

ESET ENDPOINT ANTIVIRUS

用户指南

Microsoft Windows 8 / 7 / Vista / XP / 2000 / Home Server / NT4 (SP6)

[单击此处以下载本文档的最新版本](#)

ESET ENDPOINT ANTIVIRUS

Copyright 2013 ESET, spol. s r. o.

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

有关更多信息, 请访问 www.eset.com。

保留所有权利。未经作者书面同意, 本文档的任何部分均不得复制、存入检索系统或以任何形式或任何方式传播, 包括电子的、机械的、影印、记录、扫描或其他方式。

ESET, spol. s r. o. 保留未经事先通知即更改任何所述应用程序软件的权利。

全球客户支持 : www.eset.com/support

修订日期 20. 2. 2013

目录

1. ESET Endpoint Antivirus	5
1.1 系统需求	5
1.2 预防	5
2. 安装	7
2.1 典型安装	8
2.2 自定义安装	10
2.3 输入用户名和密码	13
2.4 升级到更新版本	13
2.5 计算机扫描	14
3. 入门指南	15
3.1 用户界面设计简介	15
3.2 程序工作不正常时如何应对	16
3.3 更新设置	17
3.4 代理服务器设置	18
3.5 设置保护	19
4. 使用 ESET Endpoint Antivirus	20
4.1 计算机	21
4.1.1 病毒和间谍软件防护	22
4.1.1.1 文件系统实时防护	22
4.1.1.1.1 要扫描的对象	22
4.1.1.1.2 运行扫描于 (事件触发式扫描)	23
4.1.1.1.3 高级扫描选项	23
4.1.1.1.4 清除级别	23
4.1.1.1.5 何时修改实时防护配置	24
4.1.1.1.6 检查实时防护	24
4.1.1.1.7 实时防护不工作时如何应对	24
4.1.1.2 文档防护	25
4.1.1.3 计算机扫描	25
4.1.1.3.1 扫描类型	26
4.1.1.3.1.1 智能扫描	26
4.1.1.3.1.2 自定义扫描	26
4.1.1.3.2 扫描目标	26
4.1.1.3.3 扫描配置文件	27
4.1.1.3.4 扫描进度	27
4.1.1.4 开机扫描	28
4.1.1.4.1 自动启动文件检查	28
4.1.1.5 按路径的排除项	29
4.1.1.6 ThreatSense 引擎参数设置	30
4.1.1.6.1 对象	30
4.1.1.6.2 选项	30
4.1.1.6.3 清除	31
4.1.1.6.4 扩展名	31
4.1.1.6.5 限制	32
4.1.1.6.6 其他	32
4.1.1.7 检测到渗透	32
4.1.2 可移动磁盘	34
4.1.3 设备控制	34
4.1.3.1 设备控制规则	35
4.1.3.2 添加设备控制规则	36
4.1.4 基于主机的入侵预防系统 (HIPS)	37
4.2 Web 和电子邮件	39
4.2.1 Web 访问保护	40
4.2.1.1 HTTP, HTTPS	40
4.2.1.1.1 Web 浏览器主动模式	41
4.2.1.2 URL 地址管理	41
4.2.2 电子邮件客户端防护	42
4.2.2.1 POP3, POP3S 过滤器	43
4.2.2.2 IMAP, IMAPS 协议控制	43
4.2.2.3 电子邮件客户端集成	44
4.2.2.3.1 电子邮件客户端防护配置	45
4.2.2.4 删除渗透	45
4.2.3 协议过滤	45
4.2.3.1 Web 和电子邮件客户端	45
4.2.3.2 排除的应用程序	46
4.2.3.3 排除的 IP 地址	46
4.2.3.3.1 添加 IPv4 地址	47
4.2.3.3.2 添加 IPv6 地址	47
4.2.3.4 SSL 协议检查	47
4.2.3.4.1 证书	47
4.2.3.4.1.1 信任的证书	48
4.2.3.4.1.2 排除的证书	48
4.2.3.4.1.3 加密的 SSL 通信	48
4.3 更新程序	49
4.3.1 更新设置	51
4.3.1.1 更新配置文件	52
4.3.1.2 高级更新设置	52
4.3.1.2.1 更新模式	52
4.3.1.2.2 代理服务器	53
4.3.1.2.3 连接到 LAN	53
4.3.1.2.4 创建更新副本 - 镜像	54
4.3.1.2.4.1 从镜像更新	55
4.3.1.2.4.2 镜像更新问题故障排除	56
4.3.1.3 更新回滚	56
4.3.2 如何创建更新任务	57
4.4 工具	58
4.4.1 日志文件	59
4.4.1.1 日志维护	60
4.4.2 计划任务	61
4.4.2.1 创建新任务	63
4.4.3 防护统计	64
4.4.4 查看活动	65
4.4.5 ESET SysInspector	65
4.4.6 ESET Live Grid	66
4.4.6.1 可疑文件	66
4.4.7 运行进程	67
4.4.8 隔离区	68
4.4.9 提交文件以供分析	69
4.4.10 警报和通知	70
4.4.10.1 邮件格式	71
4.4.11 系统更新	71
4.4.12 诊断	71
4.4.13 许可证	72
4.4.14 远程管理	73
4.5 用户界面	74
4.5.1 图形	74
4.5.2 警报和通知	75
4.5.2.1 高级设置	75
4.5.3 隐藏的通知窗口	76
4.5.4 访问设置	76
4.5.5 程序菜单	77
4.5.6 右键菜单	78
4.5.7 演示模式	78
5. 高级用户	79

5.1	代理服务器设置	79
5.2	导入和导出设置	79
5.3	键盘快捷方式	80
5.4	命令行	80
5.5	ESET SysInspector	82
5.5.1	ESET SysInspector 介绍	82
5.5.1.1	启动 ESET SysInspector	82
5.5.2	用户界面和应用程序的使用	82
5.5.2.1	程序控件	83
5.5.2.2	ESET SysInspector 导航	84
5.5.2.2.1	键盘快捷方式	85
5.5.2.3	比较	86
5.5.3	命令行参数	87
5.5.4	服务脚本	87
5.5.4.1	生成服务脚本	88
5.5.4.2	服务脚本结构	88
5.5.4.3	执行服务脚本	90
5.5.5	常见问题解答	90
5.5.6	ESET SysInspector 在 ESET Endpoint Antivirus 中使用	92
5.6	ESET SysRescue	92
5.6.1	最低要求	92
5.6.2	如何创建急救光盘	93
5.6.3	目标选择	93
5.6.4	设置	93
5.6.4.1	文件夹	93
5.6.4.2	ESET Antivirus	94
5.6.4.3	高级设置	94
5.6.4.4	Internet 协议	94
5.6.4.5	可引导 USB 设备	94
5.6.4.6	刻录	95
5.6.5	使用 ESET SysRescue	95
5.6.5.1	使用 ESET SysRescue	95
6.	词汇表	96
6.1	渗透类型	96
6.1.1	病毒	96
6.1.2	蠕虫	96
6.1.3	木马	96
6.1.4	Rootkit	96
6.1.5	广告软件	97
6.1.6	间谍软件	97
6.1.7	潜在的不安全应用程序	97
6.1.8	潜在的不受欢迎应用程序	97
6.2	电子邮件	98
6.2.1	广告	98
6.2.2	恶作剧	98
6.2.3	欺诈	98
6.2.4	识别垃圾邮件欺骗	99

1. ESET Endpoint Antivirus

ESET Endpoint Antivirus 代表了真正集成计算机安全的新方法。最新版本的 ThreatSense 扫描引擎提高速度和精确性，从而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 是我们结合最高防护与最少系统占用的长期努力诞生出的完整安全解决方案。基于人工智能的高级技术能够主动消除病毒、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的计算机。

ESET Endpoint Antivirus 主要设计用于小型商业/企业环境的工作证。它可以用于 ESET Remote Administrator，允许您轻松管理任意数量的客户端工作站，应用策略与规则，监视检测，并从任何联网计算机远程配置。

1.1 系统需求

要使 ESET Endpoint Antivirus 无缝工作，系统应满足以下硬件和软件需求：

Microsoft® Windows® 2000, XP, NT4 (SP6)

400 MHz 32 位 (x86) / 64 位 (x64)

128MB RAM 系统内存

320 MB 可用空间

Super VGA (800 x 600)

Microsoft® Windows® 8, 7, Vista, Home Server

1 GHz 32 位 (x86) / 64 位 (x64)

512MB RAM 系统内存

320 MB 可用空间

Super VGA (800 x 600)

1.2 预防

使用计算机时，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[渗透](#)和以下带来的风险。攻击。要提供最大保护和便利，正确使用病毒防护系统和遵守一些有用规则非常重要。

定期更新

根据 ESET Live Grid 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，以不断提高防病毒程序用户的保护级别；更新配置如果不正确会降低程序的效果。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

恶意软件的作者喜欢利用各种系统漏洞，以提高恶意代码的传播效果。这就是软件公司密切关注其应用程序中出现的新漏洞，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。此类应用程序的示例包括 Windows 操作系统和使用广泛的 Internet 浏览器 Internet Explorer。

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，并故意破坏重要数据。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。此类预防措施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

使用正确的设置定期自动扫描计算机，可删除因病毒签名更新陈旧而漏掉的渗透。

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船舶。如果您打开新文件时比较谨慎，可为自己节省清除计算机渗透所需的大量时间和精力。一些有用的规则包括：

- 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。
- 不使用管理员帐户执行计算机的日常工作。

2. 安装

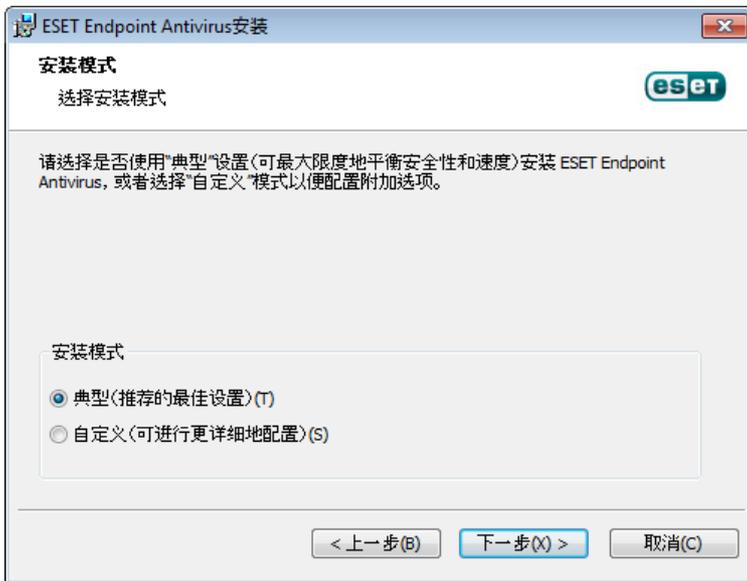
启动安装程序后，安装向导将引导您完成设置过程。

重要信息： 请确保您的计算机上没有安装其他病毒防护程序。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。参见[知识库文章](#)了解常见病毒防护软件的卸载工具列表（提供英语和多个其他语言版本）。

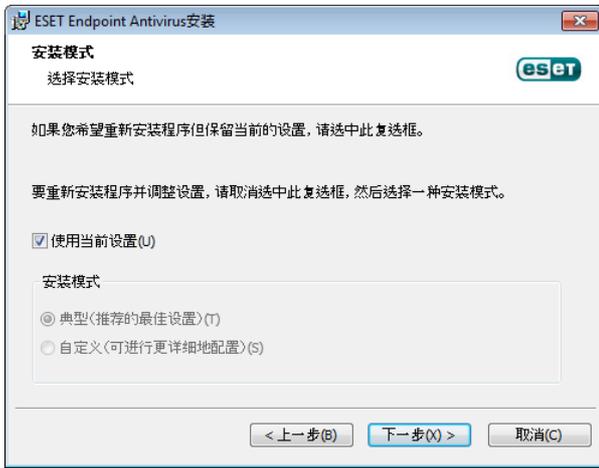


首先，程序检查是否有较新版本的 ESET Endpoint Antivirus。如果发现更新版本，将在安装过程的第一步通知您。如果您选择下载并安装新版本选项，将下载新版本并继续安装。在下一步中将显示最终用户许可证协议。请阅读并单击接受以确认接受最终用户许可证协议。接受后，安装可能以两个场景继续：

1. 如果首次在计算机上安装 ESET Endpoint Antivirus，接受最终用户许可协议后将看到下面的窗口。这里您可以在[典型安装](#)和[自定义安装](#)之间选择并相应继续。



2. 如果在 ESET Endpoint Antivirus 的以前版本上安装此软件，以下窗口允许您选择对新安装使用当前程序设置；或者，如果取消选中使用当前设置选项，则在上述两个安装模式之间选择。



2.1 典型安装

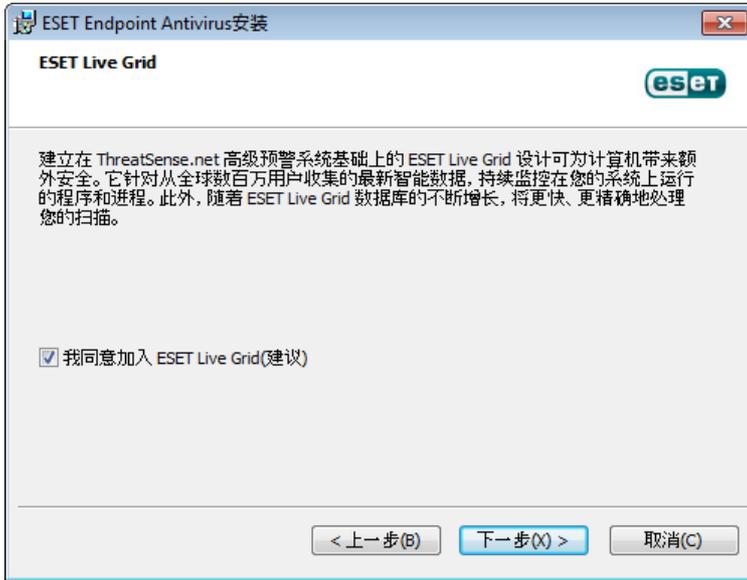
典型安装提供适合于大多数用户的配置选项。这些设置提供出色的安全性、简易设置和高系统性能。典型安装模式是默认选项，如果您对特定设置没有特别要求，建议使用此选项。

选择该安装模式并单击下一步之后，将提示您输入自动更新程序的用户名和密码。在为系统提供持续保护方面，这是不可或缺的重要步骤。



在相应字段中输入用户名和密码，这些信息即在购买或注册产品后收到的验证数据。如果当前没有用户名和密码，请单击以后设置更新参数复选框。以后可以将用户名和密码输入程序中。

下一步是配置 ESET Live Grid。ESET Live Grid 有助于确保 ESET 能够及时且不间断地获得有关新渗透的信息，以便为客户提供保护。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被分析、处理并添加到病毒库中。



默认选中选项我同意参与 ESET Live Grid，将启用此功能。

安装过程的下一步是配置潜在不受欢迎的应用程序检测。潜在不受欢迎的应用程序未必是恶意的，但可能对操作系统的运行产生不良影响。参见[潜在不受欢迎的应用程序](#)章节了解更多详细信息。



典型安装模式的最后一步是单击安装按钮来确认安装。



2.2 自定义安装

自定义安装模式适用于具有微调程序经验的用户以及希望在安装期间修改高级设置的用户。

选择安装模式并单击下一步之后，将提示您选择用于安装的目标位置。程序默认安装到以下目录：

C:\Program Files\ESET\ESET Endpoint Antivirus\

单击浏览... 可更改此位置（不建议）。

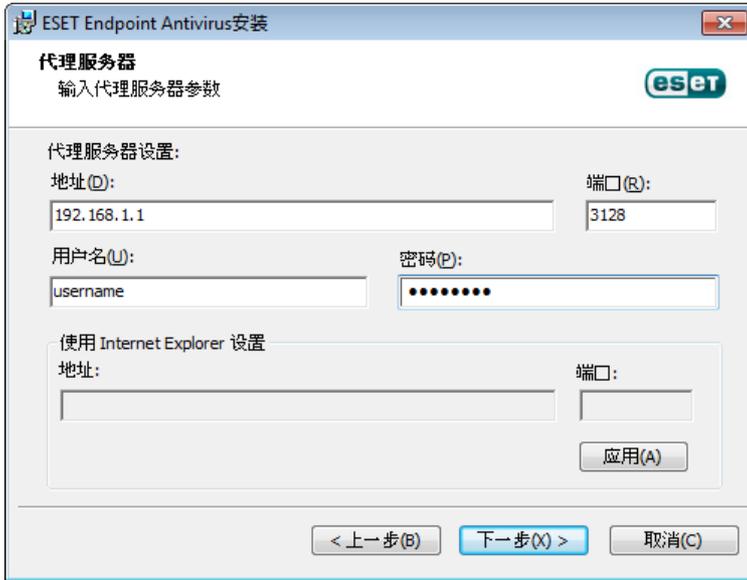


接下来，输入用户名和密码。此步骤与典型安装的步骤相同（请参见[典型安装](#)”）。

单击下一步继续配置 Internet 连接。如果使用代理服务器，则必须正确配置才能使病毒库更新正常工作。如果您不确定是否使用代理服务器连接到 Internet，请选择我不确定 Internet 连接是否使用代理服务器。使用与 Internet Explorer 相同的设置（建议）并单击下一步。如果不使用代理服务器，请选择我不使用代理服务器选项。



要配置代理服务器设置，请选择我使用代理服务器并单击下一步。在地址字段中输入代理服务器的 IP 地址或 URL。在端口字段中指定代理服务器接受连接的端口（默认情况下使用 3128 端口）。如果代理服务器要求验证，则输入有效的用户名和密码，才能访问代理服务器。如果需要，也可以从 Internet Explorer 中复制代理服务器设置。要执行此操作，请单击应用并确认选择。



此安装步骤可用于指定如何在系统上处理自动程序更新。单击更改...可访问高级设置。

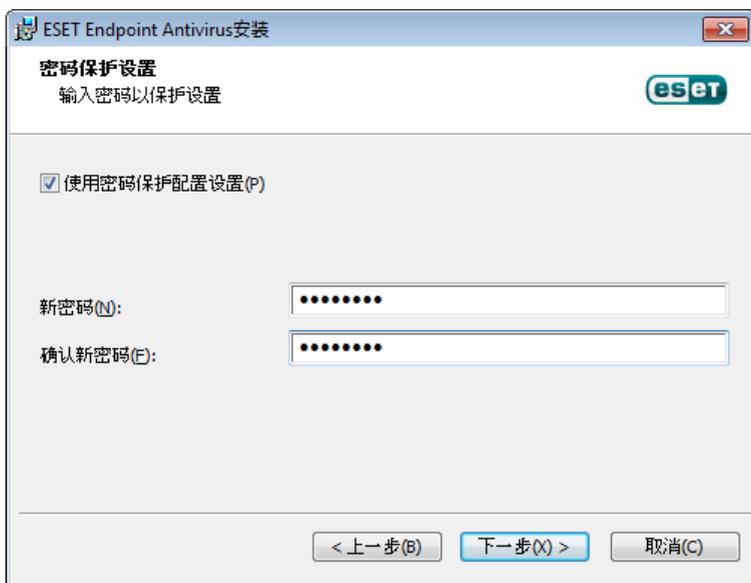


如果您不想更新程序组件，请选择从不更新程序组件选项。选择下载程序组件前询问选项会在每次系统尝试下载程序组件时显示确认窗口。要自动下载程序组件更新，请选择始终更新程序组件选项。



注意：程序组件更新后，通常需要重新启动。我们建议选择如果需要，无提示直接重新启动计算机选项。

下一个安装窗口提供用于设置密码以保护程序设置的选项。选择使用密码保护配置设置选项，在新密码和确认新密码字段中输入您的密码。更改或访问 ESET Endpoint Antivirus 设置需要此密码。两个密码字段匹配后，单击下一步继续。



接下来的安装步骤，自动更新、ESET Live Grid 和潜在不受欢迎应用程序的检测，与典型安装模式中的步骤相同（请参见[典型安装](#)”）。

单击安装（在安装准备就绪窗口中）以完成安装。完成安装后，将提示您激活产品。参见[典型安装](#)了解产品激活的更多信息。

2.3 输入用户名和密码

自动更新程序对获得最佳功能非常重要。只有将正确的用户名和密码输入到更新设置中，才可能实现这一点。

如果您在安装期间未输入用户名和密码，可以现在输入。按 CTRL+U 并在 许可证详细信息 窗口中，输入随 ESET 安全产品收到的许可证数据。

在输入用户名和密码时，精确地键入非常重要：

- 用户名和密码区分大小写，用户名中的连字符是必要的。
- 密码长度为十个字符，全部为小写。
- 我们在密码中不使用字母 L（而是使用数字 1）。
- 较大的 0 是数字零 (0)，较小的 0 是小写字母 o。

