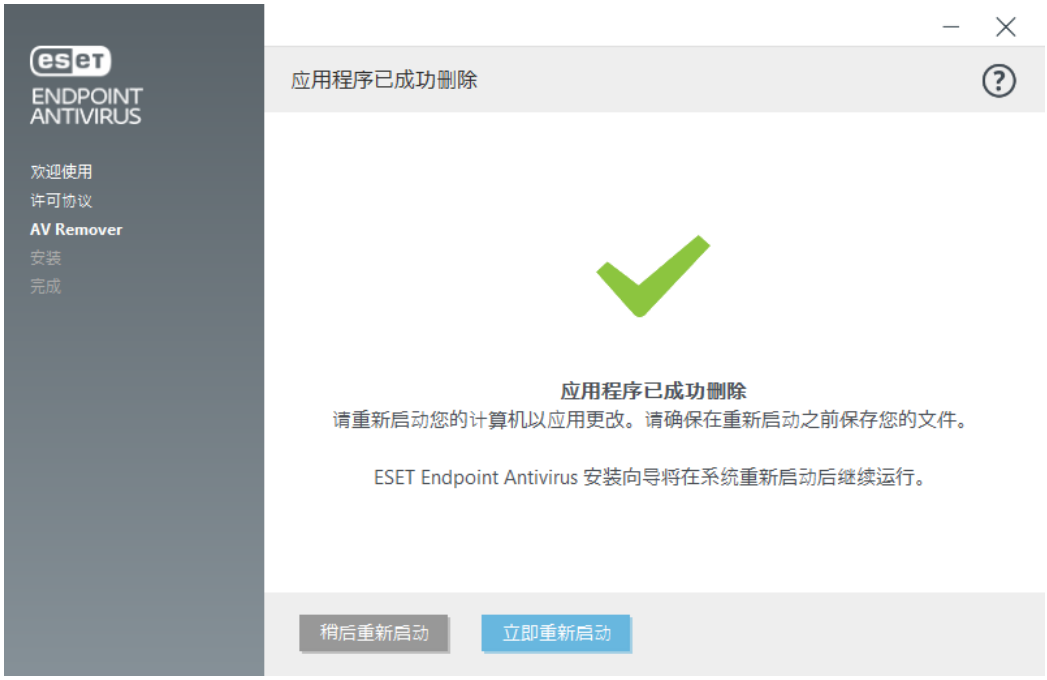
4. 选择任何列出的病毒防护应用程序并单击**删除**。删除可能需要花费一点时间。



5. 成功删除后，请单击**继续**。



6. 重新启动计算机以应用更改并继续安装 ESET Endpoint Antivirus。如果卸载不成功，请参阅本指南的通过 ESET AV Remover 卸载因出现错误而终止部分。



使用 ESET AV Remover 卸载因出现错误而终止

如果无法使用 ESET AV Remover 删除病毒防护程序，您将收到一个通知，指示您正在尝试删除的应用程序可能不受 ESET AV Remover 支持。请访问 ESET 知识库上的受支持的产品列表或常见 Windows 病毒防护软件的卸载程序以查看是否可以删除此特定程序。

当安全产品的卸载不成功或仅部分卸载了它的一些组件时，系统将提示您**重新启动并重新扫描**。在重新启动后确认 UAC□并继续扫描和卸载过程。

如果需要，请联系 ESET 技术支持以打开支持请求，并提供 **AppRemover.log** 文件以帮助 ESET 技术人员。**AppRemover.log** 文件位于 **eset** 文件夹中。在 Windows 资源管理器中浏览到 *%TEMP%* 以访问此文件夹□ESET 技术支持将尽快响应以帮助解决您的问题。

安装 (.exe)

启动 .exe 安装程序后，安装向导将引导您完成安装过程。

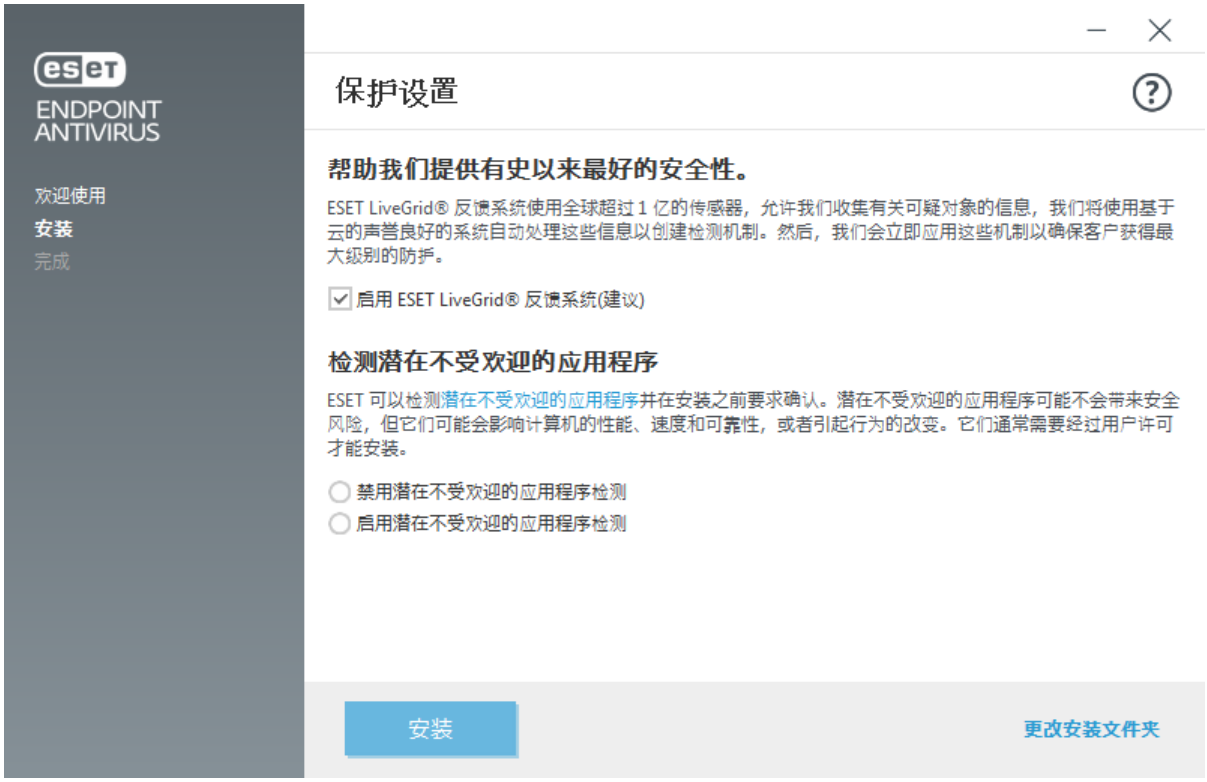
请确保您的计算机上未安装任何其他病毒防护程序。如果在一台计算机上安装两个或更多病毒防护解决方案，可能彼此冲突。建议您卸载系统上的任何其他病毒防护程序。有关常见病毒防护软件的卸载程序工具的列表，请参阅知识库文章（提供英语及其他几种语言）。

1. 阅读最终用户许可协议，并单击**我接受**以确认接受最终用户许可协议。在接受条款后，单击**下一步**以继续安装。

2. 选择是否启用 ESET LiveGrid® 反馈系统□ESET LiveGrid® 有助于确保将新渗透不断地及时通知给 ESET□这使我们可以更好地保护客户。该系统允许向 ESET 病毒实验室提交新的威胁，这些威胁将在实验室进行分析、处理并添加到检测引擎中。

3. 安装过程中的下一步是配置对潜在不受欢迎的应用程序的检测。有关更多详细信息，请参阅潜在不受欢迎的应用程序章节。

4. 最后一步是通过单击**安装**确认安装。可以通过单击更改安装文件夹，将 ESET Endpoint Antivirus 安装到特定文件夹。安装完成后，系统将提示您激活 ESET Endpoint Antivirus。



更改安装文件夹 (.exe)

在选择检测潜在不受欢迎的应用程序的首选项并单击**更改安装文件夹**后，系统将提示您选择安装 ESET Endpoint Antivirus 文件夹的位置。默认情况下，该程序将安装到以下目录：

C:\Program Files\ESET\ESET Security

您可以指定程序模块和数据的位置。默认情况下，它们将分别安装到以下目录：

C:\Program Files\ESET\ESET Security\Modules
C:\ProgramData\ESET\ESET Security

单击**浏览**以更改这些位置（不建议）。

依次单击**继续**和**安装**，以开始安装。

安装 (.msi)

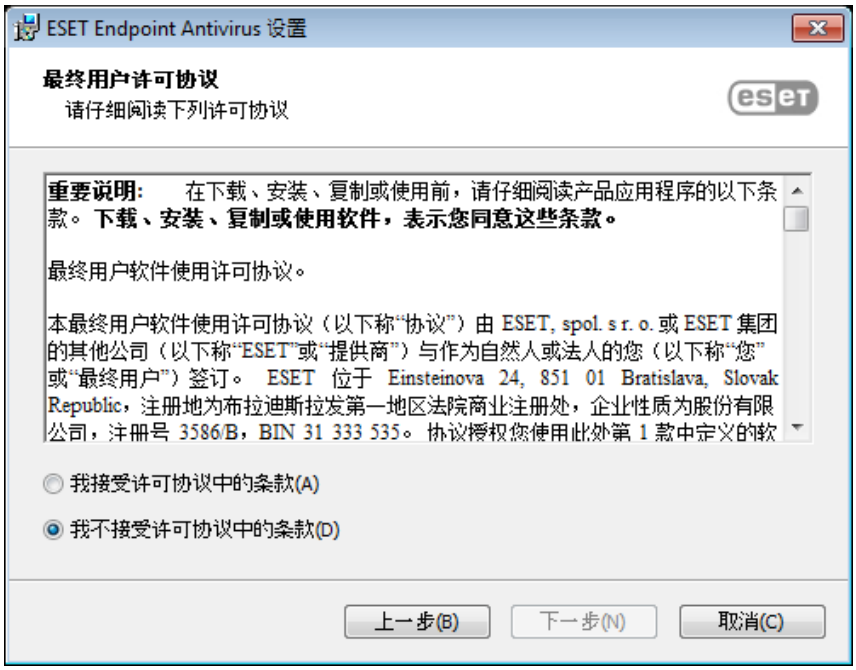
启动 .msi 安装程序后，安装向导将引导您完成安装过程。

在商业环境中，.msi 安装程序是首选安装包。这主要是由于使用 ESET PROTECT 等各种工具的脱机和远程部署。

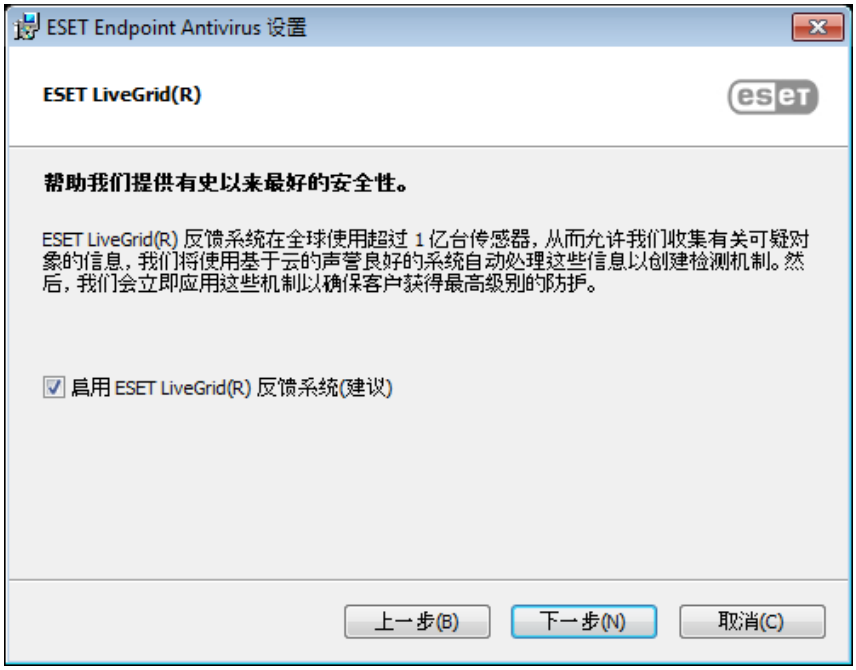
请确保您的计算机上未安装任何其他病毒防护程序。如果在一台计算机上安装两个或更多病毒防护解决方案，可能彼此冲突。建议您卸载系统上的任何其他病毒防护程序。有关常见病毒防护软件的卸载程序工具的列表，请参阅知识库文章（提供英语及其他几种语言）。

1. 选择所需语言，然后单击**下一步**。

2. 阅读最终用户许可协议，并单击**我接受许可协议中的条款**以确认接受最终用户许可协议。在接受条款后，单击**下一步**以继续安装。

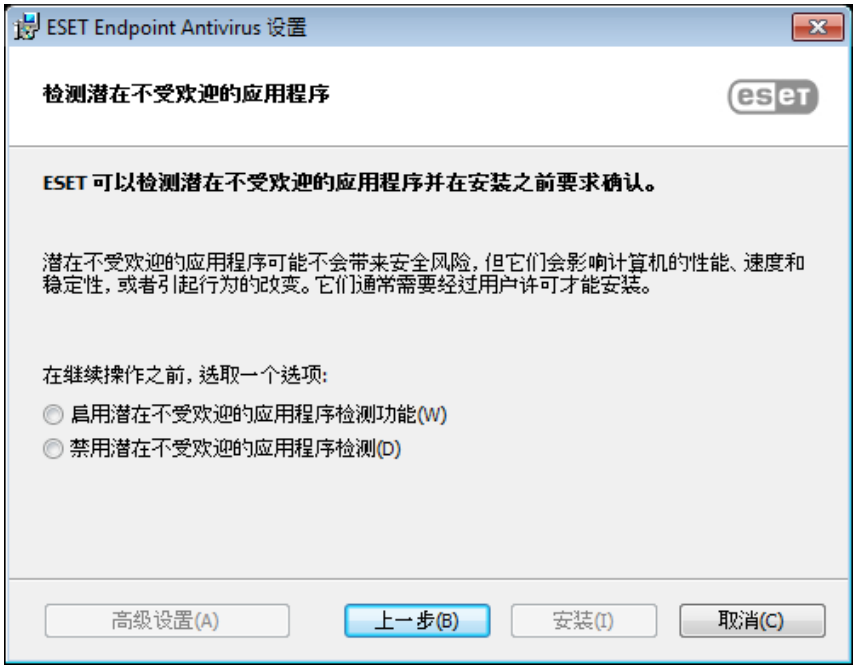


3. 选择 ESET LiveGrid® 反馈系统 的首选项□ESET LiveGrid® 有助于确保将新渗透不断地及时通知给 ESET□这使我们可以更好地保护客户。该系统允许向 ESET 病毒实验室提交新的威胁，这些威胁将在实验室进行分析、处理并添加到检测引擎中。



4. 安装过程中的下一步是配置对潜在不受欢迎的应用程序的检测。有关更多详细信息，请参阅潜在不受欢迎的应用程序章节。

如果要继续进行高级安装 (.msi)，则单击**高级设置**。



5. 最后一步是通过单击**安装**确认安装。安装完成后，系统将提示您激活 ESET Endpoint Antivirus。

高级安装 (.msi)

高级安装允许您自定义在执行典型安装时不可用的大量安装参数。

5. 在选择对潜在不受欢迎的应用程序的检测首选项并单击**高级设置**后，系统将提示您选择安装

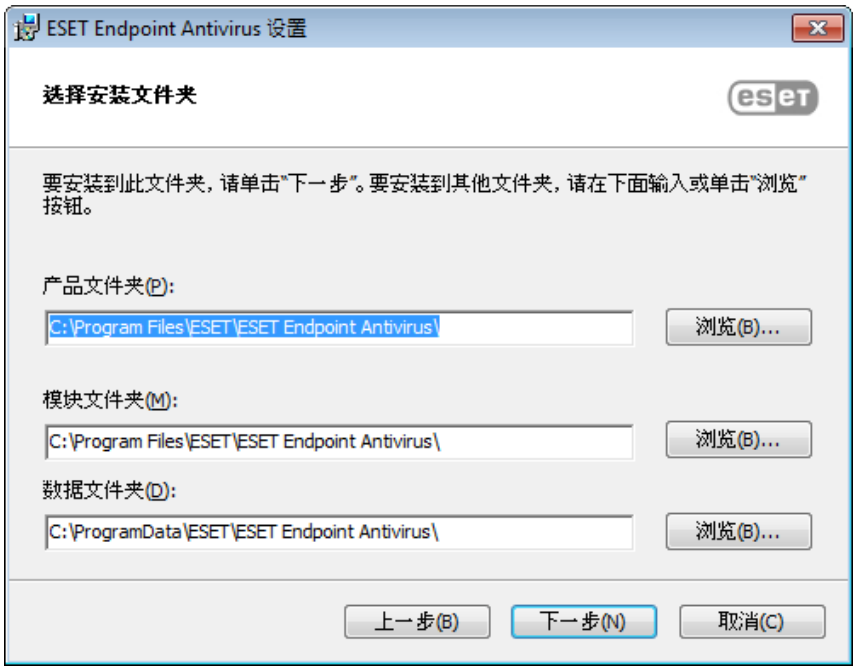
ESET Endpoint Antivirus 文件夹的位置。默认情况下，程序将安装到以下目录：

C:\Program Files\ESET\ESET Security

您可以指定程序模块和数据的位置。默认情况下，它们将分别安装到以下目录：

C:\Program Files\ESET\ESET Security\Modules
C:\ProgramData\ESET\ESET Security

单击**浏览**以更改这些位置（不建议）。



7. 最后一步是通过单击**安装**确认安装。

命令行安装

可以使用命令行本地安装 ESET Endpoint Antivirus，也可以从 ESET PROTECT 使用客户端任务远程安装。

支持的参数

APPDIR=<path>

- 路径 – 有效的目录路径。
- 应用程序安装目录。

APPDATADIR=<path>

- 路径 – 有效的目录路径。
- 应用程序数据安装目录。

MODULEDIR=<path>

- 路径 – 有效的目录路径。
- 模块安装目录。

ADDLOCAL=<list>

- 组件安装 – 要在本地安装的非强制性功能的列表。
- ESET .msi 程序包的用法：`ees_nt64_ENU.msi /qn ADDLOCAL=<list>`
- 有关 **ADDLOCAL** 属性的详细信息，请参阅 http://msdn.microsoft.com/zh-cn/library/aa367536%28v=vs.85%29.aspx

ADDEXCLUDE=<list>

- ADDEXCLUDE 列表是不需要安装的所有功能名称的列表（逗号分隔），替换已废弃的 REMOVE。
- 选择不需要安装的功能时，必须在列表中明确包含完整路径（即，其所有子功能）和相关的不可见功能。
- ESET .msi 程序包的用法：`ees_nt64_enu.msi /qn ADDEXCLUDE=Firewall,Network`

> **ADDEXCLUDE** 无法与 **ADDLOCAL** 一起使用。

请参阅文档，以了解用于相应命令行开关的 **msiexec** 版本。

规则

- **ADDLOCAL** 列表是所有要安装的功能名称的按逗号分隔的列表。
- 当选择要安装的功能时，整个路径（所有父功能）必须显式包含在该列表中。
- 有关正确用法的信息，请参阅附加规则。

组件和功能

> 使用 ADDLOCAL/ADDEXCLUDE 参数安装组件不适用于 ESET Endpoint Antivirus。

这些功能分为 4 个类别：

- **必需** – 将始终安装该功能。
- **可选** – 该功能可以取消选中，以便不进行安装。
- **不可见** – 为了使其他功能正常工作，逻辑功能是强制性的

- **占位符** – 不会对产品造成影响的功能，但必须与子功能一同列出

ESET Endpoint Antivirus 的功能集如下所示：

说明	功能名称	功能父级	状态
基础程序组件	Computer		占位符
检测引擎	Antivirus	Computer	必需
检测引擎/恶意软件扫描	Scan	Computer	必需
检测引擎/文件系统实时防护	RealtimeProtection	Computer	必需
检测引擎/恶意软件扫描/文档防护	DocumentProtection	Antivirus	可选
设备控制	DeviceControl	Computer	可选
网络防护	Network		占位符
网络防护/防火墙	Firewall	Network	可选
网络防护/网络攻击防护/...	IdsAndBotnetProtection	Network	可选
安全的浏览器	OnlinePaymentProtection	WebAndEmail	可选
Web 和电子邮件	WebAndEmail		占位符
Web 和电子邮件/协议过滤	ProtocolFiltering	WebAndEmail	不可见
Web 和电子邮件/Web 访问保护	WebAccessProtection	WebAndEmail	可选
Web 和电子邮件/电子邮件客户端访问保护	EmailClientProtection	WebAndEmail	可选
Web 和电子邮件/电子邮件客户端保护/电子邮件客户端	MailPlugins	EmailClientProtection	不可见
Web 和电子邮件/电子邮件客户端保护/反垃圾邮件防护	Antispam	EmailClientProtection	可选
Web 和电子邮件/Web 控制	WebControl	WebAndEmail	可选
工具/ESET RMM	Rmm		可选
更新/配置文件/更新镜像	UpdateMirror		可选
ESET Inspect 插件	EnterpriseInspector		不可见

组功能集：

说明	功能名称	功能状态
所有必需功能	_Base	不可见
所有可用功能	ALL	不可见

附加规则

- 如果选择安装任何一种 **WebAndEmail** 功能，则必须在列表中包含不可见的 **ProtocolFiltering** 功能。

- 所有功能的名称都区分大小写，例如 UpdateMirror 不等效于 UPDATEMIRROR。

配置属性列表

属性	值	功能
CFG_POTENTIALLYUNWANTED_ENABLED=	0 – 禁用 1 – 启用	PUA 检测

属性	值	功能
CFG_LIVEGRID_ENABLED=	见下文	请参阅以下 LiveGrid 属性
FIRSTSCAN_ENABLE=	0 – 禁用 1 – 启用	安装后计划并运行计算机扫描
CFG_PROXY_ENABLED=	0 – 禁用 1 – 启用	代理服务器设置
CFG_PROXY_ADDRESS=	<ip>	代理服务器 IP 地址
CFG_PROXY_PORT=	<port>	代理服务器端口号
CFG_PROXY_USERNAME=	<username>	用于身份验证的用户名
CFG_PROXY_PASSWORD=	<password>	用于身份验证的密码
ACTIVATION_DATA=	见下文	产品激活、许可证密钥或脱机许可证文件
ACTIVATION_DLG_SUPPRESS=	0 – 禁用 1 – 启用	如果设置为“1”，则首次启动后不会显示产品激活对话框
ADMINCFG=	<path>	导出的 XML 配置的路径（默认值 *cfg.xml*）

LiveGrid® 属性

在 `CFG_LIVEGRID_ENABLED` 的情况下安装 ESET Endpoint Antivirus 时，产品在安装后的行为将是以下情形：

功能	CFG_LIVEGRID_ENABLED=0	CFG_LIVEGRID_ENABLED=1
ESET LiveGrid® 信誉系统	开	开
ESET LiveGrid® 反馈系统	关	开
提交匿名统计	关	开

ACTIVATION_DATA 属性

格式	方法
ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE	使用 ESET 许可证密钥激活（Internet 连接应处于活动状态）
ACTIVATION_DATA=offline:C:\ProgramData\ESET\ESET Security\license.lf	使用脱机许可证文件激活

语言属性

ESET Endpoint Antivirus 语言（必须支持这两个属性）。

属性	值
PRODUCT_LANG=	LCID 十进制（区域设置 ID）例如英语(美国) 为 1033，请参阅语言代码列表。
PRODUCT_LANG_CODE=	小写的 LCID 字符串（语言文化名城），例如“英语 – 美国”为 en-us。请参阅语言代码列表。

命令行安装示例

在运行安装之前，确保已阅读最终用户许可协议并具有管理员权限。

排除安装 **NetworkProtection** 部分（还必须指定所有子功能）：
```
msiexec /qn /i ees_nt64.msi ADDEXCLUDE=Network,Firewall,IdsAndBotnetProtection
```

如果希望安装后自动配置 ESET Endpoint Antivirus，可以在安装命令中指定基本配置参数。在 ESET LiveGrid® 启用的情况下安装 ESET Endpoint Antivirus：
```
msiexec /qn /i ees_nt64.msi CFG_LIVEGRID_ENABLED=1
```

安装到非默认的其他应用程序安装目录。
```
msiexec /qn /i ees_nt64_enu.msi APPDIR=C:\ESET\
```

使用 ESET 许可证密钥安装并激活 ESET Endpoint Antivirus：
```
msiexec /qn /i ees_nt64_enu.msi ACTIVATION_DATA=key:AAAA-BBBB-CCCC-DDDD-EEEE
```

在详细日志记录（对故障排除有用）以及使用仅包含必需组件的 RMM 的情况下静默安装：
```
msiexec /qn /i ees_nt64.msi /l*xv msi.log ADDLOCAL=_Base,Rmm
```

在使用指定语言的情况下强制执行静默完整安装。
```
msiexec /qn /i ees_nt64.msi ADDLOCAL=ALL PRODUCT_LANG=1033 PRODUCT_LANG_CODE=en-us
```

安装后命令行选项

- ESET CMD – 导入 .xml 配置文件或打开/关闭安全功能
- 命令行扫描程序 – 从命令行运行计算机扫描

使用 GPO 或 SCCM 进行部署

除了将 ESET Endpoint Antivirus 直接安装在客户端工作站上之外，还可以使用诸如 Group Policy Object (GPO)、Software Center Configuration Manager (SCCM)、Symantec Altiris 或 Puppet 之类的管理工具进行安装。

托管（建议）

对于托管计算机，我们会先安装 ESET Management 服务器代理，然后通过 ESET PROTECT 部署 ESET Endpoint Antivirus。ESET PROTECT 必须安装在您的网络中。

1. 下载 ESET Management 服务器代理的独立安装程序。
2. 准备 GPO/SCCM 远程部署脚本。
3. 使用 GPO 或 SCCM 部署 ESET Management 服务器代理。
4. 确保客户端计算机已添加到 ESET PROTECT。

5. 将 ESET Endpoint Antivirus 部署到客户端计算机并激活

以下 ESET 知识库文章可能仅提供英文版：
- 通过 SCCM 或 GPO 部署 ESET Management Agent
- 使用组策略对象 (GPO) 部署 ESET Management Agent

^ ˅

升级到更新版本

发布 ESET Endpoint Antivirus 的新版本，是为了实施改进或修复程序模块的自动更新无法解决的问题。

有多种方法可以升级到更新版本：

1.自动，使用 ESET PROTECT 或 ESET PROTECT Cloud。ESET Endpoint Antivirus 版本 9 无法由 ESET Remote Administrator 进行管理。

2.自动，使用 GPO 或 SCCM。

3.通过程序更新自动升级。
因为程序升级被分发给所有用户，而且可能对某些系统配置产生影响，所以会在长时间的测试之后才发布，以确保所有可能的系统配置都能够工作。 如果发布后需要立刻升级到更新版本，请使用以下方法之一。
确保已在**高级设置 (F5) > 更新 > 配置文件 > 产品更新**中启用**更新模式**。

4.手动（通过以前的版本来下载并安装更新版本。

建议的升级方案

我管理或我希望远程管理我的 ESET 产品

如果管理 10 个以上 ESET Endpoint 产品，请考虑使用 ESET PROTECT。ESET PROTECT Cloud 执行升级。

请参阅以下文档：

- ESET PROTECT | 通过客户端任务升级 ESET 软件
- ESET PROTECT | 适用于管理最多 250 个 Windows ESET Endpoint 产品的中小型企业的指南
- ESET PROTECT Cloud 介绍

在客户端工作站上手动升级

请勿基于版本 4.x 安装版本 9；同样地，如果使用的是较旧/无法正常运行的 ESET Endpoint Antivirus 版本 5.x 或 6.x。也请勿基于它们安装较新版本。

如果计划在各个客户端工作站上手动执行升级：

1. 验证您的操作系统是否受支持（Windows Vista 和 Windows XP 不支持用于版本）。

2. 基于以前版本下载并安装较新版本。

如果要最大程度地增加成功升级到最新版本 9.x 的机会，请从以下 ESET Endpoint Antivirus 版本之一升级：
• 5.0.2272.x
• 6.5.2132.x
• 7.3.2044.x
否则，请首先卸载您的 ESET Endpoint Antivirus。有关在客户端工作站上升级 ESET Endpoint Antivirus 的其他信息，请阅读以下 ESET 知识库文章。

安全性和稳定性更新

更新 ESET Endpoint Antivirus 是维持全面防范恶意代码的重要组成部分。ESET Endpoint Antivirus 的每个新版本均具有许多改进和错误修复。强烈建议您定期更新 ESET Endpoint Antivirus，以防止出现安全漏洞和威胁。ESET Endpoint Antivirus 与其他任何 ESET 产品一样，都适用于产品生命周期的特定阶段。

阅读以下内容的更多信息：
生命周期结束策略（商业版产品）
产品更新
有关 ESET Endpoint Antivirus 中更改的其他信息，请参阅以下 ESET 知识库文章。

自动更新将确保您的产品达到最大安全性和稳定性。无法禁用安全性和稳定性更新。

常见安装问题

如果在安装期间发生问题，请查看我们的常见安装错误和解决方案列表，以查找有关您的问题的解决方案。

激活失败

如果激活 ESET Endpoint Antivirus 不成功，最常见的可能情况为：

- 许可证密钥已在使用中
- 无效的许可证密钥。产品激活表单错误
- 激活所需的附加信息丢失或无效
- 与激活数据库通信失败。请 15 分钟后重新尝试激活
- 未与 ESET 激活服务器连接或禁止与其连接

请确保已输入正确的许可证密钥或已附加脱机许可证，然后再次尝试激活。

如果无法激活，我们的欢迎程序包会引导您解决常见问题、错误、激活和许可问题（以英语和其他几种语言提供）。

- 启动 ESET 产品激活故障排除

产品激活

完成安装后，将提示您激活您的产品。

选择其中一个可用方法来激活 ESET Endpoint Antivirus。有关更多信息，请参阅如何激活 ESET Endpoint Antivirus。

计算机扫描

我们建议您执行常规计算机扫描，或计划常规扫描，以检查威胁。在主程序窗口中，单击**计算机扫描**，然后单击**智能扫描**。有关计算机扫描的更多信息，请参见计算机扫描。

入门指南

本章提供对 ESET Endpoint Antivirus 及其基本设置的初步概述。

用户界面

ESET Endpoint Antivirus 的主程序窗口分为两个主要部分。右侧的主窗口显示与左侧的主菜单中选定选项相关的信息。

以下是主菜单中选项的说明：

防护状态 – 提供有关 ESET Endpoint Antivirus 的防护状态的信息。

计算机扫描 – 此选项允许您配置和启动智能扫描、自定义扫描或可移动媒体扫描。您还可以重复上次运行的扫描。

更新 – 显示有关检测引擎的信息以及允许手动检查更新。

设置 – 选中此选项以调整您的计算机 或者 Web 和电子邮件安全设置。

工具 – 提供对日志文件、防护统计信息、查看活动、运行进程、计划任务、隔离区, ESET SysInspector 和 ESET SysRescue 的访问权限以创建修复 CD□您还可以提交样本以供分析。

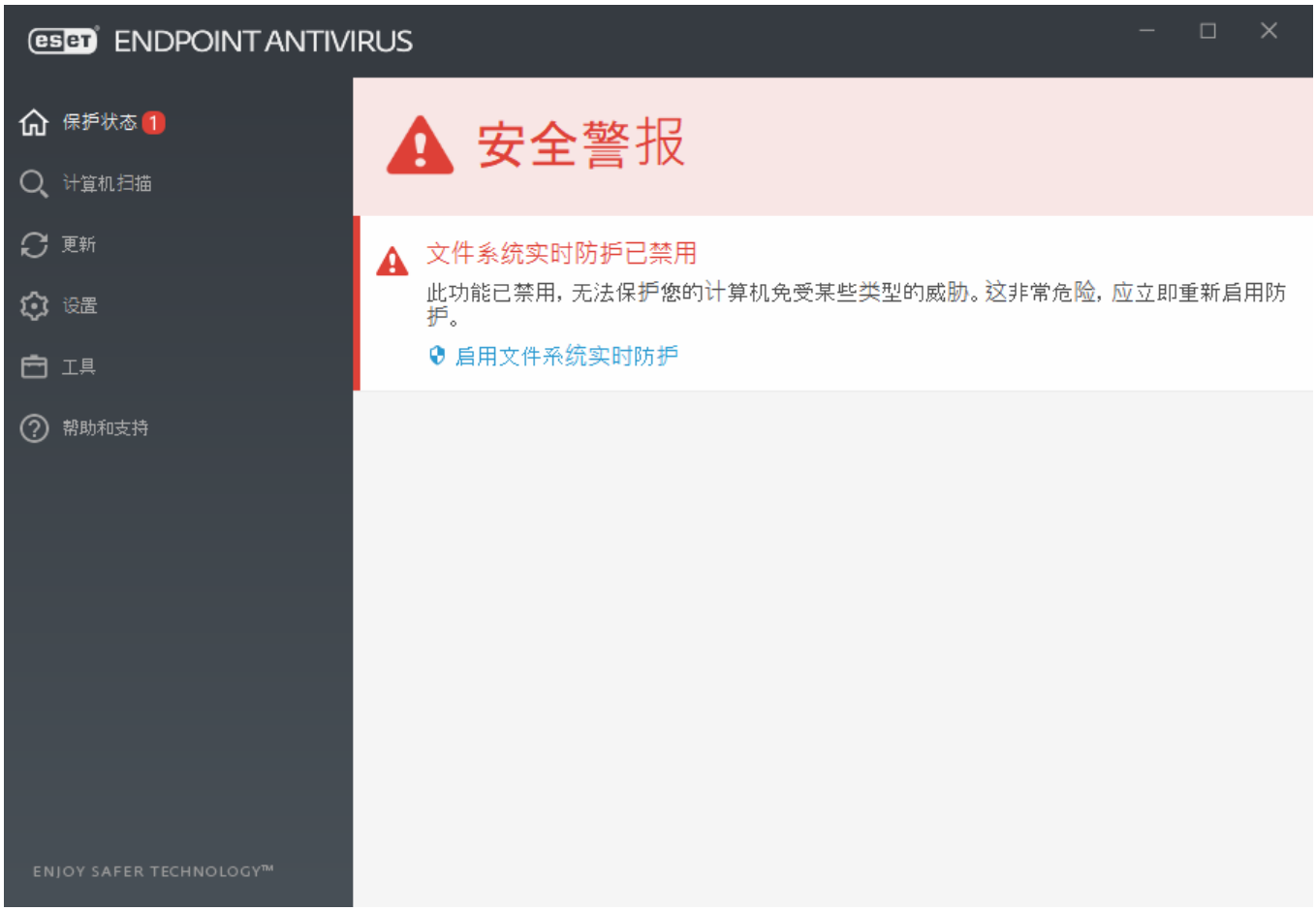
帮助和支持 – 提供对帮助文件、ESET 知识库和 ESET 公司网站的访问。还提供用于打开“技术支持”技术请求的链接、支持工具以及有关产品激活的信息。

防护状态屏幕可告知您计算机的安全性和当前的防护级别。绿色**最高防护**状态表示已确保最高防护。

状态窗口还显示指向 ESET Endpoint Antivirus 中常用功能的快速链接和有关上次更新的信息。

程序工作不正常时如何应对？

在所有完全正常工作的程序模块旁边将显示一个绿色对号标记。如果模块需要注意，将显示红色惊叹号或橙色通知图标。有关模块的其他信息（包括我们有关如何恢复全部功能的建议）将显示在窗口的上半部分。若要更改模块的状态，请在主菜单中单击**设置**，然后单击所需模块。



红色惊叹号（!）图标表示不能确保为计算机提供最大程度的防护。您可能会在以下情形中遇到此类通知：

- **病毒和间谍软件防护已暂停** – 在**防护状态**窗格中，单击**启动所有病毒和间谍软件防护模块**以重新启用病毒和间谍软件防护，或者在主程序窗口的**设置**窗格中，单击**启用病毒和间谍软件防护**。
- 病毒防护不起作用 – 病毒扫描程序初始化失败。大多数 ESET Endpoint Antivirus 模块无法正常工作。
- **网络钓鱼防护不起作用** – 此功能不起作用，因为其他所需程序模块未处于活动状态。
- **检测引擎已过期** – 此错误将在几次尝试更新检测引擎（以前称为“病毒库”）失败之后显示。建议您检查更新设置。此错误的最常见原因是错误输入验证数据或错误配置连接设置。
- **产品未激活**或**许可证已过期** – 此问题由红色防护状态图标表示。许可证过期后该程序将无法更新。按照警报窗口中的说明续订许可证。

• **主机入侵预防系统 (HIPS) 已禁用** – 从高级设置中禁用 HIPS 会导致出现此问题。您的计算机未针对某些类型的威胁提供防护，应立即通过单击**启用 HIPS** 来重新启用防护。

• **ESET LiveGrid® 已禁用** – 在高级设置中禁用 ESET LiveGrid® 会导致出现此问题。

• **未计划定期更新** – 除非您计划更新任务，否则 ESET Endpoint Antivirus 将不会检查更新或收到重要更新。

• **反隐藏技术已禁用** – 单击**启用反隐藏技术**以重新启用该功能。

• **已阻止网络访问** – 当在来自 ESET PROTECT 的此工作站上触发了**将计算机与网络隔离**客户端任务时显示。请联系系统管理员以获取详细信息。

• **文件系统实时防护已暂停** – 用户已禁用实时防护。您的计算机未针对威胁提供防护。单击启用实时防护重新启用该功能。

橙色“i”表示 ESET 产品存在一个不严重的问题，需要您关注。可能的原因包括：

• **Web 访问保护已禁用** – 单击安全通知以重新启用 Web 访问保护，然后单击**启用 Web 访问保护**。
• **您的许可证即将到期** – 此问题由显示惊叹号的防护状态图标表示。许可证过期后，程序将无法更新，防护状态图标将变为红色。

• **反垃圾邮件防护已暂停** – 单击**启用反垃圾邮件防护**以重新启用该功能。

• **Web 控制已暂停** – 单击**启用 Web 控制以重新启用该功能。**

• **策略覆盖处于活动状态** – 暂时覆盖策略设置的配置，可能直到故障排除结束为止。只有授权用户才可以覆盖策略设置。有关详细信息，请参阅如何使用覆盖模式。

• **设备控制已暂停** – 单击**启用设备控制**以重新启用该功能。

要在 ESET Endpoint Antivirus 的第一个窗格中调整产品状态的可见性，请参见应用程序状态。

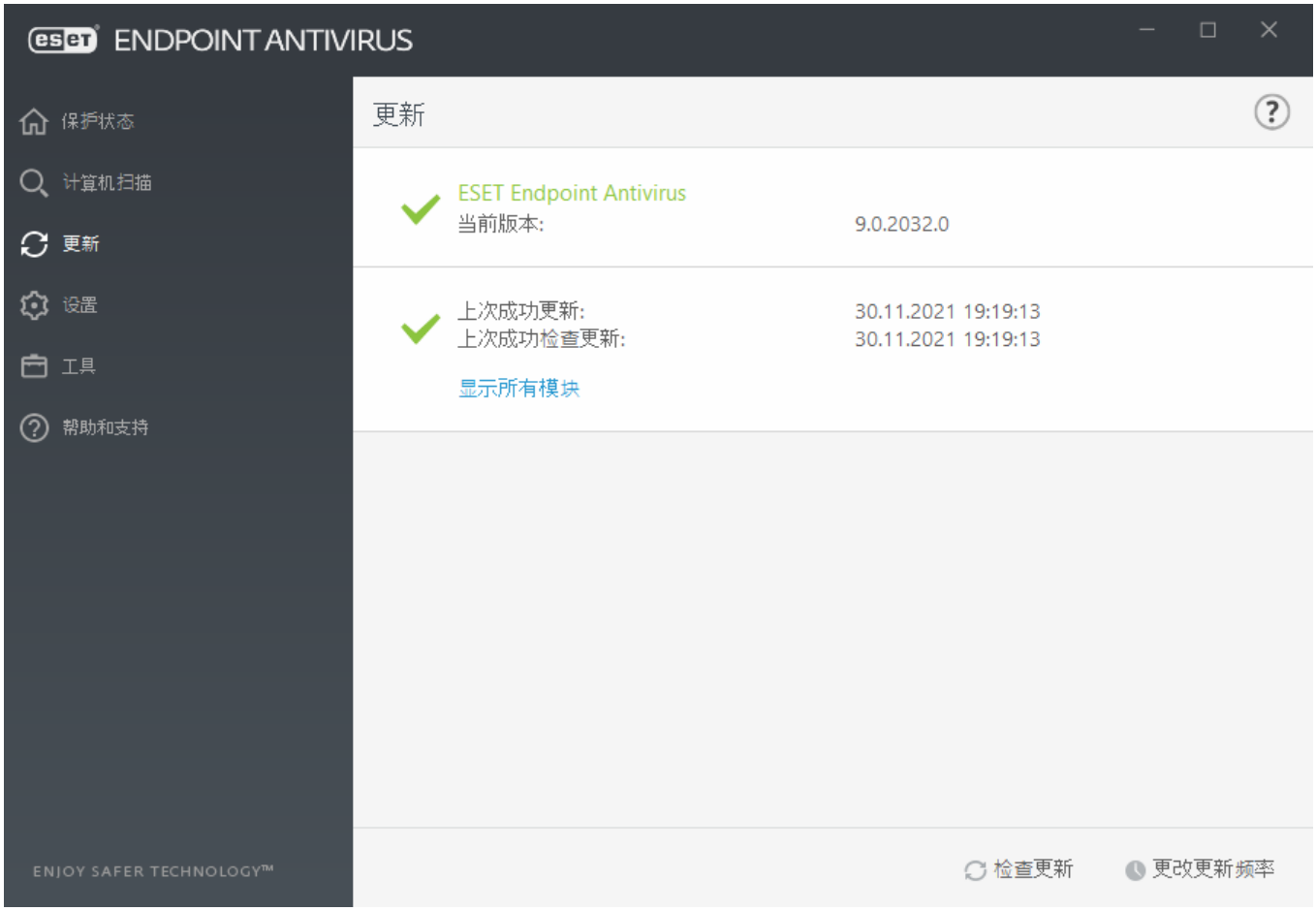
如果使用建议的解决方案无法解决问题，请单击**帮助和支持**访问帮助文件或搜索 ESET 知识库。如果仍需要帮助，可以提交 ESET 技术支持请求。ESET 技术支持将快速响应您的问题，并帮助找到解决方案。

如果状态属于受 ESET PROTECT 策略阻止的功能，该链接将处于不可点击状态。

更新设置

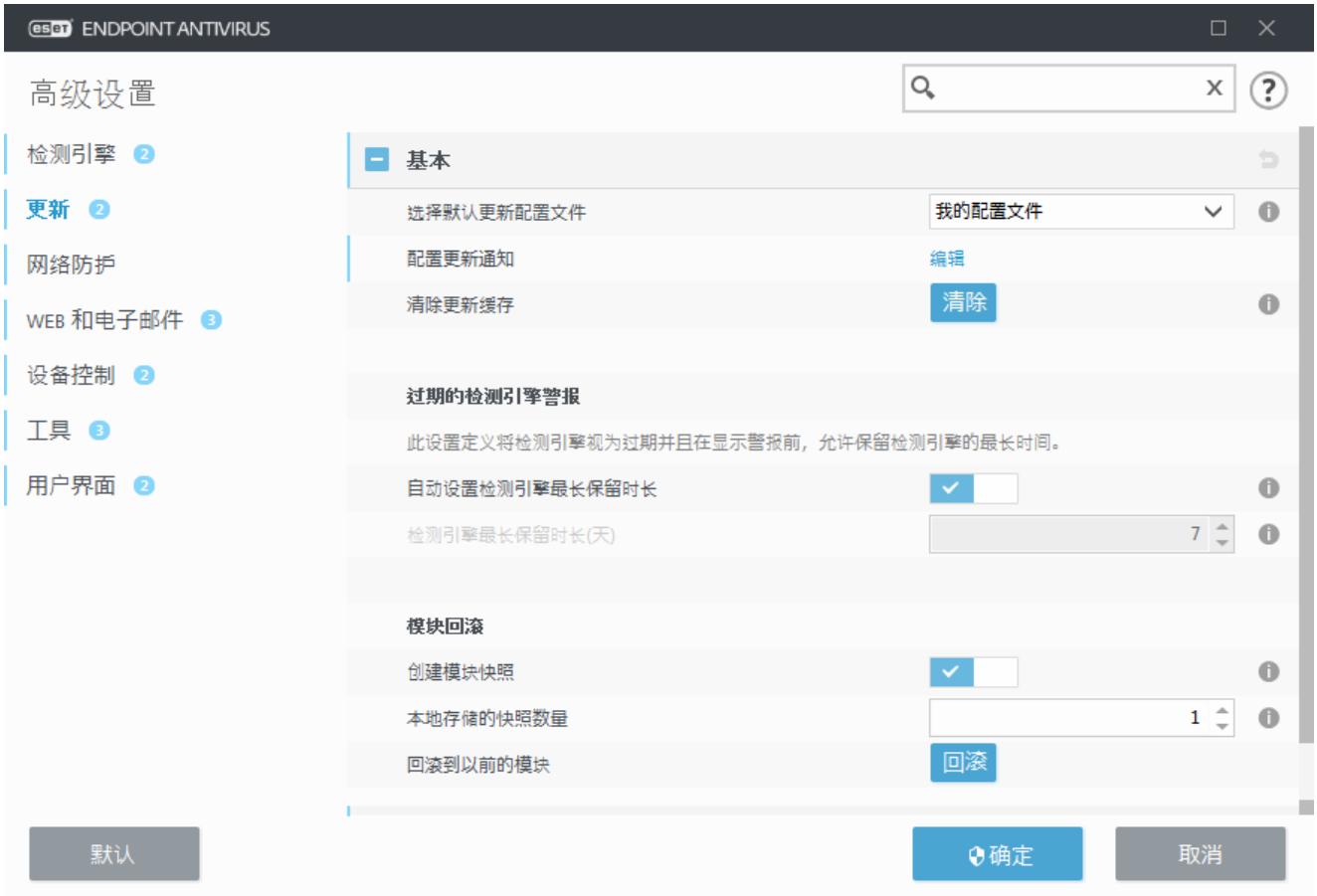
更新模块是维持对恶意代码的全面防护的重要部分。请注意更新配置和操作。在主菜单中，依次选择**更新 > 检查更新**以检查是否有较新的模块更新。

如果尚未输入您的**许可证密钥**，您将无法收到新更新，并且系统将提示您激活您的产品。



“高级设置”窗口（从主菜单中依次单击**设置 > 高级设置**，或按键盘上的 **F5** 键）中包含其他更新选项。若要配置高级更新选项（如更新模式、代理服务器访问、局域网连接和检测引擎副本创建设置），请单击“高级设置”树中的**更新**。

- 如果您遇到更新问题，请单击**清除**以清除临时更新缓存。



- **自动选择**选项（在**配置文件 > 更新 > 模块更新**中）默认启用。使用 ESET 更新服务器来接收更新时，建议您保持此选项设置不变。

- 如果不希望在屏幕右下角显示成功更新系统托盘通知，请展开**配置文件 > 更新**，单击**选择收到的更新通知**旁边的**编辑**，然后调整**检测引擎成功更新**通知的复选框。

自动更新程序对获得最佳功能非常重要。只有在**帮助和支持 > 激活产品**中输入了正确的**许可证密钥**时才可以执行此操作。

如果您在安装后没有输入**许可证密钥**，您可以随时输入此密钥。有关激活的详细信息，请参阅如何激活 ESET Endpoint Antivirus，并将您随 ESET 安全产品收到的凭据输入到**许可证详细信息**窗口。

使用 ESET Endpoint Antivirus

ESET Endpoint Antivirus 设置选项允许您调整计算机、Web 和电子邮件的防护级别。

> 从 ESET PROTECT Web 控制台创建策略时，可以为每个设置选择标志。带有强制执行标志的设置具有优先级，无法被以后的策略覆盖（即使以后的策略也具有强制执行标志）。这确保了此设置不会更改（例如，合并期间由用户或以后的策略进行更改）。有关详细信息，请参阅 ESET PROTECT 联机帮助中的标志。

设置菜单包含以下部分：

- **计算机**
- **网络**
- **Web 和电子邮件**

计算机部分允许您启用或禁用以下组件：

- **文件系统实时防护** – 在计算机上打开、创建或运行所有文件时，都将扫描文件是否带有恶意代码。
- **设备控制** – 提供自动设备 (CD/DVD/USB/...) 控制。此模块允许您阻止或调整扩展的过滤器/权限，以及定义用户访问和使用给定设备的能力。
- **Host Intrusion Prevention System (HIPS)** - HIPS 系统监视操作系统内发生的事件，并按照自定义的规则集进行响应。
- **高级内存扫描程序** – 与漏洞利用阻止程序结合使用以增强对恶意软件的防范，后者旨在通过迷惑或加密方法来逃过反恶意软件产品的检测。默认情况下，启用高级内存扫描程序。请阅读词汇表中关于此类防护的更多信息。
- **漏洞利用阻止程序** – 旨在强化那些经常被漏洞利用的应用程序类型，例如 Web 浏览

器、PDF 阅读器、电子邮件客户端和 MS Office 组件。默认启用漏洞利用阻止程序。请阅读词汇表中有关此类防护的更多信息。

• **勒索软件防护**是作为 HIPS 功能的一部分工作的另一层保护。 必须启用 ESET LiveGrid® 信誉系统才能使勒索软件防护工作。请在此处阅读关于此类防护的详细信息。

• **演示模式** – 为那些需要不中断其使用软件、不希望被弹出窗口打扰，并希望尽量减少 CPU 使用的用户提供的功能。启用演示模式后您将收到警告消息（潜在安全风险），主程序窗口将变为橙色。

网络部分允许您配置网络攻击防护 (IDS) 和僵尸网络保护。

Web 和电子邮件防护设置允许您启用或禁用以下组件：

• **Web 访问保护** – 如果已启用，将扫描所有通过 HTTP 或 HTTPS 的通信以查看是否有恶意软件。

• **电子邮件客户端防护** – 监视通过 POP3 和 IMAP 协议接收的通信。

• **网络钓鱼防护** – 防止冒充合法网站的非法网站尝试获取密码、银行数据和其他敏感信息，从而为您提供保护。

要暂时禁用单个模块，请单击所需模块旁边的绿色开关 。注意，这可能会降低对您的计算机的保护级别。

要重新启用已禁用的安全组件的防护，请单击红色开关 以使组件返回其启用状态。

应用 ESET PROTECT 策略后，将在特定组件的旁边看到锁定图标 。经登录用户（如管理员）验证身份后，可以在本地覆盖由 ESET PROTECT 应用的策略。有关详细信息，请参阅 ESET PROTECT 联机帮助。

计算机重新启动后，以这种方式禁用的所有防护措施都将重新启用。

要访问特定安全组件的详细设置，请单击任一组件旁边的齿轮 。

在设置窗口的底部还有其他选项。若要使用 *.xml* 配置文件加载设置参数，或将当前设置参数保存为配置文件，请使用**导入/导出设置**。有关更多详细信息，请参阅导入/导出设置。

有关更详细的选项，请单击**高级设置**或按 **F5**。

计算机

计算机模块可以在**设置 > 计算机**下找到。它显示之前的章节中所述的防护模块的概述。在此部分中，提供以下设置：

单击**文件系统实时防护**旁边的齿轮 并单击**编辑排除**，以打开排除设置窗口，此窗口允许您排除扫描文件和文件夹。要打开**文件系统实时防护**高级设置，请单击**配置**。

计算机部分允许您启用或禁用以下组件：

- **文件系统实时防护** – 在计算机上打开、创建或运行所有文件时，都将扫描文件是否带有恶意代码。

- **设备控制** – 提供自动设备 (CD/DVD/USB/...) 控制。此模块允许您阻止或调整扩展的过滤器/权限，以及定义用户访问和使用给定设备的能力。

- **Host Intrusion Prevention System (HIPS)** - HIPS 系统监视操作系统内发生的事件，并按照自定义的规则集进行响应。

- **高级内存扫描程序** – 与漏洞利用阻止程序结合使用以增强对恶意软件的防范，后者旨在通过迷惑或加密方法来逃过反恶意软件产品的检测。默认情况下，启用高级内存扫描程序。请阅读词汇表中关于此类防护的更多信息。

- **漏洞利用阻止程序** – 旨在强化那些经常被漏洞利用的应用程序类型，例如 Web 浏览器、PDF 阅读器、电子邮件客户端和 MS Office 组件。默认启用漏洞利用阻止程序。请阅读词汇表中有关此类防护的更多信息。

- **勒索软件防护**是作为 HIPS 功能的一部分工作的另一层保护。 必须启用 ESET LiveGrid® 信誉系统才能使勒索软件防护工作。请在此处阅读关于此类防护的详细信息。

- **演示模式** – 为那些需要不中断其使用软件、不希望被弹出窗口打扰，并希望尽量减少 CPU 使用的用户提供的功能。启用演示模式后您将收到警告消息（潜在安全风险），主程序窗口将变为橙色。

暂停病毒和间谍软件防护 – 在您临时禁用病毒和间谍软件防护时，可以使用下拉菜单选择您希望禁用所选组件的时间段，然后单击**应用**以禁用该安全组件。要重新启用防护，请单击**启用病毒和间谍软件防护**。

检测引擎

检测引擎通过控制文件、电子邮件和 Internet 通信，来抵御恶意系统攻击。例如，如果检测到归类为恶意软件的对象，将开始清除。检测引擎可以通过先阻止它，然后清除、删除或将其移至隔离区来消除威胁。

要详细配置检测引擎设置，请单击**高级设置**或按 **F5**。

在本部分中：

- 实时和机器学习保护类别
- 恶意软件扫描
- 报告设置
- 防护设置
- 最佳做法

> 从版本 7.2 起，检测引擎部分不再像 7.1 及更低版本一样提供“开/关”切换。“开/关”按钮由四个阈值替代 – 具有攻击性、均衡、注意和关闭。

实时和机器学习保护类别

针对所有防护模块（例如，文件系统实时防护、Web 访问保护...）的**实时和机器学习保护**允许您配置以下类别的报告和防护级别：

• 恶意软件 – 计算机病毒是一条预置或附加到计算机上现有文件的恶意代码。但是，术语“病毒”经常被误用。“恶意软件”（恶意的软件）是更准确的术语。恶意软件检测由结合了机器学习组件的检测引擎模块执行。
请阅读词汇表中关于这些类型的应用程序的更多信息。

• 潜在不受欢迎的应用程序 - 灰色软件或潜在不受欢迎的应用程序 (PUA) 是一种广泛的软件类别，其意图不像其他类型的恶意软件（如病毒或木马）那样具有明确的恶意。但它可能安装其他不受欢迎的软件、更改数字设备的行为，或者执行用户未批准的活动或意料之外的活动。
请阅读词汇表中关于这些类型的应用程序的更多信息。

• 潜在的不安全应用程序 – 是指有可能被滥用于恶意用途的合法商业软件。潜在的不安全应用程序 (PUA) 的示例包括远程访问工具、密码破解应用程序以及按键记录器（记录用户键盘输入信息的程序）等。此选项默认情况下处于禁用状态。
请阅读词汇表中关于这些类型的应用程序的更多信息。

- **可疑应用程序**包括使用加壳程序或保护程序压缩的程序。这些类型的保护程序通常被恶意软

件作者用来逃避检测。

高级机器学习现在作为高层次防护成为检测引擎的一部分，可根据机器学习改进检测。在词汇表中详细了解此类防护。

恶意软件扫描

可以为实时扫描程序和手动扫描程序单独配置扫描程序设置。默认情况下，**使用实时防护设置**处于启用状态。当启用时，相关手动扫描设置从**实时和机器学习保护**部分继承。

报告设置

当发生检测时（例如，发现威胁和归类为恶意软件），信息将记录到检测日志，如果在 ESET Endpoint Antivirus 中进行了配置，将发生桌面通知。

为每个类别（作为“CATEGORY”引用）配置报告阈值：

1.恶意软件

2.潜在不受欢迎的应用程序

3.潜在不安全

4.可疑应用程序

通过检测引擎进行报告，包括机器学习组件。可以设置比当前防护阈值更高的报告阈值。这些报告设置不影响阻止、清除或删除对象。

为 CATEGORY 报告修改阈值（或级别）前阅读以下内容：

阈值	解释
具有攻击性	CATEGORY 报告配置为最高敏感度。报告了更多检测。**具有攻击性**设置可能会将对象错误地识别为 CATEGORY。
均衡	CATEGORY 报告配置为均衡。优化了此设置以均衡检测率和误报对象数量的性能和准确性。
注意	CATEGORY 报告配置为最大程度地减少错误识别的对象，同时维持足够级别的防护。仅当可能性显而易见并且匹配 CATEGORY 行为时才报告对象。
关	CATEGORY 的报告不活动，并且不查找、报告或清除此类型的检测。因此，此设置将从此检测类型中禁用防护。 “关”对于恶意软件报告不可用，而且它是潜在不安全的应用程序的默认值。

ESET Endpoint Antivirus 防护模块的可用性

对于选定的 CATEGORY 阈值，防护模块的可用性（已启用或已禁用）如下：

	具有攻击性	均衡	注意	关**
高级机器学习模块*	✔ （具有攻击性模式）	✔ （保守模式）	X	X
检测引擎模块	✔	✔	✔	X
其他防护模块	✔	✔	✔	X

* 在 ESET Endpoint Antivirus 版本 7.2 及更高版本中可用。
**不建议

确定产品版本、程序模块版本和内部版本日期

1. 单击**帮助和支持 > 关于 ESET Endpoint Antivirus**。
2. 在**关于**屏幕中，文本的第一行显示 ESET 产品的版本号。
3. 单击**已安装的组件**以访问关于特定模块的信息。

要点

为环境设置适当阈值的几项要点：

- 为大多数设置建议**均衡**阈值。

- **注意**阈值表示从 ESET Endpoint Antivirus 之前的版本（7.1 及更低版本）可比较的防护级别。建议用于优先级侧重于最大程度减少由安全软件错误识别的对象的环境。

- 更高的报告阈值，更高的检测率，但错误识别对象的机会更高。
- 从真实世界角度来看，不能保证 100% 的检测率和 0% 的机会来避免错误地将干净对象归类为恶意软件。
- 保持 ESET Endpoint Antivirus 及其模块最新，以最大程度地保持性能、检测率的准确性与误报对象数量之间的平衡。

防护设置

如果报告归类为 CATEGORY 的对象，程序会阻止该对象，然后对它清除、删除或将其移动到隔离区。

为 CATEGORY 保护修改阈值（或级别）前阅读以下内容：

阈值	解释
具有攻击性	报告的具有攻击性（或更低）级别检测被阻止，自动修复（即，清除）会启动。当使用具有攻击性设置扫描了所有端点并且误报的对象已添加到检测排除中时，建议使用此设置。
均衡	报告的均衡（或更低）级别检测被阻止，自动修复（即，清除）会启动。
注意	报告的注意级别检测被阻止，自动修复（即，清除）会启动。
关	有助于识别和排除误报的对象。 “关”对于恶意软件防护不可用，而且它是潜在不安全的应用程序的默认值。

适用于 ESET Endpoint Antivirus 7.1 及更低版本的 ESET PROTECT 策略转换表

从适用于扫描程序设置的 ESET PROTECT 策略编辑器开始，不再包含每个 CATEGORY 的“开/关”开关。下表概述了防护阈值与 ESET Endpoint Antivirus 7.1 及更低版本中开关的最终状态之间的转换。

CATEGORY 阈值状态	具有攻击性	均衡	注意	关
已应用的 CATEGORY 开关	✓	✓	✓	✗

从版本 7.1 及更低版本升级到版本 7.2 及更高版本后，新的阈值状态将如下所示：

升级前的类别开关	✓	✗
升级后新的 CATEGORY 阈值	均衡	关

最佳做法

未托管（单个客户端工作站）

原样保留默认建议值。

受管环境

这些设置通常通过策略应用到工作站。

1. 初始阶段

此阶段可能需要一周的时间。

- 将所有**报告**阈值设置为**均衡**。
注意，如果需要，请设置为**具有攻击性**。
- 设置或保留恶意软件的**防护**为**均衡**。
- 将其他类别的**防护**设置为**注意**。
注意：不建议您在此阶段将**防护**阈值设置为**具有攻击性**，因为所有发现的检测（包括错误识别的检测）都将得到修复。
- 在检测日志中识别错误识别的对象，然后先将它们添加到检测排除。

2. 过渡阶段

- 对某些工作站实施“生产阶段”作为测试（不适用于网络上的所有工作站）。

3. 生产阶段

- 将所有**防护**阈值设置为**均衡**。
- 远程管理时，将适合的病毒防护预定义策略用于 ESET Endpoint Antivirus。
- 如果要求最高的检测率并且接受错误识别的对象，则可以设置**具有攻击性**防护阈值。
- 检查检测日志或 ESET PROTECT 报告，以查找可能丢失的检测。

检测引擎高级选项

反隐藏技术是一个复杂的系统，它能够检测危险程序（例如，rootkits），这些程序可在操作系统下隐藏自己。这意味着使用普通测试技术很难检测到它们。

启用通过 AMSI 的高级扫描 - Microsoft Antimalware Scan Interface 工具，允许应用程序开发人员开发新的恶意软件保护（仅 Windows 10、11）。

检测到渗透

威胁可通过各种渠道进入系统，如网页、共享文件夹、电子邮件或可移动设备（USB、外部磁盘、CD、DVD 等）。

标准行为

作为 ESET Endpoint Antivirus 处理威胁的常见示例，可以使用以下功能检测渗透：

- 文件系统实时防护
- Web 访问保护
- 电子邮件客户端防护
- 手动计算机扫描

每个功能都使用标准清除级别，将尝试清除文件并将其移动到隔离区或终止连接。通知窗口将显示在屏幕右下角的通知区域中。有关检测到/清除的对象的详细信息，请参阅日志文件。有关清除级别和行为的详细信息，请参阅清除

清除和删除

无操作如果文件系统实时防护没有预定义操作，程序将显示一个警报窗口，提示您从中选择一个选项。一般会有**清除**、**删除**和**离开**等选项。不建议选择**离开**，这样将不会清除被感染文件。除非您确信该文件无害，只是检测失误所致。

如果文件遭到了病毒攻击（该病毒在被清除文件上附加了恶意代码），请应用清除。如果是这种情况，请首先尝试清除被感染文件，使其恢复到初始状态。如果文件全部由恶意代码组成，将删除该文件。

如果被感染文件被“锁定”或正在被系统进程使用，通常只在释放后（通常是系统重新启动后）删除。

从隔离恢复

可从 ESET Endpoint Antivirus 主程序窗口中访问隔离区，方法是依次单击**工具 > 隔离**。

隔离的文件还可以恢复到其原始位置：

- 通过在隔离区中右键单击给定文件，即可使用右键菜单提供的**恢复**功能来实现此目的。
- 如果文件被标记为潜在不受欢迎的应用程序，将启用**恢复并从扫描中排除**选项。另请参阅排除。
- 右键菜单还提供**恢复至** 选项，使用此选项可将文件恢复到其被删除时位置之外的其他位置。
- 恢复功能在某些情况下不可用，例如位于只读网络共享上的文件。

多个威胁

如果在计算机扫描期间没有清除任何被感染文件（或清除级别设置为**不清除**），则会出现一个警报窗口，提示您为这些文件选择相应操作。

删除压缩文件中的文件

在默认清除模式下，仅当压缩文件只包含被感染文件而没有干净文件时，才会删除整个压缩文件。换言之，如果还包含无害的干净文件，就不会删除压缩文件。执行严格清除扫描时请小心，严格

清除已启用时，即使压缩文件只包含一个被感染文件，无论压缩文件中其他文件的状态如何，都将删除该压缩文件。

如果您的计算机有被恶意软件感染的迹象（例如速度下降、常常停止响应等），建议您执行以下操作：

- 打开 ESET Endpoint Antivirus 并单击计算机扫描
- 单击**智能扫描**（有关更多信息，请参见计算机扫描）
- 扫描完成后，查看日志中已扫描文件、被感染文件和已清除文件的数量