我们建议从注册电子邮件中进行复制和粘贴，以保证准确性。

2.4 升级到更新版本

发布 ESET Endpoint Antivirus 的更新版本可改进功能或修复自动程序模块更新无法修复的问题。有多种方法可以升级到更新版本：

1. 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，以确保所有可能系统配置能够工作。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。

2. 通过针对以前的安装来下载和安装更新版本，手动进行升级。

在安装开始时，可选择保留当前程序设置，方法是选中使用当前设置复选框。

3. 通过 ESET Remote Administrator 在网络环境中使用自动部署进行手动升级。

2.5 计算机扫描

安装 ESET Endpoint Antivirus 后，您应执行计算机扫描以检查恶意代码。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，请参阅[计算机扫描](#)一节。



3. 入门指南

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

3.1 用户界面设计简介

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：

保护状态 - 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或自定义扫描。

更新 - 显示有关病毒库更新的信息。

设置 - 选择此选项以调整计算机、Web 和电子邮件、。

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、ESET SysInspector 和 ESET SysRescue。

帮助和支持 - 提供对帮助文件、[ESET 知识库](#)和 ESET 网站以及可打开客户服务支持请求的链接的访问。



- 保护状态 屏幕可告知您计算机当前的安全性和防护级别。绿色最高防护状态表示已确保最高防护。

状态窗口还显示 ESET Endpoint Antivirus 中的常用功能。此外，还提供有关程序到期日期的信息。

3.2 程序工作不正常时如何应对

如果启用的模块工作正常，则会带有一个绿色对勾。如果工作不正常，则显示红色惊叹号或橙色通知图标。有关模块的其他信息显示在窗口的上半部分。同时还显示修复该模块的建议解决方案。要更改单个模块的状态，请在主菜单中单击设置，然后单击所需模块。



红色图标表示发生严重问题 - 未确保最大程度的防护。可能的原因包括：

- 已禁用文件系统实时防护
- 病毒库过期
- 产品未激活
- 产品许可证已过期

橙色图标表示已禁用 Web 访问保护或电子邮件客户端防护，或者程序更新有问题（病毒库过期，无法更新），或者许可证将要过期。

已禁用病毒和间谍软件防护 - 此问题由红色图标和计算机项目旁边的安全通知指示。单击启动所有病毒和间谍软件防护模块可以重新启用病毒和间谍软件防护。

已禁用 Web 访问保护 - 此问题由带有 ! 的橙色图标和安全通知状态指示。您可以通过以下方式重新启用 Web 访问保护，单击安全通知，然后单击启用 Web 访问防护。

您的许可证很快将到期 - 此问题由防护状态图标显示惊叹号来表示。许可证过期后，程序将无法更新，防护状态图标将变为红色。

许可证已过期 - 此问题由防护状态图标变为红色来表示。许可证过期后该程序将无法更新。我们建议您按照警报窗口中的说明续订许可证。

如果使用建议的解决方案无法解决问题，则单击帮助和支持以访问帮助文件或搜索 [ESET 知识库](#)。如果还需要帮助，可以提交 ESET 客户服务支持请求。ESET 客户服务将快速响应您的问题并帮助找到解决方案。

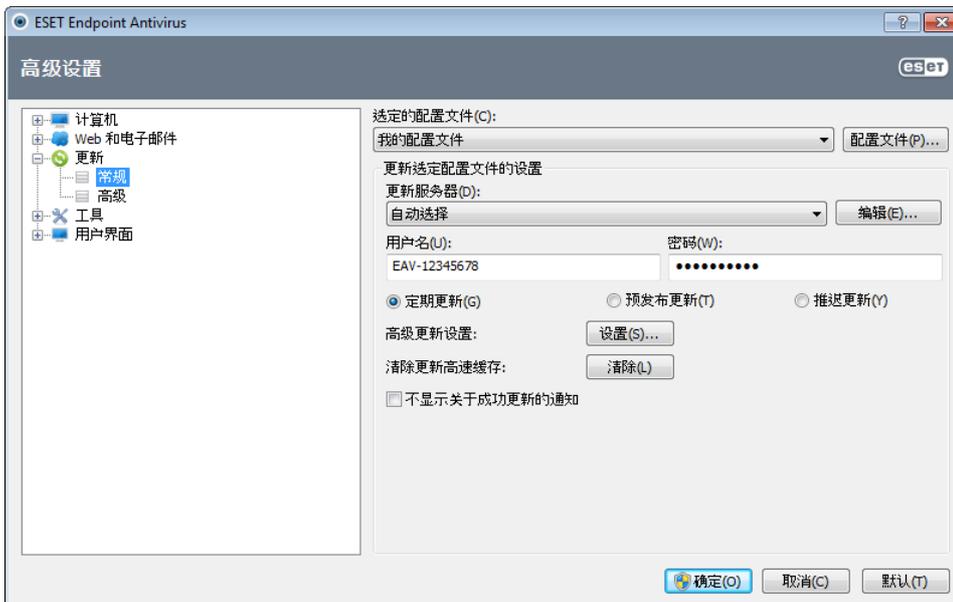
3.3 更新设置

更新病毒库和更新程序组件是全面防范恶意代码的重要组成部分。请注意其配置和操作。在主菜单中选择更新，然后单击更新病毒库，检查是否有新的数据库更新。

如果在安装 ESET Endpoint Antivirus 的过程中未输入用户名和密码，此时将提示您输入。

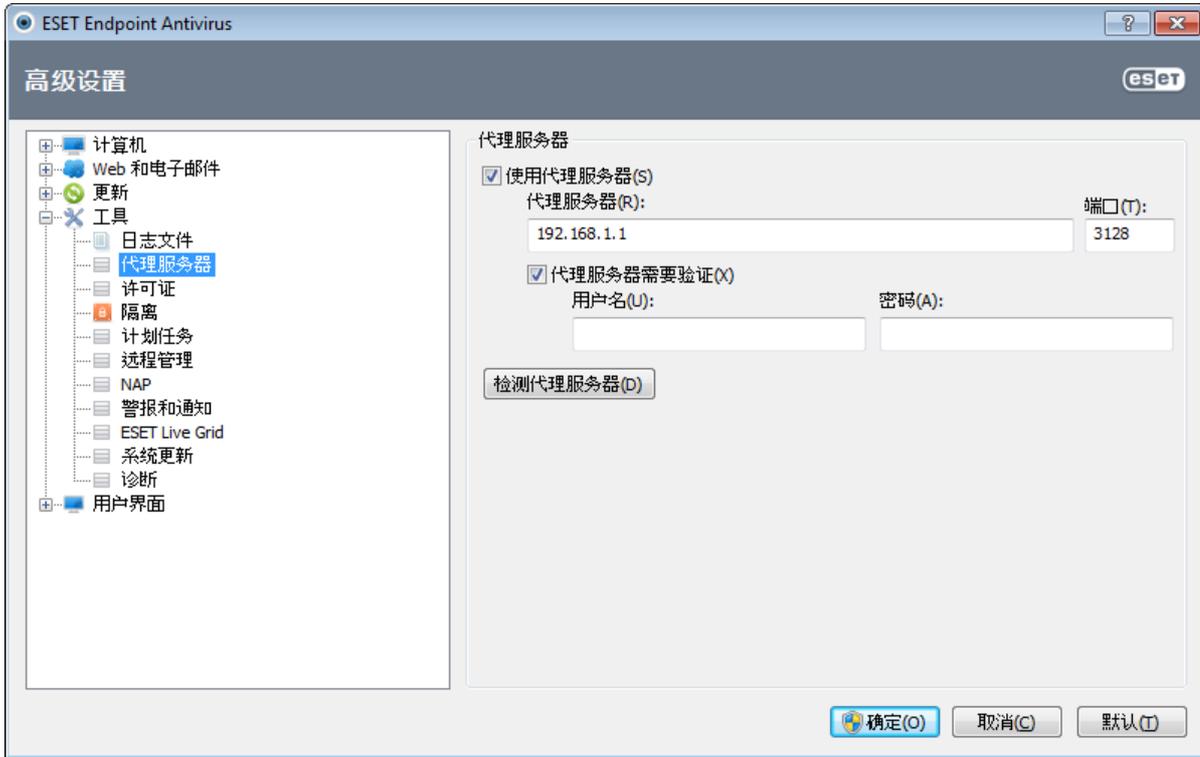


高级设置 窗口（从主菜单中单击设置，然后单击进入高级设置...，或按键盘上的 F5 键）包含其他更新选项。单击左侧 高级设置 树中的更新。更新服务器下拉菜单默认设置为自动选择。要配置高级更新选项，如更新模式、代理服务器访问、LAN 连接以及创建病毒库副本，请单击设置... 按钮。



3.4 代理服务器设置

如果在使用 ESET Endpoint Antivirus 的系统上使用代理服务器来控制 Internet 连接，则必须在高级设置中指定代理服务器的设置。要访问代理服务器配置窗口，请按 F5 打开 高级设置 窗口，并从 高级设置 树中单击工具 > 代理服务器。选择使用代理服务器选项，然后填写代理服务器（IP 地址）和端口字段。必要时，选择代理服务器需要验证选项，然后输入用户名和密码。



如果该信息不可用，可以单击检测代理服务器按钮，尝试自动检测代理服务器设置。

注意：对于不同的更新配置文件，代理服务器选项可能也有所不同。在这种情况下，单击 高级设置 树中的更新 在 高级设置 中配置不同的更新配置文件。

3.5 设置保护

ESET Endpoint Antivirus 设置对您的安全策略非常重要。未经授权的更改会潜在破坏系统的稳定和防护。要使用密码保护设置参数，在主菜单中单击设置 > 进入高级设置... > 用户界面 > 访问设置，选择密码保护设置选项，然后单击设置密码... 按钮。



在新密码和确认新密码字段输入密码，并单击确定。将来对 ESET Endpoint Antivirus 设置的任何修改将需要该密码。

4. 使用 ESET Endpoint Antivirus

ESET Endpoint Antivirus 设置选项允许您调整计算机的防护级别。



设置菜单包含以下选项：

- 计算机
- **Web 和电子邮件**

单击任意组件可以调整相应防护模块的高级设置。

计算机防护设置允许您启用或禁用以下组件：

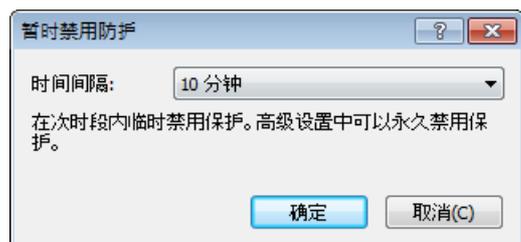
- 文件系统实时防护 - 在计算机上打开、创建或运行任何文件时，都将扫描该文件是否带有恶意代码。
- 文档防护 - 文档防护功能会在打开 Microsoft Office 文档之前对其进行扫描，还会扫描通过 Internet Explorer 自动下载的文件，如 Microsoft ActiveX 元素。
- 设备控制 - 此模块允许您扫描、阻止或调整扩展的过滤器/权限，选择用户如何访问和使用给定设备 (CD/DVD/USB...)
- HIPS - [HIPS](#) 系统监视操作系统内的事件，并按照自定义的规则集进行响应。
- 演示模式 - 启用或禁用[演示模式](#)。启用以下模式后，您将收到警告消息（潜在安全风险），主窗口将变为橙色：演示模式。
- 反隐藏防护 - 提供对可在操作系统下隐藏自己的危险程序的检测，例如 [rootkits](#)。这意味着使用普通测试技术很难检测到它们。

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** - 如果启用，则将扫描所有通过 HTTP 或 HTTPS 进行的通信以查找恶意软件。
- **电子邮件客户端防护** - 监视通过 POP3 和 IMAP 协议接收的通信。

注意：在启用进入高级设置...(F5) > 计算机 > 病毒和间谍软件防护 > 文档保护 > 集成到系统中的选项后，文档保护将显示。

单击已启用后，将显示暂时禁用防护对话框。单击确定可禁用选定的安全组件。时间间隔下拉菜单表示将禁用选定组件的时段。



要重新启用已禁用安全组件的防护，请单击已禁用。

注意：当使用此方法禁用防护时，所有禁用的防护部分将在计算机重新启动后启用。

在设置窗口的底部还有其他选项。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，请使用导入和导出设置... 选项。

4.1 计算机

在单击计算机标题后，计算机模块显示在设置窗格中。它显示所有防护模块的概要信息。要临时关闭单个模块，请单击所需模块下方的禁用。注意，这可能会降低对您的计算机的保护。要访问每个模块的详细设置，请单击配置...。

单击编辑排除... 可打开排除设置窗口，使用此窗口可排除不扫描的文件和文件夹。



暂时禁用病毒和间谍软件防护 - 禁用所有病毒防护和间谍软件防护模块。暂时禁用防护对话框显示出来，并带有时间间隔下拉菜单。时间间隔下拉菜单表示将禁用防护的时段。单击确定进行确认。

计算机扫描设置... - 单击以调整手动扫描程序（手动执行扫描）的参数。

4.1.1 病毒和间谍软件防护

病毒和间谍软件防护通过控制文件、电子邮件和 Internet 通信防范恶意系统攻击。如果检测到带有恶意代码的威胁，则病毒防护模块可以通过先阻止，然后清除、删除或将其移至隔离区，来消除威胁。

4.1.1.1 文件系统实时防护

文件系统实时防护控制系统中所有与病毒防护相关的事件。在计算机上打开、创建或运行任何文件时，都将扫描该文件是否带有恶意代码。文件系统实时防护在系统启动时启动。

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。使用 ThreatSense 技术检测方法（在 [ThreatSense 引擎参数设置](#) 部分中有描述），文件系统实时防护可能对新创建的文件和现有文件有所不同。对于新创建的文件，可以应用更深的控制级别。

为了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（除非它们已被修改）。每次病毒库更新后立刻重新扫描文件。此行为使用智能优化配置。如果禁用，则在每次访问文件时都扫描该文件。要修改此选项，请按 F5 打开高级设置窗口，并从高级设置树中单击计算机 > 病毒和间谍软件防护 > 文件系统实时防护。然后单击 ThreatSense 引擎参数设置旁的设置... 按钮，单击其他并选中或取消选中启用智能优化选项。

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。特殊情况下（比如与其他实时扫描程序存在冲突），可以通过取消选中自动启动文件系统实时防护选项来中止实时防护。



4.1.1.1.1 要扫描的对象

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 - 控制所有系统硬盘。

可移动磁盘 - 磁盘、CD/DVD、USB 存储设备等

网络驱动器 - 扫描所有映射的驱动器。

建议您保留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。

4.1.1.1.2 运行扫描于 (事件触发式扫描)

默认情况下，所有文件在打开、创建或执行时进行扫描。建议您保留默认设置，因为默认设置可为计算机提供最高级别的实时防护。

打开文件 - 启用或禁用已打开文件的扫描。

创建文件 - 启用或禁用对新创建文件或新修改文件的扫描。

执行文件 - 启用或禁用已执行文件的扫描。

可移动磁盘访问 - 启用或禁用访问具有存储空间的特定可移动磁盘触发的扫描。

4.1.1.1.3 高级扫描选项

可在计算机 > 病毒和间谍软件防护 > 系统实时防护 > 高级设置下找到更详细的设置选项。

用于新建文件和已修改文件的其他 **ThreatSense** 参数 - 新建的或修改的文件被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。除了使用基于病毒库的扫描方法外，使用高级启发式扫描可极大地提高检测率，因为它们会在发布病毒库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。要修改压缩文件扫描设置，请取消选择默认的压缩文件扫描设置选项。

用于已执行文件的其他 **ThreatSense** 参数 - 默认情况下，当文件已执行时不会使用高级启发式扫描。然而，在某些情况下，您可能想要启用此选项（通过选中执行文件时采用高级启发式扫描选项）。注意：高级启发式扫描可能会因不断增加的系统需求而使执行某些程序的速度变慢。在启用了从外部设备执行文件时采用高级启发式扫描选项时，如果您希望排除一些可移动磁盘，不对其文件执行进行高级启发式扫描，请单击例外...来打开可移动磁盘驱动器排除窗口。在这里，您可以通过选择或取消选择代表每个端口的复选框来自定义设置。

4.1.1.1.4 清除级别

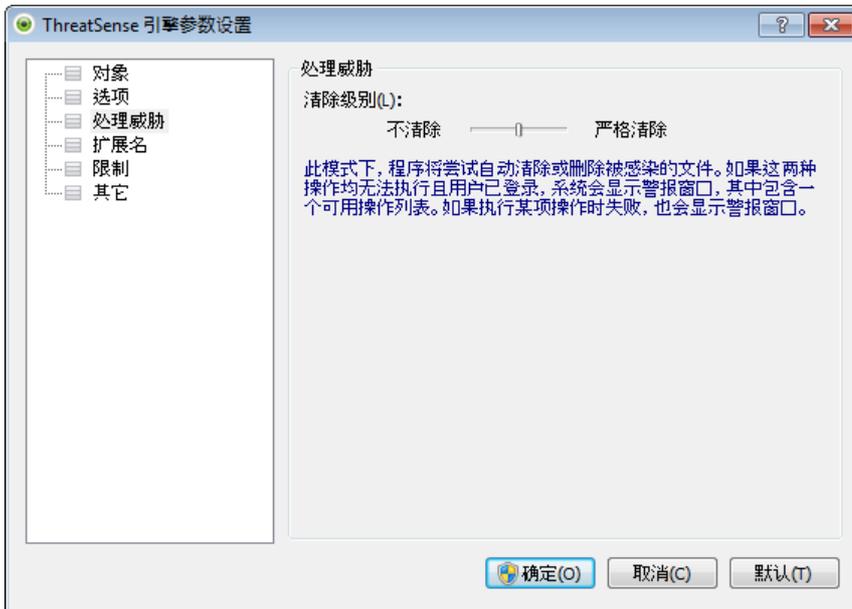
实时防护有三种清除级别（要访问它们，请单击设置...按钮，该按钮位于文件系统实时防护部分，然后单击清除分支）。

不清除 - 被感染文件将不会被自动清除。程序会显示一个警告窗口，允许用户选择操作。此级别旨在用于更高级的用户，他们了解在渗透事件中应采取哪些步骤。

标准清除 - 程序将根据预定义操作（取决于渗透类型）尝试自动清除或删除被感染文件。屏幕右下角的信息消息指示检测到或删除了被感染文件。如果无法自动选择正确操作，程序将提供一组后续操作供选择。如果预定义的操作无法完成，也会出现相同的情况。

严格清除 - 程序将清除或删除所有被感染文件。唯一例外的是系统文件。如果无法清除被感染文件，将弹出一个警告窗口，提示用户选择操作。

警告： 如果压缩文件包含一个或多个被感染的文件，有两种选择方式来处理该压缩文件。在标准模式（标准清除）中，如果压缩文件包含的文件全部被感染，则整个压缩文件将被删除。在严格清除模式中，即使压缩文件只包含一个被感染文件，则无论被压缩的其他文件是什么状态，都将删除该压缩文件。



4.1.1.1.5 何时修改实时防护配置

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。例如，与某个应用程序或另一个病毒防护程序的实时扫描程序发生冲突时。

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。要恢复默认设置，请单击文件系统实时防护窗口右下方的默认按钮（高级设置 > 计算机 > 病毒和间谍软件防护 > 文件系统实时防护）。

4.1.1.1.6 检查实时防护

要验证实时保护是否工作，是否在检测病毒，请使用测试文件 eicar.com。此文件是一个可供所有病毒防护程序检测的特殊无害文件。此文件由 EICAR（欧洲计算机防病毒研究协会）公司创建，用于测试病毒防护程序的功能。文件 eicar.com 可从以下网站下载：<http://www.eicar.org/download/eicar.com>

4.1.1.1.7 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场景，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，则需要重新启用它。要重新启用实时防护，请导航至主程序窗口中的设置并单击文件系统实时防护。

如果实时防护未能在系统启动时启动，通常是因为自动启动文件系统实时防护选项被取消选中。要启用此选项，请浏览至高级设置 (F5) 并在高级设置树中单击计算机 > 病毒和间谍软件防护 > 文件系统实时防护。在窗口底部的高级设置部分，确保选中了自动启动文件系统实时防护复选框。

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没有安装其他病毒防护程序。如果同时启用两种实时防护，它们可能互相冲突。建议您卸载系统上的任何其他病毒防护程序。