如果您只希望扫描磁盘的某一部分，请单击**自定义扫描**，然后选择要扫描的目标以查找病毒。

共享的本地缓存

通过消除网络中的重复扫描，共享的本地缓存可以提高隔离环境（例如虚拟机）中的性能。这样可以确保每个文件仅扫描一次并存储在共享缓存中。

必须先安装并配置 ESET Shared Local Cache：

- 下载 ESET Shared Local Cache
- 有关详细信息，请参阅 ESET Shared Local Cache 联机帮助

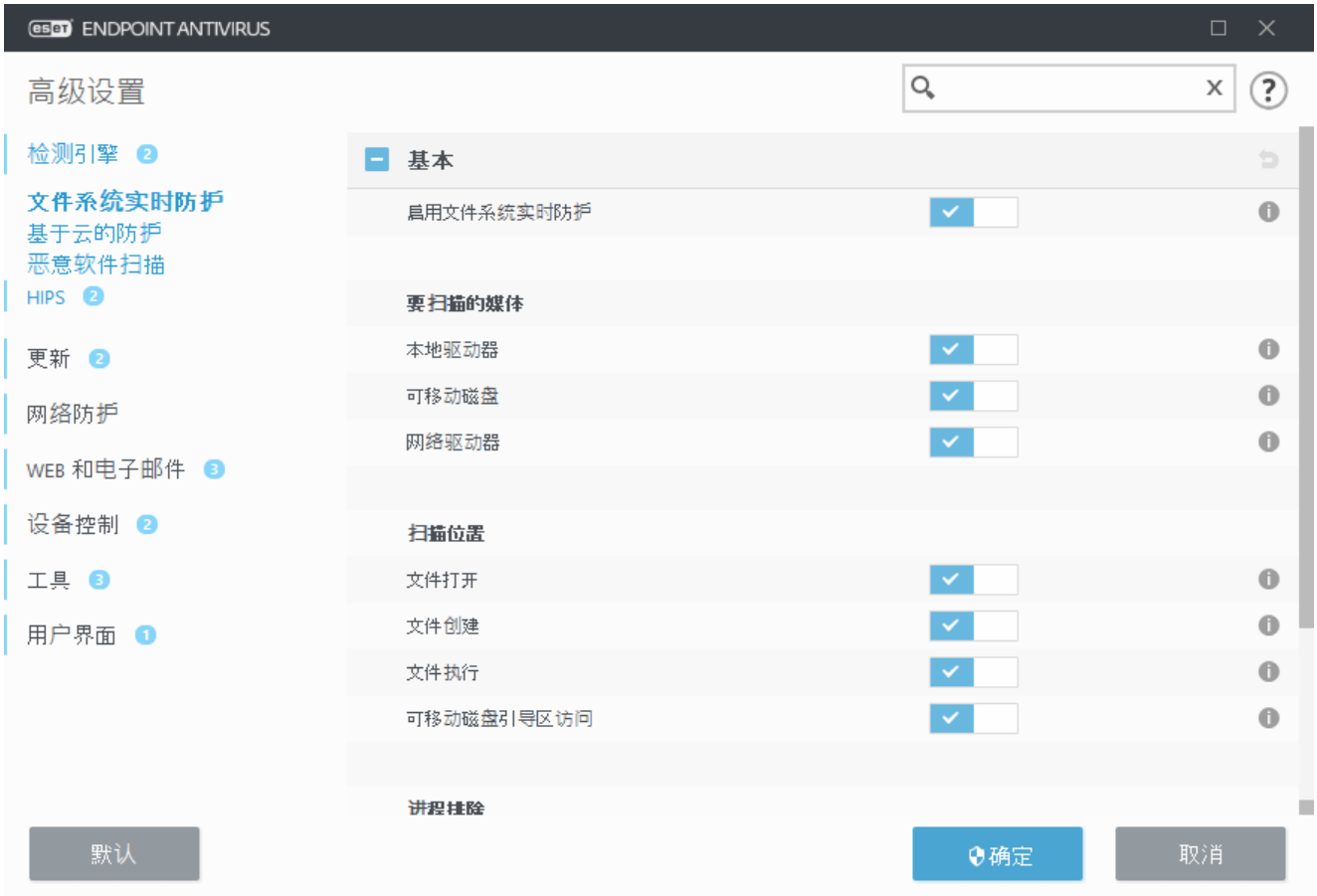
打开**缓存选项**开关，以将有关网络上文件和文件夹的扫描信息保存到 ESET Shared Local Cache。如果执行一个新扫描，ESET Endpoint Antivirus 会在 ESET Shared Local Cache 中搜索已扫描的文件。如果文件匹配，将排除扫描它们。

缓存服务器的设置包含以下内容：

- **主机名** - ESET Shared Local Cache 所在计算机的主机名或 IP 地址。
- **端口** – 用于通信的端口号（与在 ESET Shared Local Cache 中设置的相同）。
- **密码** – 指定 ESET Shared Local Cache 的密码（如果需要）。

文件系统实时防护

当打开、创建或运行文件时，文件系统实时防护会控制系统中的所有文件以查找恶意代码。



默认情况下，文件系统实时防护在系统启动时启动，并提供不间断的扫描。我们不建议在**高级设置**下的**检测引擎 > 文件系统实时防护 > 基本**中禁用**启用文件系统实时防护**。

要扫描的介质

默认情况下，所有类型的介质均可扫描以检查是否存在潜在威胁：

- **本地驱动器** – 扫描所有系统并修复硬盘（例如：*C:*、*D:*）。
- **可移动磁盘** – 扫描 CD/DVD、USB 存储、内存卡等。
- **网络驱动器** – 扫描所有已映射的网络驱动器（例如：*H:* 映射为 *\\store04*）或直接访问网络驱动器（例如：*\\store08*）。

建议您使用默认设置且仅在特殊情况（例如，当扫描某些介质使数据传输速度显著降低时）下修改这些设置。

扫描位置

默认情况下，所有文件都在打开、创建或执行时进行扫描。我们建议您保留这些默认设置，因为它们可为计算机提供最高级别的实时防护：

- **文件打开** – 打开文件时扫描。
- **文件创建** – 扫描创建或修改的文件。

• **文件执行** – 执行或运行文件时扫描。

• **可移动磁盘引导区访问** – 将包含引导区的可移动磁盘插入设备时，系统将立即扫描引导区。此选项不会启动可移动磁盘文件扫描。可移动磁盘文件扫描功能位于**要扫描的磁盘 > 可移动磁盘**。要使**可移动磁盘引导区访问**正常工作，请在 ThreatSense 参数中保持启用**引导区/UEFI**。

要排除扫描的进程 – 在进程排除章节中阅读有关此类排除的更多信息。

文件系统实时防护检查所有类型的介质，并由各种系统事件（例如，访问文件）触发。通过使用 ThreatSense 技术检测方法（如 ThreatSense 引擎参数设置部分所述），将文件系统实时防护配置为采用不同的方式对待新创建的文件和现有文件。例如，您可以将文件系统实时防护配置为更加密切地监视新创建的文件。

为确保在使用实时防护时占用最少的系统资源，已扫描的文件不会重复扫描（除非它们已修改）。在每次更新检测引擎后会立刻重新扫描文件。可使用**智能优化**控制此行为。如果已禁用**智能优化**，则每次访问文件时将扫描所有文件。要修改此设置，请按 **F5** 打开“高级设置”，然后依次展开**检测引擎 > 文件系统实时防护**。依次单击 **ThreatSense 参数 > 其他**，然后选中或取消选中**启用智能优化**。

检查实时防护

要验证实时防护是否工作，是否在检测病毒，请使用来自 eicar.com 的测试文件。此测试文件是一个可供所有病毒防护程序检测的无害文件。此文件由 EICAR 公司（欧洲计算机防病毒研究协会）创建，用于测试病毒防护程序的功能。

此文件可从以下网站下载：http://www.eicar.org/download/eicar.com
在浏览器中输入此 URL 后，您应该会看到一条消息，指出威胁已删除。

何时修改实时防护配置

文件系统实时防护是维护系统安全的最重要的组件。修改其参数时请务必小心。建议您仅在特定情况下修改其参数。

安装 ESET Endpoint Antivirus 后，所有设置都会得到优化以便为用户提供最高级别的系统安全性。若要恢复默认设置，请单击 窗口（**高级设置 > 检测引擎 > 文件系统实时防护**）中每个选项卡旁边的 。

实时防护不工作时如何应对

在本章中，我们将介绍使用实时防护时可能出现的问题，以及如何排除这些故障。

实时防护被禁用

如果用户无意中禁用了实时防护，您应该重新激活该功能。要重新激活实时防护，请在主程序窗口中转到**设置**，然后依次单击**计算机防护 > 文件系统实时防护**。

如果实时防护未能在系统启动时启动，通常是因为**启用文件系统实时防护**处于禁用状态。 若要确保启用此选项，导航至**高级设置 (F5)**，然后依次单击**检测引擎 > 文件系统实时防护**。

如果实时防护功能不检测和清除渗透

请确保您的计算机上未安装任何其他病毒防护程序。 如果同时安装了两个病毒防护程序，它们可能会彼此冲突。 建议您先卸载系统上的任何其他病毒防护程序，再安装 ESET。

实时防护不启动

如果系统启动时实时防护未启动（且**启用文件系统实时防护**已经启用），可能是因为与其他程序发生冲突。要获取解决此问题的帮助，请联系 ESET 技术支持。创建 SysInspector 日志并提交给 ESET 技术支持以供分析，这可以帮助解决问题。有关更多信息，请阅读以下 ESET 知识库文章。

计算机扫描

手动扫描程序是 ESET Endpoint Antivirus 的一个重要组成部分。它可以扫描计算机上的文件和文件夹。从安全角度说，计算机扫描不应仅在怀疑有渗透时运行，而是应作为日常安全手段的一部分定期运行，这一点非常重要。建议您执行定期（例如，一个月一次）系统深度扫描以检测文件系统实时防护未检测到的病毒。如果文件系统实时防护此时处于禁用状态、检测引擎已过时或者文件在保存到磁盘时未检测为病毒，则会发生这种情况。

提供有两种**计算机扫描**。**扫描计算机**快速扫描系统，无需进一步配置扫描参数。**自定义扫描**允许您选择任意预定义的扫描配置文件以及定义特定扫描目标。

请参见扫描进度以了解有关扫描进程的更多信息。

扫描计算机

智能扫描允许您快速启动计算机扫描和清除被感染文件而无需用户干预。智能扫描的优势是便于操作，不需要详细的扫描配置。智能扫描检查本地驱动器上的所有文件并自动清除或删除检测到的威胁。清除级别被自动设置为默认值。有关清除类型的更详细信息，请参见清除。

自定义扫描

如果您要指定扫描参数（如扫描目标和扫描方法等），自定义扫描是一个理想的解决方案。自定义扫描的优点在于可以详细配置参数。配置可以保存到用户定义的扫描配置文件中，这在使用相同的参数重复扫描时非常有用。

要选择扫描目标，请选择**计算机扫描 > 自定义扫描**，然后从**扫描目标**下拉菜单中选择某个选项，或从树结构中选择特定目标。也可以通过输入要包括的文件或文件夹路径，指定扫描目标。如果您仅想扫描系统而不进行附加的清除操作，则选择**扫描但不清除**。执行扫描时，可以通过单击**设置> ThreatSense 参数 > 清除**从三个清除级别中选择。

对于有病毒防护程序使用经验的高级用户，适合于使用自定义扫描来执行计算机扫描。

您还可以使用**拖放扫描**功能手动扫描文件或文件夹，方法是单击文件或文件夹，长按鼠标按钮的同时将鼠标指针移动到标记区域，然后释放它。 在此之后，应用程序会移动到前台。

可移动磁盘扫描

与**扫描计算机**类似 – 快速启动对当前连接到计算机的可移动磁盘（例如CD/DVD/USB）的扫描。这在将USB闪存盘连接到计算机并想要扫描其内容是否存在恶意软件和其他潜在威胁时非常有用。

这一类型的扫描还可以这样启动：单击**自定义扫描**，然后从**扫描目标**下拉菜单中选择**可移动磁盘**并单击**扫描**。

重复上次扫描

允许您使用运行时的相同设置快速启动之前执行的扫描。

可以从**扫描后的操作**下拉菜单中选择**无操作**、**关机**、**重新启动**或**按需重新启动**。根据您计算机电源和睡眠操作系统设备或计算机/笔记本电脑功能，可以使用**睡眠**或**休眠**操作。选定操作将在所有正在运行的扫描完成后开始。当选择了**关机**时，将显示一个 30 秒倒计时的关机确认对话窗口（单击**取消**即可停用请求的关机）。请参阅高级扫描选项以获取详细信息。

建议您每月至少运行一次计算机扫描。在**工具 > 计划任务**下，可以将扫描配置为计划任务。如何计划每周运行一次计算机扫描？

自定义扫描启动程序

如果只希望扫描特定目标，您可以使用自定义扫描工具，方法是依次单击**计算机扫描 > 自定义扫描**并从 ⚙ **> 扫描目标**下拉菜单中选择一个选项，或者从文件夹（树）结构中选择特定目标。

扫描目标窗口让您可以定义扫描哪些对象（内存、驱动器、扇区、文件和文件夹）以查找渗透。

扫描目标下拉菜单可使您选择预定义的扫描目标。

- **按配置文件设置** – 选择由选定的扫描配置文件指定的目标。
- **可移动磁盘** – 选择磁盘□USB 存储设备和 CD/DVD□
- **本地驱动器** – 选择所有系统硬盘。
- **网络驱动器** – 选择所有映射的网络驱动器。
- **自定义选择** – 取消之前所有的选择。

文件夹（树）结构还包含特定扫描目标。

- **系统内存** – 扫描当前由系统内存使用的所有进程和数据。
- **引导区/UEFI** – 扫描引导区和 UEFI 以查找是否存在恶意软件。在词汇表中阅读有关 UEFI 扫描程序的更多信息。
- **WMI 数据库** – 扫描整个 Windows Management Instrumentation (WMI) 数据库、所有命名空间、所有类实例和所有属性。搜索对被感染文件或嵌入为数据的恶意软件的引用。
- **系统注册表** – 扫描整个系统注册表、所有注册表项和子项。搜索对被感染文件或嵌入为数据的恶意软件的引用。清除检测时，引用会保留在注册表中，以确保不会丢失重要数据。

要快速导航到扫描目标，或者添加目标文件夹或文件，请在文件夹列表下方的空白字段中输入目标目录。

不自动清除被感染项目。扫描但不清除选项可以用于获取当前防护状态的概要信息。此外，还可以通过依次单击**高级设置 > 检测引擎 > 手动扫描 > ThreatSense 参数 > 清除**来从三个清除级别中进行选择。如果您仅想扫描系统而不进行附加的清除操作，请选择**扫描但不清除**。扫描历史记录会保存到扫描记录中。

当选择**忽略排除**时，带有之前从扫描中排除的扩展名的文件也将进行扫描，没有任何例外。

可以从**扫描配置文件**下拉菜单中选择要用于扫描所选目标的配置文件。默认配置文件为**智能扫描**。另外有三个预定义的扫描配置文件：名为**右键菜单扫描**、**深入扫描**和**计算机扫描**。这些扫描配置文件使用不同的 ThreatSense 参数。可用选项在**高级设置 > 检测引擎 > 恶意软件扫描 > 手动扫描 > ThreatSense 参数**中进行了介绍。

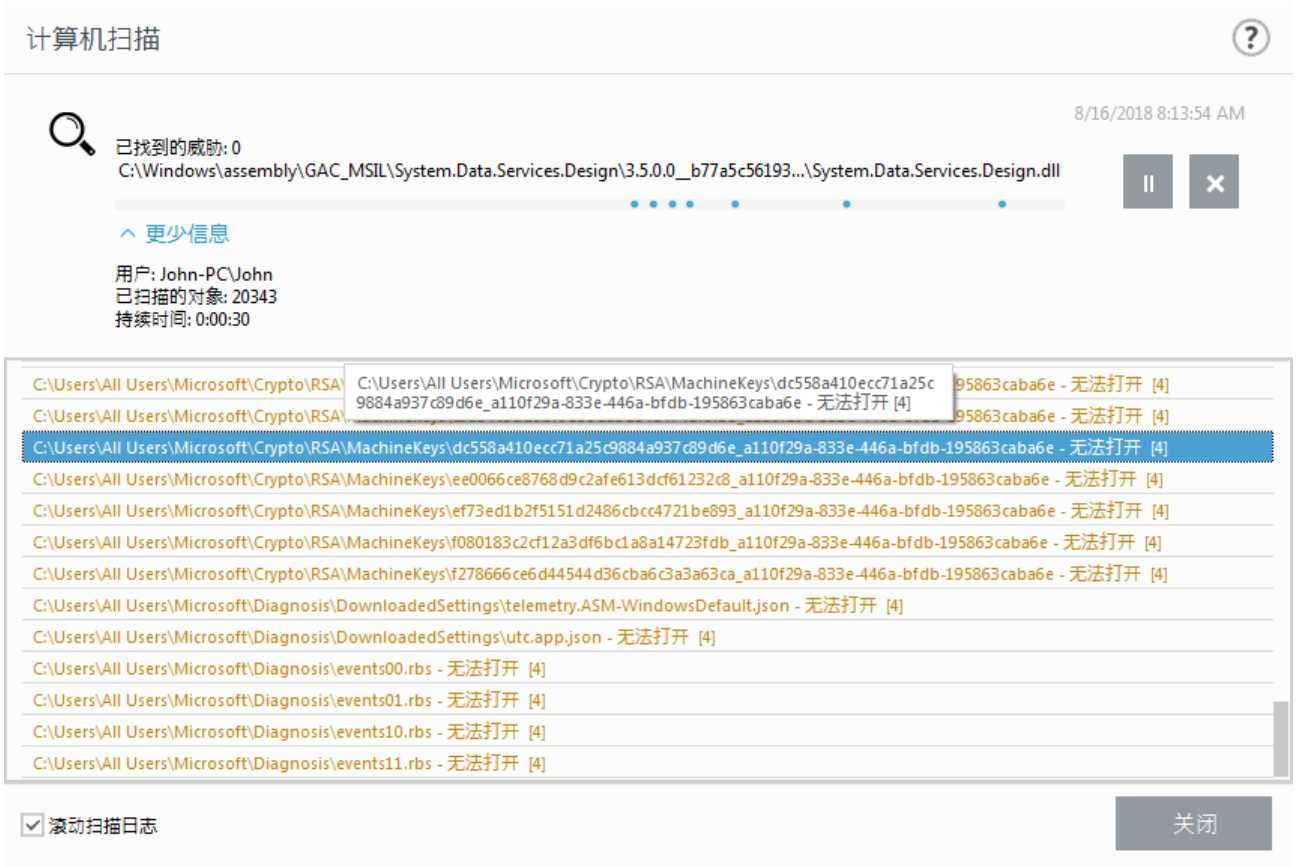
单击**扫描**以使用已设置的自定义参数执行扫描。

作为管理员扫描使您能够使用管理员帐户执行扫描。如果当前用户没有权限来访问要扫描的适当文件，则单击此选项。请注意，如果当前用户无法以管理员身份调用UAC操作，则此按钮不可用。

通过单击显示日志，您可以在扫描完成时查看计算机扫描日志。

扫描进度

扫描进度窗口显示扫描的当前状态以及有关已找到的包含恶意代码的文件数量的信息。



某些文件（比如受密码保护的文件或仅由系统使用的文件（通常为 *pagefile.sys* 和某些日志文件））无法扫描很正常。

扫描进度 – 进度条显示已扫描对象相对于待扫描对象的状态。扫描进度状态根据扫描对象总数得出。

目标 – 当前扫描的对象的名称及其位置。

已找到的威胁 – 显示在扫描过程中已找到的威胁总数。

暂停 – 暂停扫描。

继续 – 当扫描进度暂停时显示此选项。单击**继续**可继续扫描。

停止 – 终止扫描。

滚动扫描日志 – 如果已启用，扫描日志将随着新条目的添加自动向下滚动，以便显示出最新的条目。

计算机扫描日志

计算机扫描日志为您提供有关扫描的常规信息，例如：

- 扫描的日期和时间
- 已扫描的磁盘、文件夹和文件
- 已扫描的对象数
- 已找到的威胁数
- 完成时间
- 总扫描时间

恶意软件扫描

可以在“高级设置”菜单中访问**恶意软件扫描**部分。按 **F5** 键，依次单击**检测引擎 > 恶意软件扫描**，然后提供选择扫描参数的选项。本部分包括以下选项：

- **选定的配置文件** – 手动扫描程序使用的一组特定参数。

若要创建新的配置文件，请单击配置文件列表旁边的编辑。有关详细信息，请参阅扫描配置

文件。

• **手动和机器学习保护** – 请参阅检测引擎（7.2 及更高版本）。

• **扫描目标** – 如果仅希望扫描特定目标，可以单击**扫描目标**旁边的**编辑**，然后从下拉菜单中选择某个选项或从文件夹（树）结构中选择特定目标。有关详细信息，请参阅扫描目标。

• **ThreatSense** 参数 – 在此部分中，可以找到高级设置选项，例如要控制的文件扩展名、使用的检测方法等。单击以打开具有高级扫描程序选项的选项卡。

空闲状态下扫描

可以在**高级设置**（在**检测引擎 > 恶意软件扫描 > 空闲状态扫描**下）中启用空闲状态扫描程序。

空闲状态下扫描

将**启用空闲状态扫描**旁的开关设置为**开**，以启用此功能。当计算机处于空闲状态时，将在所有本地驱动器上执行静默计算机扫描。

默认情况下，当计算机（笔记本）采用电池运行时，不会运行空闲状态扫描程序。您可以通过激活“高级”设置中**计算机使用蓄电池供电时仍然运行扫描**旁边的开关来覆盖此设置。

打开高级设置中的**启用日志记录**开关，以记录日志文件部分内的计算机扫描输出（从主程序窗口依次单击**工具 > 日志文件**并从**日志**下拉菜单中选择**计算机扫描**）。

空闲状态检测

请参阅空闲状态检测触发器，以获取为触发空闲状态扫描程序必须满足的条件的完整列表。

单击 ThreatSense 引擎参数设置，以修改空闲状态扫描程序的扫描参数（例如检测方法）。

扫描配置文件

ESET Endpoint Antivirus 中有 4 个预定义的扫描配置文件：

• **智能扫描** – 这是默认的高级扫描配置文件。智能扫描配置文件使用智能优化技术，该技术会排除先前扫描中发现是干净且自该扫描以来未进行过修改的文件。这样可以缩短扫描时间，并且对系统安全性的影响最小。

• **右键菜单扫描** – 可以从右键菜单启动对任何文件的手动扫描。右键菜单扫描配置文件让您可以定义在采用此方法触发扫描时将使用的扫描配置。

• **深入扫描** – 默认情况下，全面扫描配置文件不使用智能优化，因此不会使用此配置文件排除扫描任何文件。

• **计算机扫描** – 这是标准计算机扫描中使用的默认配置文件。

可以保存您的首选扫描参数以用于将来的扫描。建议您创建不同的配置文件（带有各种扫描目标、扫描方法和其他参数）用于每次定期扫描。

要创建新配置文件，请打开“高级设置”窗口 (F5) 并依次单击**检测引擎 > 恶意软件扫描 > 手动扫描 > 配置文件列表**。**配置文件管理器**窗口包括列出现有扫描配置文件的**选定配置文件**下拉菜单以及可创建新配置文件的选项。 为了帮助您创建适合需求的扫描配置文件，请参阅ThreatSense 引擎参数设置部分，查看扫描设置中每个参数的描述。

假设要创建自己的扫描配置文件并且**扫描计算机**配置部分适用，但不希望扫描加壳程序或潜在不安全的应用程序，并且还希望应用**严格清除**。在**配置文件管理器**窗口中输入新配置文件的名称并单击**添加**。从**选定的配置文件**下拉菜单中选择新的配置文件并调整其余参数以满足要求，然后单击**确定**以保存新配置文件。

扫描目标

扫描目标窗口让您可以定义扫描哪些对象（内存、驱动器、扇区、文件和文件夹）以查找渗透。

扫描目标下拉菜单可使您选择预定义的扫描目标。

- **按配置文件设置** – 选择由选定的扫描配置文件指定的目标。
- **可移动磁盘** – 选择磁盘、USB 存储设备和 CD/DVD。
- **本地驱动器** – 选择所有系统硬盘。
- **网络驱动器** – 选择所有映射的网络驱动器。
- **自定义选择** – 取消之前所有的选择。

文件夹（树）结构还包含特定扫描目标。

- **系统内存** – 扫描当前由系统内存使用的所有进程和数据。
- **引导区/UEFI** – 扫描引导区和 UEFI 以查找是否存在恶意软件。在词汇表中阅读有关 UEFI 扫描程序的更多信息。
- **WMI 数据库** – 扫描整个 Windows Management Instrumentation (WMI) 数据库、所有命名空间、所有类实例和所有属性。搜索对被感染文件或嵌入为数据的恶意软件的引用。
- **系统注册表** – 扫描整个系统注册表、所有注册表项和子项。搜索对被感染文件或嵌入为数据的恶意软件的引用。清除检测时，引用会保留在注册表中，以确保不会丢失重要数据。

要快速导航到扫描目标，或者添加目标文件夹或文件，请在文件夹列表下方的空白字段中输入目标目录。

高级扫描选项

在此窗口中您可以为计划的计算机扫描任务指定高级选项。扫描完成后，您可以使用下拉菜单设置要自动执行的操作：

- **关机** – 扫描完成后关闭计算机。

- **重新启动** – 扫描完成后，关闭所有打开的程序并重新启动计算机。
- **需要时重新启动** – 关闭所有打开的程序，并重新启动计算机（如果扫描需要）。
- **睡眠** – 保存会话并使计算机处于低能耗状态，以便用户快速恢复工作。
- **休眠** – 获取在 RAM 上运行的所有内容并将其移动到硬盘上的特定文件。您的计算机将关闭，但在下次启动时将恢复到之前的状态。
- **无操作** – 扫描完成后，不执行任何操作。

> 请记住，睡眠中的计算机仍是一台运行中的计算机。当计算机依赖电池供电时，它仍在运行基本功能且仍在耗电。若要在办公室外移动办公时延长电池使用时间，建议您使用“休眠”选项。

选择**用户无法取消操作**，以禁止非特权用户停止扫描后执行的操作。

如果您想要允许受限用户在指定时段内暂停计算机扫描，请选择**用户可以暂停扫描(分钟)** 选项。

另请参阅扫描进度一章。

设备控制

ESET Endpoint Antivirus 提供自动设备 (CD/DVD/USB/...) 控制。此模块允许您阻止或调整扩展的过滤器/权限，并定义用户访问和使用给定设备的能力。如果计算机管理员不希望使用包含不请自来的内容的设备，此模块将很有用。

支持的外部设备：

- 磁盘存储（HDD□USB 可移动磁盘）
- CD/DVD
- USB 打印机
- FireWire 存储
- 蓝牙设备
- 智能卡读卡器
- 刻录设备
- 调制解调器
- LPT/COM 端口
- 便携式设备

- 所有设备类型

可以在**高级设置** (F5) > **设备控制**中修改设备控制设置选项。

打开**启用设备控制**旁边的开关激活 ESET Endpoint Antivirus 中的“设备控制”功能；要使此更改生效，需要重新启动计算机。启用“设备控制”后，**规则**将变为活动状态，允许您打开规则编辑器窗口。

如果插入受现有规则阻止的设备，则将显示通知窗口并且不会授予对设备的访问权限。

设备控制规则编辑器

设备控制规则编辑器窗口会显示现有规则，允许精确控制用户连接到计算机的外部设备。另请参阅添加设备控制规则

以下 ESET 知识库文章可能仅提供英文版：
- 使用 ESET 端点产品添加和修改设备控制规则

可以按照用户、用户组或规则配置中可指定的其他参数来允许或阻止特定设备。规则列表包含规则的多个说明，例如名称、外部设备类型、将外部设备连接到计算机后执行的操作以及日志严重级别。

单击**添加**或**编辑**以管理规则。取消选中规则旁边的**启用**复选框以禁用它，直到将来需要使用该规则为止。选择一个或多个规则，然后单击**删除**以将其永久删除。

复制 – 使用用于其他所选规则的预定义选项创建新规则。

单击**填充**可以为连接到计算机的设备自动填充可移动磁盘设备参数。

按优先级顺序列出规则，具有较高优先级的规则比较靠近顶端。通过单击 **最**

高/向上/向下/最低可移动规则，而且还可以单独或成组移动它们。

设备控制日志记录了所有出现的已触发的设备控制。从 ESET Endpoint Antivirus 主程序窗口的**工具 >** 日志文件可以查看日志条目。

已检测的设备

填充按钮提供了当前所有已连接设备的概述，其中包括以下信息：设备类型、设备供应商、型号以及序列号（如果有）。

如果选定某个设备（从已检测的设备列表）并且已单击**确定**，将显示具有预定义信息的规则编辑器窗口（可调整所有设置）。

设备组

⚠ 连接到计算机的设备可能会带来安全风险。

“设备组”窗口分为两个部分。该窗口右侧包含属于各个组的设备列表，而该窗口左侧包含已创建的组。通过设备列表选择要在右窗格中显示的组。

打开“设备组”窗口且选择组后，您可以从该列表添加或删除设备。另一种向组添加设备的方法是从文件导入它们。此外，还可以单击**填充**按钮，然后连接到计算机的所有设备将在**已检测的设备**窗口中列出。从已填充的列表中选择设备，然后单击**确定**以将其添加到组。

控件元素

添加 – 您可以通过输入其名称添加组或将设备添加到现有组（您可以选择指定详细信息，例如供应商名称、型号和序列号），具体取决于您在窗口哪一部分上单击了该按钮。

编辑 – 让您可以修改选定组的名称或设备的参数（供应商、型号和序列号）。

删除 – 删除选定组或设备，具体取决于您在窗口的哪一部分上单击了该按钮。

导入 – 从文本文件导入设备列表。从文本文件导入设备需要正确的格式设置：

- 每个设备都从新行开始。
- 每个设备都必须有**供应商**、**型号**和**序列号**，并使用逗号分隔。

✓ 以下是文本文件内容的示例：

```
Kingston,DT 101 G2,001CCE0DGRFC0371

04081-0009432,USB2.0 HD WebCam,20090101
```

导出 – 将设备列表导出到文件。

填充按钮提供了当前所有已连接设备的概述，其中包括以下信息：设备类型、设备供应商、型号以及序列号（如果有）。

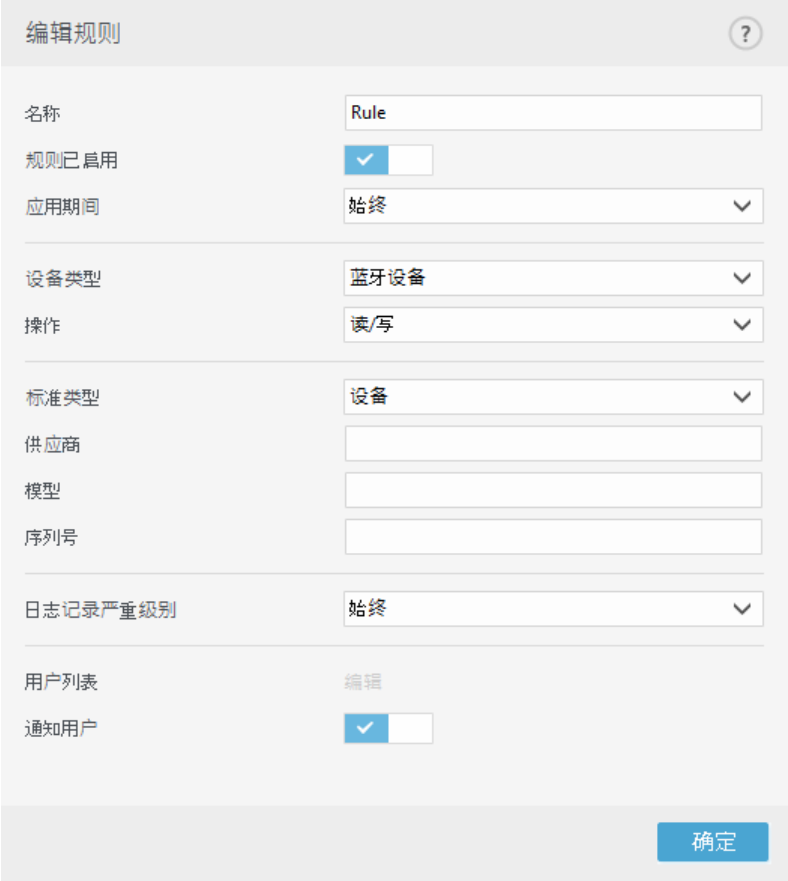
完成自定义后，单击**确定**。若要在不保存更改的情况下离开**设备组**窗口，请单击**取消**。

您可以针对应用的不同规则来创建不同的设备组。也可以针对通过**读/写**或**只读**操作所应用的规则仅创建一个设备组。这确保了在未标识的设备连接到计算机时设备控制会阻止它们。

注意，不是所有操作（权限）都可用于所有设备类型。如果是存储类型的设备，则所有四项操作均可用。对于非存储设备，只有三项操作可用（例如**只读**操作对蓝牙不可用，因此这意味着只能允许、阻止或警告蓝牙设备）。

添加设备控制规则

设备控制规则定义满足规则条件的设备连接到计算机时将采取的操作。



在**名称**字段中输入规则说明以更好识别。单击**已启用规则**旁的开关以禁用或启用此规则；如果不希望永久删除此规则，这可能会有用。

应用期间 – 允许您在一定时间内应用已创建的规则。从下拉菜单中，选择已创建的时间槽。请参阅有关时间槽的详细信息。

设备类型

从下拉菜单中选择外部设备类型（磁盘存储/便携式设备/蓝牙/FireWire/...）设备类型信息收集自操作系统，可在设备连接到计算机后在系统设备管理器中查看。存储设备包括通过 USB 或 FireWire 连接的外部磁盘或传统存储卡读卡器。智能卡读卡器包括具有嵌入式集成电路的所有智能卡读卡器，如 SIM 卡或身份验证卡。成像设备示例包括扫描仪或照相机。由于这些设备仅提供有关其操作（而非用户）的信息，因此只能全局阻止它们。

用户列表功能对于调制解调器设备类型不可用。该规则将适用于所有用户，并将删除当前用户列表。

操作

可以允许或阻止访问非存储设备。相比之下，存储设备规则允许选择以下权限设置之一：

- **读/写** – 将允许对设备的完全访问权限。
- **阻止** – 将阻止对设备的访问。
- **只读** – 仅允许对设备进行读取访问。
- **警告** – 每次连接设备时，系统都会通知用户这是否得到允许或受到阻止，并且将记录日志条目。系统不会记住设备，在以后连接同一设备时仍会显示通知。

注意，不是所有操作（权限）都可用于所有设备类型。如果是存储类型的设备，则所有四项操作均可用。对于非存储设备，只有三项操作可用（例如**只读**操作对蓝牙不可用，因此这意味着只能允许、阻止或警告蓝牙设备）。

标准类型

选择**设备组**或**设备**。

下面显示的其他参数可用于微调规则并根据设备定制。所有参数都不区分大小写：

- **供应商** – 按供应商名称或 ID 过滤。
- **型号** – 设备的给定名称。
- **序列号** – 外部设备通常具有自己的序列号。如果是 CD/DVD，这是给定介质的序列号，而不是 CD 驱动器。

如果未定义这些参数，则在匹配时规则将忽略这些字段。所有文本字段中的过滤参数都不区分大小写并且不支持通配符（*、?）。

若要查看有关设备的信息，请为此类设备创建规则、将该设备连接到计算机，然后检查设备控制日志中的设备详细信息。

日志记录严重级别

- **始终** – 记录所有事件。
- **诊断** – 记录微调程序所需的信息。
- **信息** – 记录包括成功更新消息及以上所有记录在内的信息性消息。
- **警告** – 记录严重错误和警告消息，并将它们发送到 ERA Server。

- **无** – 不记录任何日志。

可以通过将规则添加到**用户列表**，来将规则限制为特定用户或用户组：

- **添加** – 打开**对象类型：用户或组**对话框，该窗口可用来选择需要的用户。
- **删除** – 从过滤器中删除选定用户。

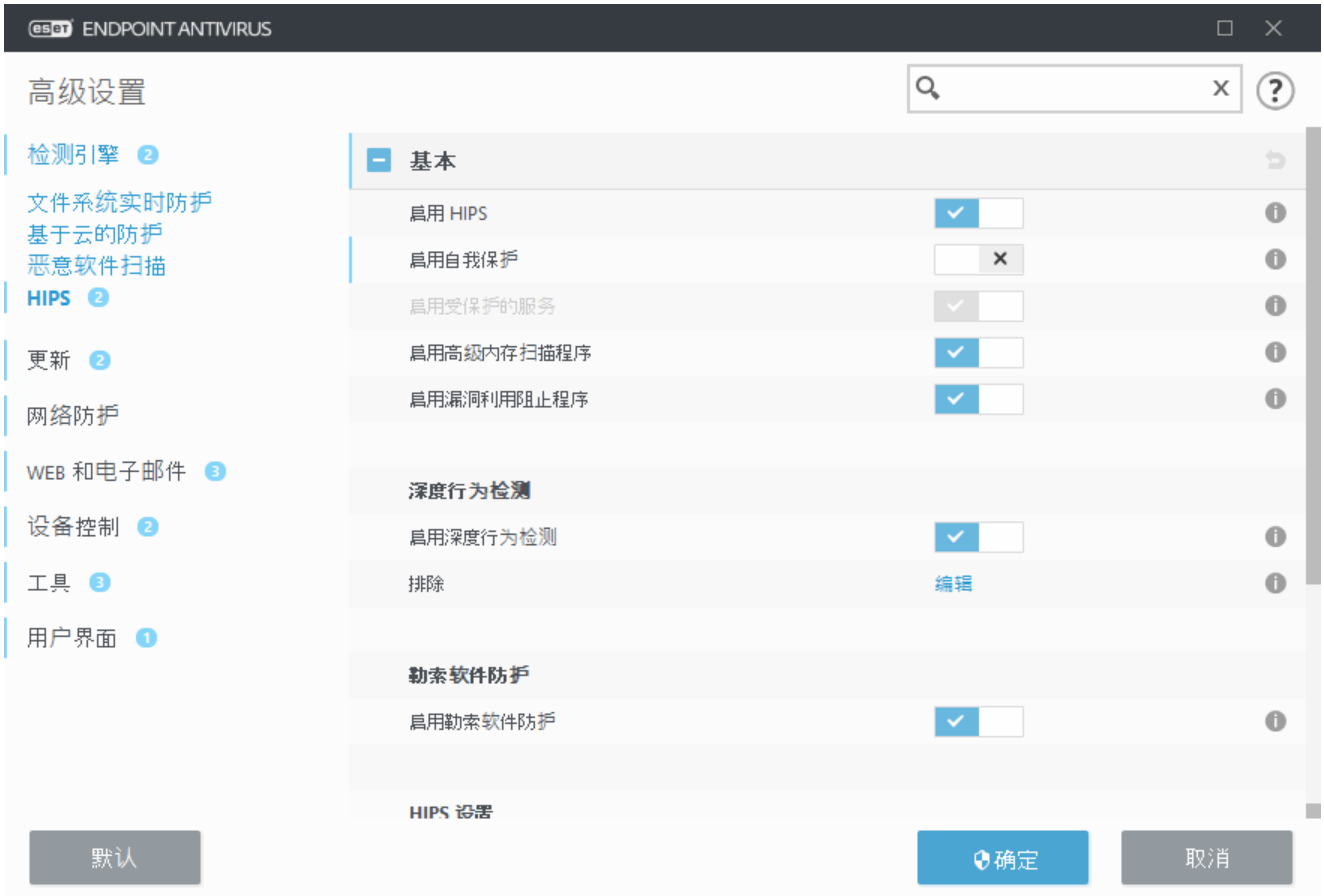
> 不是所有设备均可按用户规则进行过滤（例如，成像设备不提供用户信息，仅提供操作信息）。

基于主机的入侵预防系统 (HIPS)

> 对 HIPS 设置的更改仅应由有经验的用户进行。HIPS 设置的错误配置可能会导致系统不稳定。

基于主机的入侵防御系统 (HIPS) 可保护您的系统，以免恶意软件和任何不受欢迎的活动试图对您的计算机产生不利影响。HIPS 利用高级行为分析并配合网络过滤的检测功能来监视正在运行的进程、文件和注册表项。HIPS 独立于文件系统实时防护，并且不是防火墙；它仅监视在操作系统中运行的进程。

HIPS 设置可以在**高级设置** (F5) > **检测引擎** > **HIPS** > **基本**中找到。HIPS 状态（已启用/已禁用）显示在 ESET Endpoint Antivirus 主程序窗口中（在**设置** > **计算机**内）。



基本

启用 HIPS – 在 ESET Endpoint Antivirus 中，默认启用 HIPS。关闭 HIPS 会禁用其余 HIPS 功能（如漏洞利用阻止程序）。

启用自我防御 - ESET Endpoint Antivirus 使用内置的**自我防御**技术作为 HIPS 的一部分，来防止恶意软件损坏或禁用病毒和间谍软件防护。自我防御可保护关键系统以及 ESET 的进程、注册表项和文件免于遭篡改。ESET Management 服务器代理在安装时也受到保护。

启用受保护的服务 – 针对 ESET 服务 (ekrn.exe) 启用防护。如果启用，服务会作为受保护的 Windows 进程启动，以抵御恶意软件的攻击。此选项在 Windows 8.1 和 Windows 10 中可用。

启用高级内存扫描程序 – 与漏洞利用阻止程序结合使用以增强对恶意软件的防范，后者旨在通过迷惑或加密方法来逃过反恶意软件产品的检测。默认启用高级内存扫描程序。请阅读词汇表中有关此类防护的更多信息。

启用漏洞利用阻止程序 – 旨在强化那些经常被漏洞利用的应用程序类型，例如 Web 浏览器、PDF 阅读器、电子邮件客户端和 MS Office 组件。默认启用漏洞利用阻止程序。请阅读词汇表中有关此类防护的更多信息。

深度行为检测

启用深度行为检测 – 另一层防护，起到部分 HIPS 功能的作用。此 HIPS 的扩展会分析计算机上所有正在运行的程序的行为，并在进程的行为可疑时发出警告。

从深度行为检测的 HIPS 排除可将进程排除在分析之外。若要确保扫描所有进程以查找可能的威胁，我们建议仅在绝对必要时才创建排除。

勒索软件防护

启用勒索软件防护 – 是作为 HIPS 功能一部分工作的另一层保护。必须启用 ESET LiveGrid® 信誉系统才能使勒索软件防护工作。请阅读有关此类防护的更多信息。

启用审核模式 – 勒索软件防护检测到的所有内容不会自动进行阻止，但会以严重警告记录并发送到管理控制台（带有“AUDIT MODE”标志）。管理员可以决定排除此类检测以防止进一步检测，还是使其保持活动状态，这意味着在“审核模式”结束后，它会被阻止并删除。启用/禁用“审核模式”也会记录在 ESET Endpoint Antivirus 中。此选项仅在 ESET PROTECT 策略配置编辑器中可用。

HIPS 设置

可以使用以下模式之一执行**过滤模式**：

过滤模式	说明
自动模式	启用操作（除了保护系统的预定义规则所阻止的操作）。

过滤模式	说明
智能模式	仅通知用户极为可疑的事件。
交互模式	将提示用户确认操作。
基于策略的模式	阻止所有未由允许它们的特定规则定义的操作。
学习模式	启用操作，并在每次操作后创建规则。可在 **HIPS 规则**编辑器中查看在此模式下创建的规则，但其优先级低于手动创建的规则或在自动模式下创建的规则的优先级。当从**过滤模式**下拉菜单中选择**学习模式**后，**学习模式结束时间**设置将变为可用。选择要采用学习模式的时间范围，最长持续时间为 14 天。当指定的持续时间超过后，将会提示您编辑由 HIPS 在学习模式下所创建的规则。还可以选择其他过滤模式，或推迟决定并继续使用学习模式。

学习模式到期之后设置的模式 – 在学习模式到期后选择将使用的过滤模式。过期后，**询问用户**选项需要管理权限来执行对 HIPS 过滤模式的更改。

HIPS 系统监控操作系统内的事件，并根据规则（类似于防火墙使用的规则）相应地对事件作出反应。单击**规则**旁边的**编辑**以打开 **HIPS 规则**编辑器。在 HIPS 规则窗口中，可以选择、添加、编辑或删除规则。有关规则创建和 HIPS 操作的更多信息，可以在编辑 HIPS 规则中找到。

HIPS 交互窗口

HIPS 通知窗口允许您根据 HIPS 检测到的新操作创建规则，然后定义允许或拒绝该操作的条件。

创建自通知窗口的规则视为等同于手动创建的规则。创建自通知窗口的规则可能不如触发该对话框窗口的规则具体。这意味着，在对话框中创建某个规则后，相同的操作可以触发相同的窗口。有关详细信息，请参阅 HIPS 规则的优先级。

如果某个规则的默认操作设置为**每次询问**，则每次触发该规则时将显示对话窗口。可以选择**拒绝**或**允许**操作。如果在给定时间不选择操作，将基于规则选择新操作。

在应用程序退出之前记住操作将使系统在规则或过滤模式发生更改、HIPS 模块更新或系统重新启动之前始终使用此操作（**允许/拒绝**）。 发生这三项操作中的任意一项后，将删除临时规则。

创建规则并永久记住选项将创建一个新 HIPS 规则，该规则稍后可在 HIPS 规则管理部分中进行更改（需要管理权限）。

单击底部的**详细信息**可查看应用程序触发操作的内容，文件的信誉或者要求允许或拒绝的操作类型。

单击**高级选项**，可以访问更详细规则参数的设置。如果选择**创建规则并永久记住**，则以下选项可用：

- **创建仅对此应用程序有效的规则** – 如果取消选中此复选框，则将为所有源应用程序创建规则。
- **仅适用于操作** – 选择规则文件/应用程序/注册表操作。请参阅所有 HIPS 操作的说明。

- **仅适用于目标** – 选择规则文件/应用程序/注册表目标。

若要停止显示通知，请将过滤模式更改为**自动模式**（在**高级设置** (F5) > **检测引擎** > **HIPS** > **基本**中）。

检测到潜在的勒索软件行为

当检测到潜在的勒索软件行为时，将显示此交互窗口。 您可以选择**拒绝**或**允许**操作。

单击**详细信息**可查看特定检测参数。对话窗口允许您**提交以供分析**或**从检测中排除**。

必须启用 ESET LiveGrid®才能使勒索软件防护正常工作。

HIPS 规则管理

这是在 HIPS 系统中用户定义和自动添加的规则列表。可以在 HIPS 规则设置章节中找到有关规则创建和 HIPS 操作的更多详细信息。另请参阅 HIPS 的一般原则。

列

规则 – 用户定义的或自动选择的规则名称。

已启用 – 如果要将规则保留在列表中但不想使用，可停用此选项。

操作 – 该规则指定满足条件的情况下应执行的一项操作：**允许**、**阻止**或**询问**。

源 – 仅当事件由应用程序触发时才使用该规则。

目标 – 仅当操作与特定文件、应用程序或注册表项相关时才使用该规则。

日志记录严重级别 – 如果激活此选项，则有关此规则的信息将写入到 HIPS 日志中。

通知 – 如果触发事件，则在右下角显示一个小的弹出通知。

控件元素

添加 – 创建一个新规则。

编辑 – 使您能够编辑选定的条目。

删除 – 删除选定条目。

HIPS 规则的优先级

没有使用“上/下”按钮调整 HIPS 规则的优先级的选项。.

- 创建的所有规则具有相同的优先级
- 规则越具体，优先级越高（例如，特定应用程序的规则的优先级高于所有应用程序的规则）
- 在内部HIPS 包含有您无法访问的较高优先级规则（例如，无法覆盖自我保护定义的规则）
- 您创建的可能会冻结操作系统的规则将不会应用（具有最低优先级）

HIPS 规则设置

请先参阅 HIPS 规则管理

规则名称 – 用户定义的或自动选择的规则名称。

操作 – 指定满足条件的情况下应执行的一项操作：允许、阻止或询问。

操作影响 – 您必须选择将要应用该规则的操作的类型。该规则将仅用于此类型的操作和选定的目标。

已启用 – 如果要将规则保留在列表中但不应用，可禁用此开关。

日志记录严重级别 – 如果激活此选项，则有关此规则的信息将写入到 HIPS 日志中。

通知用户 – 如果事件已触发，在右下角将显示一个小的弹出窗口。

该规则包含以下部分，它们描述了触发使用此规则的条件：

源应用程序 – 仅当事件由此应用程序触发时才使用该规则。从下拉菜单中选择**特定应用程序**，并单击**添加**以添加新文件，或者可以从下拉菜单中选择**所有应用程序**以添加所有应用程序。

目标文件 – 仅当操作与此目标相关时才使用该规则。从下拉菜单中选择**特定文件**，然后单击**添加**

以添加新文件或文件夹，或者可以从下拉菜单中选择**所有文件**以添加所有文件。

应用程序 – 仅当操作与此目标相关时才使用该规则。从下拉菜单中选择**特定应用程序**，并单击**添加**以添加新文件或文件夹，或者可以从下拉菜单中选择**所有应用程序**以添加所有应用程序。

注册表条目 – 仅当操作与此目标相关时才使用该规则。从下拉菜单中选择**特定条目**，并单击**添加**以添加新文件或文件夹，或者可以从下拉菜单中选择**所有条目**以添加所有应用程序。

无法阻止 HIPS 预定义特定规则的一些操作，默认为允许这些操作。此外，HIPS 并不监视所有系统操作，HIPS 监视视为不安全的操作。

指定路径时，C:\example 会影响与文件夹本身有关的操作，并且 C:\example*.* 会影响文件夹中的文件。

应用程序操作

- **调试其他应用程序** – 将调试程序附加到进程。调试应用程序时，可以查看和修改其行为的许多详细信息，并访问其数据。
- **拦截其他应用程序的事件** – 源应用程序尝试捕获针对特定应用程序的事件（例如尝试捕获浏览器事件的按键记录程序）。
- **终止/暂停其他应用程序** – 暂停、恢复或中止进程（可以直接从进程浏览器或进程窗格访问）。
- **启动新应用程序** – 启动新应用程序或进程。
- **修改其他应用程序的状态** – 源应用程序尝试写入目标应用程序内存或运行自己的代码。此功能在阻止此操作使用的规则中将其配置为目标应用程序，从而保护重要应用程序。

无法拦截 64 位版本 Windows XP/Vista 上的进程操作。

注册表操作

- **修改启动设置** – 定义哪些应用程序在 Windows 启动时运行的设置的任何更改。例如，可通过在 Windows 注册表中搜索 Run 键来找到这些信息。
- **从注册表删除** – 删除注册表项或其值。
- **重命名注册表项** – 重命名注册表项。
- **修改注册表** – 创建注册表项的新值、更改现有值、在数据库树中移动数据，或设置用户或组对注册表项的权限。

在规则中使用通配符
规则中的星号只能用于替换特定键，例如“HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet*\Start”□其他使用通配符的方法不受支持。
创建以“HKEY_CURRENT_USER”键为目标的规则
此键只是指向特定于由 SID□安全标识符）标识用户的 HKEY_USERS 相应字键的链接。若要仅为当前用户创建规则，请使用指向 HKEY_USERS\%SID% 的路径，而不是使用 HKEY_CURRENT_USER 的路径。作为 SID□您可以使用星号来使规则适用于所有用户。

如果创建了太笼统的规则，将会显示关于此类规则的警告。

在以下示例中，我们将演示如何限制不需要的特定应用程序行为：

1.命名规则，并从**操作**下拉菜单中选择**阻止**（或**询问**，如果想要稍后选择）。
2.打开**通知用户**开关以在每次应用规则时显示通知。
3.在**操作影响**部分中，为将应用的规则选择至少一项操作□
4.单击**下一步**□
5.在**源应用程序**窗口中，从下拉菜单中选择**特定应用程序**，以将新规则应用于尝试在指定的应用程序上执行任何选定的应用程序操作的所有应用程序。
6.单击**添加**，单击 **...** 以选择特定应用程序的路径，然后按**确定**。添加更多应用程序（如果需要）。
例如： *C:\Program Files (x86)\Untrusted application\application.exe*
7.选择**写入文件**操作。
8.从下拉菜单中选择**所有文件**。这将阻止上一步中选定应用程序写入任何文件的任何尝试。
9.单击**完成**保存新规则。

HIPS 高级设置

以下选项用于调试和分析应用程序的行为：

始终允许加载驱动程序 – 始终允许加载选定的驱动程序，而不管配置的过滤模式是什么，除非明确地通过用户规则阻止。

记录所有被阻止的操作 – 所有被阻止的操作都会写入到 HIPS 日志中。仅在故障排除或 ESET 技术支持要求时才使用此功能，因为它可能会生成一个较大的日志文件并会降低计算机的运行速度。

当启动应用程序发生更改时发送通知 – 每次应用程序添加到系统启动或从中删除时显示桌面通知。

始终允许加载驱动程序

始终允许加载此列表中显示的驱动程序，而不管 HIPS 过滤模式是什么，除非明确地通过用户规则阻止。

添加 – 添加新驱动程序。

编辑 – 编辑选定的驱动程序。

删除 – 从列表中删除驱动程序。

重置 – 重新加载一组系统驱动程序。

> 如果您不希望包含已手动添加的驱动程序，请单击**重置**。如果您已添加多个驱动程序并且无法手动将它们从列表中删除，这将会很有用。

演示模式

演示模式是为那些需要不中断其使用软件、不希望被弹出窗口打扰，并希望尽量减少 CPU 使用的用户提供的功能。演示模式还可以用于不能被病毒防护活动中断的演示。启用时，将禁用所有弹出窗口，并且不会运行计划任务。系统保护仍在后台运行，但是不需要任何用户交互。

依次单击**设置 > 计算机**，然后单击**演示模式旁边的开关，以手动启用演示模式。**在**高级设置** (F5) 中，依次单击**工具 > 演示模式**，然后单击**全屏模式运行应用程序时自动启用演示模式旁边的开关，以在运行全屏应用程序时使 ESET Endpoint Antivirus 自动处于演示模式**。启用演示模式将存在潜在安全风险，因此任务栏上的防护状态将变成橙色，并显示警告。您还将在主程序窗口中看到此警告，其中您将看到橙色的**已启用演示模式**。

执行以全屏模式运行应用程序时自动启用演示模式时，将在启动全屏应用程序后启动演示模式，并在退出该应用程序后自动停止。这对于在启动游戏、打开全屏应用程序或开始播放演示文稿后立即启动演示模式尤为有用。

您还可以选择**自动禁用演示模式时间**，以定义将在多久后（以分钟为单位）自动禁用演示模式。

开机扫描

在默认情况下，自动启动文件检查将在系统启动时和模块更新期间执行。此扫描取决于计划任务配置和任务。

启动扫描选项是**系统启动文件检查**计划任务的一部分。要修改启动扫描设置，导航至**工具>计划任务**，单击**自动启动文件检查**，然后单击**编辑**。在最后一步中，自动启动文件检查窗口将显示（参见下一章了解更多详细信息）。

有关计划任务创建和管理的详细说明，请参见创建新任务。

自动启动文件检查

在创建系统启动文件检查计划任务时，有几个选项可用于调整以下参数：

扫描目标下拉菜单基于保密的复杂算法指定在系统启动时运行的文件的扫描深度。文件按照以下标准以降序排列：

- **所有注册文件**（扫描文件最多）
- **很少使用的文件**
- **通常使用的文件**
- **常用文件**
- **仅最常用文件**（扫描文件最少）

还包括两个特定组：

- **用户登录前运行的文件** – 包含未经用户登录即可访问的位置的文件（包括几乎所有启动位置，如服务、浏览器帮助程序对象、winlogon 通知、Windows 计划任务条目、已知 dll 等）。
- **用户登录后运行的文件** – 包含仅在用户登录后才可访问的位置的文件（包括仅由特定用户运行的文件，通常是 *HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run* 中的文件）。

上述每个组的要扫描文件列表是固定的。

扫描优先级 – 用于确定何时开始扫描的优先级别：

- **空闲时** – 仅在系统空闲时执行任务，
- **最低** – 在系统负载最低时，
- **较低** – 低系统负载，
- **正常** – 平均系统负载。

文档防护

文档防护功能会在打开 Microsoft Office 文档之前对其进行扫描，还会扫描通过 Internet Explorer 自动下载的文件，如 Microsoft ActiveX 元素。 文档防护提供文件系统实时防护之外的另一层防护，可以将其禁用以在无法处理大量 Microsoft Office 文档的系统上增强性能。

要激活文档防护，请打开**高级设置**窗口（按 **F5** > **检测引擎** > **恶意软件扫描** > **文档防护**，然后单击**启用文档防护**开关。

此功能由使用 Microsoft Antivirus API（例如 Microsoft Office 2000 及更高版本或 Microsoft Internet Explorer 5.0 及更高版本）的应用程序激活。

排除

排除让您可以将对象排除在检测引擎之外。要确保对所有对象进行扫描，建议您只在绝对有必要时才创建排除。需要排除某个对象的情况可能包括：在扫描期间会使计算机速度变慢的大型数据库条目扫描，或遇到与扫描冲突的软件。

性能排除允许您排除扫描文件和文件夹。性能排除对于排除游戏应用程序的文件级扫描、在导致出现异常系统行为时或性能提高很有用。

检测排除允许您使用检测名称、路径或其哈希排除清除对象。检测排除不会像性能排除那样排除扫描文件和文件夹。检测排除仅在检测引擎检测到对象并且排除列表中存在合适规则时才会排除对象。

版本 7.1 及更低版本中的排除会将性能排除和检测排除合并到一起。

请勿与其他类型的排除混淆：

- 进程排除 – 归因于排除的应用程序进程的所有文件操作都会被排除扫描（可能需要提高备份速度和服务可用性）。
- 排除的文件扩展名
- HIPS 排除
- 基于云的防护的排除过滤器

性能排除

性能排除允许您排除扫描文件和文件夹。

要确保对所有对象进行威胁扫描，建议您仅在绝对有必要时才创建排除。然而，在某些情况下，可能需要排除某个对象，例如，在扫描期间会使计算机速度变慢的大型数据库条目，或与扫描冲突的软件。

可以通过**高级设置 (F5) > 检测引擎 > 排除 > 性能排除 > 编辑**，以将要排除扫描的文件和文件夹添加到排除列表。

要排除扫描某个对象（路径：文件或文件夹），请单击**添加**并输入应用程序路径或在树结构中选择它。

如果某个文件满足不进行扫描的条件，那么**文件系统实时防护**模块或**计算机扫描**模块将不会检测到该文件内的威胁。

控件元素

- **添加** – 添加一个新条目以从扫描中排除对象。
- **编辑** – 使您能够编辑选定的条目。
- **删除** – 删除选定条目（CTRL + 单击可选择多个条目）。
- **导入/导出** – 当需要备份当前排除以备日后使用时，性能排除的导入和导出功能十分有用。对于未托管环境中要在多个系统上使用其首选配置的用户，导出设置选项也很便利，因为他们可以方便地导入 .txt 文件来传输这些设置。

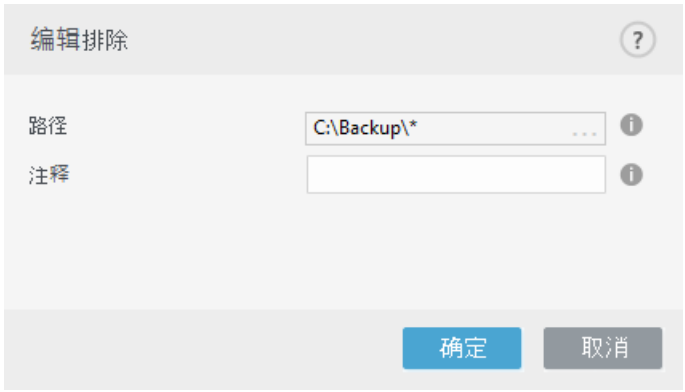
显示导入/导出文件格式的示例

```
# {"product":"endpoint","version":"7.2.2055","path":"plugins.01000600.settings.PerformanceExclusions","columns":["Path","Description"]}
C:\Backup\*,custom comment
C:\pagefile.sys
```

添加或编辑性能排除

此对话框窗口不包括此计算机的特定路径（文件或目录）。

要选择合适的路径，请在**路径**字段中单击 **...**。
手动输入时，请参阅下面的排除格式示例了解更多信息。



可使用通配符排除一组文件。问号（*?*）代表单个字符，星号（*）则代表包含零个或更多字符的字符串。

- 如果要排除文件夹中的所有文件和子文件夹，则键入文件夹的路径并使用掩码 *
- 如果要仅排除 doc 文件，则使用掩码 **.doc*
- 如果可执行文件名有特定数量的字符（字符各异）并且您只知道第一个字符（如“D”□□则使用以下格式：
D????.exe（问号将替换缺少/未知的字符）

示例：

- *C:\Tools** – 该路径必须以反斜杠 (\) 和星号 (*) 结尾，以指示它是将要排除的文件夹及所有文件夹内容（文件和子文件夹）。
- *C:\Tools*.** – 与 *C:\Tools** 相同的行为
- *C:\Tools - Tools* 文件夹将不会被排除。从扫描程序的角度来看，*Tools* 也可能是一个文件名。
- *C:\Tools*.dat* – 将排除 *Tools* 文件夹中的 .dat 文件。
- *C:\Tools\sg.dat* – 将排除位于确切路径中的此特定文件。

您可以使用类似 *%PROGRAMFILES%* 的系统变量来定义扫描排除。

- 在添加到排除时，要使用此系统变量排除 Program Files 文件夹，请使用路径 *%PROGRAMFILES%**（记住在路径末尾添加反斜杠和星号）。
- 要排除 *%PROGRAMFILES%* 子目录中的所有文件和文件夹，请使用路径 *%PROGRAMFILES%\Excluded_Directory**

展开受支持系统变量的列表

在路径排除格式中可以使用以下变量：

- *%ALLUSERSPROFILE%*
- *%COMMONPROGRAMFILES%*
- *%COMMONPROGRAMFILES(X86)%*
- *%COMSPEC%*
- *%PROGRAMFILES%*
- *%PROGRAMFILES(X86)%*
- *%SystemDrive%*
- *%SystemRoot%*
- *%WINDIR%*
- *%PUBLIC%*

用户特定的系统变量（例如 *%TEMP%* 或 *%USERPROFILE%*）或环境变量（如 *%PATH%*）不受支持。

在路径中间使用通配符（例如，*C:\Tools*\Data\file.dat*）可能起作用，但为了性能排除而不正式支持。有关详细信息，请参阅以下知识库文章。
当使用检测排除时，不限制在路径中间使用通配符。

排除顺序：
- 没有使用“上/下”按钮调整排除优先级的选项.
- 当第一个适用的规则被扫描程序匹配时，不会评估第二个适用的规则。
- 规则越少，扫描性能越好。
- 避免创建并发规则。

路径排除格式

可使用通配符排除一组文件。问号（*?*）代表单个字符，星号（*）则代表包含零个或更多字符的字符串。

- 如果要排除文件夹中的所有文件和子文件夹，则键入文件夹的路径并使用掩码 *
- 如果要仅排除 doc 文件，则使用掩码 **.doc*
- 如果可执行文件名有特定数量的字符（字符各异）并且您只知道第一个字符（如“D”），则使用以下格式：
D????.exe（问号将替换缺少/未知的字符）

示例：
- *C:\Tools** – 该路径必须以反斜杠 (\) 和星号 (*) 结尾，以指示它是将要排除的文件夹及所有文件夹内容（文件和子文件夹）。
- *C:\Tools*.** – 与 *C:\Tools** 相同的行为
- *C:\Tools - Tools* 文件夹将不会被排除。从扫描程序的角度来看，*Tools* 也可能是一个文件名。
- *C:\Tools*.dat* – 将排除 *Tools* 文件夹中的 .dat 文件。
- *C:\Tools\sg.dat* – 将排除位于确切路径中的此特定文件。

您可以使用类似 *%PROGRAMFILES%* 的系统变量来定义扫描排除。
- 在添加到排除时，要使用此系统变量排除 Program Files 文件夹，请使用路径 *%PROGRAMFILES%**（记住在路径末尾添加反斜杠和星号）。
- 要排除 *%PROGRAMFILES%* 子目录中的所有文件和文件夹，请使用路径 *%PROGRAMFILES%\Excluded_Directory**

展开受支持系统变量的列表

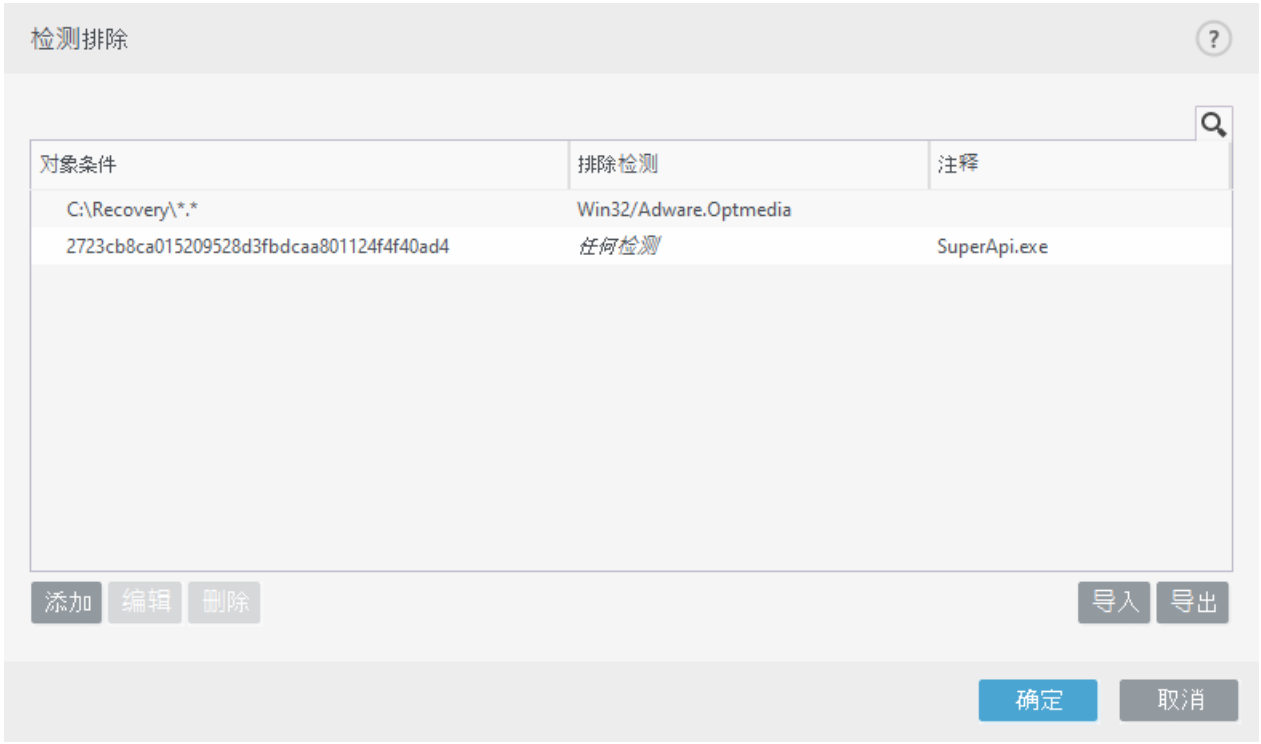
在路径排除格式中可以使用以下变量：
- *%ALLUSERSPROFILE%*
- *%COMMONPROGRAMFILES%*
- *%COMMONPROGRAMFILES(X86)%*
- *%COMSPEC%*
- *%PROGRAMFILES%*
- *%PROGRAMFILES(X86)%*
- *%SystemDrive%*
- *%SystemRoot%*
- *%WINDIR%*
- *%PUBLIC%*

用户特定的系统变量（例如 *%TEMP%* 或 *%USERPROFILE%*）或环境变量（如 *%PATH%*）不受支持。

检测排除

检测排除允许您通过过滤检测名称、对象路径或其哈希，来排除清除对象。

检测排除不会像性能排除那样排除扫描文件和文件夹。检测排除仅在检测引擎检测到对象并且排除列表中存在合适规则时才会排除对象。
例如（参见下图中的第一行），当某个对象检测为 Win32/Adware.Optmedia 并且检测到文件为 *C:\Recovery\file.exe* 时。在第二行上，尽管有检测名称，但具有合适 SHA-1 哈希的每个文件将始终被排除。