实时防护不启动

如果系统启动时实时防护未启动（且选项自动启动实时文件系统防护已经启用），可能是因为与其他程序发生冲突。如果是这种情况，请联系 ESET 客户服务。

4.1.1.2 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。集成到系统将启动防护系统。要修改此选项，请按 F5 打开高级设置窗口，并从高级设置树中单击计算机 > 病毒和间谍软件防护 > 文件防护。启用后，可从 ESET Endpoint Antivirus 主程序窗口的设置 > 计算机中查看文档防护。

此功能由使用 Microsoft Antivirus API 的应用程序（如 Microsoft Office 2000 和更高版本或 Microsoft Internet Explorer 5.0 和更高版本）启动。

4.1.1.3 计算机扫描

手动扫描程序是病毒防护解决方案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。我们建议您定期执行系统的全面扫描以检测病毒，这些病毒在写入到磁盘时无法由[文件系统实时防护](#)捕获。如果文件系统实时防护此时被禁用、病毒库未更新或将文件保存到磁盘时未检测为病毒，会发生这种情况。



提供两种计算机扫描。[智能扫描](#)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选择特定扫描目标。

请参见[扫描进度](#)一章，了解有关扫描进程的更多信息。

我们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。

4.1.1.3.1 扫描类型

4.1.1.3.1.1 智能扫描

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渗透。[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](#)部分。

4.1.1.3.1.2 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选项。此外，还可以通过单击设置... > 清除，从三种清除级别中进行选择。

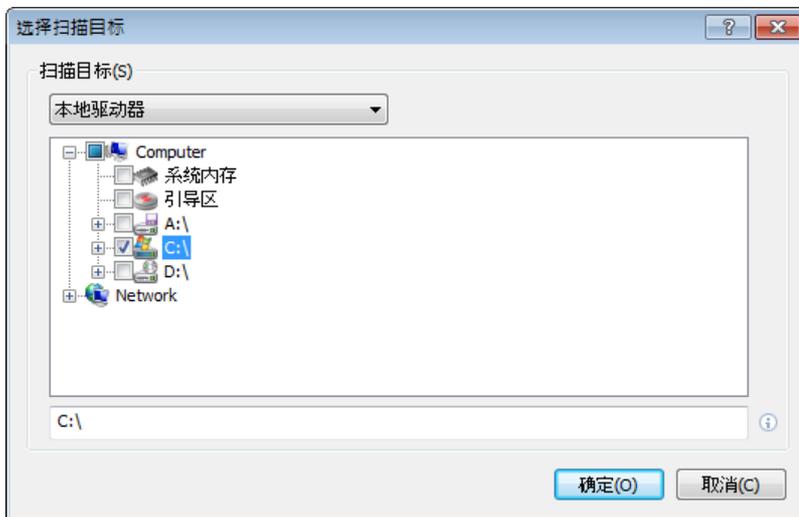
对于有病毒防护程序使用经验的高级用户，适合于使用自定义扫描来执行计算机扫描。

4.1.1.3.2 扫描目标

扫描目标窗口可定义扫描哪些对象（内存、驱动器、扇区、文件和文件夹）中的渗透。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 - 选择选定扫描配置文件中设置的目标。
- 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。
- 不选择 - 取消所有选择。

还可以通过输入要扫描的文件或文件夹路径，指定扫描目标。从列有计算机上所有可用设备的树结构中选择目标。



要迅速浏览至某个扫描目标，或直接添加某个所需的目标，请在文件夹列表下的空白字段中输入。仅当树结构中没有选定任何目标且扫描目标菜单设置为不选择时，才可执行此操作。

4.1.1.3.3 扫描配置文件

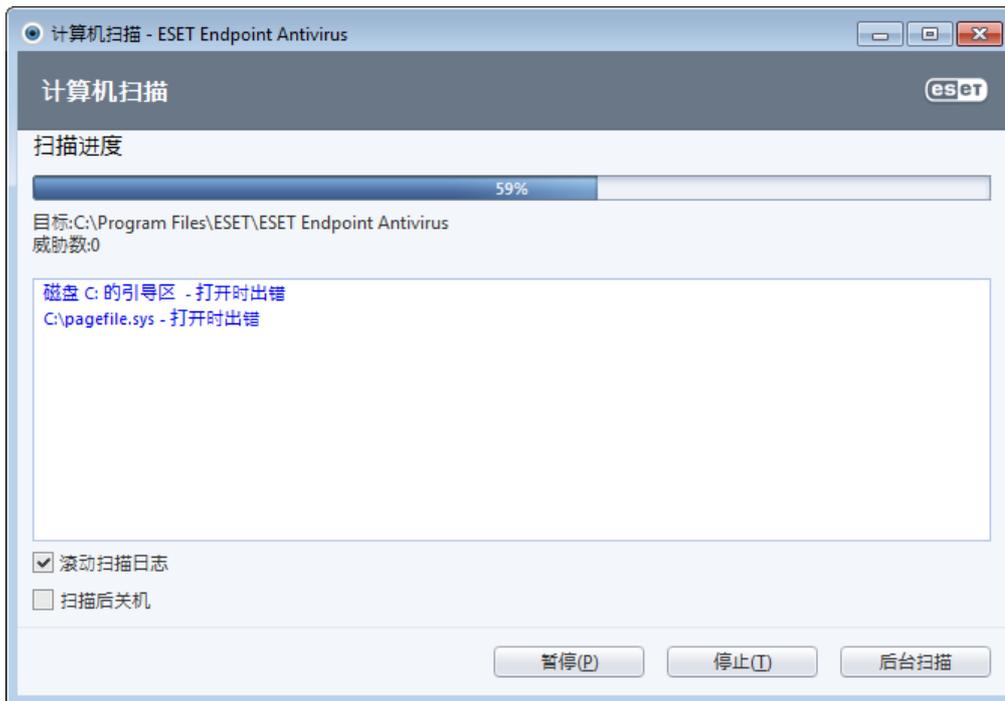
可以保存您的首选扫描参数以用于将来的扫描。建议您创建不同的配置文件（带有各种扫描目标、扫描方法和其他参数）用于每次定期扫描。

要创建新配置文件，请打开高级设置窗口 (F5) 并单击计算机 > 病毒和间谍软件防护 > 计算机扫描 > 配置文件...。设置配置文件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，请参见 [ThreatSense 引擎参数设置](#) 部分，查看扫描设置中每个参数的描述。

示例：假设您想要创建自己的扫描配置文件而且智能扫描配置部分适用，但您不希望扫描加壳程序或潜在的不安全应用程序，并且还希望应用严格清除。从设置配置文件窗口中，单击添加...按钮。在配置文件名称字段中输入新配置文件的名称，并选择智能扫描（在从以下配置文件中复制设置下拉菜单中）。然后调整其余参数以满足您的需要。

4.1.1.3.4 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。



注意：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百分比。该值根据扫描对象总数得出。

目标 - 当前扫描的对象及其位置的名称。

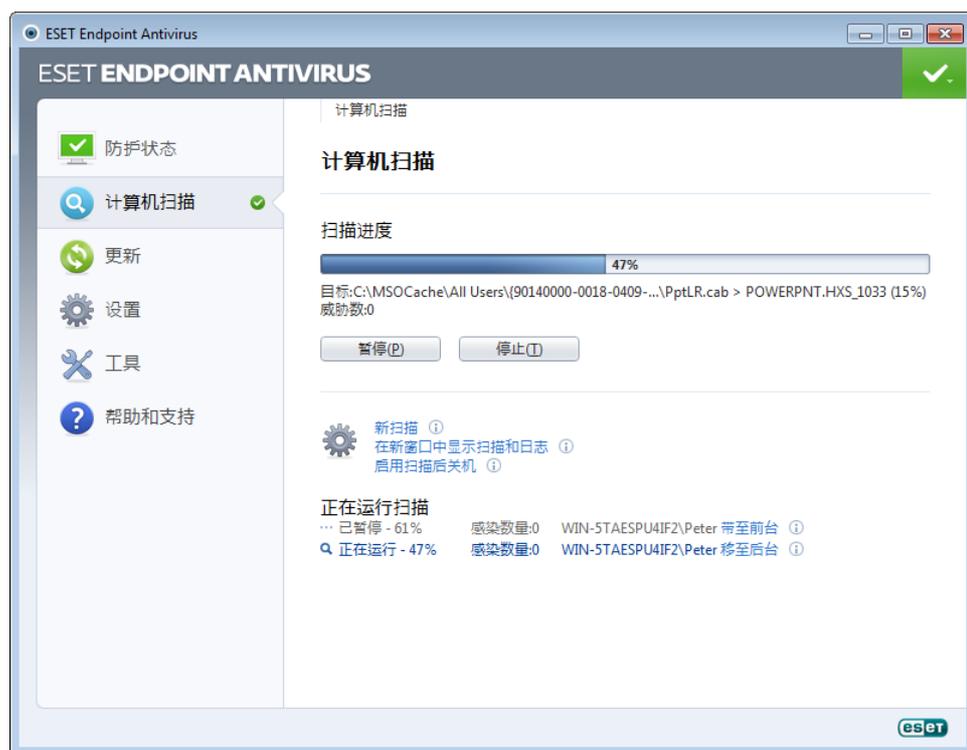
威胁数 - 显示在扫描期间已找到的威胁总数。

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。

后台扫描 - 可以运行另一个并行扫描。运行的扫描将最小化到后台。



单击移至前台 将扫描移至前台并返回扫描进程。

滚动扫描日志 - 如果启用，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。

启用扫描后关机 - 当手动扫描计算机完成时，可按计划关机。确认关机对话框将打开，60 秒超时后关机。如果希望取消请求的关机操作，则单击取消。

4.1.1.4 开机扫描

自动启动文件检查将在系统启动或病毒库更新时执行。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。要修改设置，导航至工具 > 计划任务，单击自动启动文件检查和编辑...按钮。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](#)。

4.1.1.4.1 自动启动文件检查

扫描级别下拉菜单指定系统启动时运行的文件扫描深度。文件按要扫描的文件数量以升序排列：

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

还包括两个特定扫描级别组：

- 用户登录前运行的文件 - 包含允许未经用户登录可运行文件的位置的文件（包括几乎所有启动位置，如服务、浏览器帮助对象、winlogon 通知、Windows 计划任务条目、已知 dll 等）。
- 用户登录后运行的文件 - 包含仅允许用户登录后运行文件的位置的文件（包括仅对特定用户运行的文件，通常是 HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run 中的文件）

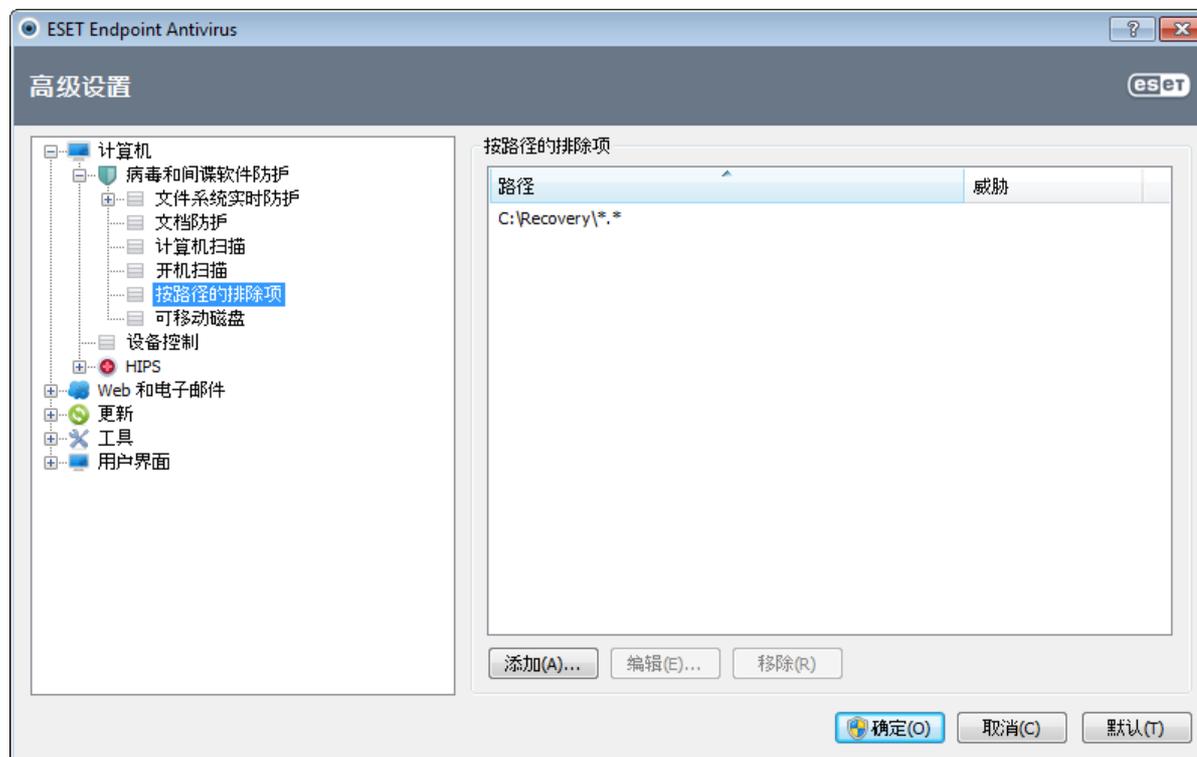
每个组的要扫描文件列表是固定的。

扫描优先级 - 用于扫描开始的优先级：

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

4.1.1.5 按路径的排除项

使用排除部分可将文件和文件夹排除在扫描之外。建议您不要改变这些选项，以确保系统扫描所有对象来查找威胁。然而，存在一些需要排除某个对象的情况。例如，会在扫描期间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。



路径 - 被排除文件和文件夹的路径。

威胁 - 如果已排除文件旁有一个威胁的名称，则表示该文件仅对给定威胁排除，并不是全部排除。因此，如果该文件稍后被其他恶意软件感染，将被病毒防护模块检测到。此类型的排除仅可用于特定类型的渗透，它既可以在报告渗透的威胁警报窗口中创建（单击显示高级选项，然后选择从检测中排除），还可以使用隔离文件上的上下文菜单选项从检测中还原和排除在设置 > 隔离中创建。

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 - 删除选择的条目。

从扫描中排除对象的步骤：

1. 单击添加...
2. 输入对象的路径或在树结构中选择对象。

可使用通配符代表一组文件。问号 (?) 代表单个可变字符，星号 (*) 则代表包含零个或多个字符的可变字符串。

示例

- 如果要排除文件夹中的所有文件，则输入文件夹路径并使用掩码 "*. *"
- 要排除包括所有文件和子文件夹在内的整个驱动器，使用掩码 D:*"
- 如果仅需要排除 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（且字符各异）且您只知道第一个字符（如 D），则使用以下格式：D?????.exe"。问号用于替代缺少（未知）的字符。

4.1.1.6 ThreatSense 引擎参数设置

ThreatSense 技术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。该技术采用了多种方法（代码分析、代码仿真、一般的识别码、病毒库等），可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 and 检测速度。ThreatSense 技术还可成功去除 Rootkit。

ThreatSense 技术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，请单击设置...按钮，该按钮位于使用 ThreatSense 技术的任何模块设置窗口中（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，
- 文档防护、
- 电子邮件客户端防护、
- Web 访问保护，
- 和计算机扫描。

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加壳程序，或在实时文件系统防护模块中启用高级启发式扫描，可能会造成系统性能下降（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。

4.1.1.6.1 对象

对象部分允许您定义将扫描渗透的计算机组件和文件。

系统内存 - 扫描攻击系统的系统内存的威胁。

引导区 - 扫描引导区以检查主引导记录中是否存在病毒。

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 以及很多其他扩展名。

自解压文件 - 自解压文件 (SFX) 是指不需要专门程序对自身进行解压的压缩文件。

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（由于有了代码仿真的原因）还支持多种加壳程序。

4.1.1.6.2 选项

使用选项部分选择在系统扫描渗透时所用的方法。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。其主要优点是能够识别过去不存在或以前的病毒库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/智能病毒库 - 高级启发式扫描具有一种独特的启发式扫描算法，该算法由 ESET 开发，它使用高级编程语言编写而成，用于优化检测计算机蠕虫和木马。有了高级启发式扫描，程序的检测功能显著提高。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。新病毒库的缺点是只能检测到它所知道的病毒（或在其基础上略做修改的病毒）。

潜在的不受欢迎应用程序 (PUA)未必是恶意的，但可能会对计算机性能造成不良影响。此类应用程序通常会在安装前提请用户同意。如果计算机上安装了这类程序，系统运行（与安装前相比）会有所不同。其中最显著的变化是：

- 以前没见过的新窗口（弹出窗口、广告），
- 启动并运行隐藏的进程，
- 系统资源的使用增加，
- 搜索结果发生改变，
- 应用程序会与远程服务器通信。

潜在的不安全应用程序 - [潜在的不安全应用程序](#)是一类用于商业目的的合法软件。其中包括远程访问工具、密码破解应用程序以及按键记录器（用于记录用户键盘输入信息）等程序。此选项默认情况下被禁用。

ESET Live Grid - 多亏 ESET 的信誉技术，可以通过基于云技术的 [ESET Live Grid](#) 的数据检查已扫描的文件，从而加快检测和扫描速度。

4.1.1.6.3 清除

清除设置决定在清除被感染文件的过程中扫描程序的行为。共有 3 个清除级别：

不清除 - 被感染文件将不会被自动清除。程序会显示一个警告窗口，允许用户选择操作。此级别旨在用于更高级的用户，他们了解在渗透事件中应采取哪些步骤。

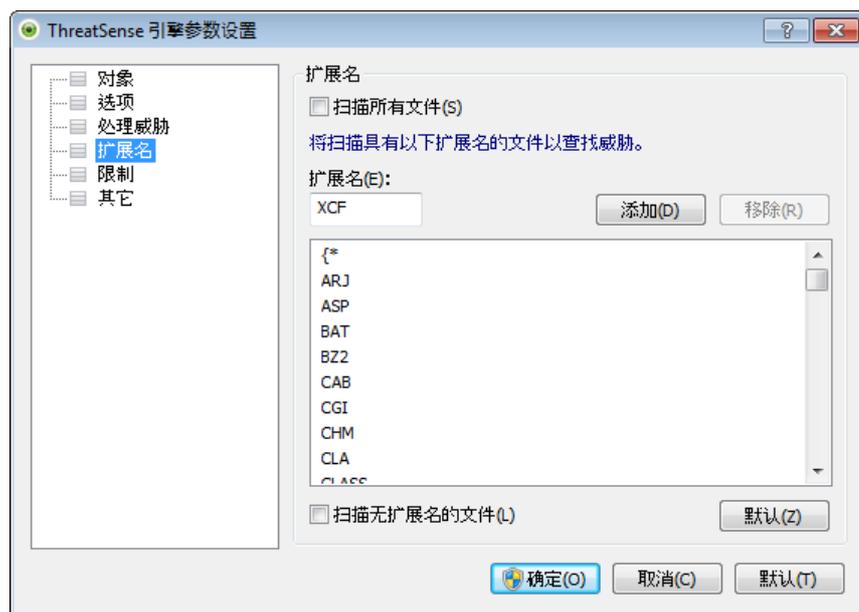
标准清除 - 程序将根据预定义操作（取决于渗透类型）尝试自动清除或删除被感染文件。屏幕右下角的信息消息指示检测到或删除了被感染文件。如果无法自动选择正确操作，程序将提供一组后续操作供选择。如果预定义的操作无法完成，也会出现相同的情况。

严格清除 - 程序将清除或删除所有被感染文件。唯一例外的是系统文件。如果无法清除被感染文件，将弹出一个警告窗口，提示用户选择操作。

警告： 如果压缩文件包含一个或多个被感染的文件，有两种选择方式来处理该压缩文件。在标准模式（标准清除）中，如果压缩文件包含的文件全部被感染，则整个压缩文件将被删除。在严格清除模式中，即使压缩文件只包含一个被感染文件，则无论被压缩的其他文件是什么状态，都将删除该压缩文件。

4.1.1.6.4 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。



默认情况下程序扫描所有文件，无论其扩展名是什么。可将任何扩展名添加到不扫描的文件列表中。如果扫描所有文件选项没有选中，则列表会更改为显示所有当前扫描的文件扩展名。

要启用对无扩展名文件的扫描，请选中扫描无扩展名的文件选项。不扫描无扩展名的文件选项将在启用了扫描所有文件选项后启用。

如果对某些文件类型的扫描导致使用该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。

使用添加和删除按钮，可以允许或禁用对特定文件扩展名的扫描。输入一个扩展名将激活添加按钮，这将在列表中添加新的扩展名。选择列表中的扩展名，然后单击删除按钮可从列表中删除该扩展名。

可使用特殊符号 *（星号）和 ?（问号）。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 ?。

仅扫描一组默认的扩展名，单击默认按钮并在提示确认时单击是确认。

4.1.1.6.5 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：

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） - 定义用于对象扫描的最大时间值。如果在此输入用户定义的值，时间用完后病毒防护模块将停止扫描对象，而不管扫描是否完成。默认值：*无限制*。