要确保检测到所有威胁，建议您仅在绝对必要时才创建检测排除。

要将文件和文件夹添加到排除列表，请依次转到**高级设置 (F5) > 检测引擎 > 排除 > 检测排除 > 编辑**。

要从清除中排除对象（按其检测名称或哈希），请单击**添加**。

对于潜在不受欢迎的应用程序和潜在不安全的应用程序，还可以按其检测名称创建排除：

- 在报告检测的警报窗口中（单击**显示高级选项**，然后选择**从检测中排除**）。
- 从“日志文件”上下文菜单，使用创建检测排除向导。
- 方法是依次单击**工具 > 隔离**，然后右键单击隔离文件并从右键菜单中选择**恢复并从扫描中排除**来创建。

检测排除对象标准

- **路径** – 对指定路径（或任何路径）限制检测排除。

- **检测名称** – 如果已排除文件旁边有一个检测的名称，则表示该文件仅对给定检测排除，并不是全部排除。如果该文件稍后被其他恶意软件感染，则会检测到该文件。
- **哈希** – 基于指定的哈希排除某个文件 SHA-1，不管文件类型、位置、名称或其扩展名如何。

控件元素

- **添加** – 添加一个新条目以从清除中排除对象。
- **编辑** – 使您能够编辑选定的条目。
- **删除** – 删除选定条目（CTRL + 单击可选择多个条目）。
- **导入/导出** – 当需要备份当前排除以备日后使用时，检测排除的导入和导出功能十分有用。对于未托管环境中要在多个系统上使用其首选配置的用户，导出设置选项也很便利，因为他们可以方便地导入 .txt 文件来传输这些设置。

显示导入/导出文件格式的示例

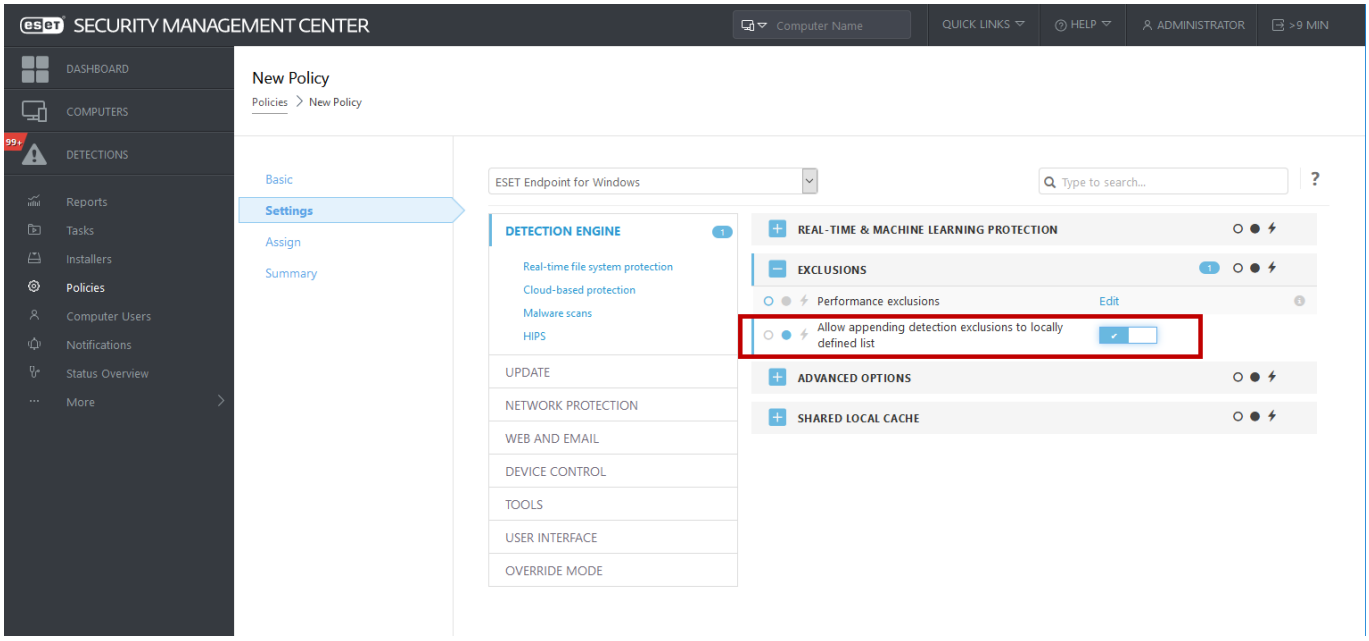
```
# {"product":"endpoint","version":"7.2.2055","path":"Settings.ExclusionsManagement.DetectionExclusions","columns":["Id","Path","ThreatName","Description","FileHash"]}
4c59cd02-357c-4b20-a0ac-ca8400000001,,,SuperApi.exe,00117F70C86ADB0F979021391A8AEAA497C2C8DF
2c362ac8-a630-496e-9665-c76d00000001,C:\Recovery\*.*,Win32/Adware.Optmedia,
```

ESET PROTECT 中的检测排除设置

ESET PROTECT 8.0 包括检测排除管理的新向导 – 创建检测排除并将其应用到更多计算机/组。

可以从 ESET PROTECT 覆盖检测排除

当存在检测排除本地列表时，管理员必须应用**允许附加检测排除到本地定义的列表**策略。之后，从 ESET PROTECT 附加检测排除将按预期工作。

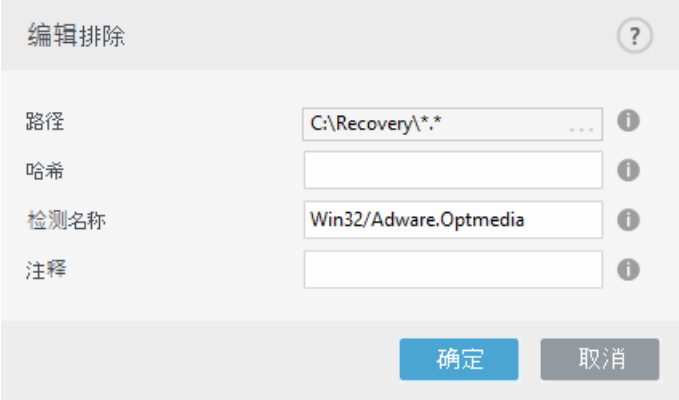


添加或编辑检测排除

排除检测

应提供有效的 ESET 检测名称。要查找有效的检测名称，请参见日志文件，然后从日志文件下拉菜单中选择**检测**。当在 ESET Endpoint Antivirus 中检测到误报样本时，这将很有用。对真正渗透的排除是非常危险的，考虑通过单击**路径掩码**中的 **...** 仅排除受影响的文件/目录，并/或在临时时期进行排除。排除还应用于潜在不受欢迎的应用程序、潜在不安全的应用程序和可疑应用程序。

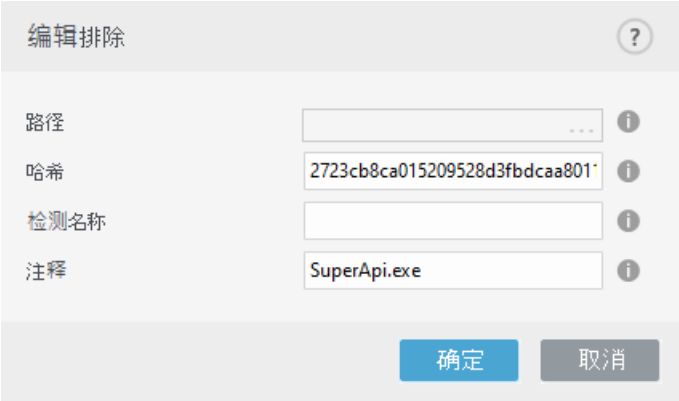
另请参阅路径排除格式



请参阅以下检测排除示例

排除哈希

基于指定的哈希排除某个文件 SHA-1，不管文件类型、位置、名称或其扩展名如何。



要按检测名称排除特定检测，请输入有效的检测名称：
Win32/Adware.Optmedia
当您从 ESET Endpoint Antivirus 警报窗口排除检测时，也可以使用以下格式：
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

控件元素

- **添加** – 选择不予检测的对象。
- **编辑** – 使您能够编辑选定的条目。
- **删除** – 删除选定条目（CTRL + 单击可选择多个条目）。

创建检测排除向导

还可以从日志文件上下文菜单创建检测排除（不适用于恶意软件检测）：

1. 在主程序窗口中，依次单击**工具 > 日志文件**。
2. 右键单击**检测日志**中的某个检测。
3. 单击**创建排除**。

要根据**排除标准**排除一个或多个检测，请单击**更改标准**。

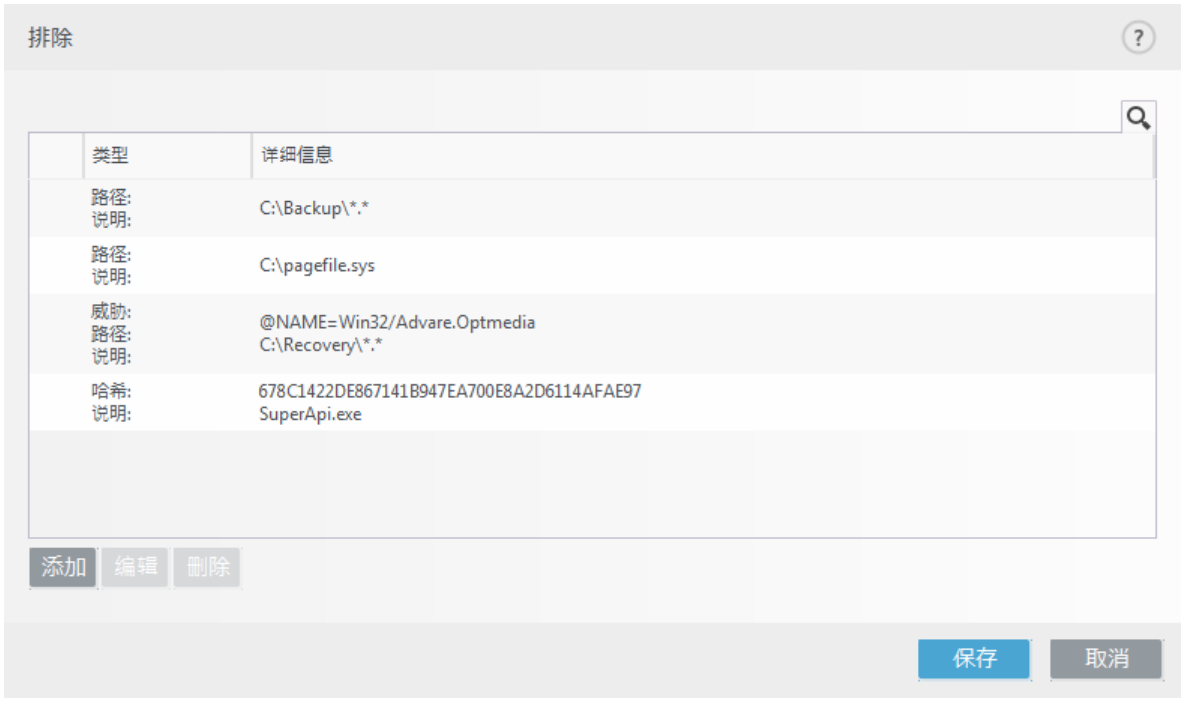
- **精确文件** – 按 SHA-1 哈希排除每个文件。
- **检测** – 按检测名称排除每个文件。
- **路径+检测** – 按检测名称和路径排除每个文件，包括文件名（例如，*file:///C:/Users/user/AppData/Local/Temp/34e1824e/ggdsfdgfd.pdf.exe*）。

建议选项是根据检测类型而预先选择的。

可以选择添加**注释**，然后再单击**创建排除**。

排除（7.1 及更低版本）

在版本 7.1 及更低版本中的排除会将性能排除和检测排除合并到一起。



进程排除

进程排除功能允许您从文件系统实时防护排除应用程序进程。为了改进备份速度、进程完整性和服务可用性，在备份时使用了已知与文件级恶意软件防护相冲突的某些技术。当试图实时迁移虚拟机时，可能发生相似的问题。避免这两种情况的唯一有效方法是停用恶意软件防护软件。通过排除特定进程（例如，备份解决方案的进程），属于此类排除进程的所有文件操作都将被忽略并认为安全，这样可以最大限度地减少对备份进程的干扰。我们建议您在创建排除时小心谨慎 – 已排除的备份工具可以访问被感染的文件而不会触发警报，这就是为什么仅在实时防护模块中允许扩展权限的原因。

进程排除帮助最大程度地减少潜在冲突的风险，并提高已排除应用程序的性能，从而对操作系统的整体性能和稳定性带来正面影响。进程/应用程序的排除是其可执行文件（*.exe*）的排除。

可以通过**高级设置 (F5) > 检测引擎 > 文件系统实时防护 > 进程排除**，将可执行文件添加到排除进程列表中。

此功能旨在排除备份工具。从扫描中排除备份工具的进程不仅可以确保系统稳定性，而且还不会影响备份性能，因为备份在运行时不会减慢速度。

单击**编辑**以打开**进程排除**管理窗口，可以在其中添加排除并浏览至将从扫描中排除的可执行文件（例如 *Backup-tool.exe*）。
在将 *.exe* 文件添加到排除中后，ESET Endpoint Antivirus 不会监控此进程的活动，也不会对此进程执行的任何文件操作进行扫描。

如果在选择进程可执行文件时不使用浏览功能，则需要手动输入可执行文件的完整路径。否则，排除将无法正常工作，并且 HIPS 可能会报告错误。

还可以在排除中**编辑**现有进程或**删除**它们。

Web 访问保护不考虑此排除，因此如果排除 Web 浏览器的可执行文件，仍将会扫描下载的文件。采用这种方法，仍会检测到渗透。此方案仅为示例，我们不建议您为 Web 浏览器创建排除。

添加或编辑进程排除

此对话窗口使您能够**添加**从检测引擎中排除的进程。进程排除帮助最大程度地减少潜在冲突的风险，并提高已排除应用程序的性能，从而对操作系统的整体性能和稳定性带来正面影响。进程/应用程序的排除是其可执行文件（*.exe*）的排除。

通过单击 ...，选择例外应用程序的文件路径（例如 *C:\Program Files\Firefox\Firefox.exe*）。请勿输入应用程序的名称。
在将 *.exe* 文件添加到排除中后，ESET Endpoint Antivirus 不会监控此进程的活动，也不会对此进程执行的任何文件操作进行扫描。

如果在选择进程可执行文件时不使用浏览功能，则需要手动输入可执行文件的完整路径。否则，排除将无法正常工作，并且 HIPS 可能会报告错误。

还可以在排除中**编辑**现有进程或**删除**它们。

HIPS 排除

排除使您能够从 HIPS 深度行为检测排除进程。

要排除某个对象，请单击**添加**并输入对象的路径或在树结构中选择它。也可以**编辑**或**删除**选定的条目。

请参阅排除章节。

ThreatSense 参数

ThreatSense 包括许多复杂的威胁检测方法。 此技术具有某种主动性防护功能，也就是说，它可在新威胁开始传播的较早阶段提供防护。 该技术采用代码分析、代码仿真、一般的识别码、病毒库的组合，以显著提高系统安全性。 扫描引擎可同时控制多个数据流，最大限度地提高效率和检测速度。ThreatSense 技术还可成功消除 Rootkit。

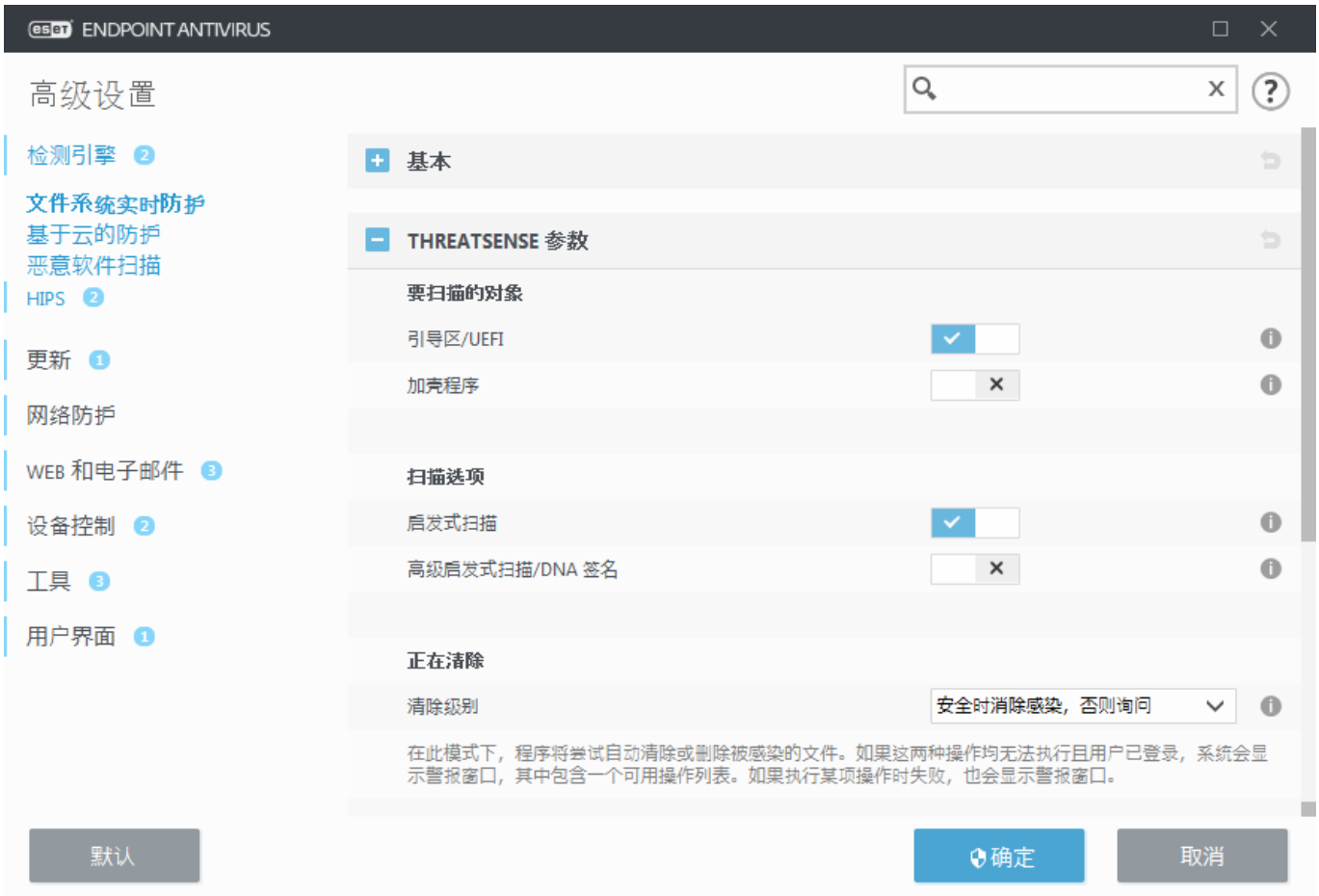
ThreatSense 引擎设置选项允许您指定若干扫描参数：

- 要扫描的文件类型和扩展名
- 不同检测方法的组合
- 清除级别等

要进入设置窗口，请单击 **ThreatSense 参数**，它位于使用 ThreatSense 技术的任何模块的“高

级设置”窗口中（请参见下文）。 不同的安全情形可能要求不同的配置。 考虑到这一点，可针对下列防护模块对 ThreatSense 进行单独配置：

- 文件系统实时防护
- 空闲状态下扫描
- 开机扫描
- 文档防护
- 电子邮件客户端防护
- Web 访问保护
- 计算机扫描



ThreatSense 参数已针对每个模块进行了高度优化，对其进行修改可能会明显影响系统操作。 例如，将参数更改为始终扫描运行时加壳程序，或在文件系统实时防护模块中启用高级启发式扫描，可能会造成系统运行缓慢（通常，只有在扫描新建文件时才使用这些方法）。 我们建议您保留所有模块（“计算机扫描”除外）的默认 ThreatSense 参数。

要扫描的对象

此部分使您可以定义要扫描的计算机组件和文件，以查找渗透。

系统内存 – 扫描攻击系统的系统内存的威胁。

引导区/UEFI – 扫描引导区以检查主引导记录中是否存在恶意软件。在词汇表中阅读有关 UEFI 的更多信息。

电子邮件文件 – 该程序支持以下扩展名：DBX (Outlook Express) 和 EML。

压缩文件 – 该程序支持以下扩展名：ARJ, BZ2, CAB, CHM, DBX, GZIP, ISO/BIN/NRG, LHA, MIME, NSIS, RAR, SIS, TAR, TNEF, UUE, WISE, ZIP, ACE 以及许多其他扩展名。

自解压文件 – 自解压文件 (SFX) 是可提取自身的压缩文件。

加壳程序 – 执行后，加壳程序在内存中解压，这一点与标准压缩文件类型不同。 除了标准静态加壳程序（UPX, yoda, ASPack, FSG 等），扫描程序能够通过使用代码仿真来识别多种其他类型的加壳程序。

扫描选项

选择在扫描系统中的渗透时所用的方法。有以下选项可供使用：

启发式扫描 – 启发式扫描是一种分析（恶意）程序行为的算法。此技术的主要优点是能够识别过去不存在或以前的检测引擎版本无法识别的恶意软件。缺点是可能发出虚假警报（尽管可能性很小）。

高级启发式扫描/DNA 病毒库 – 高级启发式扫描是一种独特的启发式扫描算法，该算法由 ESET 开发，针对检测使用高级编程语言编写的计算机蠕虫和木马进行了优化。 使用高级启发式扫描显著提高了 ESET 产品的威胁检测功能。 病毒库可以可靠地检测和识别病毒。 利用自动更新系统，可以在发现威胁后的数小时内提供新病毒库。 该病毒库的缺点是只能检测到它所知道的病毒（或在这些病毒基础上略做修改的版本）。

清除

清除设置确定 ESET Endpoint Antivirus 在清除对象期间的行为。

排除

扩展名是用句点分隔的文件名的一部分。扩展名定义文件的类型和内容。ThreatSense 参数设置的此部分允许您定义要扫描的文件类型。

其他

配置 ThreatSense 引擎参数设置以进行手动扫描计算机时，**其他**部分中的以下选项也可用：

扫描交换数据流（ADS) - NTFS 文件系统使用的交换数据流是对普通扫描技术不可见的文件和文件夹关联。 许多渗透试图通过伪装成交换数据流来避开检测。

以低优先级运行后台扫描 – 每个扫描序列都消耗一定量的系统资源。如果您使用高系统资源负载的程序，则可以激活低优先级后台扫描，并为应用程序节约资源。

记录所有对象 - 扫描日志将显示自解压存档中的所有已扫描文件，甚至包括未感染的文件（可能会生成大量扫描日志数据并增加扫描日志文件的大小）。

启用智能优化 – 启用智能优化后，使用最优化的设置可确保最高效的扫描级别，同时可保持最高的扫描速度。各种保护模块可进行智能化扫描，使用不同的扫描方法并将它们应用到特定的文件类型。如果禁用了智能优化，则在执行扫描时仅应用特定模块的 ThreatSense 核心中用户定义的设置。

保存上一个访问时戳 – 选中此选项可以保留已扫描文件的最初访问时间而不是更新时间（例如数据备份系统所使用的访问时戳）。

限制

限制部分允许您指定要扫描的对象的最大大小和嵌套压缩文件的层数：

对象设置

最大对象大小 – 定义要扫描对象的最大大小。给定的病毒防护模块将仅扫描小于指定大小的对象。此选项应仅由具有从扫描中排除大型对象的特定原因的高级用户更改。默认值：无限制

对象的最长扫描时间(秒) – 定义扫描容器对象（例如 RAR/ZIP 压缩文件或附带多个附件的电子邮件）中文件的最长时间值。此设置不适用于独立文件。如果已输入用户定义的值并且该时间已经过去，则无论容器对象中每个文件的扫描是否完成，扫描都将尽快停止。对于内含大文件的压缩文件，扫描将在提取压缩文件中的文件之前立即停止（例如，当用户定义的变量为 3 秒，但文件提取需要 5 秒时）。在此时间过后，将不会扫描压缩文件中的其余文件。要限制扫描时间（包括较大的压缩文件），请使用**最大对象大小**和**压缩文件中的最大文件大小**（由于可能存在安全风险，不建议使用）。默认值：无限制

压缩文件扫描设置

压缩文件嵌套层数 – 指定压缩文件扫描的最大深度。默认值： 10.

压缩文件中的最大文件大小 – 此选项允许您指定要扫描的压缩文件（当解压缩时）中所包含文件的最大文件大小。最大值为 3 GB

不建议更改默认值，正常情况下应该没有修改它的理由。

清除级别

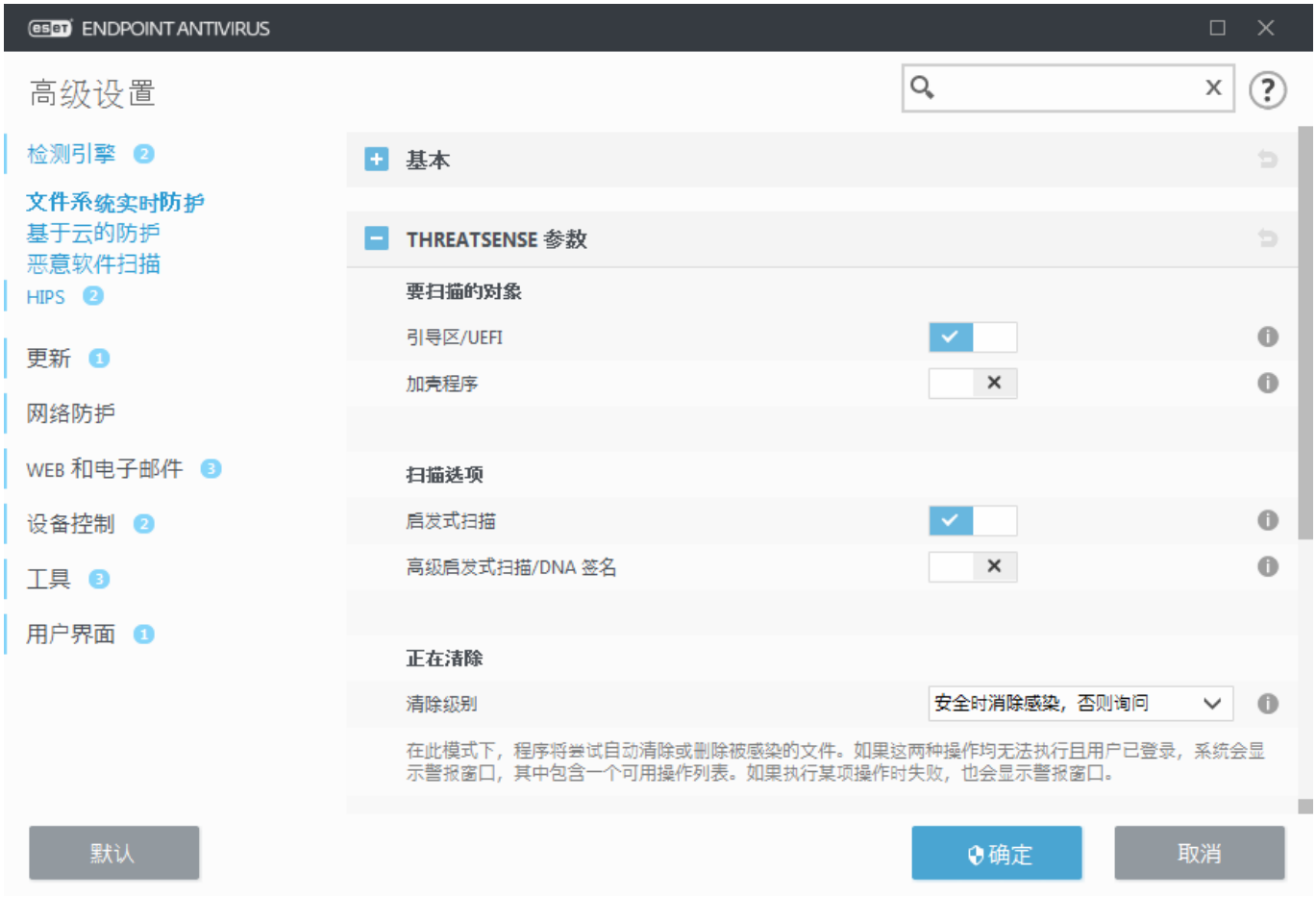
要访问所需防护模块的清除级别设置，请展开 **ThreatSense 参数**（例如，**文件系统实时防护**），然后单击**清除**

实时防护和其他防护模块具有以下修复（即清除）级别。

ESET Endpoint Antivirus 9 中的修复

清除级别	说明
始终修复检测	在清除对象时尝试修复检测，而无需任何最终用户干预。在极少数情况下（例如，系统文件），如果无法修复检测，则报告的对象将保留在其原始位置。**始终修复检测**是受管环境中建议的默认设置。

清除级别	说明
如果安全，则修复检测，否则保留	清除对象时尝试修复检测，而无需任何最终用户干涉。在某些情况下（例如，具有干净和受感染文件的系统文件或存档），如果无法修复检测，则报告的对象将保留在其原始位置。
如果安全，则修复检测，否则询问	在清除对象时尝试修复检测。在某些情况下，如果不能执行任何操作，则最终用户将收到一条交互警告并且必须选择一个修复操作（例如，删除或忽略）。大多数情况下建议使用此设置。
始终询问最终用户	最终用户在清除对象时会收到一个交互式窗口，必须选择修复操作（例如，删除或忽略）。此级别旨在面向更高级的用户，他们了解在检测事件中应采取哪些步骤。



不扫描的文件扩展名

扩展名是用句点分隔的文件名的一部分。扩展名定义文件的类型和内容。ThreatSense 参数设置的此部分允许您定义要扫描的文件类型。

请勿与其他类型的排除混淆。

默认情况下，扫描所有文件。 可将任何扩展名添加到不扫描的文件列表中。

如果对某些文件类型的扫描导致使用特定扩展名的程序运行不正常，将这些文件排除出扫描之列有时是必要的。例如，使用 Microsoft Exchange 服务器时，建议排除 `.edb`、`.eml` 和 `.tmp` 扩展名。

若要将新扩展名添加到列表，请单击**添加**。将该扩展名键入到空白字段（例如 `tmp`），然后单击**确定**。当选择**输入多个值**时，可以添加多个由行、逗号或分号分隔的文件扩展名（例如，从下拉菜单中选择**分号**作为分隔符，然后键入 `edb;eml;tmp`）。
您可以使用特殊符号 ？（问号）。问号可表示任意符号（例如 `?db`）。

为了在 Windows 操作系统中可以查看文件的确切扩展名（如果存在），必须在**控制面板 > 文件夹选项 > 查看**（选项卡）下取消选中**隐藏已知文件类型的扩展名**选项，并应用此更改。

其他 ThreatSense 参数

用于新建文件和已修改文件的其他 ThreatSense 参数 – 新建或修改的文件受感染的可能性相对于现有文件更高。这就是程序使用附加扫描参数检查这些文件的原因。除了使用普通的基于病毒库的扫描方法外，还使用高级启发式扫描，它可在发布检测引擎更新之前检测新威胁。除了新建文件，系统还扫描自解压文件 (.sfx) 和加壳程序（内部压缩的可执行文件）。默认情况下，对压缩文件的扫描可深达第 10 个嵌套层，而且不论其实际大小，都会进行检查。若要修改压缩文件扫描设置，请禁用**默认的压缩文件扫描设置**。

若要了解有关加壳程序、自解压文件以及高级启发式扫描的详细信息，请参阅 ThreatSense 引擎参数设置。

用于已执行文件的其他 ThreatSense 参数 – 默认情况下，在执行文件时将使用高级启发式扫描。启用后，强烈建议您启用智能优化和 ESET LiveGrid® 以降低对系统性能的影响。

网络

网络部分允许您快速访问**高级设置**中的以下组件或设置：

- **网络攻击防护 (IDS)** – 分析网络通信的内容并保护免受网络攻击。将阻止任何被认为有害的通信。当连接到不受保护的无线网络或保护性较弱的网络时，ESET Endpoint Antivirus 会通知您。

- **僵尸网络防护** – 快速准确地识别系统中的恶意软件。若要在特定时段禁用“僵尸网络防护”，请单击  （不建议）。

- **临时 IP 地址黑名单** – 查看 IP 地址的列表，这些地址已被检测为攻击源并添加至黑名单，以在一定时间内阻止连接。有关详细信息，请单击此选项并按 F1 键。

- **故障排除向导** – 帮助您解决由 ESET 防火墙导致的连接问题。有关更多详细信息，请参阅故障排除向导。

网络攻击防护

启用网络攻击防护(IDS) – 分析网络通信的内容并防止发生网络攻击。将阻止任何视为有害的通信。

启用僵尸网络防护 – 在计算机被感染且机器人尝试通信时，将根据典型模式检测并阻止与恶意命令和控制服务器进行通信。在词汇表中阅读有关“僵尸网络防护”的更多信息

IDS 规则 – 此选项使您可以配置高级过滤选项，以检测会对您的计算机造成危害的多种类型的攻击和漏洞利用。

高级过滤选项

“网络攻击防护”部分让您可以配置高级过滤选项，来检测可能会对计算机执行的多种类型的攻击和漏洞。

在某些情况下，您不会收到有关阻止的通信的威胁通知。有关查看防火墙日志中所有已阻止的通信的说明，请参见记录日志并从中创建规则或例外部分。

“高级设置”(F5) > **网络防护** > **网络攻击防护**中特定选项的可用性可能会有所不同，具体取决于 ESET 端点产品和防火墙模块的类别或版本以及操作系统的版本。其中一些选项可能仅适用于 ESET Endpoint Security

入侵检测

- **协议 SMB** – 检测和阻止 SMB 协议中的各种安全问题，即：

  - **流氓服务器挑战攻击身份验证检测** – 保护您免受身份验证期间使用流氓挑战获取用户凭据的攻击。

  - **命名管道打开期间 IDS 逃避检测** – 检测 SMB 协议中用于打开 MSRPC 命名管道的已知逃避技术。

  - **CVE 检测**（常见漏洞和暴露）– 对各种攻击、形式、安全漏洞和 SMB 协议漏洞实施的检测方法。请参阅 CVE 网站 (cve.mitre.org)，搜索和获取有关 CVE 标识符 (CVE) 的更详细信息。

- **协议 RPC** – 检测和阻止为分布式计算环境 (DCE) 开发的远程过程调用系统中的各种 CVE。
- **协议 RDP** – 检测和阻止 RDP 协议中的各种 CVE。如上所述）。
- **攻击检测之后阻止不安全的地址** – 将已检测为攻击源的 IP 地址添加到黑名单，以在一定时间内阻止连接。
- **攻击检测之后显示通知** – 启用屏幕右下角的系统托盘通知。
- **还为针对安全漏洞的传入攻击显示通知** – 如果检测到针对安全漏洞的攻击或威胁试图以此方式进入系统，则会发出警报。

数据包检测

- **允许在 SMB 协议下对管理员共享的传入连接** – 管理员共享是默认的网络共享，它和系统文件夹（*ADMIN$*）共享系统中的硬盘分区（*C$* 和 *D$* 等等）。禁用对管理员共享的连接将降低许多安全风险。例如，Conficker 蠕虫会执行字典攻击，以便连接到管理员共享。

- **拒绝旧的(不受支持的)SMB 方言** – 拒绝使用旧的 SMB 方言（不受 IDS 支持）的 SMB 会话。由于现代 Windows 操作系统可向后兼容旧的操作系统（例如 Windows 95），因此它支持旧的 SMB 方言。攻击者可以在 SMB 会话中使用一种旧方言从而避免通信检测。如果计算机无需与使用旧版本的 Windows 的计算机共享文件（或使用一般的 SMB 通信），请拒绝旧的 SMB 方言。

- **拒绝无扩展安全性的 SMB 会话** – 可以在 SMB 会话协商期间使用扩展的安全性，以便提供比 LAN 管理器挑战/响应 (LM) 身份验证更安全的身份验证机制。LM 方案是一种较弱的验证机制，因而不建议使用。

- **允许与安全帐户管理器服务的通信** – 有关此服务的详细信息，请参阅 [MS-SAMR]。

- **允许与本地安全验证服务的通信** – 有关此服务的详细信息，请参阅 [MS-LSAD] 和 [MS-LSAT]。

- **允许与远程注册表服务的通信** – 有关此服务的详细信息，请参阅 [MS-RRP]。

- **允许与服务控制管理器服务的通信** – 有关此服务的详细信息，请参阅 [MS-SCMR]。

- **允许与服务器服务的通信** – 有关此服务的信息，请参阅 [MS-SRVS]。

- **允许与其他服务的通信** – 其他 MSRPC 服务。MSRPC 是指 DCE RPC 机制的 Microsoft 实现。

此外，MSRPC 可以将 SMB（网络文件共享）协议中的命名管道用于传输 (ncacn_np transport)。MSRPC 服务提供用于远程访问和管理 Windows 系统的接口。在 Windows MSRPC 系统中发现了很多被恣意使用的安全漏洞（Conficker 蠕虫和 Sasser 蠕虫等等）。禁用与不需要的 MSRPC 服务的通信可降低许多安全风险（例如，远程代码执行或服务故障攻击）。

IDS 规则

在某些情况下，入侵检测服务 (IDS) 可能会将路由器或其他内部网络设备之间的通信检测为潜在攻击。例如，可以将已知安全地址添加到“从 IDS 区域中排除的地址”，以绕过 IDS。

以下 ESET 知识库文章可能仅提供英文版：
- 在 ESET Endpoint Antivirus 中的客户端工作站上创建 IDS 规则
- 在 ESET PROTECT 中为客户端工作站创建 IDS 规则

列

- **检测** – 检测类型。

- **应用程序** – 通过单击 ...，选择例外应用程序的文件路径（例如 *C:\Program Files\Firefox\Firefox.exe*）。请勿输入应用程序的名称。

- **远程 IP** – 远程 IPv4 或 IPv6 地址/范围/子网的列表。多个地址必须使用逗号分隔。

- **阻止** – 每个系统进程都具有自己的默认行为和分配的操作（阻止或允许）。若要覆盖 ESET Endpoint Antivirus 的默认行为，可以使用下拉菜单来选择是阻止还是允许它。

- **通知** – 选择是可在计算机上显示桌面通知。选择否（如果不希望显示桌面通知）。可用值为默认/是/否。

- **日志** – 选择**是**以事件记录到ESET Endpoint Antivirus 日志文件。选择**否**（如果不希望记录事件）。可用值为**默认/是/否**。

如果管理员在 ESET PROTECT Web 控制台中创建 IDS 排除，将显示选项卡排除。IDS 排除只能包含允许规则，并在 IDS 规则之前进行评估。

管理 IDS 规则

- **添加** – 单击以创建新的 IDS 规则。
- **编辑** – 单击以编辑现有 IDS 规则。

- **删除** – 如果要从 IDS 规则列表中删除现有例外，请选择并单击该选项。

-  **最高/向上/向下/最低** – 让您可以调整规则的优先级（按从最高到最低的顺序评估例外）。

希望在每次事件发生时显示通知并收集日志：
1.单击**添加**以添加新的 IDS 规则。
2.从**检测**下拉菜单中选择特定警报。
✔ 3.单击 **...**并选择要应用通知的应用程序的文件路径。
4.在**阻止**下拉菜单中保留**默认**。这将继承由 ESET Endpoint Antivirus 应用的默认操作。
5.将**通知**和**日志**下拉菜单都设置为**是**。
6.单击**确定**以保存此通知。

您希望删除不视为威胁的某类检测的反复通知：
1.单击**添加**以添加新的 IDS 例外。
2.从**检测**下拉菜单中选择特定警报，例如**无安全扩展的 SMB 会话**.
3.从方向下拉菜单中选择**入**（如果它来自入站通信）。
✔ 4.将**通知**下拉菜单设置为**否**。
5.将**日志**下拉菜单设置为**是**。
6.将**应用程序**留空。
7.如果通信不是来自特定 IP 地址，请将**远程 IP 地址**留空。
8.单击**确定**以保存此通知。

已阻止可疑的威胁

如果您的计算机上的某个应用程序通过利用安全漏洞尝试向网络上的另一台计算机发送恶意通信，或有人尝试扫描网络上的端口，则可能会发生这种情况。

威胁 – 威胁的名称。

源 – 源网络地址。

目标 – 目标网络地址。

停止阻止 – 使用允许通信的设置为可疑威胁创建一个 IDS 规则。

保持阻止 – 阻止检测到的威胁。要使用阻止通信的设置为此威胁创建一个 IDS 规则，请选中**不要再通知我**。

i 此通知窗口中显示的信息可能因检测到的威胁类型而异。
有关威胁和其他相关术语的详细信息，请参阅远程攻击类型或检测类型。

网络防护故障排除

“故障排除”向导可帮助您解决由 ESET 防火墙导致的连接问题。 从下拉菜单中，选择阻止通信的时间段。 最近阻止的通信列表向您提供了有关在该时间段内阻止的应用程序或设备类型、应用程序和设备的信誉和总数的概述。 有关已阻止通信的更多详细信息，请单击**详细信息**。 下一步是取消阻止遇到连接问题的应用程序或设备。

当您单击**取消阻止**时，将允许之前阻止的通信。 如果您继续遇到应用程序问题，或者您的设备没有按预期工作，则单击**应用程序仍无法正常工作**，并且现在将允许之前针对该设备所阻止的所有通信。 如果仍存在问题，则重新启动计算机。

单击**显示更改**以查看向导创建的规则。

单击**取消阻止另一个以解决与其他设备或应用程序的通信问题。**

临时 IP 地址黑名单

要查看已检测为攻击源的 IP 地址（这些地址已添加到黑名单，以在特定时间段内阻止连接），请在 ESET Endpoint Antivirus 中导航到**设置 > 网络 > 临时 IP 地址黑名单**。临时阻止的 IP 地址将被阻止 1 小时。

列

IP 地址 – 显示已被阻止的 IP 地址。

阻止原因 – 显示从该地址阻止的攻击类型（例如 TCP 端口扫描攻击）。

超时 – 显示地址将在黑名单中过期的时间和日期。

控件元素

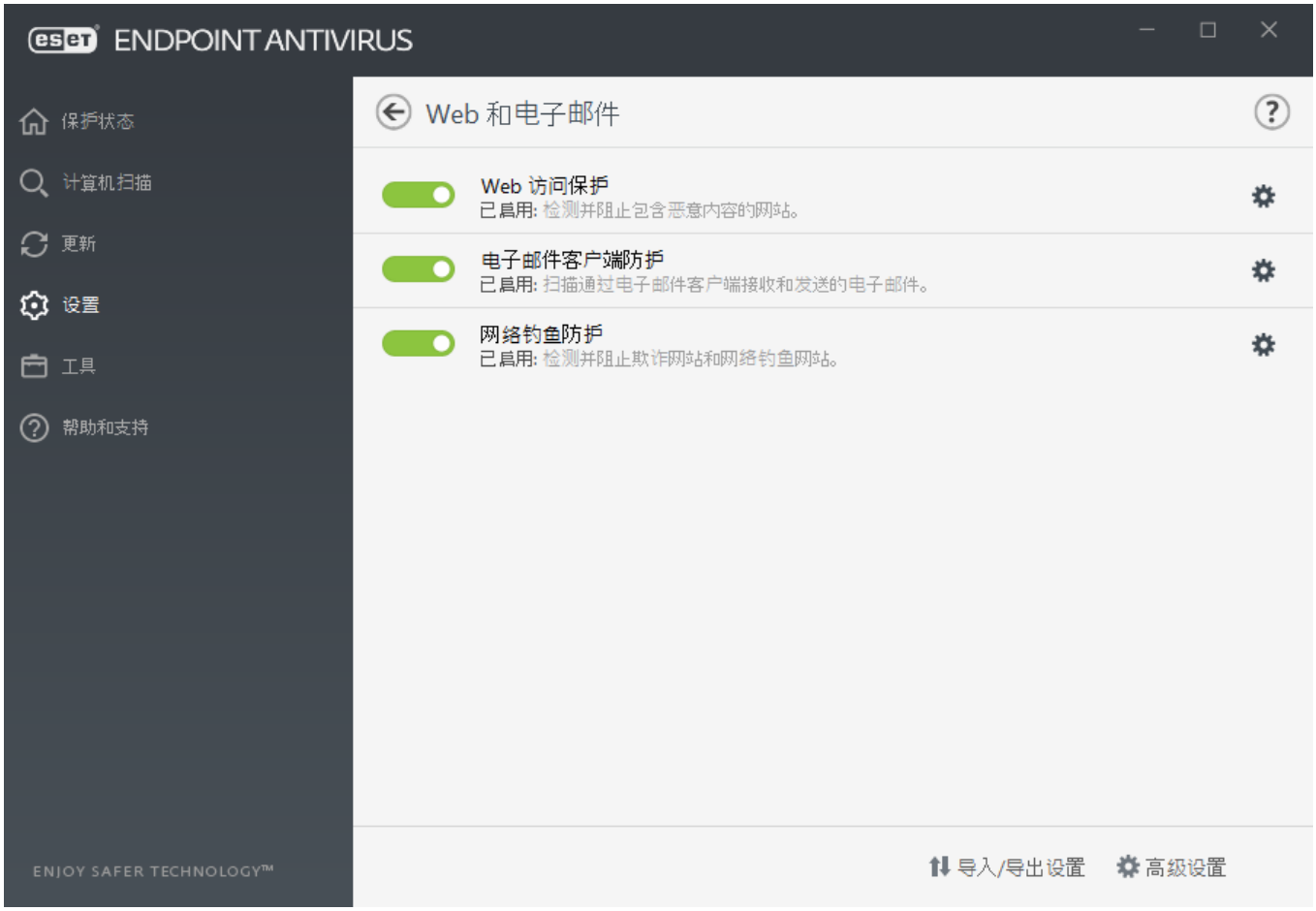
删除 – 单击以在地址过期前将其从黑名单中删除。

全部删除 – 单击以立即从黑名单中删除所有地址。

添加例外 – 单击以向 IDS 过滤添加一个防火墙例外。

Web 和电子邮件

可在**设置 > Web 和电子邮件**下找到 Web 和电子邮件配置。可以从这里访问更详细的程序设置。



Internet 连接是个人计算机的一项标准功能。 不幸地是，Internet 已成为了散布恶意代码的主要媒介。 出于此原因，仔细考虑 **Web 访问保护**设置就变得很重要。

电子邮件客户端防护可控制通过 POP3(S) 和 IMAP(S) 协议接收的电子邮件通信。使用电子邮件客户端的插件程序，ESET Endpoint Antivirus 可控制电子邮件客户端的所有通信。

网络钓鱼防护是另一层防护，可增加对尝试获取密码和其他敏感信息的非法网站的防御。网络钓鱼防护可在 Web 和电子邮件下的设置窗格中找到。有关详细信息，请参阅网络钓鱼防护。

您可以禁用 Web/电子邮件/网络钓鱼防护 防护模块（暂时），方法是单击 。

协议过滤

针对应用程序协议的病毒防护由 ThreatSense 扫描引擎提供，可与所有高级恶意软件扫描技术无缝集成。无论使用哪种 Internet 浏览器或电子邮件客户端，协议过滤都会自动工作。要编辑加密 (SSL) 设置，请转到**高级设置** (F5) > **Web 和电子邮件** > **SSL/TLS**。

启用应用程序协议内容过滤 – 可以用于禁用协议过滤。请注意，许多 ESET Endpoint Antivirus 组件（Web 访问防护、电子邮件协议防护、网络钓鱼防护、Web 控件）都依赖于此选项；如果没有此选项，这些组件将不起作用。

排除的应用程序 – 允许您从协议过滤中排除特定应用程序。在协议过滤导致兼容性问题时很有用。

排除的 IP 地址 – 允许您从协议过滤中排除特定远程地址。在协议过滤导致兼容性问题时很有用。

IPv4 地址和掩码：
• *192.168.0.10* – 添加将应用规则的单台计算机的 IP 地址。
• *192.168.0.1* 至 *192.168.0.99* – 输入开始和结束 IP 地址以指定将应用规则的（多台计算机的□IP 范围。
• 由 IP 地址和掩码定义的子网（一组计算机）。例如，*255.255.255.0* 是 *192.168.1.0/24* 前缀的网络掩码，表示 *192.168.1.1* 至 192.168.1.254 的地址范围。
IPv6 地址和掩码：
• *2001:718:1c01:16:214:22ff:fec9:ca5* – 将应用规则的单台计算机的 IPv6 地址
• *2002:c0a8:6301:1::1/64* – 前缀长度为 64 位的 IPv6 地址，它表示 *2002:c0a8:6301:0001:0000:0000:0000:0000 到 2002:c0a8:6301:0001:ffff:ffff:ffff:ffff*

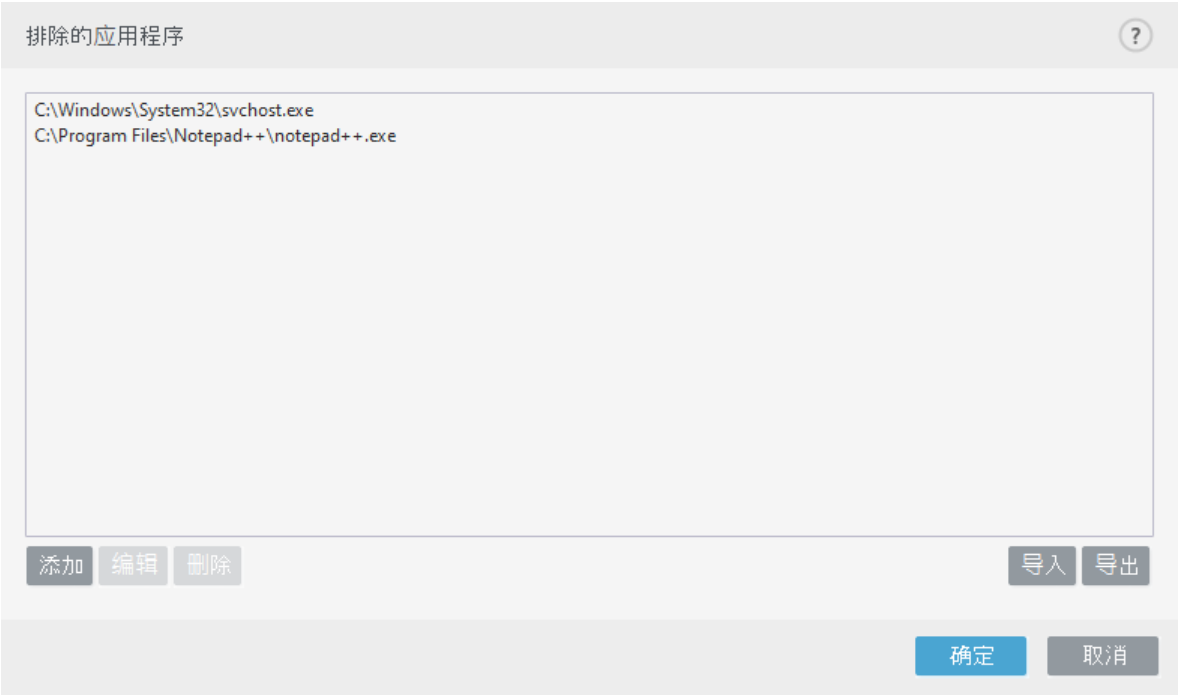
排除的应用程序

若要从协议过滤中排除用于特定网络感知应用程序的通信，请将其添加到此列表。将不检查选定应用程序的 HTTP/POP3/IMAP 通信是否存在威胁。我们建议您仅在启用的协议过滤使应用程序无法正常工作的情况下使用此技术。

单击**添加**后，将自动显示已受协议过滤影响的应用程序和服务。

编辑 – 编辑列表中的选定条目。

删除 – 删除列表中的选定条目。



排除的 IP 地址

此列表中的 IP 地址将被排除在协议内容过滤之外。将不检查往返选定地址的 HTTP/POP3/IMAP 通信是否存在威胁。我们建议仅在地址可信赖时使用此选项。

添加 – 单击以添加将应用规则的远程点的 IP 地址/地址范围/子网。

编辑 – 编辑列表中的选定条目。

删除 – 删除列表中的选定条目。

SSL/TLS

ESET Endpoint Antivirus 能够检查使用 SSL 协议的通信中是否存在威胁。通过受信任的证书、未知证书或不受 SSL 保护的通信检查的证书，可以将不同的扫描模式用于检查受 SSL 保护的通信。

启用 SSL/TLS 协议过滤 – 默认启用协议过滤。可以在**高级设置 > Web 和电子邮件 > SSL/TLS** 中或通过策略禁用“SSL/TLS 协议过滤”。如果协议过滤已禁用，则程序将不会扫描基于 SSL 的通信。

SSL/TLS 协议过滤模式在以下选项中可用：

过滤模式	说明
自动模式	默认模式将仅扫描适当的应用程序，例如 Web 浏览器和电子邮件客户端。 您可以通过选择要扫描其通信的应用程序来覆盖此选项。
交互模式	如果您输入一个受 SSL- 保护的新站点（使用未知证书），会显示操作选择对话框。 此模式允许您创建将不扫描的 SSL 证书/应用程序列表。
策略模式	选择此选项可扫描所有受 SSL 保护的通信，除了由排除在检查之外的证书保护的通信。 如果使用未知的、签署的证书建立了新通信，不会提示您，且通信将自动被过滤。 当不受信任的证书被标记为受信任（位于受信任的证书列表上）而用来访问服务器时，会允许对该服务器的通信，也会过滤通信通道的内容。

SSL/TLS 过滤的应用程序列表可用于为特定应用程序自定义 ESET Endpoint Antivirus 行为。

已知证书列表允许您自定义针对特定 SSL 证书的 ESET Endpoint Antivirus 行为。

排除使用受信任域的通信 – 启用后，将不检查使用受信任域的通信。 域信任由内置白名单确定。

阻止使用已过时 SSL v2 协议加密的通信 – 将自动阻止使用早期版本的 SSL 协议的通信。

如果设置**排除与受信任域的通信**已启用，并且域被认为是受信任的，将不会过滤地址。

根证书

根证书 – 要使 SSL 通信在您的浏览器/电子邮件客户端中正常工作，请务必将 ESET 根证书添加到已知根证书（发布者）的列表中。应启用**将根证书添加到已知浏览器**。选中此选项可自动将 ESET 根证书添加到已知浏览器（如 Opera 和 Firefox□□对于使用系统证书存储的浏览器，会自动添加证书（例如，在 Internet Explorer 中）。

要将该证书应用到不受支持的浏览器，请依次单击**查看证书 > 详细信息 > 复制到文件**，然后手动将其导入该浏览器。

证书有效性

如果无法建立证书信任 – 在某些情况下，无法使用受信任的根证书颁发机构 (TRCA) 验证网站证书。这意味着该证书将由某人（例如 Web 服务器或小型企业的管理员）签名，将此证书视为受信任并不总是存在风险。大部分大型企业（例如银行）使用 TRCA 签名的证书。如果选中了**询问证书的有效性**（默认为选中），将在建立加密通信时，提示用户选择要采取的操作。您可以选择**阻止使用该证书的通信**，以始终终止使用未验证证书站点的加密连接。

证书已损坏时 – 这意味着证书未正确签名或已损坏。在这种情况下，我们建议您将**阻止使用该证书的通信**保持处于选中状态。如果选中**询问证书有效性**，则在建立加密通信时系统会提示用户选择要执行的操作。

以下 ESET 知识库文章可能仅提供英文版：
- ESET 产品中的证书通知
- 访问 Web 页面时将显示“加密的网络通信：不信任的证书”

证书

要使 SSL 通信在您的浏览器/电子邮件客户端正常工作，请将 ESET 根证书添加到已知根证书（发布者）的列表中。 应启用**将根证书添加到已知浏览器**。 选中此选项可自动将 ESET 根证书添加到已知浏览器（如 Opera 和 Firefox□□ 对于使用系统证书存储的浏览器，会自动添加证书（如 Internet Explorer□□ 要将该证书应用到不受支持的浏览器，请单击**查看证书 > 详细信息 > 复制到文件**，然后手动将其导入该浏览器。

在某些情况下，使用受信任的根证书颁发机构（比如 VeriSign□无法验证该证书。 这意味着该证书将由某人（比如 Web 服务器或小型公司的管理员）自签名，将此证书视为受信任不总是存在风险。 大部分大型公司（比如银行）使用 TRCA 签名的证书。 如果选中了**询问证书的有效性**（默认为选中），将在建立加密通信时，提示用户选择要采取的操作。 将显示操作选择对话框，其中您可决定是否要标记该证书为受信任或排除。 如果证书不存在于 TRCA 列表中，则窗口为红色。 如果证书在 TRCA 列表中，则窗口将为绿色□

您可以选择**阻止使用该证书的通信**，以便总是终止使用未经验证证书网站的加密连接。

如果该证书无效或损坏，这意味着证书已过期或被错误自签名。 在这种情况下，我们建议阻止使用该证书的通信。

加密的网络通信

如果您的系统配置为使用 SSL 协议扫描，在两种情况下将显示用于提示您选择操作的对话窗口：

首先，如果网站使用无法验证或无效的证书，而且 ESET Endpoint Antivirus 配置为在此类情况下询问用户（默认情况下，无法验证的证书为“是”，无效的证书为“否”），将显示一个对话框询问您**允许**还是**阻止**该连接。如果证书不在 Trusted Root Certification Authorities store (TRCA) 中，则认为它不受信任。

其次，如果 **SSL 协议过滤模式**设置为**交互模式**，用于每个网站的对话框都将询问要**扫描**还是**忽略**通信。某些应用程序验证其 SSL 通信未受到任何人的修改或检查，在此类情况下，ESET Endpoint Antivirus 必须**忽略**该通信以保持应用程序正常工作。

以下 ESET 知识库文章可能仅提供英文版：
- ESET 产品中的证书通知
- 访问 Web 页面时将显示“加密的网络通信：不信任的证书”

在这两种情况下，用户可以选择记住选中的操作。保存的操作存储在已知证书列表中。

已知证书列表

已知证书列表可用于自定义特定 SSL 证书的 ESET Endpoint Antivirus 行为，如果在 **SSL/TLS 协议过滤模式**下选中**交互模式**，还可用于记住所选的操作。可以在**高级设置** (F5) > **Web 和电子邮件** > **SSL/TLS** > **已知证书列表**中查看和编辑该列表。

已知证书列表窗口包含：

列

名称 – 证书名称。

证书颁发者 – 证书创建者的名称。

证书主题 – 主题字段可标识与存储在主题公共密钥字段中的公共密钥相关联的实体。

访问 – 选择**允许**或**阻止作为访问操作**，以允许/阻止受此证书保护的通信，不管其可信度如何都是如此。选择**自动**以允许受信任的证书并询问是否允许不受信任的证书。选择**询问**以始终询问用户要执行的操作。

扫描 – 选择**扫描**或**忽略**作为**扫描操作**，以扫描或忽略受此证书保护的通信。选择**自动**以在自动模式下扫描并在交互模式进行询问。选择**询问**以始终询问用户要执行的操作。

控件元素

添加 – 可以作为带扩展名 *.cer*、*.crt* 或 *.pem* 的文件手动加载证书。单击**文件**上载本地证书或单击 **URL** 联机指定证书的位置。

编辑 – 选择您希望配置的证书，然后单击**编辑**。

删除 – 选择要删除的证书，然后单击**删除**。

确定/取消 – 如果您希望保存更改，则单击**确定**；如果要在不保存的情况下退出，则单击**取消**。

SSL/TLS 过滤的应用程序列表

SSL/TLS 过滤的应用程序列表可用于自定义特定应用程序的 ESET Endpoint Antivirus 行为，如果在 **SSL/TLS 协议过滤模式**下选中**交互模式**，还可用于记住所选的操作。可以在**高级设置** (F5) > **Web 和电子邮件** > **SSL/TLS** > **SSL/TLS 过滤的应用程序列表**中查看和编辑该列表。

SSL/TLS 过滤的应用程序列表窗口包含：

列

应用程序 – 应用程序的名称。

扫描操作 – 选择**扫描**或**忽略**以扫描或忽略通信。选择**自动**以在自动模式下扫描并在交互模式下进行询问。选择**询问**以始终询问用户要执行的操作。

控件元素

添加 – 添加过滤的应用程序。

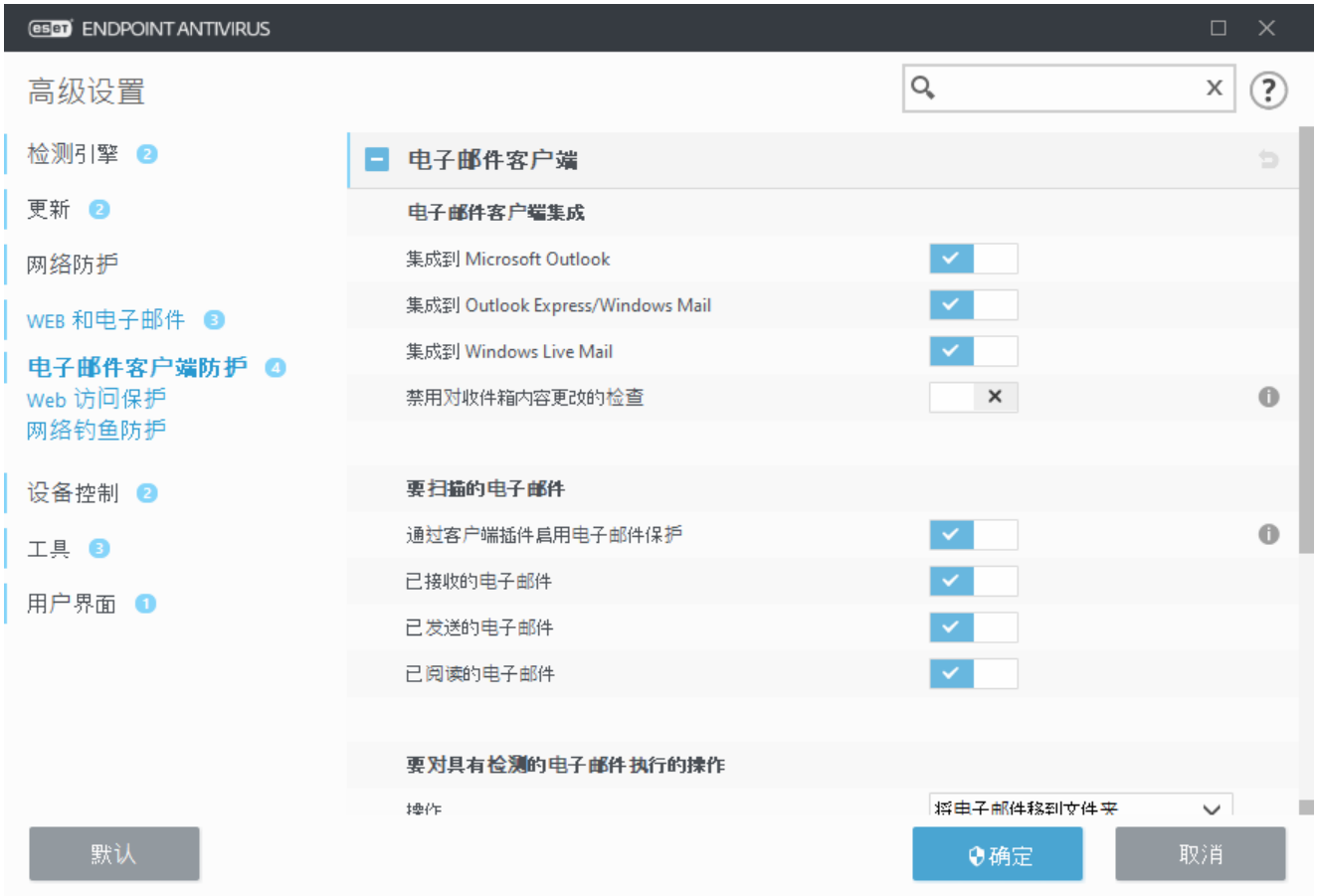
编辑 – 选择您希望配置的证书，然后单击**编辑**。

删除 – 选择要删除的证书，然后单击**删除**。

确定/取消 – 如果您希望保存更改，则单击**确定**；如果您希望在不保存的情况下退出，则单击**取消**。

电子邮件客户端防护

ESET Endpoint Antivirus 与电子邮件客户端的集成可提高针对电子邮件中恶意代码的主动防护级别。 如果您的电子邮件客户端受支持，则可以在 ESET Endpoint Antivirus 中启用集成。 当集成到电子邮件客户端时，ESET Endpoint Antivirus 工具栏将直接插入电子邮件客户端，从而提供更高效的电子邮件防护。 集成设置位于**高级设置** (F5) > **Web 和电子邮件** > **电子邮件客户端防护** > **电子邮件客户端**下。



电子邮件客户端集成

当前受支持的电子邮件客户端包括 Microsoft Outlook、Outlook Express、Windows Mail 和 Windows Live Mail。电子邮件保护的工作方式和这些程序的插件相同。插件的主要优点在于它独立于所用的协议。当电子邮件客户端收到加密邮件时，邮件会解密并发送给病毒扫描程序。有关支持的电子邮件客户端及其版本的完整列表，请参考以下 ESET 知识库文章。

如果在检索电子邮件时遇到系统运行缓慢的情况，请打开**禁用对收件箱内容更改的检查**。

要扫描的电子邮件

通过客户端插件启用电子邮件保护 – 当禁用时，通过电子邮件客户端插件的保护将关闭。

已接收的电子邮件 – 启用时，将检查已接收电子邮件。

已发送的电子邮件 – 启用时，将检查已发送电子邮件。

已阅读的电子邮件 – 启用时，将检查已阅读电子邮件。

我们建议您将**通过客户端插件启用电子邮件保护**保持为启用。 即使未启用集成或者集成不起作用，电子邮件通信仍受协议过滤（IMAP/IMAPS 和 POP3/POP3S）保护。