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。

压缩文件中文件的最大大小 - 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。默认值：*无限制*。

如果出于这些原因而提前中断扫描压缩文件，则压缩文件复选框仍将处于未选中状态。

注意： 不建议更改默认值，正常情况下应该没有修改它的理由。

4.1.1.6.6 其他

您可以在其他部分配置以下选项：

记录所有对象 - 如果选中此选项，日志文件将显示包括未感染文件在内的所有已扫描文件。例如，如果压缩文件中发现渗透，日志还将列出压缩文件中包含的干净文件。

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。

配置 ThreatSense 引擎参数进行计算机扫描时，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，可以启动低优先级后台扫描，从而为应用程序节约资源。

保存上一个访问时间戳 - 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间戳）。

滚动扫描日志 - 此选项允许您启用/禁用日志滚动。如果选中，信息将在显示窗口中向上滚动。

4.1.1.7 检测到渗透

渗透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、软盘等）。

标准行为

作为 ESET Endpoint Antivirus 处理渗透的常见示例，可以使用以下功能检测设备头：

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

每个功能使用标准清除级别，将尝试清除文件并移动到[隔离区](#)或终止连接。通知窗口显示在屏幕右下角的通知区域。有关清除级别和行为的更多信息，请参见[清除](#)。



清除和删除

如果实时文件系统防护没有预定义操作，程序将显示一个警报窗口，要求您从中选择一个选项。一般会有清除、删除和不操作等选项。不建议选择不操作，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。

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，使用严格清除时，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，参见[智能扫描](#)）。
- 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，然后选择扫描目标。

4.1.2 可移动磁盘

ESET Endpoint Antivirus 提供自动可移动磁盘 (CD/DVD/USB/...) 扫描。此模块允许您扫描插入的媒体。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，此模块将很有用。

连接外部设备后采取的操作 - 选择将可移动磁盘设备插入 (CD/DVD/USB) 后将执行的默认操作。如果选择了显示扫描选项选项，将显示通知，允许您选择所需操作：

- 现在扫描 - 将执行已插入可移动磁盘设备的手动扫描计算机。
- 稍后扫描 - 将不执行任何操作，同时将关闭检测到新设备窗口。
- 设置... - 打开可移动磁盘设置部分。



此外，ESET Endpoint Antivirus 具有设备控制功能，可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。

4.1.3 设备控制

ESET Endpoint Antivirus 提供自动设备 (CD/DVD/USB/...) 控制。此模块允许您扫描、阻止或调整扩展的过滤器/权限，选择用户如何访问和使用给定设备。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设备，此模块将很有用。

支持的外部设备

- CD/DVD/Blu-ray
- USB 存储
- FireWire 设备
- 刻录设备
- USB 打印机
- 蓝牙
- 读卡器
- 调制解调器
- LPT/COM 端口

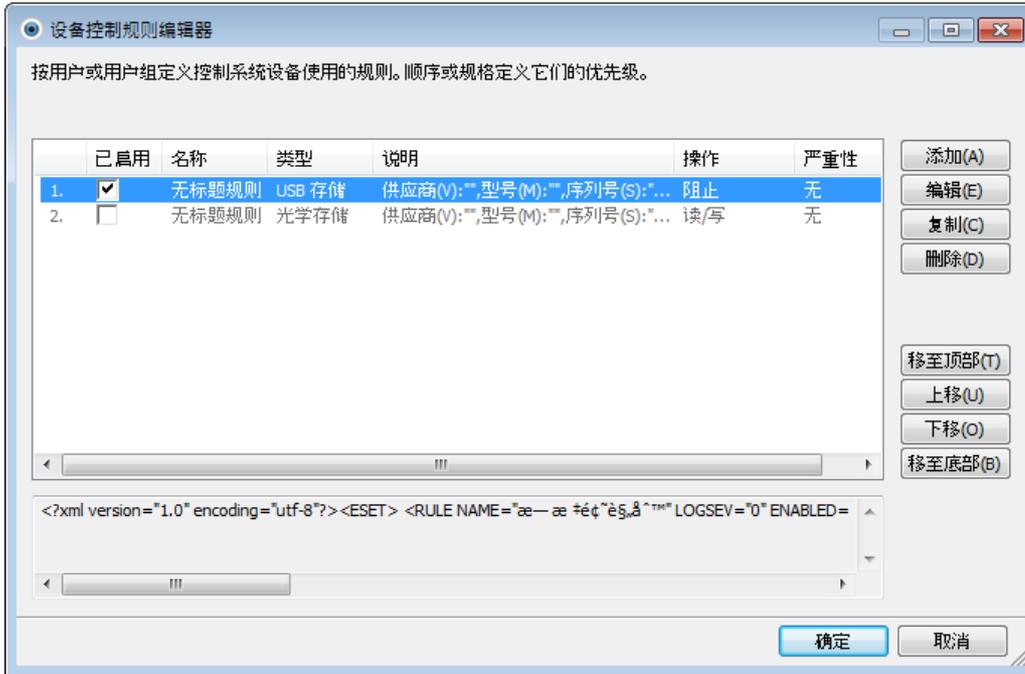
可以在高级设置 (F5) > 设备控制中修改设备控制设置选项。

选中集成到系统旁边的复选框可激活 ESET Endpoint Antivirus 中的 设备控制 功能；您需要重新启动计算机才能使此更改生效。一旦启用了 设备控制”，将激活配置规则...，可使您打开[设备控制规则编辑器](#)窗口。

如果插入的外部设备应用执行阻止操作的现有规则，将在右下角弹出通知窗口，并且不会授予对设备的访问权。

4.1.3.1 设备控制规则

设备控制规则编辑器窗口显示现有规则，允许精确控制用户连接到计算机的外部设备。



可以按照用户或用户组，根据规则配置中可指定的其他设备参数，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。

单击添加或编辑可管理规则。单击复制使用用于其他所选规则的预定义选项创建新规则。单击规则时显示的 XML 字符串可以复制到剪贴板以帮助系统管理员导出/导入这些数据并使用它们，例如在 ESET Remote Administrator 中。

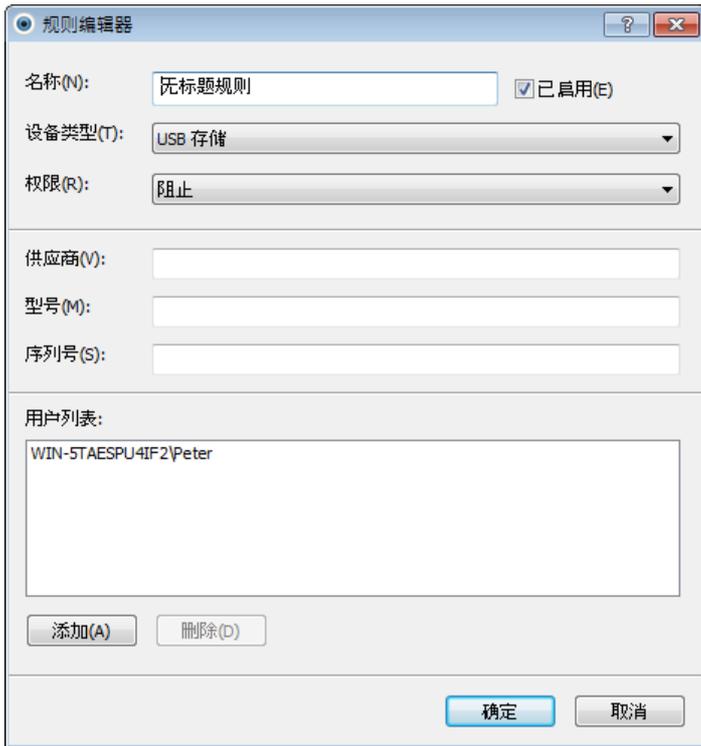
按住 CTRL 单击，可以选择多个规则和对所有所选规则应用操作，例如删除或上下移动列表。已启用复选框禁用或启用规则；当不希望永久删除规则以免未来可能要使用时，此功能有用。

控制通过规则实现，规则排序顺序决定其优先级，高优先级规则位于顶部。

您可以右键单击规则以显示右键菜单。您可以在这里设置规则的日志条目级别（严重性）。从 ESET Endpoint Antivirus 主窗口的工具 > [日志文件](#) 可以查看日志条目。

4.1.3.2 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。选中已启用旁的复选框将禁用或启用此规则；如果不希望永久删除规则，可以使用此功能。

设备类型

从下拉菜单中选择外部设备类型（USB/蓝牙/FireWire/...）。设备类型从操作系统继承，只要设备连接到计算机，就可在系统设备管理器中查看。下拉菜单中的可选存储设备类型指光学可读介质（如 CD、DVD）上的数据存储。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。成像设备示例包括扫描仪和照相机。智能卡读卡器包括具有嵌入式集成电路的智能卡读卡器，如 SIM 卡或身份验证卡。

权限

可以允许或阻止访问非存储设备。通过比较，存储设备规则允许选择以下权限之一：

- 阻止 - 将阻止对设备的访问。
- 只读 - 仅允许从设备读取。
- 读/写 - 将允许对设备的完全访问权。

注意，不是所有权限（操作）都可用于所有设备类型。如果设备具有存储空间，则所有三个操作可用。对于非存储设备，只有两个（例如只读操作对蓝牙不可用，因此这意味着只能允许或阻止设备）。

其他参数可用于微调规则并根据具体设备定制。所有参数区分大小写：

- 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，则这是给定介质的序列号，而不是 CD 驱动器。

注意：如果以上三个说明符为空白，匹配时规则将忽略这些字段。

提示：要找出设备参数，请创建相应设备类型允许的规则，将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。

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，该窗口可用于选择需要的用户。
- 删除 - 从过滤器删除选定用户。

4.1.4 基于主机的入侵预防系统 (HIPS)

基于主机的入侵预防系统 (HIPS) 可保护您的系统，以免恶意软件 and 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，而且不是防火墙；它仅监视在操作系统中运行的进程。

HIPS 可以在高级设置 (F5) 中找到，方法是单击计算机 > HIPS。HIPS 状态 (启用/禁用) 显示在 ESET Endpoint Antivirus 主窗口的设置窗格中，位于计算机部分的右侧。

HIPS 设置位于高级设置 (F5) 中。要在高级设置树中访问 HIPS，请单击计算机 > HIPS。HIPS 状态 (启用/禁用) 显示在 ESET Endpoint Antivirus 主窗口的设置窗格中，位于计算机部分的右侧。

警告： 对 HIPS 设置的更改仅应由有经验的用户进行。

ESET Endpoint Antivirus 具有内置的*自我保护*技术，可防止恶意软件损坏或禁用病毒和间谍软件防护，这样您可以确保系统随时受到保护。对启用 **HIPS** 和启用自我保护设置在 Windows 操作系统重新启动后生效。禁用整个 HIPS 系统也将需要计算机重新启动。

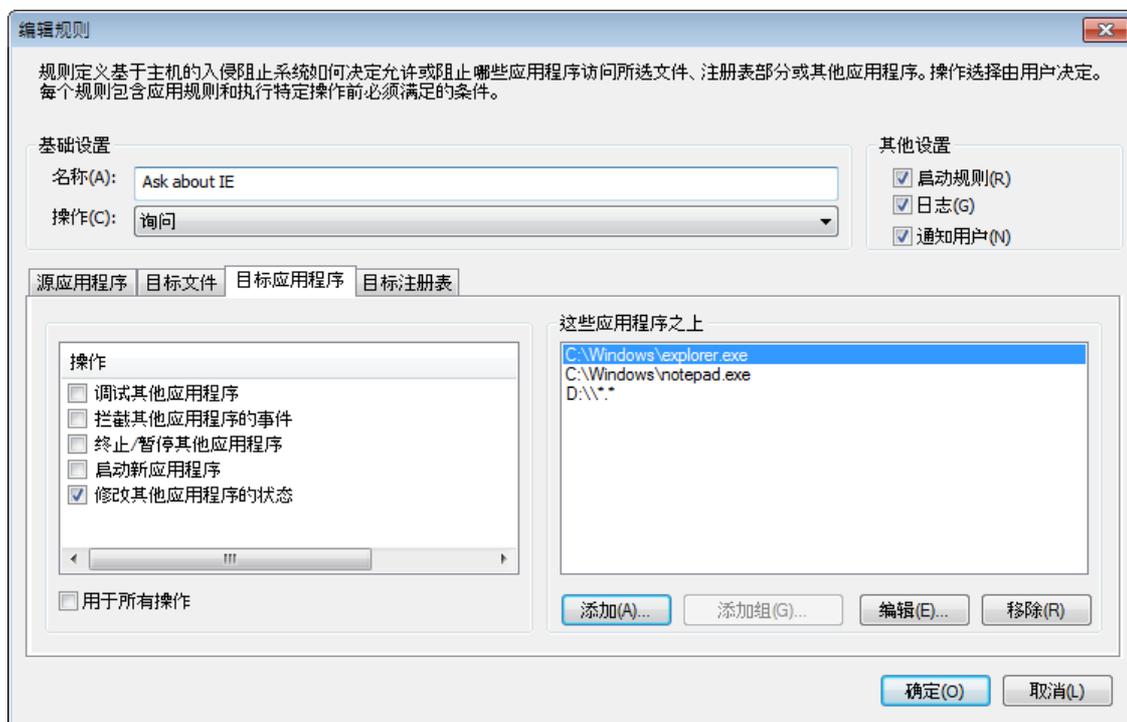
可以使用以下四种模式之一执行过滤：

- 带规则的自动模式 - 操作被启用，除了保护系统的预定义的规则。
- 交互模式 - 将提示用户确认操作。
- 基于策略的模式 - 操作被阻止。
- 学习模式 - 操作被启用，并在每次操作后创建规则。可在规则编辑器中查看以此模式创建的规则，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。在选择学习模式后，选项学习模式要在此时段过期时发送通知将变得可用。在该时段结束后，学习模式将再次被禁用。最长时段为 14 天。在此时段结束后，将打开一个弹出窗口，可在其中编辑规则并选择不同的过滤模式。

HIPS 系统监控操作系统内的事件，并根据类似于个人防火墙使用的规则相应地对事件作出反应。单击配置规则...可打开 HIPS 规则管理窗口。可在此窗口中选择、创建、编辑或删除规则。

在下面的示例中，我们将演示如何限制不需要的应用程序行为：

1. 命名规则，并从操作下拉菜单选择阻止。
2. 打开目标应用程序选项卡。保留源应用程序选项卡空白，对所有尝试对目标应用程序列表中的应用程序执行操作列表中任何选中操作的应用程序应用新规则。
3. 选择修改其他应用程序的状态（所有操作在产品帮助中介绍，在窗口中按 F1 键，和下面的图片相同）。
4. 添加要保护的一个或多个应用程序。
5. 启用通知用户选项以在应用规则时显示用户通知。
6. 单击确定保存新规则。



如果询问是默认操作，每次都显示对话框。它允许用户选择拒绝还是允许操作。如果用户在给定时间不选择操作，将基于规则选择新操作。



该对话框允许您基于 HIPS 检测到的任何新操作创建规则，然后定义在哪些条件下允许或拒绝该操作。通过单击显示选项，可以访问精确参数的设置。用这种方式创建的规则被认为等同于手动创建的规则，所以从对话框创建的规则可以比触发对话框的规则更具体。这意味着，在创建这样的规则后，相同的操作可以触发相同的窗口。

暂时对此进程记住此操作选项将导致使用该操作（允许/拒绝），直到更改了规则或过滤模式、更新了 HIPS 模块或重新启动了系统。在执行了这三项操作中的任意操作后，将删除临时规则。

4.2 Web 和电子邮件

在单击 **Web** 和电子邮件标题后，Web 和电子邮件配置显示在设置窗格中。可以从这里访问程序的更多详细设置。



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。出于此原因，务必仔细考虑Web 访问保护。

电子邮件客户端防护可控制通过 POP3 和 IMAP 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（POP3、MAPI、IMAP 和 HTTP）。

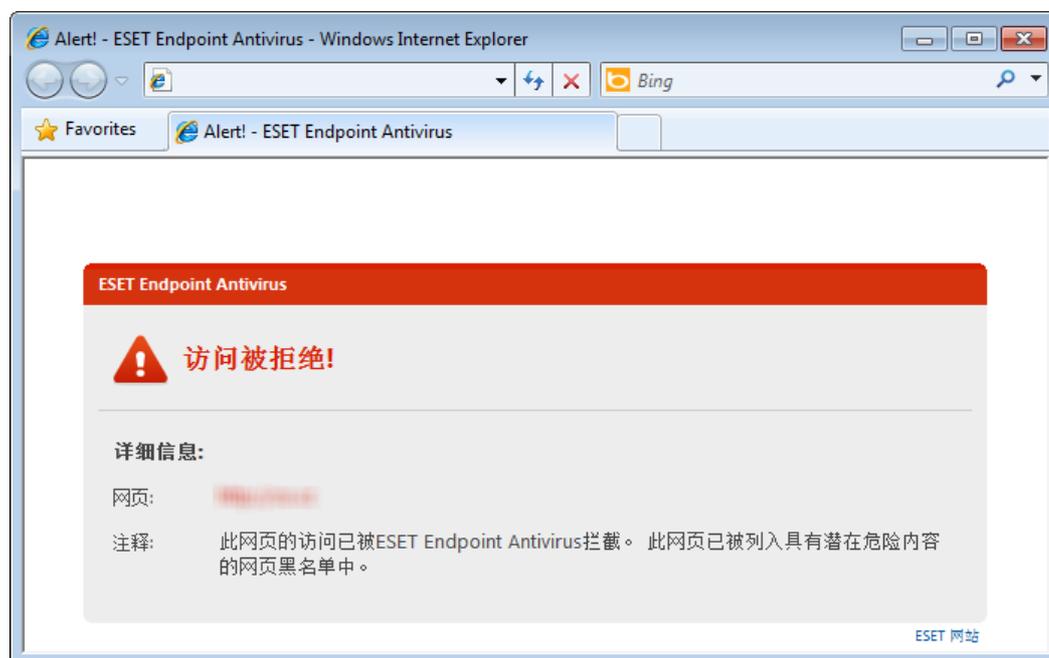
禁用 - 禁用电子邮件客户端的 Web/电子邮件 防护。

配置... - 打开 Web/电子邮件 防护高级设置。

4.2.1 Web 访问保护

Internet 连接是个人计算机的一项标准功能。不幸的是，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。

术语 欺诈 定义了一种利用社会工程学技术（为获得机密信息而操控用户）进行犯罪的行为。在[词汇表](#)中阅读此活动的更多信息。ESET Endpoint Antivirus 支持网络钓鱼防护 - 总是阻止具有此类内容的已知网页。



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 > **Web** 和电子邮件 > **Web 访问保护** 可以访问此选项。

4.2.1.1 HTTP, HTTPS

默认情况下，ESET Endpoint Antivirus 配置为使用大多数 Internet 浏览器的标准。然而，HTTP 扫描设置选项可在高级设置 (F5) > **Web** 和电子邮件 > **Web 访问保护** > HTTP, HTTPS 中修改。在主 **HTTP/HTTPS 扫描程序** 窗口中，您可以选择或取消选择启用 **HTTP 检查** 选项。您还可以定义 HTTP 通讯所使用的端口号。默认情况下，预定义端口号为 80 (HTTP)、8080 和 3128 (用于代理服务器)。