要对受感染的电子邮件执行的操作

无操作 – 如果已启用，则程序虽能识别感染的附件，但不会对电子邮件采取任何操作。

删除电子邮件 – 程序会通知用户有关渗透的信息并删除邮件。

将电子邮件移到已删除邮件文件夹 – 受感染的电子邮件将自动移至“已删除”邮件文件夹。

将电子邮件移到文件夹（默认操作） – 受感染的电子邮件将自动移至指定的文件夹。

文件夹 – 指定希望将检测到的受感染电子邮件移到的自定义文件夹。

更新后重新扫描 – 启用时，将在检测引擎更新后重新扫描受感染的电子邮件。

接受其他模块的扫描结果 – 允许电子邮件防护模块使用从其他防护模块接收的扫描结果，而无需重新扫描。

电子邮件协议

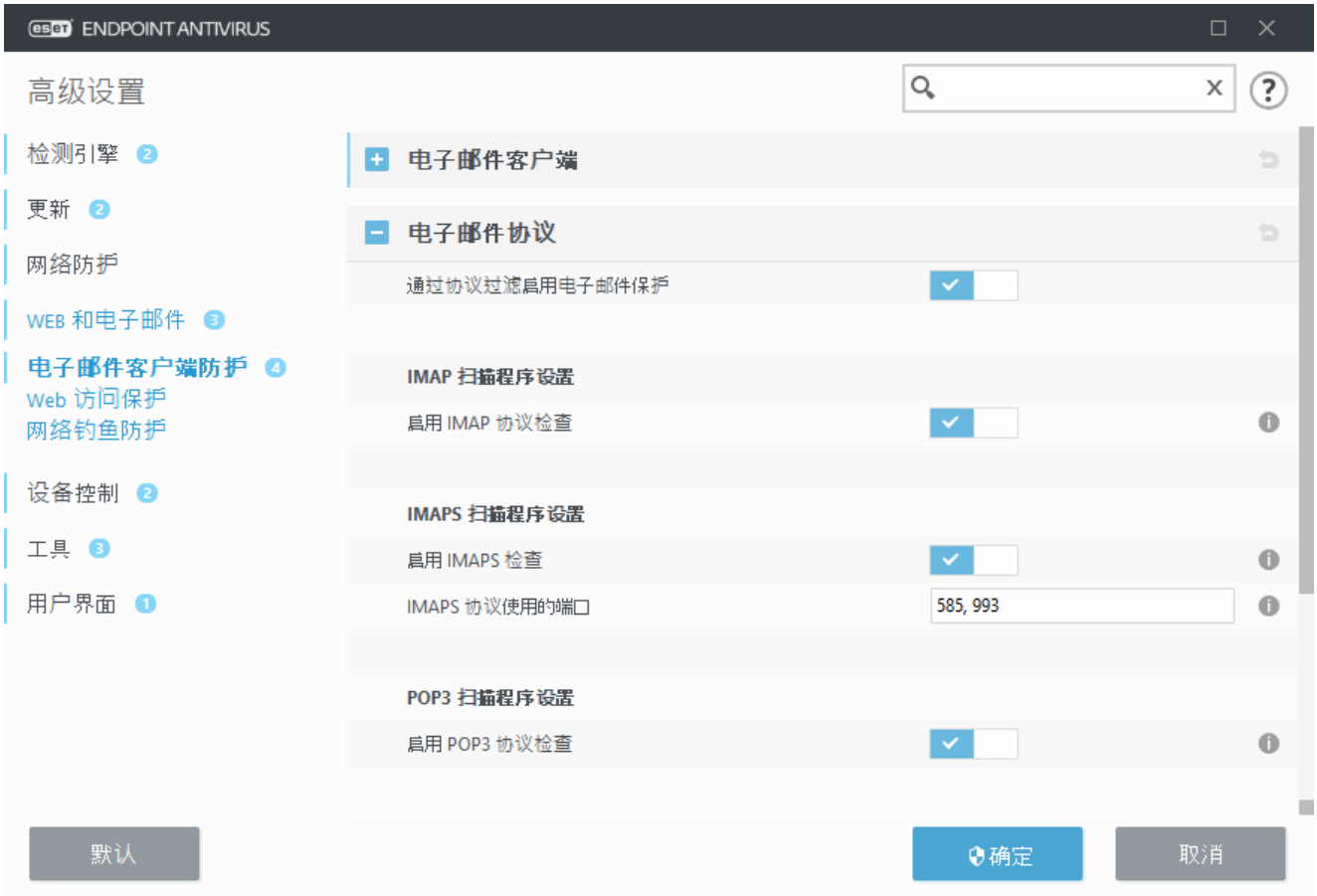
IMAP 和 POP3 协议是最广泛地用于在电子邮件客户端应用程序中接收电子邮件通信的协议。Internet 消息访问协议 (IMAP) 是另一种用于电子邮件检索的 Internet 协议。与 POP3 相比，IMAP 具有一些优势，例如多个客户端可同时连接到同一邮箱，并保留邮件状态信息（如邮件是已读、已回复还是已删除）。提供此控制的防护模块在系统启动时自动启动，然后在内存中处于活动状态。

无论使用何种电子邮件客户端，ESET Endpoint Antivirus 均提供对这些协议的保护，无需重新配置电子邮件客户端。默认情况下，将扫描通过 POP3 和 IMAP 协议的所有通信，无论默认的 POP3/IMAP 端口号是什么。
不会扫描 MAPI 协议。但与 Microsoft Exchange 服务器的通信可以由电子邮件客户端（例如，Microsoft Outlook）中的集成模块扫描。

我们建议您将**通过协议过滤启用电子邮件防护**保持为启用状态。 要配置 IMAP/IMAPS 和 POP3/POP3S 协议检查，请浏览到高级设置 > **Web 和电子邮件 > 电子邮件客户端防护 > 电子邮件协议**。

ESET Endpoint Antivirus 还支持扫描 IMAPS (585, 993) 和 POP3S (995) 协议，这些协议使用加密通道在服务器和客户端之间传输信息。ESET Endpoint Antivirus 利用 SSL（安全套接字层）和 TLS（传输层安全）协议检查通信。无论操作系统版本如何，该程序将只在 **IMAPS/POP3S 协议使用的端口**中定义的端口上扫描通信。如果必要，还可以添加其他通信端口。若有多个端口号，则必须由逗号分隔。

默认情况下，会扫描加密的通信。要查看扫描程序设置，请导航至“高级设置”部分的 SSL/TLS，依次单击 **Web 和电子邮件 > SSL/TLS**，然后启用**启用 SSL/TLS 协议过滤**选项。



电子邮件警报和通知

此功能的选项在 **Web 和电子邮件 > 电子邮件客户端防护 > 警报和通知**下的**高级设置**中可用。

选中一个电子邮件后，可将包含扫描结果的通知附加到邮件中。您可以选择**在已接收并阅读的电子邮件上添加标记消息**或**在已发送电子邮件上添加标记消息**。请注意，在少数情形下，标记消息可能被有问题的 HTML 邮件忽略，而恶意软件也可能伪造这些消息。可将标记消息添加到已接收和已阅读的电子邮件、已发送的电子邮件或两类邮件中都添加。有以下选项可供使用：

- **从不** – 不添加任何标记消息。
- **当发生检测时** – 仅将包含恶意软件的消息标记为已选中（默认）。
- **扫描时发送给所有电子邮件** – 程序将把消息附加到所有已扫描的电子邮件上。

更新已发送电子邮件的主题 – 如果不想要通过电子邮件防护在被感染的电子邮件主题中包含病毒警告，则禁用此选项。此功能允许对被感染的电子邮件进行简单的、基于主题的过滤（如果电子邮件程序支持）。它还可提高收件人的可信性，如果检测到渗透，还可提供关于给定电子邮件或发件人威胁级别的宝贵信息。

添加到已检测电子邮件主题的文本 – 如果要修改被感染电子邮件的主题前缀格式，则编辑此模板。此功能将邮件主题 "Hello" 替换为以下格式："[detection %DETECTIONNAME%] Hello"。变量 %DETECTIONNAME% 代表检测。

电子邮件客户端集成

当前受支持的电子邮件客户端包括 Microsoft Outlook、Outlook Express、Windows Mail 和 Windows Live Mail。电子邮件保护的工作方式和这些程序的插件相同。插件的主要优点在于它独立于所用的协议。当电子邮件客户端收到加密邮件时，邮件会解密并发送给病毒扫描程序。有关支持的电子邮件客户端及其版本的完整列表，请参考以下 ESET 知识库文章。

Microsoft Outlook 工具栏

Microsoft Outlook 防护以插件模块的方式工作。安装 ESET Endpoint Antivirus 后，包含病毒/防护选项的工具栏添加到 Microsoft Outlook。

ESET Endpoint Antivirus – 单击图标，打开 ESET Endpoint Antivirus 的主程序窗口。

重新扫描邮件 – 使您能够手动启动电子邮件检查。您可以指定将被检查的邮件，并且可以启用对已接收电子邮件的重新扫描。有关详细信息，请参阅电子邮件客户端防护。

扫描程序设置 – 显示电子邮件客户端防护设置选项。

Outlook Express 和 Windows Mail 工具栏

Outlook Express 和 Windows Mail 防护以插件模块的方式工作。安装 ESET Endpoint Antivirus 后，包含病毒/ 防护选项的此工具栏添加到 Outlook Express 或 Windows Mail。

ESET Endpoint Antivirus – 单击图标，打开 ESET Endpoint Antivirus 的主程序窗口。

重新扫描邮件 – 使您能够手动启动电子邮件检查。您可以指定将被检查的邮件，并且可以启用对已接收电子邮件的重新扫描。有关详细信息，请参阅电子邮件客户端防护。

扫描程序设置 – 显示电子邮件客户端防护设置选项。

用户界面

自定义外观 – 可为电子邮件客户端修改工具栏的外观。取消选中此选项可以独立于电子邮件程序参数而自定义外观。

显示文本 – 显示图标的说明。

右侧文本 – 选项说明将从图标的底部移到右侧。

大图标 – 显示菜单选项的大图标。

确认对话框

此通知用于验证用户是否确实想执行所选操作，这将消除可能发生的错误。

另一方面，该对话框也提供禁用确认的选项。

重新扫描邮件

ESET Endpoint Antivirus 工具栏与电子邮件客户端集成在一起，使用户能指定若干电子邮件检查选项。**重新扫描邮件**选项提供两种扫描模式：

当前文件夹中的所有邮件 – 扫描当前显示的文件夹中的邮件。

仅选定的邮件 – 仅扫描由用户标记的邮件。

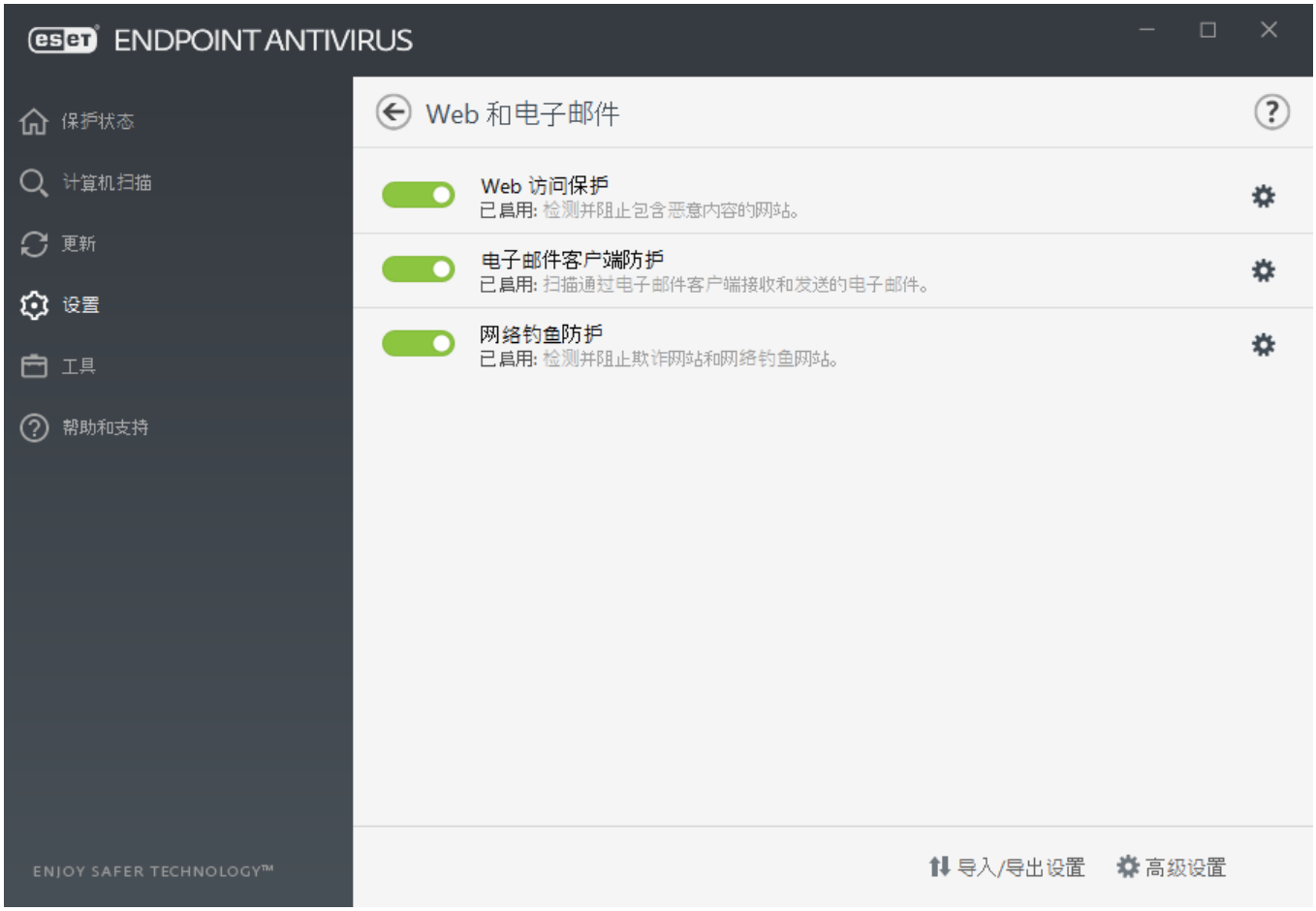
重新扫描已扫描的邮件复选框为用户提供了选项，可用来对以前已扫描的邮件再次执行扫描。

Web 访问保护

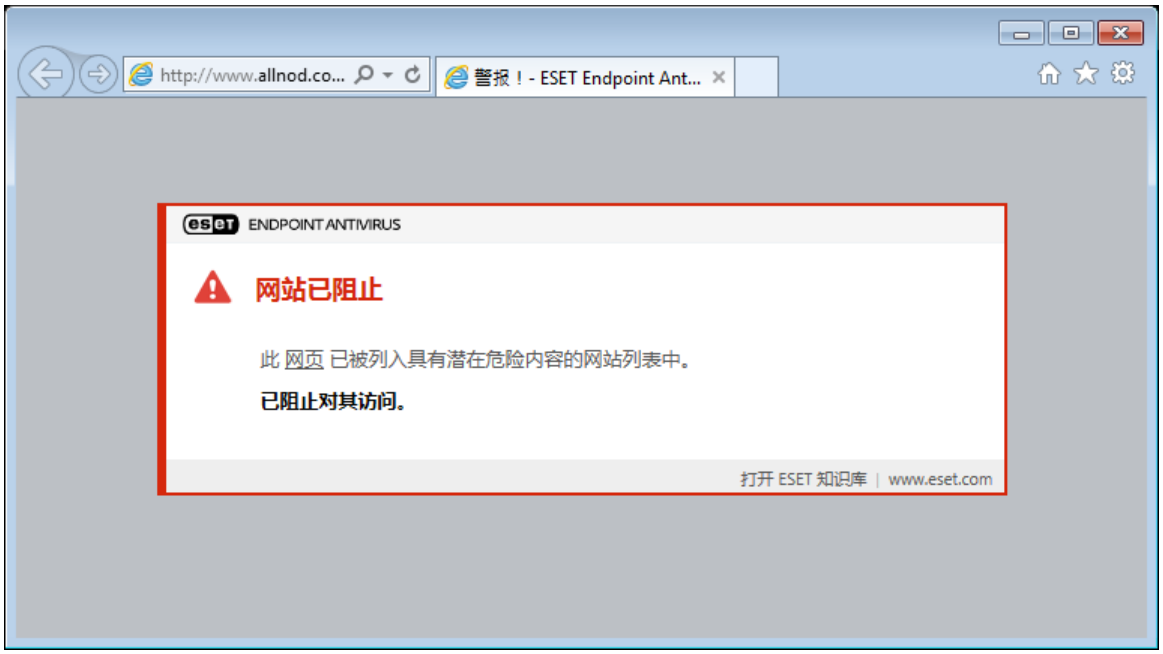
Internet 连接是个人计算机的一项标准功能。 不幸地是，它也成为传输恶意代码的主要媒介。 Web 访问保护的功能是监视 Web 浏览器和远程服务器之间的通信，并遵从 HTTP（超文本传输协议）和 HTTPS（加密通信）规则。

在下载内容之前，将阻止访问已知包含恶意内容的网页。 所有其他网页在加载时会由 ThreatSense 扫描引擎进行扫描，并且如果检测到恶意内容，将阻止它们。 Web 访问保护提供两种级别的保护：按黑名单阻止和按内容阻止。

我们强烈建议启用 Web 访问保护。 在 ESET Endpoint Antivirus 主窗口中导航至**设置 > Internet 防护 > Web 访问保护**可以访问此选项。



当网站被阻止时，Web 访问保护将在浏览器中显示以下消息：

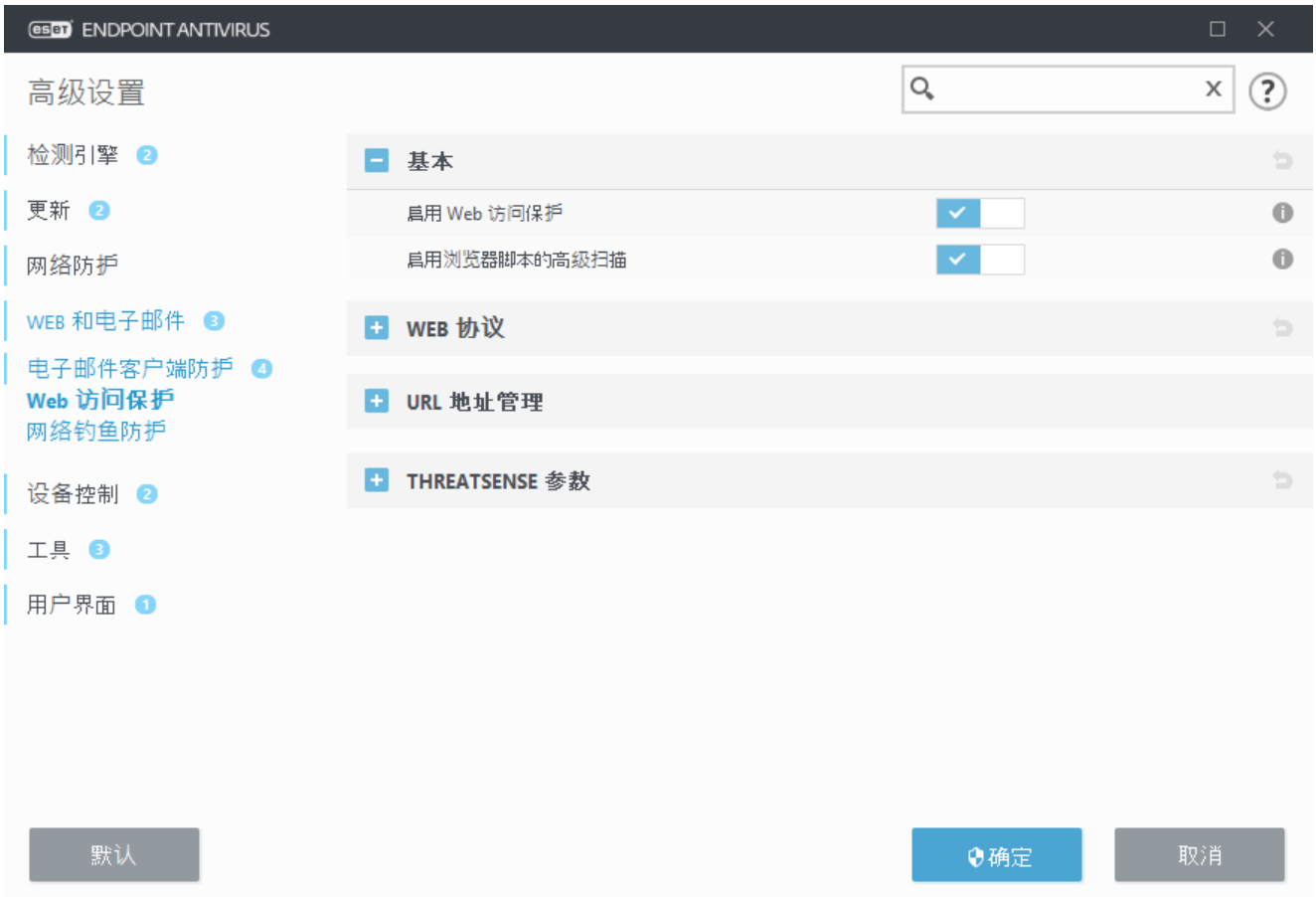


以下 ESET 知识库文章可能仅提供英文版：

- 在 ESET Endpoint Antivirus 中的单个工作站上取消阻止安全的网站

在**高级设置** (F5) > **Web 和电子邮件** > **Web 访问保护**中提供以下选项：

- **基本** – 通过高级设置启用或禁用此功能。
- **Web 协议** – 使您可以为大多数 Internet 浏览器使用的这些标准协议配置监控。
- **URL 地址管理** – 使您可以指定要对其阻止、允许或排除检查的 URL 地址。
- **ThreatSense 参数** – 高级病毒扫描程序设置 – 使您可以为 Web 访问保护配置设置，例如要扫描的对象类型（电子邮件、压缩文件等）、检测方法等。



Web 访问保护高级设置

在**高级设置** (F5) > **Web 和电子邮件** > **Web 访问保护** > **基本**中提供以下选项：

启用 Web 访问保护 – 如果禁用，则 Web 访问保护和网络钓鱼防护将无法运行。

启用浏览器脚本的高级扫描 – 如果启用，则 Web 浏览器执行的所有 JavaScript 程序都将由检测引擎进行检查。

我们强烈建议您保持启用 Web 访问保护。

Web 协议

默认情况下，ESET Endpoint Antivirus 将配置为监视由大部分 Internet 浏览器使用的 HTTP 协议。

HTTP 扫描程序设置

将始终监控所有应用程序的所有端口上的 HTTP 通信。

HTTPS 扫描程序设置

ESET Endpoint Antivirus 还支持 HTTPS 协议检查。HTTPS 通信使用加密通道在服务器和客户端之间传输信息。ESET Endpoint Antivirus 利用 SSL（安全套接字层）和 TLS（传输层安全）协议检查通信。无论操作系统版本如何，该程序将只在 **HTTPS 协议使用的端口**中定义的端口（443，0-65535）上扫描通信。

默认情况下，会扫描加密的通信。要查看扫描程序设置，请导航至“高级设置”部分的 SSL/TLS，依次单击 **Web 和电子邮件 > SSL/TLS**，然后启用**启用 SSL/TLS 协议过滤**选项。

URL 地址管理

URL 地址管理部分可使您指定要阻止、允许或排除内容扫描的 HTTP 地址。

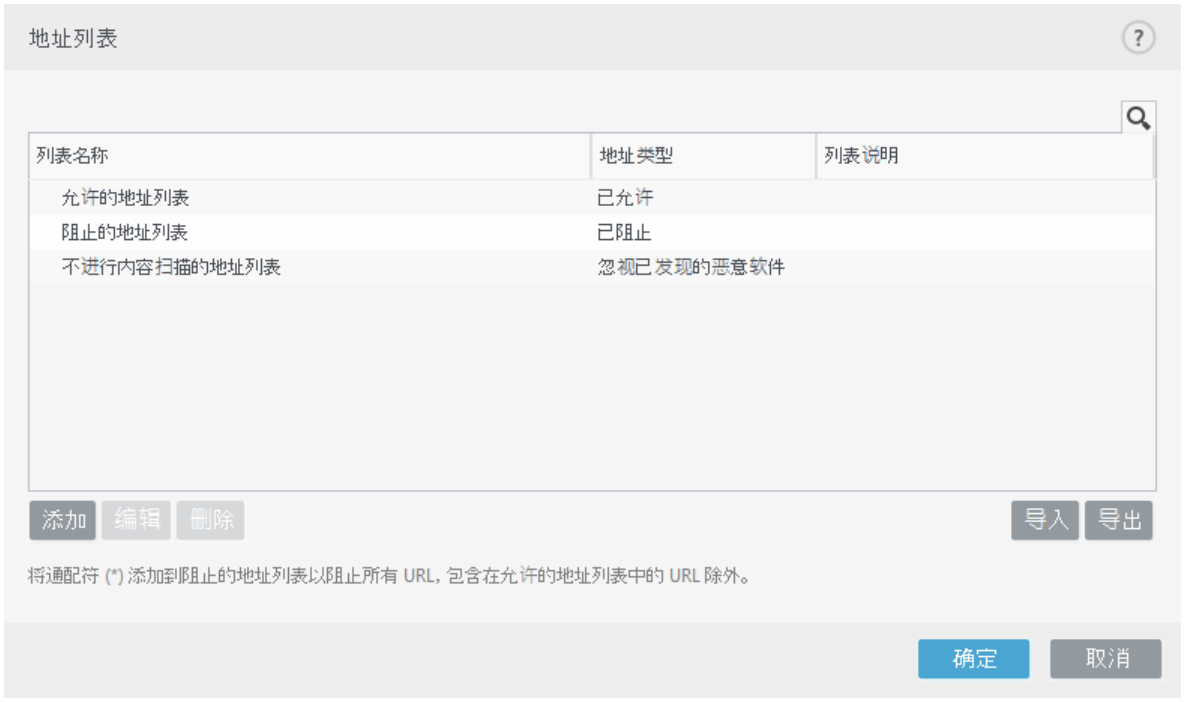
如果您在过滤 HTTP 网页之外还希望过滤 HTTPS 地址，则必须选中**启用 SSL/TLS 协议过滤**。 否则，将仅添加您访问过的 HTTPS 站点的域，而不会添加完整 URL。

将不能访问**阻止的地址列表**中的网站，除非它们还包含在**允许的地址列表**中。在访问时，不会针对**不进行内容扫描的地址列表**中的网站进行扫描以查找恶意代码。

如果您希望阻止所有 HTTP 地址（活动的**允许的地址列表**中存在的地址除外），请将 * 添加到活动的**阻止的地址列表**。

特殊符号 *（星号）和 ？（问号）可用于列表。 星号可以替代任意字符串，而问号可以替代任意符号。 指定排除的地址时，请务必谨慎，因为此列表只应包含信任的和安全的地址。 同样，必须确保在此列表中正确使用符号 * 和 ?。 有关如何安全匹配包括所有子域的整个域，请参阅添加 HTTP 地址/域掩码。 若要启用某个列表，请选择**启用列表**。 如果您希望在输入来自当前列表的地址时收到通知，请选择**应用时发送通知**。

> 如果设置 **Web 和电子邮件 > SSL/TLS > 排除与受信任域的通信**已启用，并且域被认为是受信任的，将不会过滤地址。



控件元素

添加 – 除了预定义的列表，创建新列表。 如果您希望按逻辑拆分不同的地址组，这非常有用。例如，一个阻止的地址列表可能包含外部公开黑名单中的地址，另一个阻止的地址列表可能包含您自己的黑名单，这可在保持您的黑名单不变的同时轻松更新外部列表。

编辑 – 修改现有列表。 使用此项添加或删除地址。

删除 – 删除现有列表。 仅适用于使用**添加**创建的列表，不适用于默认列表。

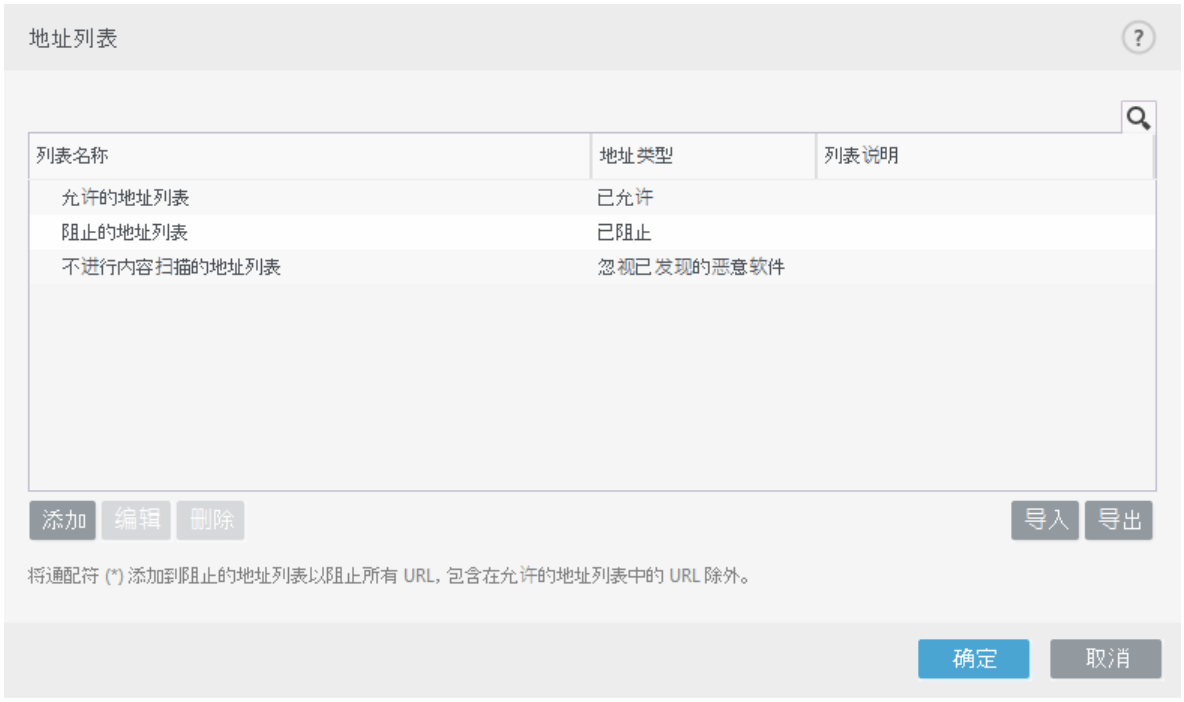
URL 地址列表

在此部分中，您可以指定将会被阻止、允许或从检查中排除的 HTTP 地址的列表。

默认情况下，有以下三种列表可供使用：

- **不进行内容扫描的地址列表** – 将不会对已添加至此列表的任何地址执行恶意代码检查。
- **允许的地址列表** – 如果启用了仅允许访问允许地址列表中的 HTTP 地址且阻止地址列表中包含 *（与所有地址相匹配），则将只允许用户访问此列表中指定的地址。允许该列表中的地址，即使这些地址包含在阻止地址列表中也是如此。
- **阻止的地址列表** – 将不允许用户访问此列表中指定的地址，除非这些地址还出现在允许的地址列表中。

单击**添加**以创建新的列表。若要删除选定列表，请单击**删除**。



以下 ESET 知识库文章可能仅提供英文版：
- 在 ESET Endpoint Antivirus 中的单个工作站上取消阻止安全的网站

有关详细信息，请参阅 URL 地址管理。

创建新的 URL 地址列表

此部分允许您指定将会被阻止、允许或从检查中排除的 URL 地址/掩码的列表。

在新建列表时，可配置以下选项：

地址列表类型 – 提供三种预定义列表类型：

- **不检查** – 不会对已添加至此列表的任何地址执行恶意代码检查。
- **已阻止** – 程序不会允许用户访问此列表中指定的地址。
- **已允许** – 如果您的策略配置为使用此功能，并且将通配符（*）值添加至该列表中，您将可以访问此列表中的地址，即使这些地址在阻止列表中也可访问。

列表名称 – 指定列表的名称。在编辑三个预定义列表之一时，此字段将不可用。

列表说明 – 键入简短的列表说明（可选）。在编辑三个预定义列表之一时，此字段将不可用。

列表活动 – 选择滑块来激活列表。

应用时发送通知 – 如果您希望在该列表用于评估您访问过的 HTTP 网站时收到通知，请选择该滑块。例如，在阻止或允许网站时将发出通知，因为网站包含在阻止或允许的地址列表中。通知将显示指定网站的列表的列表名称。

日志记录严重级别 – 从下拉菜单中选择日志记录严重级别。具有“警告”级别的记录可以由 ESET PROTECT 或 进行收集。

控件元素

添加 – 将新 URL 地址添加到列表（输入带有分隔符的多个值）。

编辑 – 修改列表中的现有地址。仅可用于使用**添加**创建的地址。

删除 – 删除列表中的现有地址。 仅可用于使用**添加**创建的地址。

导入 – 导入带有 URL 地址的文件（使用换行符分隔值，例如使用编码 UTF-8 的 *.txt）。

有关信息，请参阅如何添加 URL 掩码一章。

如何添加 URL 掩码

在输入需要的地址/域掩码之前，请参考此对话框中的说明。

ESET Endpoint Antivirus 允许用户阻止对指定网站的访问，并阻止 Internet 浏览器显示其内容。除此之外，它还允许用户指定应从检查中排除的地址。如果用户不知道远程服务器的完整名称，或想要指定整组远程服务器，可以使用所谓的掩码来标识这样的组。掩码包括符号“?”和“*”：

- 使用 ？来替代一个符号
- 使用 * 来替代一个文本字符串。

例如，*.c?m 适用于所有地址，其中，最后一部分以字母 c 开头，以字母 m 结尾，二者之间包含一个未知符号（“.com”、“.cam”等）。

例如，掩码 *x? 表示倒数第二个字符为“x”的任意地址。要匹配整个域，请以格式 *.domain.com/* 输入它。可以选择在掩码中指定协议前缀 *http://*、*https://*。如果省略，掩码将匹配任何协议。如果在域名的开头处使用，将特殊处理以“*.”开头的序列。首先，在本例中，“*”通配符不匹配斜杠字符（“/”）。这是为了避免绕过掩码，例如掩码 *.domain.com 将不匹配 *http://anydomain.com/anypath#.domain.com*（此类后缀可以附加到任何 URL，而不会影响下载）。第二，在此特殊案例中，“*.”还将匹配一个空字符串。这是为了能够使用单个掩码匹配包括任何子域在内的整个域。例如，掩码 *.domain.com 还匹配 *http://domain.com*。使用 *domain.com 是不正确的，因为它还会匹配 *http://anotherdomain.com*。

网络钓鱼防护

网络钓鱼这一术语是指利用社会工程学（操纵用户以获取机密信息）的一种犯罪活动。网络钓鱼通常用于获取敏感信息（如银行帐号、PIN 码等）的访问权限。在词汇表中阅读此活动的详细信息。ESET Endpoint Antivirus 包括网络钓鱼防护，用于阻止散布此类内容的已知网页。

我们强烈建议您启用 ESET Endpoint Antivirus 中的网络钓鱼防护。若要执行此操作，请打开**高级设置** (F5) 并导航至 **Web 和电子邮件 > 网络钓鱼防护**。

有关 ESET Endpoint Antivirus 中网络钓鱼防护的详细信息，请访问我们的知识库文章。

访问网络钓鱼网站

当访问已识别的网络钓鱼网站时，以下对话框将显示在您的 Web 浏览器中。如果您仍想要访问该网站，请单击**继续浏览此站点**（不建议）。

在默认情况下，白名单上列出的潜在网络钓鱼网站将在几小时后过期。要永久允许某一网站，可使用 URL 地址管理工具。通过**高级设置** (F5) 展开 **Web 和电子邮件 > Web 访问保护 > URL 地址管理> 地址列表**，并单击**编辑**，然后向该列表添加要编辑的网站。

报告网络钓鱼站点

报告链接使您能够向 ESET 报告网络钓鱼/恶意网站以供分析。

向 ESET 提交网站前，确保其满足以下一个或多个标准：
- 未检测到该网站；
- 该网站被错误地检测为威胁。在此情况下，您可以报告误报的网络钓鱼站点。

此外，也可以通过电子邮件提交网站。请将电子邮件发送至 samples@eset.com。请记住：邮件主题一定要描述清楚，邮件应包含尽可能多的有关此网站的信息（例如，从哪里引用了此网站，您是如何了解到它的等）。

更新程序

定期更新 ESET Endpoint Antivirus 是获取计算机最高安全级别的最佳方法。更新模块通过两种方式确保程序始终处于最新状态，即更新检测引擎和更新系统组件。程序激活后，默认自动执行更新。

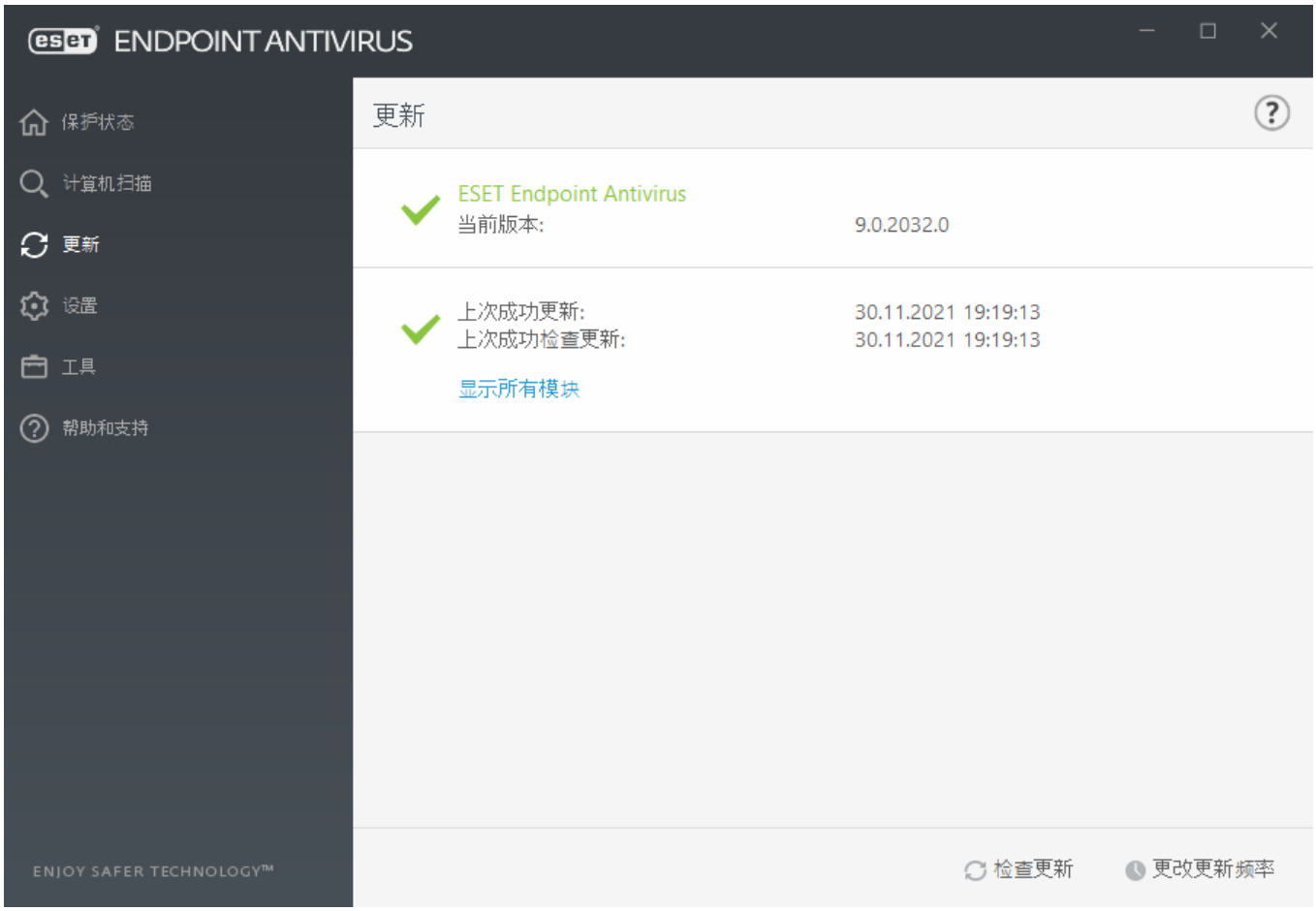
通过在主程序窗口中单击**更新**，可以查看当前更新状态，包括上一次成功更新的日期和时间以及是否需要更新。您还可以单击**显示所有模块**链接，打开已安装模块列表，查看模块版本和上一次

更新。

此外，还提供手动开始更新过程的选项**检查更新**。更新检测引擎和更新程序组件是维持全面防范恶意代码的重要组成部分。请注意其配置和操作。如果在安装期间没有输入许可证详细信息，可以在更新时通过单击**激活产品**输入许可证密钥以访问 ESET 的更新服务器。

如果在没有用户名和密码的情况下使用脱机许可证文件激活 ESET Endpoint Antivirus 并尝试更新，则红色信息**模块更新设备**指示您只能从镜像下载更新。

您的许可证密钥是在购买 ESET Endpoint Antivirus 后由 ESET 所提供的。



当前版本 – ESET Endpoint Antivirus 内部版本编号。

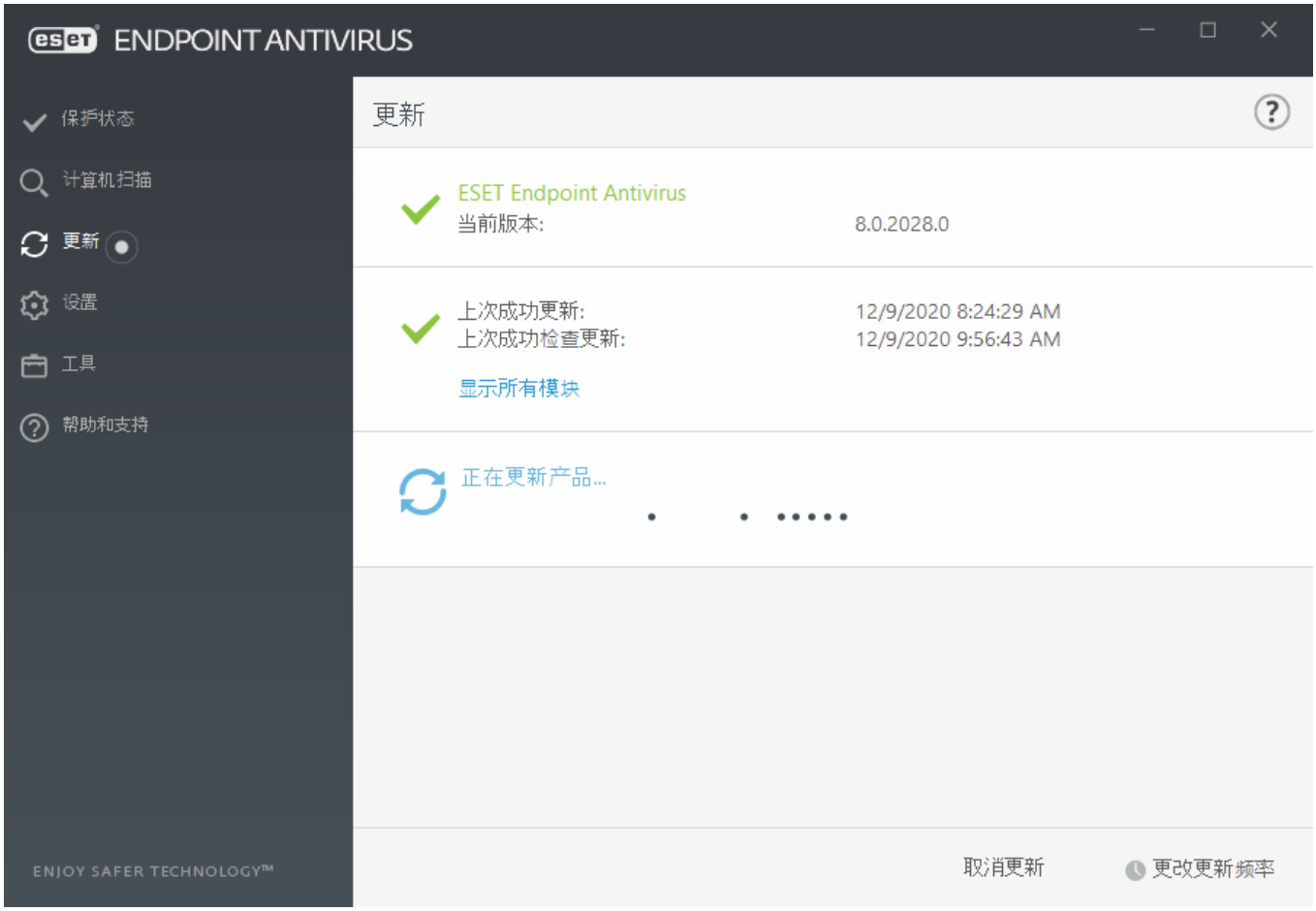
上次成功更新 – 上次成功更新的日期和时间。确保是最近日期，这表明检测引擎是最新的。

上次成功检查更新 – 上次成功尝试更新模块的日期和时间。

显示所有模块 – 单击该链接以打开已安装模块列表，查看模块版本和上一次更新。

更新过程

单击**检查更新**后，下载过程即开始。屏幕上会显示下载进度条和剩余时间。要中断更新，请单击**取消更新**。

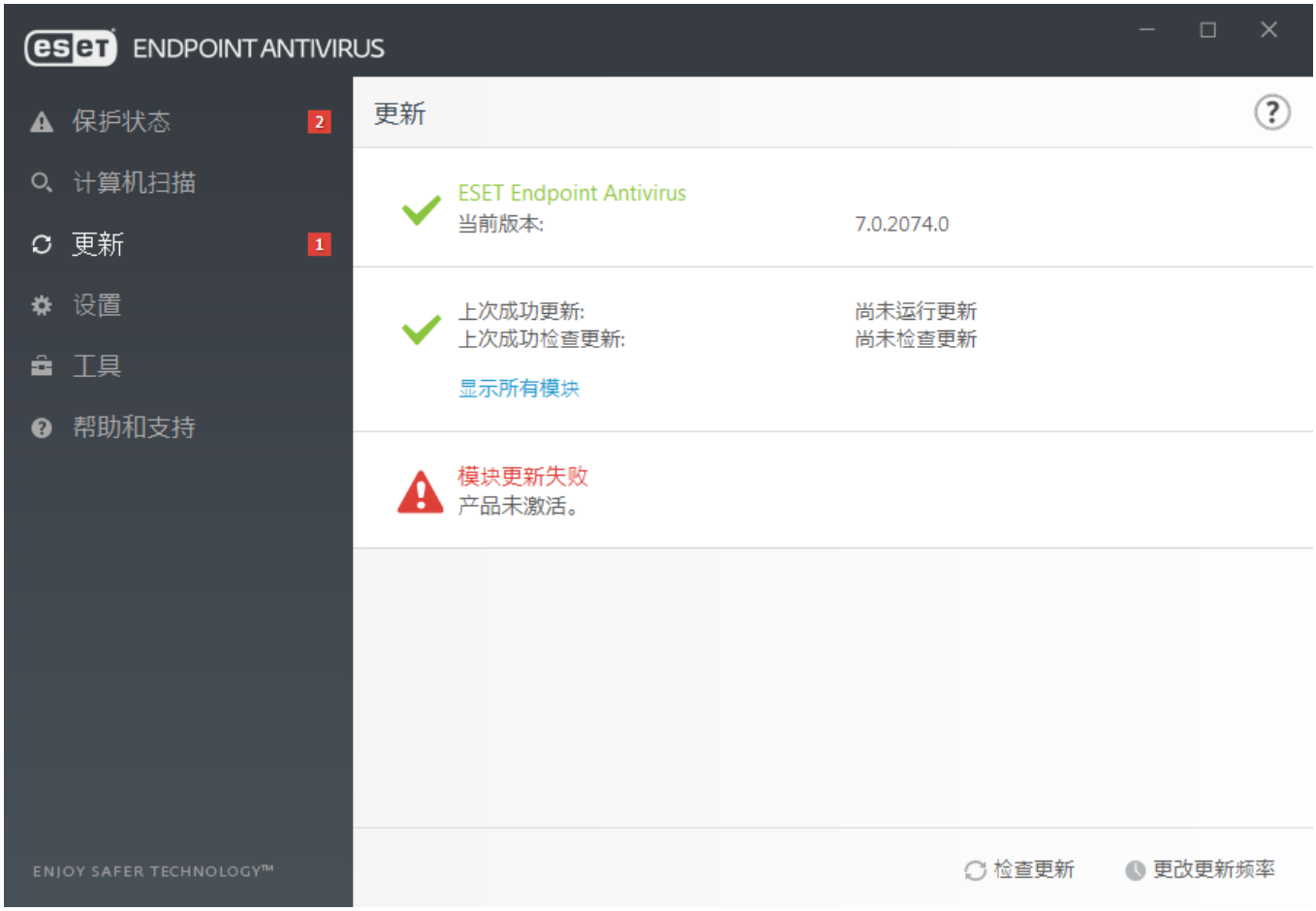


在正常情况下，模块每天更新若干次。如果不是这样，则表示程序不是最新的，并更易于遭感染。请尽快更新模块。

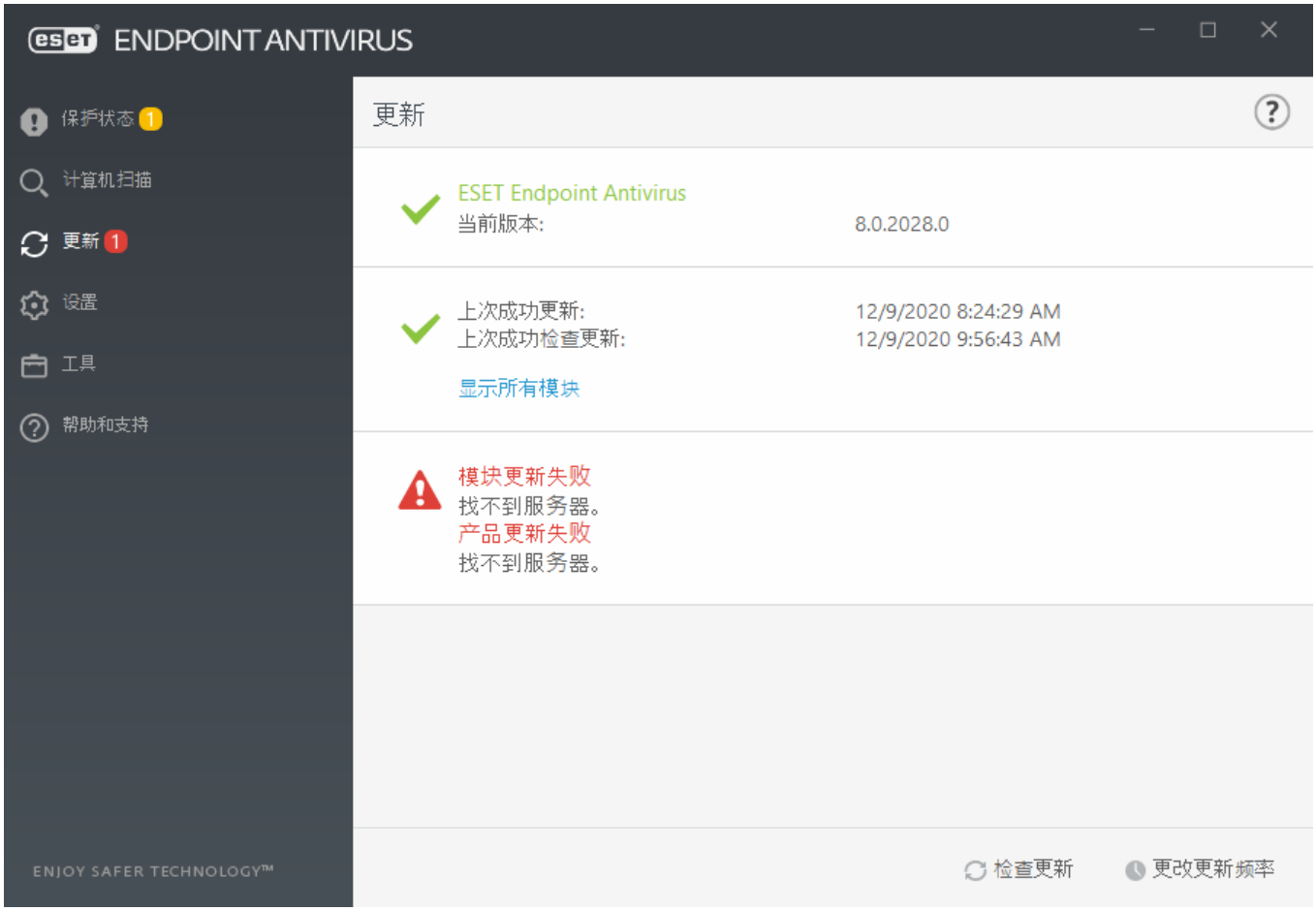
检测引擎已过期 – 此错误将在几次尝试更新模块失败之后显示。建议您检查更新设置。此错误的最常见原因是错误输入了身份验证数据或错误配置了连接设置。

以前的通知与下列有关不成功更新的两条**模块更新失败**消息相关：

1. **无效的许可证** – 在更新设置中输入的许可证密钥不正确。 建议您检查验证数据。 “高级设置”窗口（从主菜单中单击**设置**，然后单击**高级设置**，或按键盘上的F5）包含其他更新选项。从主菜单中单击**帮助和支持 > 更改许可证**以输入新的许可证密钥。



2. **下载更新文件时出错** – 此错误的原因可能是 Internet 连接设置不正确。建议您检查 Internet 连接（方法是在 Web 浏览器中打开任意网站）。如果网站不打开，很可能未建立 Internet 连接，或者计算机存在连接问题。请与 Internet 服务提供商 (ISP) 联系以确定您是否有活跃 Internet 连接。



有关详细信息，请访问此 ESET 知识库文章

更新设置

在**更新**下的**高级设置**树 (F5) 中，可以访问更新设置选项。此部分指定更新源信息，例如正在使用的更新服务器和这些服务器的验证信息。

为使更新正常下载，必须正确填写所有更新参数。如果使用防火墙，请确保您的 ESET 程序能与 Internet 通信（例如 HTTPS 通信）。

基本

当前使用的更新配置文件显示在**选择默认更新配置文件**下拉菜单中。

若要创建新的配置文件，请参阅配置文件部分。

配置更新通知 – 单击编辑以选择要显示的应用程序通知。可以选择通知在桌面上显示和/或通过电子邮件发送。

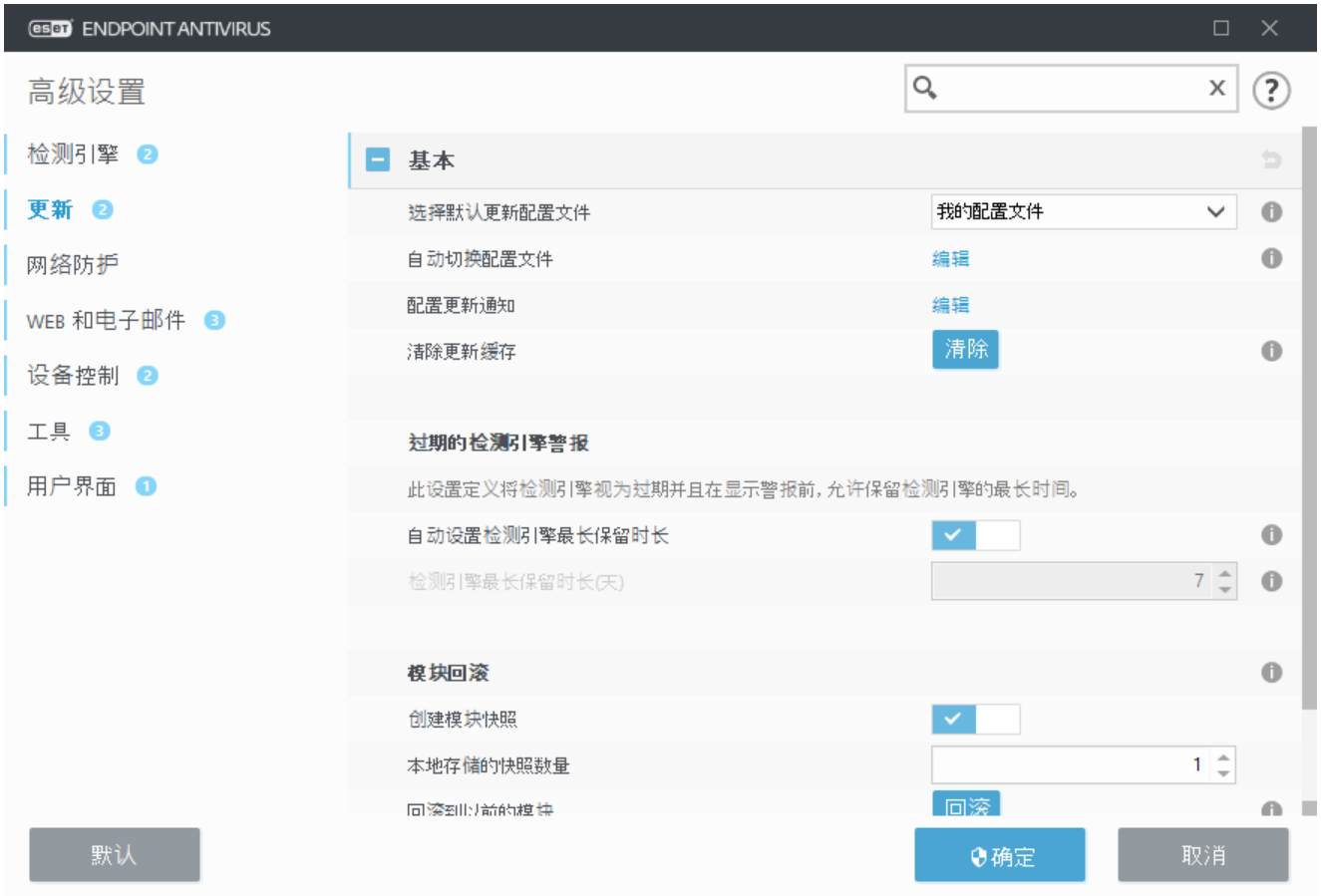
如果在尝试下载模块更新时遇到困难，请单击**清除更新缓存**旁边的**清除**，以清除临时更新文件/缓存。

过期的检测引擎警报

自动设置检测引擎最长保留时长 – 允许设置最长保留时长（以天为单位），在此之后检测引擎将报告为已过期。**检测引擎最长保留时长(天数)** 的默认值为 7。

模块回滚

如果怀疑新更新的检测引擎和/或程序模块可能不稳定或已损坏，可以回滚至以前版本并禁用更新一段时间。



配置文件

对于各种更新配置和任务，可以创建更新配置文件。创建更新配置文件对于移动用户（这些用户需要备用配置文件以用于定期更改的 Internet 连接属性）尤其有用。

选择要编辑的配置文件下拉菜单显示当前选定的配置文件，默认设置为**我的配置文件**。

若要创建新的配置文件，请单击**配置文件列表**旁边的**编辑**，输入您自己的**配置文件名称**，然后单击**添加**。

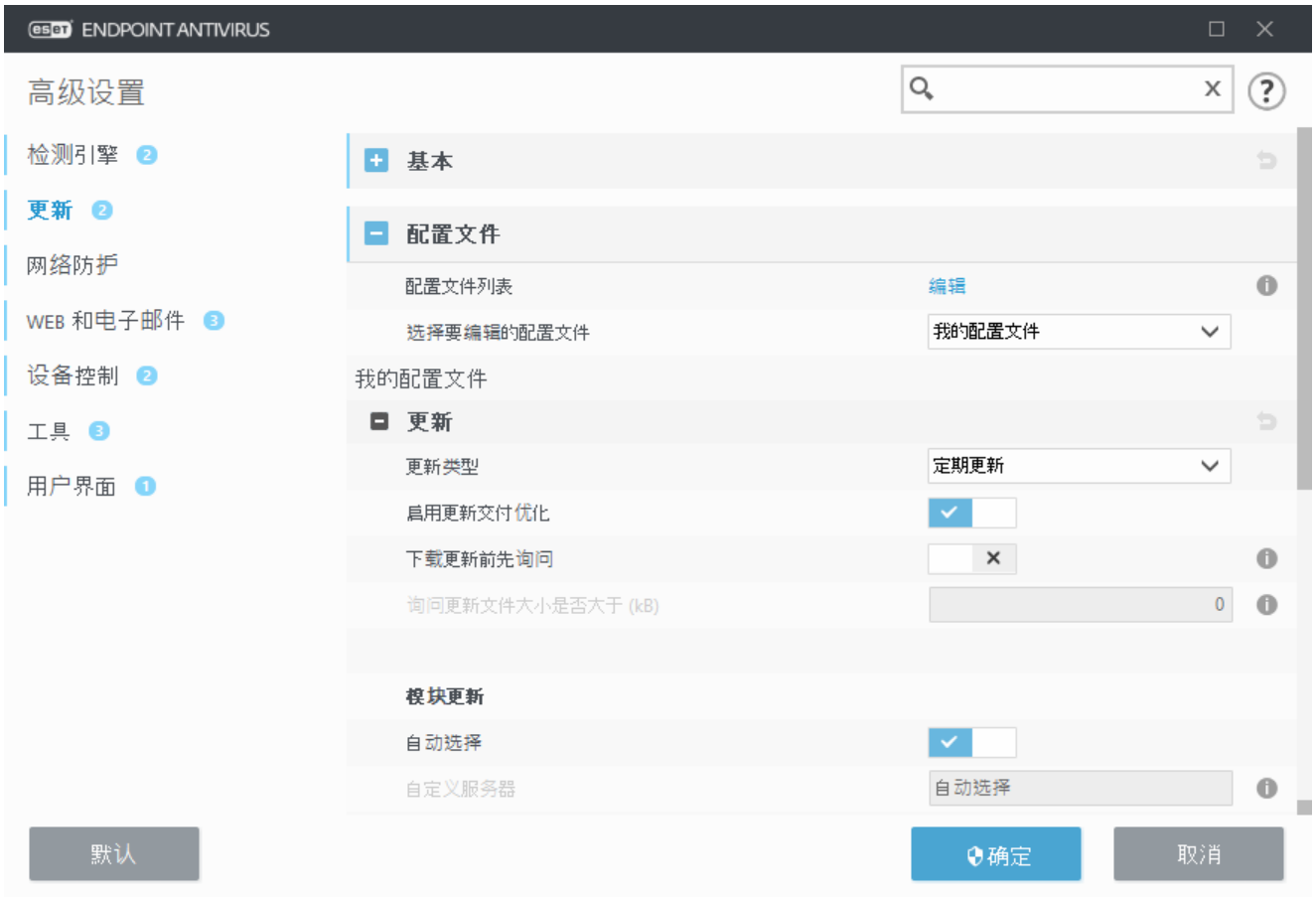
更新

默认情况下，更新类型设置为定期更新，以确保更新文件将以最小的网络流量从 ESET 服务器自动进行下载。预发布更新（预发布更新选项）是已经经过内部彻底测试的更新，将很快公开提供。您可以通过获得最新检测方法和修补程序，从启用预发布更新中获益。但是，预发布更新可能并

不始终稳定，不得在需要最大程度可用性和稳定性的生产服务器和工作站上使用。延迟更新允许从提供新版本病毒库的延迟至少 X 小时的特别更新服务器进行更新（即在真实环境中测试并因此视为稳定的数据库）。

启用更新交付优化 – 如果启用，则可以从 CDN（内容交付网络）下载更新文件。禁用此设置可能会在专用 ESET 更新服务器超载时导致下载中断和速度下降。当防火墙仅限于访问 ESET 更新服务器 IP 地址或与 CDN 服务的连接不工作时，禁用操作很有用。

下载更新前询问 – 程序将显示一条通知，可以在其中选择确认还是拒绝更新文件下载。如果更新文件大小大于在询问更新文件大小是否大于 (kB) 字段中指定的值，则程序将显示确认对话框。如果更新文件大小设置为 0 kB，则程序将始终显示确认对话框。



模块更新

默认启用**自动选择**选项。**自定义服务器**选项是存储更新的位置。如果使用 ESET 更新服务器，建议您保持选中默认选项。

启用更频繁的检测病毒库更新 – 检测病毒库将以更短的时间间隔进行更新。 禁用此设置可能会对检测速度产生负面影响。

允许从可移动磁盘进行模块更新 – 当可移动磁盘包含了创建的镜像时，允许您从该可移动磁盘更新。选中了自动后，将在后台运行更新。如果要显示更新对话框，请选中始终询问。