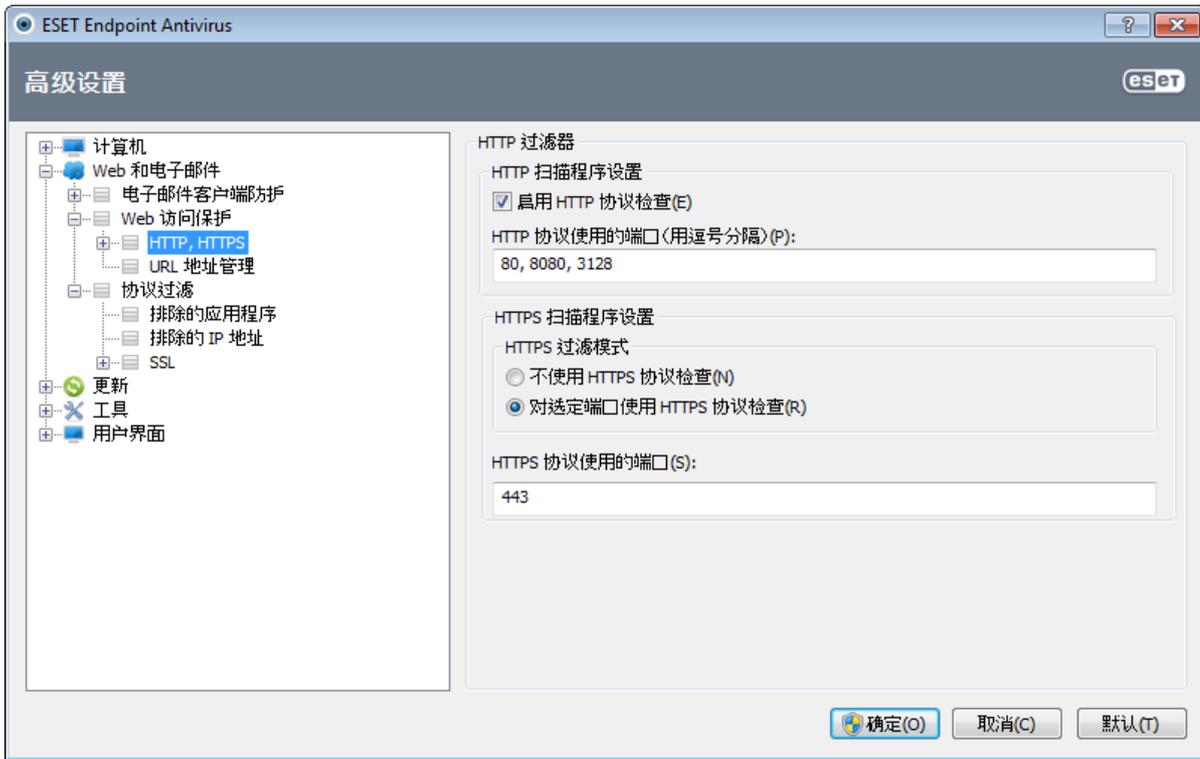
ESET Endpoint Antivirus 支持 HTTPS 协议检查。HTTPS 通信使用加密通道在服务器和客户端之间传输信息。ESET Endpoint Antivirus 利用 SSL (安全套接字层) 和 TLS (传输层安全) 加密方法检查通信。HTTPS 检查可以在下列模式下执行：

不使用 **HTTPS 协议检查** - 不检查加密通信。

对选定端口使用 **HTTPS 协议检查** - HTTPS 检查仅适用于 **HTTPS** 协议使用的端口

对选定端口使用 **HTTPS 协议检查** - 该程序将只检查在[浏览器](#)一节中指定的应用程序及使用 **HTTPS** 协议使用的端口中定义的端口的应用程序。默认端口设为 443。

加密的通信不会被扫描。要启用加密通信的扫描和查看扫描程序设置，请导航至高级设置部分的 [SSL 协议检查](#)，单击 **Web** 和电子邮件 > 协议过滤 > SSL，然后启用始终扫描 **SSL** 协议选项。



4.2.1.1.1 Web 浏览器主动模式

ESET Endpoint Antivirus 还包含主动模式子菜单，用于定义 Web 浏览器的检查模式。

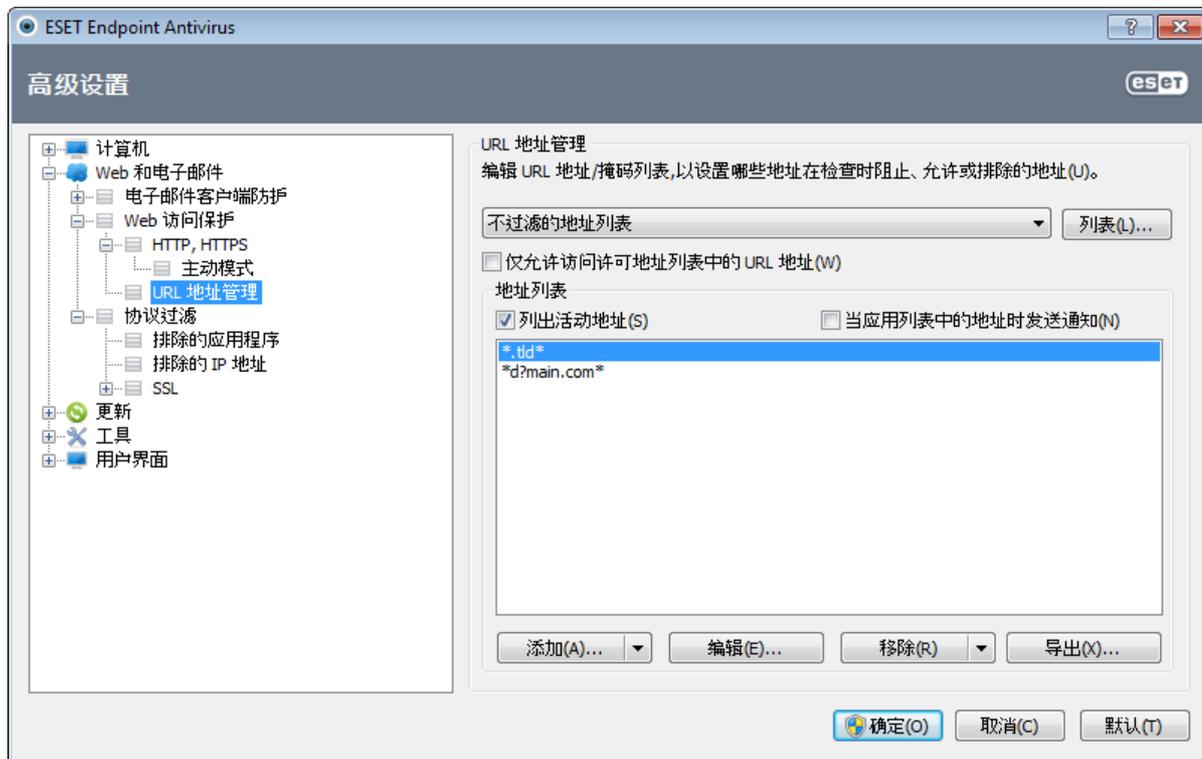
活动模式的有用之处在于它将传输的数据作为整体进行检查，无论它们是否被标记为 Web 浏览器（有关更多信息，请参见 [Web 和电子邮件客户端](#)）。如果未活动启用，则逐步按批监视应用程序的通信。这样会降低数据验证效率，但也为列出的应用程序提供了更高的兼容性。如果使用时未出现问题，建议您通过选中需要的应用程序旁边的复选框启用主动检查模式。主动模式的工作方式为：当受控的应用程序下载数据时，数据首先保存到由 ESET Endpoint Antivirus 创建的一个临时文件中。此时数据对给定应用程序不可用。一旦下载完成，即开始检查恶意代码。如果未发现渗透，则将数据发送给原来的应用程序。此过程能够完全控制受控应用程序的通信。如果启动了被动模式，数据被滴入原始应用程序以避免超时。

4.2.1.2 URL 地址管理

URL 地址管理部分可使您指定要对其阻止、允许或排除检查的 HTTP 地址。添加、编辑、删除和导出按钮可用于管理地址列表。将无法访问阻止地址列表中的网站。无需扫描恶意代码即可访问排除地址列表中的网站。如果您选中仅允许访问许可地址列表中的 URL 地址选项，则仅可以访问出现在允许地址列表中的地址，同时会阻止所有其他 HTTP 地址。

如果添加 URL 地址到不过滤的地址列表，该地址将从扫描中排除。您还可以通过添加它们到允许的地址列表或阻止的地址列表，允许或阻止某些地址。在单击列表...按钮后，将弹出 HTTP 地址/掩码列表窗口，可以在其中添加或删除地址列表。要将 HTTPS URL 地址添加到列表，必须启用总是扫描 [SSL 协议](#) 选项。

在所有列表中，您都可以使用特殊符号 *（星号）和 ?（问号）。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 ?。要启用某个列表，请选中列出活动选项。如果要在输入当前列表中的地址时获取系统通知，请选中当应用列表中的地址时发送通知。



添加.../来自文件 - 允许您将地址添加到该列表，可手动（添加），也可从简单文本文件（来自文件）添加。来自文件选项可使您添加文本文件中保存的多个 URL 地址/掩码。

编辑... - 手动编辑地址，例如以添加掩码的方式（“和？”）。

删除/全部删除 - 单击删除可删除列表中选定的地址。要删除全部地址，可选择全部删除。

导出... - 将当前列表中的地址保存至简单文本文件。

4.2.2 电子邮件客户端防护

电子邮件防护可控制通过 POP3 和 IMAP 协议接收的电子邮件通信。通过使用 Microsoft Outlook 和其他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（POP3、MAPI、IMAP 和 HTTP）。检查传入邮件时，程序使用 ThreatSense 扫描引擎提供的所有高级扫描方法。这意味着恶意程序检测在与病毒库匹配之前就已进行。对 POP3 和 IMAP 协议通信的扫描与使用何种电子邮件客户端无关。

此功能的选项可通过高级设置 > **Web 和电子邮件** > 电子邮件客户端防护使用。

ThreatSense 引擎参数设置 - 高级病毒扫描程序设置使您能够配置扫描目标、检测方法等。单击设置...可显示详细的病毒扫描程序设置窗口。

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以及在已发送电子邮件上添加标记信息。标记消息未必可靠，因为它有可能被有问题的 HTML 邮件省略，而有些病毒也会伪造标记消息。可将标记消息添加到已接收/已阅读的电子邮件、已发送的电子邮件中或两类邮件中都添加。可用选项包括：

- 从不 - 不添加任何标记信息。
- 仅对被感染的电子邮件 - 仅将包含恶意软件的邮件标记为已选中（默认）。
- 对所有扫描的电子邮件 - 程序将把消息附加到所有已扫描的电子邮件上。

在已接收并阅读/发送的被感染电子邮件主题中添加注释 - 如果要在被感染的电子邮件主题中包含病毒警告，则选中此复选框。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的威胁级别的有价值信息。

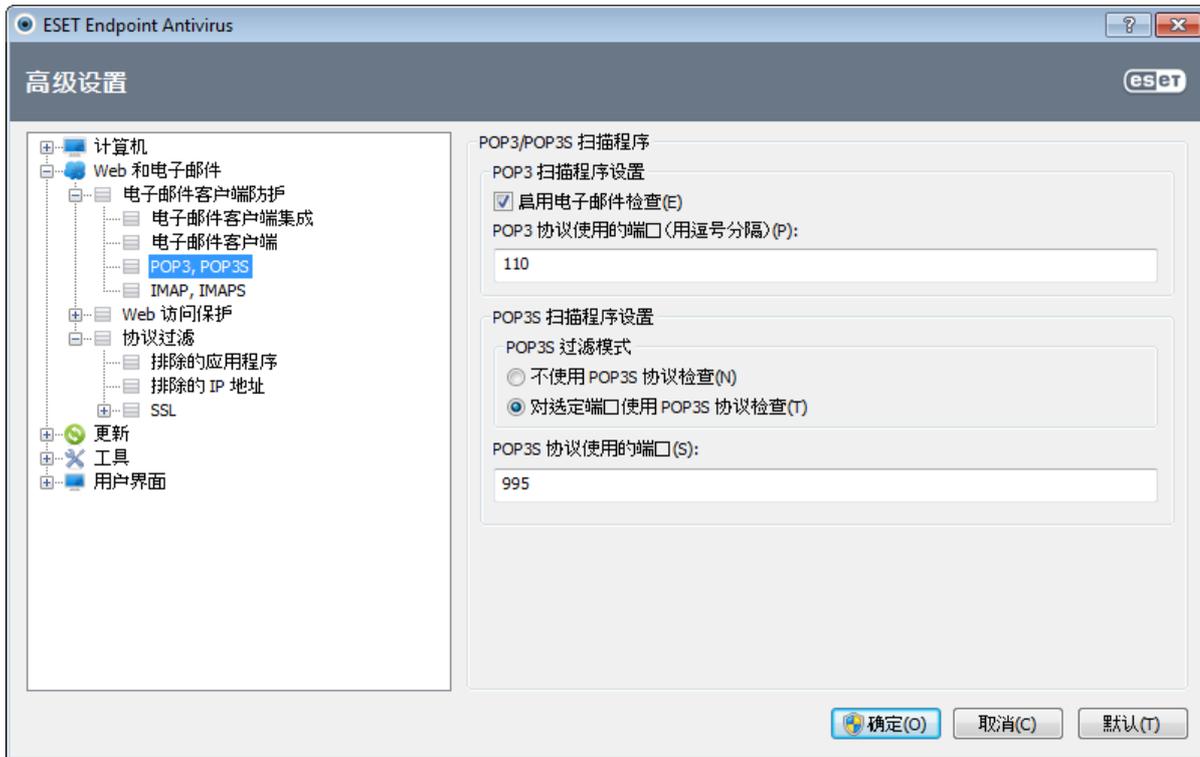
添加到被感染电子邮件主题中的模板 - 如果您希望修改被感染电子邮件的主题前缀格式，则编辑此模板。此功能将替换邮件主题 "Hello" 为以下格式的给定前缀值 "[virus]" : "[virus] Hello"。变量 %VIRUSNAME% 代表被感染的威胁。

4.2.2.1 POP3 ,POP3S 过滤器

POP3 协议是使用最广泛的在电子邮件客户端应用程序中接收电子邮件通信的协议。无论使用何种电子邮件客户端，ESET Endpoint Antivirus 均提供对此协议的保护。

系统启动时会自动启动提供此控件的防护模块，之后该模块会在内存中处于活动状态。要使模块正常工作，请确保已启用它 - POP3 协议检查会自动执行，无需重新配置电子邮件客户端。默认情况下，程序会扫描端口 110 上的所有通信，如有必要，也可以添加其他通信端口。多个端口号必须使用逗号分隔。

加密的通信不会被扫描。要启用加密通信的扫描和查看扫描程序设置，请导航至高级设置部分的 [SSL 协议检查](#)，单击 Web 和电子邮件 > 协议过滤 > SSL，然后启用始终扫描 **SSL** 协议选项。



在本节中您可以配置 POP3 和 POP3S 协议检查。

启用 POP3 协议检查 - 如果启用该选项，则将监视所有通过 POP3 进行的通信以查找恶意软件。

POP3 协议使用的端口 - POP3 协议使用的端口（默认为 110）的列表。

ESET Endpoint Antivirus 也支持 POP3S 协议检查。此类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）加密方法检查通信。

不使用 POP3S 检查 - 不检查加密通信。

对选定端口使用 POP3S 协议检查 - 选中此选项可仅对在 **POP3S** 协议使用的端口中定义的端口启用 POP3S 检查。

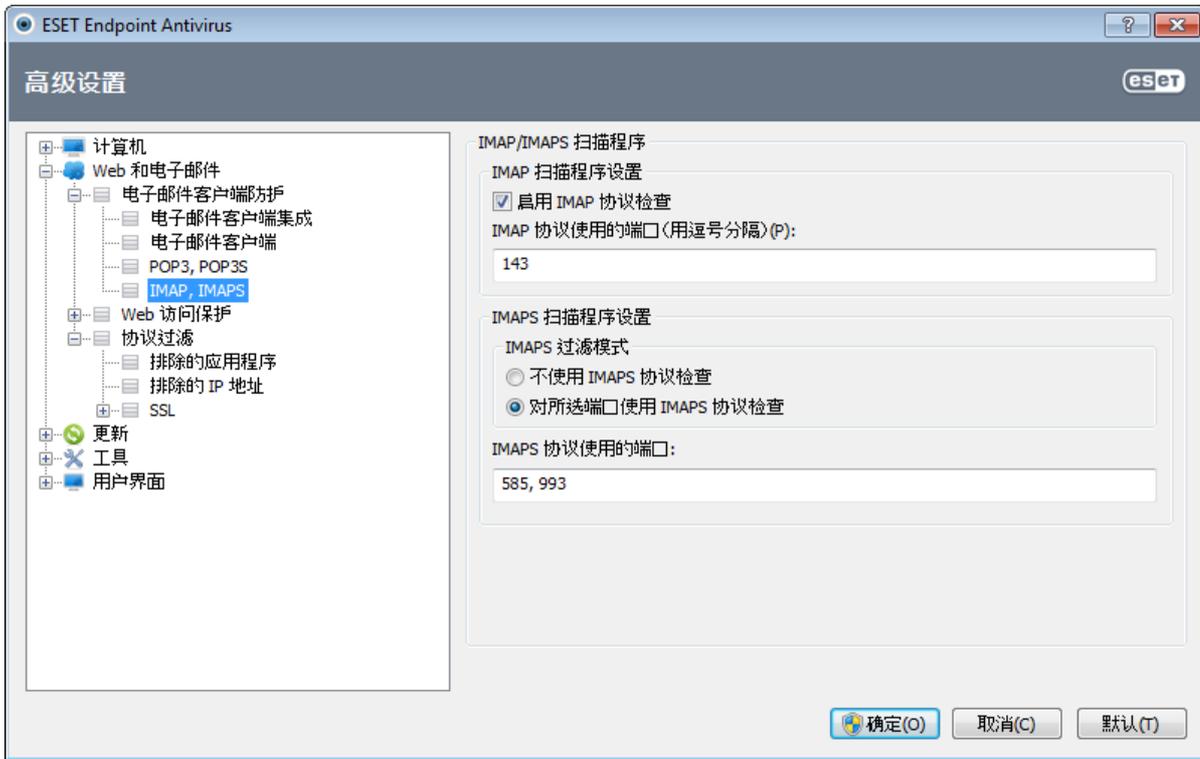
POP3S 协议使用的端口 - 要检查的 POP3S 端口（默认为 995）的列表。

4.2.2.2 IMAP ,IMAPS 协议控制

Internet 消息访问控制 (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，比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，如邮件是否已读、已回复或已删除。ESET Endpoint Antivirus 为此协议提供保护，无论使用哪种电子邮件客户端。

系统启动时会自动启动提供此控件的防护模块，之后该模块会在内存中处于活动状态。要使模块正常工作，请确保已启用它；IMAP 协议控制会自动执行，无需重新配置电子邮件客户端。默认情况下，程序会扫描端口 143 上的所有通信，如有必要，也可以添加其他通信端口。多个端口号必须使用逗号分隔。

加密的通信不会被扫描。要启用加密通信的扫描和查看扫描程序设置，请导航至高级设置部分的 [SSL 协议检查](#)，单击 Web 和电子邮件 > 协议过滤 > SSL，然后启用始终扫描 **SSL** 协议选项。

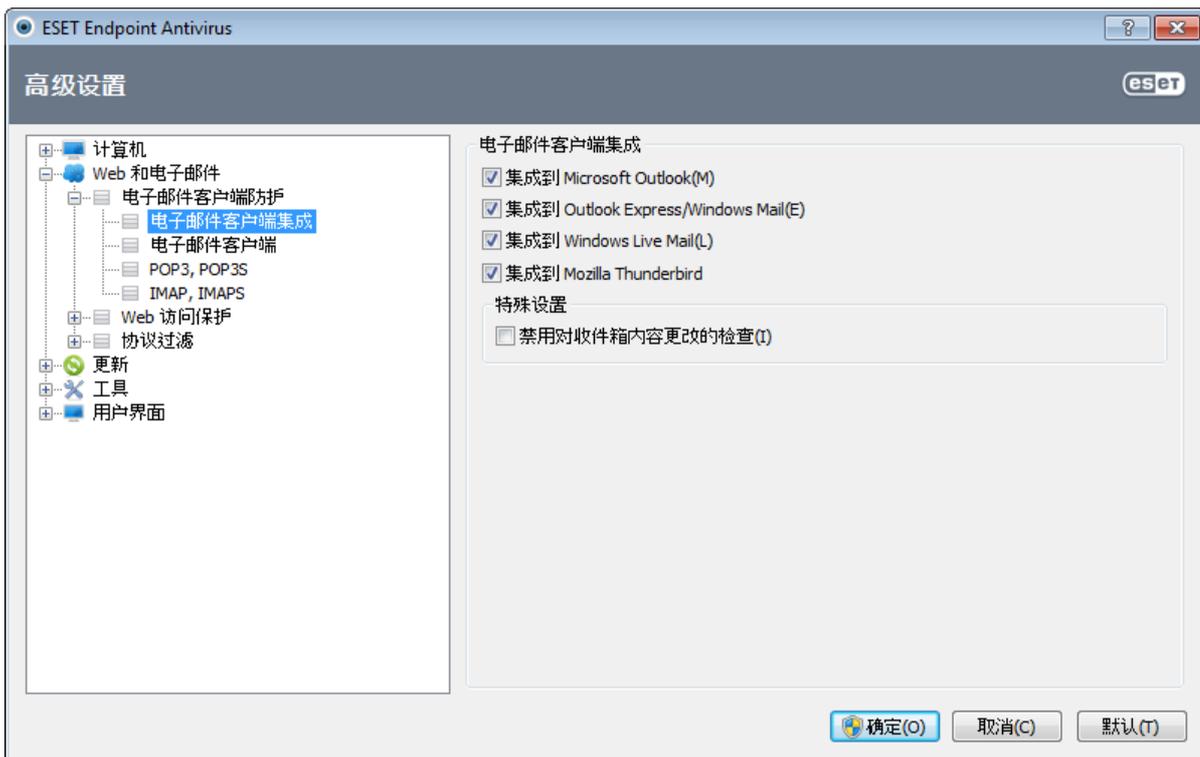


4.2.2.3 电子邮件客户端集成

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 中启用此集成。如果启用了集成，ESET Endpoint Antivirus 工具栏将被直接插入到电子邮件客户端，从而提供更高效率的电子邮件防护。通过设置 > 进入高级设置... > **Web 和电子邮件** > 电子邮件客户端保护 > 电子邮件客户端集成可以访问集成设置。