使用本地 HTTP 服务器（也称为“镜像”）时，更新服务器应进行如下设置：
http://计算机_名称_或_其_IP_地址:2221

使用启用 SSL 的本地 HTTP 服务器时，更新服务器应进行如下设置：
https://计算机_名称_或_其_IP_地址:2221

使用本地共享文件夹时，更新服务器应进行如下设置：
\\计算机_名称_或_其_IP_地址\共享_文件夹

上述示例中指定的 HTTP 服务器端口号取决于您 HTTP/HTTPS 服务器侦听的具体端口。

产品更新

请参阅产品更新。

连接选项

请参阅连接选项。

更新镜像

请参阅更新镜像。

更新回滚

如果您怀疑新的检测引擎更新或程序模块可能不稳定或已损坏，可以回滚至以前版本并暂时禁用更新。或者，还可以启用先前禁用的更新（如果曾将其无限期推迟）。

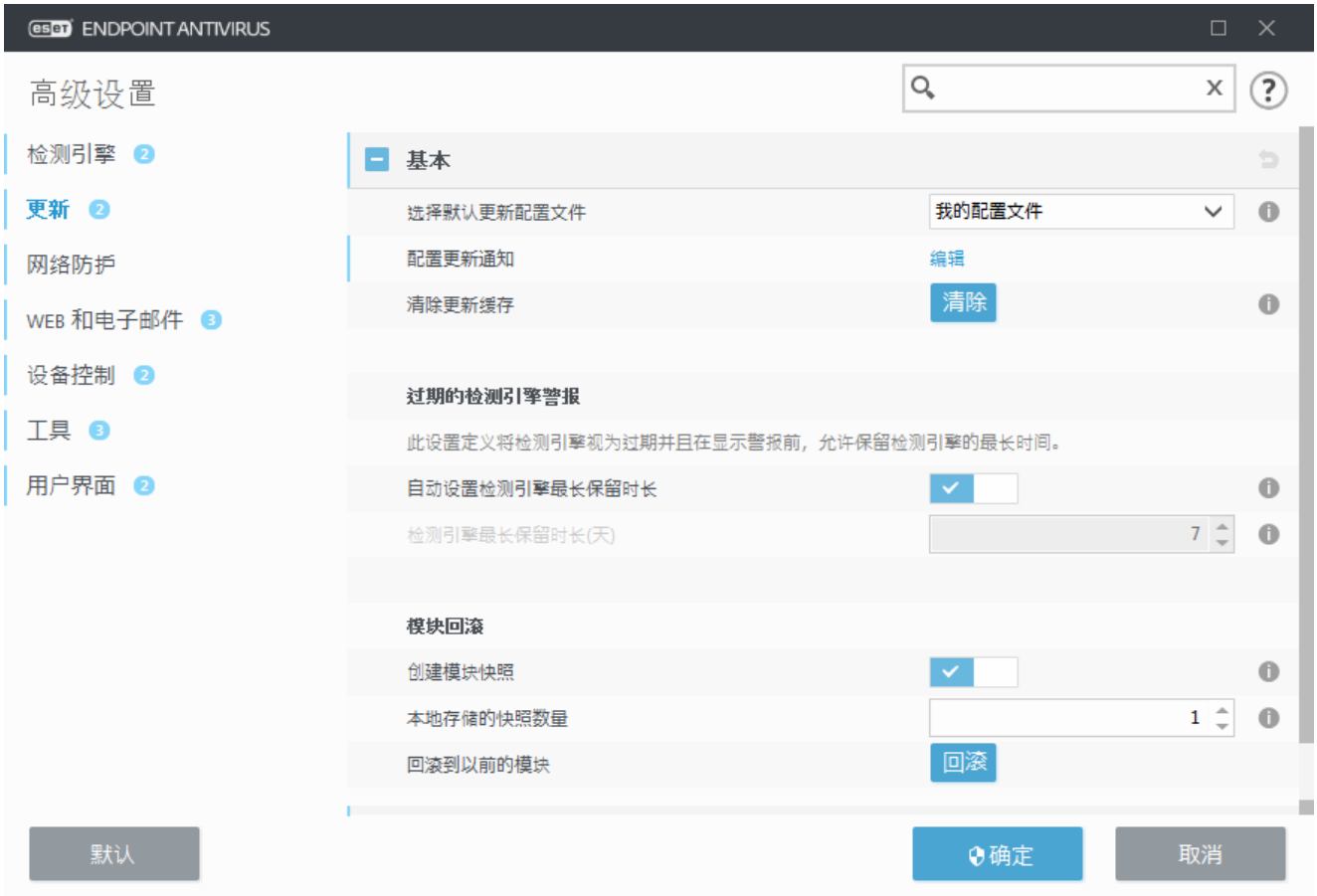
ESET Endpoint Antivirus 会记录检测引擎和程序模块的快照，以用于回滚功能。要创建病毒库快照，请保持**创建模块快照**处于启用状态。如果**创建模块快照**已启用，则会在第一次更新期间创建第一个快照。将在 48 小时后创建下一个快照。**本地存储的快照数量**字段定义存储的检测引擎快照的数量。

当达到最大快照数量（例如，三个）时，最旧的快照将每 48 小时替换为新的快照。ESET Endpoint Antivirus 会将检测引擎和程序模块更新版本回滚至最旧的快照。

如果单击**回滚**（**高级设置** (F5) > **更新** > **基本** > **模块回滚**），则必须从**持续时间**下拉菜单中选择时间间隔。

选择**直到调用**可将常规更新无限期推迟，直到您手动恢复更新功能。因为它具有潜在安全风险，我们不建议选择此选项。

如果执行回滚，**回滚**按钮会更改为**允许更新**。不允许在**暂停更新**下拉菜单中选择的时间间隔内的任何更新。检测引擎版本将降级至最旧可用版本，并作为快照存储在本地计算机文件系统中。



假定 22700 是最新的检测引擎版本号，并且 22698 和 22696 作为检测引擎快照存储。在此示例中，计算机在 22697 更新过程中关机，并且在下载 22697 之前已有较新版本的更新可用。如果**本地存储的快照数量**字段为 2 并单击**回滚**，则检测引擎（包括程序模块）将恢复为版本号 22696。此过程可能需要一些时间。在更新屏幕上验证检测引擎版本是否已降级。

产品更新

产品更新部分包含与产品更新相关的选项。该程序使您能够预定义其在新产品更新可用时的行为。

产品更新会带来新功能，或对以前版本中已存在的功能进行更改。可以无需用户介入而自动执行更新，也可以选择获取通知。产品更新安装完毕后，可能需要重新启动计算机。

自动更新 – 使用其他网络或按流量计费的连接与 Internet 连接时，暂停特定更新配置文件的自动更新会暂时禁用产品自动更新。将此设置保持处于启用状态，以实现对最新功能的持续访问并获得可能的最高保护。有关自动更新的详细信息，请参阅自动更新常见问题解答

默认情况下，从 ESET 存储库服务器下载产品更新。在大型或脱机环境中，可以分发流量以允许内部缓存产品文件。

- 为程序组件更新定义自定义服务器

1.在**自定义服务器**字段中定义产品更新的路径。
它可以是 HTTP(S) 链接、SMB 网络共享路径、本地磁盘驱动器或可移动磁盘路径。对于网络驱动器，请使用 UNC 路径，而不是使用映射的驱动器号。
2.将**用户名**和**密码**留空（如果不需要）。
如果需要，请在此处为自定义 Web 服务器上的 HTTP 身份验证定义相应的凭据。
3.确认更改，然后使用标准 ESET Endpoint Antivirus 更新来测试产品更新是否存在。

i 最适合选项的选择取决于将应用这些设置的工作站。请注意，工作站和服务器之间存在区别，例如产品更新后自动重新启动服务器可能会对您的公司造成重大损害。

连接选项

若要访问给定更新配置文件的代理服务器设置选项，请单击**高级设置**树 (F5) 中的**更新**，然后依次单击**配置文件 > 更新 > 连接选项**。

代理服务器

单击**代理模式**下拉菜单，然后选择以下三个选项之一：

- 不使用代理服务器
- 通过代理服务器连接
- 使用全局代理服务器设置

选择**使用全局代理服务器设置**可使用“高级设置”树的**工具 > 代理服务器**分支中已经指定的代理服务器配置选项。

选择**不使用代理服务器**可指定不使用代理服务器来更新 ESET Endpoint Antivirus。

在以下情况下应选择**通过代理服务器连接**选项：

- 将使用不同于工具 > **代理服务器**中定义的代理服务器来更新 ESET Endpoint Antivirus。在此配置中，应在**代理服务器**地址中指定新代理的信息、通信**端口**（默认为 3128）以及代理服务器的**用户名**和**密码**（如果需要）。
- 代理服务器设置不会全局设置，但 ESET Endpoint Antivirus 将连接到代理服务器以进行更新。
- 您的计算机通过代理服务器连接到 Internet。这些设置是在安装程序时从 Internet Explorer 获取的，但是如果设置发生更改（例如，如果您更改 ISP），请确保在此窗口中列出的代理设置正确。 否则程序将无法连接到更新服务器。

代理服务器的默认设置为**使用全局代理服务器设置**。

如果代理不可用，请使用直接连接 – 如果代理不可访问，将在更新期间绕过代理。

Windows 共享

从运行 Windows NT 版本操作系统的本地服务器更新时，默认需要对每个网络连接进行验证。

若要配置此类帐户，请在**用以下身份连接到局域网**下拉菜单中选择：

- **系统帐户(默认)**
- **当前用户**
- **指定的用户**

选择**系统帐户(默认)**以使用系统帐户进行验证。通常，如果主更新设置部分不提供验证数据，则不会进行验证。

若要确保程序使用当前登录的用户帐户验证，请选择**当前用户**。此解决方案的缺点在于，如果当前没有用户登录，则程序将无法连接到更新服务器。

如果希望程序使用特定用户帐户进行验证，请选择**指定用户**。当默认系统帐户连接失败时使用此方式。请注意，指定用户帐户必须有权访问本地服务器上的更新文件目录。否则，程序将无法建立连接并下载更新。

用户名和**密码**设置是可选项。

选择**当前用户**或**指定用户**后，如果将程序身份更改为所需用户，可能发生错误。我们建议在主更新设置部分中输入局域网验证数据。在此更新设置部分中，应按如下所示输入验证数据：*domain_name\user*（如果是工作组，请输入 *workgroup_name\name*）和密码。从本地服务器的 HTTP 版本更新时，无需验证。

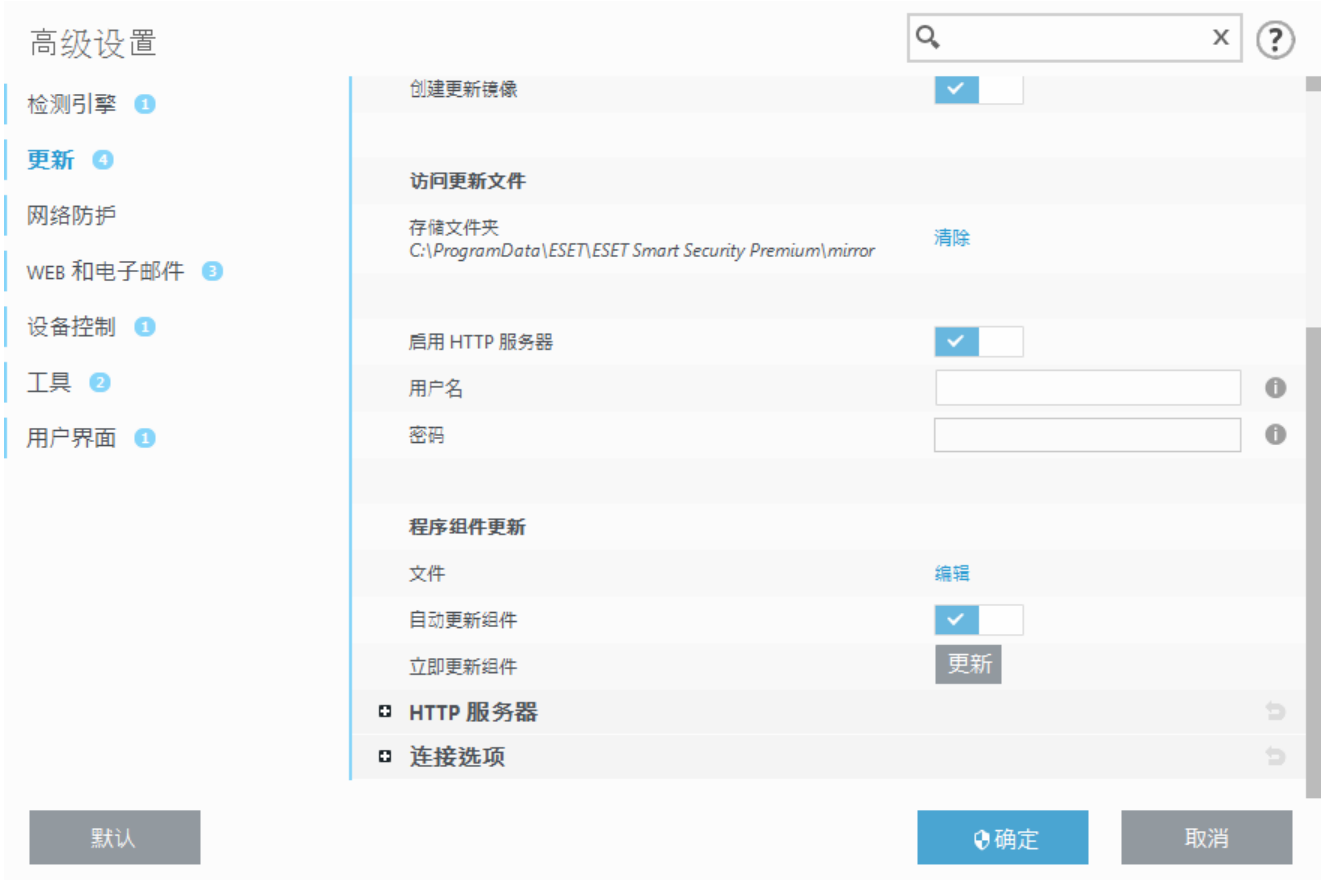
如果在更新下载后仍与服务器保持连接，则在更新后选择与服务器**断开连接**以强制断开连接。

更新镜像

ESET Endpoint Antivirus 允许您创建更新文件的副本，可用于更新位于网络中的其他工作站。使用“镜像” – 在 LAN 环境中复制更新文件很方便，因为更新文件不需要通过每台工作站从供应商更新服务器反复下载。可将更新下载到本地镜像服务器，然后分发给所有工作站，以避免网络流量过载风险。从镜像更新客户端工作站可优化网络负载平衡，并节约 Internet 连接带宽。

要最大程度地减少使用 ESET PROTECT 管理大量客户端的网络上的 Internet 通信，建议您使用 Apache HTTP 代理，而不是将客户端配置为镜像。可以使用一体式安装程序将 Apache HTTP 代理与 ESET PROTECT 一起安装，也可以作为独立组件安装。有关 Apache HTTP 代理、镜像工具和直接连接的更多信息及其之间的差异，请参阅我们的 ESET PROTECT 联机帮助页面

本地镜像服务器的配置选项位于**更新**下的“高级设置”中。要访问此部分，请按 **F5** 以访问“高级设置”，依次单击**更新 > 配置文件并选择更新镜像**选项卡。



若要在客户端工作站上创建镜像，请启用**创建更新镜像**。启用此选项后，将激活其他镜像配置选项，例如访问更新文件的方式和镜像文件的更新路径。

访问更新文件

启用 HTTP 服务器 – 如果启用，则更新文件可以通过 HTTP 访问，而无需提供凭据。

在从镜像更新中详细描述了访问镜像服务器的方法。有两种访问镜像的基本方法 – 具有更新文件的文件夹可以表示为共享网络文件夹，或者客户端可以访问位于 HTTP 服务器上的镜像。

用于为镜像存储更新文件的文件夹在**存储镜像文件的文件夹**下定义。若要选择其他文件夹，请单击**清除**以删除预定义的文件夹 *C:\ProgramData\ESET\ESET Endpoint Antivirus\mirror*，然后单击**编辑**以浏览到本地计算机上的文件夹或共享网络文件夹。如果需要对指定文件夹的授权，则必须在**用户名**和**密码**字段中输入验证数据。如果选定的目标文件夹位于运行 Windows NT/2000/XP 操作系统的网络磁盘上，则指定的用户名和密码必须对选定的文件夹有写权限。用户名和密码应按照*域/用户*或*工作组/用户*的格式输入。请记住提供相应密码。

用于镜像的 HTTP 服务器和 SSL

在**镜像**选项卡的 **HTTP 服务器**部分中，可以指定 HTTP 服务器将侦听的**服务器端口**，以及 HTTP 服务器所使用的**身份验证**类型。默认情况下，服务器端口设置为 **2221**。

验证 – 定义用于访问更新文件的验证方法。有以下选项可供使用：**无**、**基本**和 **NTLM**。选择**基本**以使用 base64 编码进行基本用户名和密码验证。**NTLM** 选项提供使用安全编码方法的编码。对于验证，将使用在共享更新文件的工作站上创建的用户。默认设置为**无**，此设置授予对更新文件

的访问权，无需验证。

用户名和**密码**等身份验证数据仅用于访问镜像 HTTP 服务器。仅当用户名和密码必填时，才会填写这些字段。

添加您的**证书链文件**，或者如果您要运行具有 HTTPS (SSL) 支持的 HTTP 服务器，也可以生成自签名证书。以下**证书类型**可用：ASN、PEM 和 PFX。若要获得更高的安全性，可以使用 HTTPS 协议来下载更新文件。几乎无法跟踪使用此协议的数据传输和登录凭据。默认情况下，**私人密钥类型**将设置为**已集成**（因此默认禁用**私人密钥文件**选项）。这意味着私人密钥是所选证书链文件的一部分。

HTTPS 镜像的自签名证书
如果使用的是 HTTPS 镜像服务器，则需要将其证书导入到所有客户端计算机上受信任的根存储中。请参阅在 Windows 中安装受信任的根证书。

从镜像更新

有两种配置镜像的基本方法，该镜像实质上是一个存储库（客户端可在其中下载更新文件）。具有更新文件的文件夹可以表示为共享网络文件夹或 HTTP 服务器。

使用内部 HTTP 服务器访问镜像

这是在预定义的程序配置中指定的默认配置。若要允许使用 HTTP 服务器访问镜像，请依次导航到**高级设置 > 更新 > 配置文件 > 更新镜像**，然后选择**创建更新镜像**。

在**镜像**选项卡的 **HTTP 服务器**部分中，可以指定 HTTP 服务器将侦听的**服务器端口**，以及 HTTP 服务器所使用的**身份验证**类型。默认情况下，服务器端口设置为 **2221**。

验证 – 定义用于访问更新文件的验证方法。有以下选项可供使用：**无**、**基本**和 **NTLM**。选择**基本**以使用 base64 编码进行基本用户名和密码验证。**NTLM** 选项提供使用安全编码方法的编码。对于验证，将使用在共享更新文件的工作站上创建的用户。默认设置为**无**，此设置授予对更新文件的访问权，无需验证。

如果您希望允许通过 HTTP 服务器访问更新文件，镜像文件夹必须和创建它的 ESET Endpoint Antivirus 实例位于同一计算机上。

在几次尝试从镜像更新失败之后，将在主菜单的“更新”窗格中显示**用户名和/或密码无效**错误。建议您导航到**高级设置 > 更新 > 配置文件 > 更新镜像**并检查用户名和密码。此错误的最常见原因是输入的身份验证数据不正确。

配置镜像服务器后，您必须在客户端工作站上添加新的更新服务器。要执行该操作，请遵循以下步骤：

- 访问**高级设置** (F5)，然后依次单击**更新 > 配置文件 > 更新 > 模块更新**。
- 取消**自动选择**并采用以下格式之一将新服务器添加到**更新服务器**字段：
http://IP_address_of_your_server:2221

https://IP_address_of_your_server:2221 （如果使用 SSL）

通过系统共享访问镜像

首先，应在本地或网络设备上创建共享文件夹。为镜像创建文件夹时，必须为将更新文件保存到文件夹的用户提供“写入”权限，为所有将从镜像文件夹更新 ESET Endpoint Antivirus 的用户提供“读取”权限。

接下来，在**高级设置 > 更新 > 配置文件 > 更新镜像**选项卡中通过禁用**启用 HTTP 服务器**，来配置对镜像的访问。程序安装包中默认启用此选项。

如果共享文件夹位于网络中的另一台计算机上，则必须输入身份验证数据才能访问其他计算机。要输入身份验证数据，请打开 ESET Endpoint Antivirus **高级设置 (F5)**，然后依次单击**更新 > 配置文件 > 更新 > 连接选项 > Windows 共享 > 用以下身份连接到局域网**。如用以下身份连接到局域网部分中所述，此设置与用于更新的设置相同。

若要访问镜像文件夹，需要在用于登录其上创建镜像的计算机的相同帐户下进行操作。如果计算机位于域中，则应使用“domain\user”用户名。如果计算机不在域中，则应使用“IP_address_of_your_server\user”或“hostname\user”。

完成镜像配置后，在客户端工作站上使用以下步骤将 *\\UNC\PATH* 设置为更新服务器：

1.打开 ESET Endpoint Antivirus **高级设置**，然后依次单击**更新 > 配置文件 > 更新**。

2.取消**模块更新**旁边的**自动选择**，然后采用 *\\UNC\PATH* 格式将新服务器添加到**更新服务器**字段。

为使更新正常工作，镜像文件夹的路径必须指定为 UNC 路径。从映射驱动器进行的更新可能无法工作。

使用镜像工具创建镜像
镜像工具创建的文件夹结构不同于 Endpoint 镜像。每个文件夹都包含一组产品的更新文件。需要在使用镜像的产品更新设置中指定指向正确文件夹的完整路径。
例如，要从镜像更新 ESET PROTECT，请将更新服务器设置为（根据 HTTP 服务器根位置）：
`http://your_server_address/mirror/eset_upd/era6`

最后一个部分控制程序组件 (PCU)。默认情况下，已下载的程序组件将准备复制到本地镜像。如果**产品更新**处于激活状态，则无需单击**更新**，因为当文件可用时将自动复制到本地镜像。有关产品更新的详细信息，请参阅更新模式。

镜像更新问题故障排除

在大多数情况下，在从镜像服务器更新的过程中发生的问题可能因以下一种或多种情况引起：错误地指定镜像文件夹选项，镜像文件夹验证数据不正确，尝试从镜像下载更新文件的本地工作站上的配置不正确，或以上原因的综合。下面我们简要介绍在从镜像更新的过程中可能发生的最常见问题：

连接到镜像服务器时 ESET Endpoint Antivirus 报告错误 – 可能因错误地指定本地工作站从

中下载更新的更新服务器（镜像文件夹的网络路径）引起。要验证文件夹，请单击 Windows **开始**菜单、单击**运行**、输入文件夹名称并单击**确定**。应显示文件夹的内容。

ESET Endpoint Antivirus 需要用户名和密码 – 可能因在更新部分中输入了错误的验证数据（用户名和密码）引起。用户名和密码用于授予对更新服务器的访问权，程序将从更新服务器自行更新。确保验证数据正确并以正确格式输入。例如，域/用户名或工作组/用户名，再加上相应的密码。如果镜像服务器可供“所有人”访问，请注意，这并不意味着向任何用户授予访问权限。“所有人”不意味着任何非授权用户，它仅表示文件夹可供所有域用户访问。因此，如果文件夹可供“所有人”访问，仍需要在更新设置部分中输入域用户名和密码。

连接到镜像服务器时 ESET Endpoint Antivirus 报告错误 – 定义用于访问 HTTP 版镜像的端口上的通信被阻止。

ESET Endpoint Antivirus 在下载更新文件时报告错误 – 可能因错误地指定本地工作站从其中下载更新的更新服务器（镜像文件夹的网络路径）引起。

如何创建更新任务

更新可以手动触发，方法是在主菜单中单击**更新**后，在显示的主窗口中单击**检查更新**。

更新还可以作为计划任务运行。若要配置计划任务，请单击**工具 > 计划任务**。默认情况下，在 ESET Endpoint Antivirus 中会启用以下任务：

- **定期自动更新**
- **拨号连接后自动更新**
- **用户登录后自动更新**

可以修改每个更新任务以满足您的需要。除了默认更新任务外，您还可以使用用户定义的配置创建新更新任务。有关创建和配置更新任务的更多详细信息，请参阅计划任务。

工具

工具菜单包含的模块可帮助简化程序管理并为高级用户提供更多选项。

此菜单包括下列工具：

- 日志文件
- 安全报告（适用于非托管端点）
- 运行进程（如果 ESET LiveGrid® 已在 ESET Endpoint Antivirus 中启用）
- 查看活动
- 计划任务

• ESET SysInspector

• ESET SysRescue Live – 将您重定向到 ESET SysRescue Live 网站，可以在其中下载 ESET SysRescue Live .iso CD/DVD 映像。

• 隔离区

• 提交样本以供分析 – 允许您将要分析的可疑文件提交给 ESET 研究实验室（根据 ESET LiveGrid® 的配置，可能无法提交）。

日志文件

日志文件包含所有已发生的重要程序事件的信息，并提供检测到的威胁的概要信息。日志是系统分析、威胁检测以及故障排除的必要工具。日志记录在后台主动执行，无需用户交互。对信息的记录是根据当前日志级别设置进行的。可直接从 ESET Endpoint Antivirus 环境查看文本消息和日志。还可压缩日志文件。

日志文件可从主程序窗口中访问，方法是单击**工具 > 日志文件**。从**日志**下拉菜单选择所需日志类型。可用日志包括：

• **检测** – 此日志提供有关检测和由 ESET Endpoint Antivirus 模块检测到的渗透的详细信息。该信息包括检测时间、检测名称、位置、执行的操作以及检测到渗透时登录用户的名称。双击任何日志条目可在单独窗口中显示其详细信息。未清除的渗透始终以浅红色背景的红色文字进行标记，已清除的渗透以白色背景的黄色文字进行标记。未清除的 PUA 或潜在不安全的应用程

序以白色背景的黄色文字进行标记。

• **事件** - ESET Endpoint Antivirus 执行的所有重要操作都记录在事件日志中。事件日志包含有关程序中发生的事件和错误的信息。它旨在帮助系统管理员和用户解决问题。通常这里找到的信息可以帮助您找到程序中所发生问题的解决方案。

• **计算机扫描** – 所有扫描结果显示在此窗口中。每一行对应一个计算机控件。双击任意条目以查看相应扫描的详细信息。

• **阻止的文件** – 包含在连接到 ESET Enterprise Inspector 时无法访问的已阻止文件的记录。该协议显示阻止文件的理由和源模块，以及执行该文件的应用程序和用户。有关详细信息，请参阅 ESET Enterprise Inspector 联机用户指南。

• **已发送的文件** – 包含已发送到 ESET LiveGrid® 或 ESET LiveGuard 以供分析的文件的记录。

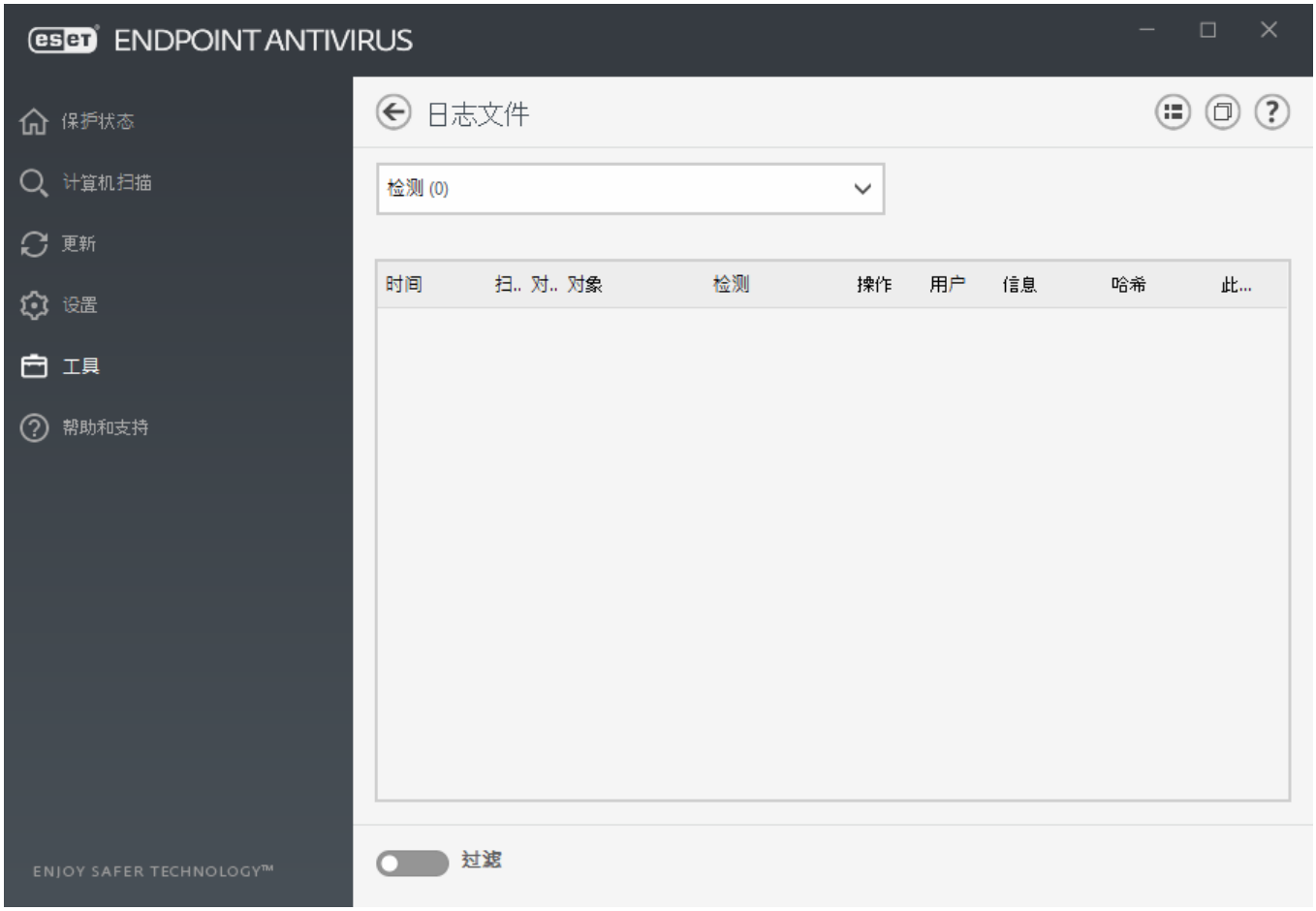
• **审核日志** – 每个日志包含有关执行更改的日期和时间、更改类型、描述、来源和用户的信息。有关更多详细信息，请参阅审核日志。

• **HIPS** – 包含特定规则的记录，这些规则标记为用于记录。该协议显示调用操作的应用程序、结果（无论已允许还是已禁止规则）以及所创建的规则的名称。

• **网络保护** – 防火墙日志显示由网络攻击防护检测到的所有远程攻击。 您可以在这里找到计算机上所有攻击的信息。事件列可列出检测到的攻击。来源列提供关于攻击者的更多信息。协议列说明了攻击使用的通信协议。对防火墙日志的分析有助于及时检测到系统渗透尝试，以防止对系统进行未授权访问。有关特定网络攻击的更多详细信息，请参见 IDS 和高级选项。

• **已过滤的网站** – 此列表可用于查看被 Web 访问保护阻止的网站的列表。 在这些日志中，您可以查看时间、URL、用户和打开了到特定网站的连接的应用程序。

• **设备控制** – 包含与计算机连接的可移动磁盘或设备的记录。只有具有设备控制规则的设备才会记录到日志文件。如果规则不匹配连接的设备，则不会创建所连接设备的日志条目。您还可以在这里找到设备类型、序列号、供应商名称和磁盘大小（如果可用）等详细信息。



选择任何日志的内容，然后按 Ctrl + C **将它复制到剪贴板**。按住 Ctrl + Shift 可选择多个条目。

单击 **过滤**以打开日志过滤窗口，您可以在该窗口中定义过滤条件。

右键单击指定的记录来打开右键菜单。 右键菜单中提供以下选项：

- **显示** – 在新窗口中显示有关选中日志的更多详细信息。
- **过滤相同记录** – 激活此过滤器后，您将仅看到相同类型的记录（诊断、警告...）。
- **过滤** – 在单击此选项后，日志过滤窗口将允许您为特定日志条目定义过滤条件。
- **启用过滤器** – 激活过滤器设置。
- **禁用过滤器** – 清除所有过滤器设置（如上文所述）。
- **复制/全部复制** – 复制有关窗口中所有记录的信息。
- **删除/全部删除** – 删除选定记录或显示的所有记录 – 此操作需要管理员权限。
- **导出** – 以 XML 格式导出有关记录的信息。
- **全部导出** – 以 XML 格式导出有关所有记录的信息。
- **查找/查找下一个/查找上一个** – 在单击此选项后，可以使用日志过滤窗口来定义过滤条件，

以亮显特定条目。

- **创建排除** – 使用向导创建新的检测排除（不适用于恶意软件检测）。

日志过滤

单击 **过滤**（在**工具 > 日志文件**）可定义过滤条件。

“日志过滤”功能可帮助您查找所需信息，尤其是在有许多记录时。它让您可以缩小日志记录范围（例如，如果要查找特定类型的事件、状态或时段）。可以通过指定特定搜索选项来过滤日志记录，从而仅相关记录（根据上述搜索选项）将显示在日志文件窗口中。

在**查找文本**字段中键入要搜索的关键字。使用**在列中搜索**下拉菜单，来缩小搜索范围。从**记录日志类型**下拉菜单中选择一条或多条记录。定义要显示其结果的**时段**。还可以使用其他搜索选项，例如**全字匹配**或 **区分大小写**。

查找下一个

键入字符串（单词或单词的一部分）。仅显示包含此字符串的记录。其他记录将忽略。

在列中搜索

选择搜索时要考虑使用的列。可以选中一个或多个要用于搜索的列。

记录类型

从下拉菜单中选择一个或多个日志记录类型：

- **诊断** – 记录微调程序所需的信息和以上所有记录。
- **信息性** – 记录包括成功更新消息及以上所有记录在内的信息性消息。
- **警告** – 记录严重错误和警告消息。
- **错误** – 将记录类似“下载文件时出错”等错误和严重错误。
- **严重** – 仅记录严重错误（启动病毒防护

时段

定义想要显示其结果的时段。

- **未指定**（默认） – 不在时段内搜索，搜索整个日志。
- **前一天**
- **上一周**
- **上个月**
- **时段** – 可以指定确切时段（“从:”和“到:”），以仅过滤指定时段的记录。

全字匹配

如果要搜索全字以得到更精确的结果，则使用此复选框。

区分大小写

如果在过滤时使用大写字母或小写字母对您而言很重要，则**启用**此选项。完成配置过滤/搜索

选项后，单击**确定**以显示过滤的日志记录，或单击“查找”以开始搜索。从当前位置（亮显的记录）开始，按从上到下的顺序搜索日志文件。搜索会在找到第一条相应记录时停止。按 **F3** 可搜索下一条记录，或单击右键并选择**查找**以优化搜索选项。

日志记录配置

可从主程序窗口访问 ESET Endpoint Antivirus 的日志记录配置。依次单击**设置 > 高级设置 > 工具 > 日志文件**。日志部分用来定义如何管理日志。程序自动删除旧的日志以节省硬盘空间。您可以为日志文件指定以下选项：

日志记录的最低级别 – 指定要记录的事件的最低级别：

- **诊断** – 记录微调程序所需的信息和以上所有记录。
- **信息性** – 记录包括成功更新消息及以上所有记录在内的信息性消息。
- **警告** – 记录严重错误和警告消息。
- **错误** – 将记录类似“下载文件时出错”等错误和严重错误。
- **严重** – 仅记录严重错误（启动病毒防护等时出错）。

当选择**诊断**级别时，将记录所有受阻止的连接。

自动删除早于以下天数的记录字段中指定天数以前的日志条目将自动删除。

自动优化日志文件 – 如果执行，则碎片百分比高于**如果未使用记录数超过（%）**字段中指定的值后，将自动整理日志文件碎片。

单击**优化**以开始日志文件的碎片整理。将删除所有空白日志条目，以改善性能并提高日志处理速度。可以感受到这种提高，尤其在日志包含大量条目时。

启用文本协议支持采用不同于日志文件的其他文件格式存储日志：

- **目标目录** – 选择将存储日志文件的目录（仅适用于文本/CSV□□您可以复制路径或通过单击**清除**选择另一个目录。每个日志部分都具有其自己的文件，该文件具有预定义的文件名（例如，如果您使用纯文本文件格式存储日志，则日志文件的**检测到的威胁**部分具有 *virlog.txt*□□
- **类型** – 如果您选择**文本**文件格式，日志将存储在文本文件中，并且数据将由制表符分隔。这也适用于由逗号分隔的 **CSV** 文件格式。如果您选择**事件**，则日志将存储在 Windows 事件日志（可以使用控制面板中的事件查看器进行查看）而非文件中。
- **删除所有日志文件** – 将擦除当前在**类型**下拉菜单中选定的所有存储日志。将显示关于成功删除这些日志的通知。

启用跟踪审核日志中的配置更改 – 通知您有关每个配置更改的信息。有关详细信息，请参阅审核日志□

为了帮助更快地解决问题，ESET 会要求您提供计算机日志。 ESET Log Collector 可使您轻松收集所需信息。 有关 ESET Log Collector 详细信息，请访问我们的 ESET 知识库文章。

审核日志

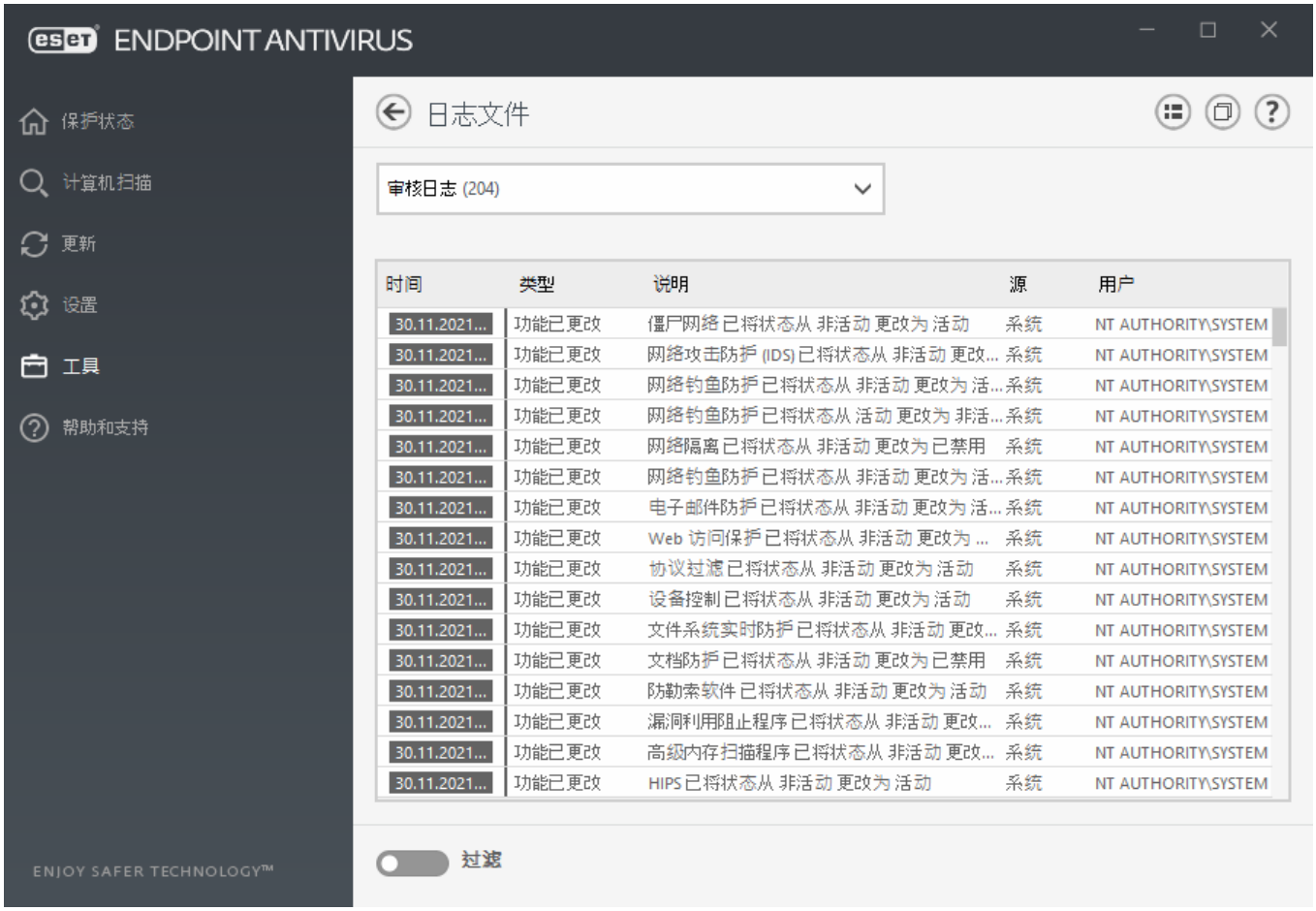
在企业环境中，通常有多个用户拥有为配置端点而定义的访问权限。由于产品配置的修改可能会极大地影响产品运行的方式，因此管理员必定想要跟踪用户所做的更改，以帮助管理员快速识别、解决以及防止将来出现相同或类似的问题。

审核日志是 ESET Endpoint Antivirus 版本 7.1 中一种新的日志记录类型，也是用于识别问题根源的解决方案。审核日志跟踪配置或保护状态的更改，并记录快照以供以后参考。

若要查看**审核日志**，请在主菜单中单击**工具**，然后单击**日志文件**并从下拉菜单中选择**审核日志**。

审核日志包含以下相关信息：

- 时间 – 何时执行更改
- 类型 – 更改了哪些类型的设置或功能
- 说明 – 确切更改了哪些内容，设置的哪些部分已更改以及已更改设置的的数量
- 源 – 更改源的位置
- 用户 – 谁进行了更改



在日志文件窗口中右键单击任何审核日志的**设置更改**类型，然后从右键菜单中选择**显示更改**以显示有关所执行更改的详细信息。此外，通过在右键菜单中单击**恢复**即可恢复设置更改（不适用于由 ESET PROTECT 管理的产品）。如果从右键菜单中选择**全部删除**，将创建包含有关此操作的信息的日志。

如果**自动优化日志文件**在**高级设置 > 工具 > 日志文件**中已启用，将自动对审核日志进行碎片整理（如同其他日志一样）。

如果**自动删除早于相应天数的记录**在**高级设置 > 工具 > 日志文件**中已启用，将自动删除早于指定天数的日志条目。

计划任务

计划任务管理和启动具有预定义配置和属性的计划任务。

“计划任务”可从 ESET Endpoint Antivirus 主程序窗口中单击**工具 > 计划任务**来访问。**计划任务**包含所有计划任务和配置属性（如预定义的日期、时间和使用的扫描配置文件）的列表。

任务计划用于计划以下任务：检测引擎更新、扫描任务、系统启动文件检查以及日志维护。您可以直接从主“计划任务”窗口中添加或删除任务（单击底部的**添加任务**或**删除**）。在“计划任务”窗口中右键单击任意位置可执行以下操作：显示详细信息、立即执行任务、添加新任务和删除现有任务。使用每个条目开头的复选框来启用/停用任务。

默认情况下，**计划任务**中显示以下计划任务：

- **日志维护**
- **定期自动更新**
- **拨号连接后自动更新**
- **用户登录后自动更新**
- **自动启动文件检查**（用户登录后）
- **自动启动文件检查**（模块更新成功后）

要编辑现有计划任务（包括默认和用户定义的）的配置，请右键单击任务然后单击**编辑**，或选择要修改的任务然后单击**编辑**按钮。

添加新任务

1. 单击窗口底部的**添加任务**。
2. 输入任务的名称。
3. 从下拉菜单中选择所需任务：
   - **运行外部应用程序** – 计划外部应用程序的执行。
   - **日志维护** – 日志文件中仍会包含已删除记录的残余信息。此任务定期优化日志文件中的记

录以提高工作效率。

- **系统启动文件检查** – 检查在系统启动或登录时允许运行的文件。

- **创建计算机状态快照** – 创建 ESET SysInspector 计算机快照 – 收集有关系统组件的详细信息（例如，驱动程序、应用程序）并评估每个组件的风险级别。

- **手动计算机扫描** – 执行计算机上文件和文件夹的计算机扫描。

- **更新** – 通过更新检测引擎和程序模块，计划更新任务。

4. 如果要激活任务（您可以之后通过选中/取消选中计划任务列表中的复选框来执行此操作），请打开**启用**开关，单击**下一步**并选择其中一个计时选项：

- **一次** – 任务将在预定义的日期和时间执行。

- **重复** – 任务将以指定的时间间隔执行。

- **每天** – 任务将在每天的指定时间重复运行。

- **每周** – 任务将在选定的星期和时间运行。

- **由事件触发** – 任务将在发生指定事件时执行。

5. 在便携式计算机靠电池供电时，**选择靠电池供电时跳过任务**以最大限度地减少系统资源。将在**任务执行**字段中指定的日期和时间运行该任务。如果任务无法在预定义的时间运行，可以指定其再次执行时间：

- **在下一个计划时间**

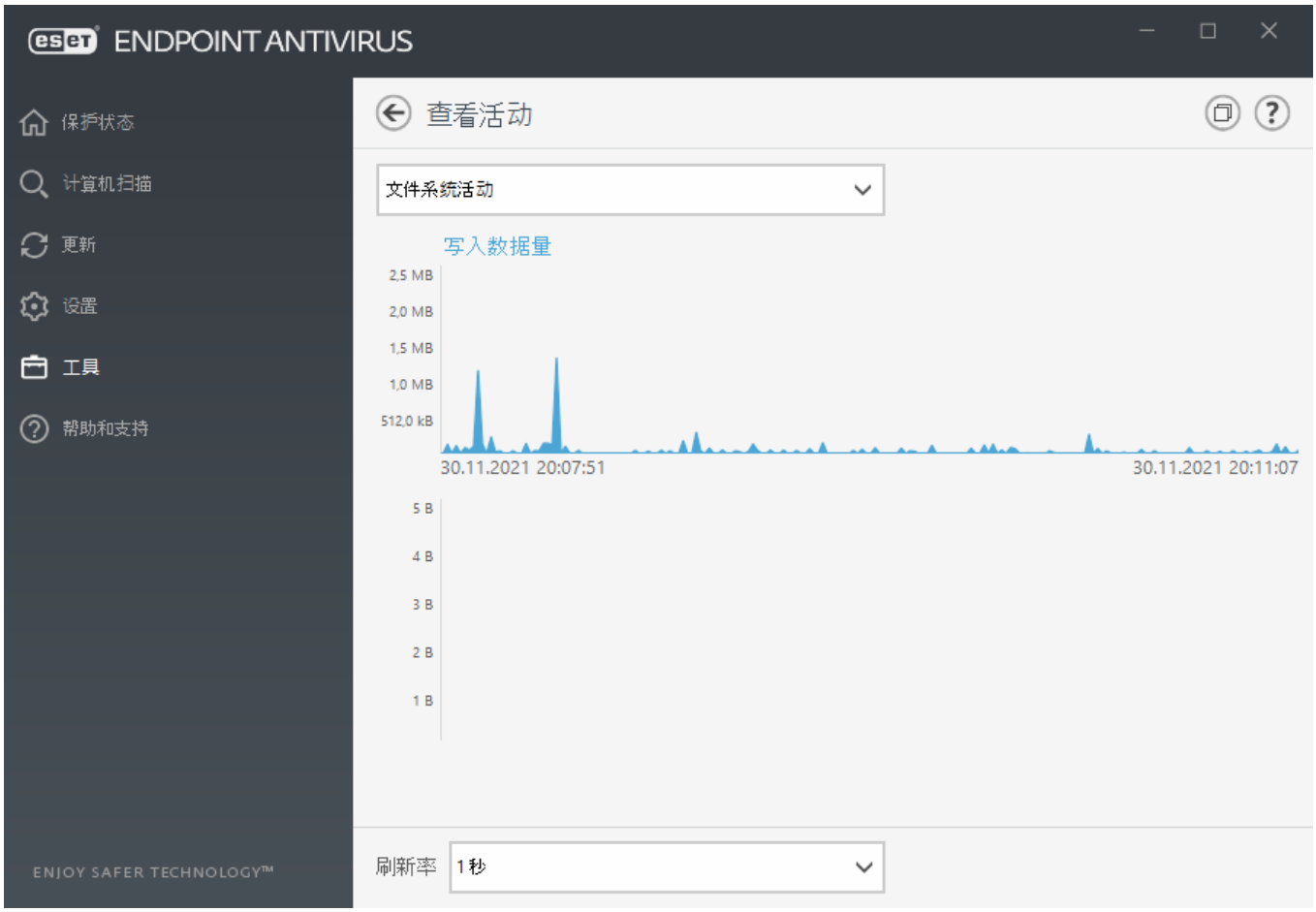
- **尽快**

- **如果自上次运行时间之后经过的时间超过指定值，则立即跳过任务**（可使用**自上次运行时间之后经过的时间**滚动框来定义间隔）

您可以通过右键单击并单击**显示任务详细信息**来查看计划任务。

查看活动

要以图表方式查看当前**文件系统活动**，请单击**工具 > 查看活动**。图表的底部是时间线，用于实时记录选定时间范围内的文件系统活动。若要更改时间范围，请从**刷新率**下拉菜单中进行选择。



有以下选项可供使用：

- **步进:1 秒** – 图表每秒刷新一次，时间线范围为最后 10 分钟。

- **步进:1 分钟(最后 24 小时)** – 图表每分钟刷新一次，时间线范围为最后 24 小时。
- **步进:1 小时(最后 1 个月)** – 图表每小时刷新一次，时间线范围为最后一个月。
- **步进:1 小时(选定月份)** – 图表每小时刷新一次，时间线范围为选定的最后 X 个月。

文件系统活动图表的纵轴表示读取的数据量（蓝色）和写入的数据量（蓝绿色）。两个值均以 KB（千字节）/MB/GB 为单位。如果将鼠标移到图表下方图例中的读取数据或写入数据的上方，图表将仅显示该活动类型的数据。

ESET SysInspector

ESET SysInspector 是一个可彻底检查计算机、收集有关系统组件（例如，驱动程序和应用程序、网络连接或重要注册表项）的详细信息以及评估每个组件风险级别的应用程序。 该信息有助于确定可能由于软硬件不兼容或恶意感染而导致出现可疑系统行为的原因。另请参阅 ESET SysInspector 的在线用户指南。

SysInspector 窗口显示下列有关已创建的日志的信息：

- **时间** – 日志创建时间。
- **注释** – 简短注释。
- **用户** – 创建日志的用户的姓名。
- **状态** – 日志创建的状态。

可用操作包括：

- **显示** – 打开已创建的日志。 还可以右键单击给定日志文件，然后在右键菜单中选择**显示**。
- **比较** – 比较两个现有日志。
- **创建** – 创建新日志。请在 ESET SysInspector 完成（日志状态将显示为“**已创建**”）之前稍作等待，完成后再尝试访问日志。
- **删除** – 删除列表中选定的日志。

当选中一个或多个日志文件时，右键菜单中的以下项将为可用：

- **显示** – 在 ESET SysInspector 中打开选定日志（相当于双击日志）。
- **比较** – 比较两个现有日志。
- **创建** – 创建新日志。请在 ESET SysInspector 完成（日志状态将显示为“**已创建**”）之前稍作等待，完成后再尝试访问日志。
- **删除** – 删除选定的日志。

- **全部删除** – 删除所有日志。
- **导出** – 将日志导出为 .xml 文件或压缩的 .xml。

基于云的防护

ESET LiveGrid®（建立在 ESET ThreatSense.Net 高级早期预警系统之上）利用 ESET 用户在世界各地提交并发送给 ESET 研究实验室的数据。 通过提供可疑的样本和原始的元数据，ESET LiveGrid® 使我们能够立即对客户的需求作出反应并使 ESET 能够持续应对最新的威胁。

有三个选项：

选项 1：启用 ESET LiveGrid® 信誉系统

ESET LiveGrid® 信誉系统提供基于云的白名单和黑名单。

直接从程序界面或右键菜单通过 ESET LiveGrid® 提供的额外信息来检查正在运行的进程和文件的信誉。

选项 2：启用 ESET LiveGrid® 反馈系统

除了 ESET LiveGrid® 信誉系统，ESET LiveGrid® 反馈系统将收集您的计算机中与新检测到的威胁相关的信息。这些信息可能包括出现威胁的文件的样本或副本、该文件的路径、文件名、日期和时间、威胁出现在计算机上的过程，以及有关您的计算机操作系统的信息。

默认情况下，ESET Endpoint Antivirus 配置为提交可疑文件，以供 ESET 病毒实验室详细分析。始终排除具有特定扩展名的文件（例如 *.doc* 或 *.xls*）。如果您或贵组织希望避免发送特定类型的文件，还可以添加其他扩展名。

选项 3：选择不启用 ESET LiveGrid®

您不会失去软件中的任何功能，但启用 ESET LiveGrid®后，ESET Endpoint Antivirus 在某些情况下可能会比检测引擎更新更快地响应新威胁。

> 请阅读词汇表中有关 ESET LiveGrid® 的更多信息。
> 有关如何在 ESET Endpoint Antivirus 中启用或禁用 ESET LiveGrid® 的信息，请参阅我们以英语和其他几种语言提供的图文并茂说明。

高级设置中基于云的防护配置

要访问 ESET LiveGrid® 的设置，请按 **F5** 进入“高级设置”，然后展开**检测引擎 > “基于云的防护”**。

启用 ESET LiveGrid® 信誉系统（建议） - ESET LiveGrid® 信誉系统通过将已扫描的文件与云中白名单和黑名单项目数据库进行比较，可提高 ESET 恶意软件防护解决方案的效率。

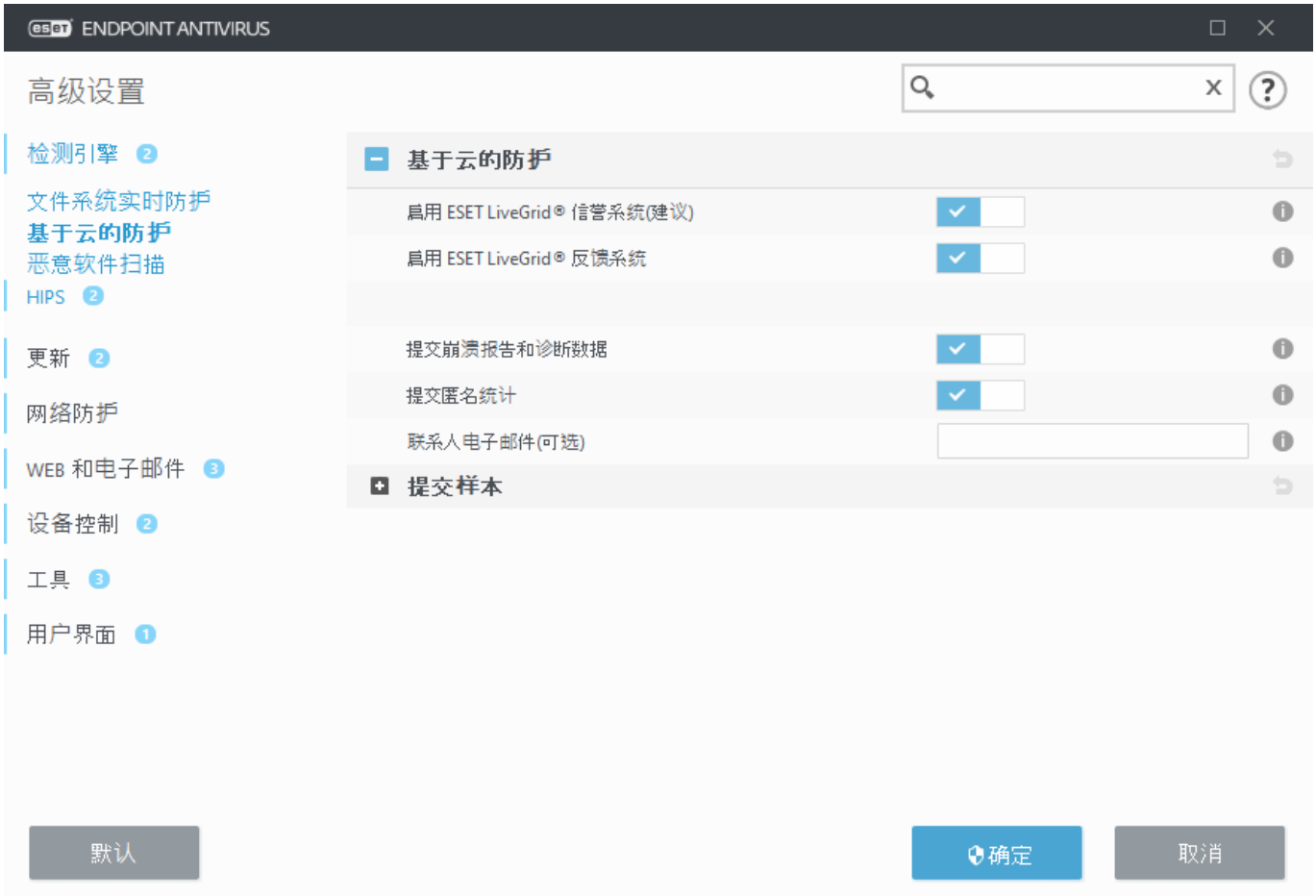
启用 ESET LiveGrid® 反馈系统 – 将相关提交数据（在下面的**样本提交部分**中描述）以及崩溃报告和统计信息发送到 ESET 研究实验室以供进一步分析。

启用 ESET LiveGuard（在 ESET Endpoint Antivirus 中不可见）- ESET LiveGuard 是 ESET 提供的付费服务。其目的是增加一层保护，专门用于缓解自然环境中新出现的威胁。可疑文件会自动提交到 ESET 云。在云中，我们的高级恶意软件检测引擎会对这些可疑文件进行分析。提供样本的用户将收到一个行为报告，其中提供有观察到的样本行为的摘要。

提交崩溃报告和诊断数据 – 提交 ESET LiveGrid® 相关的诊断数据，例如崩溃报告和模块内存转储。我们建议将其保持为启用状态以帮助 ESET 诊断问题、改进产品和确保对最终用户的更好保护。

提交匿名统计 – 允许 ESET 收集有关新检测到的威胁的信息，如威胁名称、检测日期和时间、检测方法和相关联的元数据、产品版本以及配置，其中包括有关您的系统的信息。

联系人电子邮件（可选） – 您的联系人电子邮件可以与任何可疑文件一起发送，而且可能用于在需要进一步信息以供分析时联系您。请注意，除非需要更多信息，否则 ESET 不会与您联系。



提交样本

手动提交样本 – 启用该选项，以上下文菜单、隔离或工具 > 提交样本以供分析将样本手动提交给 ESET。

自动提交已检测的样本

选择哪种样本将提交到 ESET 以供分析并改进以后的检测。以下选项可用：

- **所有已检测的样本** – 由检测引擎检测到的所有对象（包括在扫描程序设置中启用的潜在不受欢迎的应用程序）。
- **除文档外的所有样本** – 除**文档**外的所有检测的对象（见下文）。
- **不提交** – 检测的对象不会发送给 ESET。

自动提交可疑样本

这些样本还将发送给 ESET 以免检测引擎没有检测它们。例如，差点错过检测的样本，或者某个 ESET Endpoint Antivirus 防护模块认为这些样本是可疑的或者具有不明行为。

- **可执行文件** – 包括诸如 .exe, .dll, .sys 等文件。
- **压缩文件** – 包括诸如 .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab 等文件类型。
- **脚本** – 包括诸如 .bat, .cmd, .hta, .js, .vbs, .ps1 等文件类型。
- **其他** – 包括诸如 .jar, .reg, .msi, .sfw, .lnk 等文件类型。
- **可能的垃圾电子邮件** – 这将允许向 ESET 发送可能的垃圾邮件部分或整个可能的垃圾电子邮件以及附件，以供进一步分析。启用此选项可改进垃圾邮件的全局检测，包括为您改进将来的垃圾邮件检测。
- **文档** – 包括具有或没有活动内容的 Microsoft Office 或 PDF 文档。

扩展所有包含的文档文件类型的列表

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

排除

“排除”过滤器允许您不提交某些文件/文件夹（例如，排除诸如文档或电子表格等可能包含机密信息的文件会很有用）。列出的文件即使包含可疑代码也不会发送给 ESET 实验室以供分析。默认情况下，最常见的文件类型均会排除（.doc 等）。如果需要，可以添加到排除文件列表。

要排除从 download.domain.com 下载的文件，请导航到**高级设置 > 基于云的防护 > 提交样本 > 排除**并添加排除 .download.domain.com。

ESET LiveGuard

要在使用 ESET LiveGuard Web Console 的客户端计算机上启用 ESET PROTECT 服务，请参阅 ESET Endpoint Antivirus 的 ESET LiveGuard 配置。

如果您以前使用过 ESET LiveGrid® 但已禁用它，可能仍会发送数据包。即使已停用，此类数据包也会发送给 ESET。发送完当前所有信息后，将不会再创建任何数据包。

基于云的防护的排除过滤器

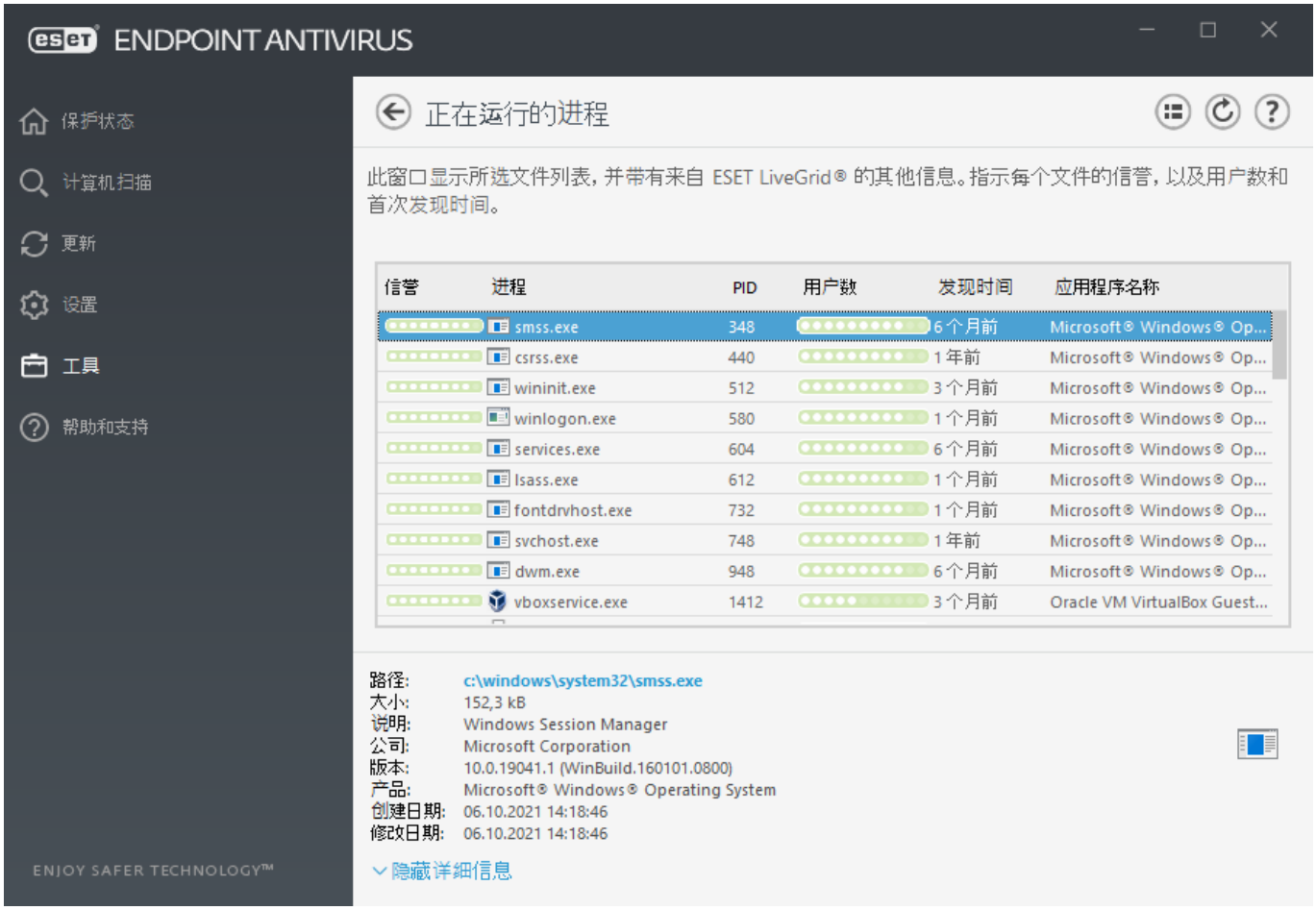
排除过滤器允许您不提交某些文件或文件夹样本。列出的文件即使包含可疑代码也不会发送给 ESET 实验室以供分析。默认情况下常见文件类型（例如 doc 等）均被排除。

此功能对将可能包含机密信息的文件（例如文档或电子表格）排除在外很有用。

要排除从 download.domain.com 下载的文件，请导航到**高级设置 > 基于云的防护 > 提交样本 > 排除**并添加排除 .download.domain.com。

正在运行的进程

运行进程显示计算机上运行的程序或进程，并保持 ESET 立刻持续获知新入侵。ESET Endpoint Antivirus 提供有关运行的进程的详细信息，以通过启用 ESET LiveGrid® 技术来保护用户。



信誉 – 在大多数情况下，ESET Endpoint Antivirus 和 ESET LiveGrid® 技术使用一系列启发式规则检查每个对象的特性，然后评估恶意活动的可能性，将风险级别指定给对象（文件、过程、注

册表项等）。基于这些启发式扫描，将向对象指定风险级别（级别从 9 – 最佳信誉（绿色）到 – 最差信誉（红色）。

进程 – 当前在计算机上运行的程序或进程的映像名称。要查看计算机上运行的所有进程，还可以使用 Windows 任务管理器。可以通过右键单击任务栏中的空白区域，然后单击任务管理器，或者通过按下键盘上的 **Ctrl+Shift+Esc** 来打开任务管理器。

PID – 是在 Windows 操作系统中运行的进程的 ID。

> 标记为绿色的已知应用程序肯定干净（列入白名单）并将排除扫描，因为这样将改善手动计算机扫描的扫描速度或计算机上的文件系统实时防护。

用户数 – 使用给定应用程序的用户数量。此信息由 ESET LiveGrid® 技术收集。

发现时间 – 自应用程序由 ESET LiveGrid® 技术发现以来的时段。

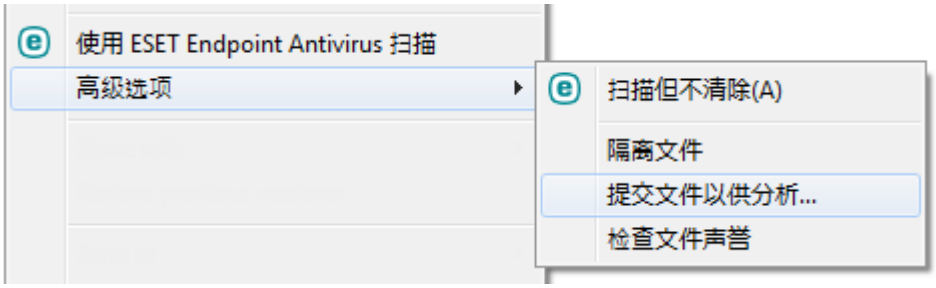
> 当应用程序被标记为“未知（橙色）”安全级别时，它不一定就是恶意软件。通常它是一个较新的应用程序。如果您对文件不确定，使用提交文件以供分析功能将该文件发送到 ESET 病毒实验室。如果文件被证实是一个恶意应用程序，则以后的检测引擎更新中将增加对它的检测。

应用程序名称 – 程序或进程的给定名称。

通过单击底部的给定应用程序，将在窗口底部显示以下信息：

- **路径** – 计算机上应用程序的位置。
- **大小** – 以 kB（千字节）或 MB（兆字节）为单位的文件大小。
- **说明** – 基于操作系统说明的文件特性。
- **公司** – 供应商或应用程序进程的名称。
- **版本** – 来自应用程序发布者的信息。
- **产品** – 应用程序名称和/或企业名称。
- **创建日期** – 创建应用程序的日期和时间。
- **修改日期** – 上次修改应用程序的日期和时间。

> 还可以对不充当运行程序/进程的文件检查信誉 – 标记要检查的文件，右键单击它们，从右键菜单中选择**高级选项 > 使用 ESET LiveGrid® 检查文件信誉**。



安全报告

此功能可提供以下类别统计信息的概述：

已阻止的网页 – 显示已阻止网页的数量（PUA 的黑名单 URL、网络钓鱼、受攻击的路由器、IP 或证书）。

已检测到的被感染电子邮件对象 – 显示已检测到的被感染电子邮件对象的数量。

已检测到的 PUA – 显示潜在不受欢迎的应用程序 (PUA) 的数量。

已检查的文档 – 显示已扫描的文档对象的数量。

已扫描的应用程序 – 显示已扫描的可执行文件对象的数量。

已扫描的其他对象 – 显示其他已扫描的对象的数量。

已扫描的网页对象 – 显示已扫描的网页对象的数量。

已扫描的电子邮件对象 – 显示已扫描的电子邮件对象的数量。

这些类别的顺序取决于从最高到最低的数值。不会显示值为零的类别。单击**显示更多**可展开并显示隐藏的类别。

在类别下方，会看到采用世界地图形式呈现的实际病毒情况。每个国家/地区存在的病毒使用颜色表示（颜色越深，数字越高）。没有数据的国家/地区将灰显。将鼠标光标悬停在国家/地区上方，即可显示所选国家/地区的数据。可以选择特定大洲，地图会自动缩放。

单击右上角的齿轮 ⚙，即可**启用/禁用安全报告通知**，或者选择是否显示最后 30 天的数据（自产品激活以后）。如果 ESET Endpoint Antivirus 安装的天数不足 30 天，那么仅可选择完成安装之后算起的天数。默认情况下，设置的时间段为 30 天。

重置数据会清除所有统计信息，并删除安全报告的现有数据。除非在**高级设置 > 用户界面 > 警报和消息框 > 确认消息**中取消选择**重置统计前先询问**选项，否则必须确认此操作。

ESET SysRescue Live

ESET SysRescue Live 是一种免费的实用程序，让您可以创建可启动的救援 CD/DVD 或 USB 驱动器。可以通过救援媒体启动受感染的计算机，来扫描恶意软件并清除受感染的文件。

ESET SysRescue Live 的主要优点是：它独立于主机操作系统运行，但可直接访问磁盘和文件系统。这样，便可以删除正常操作条件下（例如，操作系统正在运行时等）可能无法删除的威胁。

- ESET SysRescue Live 在线帮助

提交样本以供分析

如果在计算机上发现可疑文件或在 Internet 上发现可疑站点，可以将它提交给 ESET 研究实验室以供分析（根据 ESET LiveGrid® 的配置，也许无法提交）。

除非样本至少满足以下条件之一，否则请勿提交该样本：
• ESET 产品并未检测到样本
• 将样本错误检测为威胁
• 我们不接受个人文件（希望由 ESET 扫描以查找恶意软件）作为样本（ESET 研究实验室不会为用户手动执行扫描）
• 使用描述性主题行，并尽可能多地包含有关文件的信息（例如，屏幕截图或下载该文件的网站）

样本提交使您可以使用以下方法之一将文件或站点发送给 ESET 以供分析：

1. 可以在**工具 > 提交样本以供分析**中找到“使用样本提交”对话框。

2. 此外，也可以通过电子邮件提交文件。如果您选用此方式，请使用 WinRAR/ZIP 压缩文件，用密码“infected”保护压缩文件，然后将它发送至 samples@eset.com。

3. 报告垃圾邮件或垃圾邮件误报，请参阅我们的 ESET 知识库文章。

在已打开**选择样本以供分析**时，从**提交样本的理由**下拉菜单中选择最适合您的邮件的描述：

- 可疑文件
- 可疑站点（**被任何恶意软件感染的网站**）。
- 误报文件（文件检测为感染，但并未感染），
- 误报站点
- 其他

文件/站点 – 您想要提交的文件或网站的路径。

联系人电子邮件 – 此联系人电子邮件随可疑文件一起发送给 ESET。如果需要更多信息以供分析，可能会使用该电子邮件与您联系。可选择是否输入联系人电子邮件。选择**匿名提交**可将它留空。

除非需要您提供更多信息，否则您不会收到 ESET 的回复。由于我们的服务器每天都会收到数以万计的文件，因此不可能对所有提交一一回复。
如果样本被证实是一个恶意应用程序或网站，则以后的 ESET 更新中将增加对它的检测。

选择样本以供分析 – 可疑文件

观察到的恶意软件感染迹象和症状 – 输入在您的计算机上观察到的可疑文件行为的描述。

文件来源(URL 地址或供应商) – 请输入文件出处（来源），并注明您是如何遇到该文件的。

注释和其他信息 – 您可以在这里输入有助于识别可疑文件过程的其他信息或描述。

第一个参数（即**观察到的恶意软件感染迹象和症状**）为必填项，但是提供其他信息将会很大程度地帮助我们实验室进行样本的识别过程。

选择样本以供分析 – 可疑站点

请从**网站问题**下拉菜单选择以下内容之一：

- **被感染** – 包含由各种方法分发的病毒或其他恶意软件的网站。
- **网络钓鱼** – 通常用于获取对敏感数据（如银行帐号、PIN 码等）的访问权限。请阅读词汇表中关于此类攻击的更多信息。
- **欺诈** – 欺骗或欺诈性网站，尤其是旨在快速获利的此类网站。
- 如果上述选项与您要提交的站点不符，请选择**其他**。

注释和其他信息 – 您可以在这里输入有助于分析可疑网站的其他信息或描述。

选择样本以供分析 – 误报文件

我们请求您提交已检测为感染但却未感染的文件，以便改进病毒和间谍软件防护引擎并为其他用户提供防护。当文件模式匹配检测引擎中包含的同一模式时，可能会发生误报 (FP)。

应用程序名称和版本 – 程序标题及其版本（例如，编号、别名或代码名称）。

文件来源(URL 地址或供应商) – 请输入文件出处（来源），并注明您是如何遇到该文件的。

应用程序用途 – 一般应用程序描述、应用程序类型（例如浏览器、媒体播放器...）及其功能。

注释和其他信息 – 您可以在这里添加有助于处理可疑文件的其他信息或描述。

> 前三个参数是必填的，以识别合法应用程序并将它与恶意代码区分开来。通过提供其他信息，您将对我们实验室的识别过程和样本的处理提供极大帮助。

选择样本以供分析 – 误报站点

我们请求您提交已检测为感染、欺诈或网络钓鱼但实际是误报的站点。当文件模式匹配检测引擎中包含的同一模式时，可能会发生误报 (FP)。请提供该网站以帮助我们改进病毒和网络钓鱼防护引擎，并帮助为其他用户提供防护。

备注和附加信息 – 可以在此处添加有助于处理可疑网站的附加信息或描述。

选择样本以供分析 – 其他

如果文件无法被归类为**可疑文件**或**误报**，请使用此表格。

提交文件的原因 – 请输入详细描述和发送文件的原因。

通知

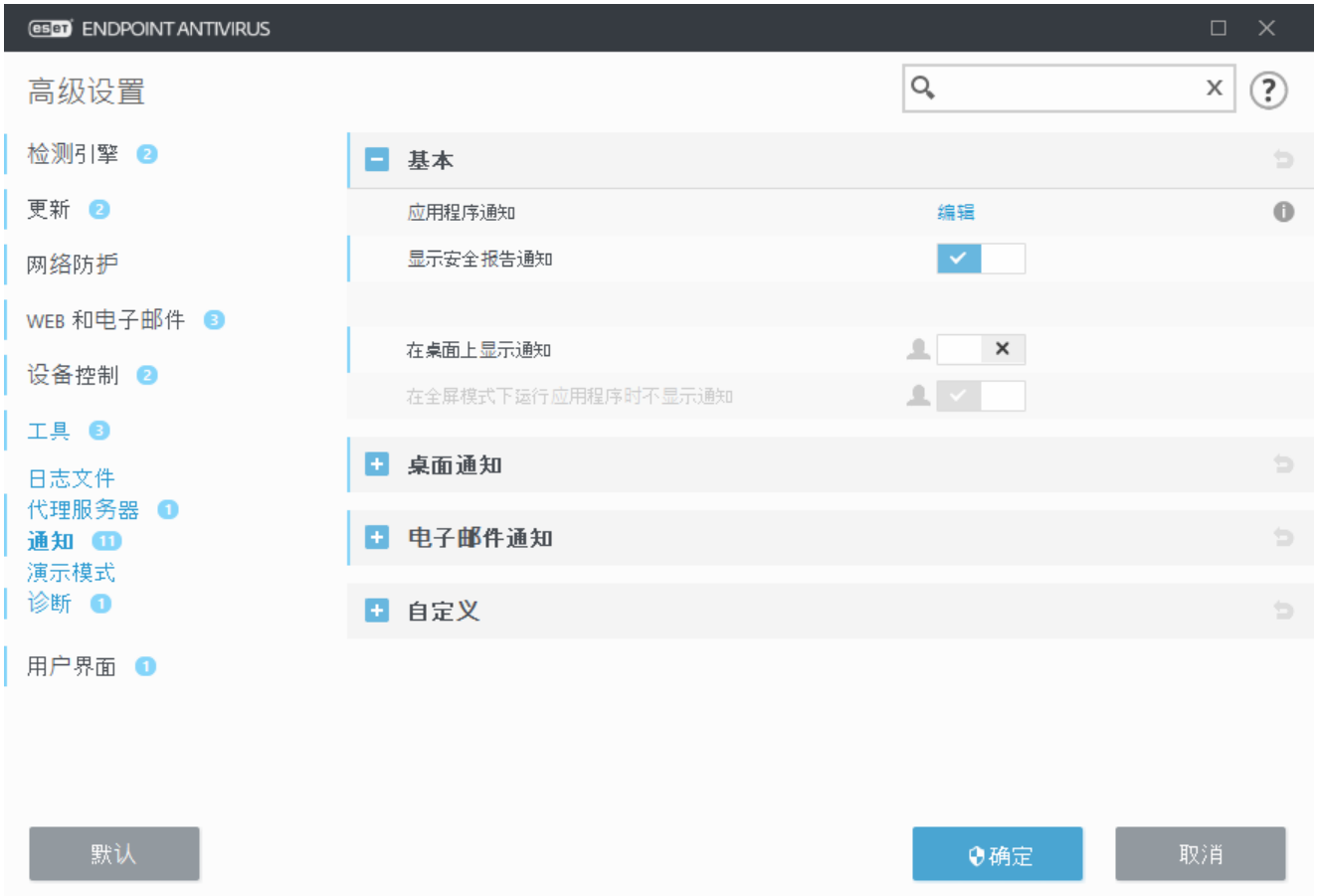
若要管理 ESET Endpoint Antivirus 就事件与用户通信的方式，请导航到**高级设置**(F5) > **工具** > **通知**。此配置窗口允许您设置以下类型的通知：

- 应用程序通知 – 直接显示在主程序窗口中。
- 桌面通知 – 桌面通知显示为系统任务栏旁边的小弹出窗口。
- 电子邮件通知 – 电子邮件通知发送到指定的电子邮件地址。
- 通知自定义 – 将自定义消息添加到桌面通知等。

在**基本**部分中，使用相应开关即可调整以下各项：

开关	默认	说明
在桌面上显示通知		禁用以隐藏系统任务栏旁边的弹出通知。建议您将此选项保持为启用，以便产品可能在发生新事件时给您发送通知。
在以下情况下不显示通知...		保持**在全屏模式下运行应用程序时不显示通知**为启用，以阻止所有非交互通知。
显示安全报告通知		启用以在生成新版本的安全报告时接收通知（仅当不由 ESET PROTECT 管理时可用）。
显示关于成功更新的通知		启用以在产品更新其组件和检测引擎模块时接收通知。
通过电子邮件发送事件通知		启用以激活电子邮件通知。

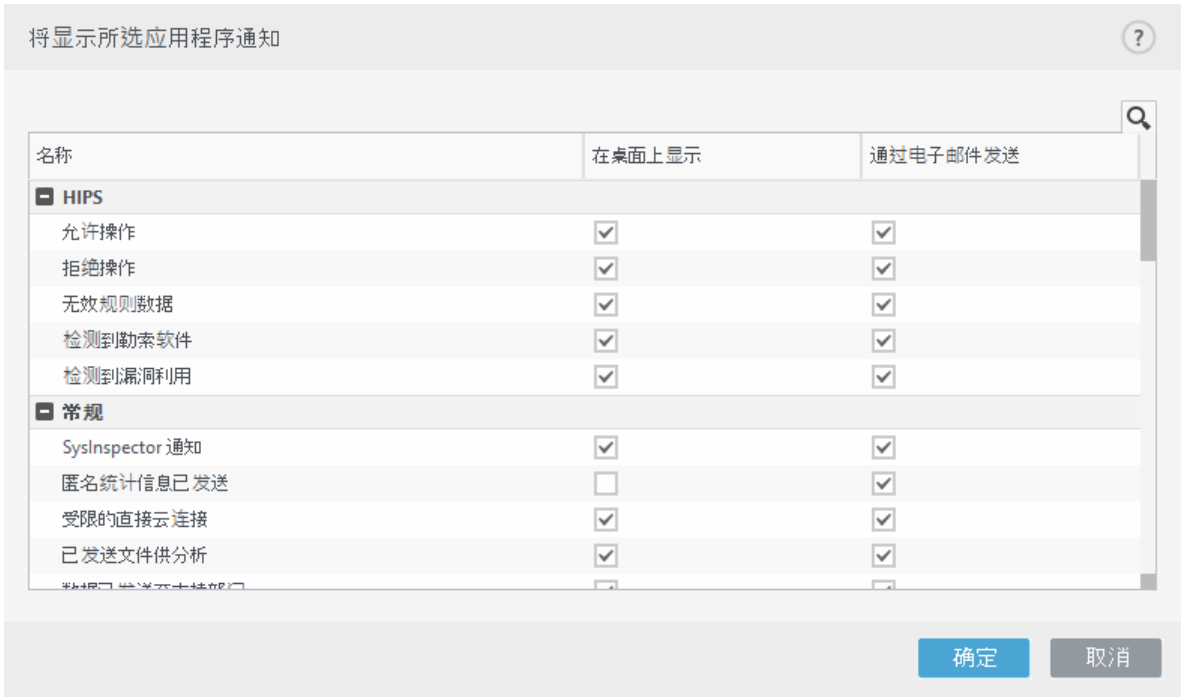
若要启用或禁用特定应用程序通知，请单击**应用程序通知**旁边的**编辑**。



应用程序通知

若要调整应用通知的可见性（显示在屏幕的右下角），请导航到 ESET Endpoint Antivirus 高级设置树的**工具 > 通知 > 基本 > 应用程序通知**。

通知列表分为三列。通知名称在第一列中按类别排序。若要更改产品通知新的应用程序事件的方式，请选中相应列**在桌面上显示**和**通过电子邮件发送**中的复选框。



若要设置桌面通知的常规设置，例如消息的显示时长或要显示事件的最低级别，请参阅**高级设置 > 工具 > 通知**中的桌面通知。

若要设置电子邮件消息格式以及配置 SMTP 服务器设置，请参阅**高级设置 > 工具 > 通知**中的电子邮件通知。

> 如果要设置通知**文件已分析**和**文件未分析**（在使用 ESET LiveGuard 期间），必须将主动防护设置为**阻止执行，直到收到分析结果**。

桌面通知

桌面通知由系统任务栏旁边的小弹出窗口表示。默认情况下，它设置为显示 10 秒，然后它会慢慢消失。这是 ESET Endpoint Antivirus 与用户通信的主要方式，以便通知产品更新成功、已连接新设备、病毒扫描任务完成或找到新威胁。

桌面通知部分允许自定义弹出通知的行为。可以设置以下属性：

持续时间 – 设置通知消息可见的时长。该值必须在 3 秒到 30 秒的范围内。

透明度 – 以百分比为单位设置通知消息的透明度。支持的范围为 0（不透明）到 80（非常高的透明度）

要显示事件的最低级别 – 从下拉菜单中，可以选择要显示通知的起始严重性级别：

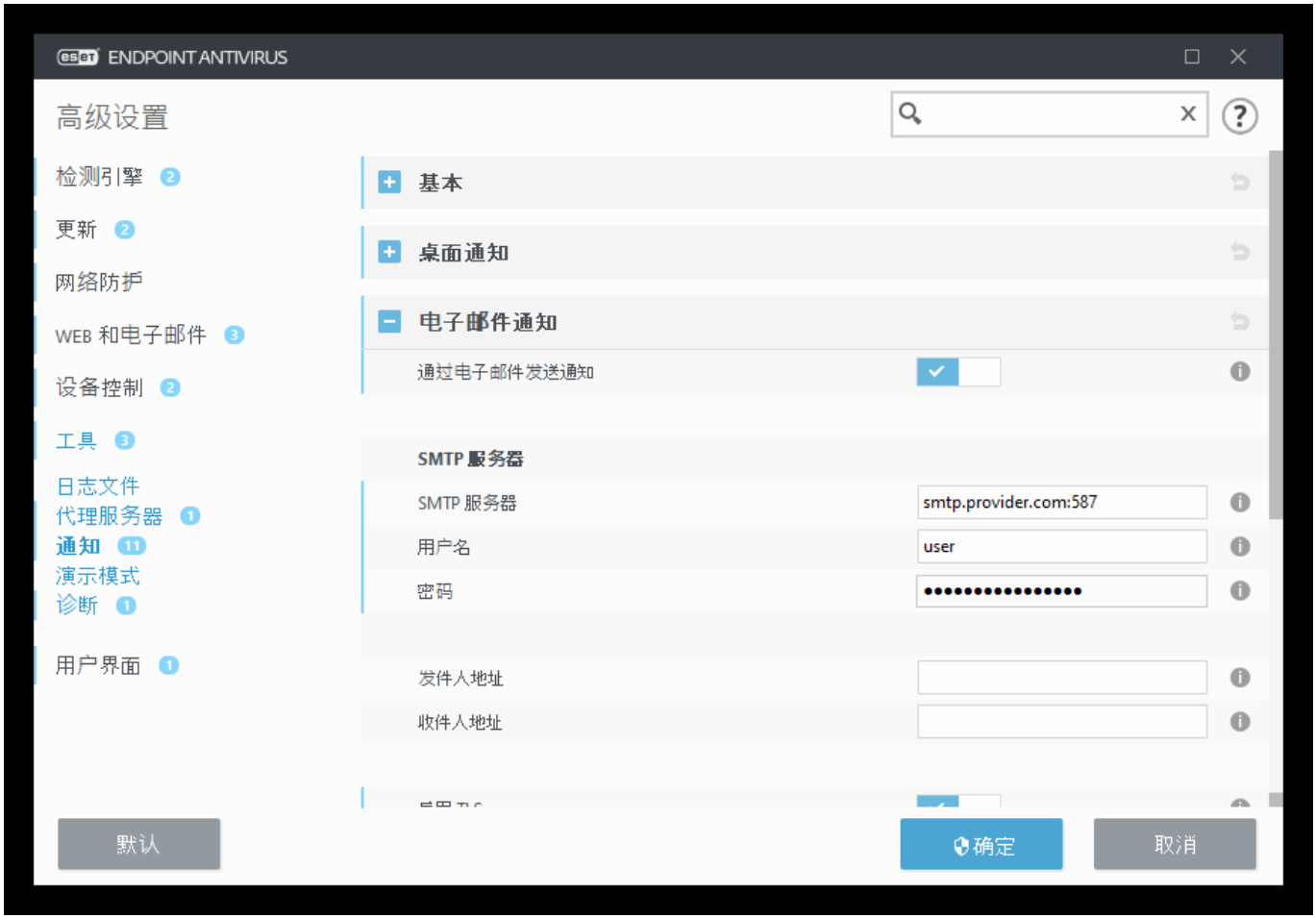
- **诊断** – 记录微调程序所需的信息和以上所有记录。
- **信息性** – 记录信息性消息（如非标准的网络事件），其中包括成功更新消息及以上所有记录。
- **警告** – 记录严重错误和警告消息（未正确运行反隐藏技术或者更新失败）。
- **错误** – 将记录错误（未启动文档防护）和严重错误。
- **严重** – 仅记录严重错误（启动病毒防护或被感染的系统时出错）。

对于多用户系统，在此用户的屏幕上显示通知 – 允许选定帐户接收桌面通知。例如，如果您使用的不是管理员帐户，则键入完整帐户名称，将显示指定帐户的桌面通知。只有一个用户帐户可以接收桌面通知。

允许通知占据屏幕焦点 – 通知将占据屏幕焦点，并可通过 Alt+Tab 进行访问。

电子邮件通知

如果发生具有所选级别的事件，ESET Endpoint Antivirus 可以自动发送通知电子邮件。在**基本**部分中，启用**通过电子邮件发送事件通知**以激活电子邮件通知。



SMTP 服务器

SMTP 服务器 – 用于发送通知的 SMTP 服务器（例如 *smtp.provider.com:587*，预定义的端口为 25）。

ESET Endpoint Antivirus 支持采用 TLS 加密的 SMTP 服务器。

用户名和密码 – 如果 SMTP 服务器需要验证，则应在这些字段中填写有效的用户名和密码，以便访问 SMTP 服务器。

发件人地址 – 该字段用于指定发件人地址，发件人地址将显示在通知电子邮件的标题中。

收件人地址 – 该字段用于指定收件人地址，收件人地址将显示在通知电子邮件的标题中。使用分号“;”分隔多个电子邮件地址。

启用 TLS – 允许发送 TLS 加密支持的警报和通知消息。

电子邮件设置

从**通知的最低级别**下拉菜单中，可以选择要发送的通知的起始严重性级别。

- **诊断** – 记录微调程序所需的信息和以上所有记录。
- **信息性** – 记录信息性消息（如非标准的网络事件），其中包括成功更新消息及以上所有记录。

- **警告** – 记录严重错误和警告消息（未正确运行反隐藏技术或者更新失败）。
- **错误** – 将记录错误（未启动文档防护）和严重错误。
- **严重** – 仅记录严重错误（启动病毒防护或被感染的系统时出错）。

在单独的电子邮件中发送每个通知 – 启用后，收件人将收到有关每个单独通知的新电子邮件。这可能导致在短时间内收到大量的电子邮件。

在此间隔后将发送新的通知电子邮件(分钟) – 在此间隔（以分钟为单位）后将新的通知发送到电子邮件。若将该值设置为 0，则将立即发送这些通知。

邮件格式

程序和远程用户或系统管理员之间的通信通过电子邮件或 LAN 消息（使用 Windows 消息服务）来进行。在大多数情况下，警报消息和通知的默认格式是最适用的。而在某些情况下，您可能需要更改事件消息的消息格式。

事件消息的格式 – 显示在远程计算机上的事件消息的格式。

威胁警告消息的格式 – 威胁警报和通知消息具有预定义的默认格式。 我们建议您不要更改该格式。 但是在某些情况下（例如，如果有自动电子邮件处理系统），可能需要更改邮件格式。

字符集 – 基于 Windows 区域设置（例如□windows-1250□Unicode (UTF-8)□ACSII 7-bit 或日语 (ISO-2022-JP)□□因此□"á" 将更改为 "a" 以及将未知符号更改为 ″?″。

使用可打印字符引用编码 – 电子邮件源将编码为使用 ASCII 字符的引用可打印 (QP) 格式，可通过 8 位格式电子邮件正确传输特殊国家字符 (áéíóú)□

在消息中，关键字（用 % 符号隔开的字符串）由指定的实际信息替换。以下关键字可用：

- **%TimeStamp%** – 事件的日期和时间
- **%Scanner%** – 相关模块
- **%ComputerName%** – 发生警报的计算机的名称
- **%ProgramName%** – 生成警报的程序
- **%InfectedObject%** – 被感染文件、邮件等的名称
- **%VirusName%** – 感染标识
- **%Action%** – 针对渗透采取的操作
- **%ErrorDescription%** – 非病毒事件的说明

关键字 **%InfectedObject%** 和 **%VirusName%** 仅用于威胁警告邮件，而 **%ErrorDescription%** 仅用于事件邮件。

通知自定义

在此窗口中，您可以自定义通知中使用的消息。

默认通知消息 – 要显示在通知页脚的默认消息。

威胁

启用**不要自动关闭恶意软件通知**使恶意软件通知保留在屏幕上，直到用户手动将其关闭。

禁用**使用默认消息**并在**威胁通知消息**字段中输入您自己的消息，以使用自定义的通知消息。

隔离区

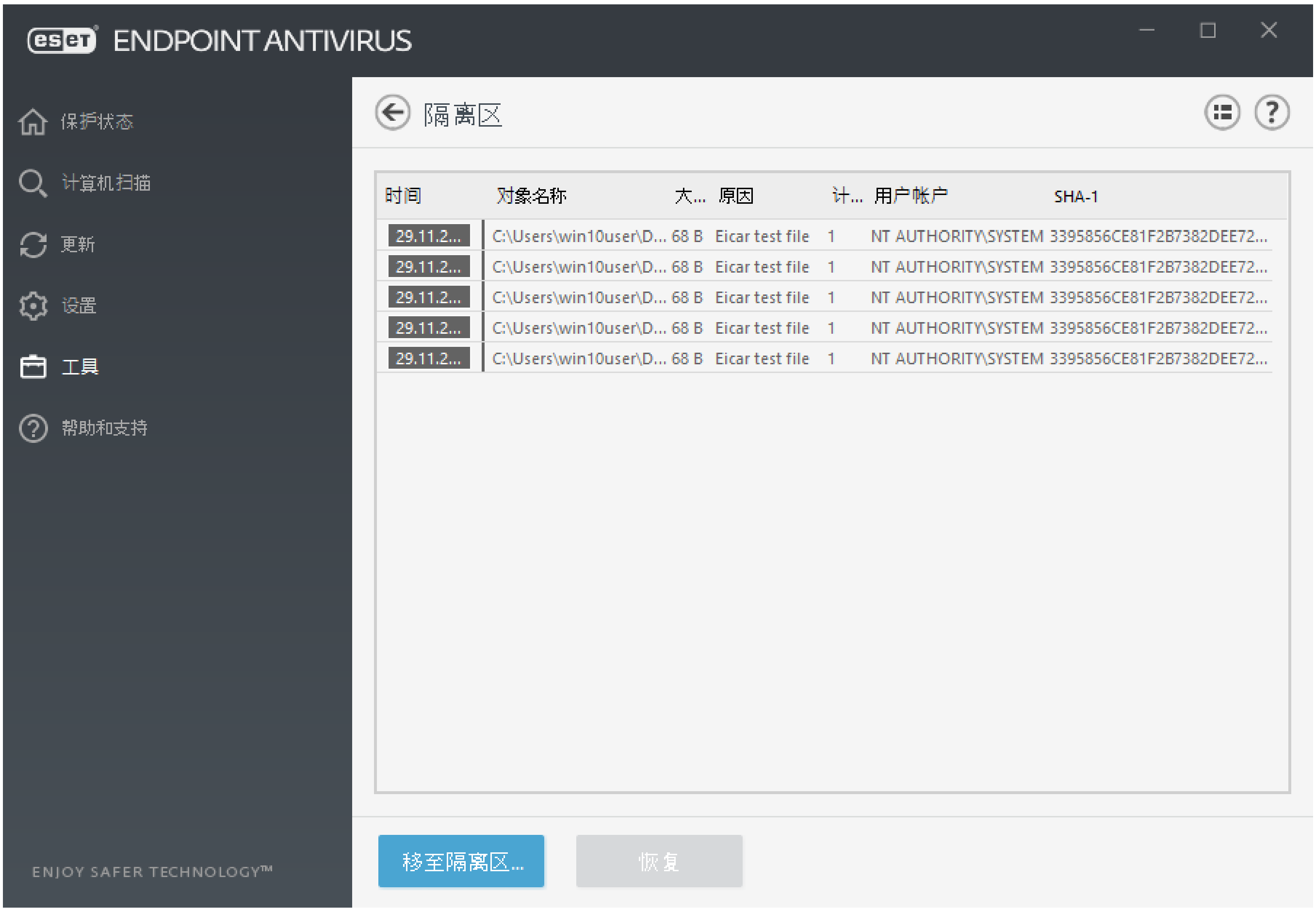
隔离区的主要功能是安全地存储报告的对象（例如恶意软件、被感染的文件或潜在不受欢迎的应用程序）。

可从 ESET Endpoint Antivirus 主程序窗口中访问隔离区，方法是依次单击**工具 > 隔离**。

可在表格中查看储存在隔离区文件夹中的文件，该表格中将显示以下内容：

- 隔离的日期和时间、
- 文件原始位置的路径、
- 文件大小（字节数）、
- 原因（例如，用户添加的对象）、
- 以及许多检测（例如，同一文件的重复检测，或者如果该文件是包含多个渗透的压缩文件）。

- 我远程管理客户端工作站上的隔离区



隔离文件

ESET Endpoint Antivirus 会自动隔离已删除的文件（如果尚未在警告窗口中取消该选项）。

如果其他文件出现以下情况，还应隔离这些文件：

a.无法清除、

b.如果不安全或建议删除、

c.如果它们由 ESET Endpoint Antivirus 误检测到、

d.或者，如果文件行为可疑但未被扫描程序检测到。

要隔离文件，有多个选项可供使用：

a.使用拖放功能手动隔离文件，方法是单击文件、长按鼠标按钮的同时将鼠标指针移动到标记区域，然后释放它。在此之后，应用程序会移动到前台。

b.在主程序窗口中，单击**移至隔离区**

c.还可以使用右键菜单达到此目的；在**隔离区**窗口中右键单击，然后选择**隔离**

从隔离恢复

隔离的文件还可以恢复到其原始位置：

- 通过在隔离区中右键单击给定文件，即可使用右键菜单提供的**恢复**功能来实现此目的。
- 如果文件被标记为潜在不受欢迎的应用程序，将启用**恢复并从扫描中排除**选项。另请参阅排除。
- 右键菜单还提供**恢复至** 选项，使用此选项可将文件恢复到其被删除时位置之外的其他位置。
- 恢复功能在某些情况下不可用，例如位于只读网络共享上的文件。

从隔离区中删除

右键单击给定项并选择**从隔离区中删除**，或者选择要删除的项并在键盘上按 **Delete** 键。还可以选择多个项，然后将它们一起删除。删除的项将从设备和隔离区中永久删除。

提交隔离区中的文件

如果程序未检测到您隔离的可疑文件，或文件被错误地确认为被感染（如启发式扫描代码分析所做的评估）并被隔离，请将该样本发送到 ESET 研究实验室进行分析。要提交文件，请右键单击该文件并从右键菜单中选择**提交供分析**。

以下 ESET 知识库文章可能仅提供英文版：
- 管理 ESET PROTECT 中的隔离区
- 我的 ESET 产品向我发送检测通知，我该怎么办？

代理服务器设置

在大型局域网网络中，计算机与 Internet 之间的通信可通过代理服务器进行协调。使用此配置时需要定义以下设置。否则程序将无法自动更新。在 ESET Endpoint Antivirus 中，“高级设置”树中的两个不同部分提供了代理服务器设置。

首先，可以在**高级设置**（在**工具 > 代理服务器**下）中配置代理服务器设置。在此级别指定的代理服务器定义了所有 ESET Endpoint Antivirus 的全局代理服务器设置。此处的参数将用于需要连接到 Internet 的所有模块。

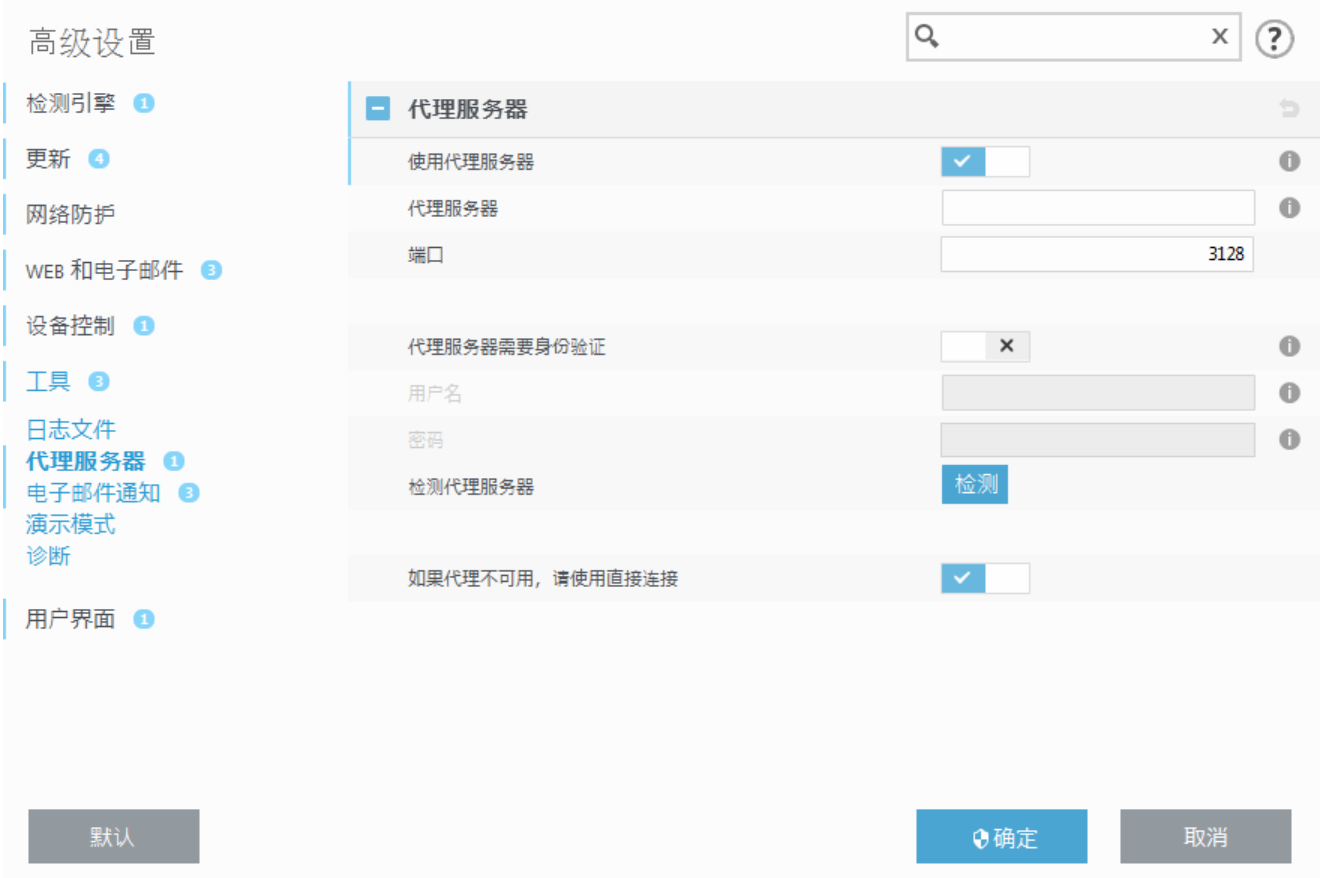
若要指定此级别的代理服务器设置，请选中**使用代理服务器**，然后在**代理服务器**字段输入代理服务器地址以及该代理服务器的**端口**号。

如果与代理服务器的通信需要验证，请选中**代理服务器需要验证**，然后在相应字段中输入有效**用户名**和**密码**。单击**检测代理服务器**以自动检测和填充代理服务器设置。将复制在 Internet Explorer 或 Google Chrome 的 Internet 选项中指定的参数。

您必须在**代理服务器**设置中输入用户名和密码。

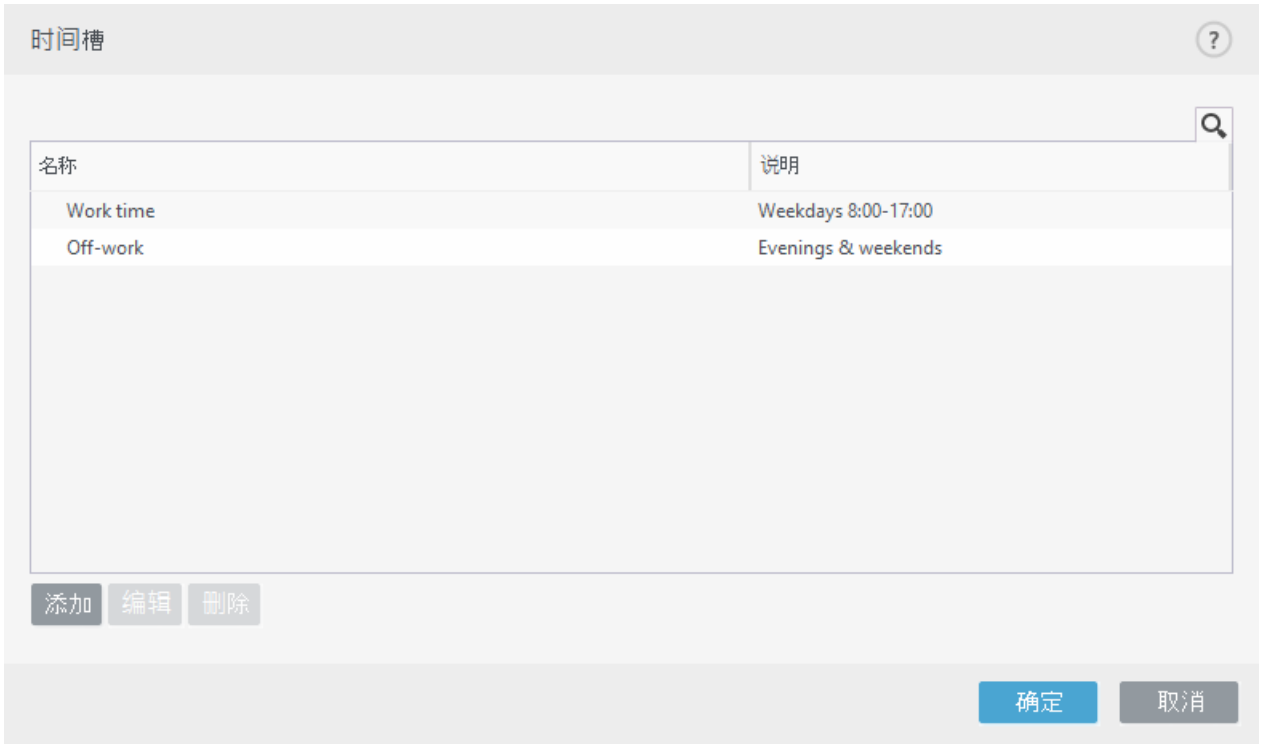
如果代理不可用，则使用直接连接 – 如果 ESET Endpoint Antivirus 配置为通过代理连接且代理不可用，ESET Endpoint Antivirus 将绕过代理并直接与 ESET 服务器通信。

还可以在“高级更新”设置中建立代理服务器设置（通过从**代理模式**下拉菜单中选择**通过代理服务器连接**来选择**高级设置 > 更新 > 配置文件 > 更新 > 连接选项**）。此设置适用于给定更新配置文件，并建议笔记本电脑用户使用，因为他们经常从远程位置接收检测引擎更新。有关此设置的详细信息，请参阅高级更新设置。



时间槽

可以创建时间槽，然后将其分配到**设备控制时间槽**设置可在**高级设置 > 工具**中找到。这使您可以定义常用时间槽（例如，工作时间、周末等）并轻松地重新使用它们，而无需重新定义每个规则的时间范围。时间槽适用于支持基于时间控制的任何相关类型的规则。



若要创建时间槽，请完成以下操作：

1.依次单击**编辑 > 添加**。

2.键入时间槽的名称和**说明**，然后单击**添加**。

3.指定时间槽的日期和开始/结束时间，或选择**整天**。

4.单击**确定**以确认。

可以使用基于日期和时间的一个或多个时间范围来定义单个时间槽。在创建时间槽后，它将显示在**应用期间**下拉菜单中（该菜单位于设备控制规则编辑器窗口.

Microsoft Windows 更新

Windows 更新功能是防止用户遭受恶意软件攻击的重要组件。出于此原因，即时安装 Microsoft Windows 更新很重要。ESET Endpoint Antivirus 会根据您指定的级别，通知您有关错过的更新。可用级别包括：

- **无更新** – 没有提供可供下载的系统更新。
- **可选更新** – 将提供标记为低优先级及更高优先级的更新以供下载。
- **建议的更新** – 将提供标记为常用及更高优先级的更新以供下载。
- **重要更新** – 将提供标记为重要及更高优先级的更新以供下载。
- **关键更新** – 仅提供关键更新以供下载。

单击**确定**可保存更改。在验证更新服务器的状态后将显示系统更新窗口。因此，在保存更改后系统更新信息可能无法立即使用。

许可证间隔检查

ESET Endpoint Antivirus 需要自动连接到 ESET 服务器。若要更改此设置，请导航到**高级设置 (F5) > 工具 > 许可证**。默认情况下，**间隔检查**设置为**自动**。ESET 许可证服务器每小时检查产品数次。如果网络通信量增加，请将设置更改为**限制**以降低负载。如果选择**限制**，则 ESET Endpoint Antivirus 将每天只检查许可证一次，或在计算机重启时进行检查。

如果**间隔检查**设置设定为**限制**，则通过 ESET Business Account/ESET MSP Administrator 所做的与许可证有关的所有更改可能需要一天时间才能应用到 ESET Endpoint Antivirus 设置。

用户界面

用户界面允许您配置程序的图形用户界面 (GUI) 行为。

使用用户界面元素工具，您可以调整程序的视觉外观和使用的效果。

为提供您的安全软件的最大安全性，您可以使用访问设置工具来阻止所有未经授权的更改。

通过配置警报和消息框和通知，即可更改检测警报和系统通知的行为。可根据您的需求自定义这些设置。

如果您选择不显示某些通知，它们将显示在**用户界面元素 > 应用程序状态**中。您可以在此处检查这些通知的状态，或者可以阻止显示它们。

右键单击选中的对象后，就会显示右键菜单集成。使用此工具将 ESET Endpoint Antivirus 控件元素集成到右键菜单中。

演示模式对于用户来说非常有用，他们希望在不受弹出窗口、计划任务和任何会加重处理器和 RAM 负担组件的影响下使用应用程序。

另请参阅如何最小化 ESET Endpoint Antivirus 用户界面（可用于托管环境）。

用户界面元素

ESET Endpoint Antivirus 中的用户界面配置选项允许您调整工作环境以符合您的需要。可以从 ESET Endpoint Antivirus 高级设置树的**用户界面 > 用户界面元素**分支访问这些配置选项。

在**用户界面元素**部分中，可以调整工作环境。使用**启动模式**下拉菜单来从以下图形用户界面 (GUI) 启动模式中进行选择：

完整 – 将显示完整 GUI。

最小 - GUI 正在运行，但仅向用户显示通知。

手动 - GUI 在登录时不会自动启动。任何用户都可以手动启动它。

静默 – 将不会显示任何通知或警报。GUI 只能由管理员启动。此模式在托管环境中或在需要保留系统资源的情况下可能非常有用。

选择最小 GUI 启动模式且重新启动计算机后，将显示通知，但不显示图形界面。若要还原到完整的图形用户界面模式，请以管理员身份在“开始”菜单中的**所有程序 > ESET > ESET Endpoint Antivirus** 下运行 GUI，或者通过 ESET PROTECT 并使用某个策略来执行此操作。

如果希望停用 ESET Endpoint Antivirus 初始屏幕，则取消选择**启动时显示初始屏幕**。

若要使 ESET Endpoint Antivirus 在扫描期间发生重要事件时（例如，在发现威胁时或已完成扫描时）发出声音，请选中**使用声音信号**。

集成到右键菜单 – 将 ESET Endpoint Antivirus 控件元素集成到右键菜单中。

状态

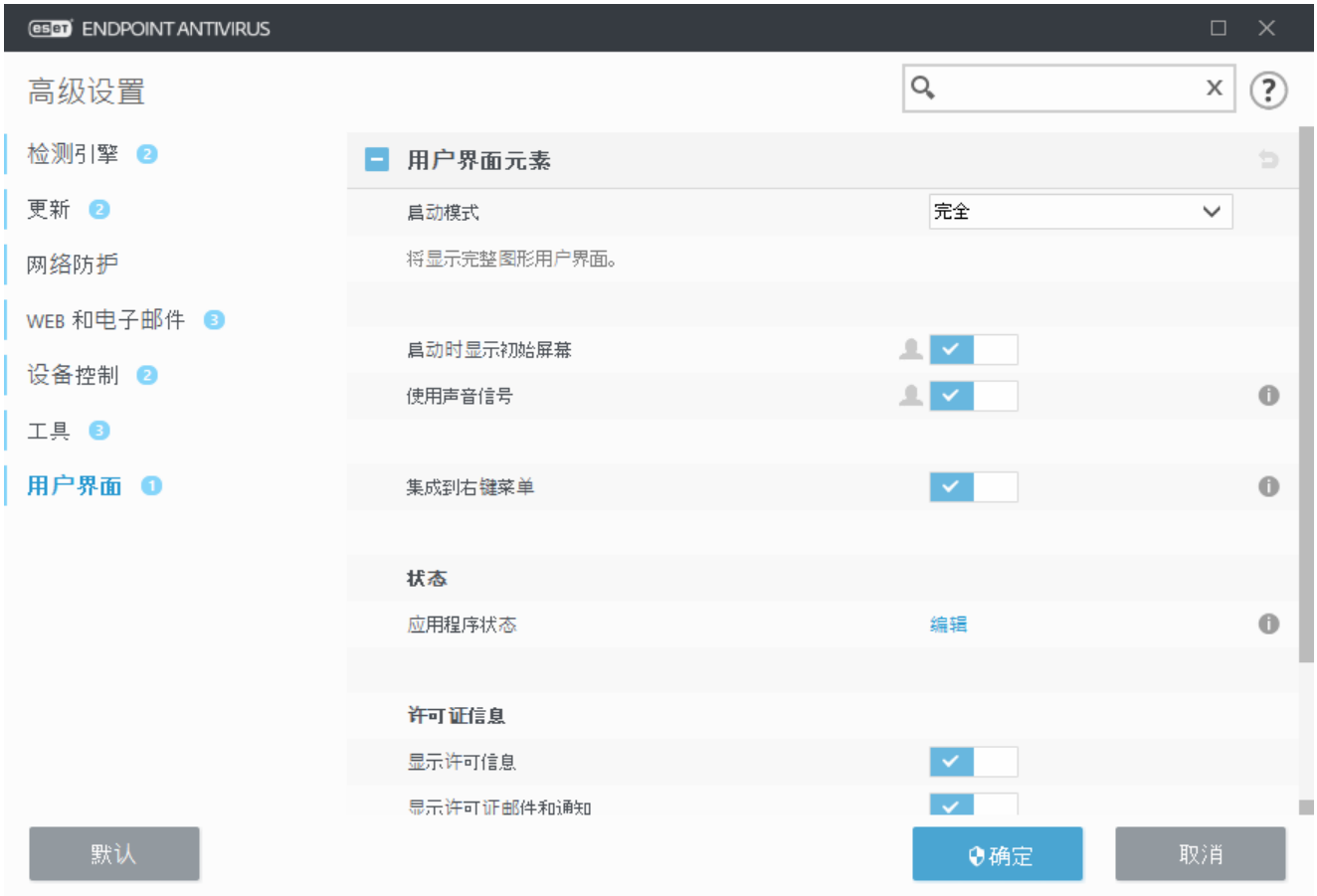
应用程序状态 – 单击**编辑**按钮以管理（禁用）在主菜单的**防护状态**窗格中显示的状态。

许可证信息

显示许可证信息 – 如果禁用，将不会在**防护状态**和**帮助和支持**屏幕上显示许可证过期日期。

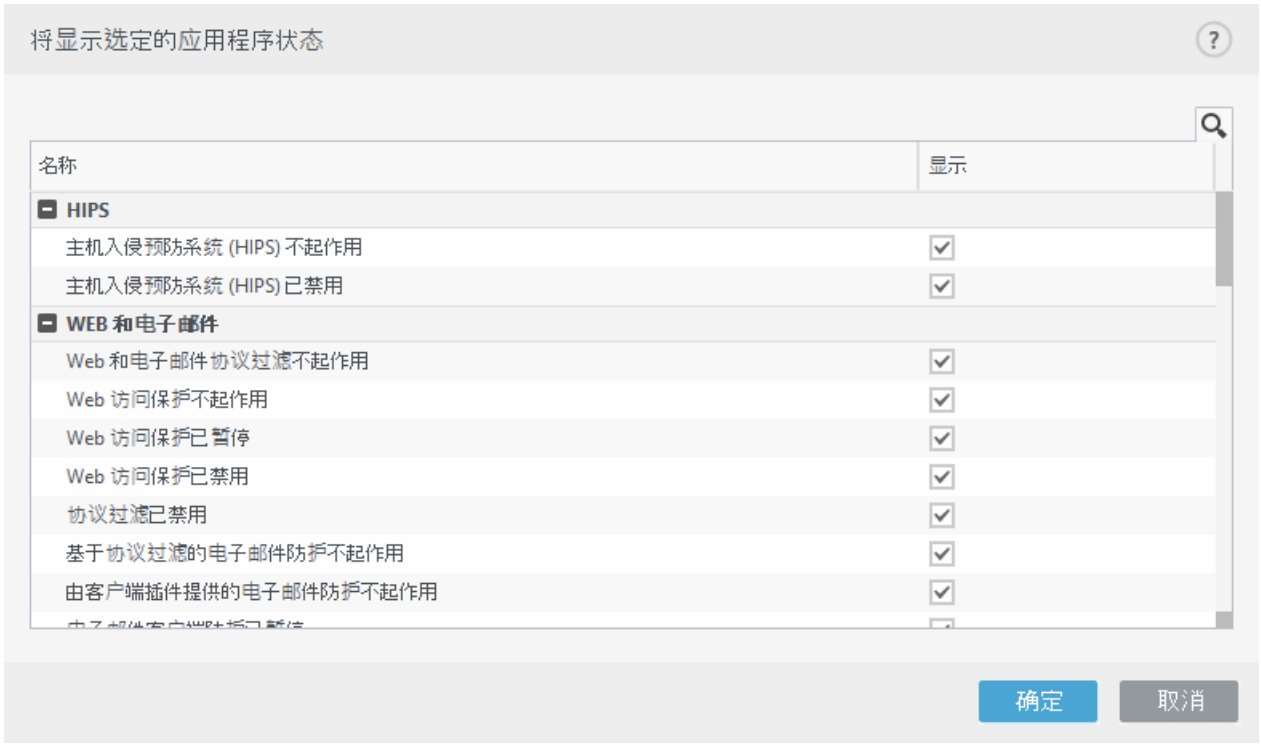
显示许可证邮件和通知 – 禁用该选项后，仅当许可证到期后才会显示通知和消息。

将应用许可证信息设置，但不适用于 MSP 许可证激活的 ESET Endpoint Antivirus。



应用程序状态

若要在 ESET Endpoint Antivirus 的第一个窗格中调整产品内状态，请导航到 ESET Endpoint Antivirus 高级设置树的**用户界面 > 用户界面元素 > 应用程序状态**。



可以启用或禁用将显示哪些应用程序状态。例如，在暂停病毒和间谍软件防护或者启用演示模式

的情况下。如果您的产品未激活或者许可证已到期，也将显示应用程序状态。可以通过 ESET PROTECT 策略更改此设置。

访问设置

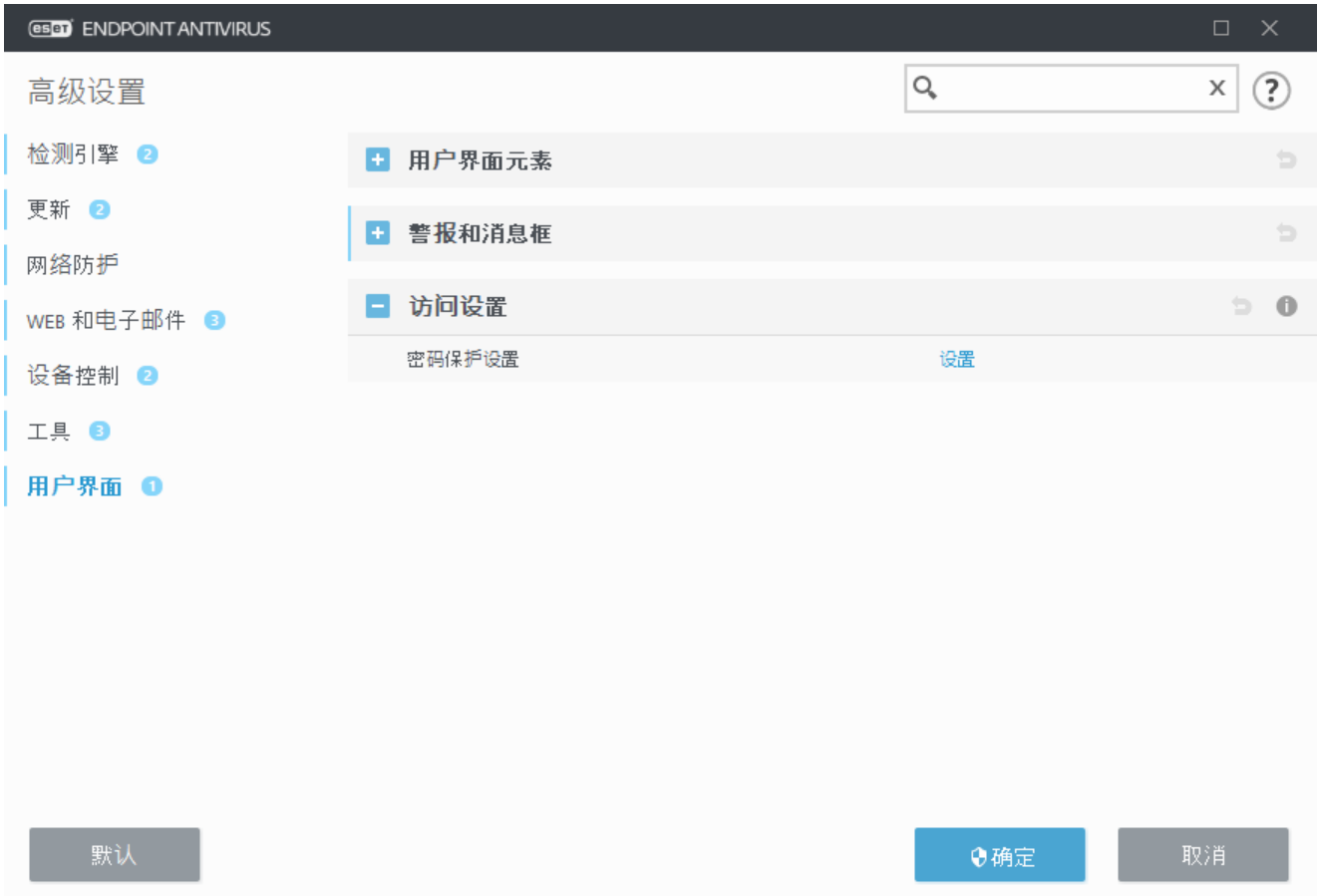
为最大限度地保障系统安全，必须正确配置 ESET Endpoint Antivirus。任何未经授权的更改都可能导致丢失重要数据。为避免进行未经授权的更改，可用密码保护 ESET Endpoint Antivirus 的设置参数。

托管环境

管理员可以创建策略以密码保护连接的客户端计算机上 ESET Endpoint Antivirus 的设置。若要创建新策略，请参阅受密码保护的设置。

未托管

密码保护的配置设置位于**高级设置 (F5)** 中的**用户界面 > 访问设置**下。



密码保护设置 – 指示密码设置。单击以打开“密码设置”窗口。

若要设置或更改密码以保护设置参数，请单击**设置**。

高级设置的密码

若要保护 ESET Endpoint Antivirus 的设置参数以避免发生未经授权的修改，必须设置新密码。

托管环境

管理员可以创建策略以密码保护连接的客户端计算机上 ESET Endpoint Antivirus 的设置。若要创建新策略，请参阅受密码保护的设置。

未托管

如果要更改现有密码：

1. 在**旧密码**字段中键入旧密码。
2. 在**新密码**和**确认密码**字段中输入新密码。
3. 单击**确定**。

以后对 ESET Endpoint Antivirus 的任何修改将需要该密码。

如果忘记密码，可以恢复对高级设置的访问。

- 使用“恢复密码”方法恢复（版本 7.1 及以上版本）
- 使用 ESET 解锁工具恢复（版本 7.0 及以下版本）

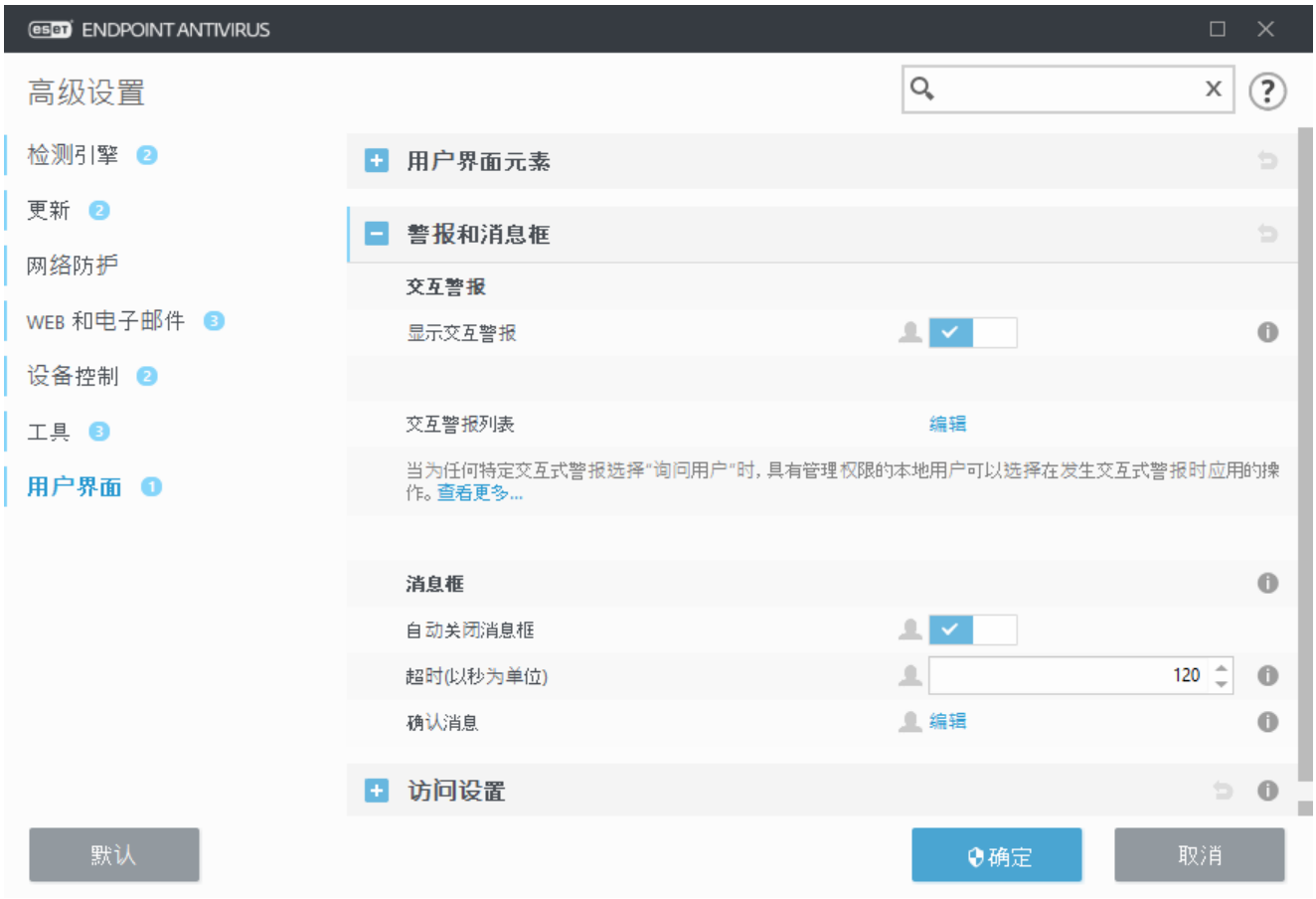
如果忘记了 ESET 发布的许可证密钥、许可证的到期日期或 ESET Endpoint Antivirus 的其他许可证信息，请阅读更多信息。

警报和消息框

正在查找有关常见警报和通知的信息？
- 发现威胁
- 地址已被阻止
- 产品未激活
- 已有可用更新
- 更新信息不一致
- “模块更新失败”消息的疑难解答
- “文件损坏”或“无法重命名文件”
- 已吊销网站证书
- 已阻止网络威胁

用户界面下的**警报和消息框**部分让您可以配置 ESET Endpoint Antivirus 如何处理检测，其中需要

由用户做出决定（例如，潜在的网络钓鱼网站）。



交互警报

如果找到检测或者如果要求用户干预，则显示交互警报窗口。

显示交互警报

ESET Endpoint Antivirus 版本 7.2 及更高版本：

- 对于未托管的用户，我们建议将此选项保留为其默认设置（启用）。
- 对于托管用户，将此设置保留为启用，并在交互警报列表中为用户选择一项预定义的操作。

禁用**显示交互警报**将隐藏所有警报窗口和浏览器内对话框。将自动选择预定义的默认操作（例如，将阻止“潜在网络钓鱼网站”）。

ESET Endpoint Antivirus 版本 7.1 及更低版本：

此设置的名称为**显示警报**，而且不能为特定交互式警报窗口自定义预定义的操作。

桌面通知

桌面通知和气球提示仅作为信息提示方式，不需要用户交互。**桌面通知**部分已移动到“高级设置”中的**工具 > 通知**下（版本 7.1 及更高版本）。

消息框

若要在一段时间后自动关闭弹出窗口，请选择**自动关闭消息框**。如果未手动关闭，警报窗口会在超过指定时限后自动关闭。

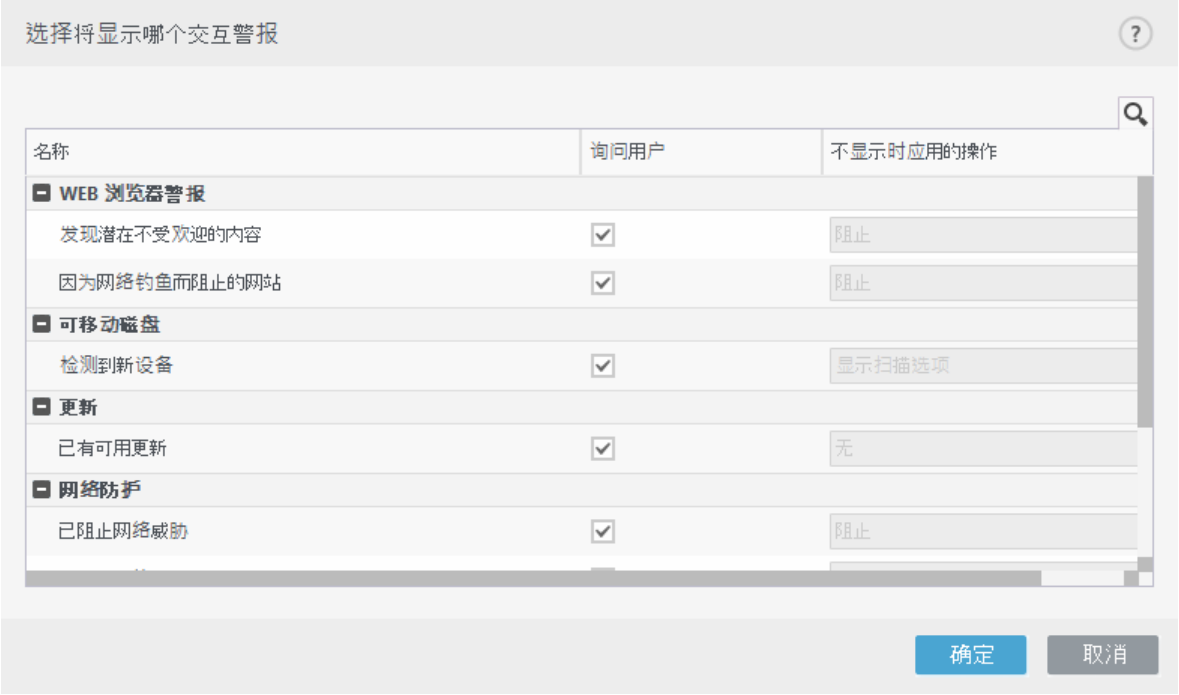
确认消息 – 向您显示确认消息列表（可以从中选择是否显示相应确认消息）。

交互警报

本部分概述了在执行任何操作之前 ESET Endpoint Antivirus 将显示的几个交互警报窗口。

要调整可配置的交互警报的行为，请导航到 ESET Endpoint Antivirus 高级设置树的**用户界面 > 警报和消息框 > 交互警报列表**，并单击**编辑**。