当前受支持的电子邮件客户端包括 Microsoft Outlook、Outlook Express、Windows Mail、Windows Live Mail 和 Mozilla Thunderbird。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。

如果使用电子邮件客户端时遇到系统运行缓慢的情况，请选中禁用对收件箱内容更改的检查旁的复选框。当从 Kerio Outlook Connector Store 中下载电子邮件时可能会发生这种情况。



即使未启用集成，电子邮件通信仍受电子邮件客户端防护模块（POP3、IMAP）保护。

4.2.2.3.1 电子邮件客户端防护配置

电子邮件客户端保护模块支持下列电子邮件客户端：Microsoft Outlook、Outlook Express、Windows Mail、Windows Live Mail 和 Mozilla Thunderbird。电子邮件保护的工作方式和这些程序的插件相同。插件控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，邮件会被解密并发送给病毒扫描程序。

要扫描的电子邮件

已接收的电子邮件 - 切换到检查已接收到的邮件。

已发送的电子邮件 - 切换到检查已发送的邮件。

已阅读的电子邮件 - 切换到检查已阅读的邮件。

对被感染的电子邮件执行的操作

不操作 - 如果启用，则程序虽能识别被感染的附件，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文件夹 - 被感染的电子邮件将被自动移至已删除文件夹。

将电子邮件移至文件夹 - 指定希望将检测到的被感染电子邮件移动到自定义文件夹。

其他

更新后重新扫描 - 在病毒库更新后切换到重新扫描。

接受其他模块的扫描结果 - 如果选中此选项，电子邮件保护模块会接受其他保护模块的扫描结果。

4.2.2.4 删除渗透

如果收到被感染的电子邮件，将显示警报窗口。警报窗口显示发件人姓名、电子邮件和渗透的名称。在窗口的下半部分，提供了清除、删除或保留选项以用于检测的对象。在几乎所有情况下，我们建议您选择清除或删除。在某些情况下，如果希望接收被感染文件，则选择保留。如果启用严格清除，将显示一个信息窗口，其中没有提供对被感染对象可用的选项。

4.2.3 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，该控件都会自动工作。有关加密的 (SSL) 通信，请参见协议过滤 > SSL。

集成到系统 - 允许 ESET Endpoint Antivirus 协议过滤功能的驱动程序。

启用应用程序协议内容过滤 - 如果启用，所有 HTTP(S)、POP3(S) 和 IMAP(S) 通信都会由病毒防护扫描程序检查。

注意：从 Windows Vista Service Pack 1 和 Windows 7 开始，使用新的 Windows 过滤平台 (WFP) 架构检查网络通信。由于 WFP 技术使用了特殊的监视技术，所以以下选项不可用：

- **HTTP 和 POP3 端口** - 仅将 HTTP 和 POP3 端口上的通信路由至内部代理服务器。
- 标记为 **Web 浏览器** 和电子邮件客户端的应用程序 - 仅将标记为浏览器和电子邮件客户端的应用程序发生的通信路由至内部代理服务器 (**Web 和电子邮件** > 协议过滤 > **Web 和电子邮件客户端**)。
- 标记为 **Web 浏览器** 或电子邮件客户端的端口和应用程序 - 将 HTTP 和 POP3 端口上发生的所有通信，以及标记为浏览器和电子邮件客户端的应用程序上发生的所有通信路由至内部代理服务器。

4.2.3.1 Web 和电子邮件客户端

注意：从 Windows Vista Service Pack 1 和 Windows 7 开始，使用新的 Windows 过滤平台 (WFP) 架构检查网络通信。由于 WFP 技术使用了特殊的监视技术，所以 **Web 和电子邮件客户端** 部分不可用。

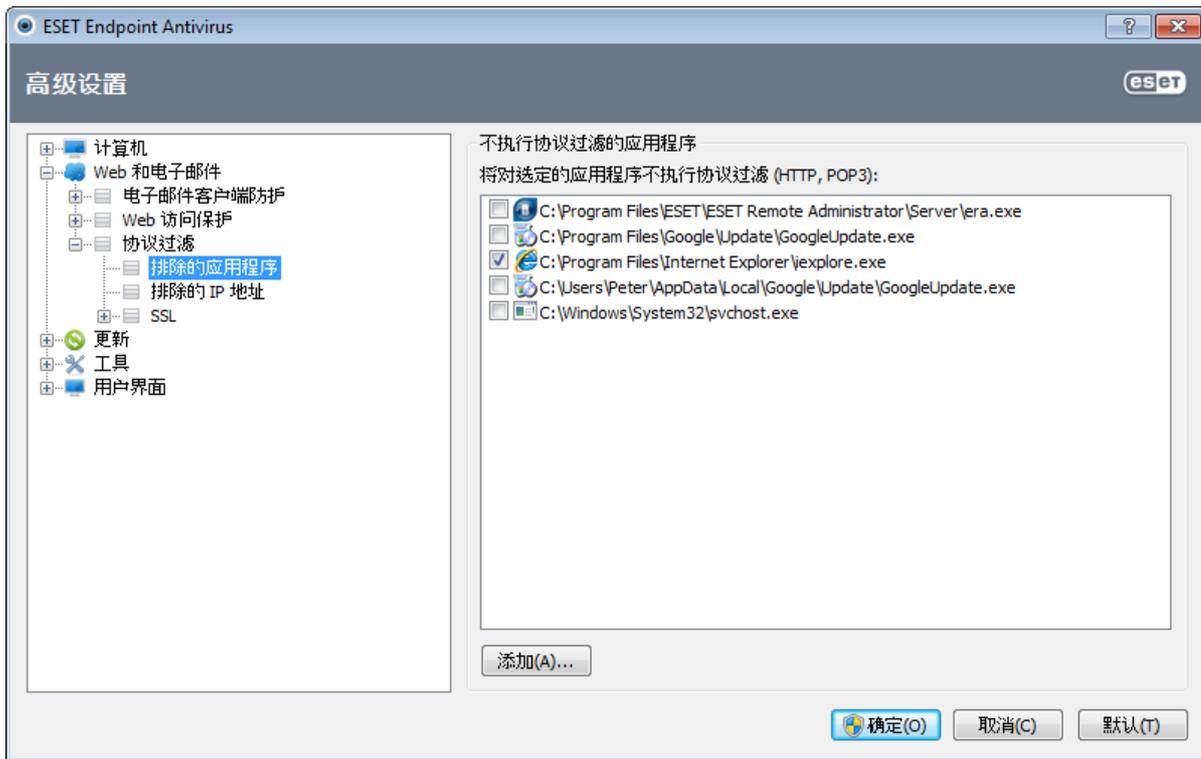
由于 Internet 上充斥着大量恶意代码，安全浏览 Internet 就成了计算机保护的一个非常重要的方面。Web 浏览器的漏洞和欺骗链接能够帮助恶意代码进入系统且不会引起注意，这也是 ESET Endpoint Antivirus 注重 Web 浏览器安全性的原因所在。访问网络的每个应用程序都可以标记为 Internet 浏览器。复选框为以下两种状态：

- 未选 - 仅过滤指定端口的应用程序通信。
- 已选 - 始终过滤通信（即使设置了其他端口）。

4.2.3.2 排除的应用程序

要将特定网络感知应用程序的通信排除在内容过滤之外，请在列表中选择它们。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，仅当应用程序无法正常工作而需要检查其通信时才使用此选项。

将在这里自动显示正在运行的应用程序和服务。单击添加...按钮手动选择未显示在协议过滤列表上的应用程序。

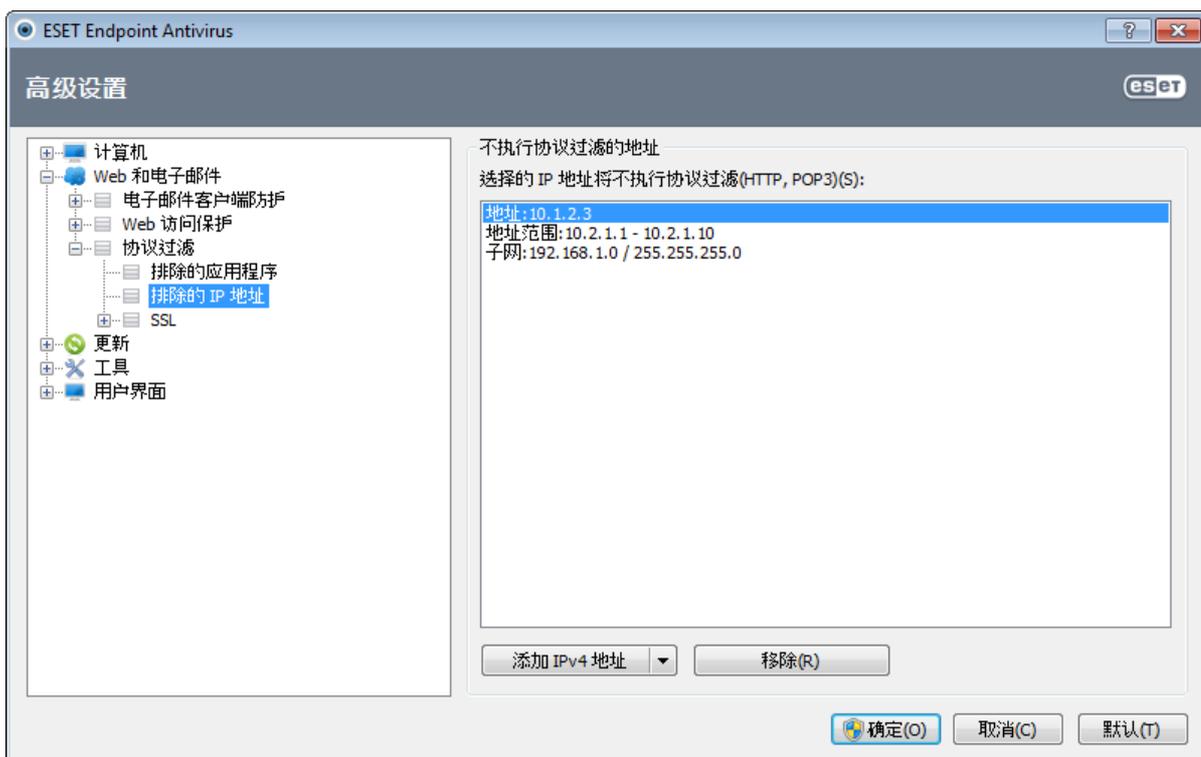


4.2.3.3 排除的 IP 地址

地址列表中的条目将被自动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 IPv4/IPv6 地址 - 此选项可让您添加将应用规则的远程点的 IP 地址/地址范围/子网。

删除 - 删除列表中的选定条目。



4.2.3.3.1 添加 IPv4 地址

通过该选项，您可以为要应用规则的远程点添加 IP 地址/地址范围/子网。Internet 协议版本 4 是旧版本，但仍是使用范围最广泛的版本。

单个地址 - 添加将应用规则的单台计算机的 IP 地址，（例如 192.168.0.10）。

地址范围 - 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（例如 192.168.0.1 至 192.168.0.99）。

子网 - 子网（一组计算机）由 IP 地址和掩码定义。

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。

4.2.3.3.2 添加 IPv6 地址

通过该选项，您可以为要应用规则的远程点添加 IPv6 地址/子网。这是最新版本的 Internet 协议，将代替旧的版本 4。

单个地址 - 添加将应用规则的单台计算机的 IP 地址，（例如 2001:718:1c01:16:214:22ff:fec9:ca5）。

子网 - 子网（一组计算机）由 IP 地址和掩码定义（例如：2002:c0a8:6301:1::1/64）。

4.2.3.4 SSL 协议检查

ESET Endpoint Antivirus 使您能够检查 SSL 协议中封装的协议。使用受信任的证书、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受 SSL 保护的通信。

始终扫描 SSL 协议 - 选择此选项来扫描所有受 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您标记为受信任（添加到受信任的证书列表）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。

询问未访问过的站点（可以设置排除列表） - 如果您输入受 SSL 保护的新站点（具有未知证书），将显示一个操作选择对话框。此模式可用于创建将不扫描的 SSL 证书列表。

不扫描 SSL 协议 - 如果选中此选项，则程序将不扫描通过 SSL 的通信。

应用基于证书创建的异常 - 使用排除和信任的证书中指定的排除列表启动，以扫描 SSL 通信。要使此选项可用，可以选择总是扫描 SSL 协议。

阻止使用通过 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。

4.2.3.4.1 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, spol s r.o. 根证书添加到已知根证书（发布者）的列表中。因此，应启用将根证书添加到已知浏览器选项。选中此选项可自动将 ESET 根证书添加到已知浏览器（如 Opera、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。如果选择了询问证书的有效性选项（默认），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选项，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。

4.2.3.4.1.1 信任的证书

除了集成的受信任的根证书颁发机构（ESET Endpoint Antivirus 存储信任的证书的位置），您还可以创建信任的证书的自定义列表，该列表可以在高级设置 (F5) > **Web** 和电子邮件 > 协议过滤 > SSL > 证书 > 信任的证书中查看。ESET Endpoint Antivirus 将使用此列表中的证书来检查加密通信的内容。

要从列表中删除选定项目，请单击删除按钮。单击显示选项（或双击证书）可显示有关选定证书的信息。

4.2.3.4.1.2 排除的证书

排除的证书部分包含被认为安全的证书。使用此列表中证书的加密通信的内容将不会被检查是否存在威胁。建议仅排除保证安全的 Web 证书和使用不需要检查的证书的通信。要从列表中删除选定项目，请单击删除按钮。单击显示选项（或双击证书）可显示有关选定证书的信息。

4.2.3.4.1.3 加密的 SSL 通信

如果计算机配置为 SSL 协议扫描，则在尝试建立加密的通信（使用未知证书）时，将打开一个对话框，提示您选择操作。该对话框包括以下信息：发起通信的应用程序的名称和所用证书的名称。



如果信任的根证书颁发机构中没有该证书，会将其视为不受信任。



可对证书执行下列操作：

是 - 该证书将暂时被标记为受当前会话信任 - 下次尝试使用该证书时将不会显示警报窗口。

是，总是信任 - 将该证书标记为受信任，并将其添加到受信任证书的列表 - 不会显示受信任证书的任何警报窗口。

否 - 将该证书标记为不受当前会话信任 - 下次尝试使用该证书时将会显示警报窗口。

排除 - 将该证书添加到排除证书的列表 - 完全不会检查通过给定加密通道传输的数据。

4.3 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，即更新病毒库和更新系统组件。

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。主窗口还包含病毒库版本。此数值指示是指向 ESET 网站的活动链接，其中列有在给定更新内添加的所有病毒库。

此外，还提供手动开始更新过程的选项更新病毒库。更新病毒库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（用户名和密码），可以在更新时输入用户名和密码以访问 ESET 更新服务器。

注意: 在购买 ESET Endpoint Antivirus 之后，ESET 会为您提供用户名和密码。



上次成功更新 - 最近一次更新的日期。确保是最近的日期，表明病毒库是最新的。

病毒库版本 - 病毒库编号，它也是指向 ESET 网站的活跃链接。单击可以查看给定更新中添加的所有特征码列表。

更新过程

单击更新病毒库后，即开始下载过程。屏幕上会显示下载进度条和剩余时间。要中断更新，请单击中止。



重要信息：一般情况下，如果更新正常下载，消息无需进行更新 - 所安装的病毒库为当前版本将显示在更新窗口中。如果不是这样，则表示程序不是最新的，且更容易被感染。请尽快更新病毒库。否则，会显示下列消息之一：

病毒库已过期 - 此错误将在几次尝试更新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](#)。

以前的通知与下列有关不成功更新的两条病毒库更新失败消息相关：

1. 用户名和/或密码无效 - 更新设置中输入了错误的用户名和密码。建议您检查[验证数据](#)。高级设置 窗口（从主菜单中单击设置，然后单击进入高级设置...，或按键盘上的 F5 键）包含其他更新选项。在高级设置 树中单击更新 >常规 以输入新用户名和密码。



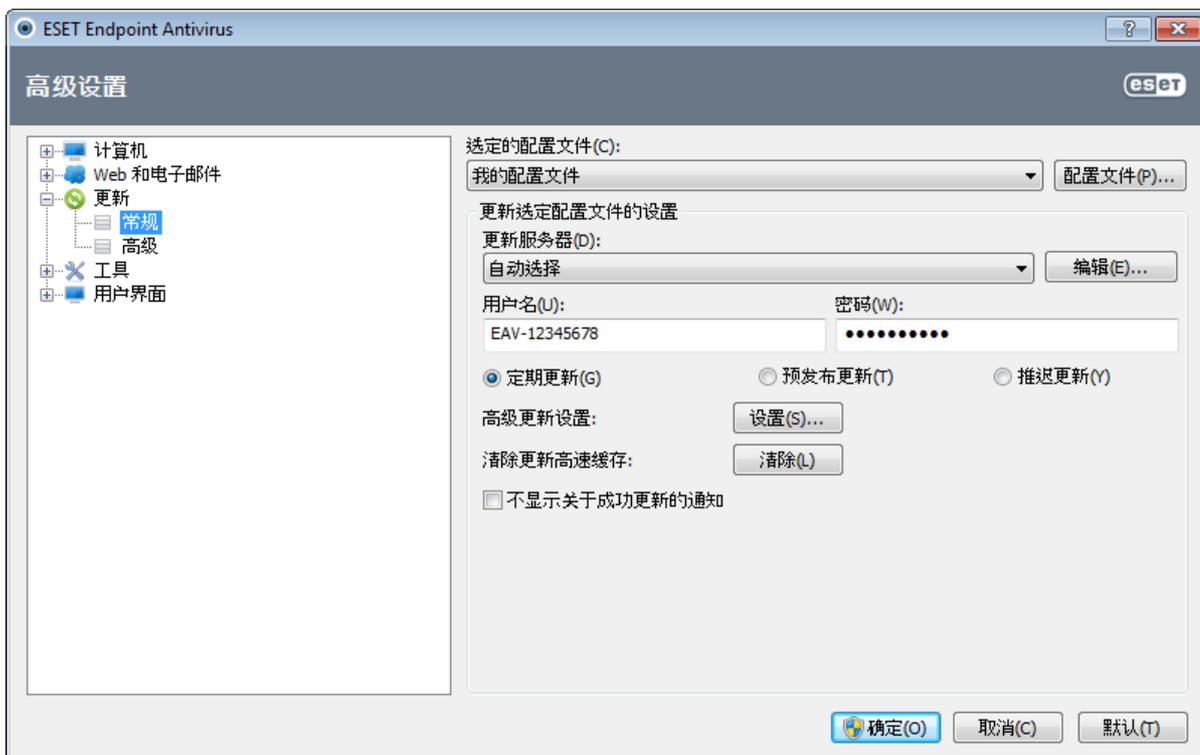
2. 下载更新文件时出错 - 此错误的原因可能是 [Internet 连接设置](#)。建议您检查 Internet 连接（方法是在 Web 浏览器中打开任意网站）。如果网站不打开，很可能未建立 Internet 连接，或者计算机存在连接问题。请与 Internet 服务提供商 (ISP) 联系以确定您是否有活跃 Internet 连接。



4.3.1 更新设置

在高级设置树（按 F5 键）中单击更新 > 常规，可以访问更新设置选项。该部分指定更新源信息，例如更新服务器和这些服务器的验证信息。默认情况下，更新服务器下拉菜单设置为自动选择，以确保更新文件将以最小的网络流量从 ESET 服务器自动下载。

为使更新正常下载，必须正确填写所有参数。如果使用防火墙，请确保程序能与 Internet 通信（即 HTTP 通信）。



当前使用的更新配置文件显示在选定的配置文件下拉菜单中。单击配置文件...可创建新的配置文件。

可用更新服务器列表可通过更新服务器下拉菜单访问。更新服务器是存储更新的地方。如果使用 ESET 服务器，请保持选中

默认选项自动选择。若要添加新更新服务器，请单击更新选定配置文件的设置部分中的编辑...，然后单击添加按钮。

使用本地 HTTP 服务器（也称为 镜像）时，更新服务器应如下设置：

http://computer_name_or_its_IP_address:2221

使用启用 SSL 的本地 HTTP 服务器时，更新服务器应如下设置：

https://computer_name_or_its_IP_address:2221

更新服务器的验证基于用户名和密码，该信息在您购买之后生成并发送给您。使用本地镜像服务器时，则根据其配置进行验证。默认情况下无需进行验证，即用户名和密码字段留空。

预发布更新（预发布更新选项）已经经过内部彻底测试，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。当前模块的列表可在帮助和支持 > 关于 **ESET Endpoint Antivirus** 中找到。建议基础用户将定期更新选项保留为默认选中状态。商业用户可以选择延迟更新选项，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因此视为稳定的数据库。

单击高级更新设置旁边的设置...按钮，显示包含高级更新选项的窗口。

如果更新时出现问题，请单击清除...按钮，以清理具有临时更新文件的文件夹。

不显示关于成功更新的通知 - 关闭屏幕右下角的系统托盘通知。如果正在运行全屏应用程序或游戏，选择此选项很有用。请注意，[演示模式](#)将关闭所有通知。

4.3.1.1 更新配置文件

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尤其有用，这些用户可以创建备用配置文件用于定期更改的 Internet 连接属性。

选定的配置文件下拉菜单显示当前选定的配置文件，默认情况下设置为我的配置文件。若要创建新配置文件，请单击配置文件...按钮，然后单击添加...按钮并输入您自己的配置文件名称。当创建新配置文件时，可以从现有配置文件中复制设置，方法是在从以下配置文件中复制设置下拉菜单中选择现有配置文件。

在配置文件设置窗口中，可以从可用服务器列表中指定更新服务器或添加新服务器。现有更新服务器列表列在更新服务器下拉菜单中。若要添加新更新服务器，请单击更新选定配置文件的设置部分中的编辑...，然后单击添加按钮。

4.3.1.2 高级更新设置

要查看高级更新设置，请单击设置...按钮。高级更新设置选项包括更新模式、HTTP代理？，LAN 和镜像。

4.3.1.2.1 更新模式

更新模式选项卡包含关于程序组件更新的选项。此程序使您能够预定义在有新的程序组件升级时执行何种操作。

程序组件更新会增加新的功能，或对以前版本中已存在的功能进行更改。更新无需用户介入即可自动执行，您也可以选择执行时收取通知。程序组件更新安装完毕后，可能需要重新启动。在程序组件更新部分中，提供以下三个选项：

- 从不更新程序组件 - 不执行程序组件更新。该选项适用于服务器安装，因为服务器通常只在进行维护时才重新启动。
- 总是更新程序组件 - 将自动下载并安装程序组件更新。请记住，计算机可能需要重新启动。
- 下载程序组件前询问 - 这是默认选项。当更新可用时，将提示您确认或拒绝程序组件更新。

程序组件更新后，可能需要重新启动计算机才能提供所有模块的全部功能。程序组件升级后重新启动部分允许您从以下选项选择一个：

- 从不重新启动计算机 - 将不要求您重新启动，即使需要重新启动。请注意，这不是我们建议的操作，因为计算机可能仅在下次重新启动后才能正常工作。
- 需要时重新启动计算机 - 默认选项。程序组件更新后，将有一个对话框提示您重新启动计算机。
- 需要时不通知即重新启动计算机 - 程序组件升级后，计算机将重新启动（如果需要）。

注意：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，例如程序升级后自动重新启动服务器可能会造成严重损害。

如果选中了下载更新前先询问选项，在新更新可用时将显示通知。

如果更新文件大小大于询问的前提是更新文件大于字段中指定的值，程序将显示通知。

4.3.1.2.2 代理服务器

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**，然后单击高级更新设置右侧的 **设置...** 按钮。单击 **HTTP 代理** 选项卡并选择以下三个选项之一：

- 使用全局代理服务器设置
- 不使用代理服务器
- 通过代理服务器连接

选择使用全局代理服务器设置选项将使用 **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选项可指定不使用代理服务器来更新 ESET Endpoint Antivirus。

以下情况下应使用通过代理服务器连接选项：

- 应使用代理服务器来更新 ESET Endpoint Antivirus，同时与全局设置（**工具 > 代理服务器**）中指定的代理服务器不同。如果是这种情况，应在此处指定设置：代理服务器地址、通信端口，再加上代理服务器的用户名和密码（如果需要）。
- 代理服务器设置未全局设置，但是 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，如果之后设置发生更改（比如更换了 Internet 服务提供商），请在此窗口中检查 HTTP 代理设置是否正确。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。

注意： 用户名和密码等验证数据用于访问代理服务器。仅当需要用户名和密码时才填写这些字段。请注意，这些字段中不能填写 ESET Endpoint Antivirus 的用户名/密码，仅当您知道通过代理服务器访问 Internet 需要填写密码时才提供这些信息。

4.3.1.2.3 连接到 LAN

从运行 NT 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。在大部分情况下，本地系统帐户对于镜像文件夹（镜像文件夹包含更新文件的副本）没有足够访问权。如果是这种情况，请在更新设置部分中输入用户名和密码，或指定程序将在哪个现有帐户下访问更新服务器（镜像）。

要配置这样的帐户，请单击 LAN 选项卡。连接到 **LAN** 作为部分提供系统帐户（默认）、当前用户和指定用户选项。

选择系统帐户（默认）选项，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。

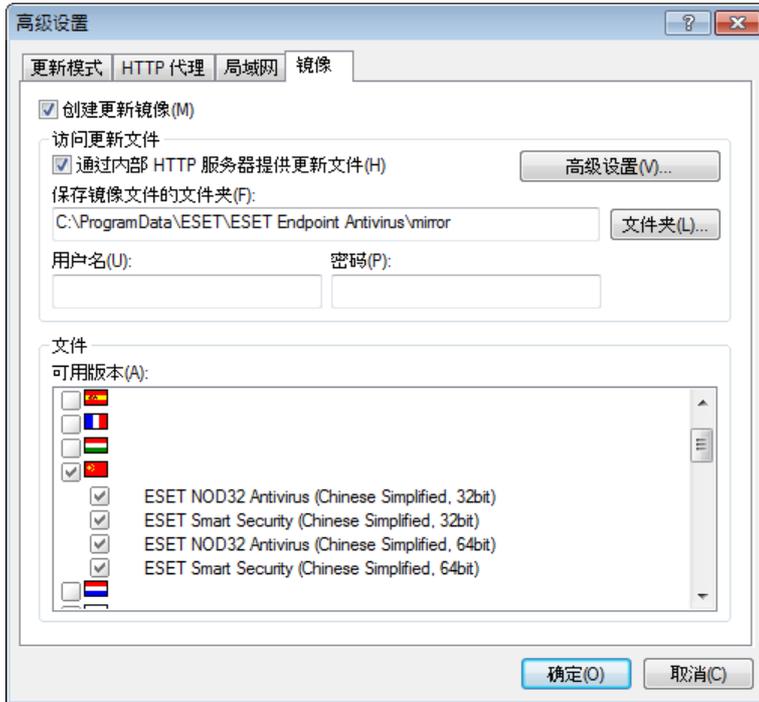
警告： 选择当前用户或指定用户后，如果将程序身份更改为所需用户，可能发生错误。我们建议在主更新设置部分中输入 LAN 验证数据。在此更新设置部分中，应按如下所示输入验证数据：domain_name\user（如果是工作组，请输入 workgroup_name\name）和密码。从本地服务器的 HTTP 版本更新时，无需验证。

如果更新下载后与服务器的连接仍然保持活动状态，则选择更新后断开与服务器的连接选项。

4.3.1.2.4 创建更新副本 - 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。创建“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从厂商更新服务器反复下载，也不需要每台工作站都下载。可将其集中下载到本地镜像服务器，然后分发给所有工作站，由此避免了潜在的网络流量过载风险。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。

本地镜像服务器的配置选项可从高级更新设置部分访问（在 ESET Endpoint Antivirus 的高级设置部分的[许可证管理器](#)中添加有效许可密钥之后）。要访问此部分，按 F5 键并单击高级设置 树中的更新，然后单击设置... 按钮（在高级更新设置的旁边）并选择镜像选项卡。



配置镜像的第一步是选择创建更新镜像选项。选择此选项将启用其他镜像配置选项，例如访问更新文件的方式和镜像文件的更新路径。

通过内部 HTTP 服务器提供更新文件 - 如果启用，通过 HTTP 即可方便地访问更新文件，无需用户名和密码。单击[高级设置...](#)来配置扩展镜像选项。

注意：在 Windows XP 上，HTTP 服务器要求 SP2 及更高版本。

在[从镜像更新](#)部分中，详细描述了镜像启动的方法。请注意，目前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 HTTP 服务器。

用于为镜像存储更新文件的文件夹在保存镜像文件的文件夹部分中定义。单击文件夹... 可浏览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。

配置镜像时，还可以指定用户配置镜像服务器当前支持的用于下载更新副本的语言版本。语言版本设置可在可用版本列表中访问。

4.3.1.2.4.1 从镜像更新

有两种配置镜像的基本方法 - 具有更新文件的文件夹可以表示为共享网络文件夹或 HTTP 服务器。

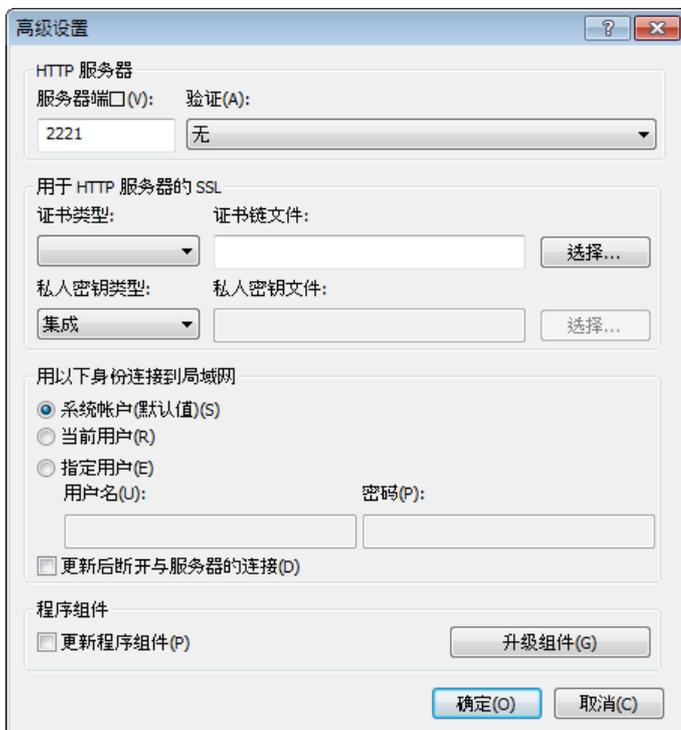
使用内部 HTTP 服务器访问镜像

此配置是默认的，在预定义的程序配置中指定。为了允许使用 HTTP 服务器访问镜像，请浏览至高级更新设置（单击镜像选项卡）并选择创建更新镜像选项。

在高级设置部分（镜像选项卡），可以指定 HTTP 服务器将侦听的服务器端口，以及 HTTP 服务器使用的验证类型。默认情况下，服务器端口设置为 2221。验证选项定义用于访问更新文件的验证方法。可用选项包括：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。

警告： 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。

添加您的证书链文件，或生成自签名证书以允许具有 HTTPS (SSL) 支持的 HTTP 服务器。可用类型包括：ASN、PEM 和 PFX。可以通过 HTTPS 协议下载更新文件，这样更加安全。几乎无法跟踪使用此协议的数据传输和登录凭据。私人密钥类型选项默认设置为已集成（因此默认禁用私人密钥文件选项），这意味着私人密钥已经是所选证书链文件的一部分。



配置完镜像后，转到工作站并添加新更新服务器。要执行该操作，请遵循以下步骤：

- 打开 **ESET Endpoint Antivirus** 高级设置并单击更新 > 常规。
- 单击更新服务器下拉菜单右侧的编辑...，并使用以下格式之一添加新服务器：
http://IP_address_of_your_server:2221
https://IP_address_of_your_server:2221（如果使用 SSL）
- 从更新服务器列表中选择新添加的服务器。

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，继续在高级更新设置部分镜像选项卡中配置对镜像的访问，方法是禁用通过内部 HTTP 服务器提供更新文件选项。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，必须输入验证数据以访问该计算机。要输入验证数据，请打开 ESET Endpoint Antivirus 高级设置 (F5) 并单击更新 > 常规。单击设置...按钮，然后单击 LAN 选项卡。如[连接到 LAN](#)部分所述，此设置和用于更新的设置相同。

完成镜像配置后，请进入工作站并将 \\UNC\PATH 设置为更新服务器。此操作可使用以下步骤完成：

- 打开 ESET Endpoint Antivirus 高级设置并单击更新 > 常规。
- 单击更新服务器旁的编辑...，使用 \\UNC\PATH 格式添加新服务器。
- 从更新服务器列表中选择此新添加的服务器。

注意：要正常工作，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。

最后一个部分控制程序组件 (PCU)。默认准备下载的程序组件复制本地镜像。如果选中更新程序组件旁的复选框，则无需单击升级组件，因为当文件可用时将自动复制到本地镜像。参见[更新模式](#)了解程序组件更新的更多信息。

4.3.1.2.4.2 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。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。

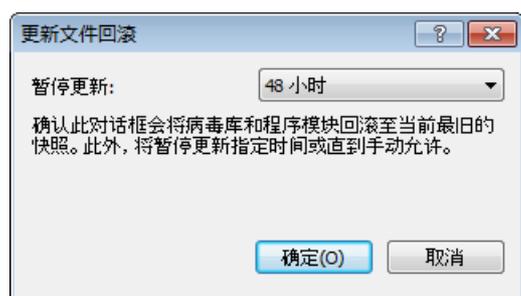
连接到镜像服务器时 ESET Endpoint Antivirus 报告错误 -定义用于访问 HTTP 版镜像的端口上的通信被阻止。

4.3.1.3 更新回滚

如果您怀疑病毒库的新更新不稳定或损坏，可以回滚至以前版本并禁用所选时期的任何更新。或者您可以启用以前禁用的更新。

ESET Endpoint Antivirus 提供病毒库的模块备份和恢复（称为回滚）功能。要创建病毒库快照，请选中允许更新文件快照复选框。本地存储的快照数字段定义本地计算机文件系统中存储的以前病毒库快照数量。

如果您单击回滚（高级设置 (F5) > 更新 > 高级），必须从暂停更新下拉菜单选择时间间隔，该间隔表示将暂停病毒库和程序模块更新的时段。

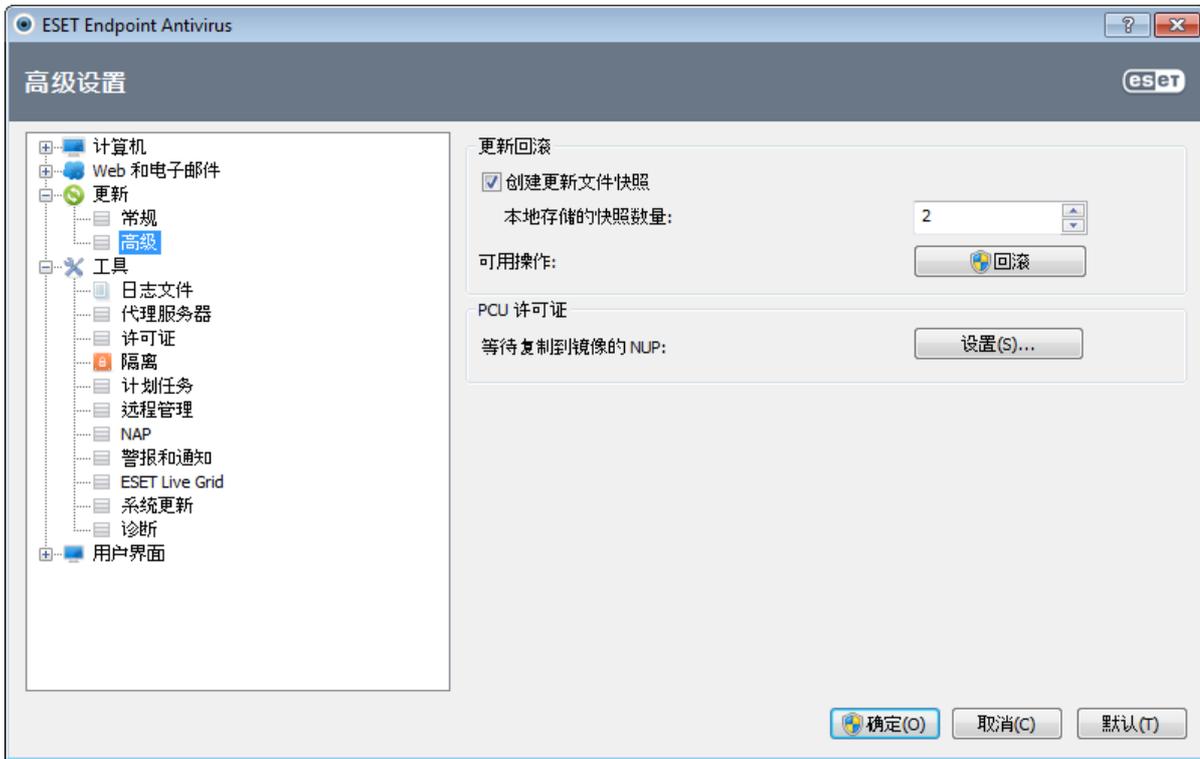


如果要手动允许定期更新，则选择直到调用。因为它具有潜在安全风险，我们不建议选择此选项。

如果启用回滚，回滚按钮变为允许更新。不允许时间间隔下拉菜单选择的时间间隔内的任何更新。病毒库版本降级至最旧版本，并作为快照存储在本地计算机文件系统中。

示例：以 6871 作为病毒库最新版本。6870 和 6868 存储作为病毒库快照。注意 6869 现在不可用，例如，因为计算机长时间关闭。如果您在本地存储的快照数字段中输入 2 并单击回滚，病毒库将恢复至版本号 6868。此过程需要一定时间。在 ESET Endpoint Antivirus 主程序窗口的[更新](#)部分检查病毒库版本是否已降级。

本地镜像服务器的配置选项可在 ESET Endpoint Antivirus 高级设置 部分的[许可证管理器](#)中添加有效许可密钥之后访问。如果您使用工作站作为镜像，更新副本必须先接受最新最终用户许可协议 (EULA)，然后才能作为用于更新网络中其他工作站的副本更新文件创建。如果更新时出现更新版本的 EULA，将显示一个用于确认的对话框窗口，超时时间为 60 秒。要手动进行此操作，请单击此窗口 PCU 许可部分中的设置...