> 可用于托管环境，其中管理员可以在任何地方取消选择**询问用户**，并选择一项在显示交互警报窗口时应用的预定义操作。
> 另请参阅产品内应用程序状态。



查看其他帮助部分，获取对特定交互警报窗口的参考：

可移动磁盘

- 检测到新设备

安全的浏览器

- 允许在默认浏览器中继续

网络防护

- 当在来自 ESET PROTECT 的此工作站上触发了**将计算机与网络隔离**客户端任务时显示已阻止网络访问。
- 已阻止网络通信
- 已阻止网络威胁

Web 浏览器警报

- 发现潜在不受欢迎的内容
- 因为网络钓鱼而阻止的网站

计算机

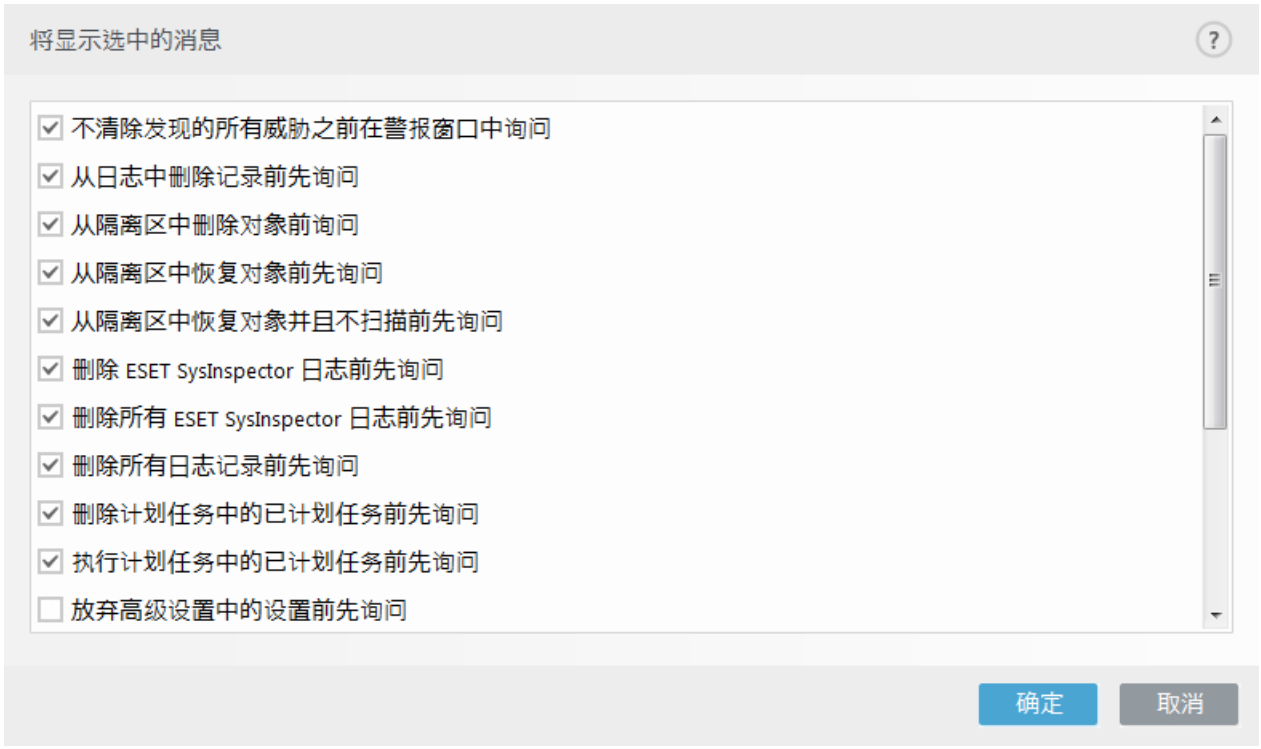
这些警报的出现会将用户界面更改为橙色：

- 重新启动计算机（必需）
- 重新启动计算机（建议）

> 交互警报不包含检测引擎、HIPS 或防火墙交互窗口 – 因为在特定功能中可以单独配置其行为。

确认消息

若要调整确认消息，请导航到 ESET Endpoint Antivirus 高级设置树的**用户界面 > 警报和消息框 > 确认消息**，并单击**编辑**。



该对话窗口将显示在执行任何操作之前 ESET Endpoint Antivirus 显示的确认消息。选中或取消选中每条确认消息旁的复选框以启用或禁用它。

详细了解与确认消息有关的特定功能：

- 删除 ESET SysInspector 日志前先询问
- 删除所有 ESET SysInspector 日志前先询问
- 从隔离区中删除对象前询问
- 放弃高级设置中的设置前先询问
- 不清除发现的所有威胁之前在警报窗口中询问
- 从日志中删除记录前先询问
- 删除计划任务中的已计划任务前先询问
- 删除所有日志记录前先询问
- 重置统计前先询问
- 从隔离区中恢复对象前先询问
- 从隔离区中恢复对象并且不扫描前先询问
- 执行计划任务中的已计划任务前先询问
- 显示 Outlook Express 和 Windows Mail 电子邮件客户端的产品确认对话框

- 显示 Windows Live Mail 的产品确认对话框
- 显示 Outlook 电子邮件客户端的产品确认对话框

高级设置冲突错误

如果某个组件（如 HIPS、和用户同时在交互或学习模式下创建规则，可能会发生此错误。

> 如果您想要创建自己的规则，我们建议将过滤模式更改为默认的**自动模式**。 阅读有关 HIPS 和 HIPS 过滤模式的更多信息。

可移动磁盘

当可移动磁盘 (CD/DVD/USB/...) 插入计算机时、ESET Endpoint Antivirus 对其进行自动扫描。如果计算机管理员希望防止用户使用带有不请自来内容的可移动磁盘，此模块可能很有用。

插入可移动磁盘并且在 ESET Endpoint Antivirus 中设置了**显示扫描选项**后，将显示以下对话框：

用于此对话框的选项：

- **立即扫描** – 这将触发对可移动磁盘的扫描。
- **稍后扫描** – 将推迟对可移动磁盘的扫描。
- **设置** – 打开**“高级设置”**部分。
- **始终使用选择的选项** – 选中后，在其他时间插入可移动磁盘时将执行相同的操作。

此外、ESET Endpoint Antivirus 具有设备控制功能，允许您为给定计算机上的外部设备使用定义规则。在设备控制部分可找到设备控制的更多详细信息。

ESET Endpoint Antivirus 7.2 及更高版本

要访问可移动磁盘扫描的设置，请依次打开高级设置（**F5**）> **用户界面** > **警报和消息框** > **交互警报** > **交互警报列表** > **编辑** > **检测到的新设备**、

如果未选择**询问用户**，请在将可移动磁盘插入到计算机后选择所需操作：

- **不扫描** – 将不执行任何操作，并且不打开**检测到新设备**窗口。

- **自动设备扫描** – 将执行已插入可移动磁盘设备的计算机扫描。
- **显示扫描选项** – 打开**交互警报**设置部分。

ESET Endpoint Antivirus 7.1 及以下版本

要访问可移动磁盘扫描的设置，请打开高级设置（**F5**）> **检测引擎** > **恶意软件扫描** > **可移动磁盘**。

插入可移动磁盘后要采取的操作 – 选择将可移动磁盘设备 (CD/DVD/USB) 插入到计算机时将执行的默认操作。选择在将可移动磁盘插入计算机时的所需操作：

- **不扫描** – 将不执行任何操作，并且不打开**检测到新设备**窗口。
- **自动设备扫描** – 将执行已插入可移动磁盘设备的计算机扫描。
- **显示扫描选项** – 打开**可移动磁盘**设置部分。

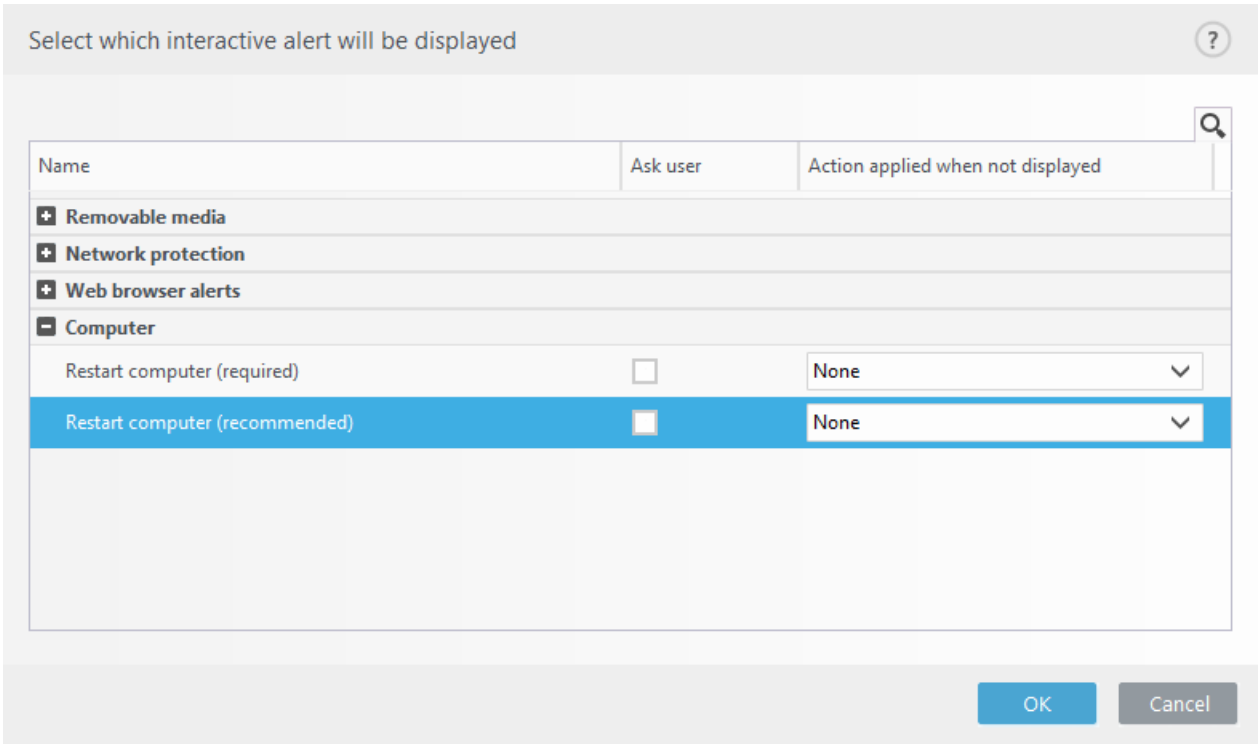
需要重新启动

如果端点计算机正在接收“需要重新启动”红色警报，可以禁止显示该警报。

要禁用“需要重新启动”或“建议重新启动”警报，请按照以下步骤操作：

1. 按 **F5** 键以访问高级设置，然后展开**警报和消息框**部分。

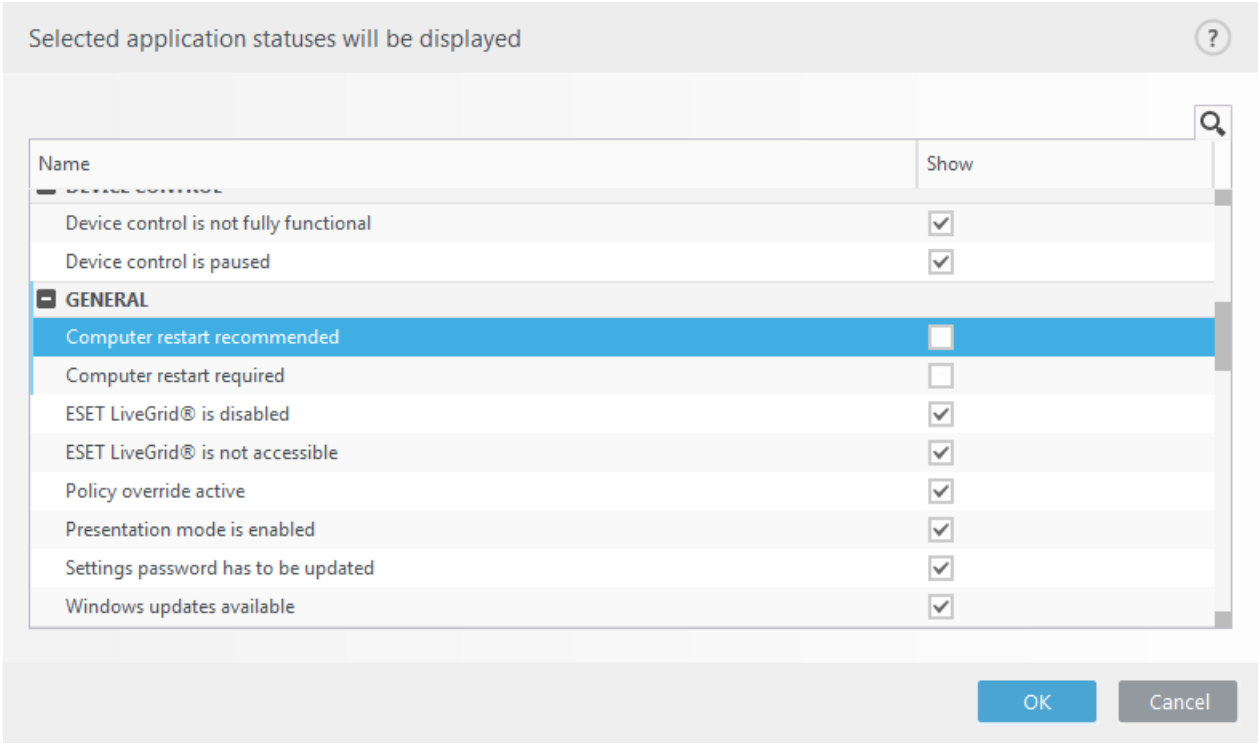
2. 单击**交互警报列表**旁边的**编辑**。在**计算机**部分中，取消选中**重新启动计算机（需要）**和**重新启动计算机（建议）**旁边的复选框。



3. 单击**确定**以将更改保存在两个打开的窗口中。

4. 警报将不再显示在端点计算机上。

5. （可选）要禁用 ESET Endpoint Antivirus 主程序窗口中的应用程序状态，请在应用程序状态窗口中取消选中**需要重新启动计算机**和**建议重新启动计算机**旁边的复选框。



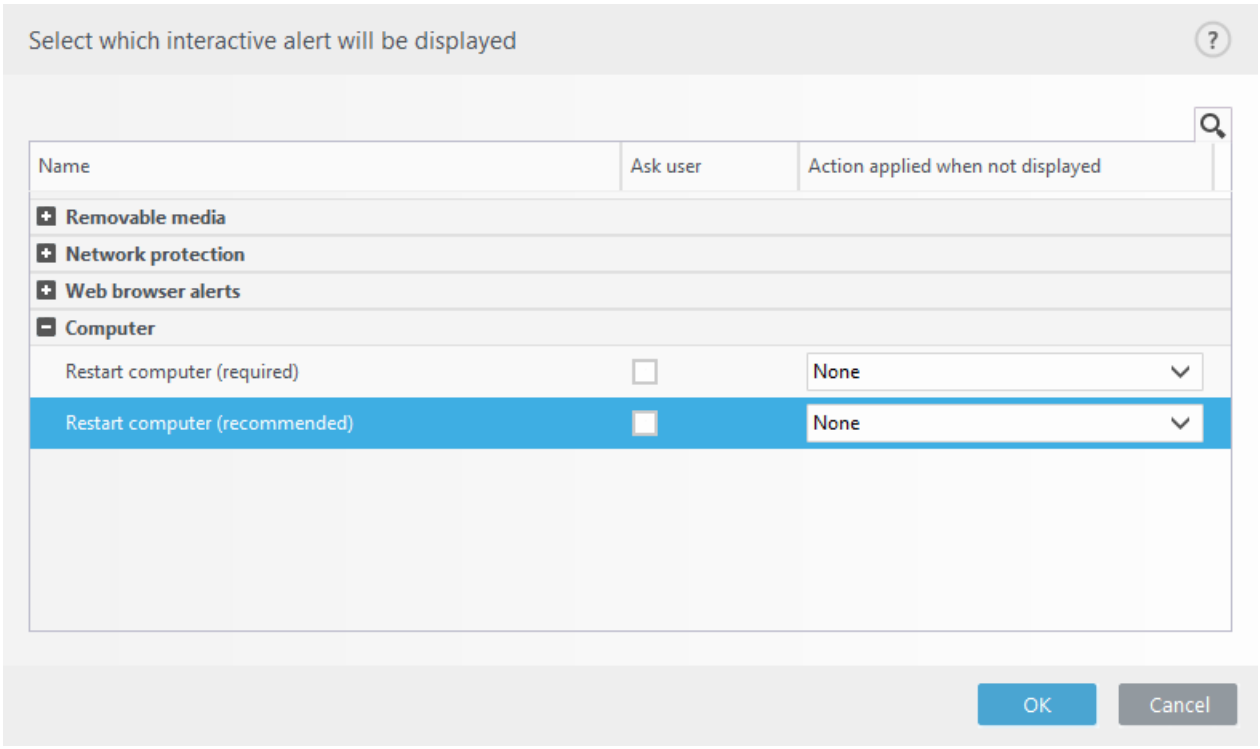
建议重新启动

如果端点计算机正在接收“建议重新启动”黄色警报，可以禁止显示该警报。

要禁用“需要重新启动”或“建议重新启动”警报，请按照以下步骤操作：

1. 按 **F5** 键以访问高级设置，然后展开**警报和消息框**部分。

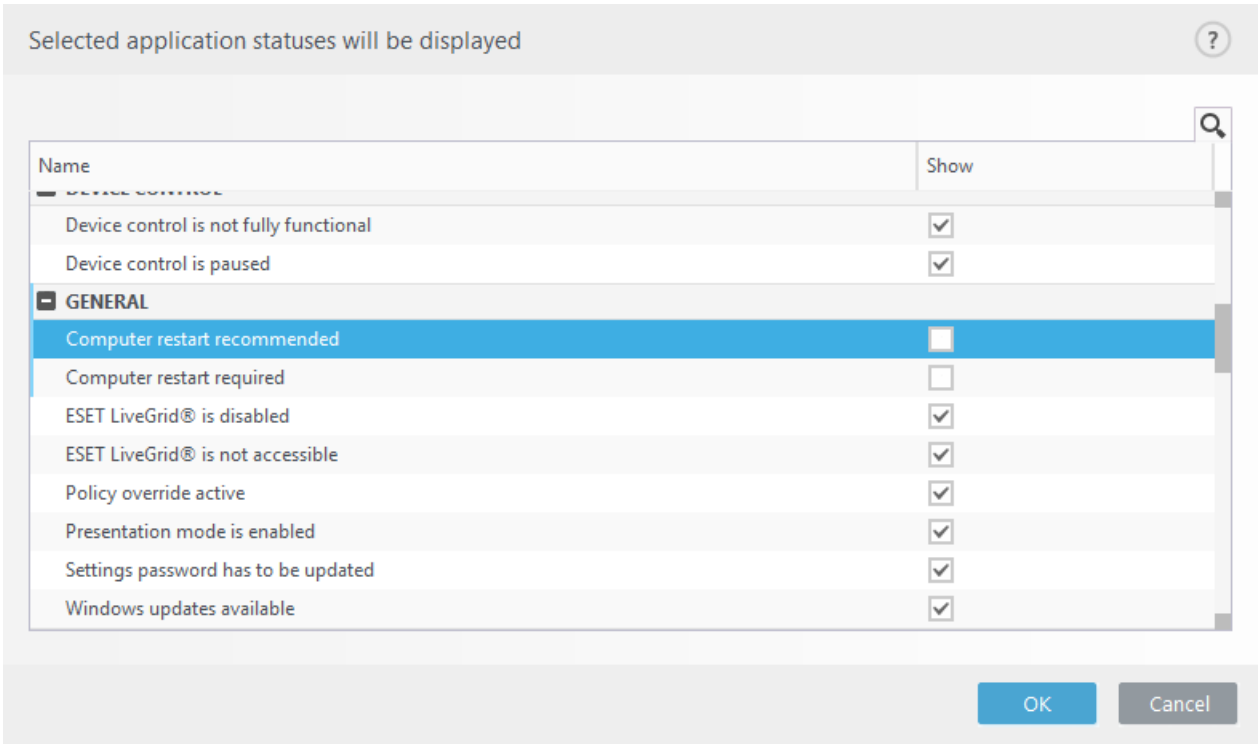
2. 单击**交互警报列表**旁边的**编辑**。在**计算机**部分中，取消选中**重新启动计算机(需要)** 和**重新启动计算机(建议)**旁边的复选框。



3. 单击**确定**以将更改保存在两个打开的窗口中。

4. 警报将不再显示在端点计算机上。

5. （可选）要禁用 ESET Endpoint Antivirus 主程序窗口中的应用程序状态，请在应用程序状态窗口中取消选中**需要重新启动计算机**和**建议重新启动计算机**旁边的复选框。



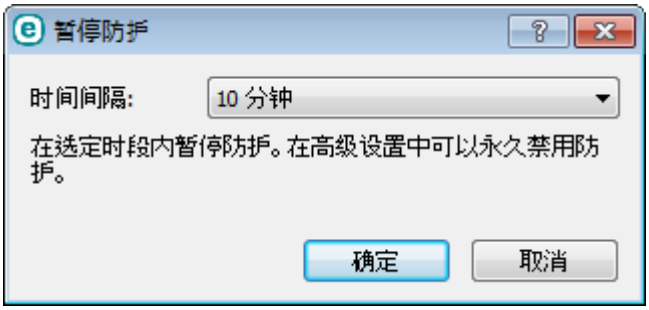
系统托盘图标

可通过右键单击系统托盘图标 使用一些最重要的设置选项和功能。

要访问系统托盘图标菜单，请确保用户界面元素的启动模式设置为“完全”。

暂停防护 – 显示禁用检测引擎的确认对话框，这些防护通过控制文件Web 和电子邮件通信来保护系统免受攻击。

时间间隔下拉菜单表示将为其禁用防护的时段。



高级设置 – 选择此项以进入**高级设置**树。您还可以通过按 F5 键或导航到**设置 > 高级设置**来访问高级设置。

日志文件 - 日志文件包含所有已发生的重要程序事件的信息，并提供检测的概要信息。

打开 ESET Endpoint Antivirus – 从托盘图标打开 ESET Endpoint Antivirus 主程序窗口。

重置窗口布局 – 将 ESET Endpoint Antivirus 窗口重置为其默认大小和屏幕位置。

检查更新 – 开始更新程序模块，以确保对恶意代码的防护级别。

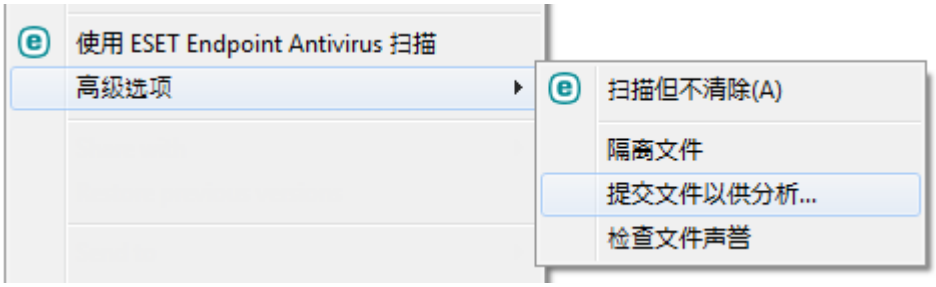
关于 – 提供系统信息、有关已安装的 ESET Endpoint Antivirus 版本和安装的程序模块的详细信息，以及您的许可证到期日期。有关您的操作系统和系统资源的信息可以在页面底部找到。

右键菜单

右键单击对象（文件）后，就会显示右键菜单。该菜单将列出您可以在对象上执行的所有操作。

可以将 ESET Endpoint Antivirus 控件元素集成到右键菜单中。此功能的设置选项在**用户界面 > 用户界面元素**下的高级设置树中提供。

集成到右键菜单 – 将 ESET Endpoint Antivirus 控件元素集成到右键菜单中。



帮助和支持

ESET Endpoint Antivirus 包含故障排除工具和支持信息，可用于帮助您解决可能遇到的问题。

已安装的产品

- **关于 ESET Endpoint Antivirus** – 显示有关 ESET Endpoint Antivirus 副本的信息。
- 产品疑难解答 – 单击此链接以查找大多数常见问题的解决方案。
- 许可证疑难解答 – 单击此链接以查找激活或许可证更改问题的解决方案。
- 更改许可证 – 单击以启动激活窗口并激活您的产品。

帮助页面 – 单击此链接以启动 ESET Endpoint Antivirus 帮助页面。

技术支持

- **请求支持** – 如果找不到问题的答案，可以使用位于 ESET 网站上的该表单，来快速联系技术支持部门。根据您的设置，在填写 Web 表单之前将显示提交系统配置数据窗口。
- **技术支持详细信息** – 如果出现提示，可以复制信息并将其发送给 ESET 技术支持（如产品名称、产品版本、操作系统和处理器类型）。
- **ESET Log Collector** – 链接到 ESET 知识库文章，可以在其中下载 ESET Log Collector。它是一种从计算机自动收集信息和日志以帮助更快速地解决问题的应用程序。有关详细信息，请参阅 ESET Log Collector 联机用户手册。

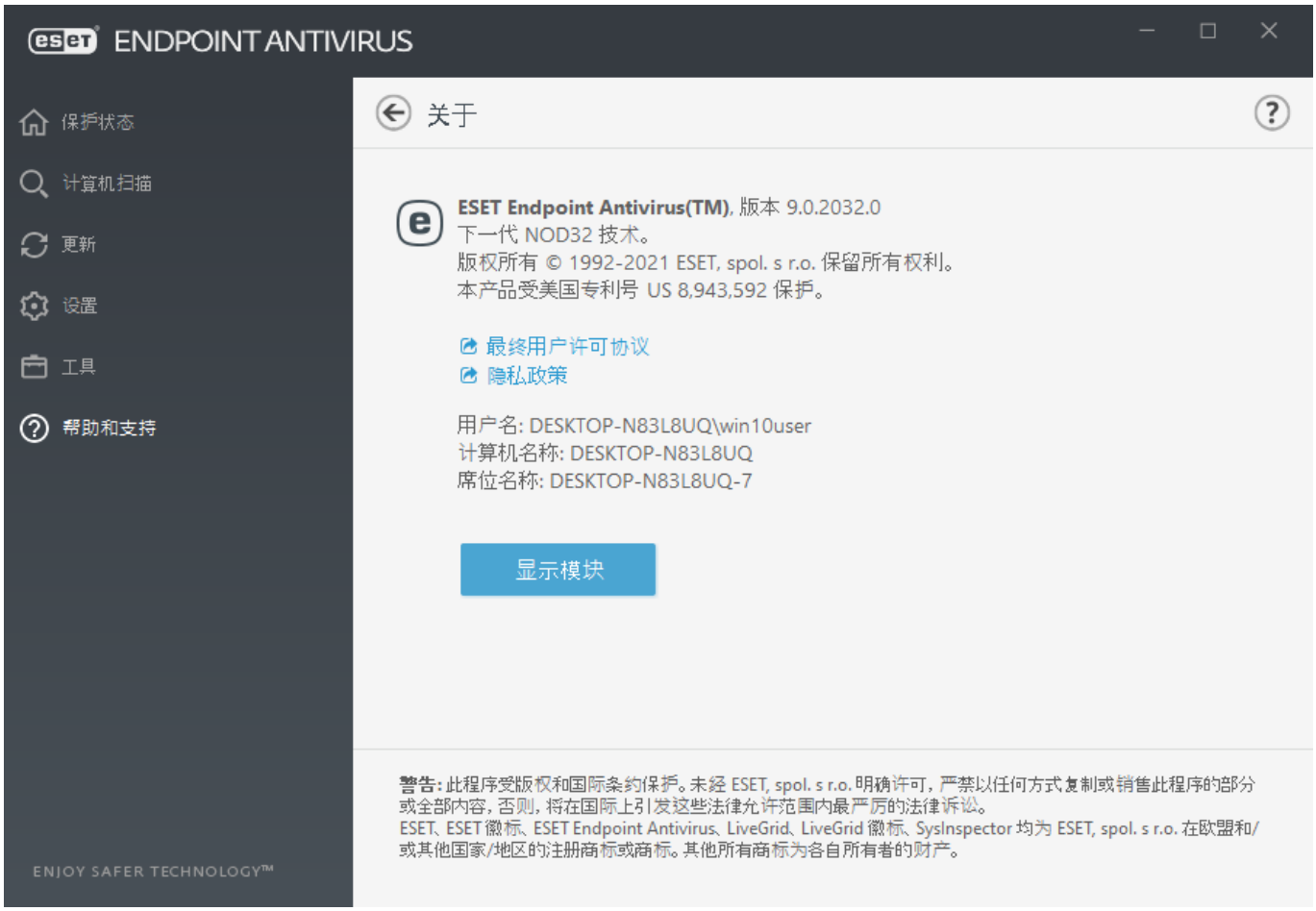
• 启用高级日志记录以为所有可用功能创建高级日志，从而帮助开发人员诊断并解决问题。日志记录的最低级别设置为诊断级别。高级日志记录将在两小时后自动禁用，除非通过单击停止高级日志记录提前将其停止。创建所有日志后，会显示通知窗口，从而可直接访问含有已创建日志的“诊断”文件夹。

知识库 - ESET 知识库包含对大多数常见问题的解答以及各种问题的建议解决方案。 知识库由 ESET 专业技术人员定期更新，它已成为解决各类问题的最强大工具。

关于 ESET Endpoint Antivirus

此窗口提供有关 ESET Endpoint Antivirus 的已安装版本、您的操作系统和系统资源的详细信息。

单击**已安装的组件**，可查看有关已安装程序模块及其版本列表的信息。可以单击**复制**将有关模块的信息复制到剪贴板。这在排除故障或联系技术支持时可能有用。



提交系统配置数据

为了尽可能快速准确地提供支持，ESET 需要有关 ESET Endpoint Antivirus 配置的信息、详细的系统信息以及关于正在运行的进程（ESET SysInspector 日志文件）和注册表数据的信息。 ESET 仅将此数据用于为客户提供技术帮助。

提交 Web 表单后，系统配置数据将提交给 ESET。如果希望记住对此过程执行的该操作，请选择

始终提交此信息。若要在不发送任何数据的情况下提交此表格，请单击**不提交数据**，然后可以通过在线支持表单来联系 ESET 技术支持。

也可以在**高级设置 > 工具 > 诊断 > 技术支持**中配置此设置。

> 如果您已决定提交系统数据，则需要填写并提交 Web 表单；否则将不会创建您的票证，而且您的系统数据将会丢失。

技术支持

联系技术支持

请求支持 – 如果找不到问题的答案，可以使用位于 ESET 网站上的该表单，来快速联系 ESET 技术支持部门。根据您的设置，在填写 Web 表单之前将显示提交系统配置数据窗口。

获取技术支持信息

技术支持详细信息 – 当出现提示时，可以复制信息并将其发送给 ESET 技术支持（例如，许可证详细信息、产品名称、产品版本、操作系统和计算机信息）。

ESET Log Collector – 链接到 ESET 知识库文章，可以在其中下载 ESET Log Collector它是一种从计算机自动收集信息和日志以帮助更快速地解决问题的应用程序。有关详细信息，请参阅 ESET Log Collector 联机用户手册

启用高级日志记录以为所有可用功能创建高级日志，从而帮助开发人员诊断并解决问题。日志记录的最低级别设置为**诊断**级别。高级日志记录将在两小时后自动禁用，除非通过单击**停止高级日志记录**提前将其停止。创建所有日志后，会显示通知窗口，从而可直接访问含有已创建日志的“诊断”文件夹。

配置文件管理器

配置文件管理器用在 ESET Endpoint Antivirus 中的两个地方 – 在**手动计算机扫描**部分和**更新**部分中。

手动计算机扫描

可以保存您的首选扫描参数以用于将来的扫描。建议您创建不同的配置文件（带有各种扫描目标、扫描方法和其他参数）用于每次定期扫描。

要创建新配置文件，请打开“高级设置”窗口 (F5) 并单击**病毒防护 > 手动计算机扫描**，然后单击**配置文件列表**旁边的**编辑**。列出现有扫描配置文件的**更新配置文件**下拉菜单。为了帮助您创建适合需求的扫描配置文件，请参阅 ThreatSense 引擎参数设置部分，查看扫描设置中每个参数的描述。

假设要创建自己的扫描配置文件并且**扫描计算机**配置部分适用，但不希望扫描加壳程序或潜在不安全的应用程序，并且还希望应用**严格清除**。在**配置文件管理器**窗口中输入新配置文件的名称并单击**添加**。从**选定的配置文件**下拉菜单中选择新的配置文件并调整其余参数以满足要求，然后单击**确定**以保存新配置文件。

更新

更新设置部分中的配置文件编辑器允许用户创建新的更新配置文件。请只在计算机使用多种方式连接更新服务器时，创建和使用您自己的自定义配置文件（不是默认的**我的配置文件**）。

例如，一台笔记本电脑通常连接的是本地网络中的本地服务器（镜像），但在断开与本地网络的连接时（比如出于商务旅行的需要）可能会使用两种配置文件直接从 ESET 的更新服务器下载更新：第一个连接到本地服务器，另一个连接到 ESET 的服务器。配置完这些配置文件后，浏览到**工具 > 计划任务**，编辑更新任务参数。将其中一个配置文件指定为主配置文件，另一个为次配置文件。

更新配置文件 – 当前使用的更新配置文件。要更改它，请从下拉菜单中选择一个配置文件。

配置文件列表 – 新建或删除现有更新配置文件。

键盘快捷键

若要在 ESET Endpoint Antivirus 中更好地导航，可以使用以下键盘快捷键：

键盘快捷键	已采取操作
F1	打开帮助页面
F5	打开“高级设置”
Up/Down	在产品中的项目之间导航
TAB	在窗口中移动光标
Esc	关闭活动对话窗口
Ctrl+U	显示有关 ESET 许可证和计算机的信息（技术支持详细信息）
Ctrl+R	将产品窗口重置为其默认大小和屏幕位置

诊断

诊断提供 ESET 进程（如 ekrn）的应用程序崩溃转储。如果应用程序崩溃，将生成一个转储。这能够帮助开发人员调试和修复各种 ESET Endpoint Antivirus 问题。

单击**转储类型**旁的下拉菜单，并选择以下三个可用选项之一：

- 选择**禁用**可禁用此功能。

- **小型**（默认）– 记录可能有助于识别应用程序意外崩溃原因的最小有用信息集。 此类转储文件在空间有限时有用，但是，因为所包含的信息有限，分析此文件可能无法找到不是由出现问题时正在运行的线程直接导致的错误。

• **完整** – 当应用程序意外停止时记录系统内存的所有内容。 完整的内存转储可能包含在收集内存转储时正在运行进程的数据。

目标目录 – 在崩溃期间将生成转储的目录。

打开诊断文件夹 – 单击**打开**以在新的 *Windows 资源管理器*窗口中打开此目录。

创建诊断转储 – 单击**创建**以在**目标目录**中创建诊断转储文件。

高级日志记录

启用计算机扫描程序高级日志记录 – 记录“计算机扫描”或“文件系统实时防护”扫描文件和文件夹时发生的所有事件。

启用设备控制高级日志记录 – 记录设备控制中发生的所有事件。这可以帮助开发人员诊断和修复与设备控制有关的问题。

启用 Direct Cloud 高级日志记录 – 记录产品与 Direct Cloud 服务器之间的所有产品通信。

启用文档防护高级日志记录 – 记录在文档防护中发生的所有事件，以便诊断和解决问题。

启用内核高级日志记录 – 记录 ESET 内核服务 (ekrn) 中发生的所有事件，以便诊断和解决问题（适用于版本 7.2 及更高版本）。

启用许可高级日志记录 – 记录与 ESET 激活和 ESET Business Account 服务器之间的所有产品通信。

启用内存跟踪 – 记录所有将帮助开发人员诊断内存泄漏的事件。

启用网络防护高级日志记录 – 采用 PCAP 格式记录所有通过防火墙传递的网络数据，从而帮助开发人员诊断和修复与防火墙有关的问题。

启用操作系统高级日志记录 – 将收集有关操作系统的其他信息，比如正在运行的进程□CPU 活动和磁盘操作。这可以帮助开发人员诊断并修复与操作系统上运行的 ESET 产品有关的问题。

启用协议过滤高级日志记录 – 采用 PCAP 格式记录所有通过协议过滤引擎传递的数据，从而帮助开发人员诊断并修复与协议过滤有关的问题。

启用推送邮件高级日志记录 – 记录在推送邮件过程中发生的所有事件，以允许诊断和解决问题。

启用文件系统实时防护高级日志记录 – 记录在文件系统实时防护中发生的所有事件，以方便诊断和解决问题。

启用更新引擎高级日志记录 – 记录更新过程中发生的所有事件。这可以帮助开发人员诊断并修复与更新引擎有关的问题。

日志文件位置

C:\ProgramData\ESET\ESET Endpoint Antivirus\Diagnostics

命令行扫描程序

可通过命令行启动 ESET Endpoint Antivirus 的病毒防护模块 – 手动（使用“ecls”命令）或使用批处理“bat”文件启动。

ESET 命令行扫描程序用法：

```
ecls [OPTIONS..] FILES..
```

从命令行运行手动扫描程序时，可使用以下参数和开关：

选项

/base-dir=文件夹	从“文件夹”加载模块
/quar-dir=文件夹	隔离“文件夹”
/exclude=MASK	不扫描与“掩码”匹配的文件
/subdir	扫描子文件夹（默认）
/no-subdir	不扫描子文件夹
/max-subdir-level=级别	要扫描的文件夹中的最大子文件夹层数
/symlink	跟踪符号链接（默认）
/no-symlink	跳过符号链接
/ads	扫描 ADS（默认）
/no-ads	不扫描 ADS
/log-file=文件	将结果记录到“文件”
/log-rewrite	覆盖输出文件（默认 – 附加）
/log-console	将结果记录到控制台（默认）
/no-log-console	不将结果记录到控制台
/log-all	同时记录清除文件
/no-log-all	不记录干净的文件（默认）
/aind	显示活动指示器
/auto	扫描并自动清除所有本地磁盘中的病毒

扫描程序选项

/files	扫描文件（默认）
/no-files	不扫描文件
/memory	扫描内存
/boots	扫描引导区
/no-boots	不扫描引导区（默认）
/arch	扫描压缩文件（默认）
/no-arch	不扫描压缩文件
/max-obj-size=大小	仅扫描小于指定“大小”兆字节的文件（默认值 0 = 无限制）

/max-arch-level=级别	要扫描的压缩档（嵌套压缩档）中的最大子压缩档层数
/scan-timeout=限制	扫描压缩文件超时时间（秒）
/max-arch-size=大小	如果压缩文件中的文件小于指定“大小”（默认值 0 = 无限制），则仅扫描这些文件
/max-sfx-size=大小	如果自解压文件中的各个文件小于指定“大小”兆字节（默认值 0 = 无限制），则只扫描这些文件
/mail	扫描电子邮件文件（默认）
/no-mail	不扫描电子邮件文件
/mailbox	扫描邮箱（默认）
/no-mailbox	不扫描邮箱
/sfx	扫描自解压文件（默认）
/no-sfx	不扫描自解压文件
/rtp	扫描加壳程序（默认）
/no-rtp	不扫描加壳程序
/unsafe	扫描潜在的不安全应用程序
/no-unsafe	不扫描可能不安全的应用程序（默认）
/unwanted	扫描潜在的不受欢迎应用程序
/no-unwanted	不扫描潜在不受欢迎的应用程序（默认）
/suspicious	扫描可疑应用程序（默认）
/no-suspicious	不扫描可疑应用程序
/pattern	使用病毒库（默认）
/no-pattern	不使用病毒库
/heur	启用启发式扫描（默认）
/no-heur	禁用启发式扫描
/adv-heur	启用高级启发式扫描（默认）
/no-adv-heur	禁用高级启发式扫描
/ext-exclude=具有指定扩展名的文件	不扫描具有指定“扩展名”的文件（用冒号分隔）
/clean-mode=模式	对被感染的对象使用清除“模式” 有以下选项可供使用： • `none`（默认）- 不会自动进行清除。 • `standard` - ecls.exe 将尝试自动清除或删除被感染的文件。 • `strict` - ecls.exe 将尝试自动清除或删除被感染的文件，且无需用户干预（在删除文件之前，您不会收到提示）。 • `rigorous` - ecls.exe 将在不尝试清除的情况下删除文件，无论文件是什么。 • `delete` - ecls.exe 将在不尝试清除的情况下删除文件，但将避免删除敏感文件，如 Windows 系统文件。
/quarantine	将被感染的文件（若已清除）复制到隔离区 （补充清理时执行的操作）
/no-quarantine	不将被感染的文件复制到隔离区

常规选项

/help	显示帮助并退出
/version	显示版本信息并退出
/preserve-time	保存上一个访问时戳

退出代码

0	未发现威胁
1	发现威胁并已清除
10	某些文件无法扫描（可能是威胁）
50	发现威胁
100	错误

退出代码大于 100 表示未扫描文件，该文件可能被感染。

ESET CMD

该功能支持高级 ecmd 命令。 它允许您使用命令行 (ecmd.exe) 导出和导入设置。 到目前为止，只可以使用 GUI 导出设置。ESET Endpoint Antivirus 配置可以导出为 *.xml* 文件。

启用 ESET CMD 后，有两种授权方法可用：

- **无** – 无授权。 不建议您使用此方法，因为它允许导入任何未签名的配置，这可能存在风险。
- **高级设置密码** – 需要密码才可从 *.xml* 文件导入配置，此文件必须已签名（请参阅下面的签名 *.xml* 配置文件）。 可以导入新配置之前，必须提供访问设置中指定的密码。 如果未启用访问设置、密码不匹配或 *.xml* 配置文件未签名，将不会导入配置。

ESET CMD 启用后，可使用命令行导入或导出 ESET Endpoint Antivirus 配置。 可以手动执行上述操作，也可以创建用于自动执行的脚本。

若要使用高级 ecmd 命令，您需要具有管理员权限才可以运行这些命令，或者使用**以管理员身份运行**打开 Windows 命令提示符 (cmd)。 否则，您会收到 **Error executing command** 消息。 此外，导出配置时，目标文件夹必须已存在。 ESET CMD 设置关闭时，导出命令仍可正常工作。

高级 ecmd 命令只能在本地运行。暂停 ecmd 命令只能通过客户端任务**运行命令**使用 ESET PROTECT 来执行。

导出设置命令：

```
ecmd /getcfg c:\config\settings.xml
```

导入设置命令：

```
ecmd /setcfg c:\config\settings.xml
```

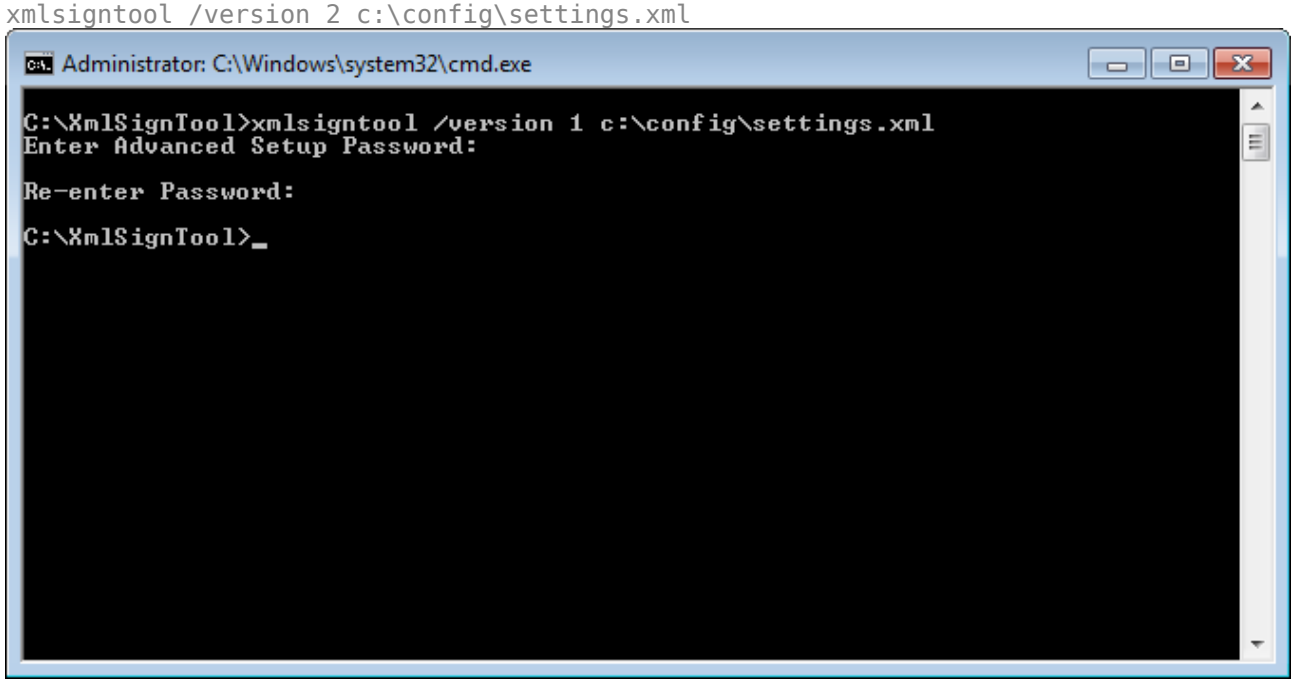
对 *.xml* 配置文件签名：

1. 下载 XmlSignTool 可执行文件。
2. 使用**以管理员身份运行**打开 Windows 命令提示符 (cmd)。
3. 导航到 `xmlsigntool.exe` 的保存位置。
4. 执行对 *.xml* 配置文件进行签名的命令，用法：`xmlsigntool /version 1|2 <xml_file_path>`

`/version` 参数的值取决于 ESET Endpoint Antivirus 的版本。针对版本 7 或更高版本使用 `/version 2`。

5. XmlSignTool 提示输入两遍高级设置密码。 您的 *.xml* 配置文件现已完成签名，可以用于使用 ESET CMD 以及密码授权方法导入 ESET Endpoint Antivirus 的另一个实例。

对导出的配置文件进行签名的命令：
`xmlsigntool /version 2 c:\config\settings.xml`



如果访问设置密码更改，并且想要导入之前使用旧密码签名的配置，需要重新使用当前密码对 *.xml* 配置文件进行签名。 这使您在导入之前无需在另一台运行 ESET Endpoint Antivirus 的计算机上导出旧版本配置文件，即可使用该配置文件。

不建议在未授权的情况下启用 ESET CMD，因为这会允许导入任何未签名的配置。在**高级设置 > 用户界面 > 访问设置**中设置密码，以防止用户未经授权进行修改。

ecmd 命令列表

使用 ESET PROTECT 客户端任务“运行命令”，可以启用和临时禁用各个安全功能。这些命令不会覆盖策略设置，并且任何已暂停的设置将在命令执行后或设备重启后恢复为其原始状态。若要

利用此功能，请指定要在相同名称的字段中运行的命令行。

查看以下每个安全功能的命令列表：

安全功能	暂时暂停命令	启用命令
文件系统实时防护	ecmd /setfeature onaccess pause	ecmd /setfeature onaccess enable
文档防护	ecmd /setfeature document pause	ecmd /setfeature document enable
设备控制	ecmd /setfeature devcontrol pause	ecmd /setfeature devcontrol enable
演示模式	ecmd /setfeature presentation pause	ecmd /setfeature presentation enable
反隐藏技术	ecmd /setfeature antistealth pause	ecmd /setfeature antistealth enable
个人防火墙	ecmd /setfeature firewall pause	ecmd /setfeature firewall enable
网络攻击防护 (IDS)	ecmd /setfeature ids pause	ecmd /setfeature ids enable
僵尸网络防护	ecmd /setfeature botnet pause	ecmd /setfeature botnet enable
Web 控制	ecmd /setfeature webcontrol pause	ecmd /setfeature webcontrol enable
Web 访问保护	ecmd /setfeature webaccess pause	ecmd /setfeature webaccess enable
电子邮件客户端防护	ecmd /setfeature email pause	ecmd /setfeature email enable
反垃圾邮件防护	ecmd /setfeature antispam pause	ecmd /setfeature antispam enable
网络钓鱼防护	ecmd /setfeature antiphishing pause	ecmd /setfeature antiphishing enable

空闲状态检测

可以在**高级设置**（在**检测引擎 > 恶意软件扫描 > 空闲状态扫描 > 空闲状态检测**下）中配置空闲状态检测设置。这些设置为以下情况下的空闲状态下扫描指定触发器：

- 屏幕保护程序正在运行；
- 计算机已锁定；
- 用户注销。

使用每种状态的开关以启用或禁用不同的空闲状态检测触发器。

导入和导出设置

您可以从**设置**菜单导入或导出自定义的 ESET Endpoint Antivirus .xml 配置文件。

当需要备份 ESET Endpoint Antivirus 的当前配置以备日后使用时，配置文件的导入和导出功能十分有用。对于想要在多个系统上使用其首选配置的用户，导出设置选项也很便利，因为他们可以方便地导入 .xml 文件来传输这些设置。

导入配置非常简单。在主程序窗口中，依次单击**设置 > 导入/导出设置**，然后选择**导入设置**。输入配置文件的文件名，或单击**...**按钮来找到想要导入的配置文件。

导出配置的步骤非常相似。在主程序窗口中，依次单击**设置 > 导入/导出设置**。选择**导出设置**并

输入配置文件的文件名（即 *export.xml*）。使用浏览器在计算机上选择要保存配置文件的位置。

如果您没有足够的权限将导出的文件写入到指定的目录，则在导出设置时可能遇到错误。

将所有设置恢复成默认值

对于所有模块，在“高级设置”(F5) 中单击**默认值**可恢复所有程序设置。这将重置为它们在全新安装后所具有的状态。

另请参阅导入和导出设置

恢复当前部分中的所有设置

单击弯曲箭头 ↩，以将当前部分中的所有设置恢复为 ESET 定义的默认设置。

请注意，单击**恢复为默认值**后，进行过的所有更改都将丢失。

恢复表格内容 – 启用后，已手动或自动添加的规则、任务或配置文件将丢失。

另请参阅导入和导出设置

保存配置时出错

此错误消息表明，这些设置因出现错误而未正确保存。

这通常表示尝试修改程序参数的用户：

- 没有足够的访问权限或没有修改配置文件和系统注册表所需的必要操作系统权限。
  > 要执行所需的修改，系统管理员必须登录。

- 最近已在 HIPS 或防火墙中启用了“学习”模式，并尝试更改“高级”设置。
  > 要保存配置并避免配置冲突，请关闭“高级”设置而不保存，并尝试再次进行所需的更改。

第二种最常见的原因是程序无法再正常工作或者已损坏，从而需要重新安装。

远程监控和管理

远程监控和管理 (RMM) 是使用可供管理服务提供商访问的本地安装的服务器代理监管和控制软件系统的过程。

ERMM - 适用于 RMM 的 ESET 插件

- 默认 ESET Endpoint Antivirus 安装包含位于以下目录内 Endpoint 应用程序中的文件 `ermm.exe`
  C:\Program Files\ESET\ESET Security\ermm.exe

- `ermm.exe` 是一个命令行实用工具，旨在帮助管理端点产品以及与任何 RMM 插件的通信。

- `ermm.exe` 会与 RMM 插件交换数据，该插件会与链接到 RMM 服务器的 RMM 服务器代理进行通信。默认情况下，ESET RMM 工具处于禁用状态。

其他资源

- ERMM 命令行

- ERMM JSON 命令列表

- 如何激活远程监控和管理ESET Endpoint Antivirus

适用于第三方 RMM 解决方案的 ESET Direct Endpoint Management 插件

RMM 服务器在第三方服务器上作为服务运行。有关详细信息，请参阅以下 ESET Direct Endpoint

Management 联机用户指南：

- 适用于 ConnectWise Automate 的ESET Direct Endpoint Management 插件
- 适用于 DattoRMM 的 ESET Direct Endpoint Management 插件
- 适用于 Solarwinds N-Central 的 ESET Direct Endpoint Management
- 适用于 NinjaRMM 的 ESET Direct Endpoint Management

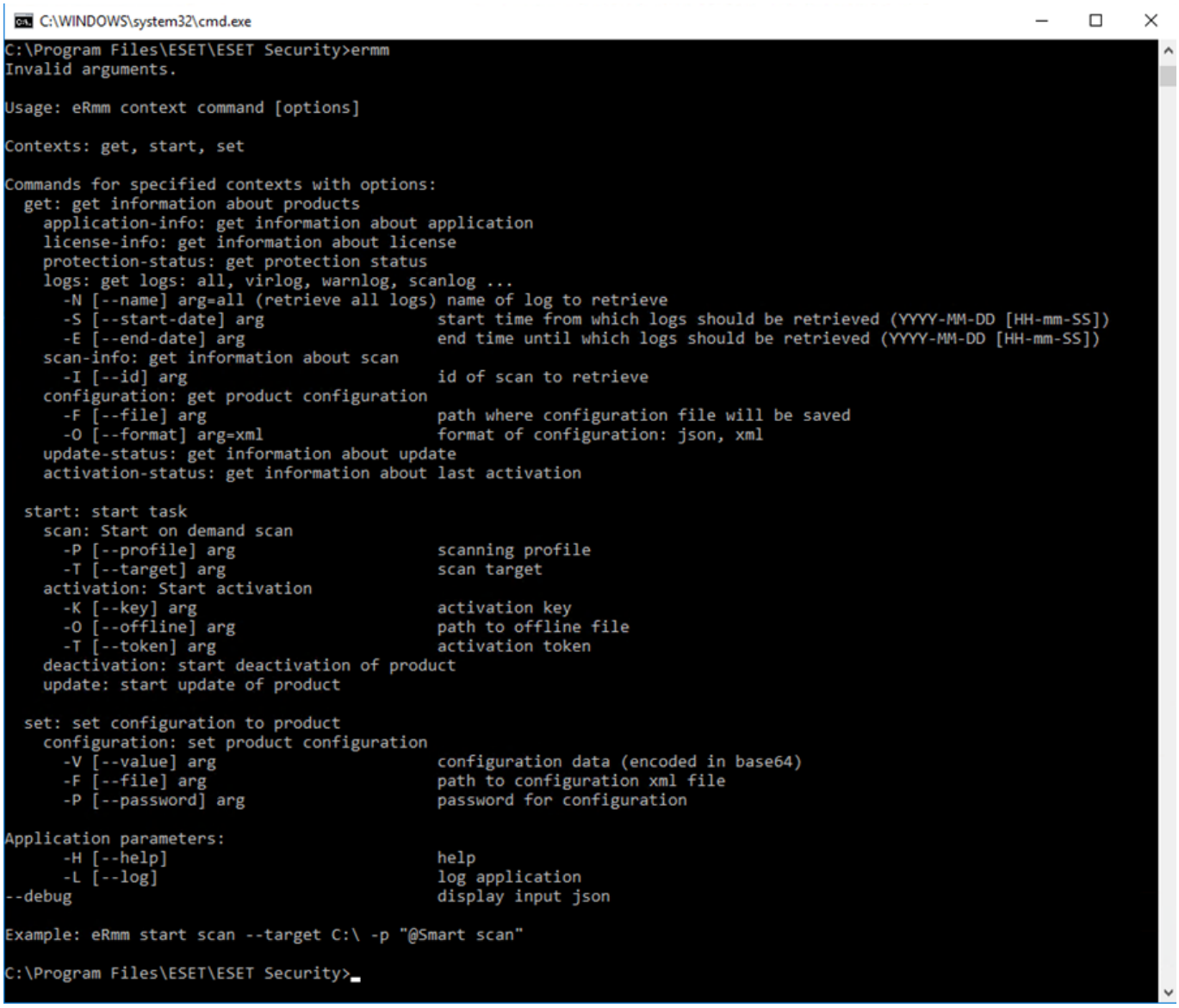
ERMM 命令行

Remote monitoring management is run using the command line interface. The default ESET Endpoint Antivirus installation contains the file ermm.exe located in the Endpoint application within the directory *c:\Program Files\ESET\ESET Security*.

Run the Command Prompt (cmd.exe) as an Administrator and navigate to the mentioned path. (To open Command Prompt, press Windows button + R on your keyboard, type a cmd.exe into the Run window and press Enter.)

The command syntax is: `ermm context command [options]`

Also note that the log parameters are case sensitive.



ermm.exe uses three basic contexts: Get, Start and Set. In the table below you can find examples of commands syntax. Click the link in the Command column to see the further options, parameters, and usage examples. After successful execution of command, the output part (result) will be displayed. To see an input part, add parameter `--debug` at the of the command.

Context	Command	Description
get		**Get information about products**
	应用程序信息	Get information about product
	许可证信息	Get information about license
	防护状态	Get protection status
	日志	Get logs
	扫描信息	Get information about running scan
	配置	Get product configuration
	更新状态	Get information about update
	激活状态	Get information about last activation
start		**Start task**
	扫描	Start on demand scan

Context	Command	Description
	激活	Start activation of product
	停用	Start deactivation of product
	更新	Start update of product
set		**Set options for product**
	配置	Set configuration to product

In the output result of every command, the first information displayed is result ID. To understand better the result information, check the table of IDs below.

Error ID	Error	Description
0	Success	
1	Command node not present	"Command" node not present in input json
2	Command not supported	Particular command is not supported
3	General error executing the command	Error during execution of command
4	Task already running	Requested task is already running and has not been started
5	Invalid parameter for command	Bad user input
6	Command not executed because it's disabled	RMM isn't enabled in advanced settings or isn't started as an administrator

ERMM JSON 命令列表

- 获取防护状态
- 获取应用程序信息
- 获取许可证信息
- 获取日志
- 获取激活状态
- 获取扫描信息
- 获取配置
- 获取更新状态
- 启动扫描
- 启动激活
- 启动停用

- 启动更新
- 设置配置

get protection-status

Get the list of application statuses and the global application status

Command line

```
ermm.exe get protection-status
```

Parameters

None

Example

call

```
{

"command":"get_protection_status",

"id":1,

"version":"1"

}
```

result

```
{
"id":1,
"result":{
"statuses":[{
"id":"EkrnNotActivated",
"status":2,
"priority":768,
"description":"Product not activated"
}],
"status":2,
"description":"Security alert"
},
"error":null
}
```


get application-info

Get information about the installed application

Command line

```
ermm.exe get application-info
```

Parameters

None

Example

call

```
{

"command":"get_application_info",

"id":1,

"version":"1"

}
```

result

```
{
"id":1,
"result":{
"description":"ESET Endpoint Antivirus",
"version":"6.6.2018.0",
"product":"eea",
"lang_id":1033,
"modules":[{
"id":"SCANNER32",
"description":"Detection engine",
"version":"15117",
"date":"2017-03-20"
},{
"id":"PEGASUS32",
"description":"Rapid Response module",
"version":"9734",
"date":"2017-03-20"
},{
"id":"LOADER32",
"description":"Update module",
"version":"1009",
"date":"2016-12-05"
},{
"id":"PERSEUS32",
"description":"Antivirus and antispyware scanner module",
"version":"1513",
"date":"2017-03-06"
},{
"id":"ADVHEUR32",
"description":"Advanced heuristics module",
"version":"1176",
"date":"2017-01-16"
},{
"id":"ARCHIVER32",
"description":"Archive support module",
"version":"1261",
"date":"2017-02-22"
},{
"id":"CLEANER32",
"description":"Cleaner module",
"version":"1132",
"date":"2017-03-15"
},{
"id":"ANTISTEALTH32",
"description":"Anti-Stealth support module",
"version":"1106",
"date":"2016-10-17"
},{
"id":"SYSTEMSTATUS32",
"description":"ESET SysInspector module",
"version":"1266",
"date":"2016-12-22"
},{
"id":"TRANSLATOR32",
"description":"Translation support module",
"version":"1588B",
"date":"2017-03-01"
},{
"id":"HIPS32",
"description":"HIPS support module",
"version":"1267",
"date":"2017-02-16"
},{
"id":"PROTOSCAN32",
"description":"Internet protection module",
"version":"1300",
"date":"2017-03-03"
},{
"id":"DBLITE32",
"description":"Database module",
"version":"1088",
"date":"2017-01-05"
},{
"id":"CONFENG32",
"description":"Configuration module (33)",
"version":"1496B",
"date":"2017-03-17"
},{
"id":"IRIS32",
"description":"LiveGrid communication module",
"version":"1022",
"date":"2016-04-01"
},{
"id":"SAURON32",
"description":"Rootkit detection and cleaning module",
"version":"1006",
"date":"2016-07-15"
},{
"id":"SSL32",
"description":"Cryptographic protocol support module",
"version":"1009",
"date":"2016-12-02"
}
},
"error":null
}
}
```

get license-info

Get information about the license of the product

Command line

```
ermm.exe get license-info
```

Parameters

None

Example

call

```
{

"command":"get_license_info",

"id":1,

"version":"1"

}
```

result

```
{
"id":1,
"result":{
"type":"NFR",
"expiration_date":"2020-12-31",
"expiration_state":"ok",
"public_id":"3XX-7ED-7XF",
"seat_id":"6f726793-ae95-4e04-8ac3-e6a20bc620bf",
"seat_name":"M"
},
"error":null
}
```


get logs

Get logs of the product

Command line

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-
date "2017-04-04 12-00-00"
```

Parameters

Name	Value
name	{ all, virlog, warnlog, scanlog, blocked, hipslog, urllog, devctrllog } : log to retrieve
start-date	start date from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
end-date	end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

Example

call

```
{

"command":"get_logs",

"id":1,

"version":"1",

"params":{

"name":"warnlog",

"start_date":"2017-04-04 06-00-00",

"end_date":"2017-04-04 12-00-00"

}

}
```

result

```
{
"id":1,
"result":{
"warnlog":{
"display_name":"Events",
"logs":[{
"Time":"2017-04-04 06-05-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15198 (20170404).",
"UserData":""
},{
"Time":"2017-04-04 11-12-59",
"Severity":"Info",
"PluginId":"ESET Kernel",
"Code":"Malware database was successfully updated to version 15199 (20170404).",
"UserData":""
}]
}
},
"error":null
}
```


get activation-status

Get information about the last activation. Result of status can be { success, error }

Command line

```
ermm.exe get activation-status
```

Parameters

None

Example

call

```
{

"command":"get_activation_status",

"id":1,

"version":"1"

}
```

result

```
{

"id":1,

"result":{

"status":"success"

},

"error":null

}
```

get scan-info

Get information about running scan.

Command line

```
ermm.exe get scan-info
```

Parameters

None

Example

call

```
{

"command":"get_scan_info",

"id":1,

"version":"1"

}
```

result

```
{
"id":1,
"result":{
"scan-info":{
"scans":[{
"scan_id":65536,
"timestamp":272,
"state":"finished",
"pause_scheduled_allowed":false,
"pause_time_remain":0,
"start_time":"2017-06-20T12:20:33Z",
"elapsed_tickcount":328,
"exit_code":0,
"progress_filename":"Operating memory",
"progress_arch_filename":"",
"total_object_count":268,
"infected_object_count":0,
"cleaned_object_count":0,
"log_timestamp":268,
"log_count":0,
"log_path":"C:\\ProgramData\\ESET\\ESET Security\\Logs\\eScan\\ndl31494.dat",
"username":"test-PC\\test",
"process_id":3616,
"thread_id":3992,
"task_type":2
}],
"pause_scheduled_active":false
}
},
"error":null
}
```

get configuration

Get the product configuration. Result of status may be { success, error }

Command line

```
ermm.exe get configuration --file C:\tmp\conf.xml --format xml
```

Parameters

Name	Value
file	the path where the configuration file will be saved
format	format of configuration: json, xml. Default format is xml

Example

call

```
{

"command":"get_configuration",

"id":1,

"version":"1",

"params":{

"format":"xml",

"file":"C:\\tmp\\conf.xml"

}

}
```

result

```
{
"id":1,
"result":{
"configuration":"PD94bWwgdmVyc2lvbj0iMS4w=="
},
"error":null
}
```


get update-status

Get information about the update. Result of status may be { success, error }

Command line

```
ermm.exe get update-status
```

Parameters

None

Example

call


```
{
"command":"get_update_status",
"id":1,
"version":"1"
}
```


result

```
{
"id":1,
"result":{
"last_update_time":"2017-06-20 13-21-37",
"last_update_result":"error",
"last_successful_update_time":"2017-06-20 11-21-45"
},
"error":null
}
```


start scan

Start scan with the product

Command line

```
ermm.exe start scan --profile "profile name" --target "path"
```

Parameters

Name	Value
profile	Profile name of On-demand computer scan defined in product
target	Path to be scanned

Example

call

```
{

"command":"start_scan",

"id":1,

"version":"1",

"params":{

"profile":"Smart scan",

"target":"c:\\"

}

}
```

result

```
{

"id":1,

"result":{

"task_id":458752

},

"error":null

}
```

start activation

Start activation of product

Command line

```
ermm.exe start activation --key "activation key" | --offline "path to offline file"
```

Parameters

Name	Value
key	Activation key
offline	Path to offline file

Example

call

```
{

"command":"start_activation"

"id":1,

"version":"1",

"params":{

"key":"XXXX-XXXX-XXXX-XXXX-XXXX"

}

}
```

result

```
{

"id":1,

"result":{

},

"error":null

}
```

start deactivation

Start deactivation of the product

Command line

```
ermm.exe start deactivation
```

Parameters

None

Example

call

```
{
"command":"start_deactivation",
"id":1,
"version":"1"
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

start update

Start update of the product. Only one update may be running in the product so in case the update is already running, "Task already running" error code is returned

Command line

```
ermm.exe start update
```

Parameters

None

Example

call

```
{

"command":"start_update",

"id":1,

"version":"1"

}
```

result

```
{

"id":1,

"result":{

},

"error":{

"id":4,

"text":"Task already running."

}

}
```

set configuration

Set configuration to the product. Result of status may be { success, error }

Command line

```
ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass
```

Parameters

Name	Value
file	the path where the configuration file will be saved
password	password for configuration
value	configuration data from the argument (encoded in base64)

Example

call

```
{
"command":"set_configuration",
"id":1,
"version":"1",
"params":{
"format":"xml",
"file":"C:\\tmp\\conf.xml",
"password": "pass"
}
}
```

result

```
{
"id":1,
"result":{
},
"error":null
}
```

常见问题

本章介绍一些最常见的问题和难题。单击主题标题了解如何解决您的难题：

- 如何更新 ESET Endpoint Antivirus
- 如何激活 ESET Endpoint Antivirus
- 如何使用当前凭据激活新产品
- 如何从 PC 中删除病毒
- 如何在计划任务中创建新任务
- 如何计划每周计算机扫描
- 如何将我的产品连接到 ESET PROTECT

- 如何使用覆盖模式
- 如何应用适用于 ESET Endpoint Antivirus 的建议策略

- 如何配置镜像
- 如何使用 ESET Endpoint Antivirus 升级到 Windows 10
- 如何激活远程监控和管理
- 如何阻止从 Internet 下载特定文件类型
- 如何最小化 ESET Endpoint Antivirus 用户界面

如果问题没有包括在上面列出的帮助页面中，则尝试在 ESET Endpoint Antivirus 帮助页面中按描述问题的关键字或短语搜索。

如果您无法在帮助页面中找到您的难题或问题的解决方案，请访问 ESET 知识库，此处提供常见问题的解答。

- 防御 Filecoder（勒索软件）恶意软件的最佳做法
- ESET Endpoint Security 和 ESET Endpoint Antivirus 常见问题解答
- 应打开我的第三方防火墙上的哪些地址和端口以便 ESET 产品提供完整功能？

如有必要，您可以联系我们的在线技术支持中心咨询您的问题或难题。可以在主程序窗口的**帮助和支持**窗格中找到我们的在线联系表格。

自动更新常见问题解答

假定我有大约 3000 台计算机。所有计算机会同时下载更新吗？是否可以为这么多计算机使用代理进行自动更新？

我们为大型网络提供了“镜像工具”和“代理”解决方案，因此更新只需通过 Internet 下载一次，然后在本地进行分发。更新的大小较小，通常为 5–10 MB，并且在可用的最初几周内会应用限制。因此，并非所有客户端在直接连接到 ESET 服务器时都会同时开始下载。