4.3.2 如何创建更新任务

更新可以手动方式触发，方法是在主菜单中单击更新，在显示的主窗口中单击更新病毒库。

更新还可以作为计划任务运行。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，请参见[计划任务](#)部分。

4.4 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](#)
- [防护统计](#)
- [查看活动](#)
- [运行进程](#)
- [计划任务](#)
- [隔离区](#)
- [ESET SysInspector](#)

[提交文件以供分析](#) - 允许您提交可疑文件供 ESET 的病毒实验室进行分析。单击此选项后显示的对话框在[提交文件以供分析](#)部分中介绍。

ESET SysRescue - 启动 ESET SysRescue 创建向导。

4.4.1 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。日志记录是系统分析、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。可以直接从 ESET Endpoint Antivirus 环境以及归档日志中查看文本消息和日志。



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：

- **检测到的威胁** - 威胁日志提供有关 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、渗透名称、位置、执行的操作以及检测到渗透时登录用户的名称。双击任何日志条目以在单独的窗口中显示其详细信息。
- **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。它为系统管理员和用户解决问题而设计。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** - 所有已完成的手动或计划扫描的结果显示在此窗口中。每一行对应一个计算机控件。双击任意条目可查看相应扫描的详细信息。
- **HIPS** - 包含特定规则的记录，这些规则被标记为用于进行记录。该协议显示调用操作、结果（规则被允许还是被禁止）以及创建的规则名称的应用程序。
- **设备控制** - 包含与计算机连接的可移动磁盘或设备的记录。只有具有相应设备控制规则的设备将记录到日志文件。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。

在每一部分中，显示的信息都可以直接复制到剪贴板（键盘快捷方式为 Ctrl+C），方法是选择条目并单击复制。要选择多个条目，可以使用 CTRL 和 SHIFT 键。

通过右键单击特定记录，可以显示右键菜单。右键菜单中提供以下选项：

- 过滤相同类型的记录 - 启用此过滤器后，您将只能看到相同类型的记录（诊断、警告...）。
- 过滤.../查找... - 单击此选项后，将弹出日志过滤窗口，您可以定义过滤条件。
- 禁用过滤器 - 清除所有过滤器设置（如上文所述）。
- 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。
- 滚动日志 - 使此选项保持为启用状态以自动滚动旧日志，并在日志文件窗口中查看活动日志。

4.4.1.1 日志维护

可从主程序窗口访问 ESET Endpoint Antivirus 的日志文件配置。单击设置 > 进入高级设置...> 工具 > 日志文件。日志文件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：

自动删除早于以下天数的记录 - 将自动删除早于指定天数的日志条目。

自动优化日志文件 - 如果选中该选项，则碎片百分比高于如果未使用记录数超过(%)中指定的值后将自动整理日志文件碎片。

单击立即优化启动日志文件的碎片整理。在此过程中会删除所有空日志条目，这将在处理日志时提高性能和速度。尤其在日志包含大量条目数时，可以感受到这种提高。

最低日志记录级别 - 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（启动病毒防护出错等）。

单击启用文本协议，以其他文件格式并在[日志文件](#)之外存储日志：

- 类型 - 如果选择纯文本文件格式，日志将存储在文本文件中；按制表符来分隔数据。同样适用于逗号分隔的 CSV 文件格式。如果选择事件，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）中，而不是存储为文件。
- 目标目录 - 将存储文件的位置（仅适用于纯文本/CSV 格式）。每个日志部分都有其自己的预定义了文件名的文件（例如，如果您使用纯文本文件格式来存储日志，则日志文件的检测到的威胁部分为 virlog.txt）。

删除日志按钮可删除当前在类型下拉菜单中选定的所有存储的日志。

4.4.2 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：病毒库更新、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...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。



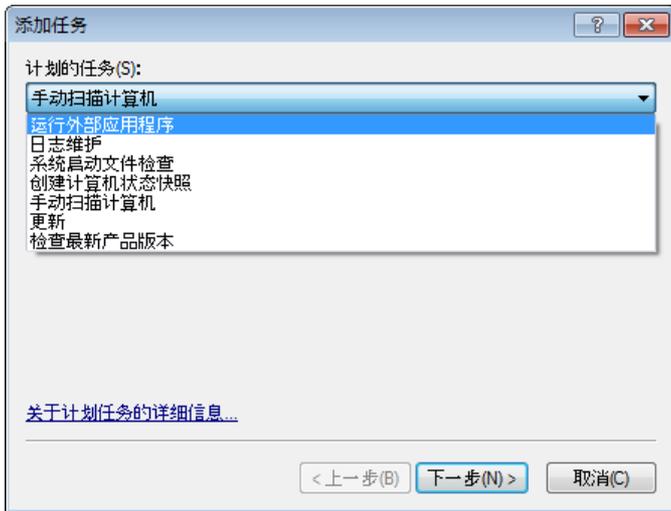
默认情况下，计划任务中显示以下计划任务：

- 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（成功更新病毒库以后）

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...。
2. 从下拉菜单中选择需要的任务。



3. 输入任务名称并选择以下计时选项之一：

- 一次 - 任务将仅在预定义的日期和时间执行一次。
- 重复 - 任务将以指定的时间间隔（以小时为单位）执行。
- 每天 - 任务将在每天指定时间运行。
- 每周 - 任务将在每周所选日期和时间运行一次或多次。
- 由事件触发 - 任务将在发生指定事件时执行。



4. 根据您在上一步骤中选择的计时选项，将显示以下对话框之一：

- 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 - 任务将在每天指定时间重复运行。
- 每周 - 任务将在选定的日期和时间运行。

5. 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：

- 等待至下次计划时间
- 尽快运行任务
- 如果自上次执行任务至今已超过 -- 小时则立即执行任务

6. 在最后一个步骤中，您可以检查将被排入计划的任務。单击完成应用此任务。



4.4.2.1 创建新任务

要在计划任务中创建新任务，请单击添加...按钮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。
- 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 - 通过更新病毒库和更新程序模块，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。单击下一步并将任务名输入到任务名称字段。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。当笔记本电脑在靠电池供电时，使用如果计算机正在靠电池供电，则不执行任务选项来最大程度地降低系统资源消耗。将根据选定的频率为您提供不同的更新参数。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。有以下三个可用选项：

- 等待至下次计划时间
- 尽快执行任务
- 如果自上次执行任务至今已超过指定时间间隔则立即执行任务（可以使用 任务间隔 滚动框定义该时间间隔）

在下一步中，将显示带有当前计划任务信息的摘要窗口；选项以特定参数执行任务应自动启用。单击完成按钮。

将显示一个对话框，允许您选择用于计划任务的配置文件。您可以在这里指定主要配置文件和备用配置文件，后者用于使用主要配置文件无法完成的情况。在更新配置文件窗口中单击确定表示确认。新的计划任务将添加到当前计划任务列表中。

4.4.3 防护统计

要查看与 ESET Endpoint Antivirus 的防护模块相关的统计数据图表，请单击防护状态 > 防护统计。从统计下拉菜单中选择所需的防护模块可以查看相应的图表和图例。如果将鼠标移到图例中的项目上，则图表中将仅显示该项目的数据。



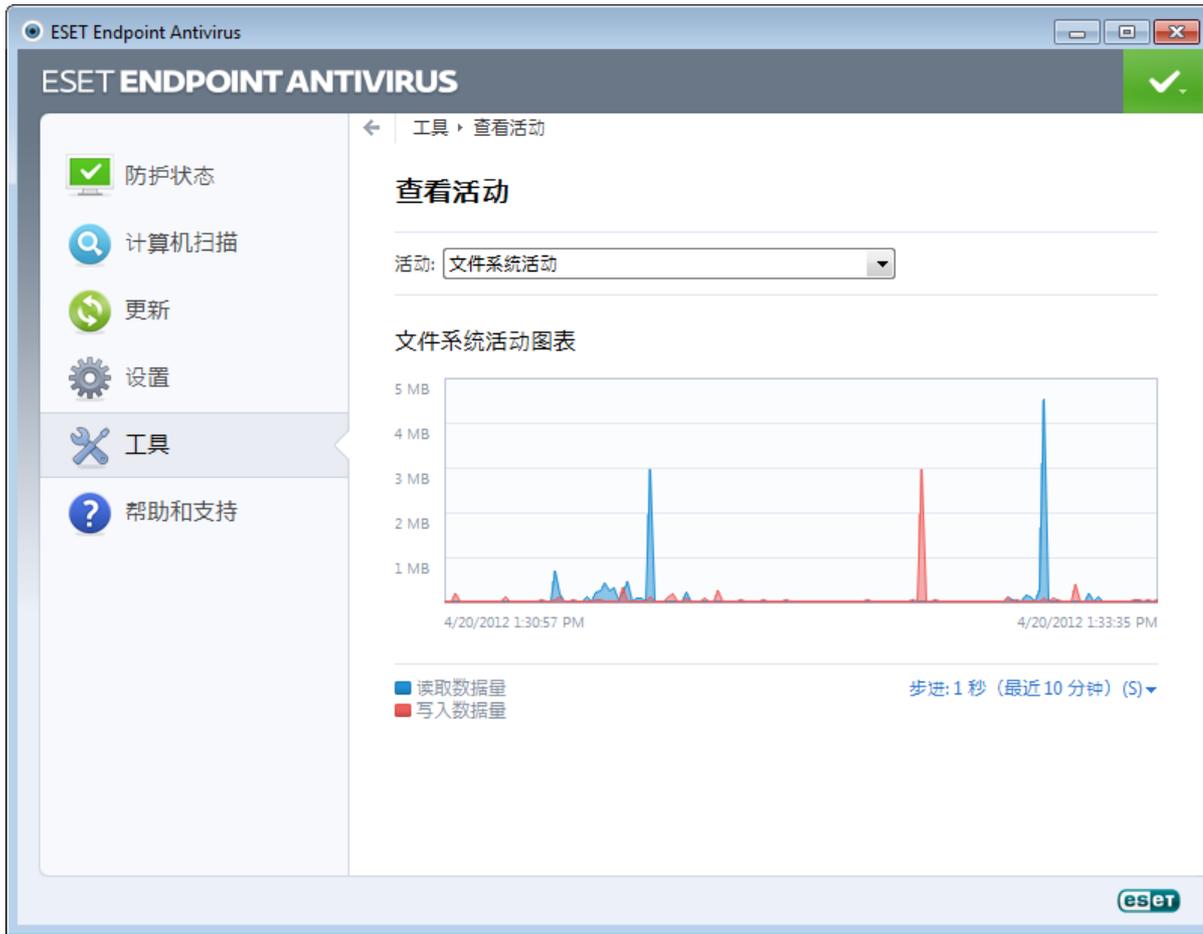
以下统计图表可供使用：

- 病毒和间谍软件防护 - 显示被感染对象和已清除对象的数量。
- 文件系统防护 - 仅显示已读取或写入文件系统的对象。
- 电子邮件客户端防护 - 仅显示电子邮件客户端发送或接收的对象。
- **Web 访问保护** - 仅显示 Web 浏览器下载的对象。

在统计图表下，可以看到扫描对象的总数、最近扫描的对象和统计时戳。单击重置以清除所有统计信息。

4.4.4 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。要更改时间范围，请单击位于窗口右下角的步进 1...选项。



有以下选项可供使用：

- 步进：1 秒（最近 10 分钟） - 图表每秒刷新一次，时间线范围为最后 10 分钟
- 步进：1 分钟（最近 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（最后一个月） - 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（蓝色）和写入的数据（红色）。这两个值都以 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。

4.4.5 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，已安装的驱动程序和应用程序、网络连接或重要注册表条目）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。

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：

- 比较 - 比较两个现有日志。
- 创建... - 创建新日志。在 ESET SysInspector 日志完成（状态显示为“已创建”）之前，请稍候。
- 删除 - 删除列表中选定的日志。

右键单击一个或多个选定日志后，可从右键菜单中使用以下选项：

- 显示 - 在 ESET SysInspector 中打开选定日志（相当于双击日志）。
- 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。

4.4.6 ESET Live Grid

ESET Live Grid（下一代 ESET ThreatSense.Net）是基于信誉防范即将出现的威胁的先进预警系统。ESET 病毒实验室利用来自云技术的威胁相关信息实时流保持防御处于最新状态，确保稳定的防护水平。用户可以直接从程序界面或右键菜单检查运行进程和文件的信誉，以及来自 ESET Live Grid 的其他信息。有两种选择：

1. 您可以决定不启用 ESET Live Grid。您不会失去软件中的任何功能，而且仍将收到我们提供的最好保护。
2. 您可以配置 ESET Live Grid 提交关于新威胁以及新威胁代码所在位置的匿名信息。此文件可以发送到 ESET 以供详细分析。研究这些威胁将帮助 ESET 更新其威胁检测功能。

ESET Live Grid 将收集您的计算机中与新检测到的威胁相关的信息。这些信息可以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）。如果您或您的组织希望避免发送特定类型的文件，也可以添加其他扩展名。

ESET Live Grid 的设置菜单提供了几个启用/禁用 ESET Live Grid 的选项，使用此功能可将可疑文件和匿名统计信息提交给 ESET 实验室。可从 **高级设置** 树单击 **工具 > ESET Live Grid** 访问它。

参与 ESET Live Grid - 启用/禁用 ESET Live Grid，使用此功能可将可疑文件和匿名统计信息提交至 ESET 实验室。

不提交统计 - 如果您不希望从 ESET Live Grid 提交有关您的计算机的匿名信息，则选择此选项。此信息与新检测到的威胁有关，其中可能包括渗透名称、有关检测到的日期和时间信息、ESET Endpoint Antivirus 版本、计算机操作系统版本信息和位置设置等。统计信息通常一天一次或两次发送给 ESET 的服务器。

不提交文件 - 在内容或行为上类似渗透的可疑文件不通过 ESET Live Grid 技术提交给 ESET 以供分析。

高级设置... - 带有具有更多 ESET Live Grid 设置的窗口。

如果您以前使用过 ESET Live Grid，可能仍会发送数据包。即使预警系统已关闭，此类数据包也会在下次启用时发送给 ESET。之后不会再创建任何数据包。

4.4.6.1 可疑文件

ESET Live Grid 高级设置中的文件选项卡可用于配置威胁提交到 ESET 威胁实验室以供分析的方式。

如果发现可疑文件，可以将其提交到我们的威胁实验室进行分析。如果文件是一个恶意应用程序，则下次病毒库更新中将添加对此程序的检测。

排除过滤器 - 排除过滤器允许您不提交某些文件/文件夹。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。例如，将可能包含机密信息的文件（如文档或电子表格）排除在外可能很有用。默认情况下最常见的文件类型均被排除（.doc 等）。如果需要，可以添加排除文件列表。

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。

在本部分中，您还可以选择通过 ESET Remote Administrator 或直接将文件和统计信息提交至 ESET。如果您希望确保将可疑文件和统计信息提供至 ESET，请选择通过 **远程管理员** 或 **直接提交给 ESET** 选项。在此情况下，通过所有可用方法提交文件和统计信息。通过远程管理员提交可疑文件会将文件和统计信息提交至远程管理服务器，服务器将确保后续提交给 ESET 的病毒实验室。如果选择 **直接提交给 ESET** 选项，将直接通过该程序将所有可疑文件和统计信息发送给 ESET 的病毒实验室。

选择启用日志记录选项，创建记录文件和统计信息提交的事件日志。它将启用发送文件或统计信息时记录到 [事件日志](#)。

4.4.7 运行进程

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，使用 [ESET Live Grid](#) 技术保护用户。



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。

风险级别 - 在大多数情况下，ESET Endpoint Antivirus 和 ESET Live Grid 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，会向对象指派风险级别，级别从 **1 - 良好（绿色）** 到 **9 - 危险（红色）**。

注意： 标记为 **良好（绿色）** 的已知应用程序肯定干净（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实时文件系统防护。

用户数量 - 使用给定应用程序的用户数量。此信息由 ESET Live Grid 技术收集。

发现时间 - 自从应用程序被 ESET Live Grid 技术发现以来的时段。

注意： 当应用程序被标记为 **未知（橙色）** 安全级别时，它不一定是恶意软件。通常它是一个较新的应用程序。如果您不确定文件，可以 [提交文件](#) 至 ESET 病毒实验室以供分析。如果文件被证实是一个恶意应用程序，则以后的更新中将增加对它的检测。

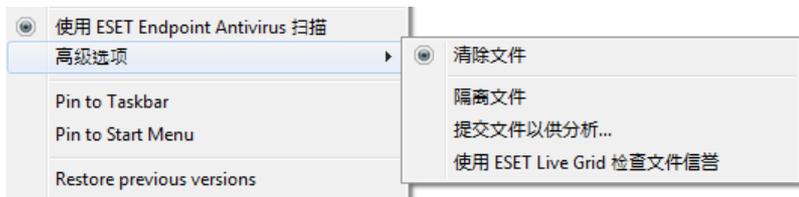
应用程序名称 - 程序或进程的给定名称。

在新窗口中打开 - 将在新窗口中打开运行进程的信息。

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：

- 文件 - 计算机上应用程序的位置。
- 文件大小 - 文件大小，以 KB（千字节）或 MB（兆字节）为单位。
- 文件说明 - 基于操作系统说明的文件特性。
- 公司名称 - 供应商或应用程序进程的名称。
- 文件版本 - 来自应用程序发布者的信息。
- 产品名称 - 应用程序名称和/或企业名称。

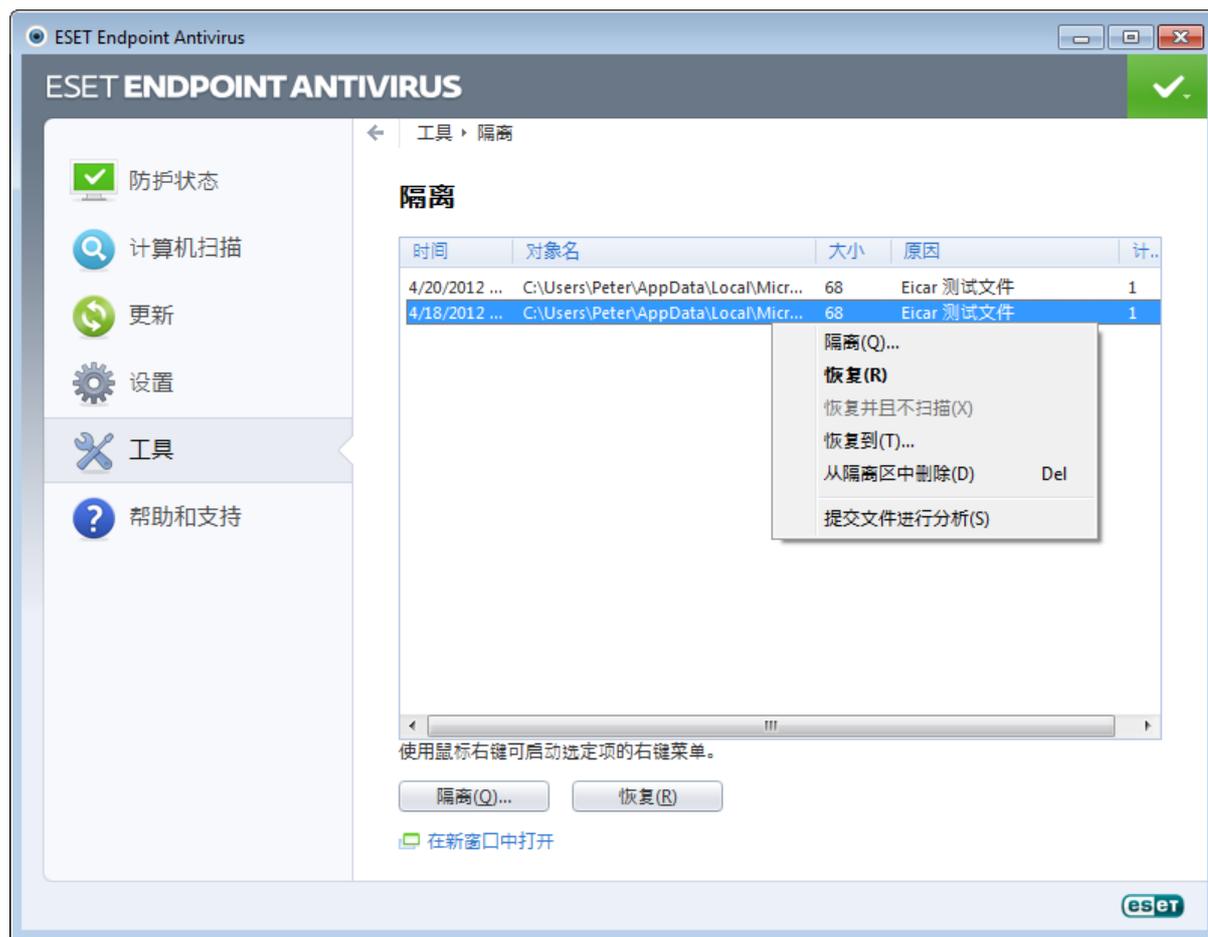
注意：还可以对不作为运行程序/进程检查信誉 - 标记要检查的文件，右键单击文件，从**右键菜单**中选择高级选项 > 使用 ESET Live Grid 检查文件信誉。



4.4.8 隔离区

隔离区的主要功能是安全储存被感染文件。隔离文件的前提是文件出现以下情况：无法清除、不安全或被建议删除，或被 ESET Endpoint Antivirus 错误检测。

您可以选择隔离任何文件。如果文件行为可疑但未被病毒防护扫描程序检测到，建议采取隔离措施。可将隔离的文件提交 ESET 的病毒实验室进行分析。



可在表格中查看储存在隔离区文件夹中的文件，表格中显示隔离的日期和时间、被感染文件原始位置的路径、文件大小（字节数）、原因（例如，由用户添加的对象）以及威胁数量（例如，是否为包含多个渗透的压缩文件）等。

隔离文件

ESET Endpoint Antivirus 自动隔离被删除的文件（如果您尚未在警报窗口中取消该选项）。如果需要，您可以手动隔离任何可疑文件，方法是单击隔离...。这种情况下，程序不会将原文件从其初始位置删除。也可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...

从隔离区恢复

隔离的文件还可以恢复到其初始位置。使用恢复功能可达到此目的，在 隔离区 窗口中右键单击给定文件，然后从右键菜单中选择相关项即可完成恢复操作。如果文件标记为潜在不受欢迎的应用程序，则启用恢复并且不扫描选项。请阅读[词汇表](#)中更多关于此类应用程序的信息。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。

注意: 如果程序错误地隔离了无害文件，请在文件恢复后将其[移出扫描队列](#)，并发送给 ESET 客