计算机会自动更新吗？更新是在重新启动之前还是之后下载的？

下载发生在重新启动之前，这意味着更新的文件也在此阶段准备就绪。重新启动后，更新后的文件仍只是准备供使用，当前安装的版本会提供不间断的保护。更改将在 ESET 端点产品下次启动后应用。

是否可以决定自动更新多少台计算机或哪些计算机？我不想每小时为十台以上计算机下载，或者我只想现在更新十台计算机，几天后再更新其余计算机。

托管环境有自动更新策略，在其中可以指定所需的最高版本。 还支持通配符（例如，9.0.2032.*）。有关详细信息，请访问以下联机帮助页面。不幸的是，目前没有可用于限制自动更新的其他选项。可以为多个组分配多个策略。

对于服务器产品，自动更新是否也执行相同操作？服务器是否需要重新启动？

将发布服务器产品 (uPCU) 的更新，其严重级别为 2。将显示对话窗口，可以推迟或跳过更新。在此情况下，产品处于绿色状态 – 正常状态。完成更新产品后，状态会变为黄色，并显示状态**建议重新启动**。如果发生严重事件，我们会使用较高严重级别来强制执行更新。在这种情况下，重新启动必须尽快应用更改。不会以任何方式强制重新启动。何时重新启动由管理员在方便的时候决定。

是否仅通过策略配置自动更新？如果我不想更新 ESET 产品，是否可以禁用该策略？

如果有适用于 ESET Endpoint Security 的安全修补程序，即使自动更新处于禁用状态，产品也会根据适用最终用户许可协议中设置的条款进行更新。这是因为市面上的安全形势频繁发生变化，新的漏洞迫使我们要快速响应。

可以将自动更新策略分配给任何端点组，而无需考虑其当前的自动更新配置。在非托管环境中，用户可以在 ESET 端点产品的高级设置屏幕中本地配置自动更新。

如果我将策略配置为使用最旧的可用版本，该怎么办？即便如此，ESET 仍会更新我的产品吗？

修补程序和关键修补程序（安全性和稳定性更新）是略有不同的更新类别。当接受用户设置时，将向自动更新分配优先级为标准的常规修补程序。无论用户设置如何，都会优先应用关键修补程序。

它在脱机场景中将如何工作？用户何时使用脱机存储库？

脱机存储库还包含 .dup 和 .fup 文件。存储库部分必须由镜像工具下载，而不是由模块更新下载。

ESET 产品如何知道需要更新？从存储库？是否要向服务器发送一些数据？如果 ESET 计划在版本发布一个月后进行更新，如果这适用于全世界，ESET 服务器是否对此做好了准备？

ESET 产品会从存储库下载自动更新。服务器已为此做好了准备，因为关键更新只有几 KB 大小。关键更新不会对存储库服务器应用任何限制。但是，如果自动更新较大，则可以选择对服务器启用限制。在下表中，可以查看发生差异自动更新时的修补程序大小示例：

以前版本	新版本	大小
9.0.2032.2	9.0.2032.6	420 KB
8.1.2037.2	9.0.2032.2	6.5 MB
8.0.2028.0	9.0.2032.2	11.5 MB

如果差异自动更新由于某种原因而失败，则可能原因是 ESET 产品将启动完整更新。它仍是一个

具有功能保证的自动更新，但将下载 .fup 文件（这是一个较大文件）而不是 .dup 文件。对于版本 9.0.2032.2，它是 27 MB。但是，这种情况很少见。

ESET Endpoint Security/ESET Endpoint Antivirus 的更新是否带限制发布？如果答案为否，那么该更新的限制时间是多久？

在部署新版本的最初几周内应用限制，以减少我们服务器上的负载并均衡分发新版本。

此外，我认为自动更新将成为主流的升级方式之一。它具体是如何工作的？

这是正确的。该想法是要让尽可能多的客户通过自动更新进行更新。拥有如此多的可用旧版本时，难以提供支持。自动更新功能的工作方式十分简单。在首次模块更新检查期间，会下载 .dup 文件。在更新过程中，产品完全正常运行并始终保护计算机。重新启动后，激活新版本。在 ESET PROTECT（服务器端）中，可以使用策略来指定要更新到的最高版本。此外，还可以使用通配符。有关详细信息，请访问以下联机帮助页面。

自动更新以 1/10 的方式工作，对吗？我现在使用的是 ESET Endpoint Security 8.0.2028.1。如果自动更新运行，它将更新到哪个版本？

由于存储库服务器上的限制，使用“自动更新”更新产品可能会延迟。如果带限制发布产品更新，则自动更新检查可能不会立即收到它。如果更新被认为是安全且稳定的，则可能会随后减少或完全删除限制，以便所有其余客户端都会收到更新。

限制是一个过程，每次更新可能需要不同的时间。它取决于有多少客户端请求更新、我们服务器上的通信量以及其他因素。这一过程始终在不断演变，并随时会发生变化。此外，由于“自动更新”功能是一个较新功能，我们很可能会在未来调整此过程以改善客户体验。

如果我在上午 8:45 启动计算机并在下午 5:00 将其关闭，那么自动更新何时执行？

在下一个成功计划模块更新时，最多每 24 小时更新一次。

如果计算机在自动更新运行时关机，那么下次何时运行更新？

更新将在下一个计划更新窗口期间运行。自动更新（以前称为 uPCU）过程有一个强大的错误保护机制。下载更新并重启计算机后，更新后的文件仍只是处于准备使用状态，当前安装的版本会提供不间断的保护。更改将在 ESET 端点产品下次启动后应用。

如何立即运行自动更新，而无需每 24 小时等待一次常规连接？还有其他方法可以单击“检查更新”吗？

当前，只能在打开主程序窗口并依次单击**更新 > 检查更新**时，手动调用自动更新过程。调用模块更新的所有其他方式都反映了 24 小时自动更新计划任务策略。目前，无法远程启动自动更新下载。我们将在以后的更新中添加此功能。

如何更新 ESET Endpoint Antivirus

可以通过手动或自动方式更新 ESET Endpoint Antivirus。若要触发更新，请在主程序窗口中单击**更新**，然后单击**检查更新**。

默认安装设置会创建每小时执行一次的自动更新任务。要更改时间间隔，请导航到**工具 > 计划任务**（请参阅有关计划任务的详细信息。

如何激活 ESET Endpoint Antivirus

完成安装后，将提示您激活您的产品。

有几种激活产品的方法。激活窗口中特定激活方案的可用性可能有所不同，具体取决于国家/地区以及分发方式（ESET 网页、安装程序类型 .msi 或 .exe 等）。

要在程序中直接激活您的 ESET Endpoint Antivirus 副本，请打开 ESET Endpoint Antivirus 主程序窗口，并从主菜单中单击**帮助与支持 > 激活产品**或**保护状态 > 激活产品**。

您可以使用以下任一方法来激活 ESET Endpoint Antivirus。

- **使用购买的许可证密钥** – 采用 XXXX-XXXX-XXXX-XXXX-XXXX 格式的唯一字符串，用于标识许可证所有者和激活许可证。
- **ESET Business Account** – 在 ESET Business Account 门户上使用凭据（电子邮件地址 + 密码）创建的帐户。此方法允许您在一个位置管理多个许可证。
- **脱机许可证** – 将传输到 ESET 产品以提供许可证信息的自动生成的文件。如果许可证允许您下载可用于执行脱机激活的脱机许可证文件 (.lf)。将从可用许可证的总数中减去脱机许可证的数量。有关生成脱机文件的更多详细信息，请参阅 ESET Business Account 用户指南。

如果您的计算机是托管网络的成员，请单击**稍后激活**，您的管理员将通过 ESET PROTECT 执行远程激活。如果您希望稍后激活此客户端，也可以使用此选项。

如果拥有用于激活旧版 ESET 产品的用户名和密码，但不知道如何激活 ESET Endpoint Antivirus。请将旧凭据转换为许可证密钥。

⚠ 产品激活失败？

可以随时更改您的产品许可证。为此，请在主程序窗口中依次单击**帮助和支持 > 更改许可证**。将看到 ESET 支持用来识别您的许可证的公共许可证 ID。用于注册计算机的用户名存储在**关于**部分中，可以通过右键单击系统托盘图标  来查看它。

ESET PROTECT 7.2 或 ESET PROTECT 9 可以使用管理员提供的许可证静默激活客户端计算机。有关执行此操作的说明，请参阅 ESET PROTECT 联机帮助。

激活期间输入许可证密钥

自动更新对您的安全很重要。ESET Endpoint Antivirus 仅在使用您的**许可证密钥**激活后才接收更新。

如果您未在安装后输入您的许可证密钥，将不会激活您的产品。 您可以在主程序窗口中更改您的许可证。 若要执行此操作，请依次单击**帮助和支持 > 激活许可证**，然后将随 ESET 安全产品一起收到的许可证数据输入到产品激活窗口中。

当输入您的**许可证密钥**时，请务必按照其写入形式准确键入它：

- 您的许可证密钥是采用 XXXX-XXXX-XXXX-XXXX-XXXX 格式的唯一字符串，用于标识许可证所有者和激活许可证。

我们建议您从您的注册电子邮件复制并粘贴许可证密钥，以确保准确性。

登录到 ESET Business Account

“安全管理员”帐户是使用您的**电子邮件地址**和**密码**在 ESET Business Account 门户上创建的帐户，它能够看到所有席位授权。“安全管理员”帐户允许您管理多个许可证。如果您没有“安全管理员”帐户，请单击**创建帐户**，您将重定向到“ESET Business Account”门户，您可在其中使用凭据进行注册。

如果忘记了密码，请单击**我忘记了我的密码**，然后系统将您重定向到 ESET Business Account 门户。输入您的电子邮件地址并单击**提交**以确认。之后，您将收到一封包含如何重置密码的说明的邮件。

如何使用旧许可证凭据激活较新的 ESET 端点产品

如果您已拥有用户名和密码，并希望收到一个许可证密钥，请访问 ESET Business Account 门户，可以在其中将您的凭据转换为新的许可证密钥。

如何从 PC 中删除病毒

如果您的计算机显示感染恶意软件的迹象，例如速度变慢，常常停止响应，我们建议您执行以下操作：

1. 在主程序窗口中，单击**计算机扫描**。
2. 单击**智能扫描**以开始扫描您的系统。

3. 扫描完成后，查看日志中扫描文件、被感染文件和已清除文件的数量。

4. 如果您希望仅扫描磁盘的特定部分，请单击**自定义扫描**，然后选择要进行病毒扫描的目标。

有关其他信息，请参阅我们定期更新的 ESET 知识库文章。

如何在计划任务中创建新任务

要在**工具 > 计划任务**中创建新任务，请单击**添加任务**或右键单击并从右键菜单中选择**添加**。共有 5 种类型的计划任务：

- **运行外部应用程序** – 计划外部应用程序的执行。
- **日志维护** – 日志文件中仍会包含已删除记录的残余信息。此任务定期优化日志文件中的记录以提高工作效率。
- **系统启动文件检查** – 检查在系统启动或登录时允许运行的文件。
- **创建计算机状态快照** – 创建 ESET SysInspector 计算机快照 – 收集有关系统组件的详细信息（例如，驱动程序、应用程序）并评估每个组件的风险级别。
- **手动计算机扫描** – 执行计算机上文件和文件夹的计算机扫描。
- **更新** – 通过更新模块，计划更新任务。

因为**更新**是最常用的计划任务之一，所以下面我们将解释如何添加新的更新任务：

从**计划任务**下拉菜单中选择**更新**。将任务名称输入**任务名称**字段中并单击**下一步**。选择任务执行频率。有以下选项可供使用：**一次**、**重复**、**每天**、**每周**和**由事件触发。在便携式计算机靠电池供电时，选择靠电池供电时跳过任务**以最大限度地减少系统资源。将在**任务执行**字段中指定的日期和时间运行该任务。然后，定义无法在计划时间执行或完成任务时要采取的操作。有以下选项可供使用：

- **在下一个计划时间**
- **尽快**
- **如果自上次运行时间之后经过的时间超过指定值，则立即跳过任务**（可使用**自上次运行时间之后经过的时间**滚动框来定义间隔）

在下一步中，显示有关当前计划任务信息的摘要窗口。当您完成更改时，单击**完成**。

将显示一个对话窗口，允许您选择用于计划任务的配置文件。此处，您可以设置主要和替代配置文件。如果任务不能用主要配置文件来完成，则使用替代配置文件。单击**完成**以进行确认，新计划任务将添加到当前计划任务列表中。

如何计划每周计算机扫描

要计划定期任务，请打开主程序窗口，然后依次单击**工具 > 计划任务**。下面是介绍如何计划每周扫描一次本地驱动器的任务的简要指南。有关更详细的说明，请参阅我们的知识库文章。

要计划扫描任务：

1. 单击主计划任务屏幕中的**添加**。
2. 从下拉菜单中选择**手动计算机扫描**。
3. 输入任务名称，然后为任务频率选择**每周**。
4. 设置将执行任务的日期和时间。
5. 如果计划任务由于任何原因（例如，计算机已关闭）而无法运行，请选择**尽快运行任务**以便在稍后执行任务。
6. 检查计划任务的摘要并单击**完成**。
7. 从**目标**下拉菜单中选择**本地驱动器**。
8. 单击**完成**以应用此任务。

如何将 ESET Endpoint Antivirus 连接至 ESET PROTECT

如果在计算机上安装了 ESET Endpoint Antivirus 并且想要通过 ESET PROTECT 连接，请确保在客户端工作站上也安装了 ESET Management 服务器代理。它是与 ESET PROTECT 服务器通信的每个客户端解决方案的重要组成部分。

- 在客户端工作站上安装或部署 ESET Management 服务器代理

另请参阅：

- 远程管理端点的文档
- 如何使用覆盖模式
- 如何应用适用于 ESET Endpoint Antivirus 的建议策略

如何使用覆盖模式

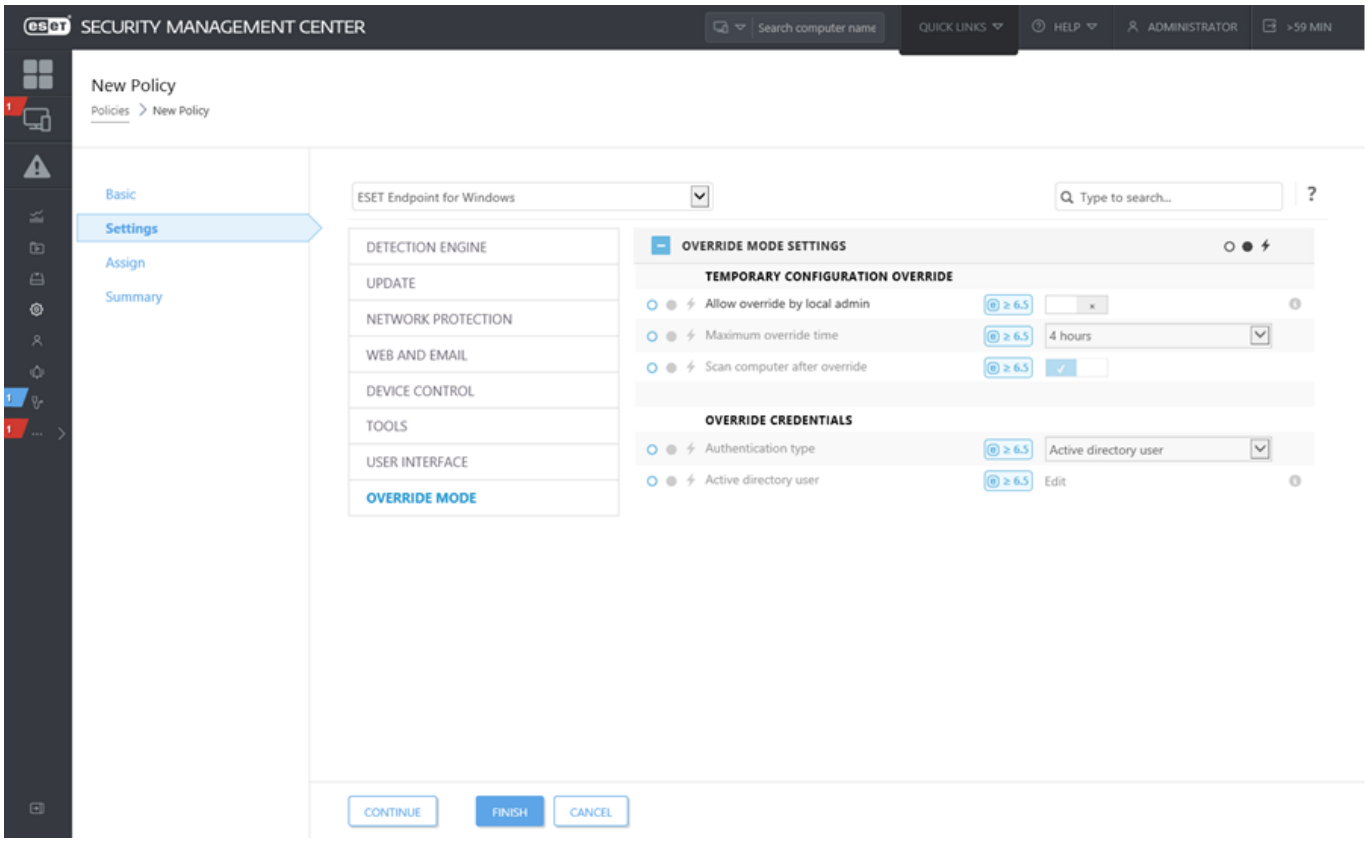
在计算机上已安装适用于 Windows 的 ESET Endpoint 产品（版本 6.5 和更高版本）的用户可以使用覆盖功能。覆盖模式允许客户端计算机级别上的用户更改已安装的 ESET 产品中的设置，即

使已对这些设置应用了策略。可以为某些 AD 用户启用覆盖模式，也可以对覆盖模式进行密码保护。启用一次该功能的时长不能超过 4 个小时。

- 覆盖模式启用后，无法从 ESET PROTECT Web 控制台停止该模式。覆盖模式将在覆盖时间段到期后自动禁用。还可以在客户端计算机上关闭它。
- 使用覆盖模式的用户还需要拥有 Windows 管理员权限。否则，用户无法将更改保存在 ESET Endpoint Antivirus 的设置中。
- ESET Endpoint Antivirus 版本 7.0.2100.4 及更高版本支持 Active Directory 组身份验证。

若要设置**覆盖模式**，请执行以下步骤：

1. 导航到 **策略 > 新策略**。
2. 在 **基本**部分中，键入该策略的**名称**和**说明**。
3. 在 **设置**部分中，选择 **ESET Endpoint for Windows**。
4. 单击**覆盖模式**，然后配置覆盖模式的规则。
5. 在 **分配**部分中，选择将应用该策略的计算机或计算机组。
6. 在 **摘要**部分中检查这些设置，然后单击**完成**以应用该策略。



如果 *John* 的计算机上的端点设置阻止了某些重要功能或 Web 访问，管理员可以允许 *John* 覆盖其现有端点策略，然后手动调整其计算机上的设置。之后，ESET PROTECT 可以请求这些新设置，以便管理员可以基于这些设置创建新策略。

要执行该操作，请遵循以下步骤：

1.导航到**策略 > 新策略**。

2.填写**名称**和**说明**字段。在**设置**部分中，选择 **ESET Endpoint for Windows**。

3.单击**覆盖模式**、启用覆盖模式一个小时，然后选择 *John* 作为 AD 用户。

4.将策略分配给 *John 的计算机*，然后单击**完成**以保存策略。

5.*John* 必须在其 ESET Endpoint 上启用**覆盖模式**，并手动在其计算机上更改设置。

✔ 6.在 ESET PROTECT Web 控制台上，导航到**计算机**、选择 *John 的计算机*，然后单击**显示详细信息**。

7.在**配置**部分中，单击**请求配置**，尽快计划从客户端 ASAP 获取配置的客户端任务。

8.过一会，将显示新配置。单击要保存设置的产品，然后单击**打开配置**。

9.您可以检查设置，然后单击**转换为策略**。

10.填写**名称**和**说明**字段。

11.在**设置**部分中，必要时可修改设置。

12.在**分配**部分中，可以将该策略分配给 *John 的计算机*（或其他计算机）。

13.单击**完成**以保存设置。

14.不再需要覆盖策略后，务必将覆盖策略删除。

如何应用适用于 ESET Endpoint Antivirus 的建议策略

将 ESET Endpoint Antivirus 连接到 ESET PROTECT 后的最佳做法是应用建议的策略或应用自定义策略。

有多个适用于 ESET Endpoint Antivirus 内置策略：

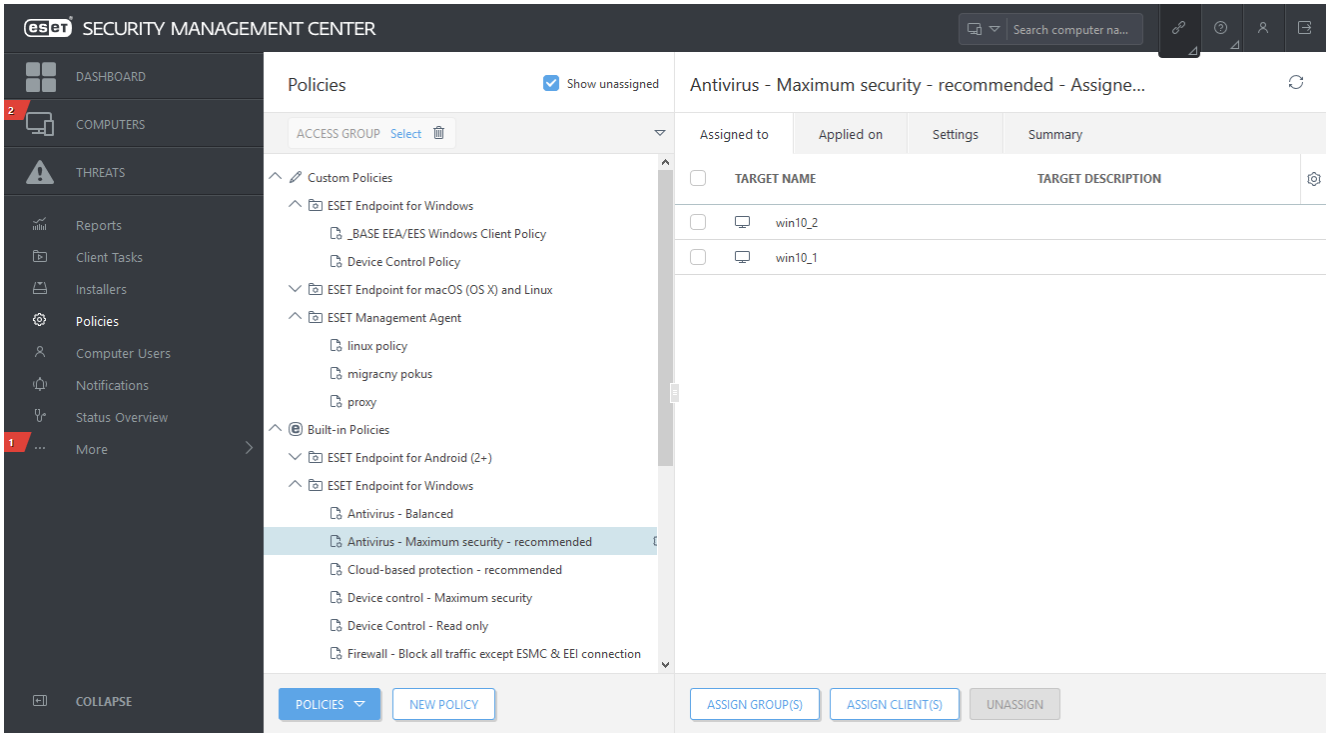
策略	说明
病毒防护 – 平衡	建议用于大多数设置的安全配置。
病毒防护 – 最大安全性	利用机器学习、深度行为检测和 SSL 过滤。对潜在不安全的、不受欢迎的和可疑应用程序的检测会有影响。
基于云的信誉和反馈系统	启用 ESET LiveGrid® 基于云的信誉和反馈系统，可改善对最新威胁的检测，有助于共享恶意威胁或未知潜在威胁以供进一步分析。
设备控制 – 最大安全性	阻止所有设备。当任何设备要进行连接时，需要得到管理员的允许。
设备控制 – 只读	所有设备都为只读。不允许写入。
防火墙 – 阻止所有通信（ESET PROTECT 和 ESET Inspect 连接除外）	阻止与 ESET PROTECT 和 ESET Inspect 服务器连接以外的所有通信（仅限 ESET Endpoint Security）。
日志记录 – 完整的诊断日志记录	此模板将确保在管理员需要时所有日志都可用。所有内容都从最低级别开始记录，其中包括 HIPS 和 Threatsense 参数、防火墙。日志将在 90 天后自动删除。
日志记录 – 仅记录重要事件	策略确保将记录警告、错误和关键事件。日志将在 90 天后自动删除。
可见性 – 平衡	可见性的默认设置。启用状态和通知。

策略	说明
可见性 – 不可见模式	禁用通知、警报、GUI、集成到右键菜单。将不运行 egui.exe。适用于仅通过 ESET PROTECT Cloud 的管理。
可见性 – 减少与用户交互	禁用状态、禁用通知、显示 GUI

要设置名为**病毒防护 – 最大安全性**的策略（其中强制执行 50 多个针对工作站上安装的 ESET Endpoint Antivirus 建议的设置），请按照以下步骤操作：

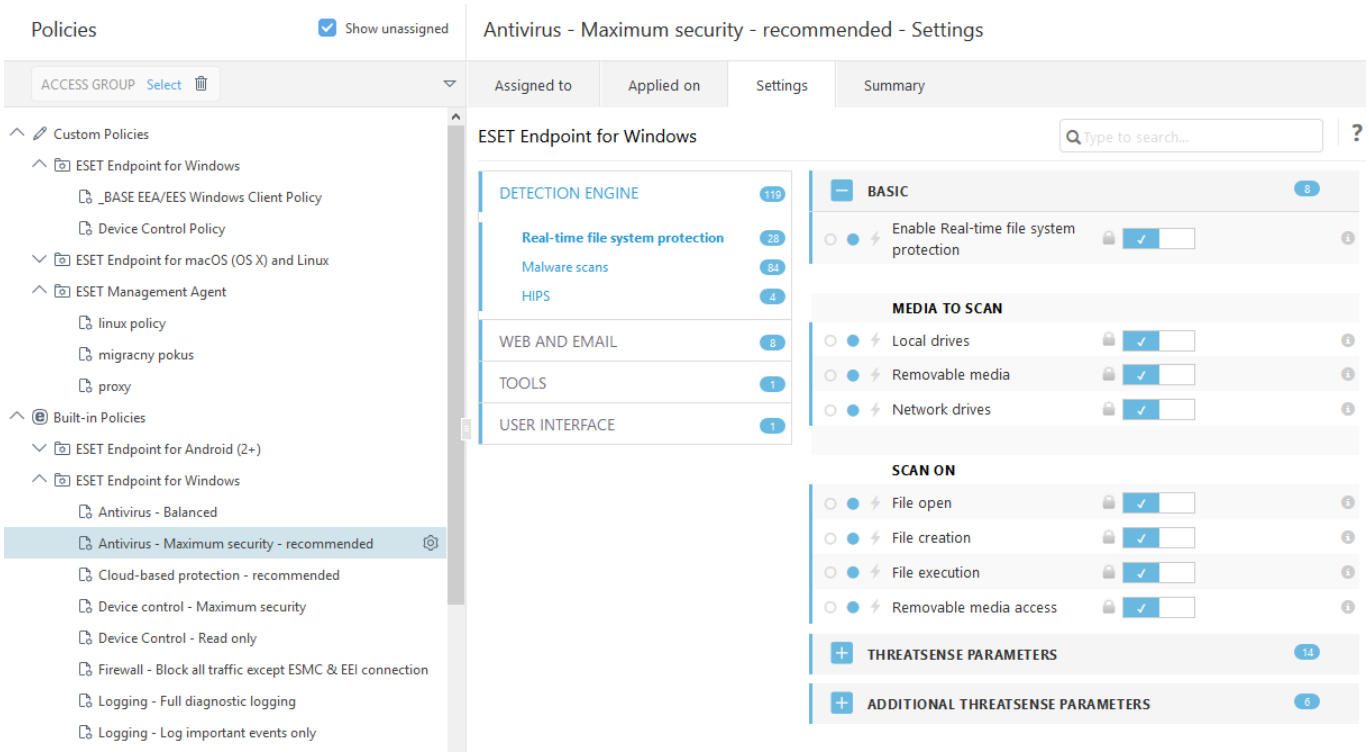
以下 ESET 知识库文章可能仅提供英文版：
- 使用 ESET PROTECT 应用适用于 ESET Endpoint Antivirus 的建议或预定义策略

1. 打开 ESET PROTECT Web 控制台。
2. 导航到 **策略**，然后展开**内置策略 > ESET Endpoint for Windows**。
3. 单击**病毒防护 – 最大安全性 – 建议**。
4. 在**已分配给**选项卡中，单击**分配客户端**或**分配组**，然后选择要应用此策略的相应目标计算机。



要查看此策略应用的设置，请单击**设置**选项卡，然后展开“高级设置”树。

- 蓝点表示此策略的更改设置
- 蓝色框中的数字表示此策略的一些更改设置
- 在此处详细了解 ESET PROTECT 策略



如何配置镜像

可对 ESET Endpoint Antivirus 进行配置，以存储检测引擎更新文件副本，并将更新分发到正在运行 ESET Endpoint Security 或 ESET Endpoint Antivirus 的其他工作站。

将 ESET Endpoint Antivirus 配置为镜像服务器，以通过内部 HTTP 服务器提供更新

1. 按 **F5** 访问“高级设置”，然后依次展开**更新** > **配置文件** > **更新镜像**。
2. 展开**更新**，并确保**模块更新**下的**自动选择**选项已启用。
3. 展开**更新镜像**，然后启用**创建更新镜像**和**启用 HTTP 服务器**。

有关详细信息，请参阅更新镜像。

配置镜像服务器以通过共享网络文件夹提供更新

1. 在本地或网络设备上创建共享文件夹。此文件夹必须可由运行 ESET 安全解决方案的所有用户读取，且可由本地 SYSTEM 帐户写入。
2. 在**高级设置** > **更新** > **配置文件** > **更新镜像**下激活**创建更新镜像**。
3. 通过单击**清除**，然后单击**编辑**来选择一个合适的**存储文件夹**。浏览并选择创建的共享文件夹。

如果不希望通过内部 HTTP 服务器提供模块更新，请取消**创建更新镜像**。

如何使用 ESET Endpoint Antivirus 升级到 Windows 10

我们强烈建议您先升级到最新版本的 ESET 产品并下载最新的模块更新，然后再升级到 Windows 10。在升级到 Windows 10 期间，此操作可确保您获取最大程度的防护并将保留您的程序设置和许可证信息。

版本 7.x

单击下方相应的链接下载并安装最新版本，以便为升级到 Microsoft Windows 10 做好准备：

下载 ESET Endpoint Security 7 32 位 下载 ESET Endpoint Antivirus 7 32 位

下载 ESET Endpoint Security 7 64 位 下载 ESET Endpoint Antivirus 7 64 位

版本 5.x

版本 5 中的 ESET Endpoint 产品目前处于生命周期结束状态。这意味着内部版本不再公开可供下载。强烈建议您升级到最新版本的 ESET Endpoint 产品。

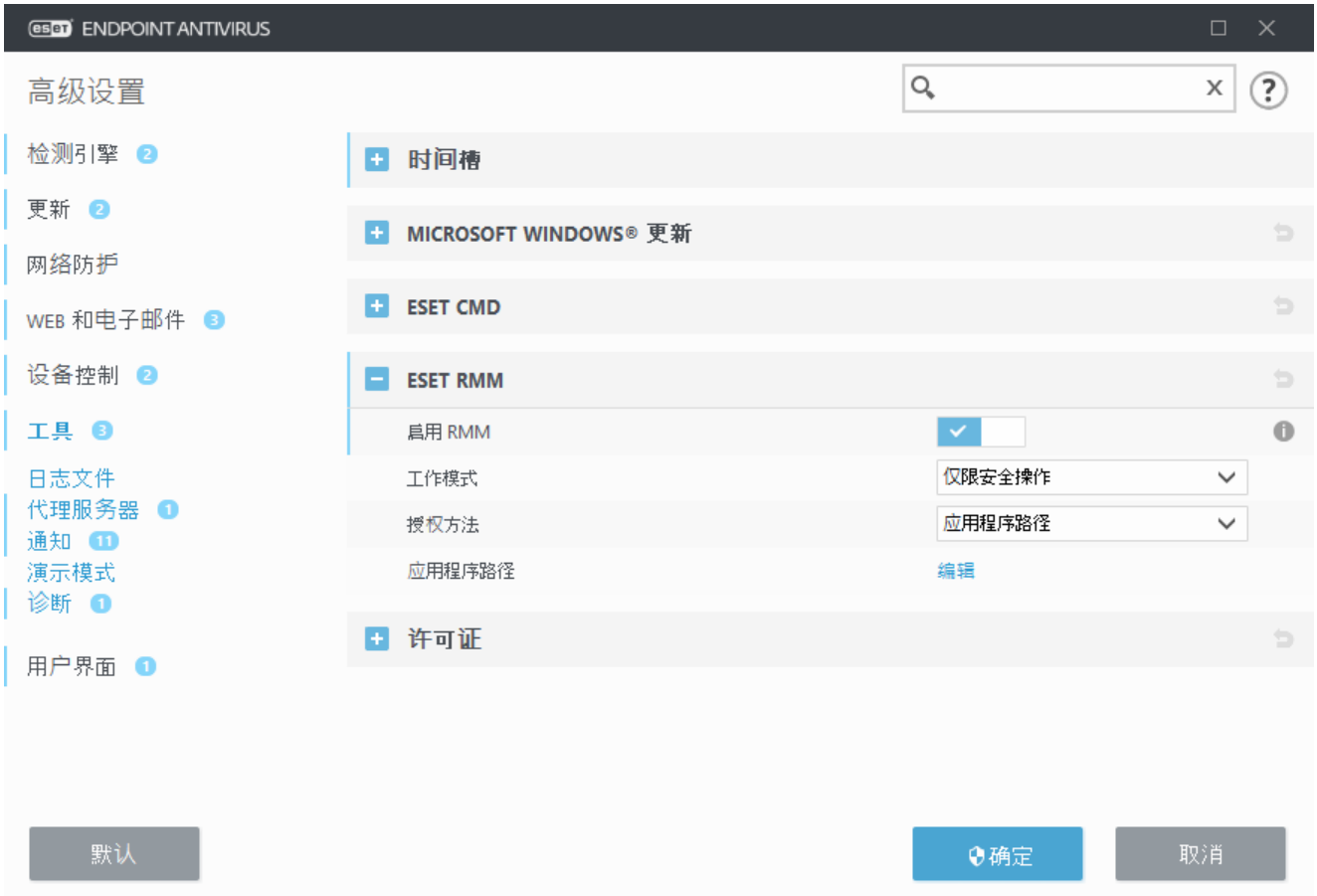
其他语言版本：

如果您正在查找 ESET Endpoint 产品的其他语言版本，请访问我们的下载页面。

有关 ESET 商业版产品与 Windows 10 兼容性的详细信息。

如何激活远程监控和管理

远程监控和管理 (RMM) 是使用可供管理服务提供商访问的本地安装的服务器代理监管和控制软件系统（例如桌面、服务器和移动设备上的软件系统）的过程。ESET Endpoint Antivirus 可以由 RMM 进行管理（从版本 6.6.2028.0 开始）。



默认情况下，ESET RMM 处于禁用状态。若要启用 ESET RMM，请按 **F5** 访问“高级设置”，单击**工具**，展开 **ESET RMM** 并打开**启用 RMM** 旁边的开关。

工作模式 – 如果要为安全和只读操作启用 RMM 接口，请选择**仅安全操作**。如果要为所有操作启用 RMM 接口，请选择**所有操作**。

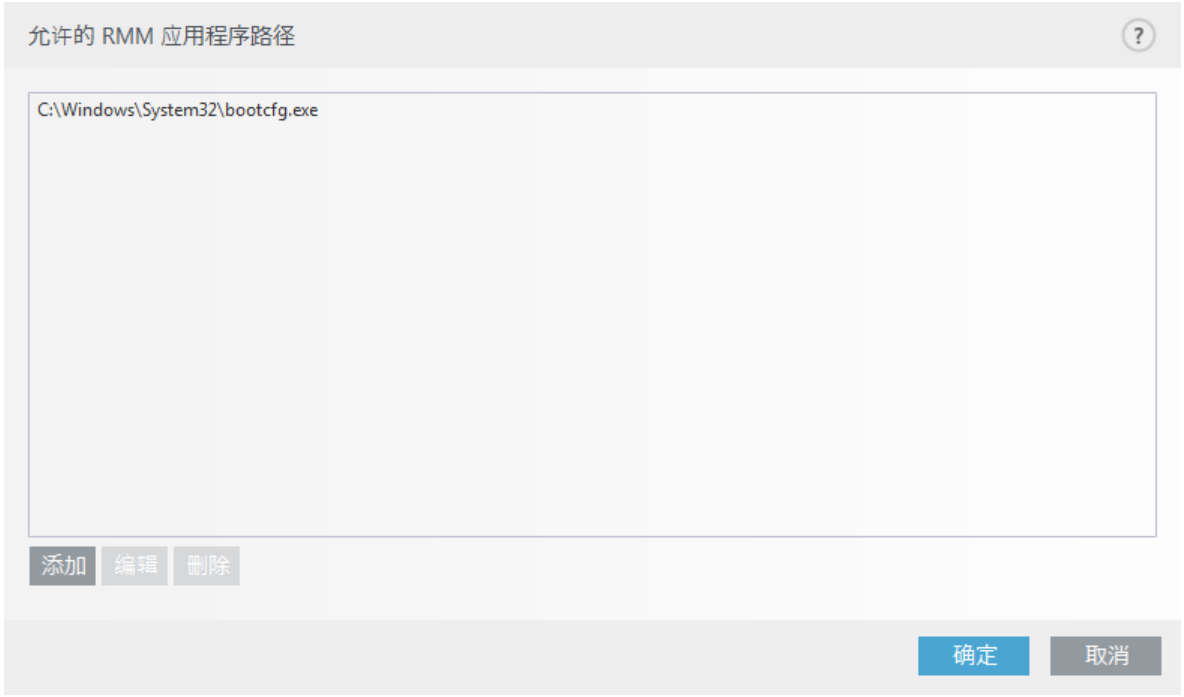
操作	仅安全操作模式	所有操作模式
获取应用程序信息	✔	✔
获取配置	✔	✔
获取许可证信息	✔	✔
获取日志	✔	✔
获取防护状态	✔	✔
获取更新状态	✔	✔
设置配置		✔
启动激活		✔
启动扫描	✔	✔
启动更新	✔	✔

授权方法 – 设置 RMM 授权方法。若要使用授权，在下拉菜单中选择**应用程序路径**，或者选择**无**。

RMM 应始终使用授权以防止恶意软件禁用或规避 ESET Endpoint 防护。

应用程序路径 – 允许运行 RMM 的特定应用程序。如果选择**应用程序路径**作为授权方法，请单击

编辑以打开**允许的 RMM 应用程序路径**配置窗口。



添加 – 创建新的允许的 RMM 应用程序路径。输入路径或单击 **...** 按钮以选择可执行文件。

编辑 – 修改现有的允许的路径。如果可执行文件的位置更改为另一个文件夹，则使用**编辑**

删除 – 删除现有允许的路径。

默认 ESET Endpoint Antivirus 安装包含位于 Endpoint 应用程序目录（默认路径为 *C:\Program Files\ESET\ESET Security*）中的 ermm.exe 文件ermm.exe 与 RMM 插件交换数据，该插件可与链接到 RMM 服务器的 RMM 服务器代理通信。

- ermm.exe – ESET 开发的命令行实用工具，允许管理 Endpoint 产品以及与任何 RMM 插件通信。
- RMM 插件是在 Endpoint 窗口系统上本地运行的第三方应用程序。该插件旨在与特定的 RMM 服务器代理（如 Kaseya 和 ermm.exe 通信。
- RMM 服务器代理是在 Endpoint 窗口系统上本地运行的第三方应用程序（如来自 Kaseya 的程序）。服务器代理与 RMM 插件和 RMM 服务器通信。

如何阻止从 Internet 下载特定文件类型

如果您不希望允许从 Internet 下载特定文件类型（例如exepdf 或 zip请结合通配符来使用 URL 地址管理。按 F5 键以访问**高级设置**。依次单击 **Web 和电子邮件 > Web 访问保护**，然后展开 **URL 地址管理**。单击**地址列表**旁边的**编辑**

在**“地址列表”**窗口中，选择**“阻止的地址列表”**，然后单击**“编辑”**，或单击**“添加”**以创建

新列表。将打开一个新窗口。如果要创建新列表，请从**“地址”**列表类型下拉菜单中选择**“已阻止”**，并命名该列表。如果要在访问当前列表中的文件类型时收到通知，请在应用滑块条时启用**“通知”**。从下拉菜单中选择**“日志记录”**严重级别。远程管理员可以收集带有**“警告”**最低级别的记录。

单击**“添加”**以输入掩码，该掩码可指定要阻止下载的文件类型。如果要阻止从特定网站下载特定文件（例如 *http://example.com/file.exe*），请输入完整的 URL。可使用通配符来涵盖一组文件。问号（?）代表单个可变字符，星号（*）则代表包含零个或更多字符的可变字符串。例如，掩码 **/*.zip* 可阻止下载所有的 zip 压缩文件。

请注意，仅当文件扩展名是文件 URL 的一部分时，才可以使用此方法阻止特定文件类型的下载。如果网页使用文件下载 URL（例如 *www.example.com/download.php?fileid=42*），则会下载位于此链接中的任何文件，即使该文件的扩展名已在阻止之列也是如此。

如何最小化 ESET Endpoint Antivirus 用户界面

当远程管理时，可以应用“可见性”预定义策略。

如果不远程管理，请手动执行以下步骤：

1. 按 **F5** 访问“高级”设置并展开**用户界面 > 用户界面元素**。
2. 将**启动模式**设置为所需的值。关于启动模式的更多信息。
3. 禁用**启动时显示初始屏幕**和**使用声音信号**。
4. 配置通知。
5. 配置应用程序状态。
6. 配置确认消息。
7. 配置警报和消息框。

最终用户许可协议

自 2021 年 10 月 19 日起生效。

重要说明：在下载、安装、复制或使用前，请仔细阅读产品应用程序的以下条款。**下载、安装、复制或使用本软件即表示您同意这些条款和条件并承认隐私政策** 隐私政策。

最终用户许可协议

本最终用户使用许可协议（“协议”）由 ESET, spol. s r. o..(“ESET”或“提供商”）与作为自然人或法人的您（“您”或“最终用户”）签订。ESET 位于 Einsteinova 24, 85101 Bratislava, Slovak Republic。注册地为布拉迪斯拉发第一地区法院商业注册处，企业性质为股份有限公司，注册号 3586/B。BIN 31333532。 协议授权您使用此处第 1 条中定义的软件。此处条款 1 中定义的软件可能存储在数据承载工具上、通过电子邮件发送、从 Internet 下载、从提供商的服务器下载或者按照以下指定的条款从其他来源获得。

这不是购买合同，而是关于最终用户权利的协议。无论是此软件的副本，还是经过商业包装的包含此软件的物理介质，亦或根据本协议最终用户有权使用的任何其他副本，所有权均归提供商所有。

在安装、下载、复制或使用软件过程中单击“我接受”或“我接受…”，即表示您同意本协议的条款和条件并确认隐私政策。如果您不同意本协议的任意条款及条件和/或隐私政策，请立刻单击取消选项、取消安装或下载、销毁或退还本软件、安装介质、随附文档和购买发票给提供商或您从中获取软件的渠道。

您同意使用软件表示您已经阅读本协议，您理解并同意遵守本协议的条款。

1.**软件。**本协议中的“软件”是指: (i) 本协议附带的计算机程序及其所有组成部分；(ii) 磁盘、CD-ROM、DVD、电子邮件及任何附件或附带本协议提供的其他介质的所有内容，包括数据承载工具提供、通过电子邮件提供或通过 Internet 下载的对象代码形式的软件；(iii) 任何有关本软件的书面说明材料和任何其他相关文档，包括但不限于所有软件说明、软件规格、软件特点或操作说明、使用软件的操作环境的说明、使用或安装软件的说明，或任何关于如何使用软件的说明（以下称“文档”）；(iv) 软件的副本、软件错误的修复程序、软件的附加程序、软件的扩展、软件的修改版本及

软件组件更新(如果有)，关于这一点，提供商根据本协议第 3 条授予您许可。软件将仅以可执行目标代码的形式提供。

2.**安装、计算机和许可证密钥。**数据承载工具上提供、通过电子邮件发送、从 Internet 下载、从提供商服务器下载或从其他来源获得的软件需要安装。文档中指定了安装方式。任何可能对本软件有不利影响的计算机程序或硬件都不能安装在安装本软件的计算机上。计算机是指硬件，包括但不限于个人计算机、笔记本电脑、工作站、掌上电脑、智能电话、手持电子设备或本软件针对其而设计并将于其上安装和/或使用的其他电子设备。任何可能对本软件有不利影响的计算机程序或硬件都不能安装在安装本软件的计算机上。计算机是指硬件，包括但不限于个人计算机、笔记本电脑、工作站、掌上电脑、智能电话、手持电子设备或本软件针对其而设计并将于其上安装和/或使用的其他电子设备。许可证密钥是指唯一的符号、字母、数字或特殊符号的序列，提供给最终用户以允许本软件的合法使用、其特定版本或根据本协议延长许可证的期限。

3.**许可**。如果您同意本条件，同意本协议条款并且遵守此处规定的所有条款，提供商将授予您以下权利(“许可”)：

a) **安装和使用。**您将具有在计算机硬盘或其他永久介质中安装软件以进行数据存储，在计算机系统内存中安装和存储软件，实施、存储和显示软件的非独占、不可转让的权利。

b) **许可数量规定。**软件的使用权利受最终用户数量约束。一位最终用户指(i) 在一个计算机系统上安装软件；或 (ii) 如果许可约束范围为邮箱数量，则单个用户指的是通过邮件用户代理(“MUA”)接收电子邮件的计算机用户。如果 MUA 接受电子邮件，然后将其自动分发到多个用户，则最终用户数量应根据收到电子邮件的实际用户数量确定。如果邮件服务器执行邮件网关的功能，则最终用户数量应等于上述网关所服务的邮件服务器用户数量。如果未指定数量的电子邮件地址（例如通过别名）指向一个用户，用户接受这些地址，并且客户端不自动将邮件分发给大量用户，则需要一台计算机的许可证。您不得同时在多台计算机上使用同一许可。仅当最终用户根据限制（因提供商授予的许可证数量而引起）而有权使用本软件时，最终用户才有权输入本软件的许可证密钥。许可证密钥被视为保密信息，除非本协议或提供商允许，否则您不得与第三方共享许可证或允许第三方使用许可证密钥。如果您的许可证密钥被盗用，请立即通知提供商。

c) **家庭版/商业版。**本软件的家庭版应仅在私人和/或非商业环境中专供家庭和家人使用。必须获得本软件的商业版，才能在商业环境中使用，以及将本软件用于邮件服务器、邮件中继、邮件网关或 Internet 网关。

d) **许可条款。**您使用软件的权利将受时间限制。

e) **OEM 软件。**分类为“OEM”的软件应限于在您获得该软件的计算机上使用。不得转移到其他计算机。

f) **NFR、试用软件。**分类为“非转售性”、NFR 或试用的软件不得用于付费用途，只能用于演示或测试软件功能。

g) **许可终止。**许可将在授予的期限结束时自动终止。如果不遵守本协议的任何条款，提供商有权撤销协议，不影响提供商在此类不测事件下的任何权利或合法补救措施。如果取消许可，您必须立刻删除、销毁本软件及所有备份副本，或自行承担费用将软件及所有备份副本返还至 ESET 或您购买软件的地方。在许可终止后，提供商有权取消最终用户使用本软件功能（这些功能需要连接到提供商的服务器或第三方服务器）的权利。

4.**具有数据收集和 Internet 连接要求的功能。**要正确操作本软件，需要连接到 Internet、并且必须定期连接到提供商服务器或第三方服务器和遵循“隐私政策”的适用的数据收集。以下软件功

能要求必须连接到 Internet 和适用的数据收集：

a) **软件更新。**提供商有权时常发布本软件的更新或升级（即“更新”），但没有义务提供更新。此功能在软件标准设置下启用，因此自动安装更新，除非最终用户禁用自动安装更新。为了提供更新，需要进行许可证真实性验证，包括根据“隐私政策”获取其上安装本软件的计算机和/或平台的相关信息。

任何更新的提供可能都要遵循生命周期结束政策（即“EOL 政策”），可通过访问 https://go.eset.com/eol_business 了解该政策。在本软件或其任何功能达到 EOL 政策中定义的生命周期结束日期后，将不会提供任何更新。

b) **将渗透和信息发送给提供商**。本软件包含多项功能，这些功能用于收集计算机病毒和其他恶意计算机程序与可疑对象、问题对象、潜在不受欢迎对象或潜在不安全对象(例如文件□URL□IP 数据包和以太网帧)的样本(“渗透”)并将其发送给提供商，包括但不限于安装过程、安装本软件的计算机和/或平台的信息，本软件的操作和功能信息(“信息”)。这些信息和渗透可能包含已安装本软件的计算机上的最终用户或其他用户的数据(包括随机或意外获得的个人数据)，以及受附带相关联元数据的渗透影响的文件。

信息和渗透可通过以下软件功能进行收集：

i.LiveGrid 信誉系统功能包括将与渗透有关的单向哈希收集起来并发送给提供商。可在本软件的标准设置下启用此功能。

ii.LiveGrid 反馈系统功能包括将附带相关元数据的威胁和信息收集起来并发送给提供商。此功能可在本软件的安装过程中由最终用户激活。

提供商将仅使用获得用于分析和检查威胁以及改善软件和许可证真实性验证的“信息”和“威胁”，并将采取合理措施保证所获信息安全。如果您启用本软件的上述功能，则“威胁”和“信息”可由提供商按照“隐私政策”和相关法规收集和处理。您可以随时停用此功能。

就本协议而言，有必要收集、处理和存储数据，使提供商能够根据隐私政策识别您的身份。您特此承认提供商以自有方式检查您是否按照本协议条款使用此软件。您特此承认，就本协议而言，需要通过与提供商计算机系统或作为其分销和支持网络的商业合作伙伴进行软件通信来传输数据，以确保软件功能正常、授权使用软件以及保护提供商的权利。

本协议缔结后，提供商或作为其分销和支持网络的任何商业合作伙伴均有权传输、处理和存储标识您的重要数据，用于计费目的、本协议的履行以及您计算机上通知的传输。

关于隐私、个人数据保护和您作为数据主体所拥有权利的详细信息可以在“隐私政策”(“隐私政策”可在提供商的网站上找到，并可在安装过程中直接访问)中找到。您还可以从软件的帮助部分中访问此信息。

5.**行使最终用户的权利**。您必须亲自或通过员工行使最终用户权利。您只能将软件用于确保操作安全和保护购买了许可证的计算机或计算机系统

6.**权利的限制。**您不得复制、分发、提取组件或创建软件的衍生版本。使用软件时，您必须遵守以下限制：

a) 您可以在永久存储介质上创建一份软件副本作为备份副本，前提是不在任何其他计算机上安装或使用该存档备份副本。创建软件的任何其他副本应视为违反本协议。

b) 您不得以本协议明确提供的方式以外的任何其他方式使用、修改、翻译、复制或转让软件或软件副本的使用权。

c) 您不得出售软件、授予从属许可、将软件出租给他人，或从他人租用软件或借出软件用于提供商业服务。

d) 您不得在法律明确禁止此类限制的范围之外以任何其他方式反向工程、反编译、反汇编软件，或试图获得软件的源代码。

e)您同意使用软件的方式必须符合有关软件使用的相关法律中的所有适用法规，包括但不局限于，符合版权法和其他知识产权中适用的限制。

f) 您同意将只以不会限制其他最终用户获取这些服务的可能性的方式使用该软件及其功能。提供商保留限制向个体最终用户提供的服务范围，以确保最大数量的最终用户能够使用服务的权利。限制服务范围还将意味着完全杜绝在提供商的服务器或与软件的特定功能相关的第三方服务器上使用软件的任何功能和删除数据及信息的可能性。

g) 您同意不从事涉及使用许可证密钥的任何违反本协议条款的活动，或向任何无权使用本软件的人员提供许可证密钥，例如以任何形式转让已使用或未使用的许可证密钥，以及未经授权复制或分发复制或生成的许可证密钥，或从提供商以外的来源获得许可证密钥从而使用本软件。

7.**版权**。软件及所有权利，包括但不局限于所有权和知识产权，归ESET和/或其许可提供商所有。它们受国际条约条款以及使用此软件的国家的所有其他适用法律保护。软件的结构、组织和代码均为 ESET 和/或其许可提供商的重要商业机密和保密信息。您不得复制软件，第 6 (a) 款中指定的情况除外。允许按照本协议创建的任何副本必须包含与软件上显示的相同版权和其他所有权声明。如果您反向工程、反编译、反汇编源或试图以违反本协议条款的方式获得软件源代码，则您同意自此类行为开始起获得的任何信息将自动且不可逆地转让给提供商，并全部为提供商所有。

8.**保留权利**。除本协议中未明确授予您作为软件最终用户的权利以外，提供商特此保留所有软件权利。

9.**多个语言版本，双介质软件，多个副本**。如果软件支持多个平台或多种语言，或者如果您获得多个软件副本，则只能将软件用于已购买许可的计算机系统数量和版本。您不得将不使用的软件的任何版本或副本出售、出租、租用、授予从属许可、借出或转让给其他人。

10.**协议开始和终止。**本协议自您同意本协议条款之日起生效。您可以通过永久卸载、销毁或返还（费用自付）软件、所有备份副本以及提供商或其商业合作伙伴提供的所有相关材料来随时终止本协议。您使用软件及其任何功能的权利可能要遵循 EOL 政策。在本软件或其任何功能达到 EOL 政策中定义的生命周期结束日期后，您使用本软件的权利将终止。不考虑本协议终止方式，第 7、8、11、13、19 和 21 款的条款应保持无限期有效。

11.**最终用户声明**。作为最终用户，您了解软件“按原样”提供，不带任何明示或暗示担保，在适用法律允许的最大范围内。提供商、其许可提供商或分支机构或者版权所有者都不得提供任何明示或暗示的陈述或保证，包括但不限于适销性保证、特定用途适用性保证或对软件不侵犯任何第三方专利、版权、商标或其他权利的保证。提供商或任何其他方均不保证软件包含的功能符合您的要求，或软件操作将顺畅无错为实现预期目的而选择此软件以及安装、使用此软件和软件应用结果的全部责任和风险由您承担。

12.**无其他义务**。除本协议特别列出的义务以外，本协议不对提供商及其许可提供商施加任何其他义务。

13.**责任限制**。在适用法律允许的最大范围内，任何情况下提供商、其员工或许可提供商均不对以下损失负责：在适用法律允许的最大范围内，任何情况下提供商、其员工或许可提供商均不对以下损失负责：以任何形式造成的任何赢利、收入或销售额损失，任何数据损失，为获得备用物品或服务支付的额外费用，财产损失、人身伤害，营业中断，商业信息损失，或任何特殊、直接、间接、意外、经济、涵盖、犯罪、特殊或后继损失。无论这些损失是由合约、故意误操作、疏忽或其他责任理论造成，还是因安装、使用或无法使用本软件导致，提供商、其员工或许可提供商均不负责，即使已经通知提供商或其许可提供商或分支机构此类损失的可能。由于某些国家和某些法律不允许免责，但可能允许责任限制，因此提供商、其员工或许可提供商的责任应限制为您购买许可所支付的价格。

14. 本协议中的任何条款均不影响被法律认可具备消费者权利和地位的一方的权利。

15.**技术支持**□ESET 或 ESET 委托的第三方将出于自行考量提供技术支持，不具有任何保证或声明。在本软件或其任何功能达到 EOL 政策中定义的生命周期结束日期后，将不会提供任何技术支持。提供技术支持前，最终用户需要备份所有现有数据、软件和程序工具□ESET 和/或 ESET 委托的第三方不承担因提供技术支持导致的数据、财产、软件或硬件破坏或损失或者利润损失□ESET 和/或 ESET 委托的第三方保留决定解决问题是否超出技术支持范围的权利□ESET 保留出于自行考量拒绝、暂停或终止提供技术支持的权利。出于提供技术支持的目的，可能需要遵循“隐私政策”的许可证信息、信息和其他数据。

16.**转让许可**。除非违背协议条款，否则软件可以在不同计算机系统之间转移。如果不违背协议条款，最终用户仅有权在提供商同意下，将许可及从本协议产生的所有权利转让给其他最终用户，并受以下条款约束□(i) 原始最终用户不得保留软件的任何副本□(ii) 权利转让必须从原始最终用户转交给新最终用户□(iii) 新最终用户必须承担原始最终用户在本协议条款下承担的所有权利和义务□(iv) 原始最终用户必须向新最终用户提供文档，证明第 17 款下指定的软件正版性。

17.**证明软件的正版性。**最终用户可以采用以下任意方式证明软件的使用权□(i) 通过提供商或提供商指定的第三方发布的许可证书□(ii) 通过书面许可协议，如果已缔结此类协议□(iii) 通过提交发送给提供商的包含许可详细信息(用户名和密码)的电子邮件。出于证明软件正版性的目的，可能需要遵循“隐私政策”的许可证信息和最终用户身份数据。

18.**政府当局和美国政府许可**。软件提供给政府当局（包括美国政府）时具有本协议介绍的许可权利和限制。

19.**贸易控制合规性**□

a) 您将不得直接或间接地向任何人出口、再出口、转让或以其他方式提供该软件，不得以任何方式使用该软件，也不得涉及任何行为，否则可能导致 ESET 或其控股公司、其子公司及其任何控股公司的子公司以及由其控股公司控制的实体（“关联公司”）违反《贸易管制法》或承担《贸易管制法》所规定的不良后果，包括

i. 美国、新加坡、英国、欧盟或其任何成员国的任何政府、州或监管机构、将履行本协议规定义务的国家/地区、成立或运维 ESET 或其任何关联企业的国家/地区颁布或通过的针对出口、再出口或转让商品、软件、技术或服务进行控制、限制或施加许可要求的任何法律，和

ii. 美国、新加坡、英国、欧盟或其任何成员国的任何政府、州或监管机构、将履行本协议规定义务的国家/地区、成立或运维 ESET 或其任何关联企业的国家/地区实施的任何经济、金融、贸易或其他方式的制裁、限制、禁运、进出口禁令、禁止转移资金或资产或提供服务或其他等效措施。

（上述“i.”和“ii.”部分中提到的法律行为统称为“《贸易管制法》”）。

b) 如果发生以下情况，ESET 有权立即中止或终止这些条款所规定的义务：

i.ESET 合理认为用户已违反或可能违反了本协议第 19 a) 款的规定；或

ii. 最终用户和/或软件受《贸易管制法》约束，因此 ESET 合理认为继续履行本协议所规定的义务可能会导致 ESET 或其关联公司违反《贸易管制法》，或承担《贸易管制法》所规定的不良后果。

c) 本协议无意，也不应理解或解释为诱导或要求任何一方以不遵循《贸易管制法》、受《贸易管制法》处罚或禁止的方式行事或不作为（或者同意行事或不作为）。

20.**通知**。所有通知、返还的软件和文档必须交付给：ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic，但不影响 ESET 根据本协议的第 22 条有权向您传达对本协议、隐私政策、EOL 政策以及文档所做的任何更改。ESET 可能会通过软件向您发送电子邮件、应用内通知，也可能会在我们的网站上发布通信帖子。您同意接收 ESET 以电子形式发送的法律通信，包括有关条款、特殊条款或隐私政策变更的任何通信、任何合同修改/赞同、要约邀请、通知或其他法律通信。此类电子通信应等同于书面形式接收，除非适用法律明确要求采用其他形式的通信。

21.**适用法律**。本协议受斯洛伐克法律管辖，并按斯洛伐克法律解释。最终用户和提供商同意，法律与联合国国际货物销售合同公约之间的冲突原理不适用。您明确同意，与提供商之间发生的任何索赔或争端，或任何方式的与软件使用相关的索赔或争端，其唯一裁决权属于斯洛伐克布拉迪斯拉发第一地区法院，并且您明确同意上述法院作出的裁决。

22.**通用条款**。如果本协议中的任何条款无效或无法执行，将不影响协议其他条款的有效性，按照此处规定的条款这些条款仍然有效且可执行。本协议已以英文履行。如果出于方便目的或任何其他目的而准备了本协议的任何翻译，或者本协议的各语言版本之间存在差异，则以英文版本为准。

ESET 保留随时更改本软件以及出于以下目的修订本协议的条款、其附件、附录、隐私政策、EOL 政策和文档或其任何部分的权利：(i) 反映对本软件或 ESET 开展业务方式的更改；(ii) 出于法律、法规或安全原因，或 (iii) 防止滥用或损害。将通过电子邮件、应用内通知或其他电子方式通知您本协议的任何修订。如果您不同意对本协议的拟议变更，可以在收到变更通知后的 30 内，根据第 10 条终止履行本协议。除非您在该时限内终止履行本协议，否则拟议变更将视为被接受，并自您收到变更通知之日起开始对您生效。

您与提供商签署的本协议是关于本软件的唯一完整协议，它完全取代任何之前的关于软件的表述、讨论、承诺、沟通或广告。

EULAID: EULA-PRODUCT-LG; 3537.0

隐私政策

ESET, spol. s r. o.，注册办公室位于斯洛伐克共和国 Einsteinova 24, 851 01 Bratislava，在布拉迪斯拉发第一地区法院商业注册处注册，企业性质为股份有限公司，注册号为3586/B，业务识别号：31333532（简称为“ESET”或“我们”）。ESET 希望在处理个人数据和客户隐私时保持透明。为了达到上述目的，我们发布了此隐私政策，唯一目的是告知我们的客户（“最终用户”或“您”）有关以下主题的信息：

- 个人数据处理、
- 数据机密性、

• 数据主体的权利。

个人数据处理

在我们的产品中实施的由 ESET 提供的服务是根据最终用户许可协议（“EULA”）提供的，但其中一些可能需要特别注意。我们希望为您提供与服务提供有关的数据收集的更多详细信息。我们提供最终用户许可协议和产品文档中所述的各种服务，例如更新/升级服务（ESET LiveGrid®）防止数据滥用、支持等。为了正常运行，我们需要收集以下信息：

• 涵盖涉及安装过程和计算机信息的更新和其他统计数据，包括产品安装所在的平台以及我们产品的操作和功能信息，例如操作系统、硬件信息、安装 ID（许可证 ID）IP 地址（MAC 地址、产品的配置设置。

• 作为 ESET LiveGrid® 信誉系统的一部分、与渗透有关的单向哈希，通过将已扫描的文件与云中白名单和黑名单项目数据库进行比较，可提高我们恶意软件防护解决方案的效率。

• 作为 ESET LiveGrid® 反馈系统的一部分、野生的可疑样本和元数据使 ESET 能够立即应对我们的最终用户的需求，以及使我们持续响应最新的威胁（如果有的话）。我们依赖您向我们发送

o渗透，如病毒和其他恶意程序以及可疑程序的潜在样本；有问题、潜在不受欢迎或潜在不安全的对象，如可执行文件、由您报告为垃圾邮件的电子邮件或我们的产品标记的电子邮件；

o关于本地网络中的设备的信息，例如设备的类型、供应商、型号和/或名称；

o涉及 Internet 使用的信息，例如 IP 地址和地理信息（IP 数据包（URL 和以太网帧；

o崩溃转储文件及包含的信息。

我们不希望收集超出此范围的数据，但有时不可避免。意外收集的数据可能包含在恶意软件本身中（在您不知情或未批准的情况下收集）或者作为文件名或 URL 的一部分包含在内，我们不打算将其构成我们系统的一部分，或为了本隐私政策中声明的目的而对其进行处理。

• 出于计费目的、许可证真实性验证以及我们服务的提供，需要提供许可信息（如许可证 ID）和个人资料（如名字、姓氏、地址、电子邮件地址）。

• 支持服务可能需要您的支持请求中包含联系信息和数据。根据您选择与我们联系的渠道，我们可能会收集您的电子邮件地址、电话号码、许可证信息、产品详细信息和支持案例的描述。可能会要求您向我们提供其他信息，以便于提供支持服务。

数据机密

ESET 是一家通过附属实体或合作伙伴（作为我们分销、服务和支持网络的一部分）在全球运营的公司。出于 EULA 的履行（例如，提供服务、支持或计费）考虑，经 ESET 处理的信息可能会在附属实体或合作伙伴之间传输。根据您的位置和选择要使用的服务，欧盟委员会可能会要求我们将您的数据传输到缺乏妥善决策的国家/地区。即使在这种情况下，每一次信息传输都会遵守数据保护法规，并且仅在需要时才会进行传输。必须毫无例外地建立标准合同条款、约束性企业规则或其他适当保护措施。

在根据最终用户许可协议提供服务的同时，我们会尽最大努力防止存储数据超过必要时间。我们的保留期可能长于许可证的有效期，只是让您有时间轻松方便地续订。出于统计目的，可能会进一步处理来自 ESET LiveGrid® 的必要和匿名统计信息和其他数据。

ESET 会实施适当技术和组织措施来确保与潜在风险相称的安全级别。我们会尽最大努力来确保提供处理系统和服务所需的持续机密性、完整性、可用性和灵活性。但当发生导致您的权利和自由遭受威胁的数据泄漏时，我们会随时通知监管机构以及数据主体。作为数据主体，您有权向监管机构提出投诉。

数据主体的权利

ESET 遵守斯洛伐克法律的规定，并且我们受欧盟的数据保护法的约束。在遵守适用数据保护法律规定条件的前提下，您作为数据主体享有以下权利：

- 有权请求访问 ESET 收集的您的个人数据，
- 有权更正可能不准确的个人数据（您也有权补充不完整的个人数据），
- 有权请求清除您的个人数据，
- 有权请求限制处理您的个人数据，
- 有权反对处理
- 还有权提出投诉
- 数据迁移。

我们确信：出于我们向我们的客户提供服务和产品的合法权益，我们处理的每一条信息都是有价值和有必要的。

如果您希望行使作为数据主体的权利或有疑问，请发送邮件至：

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk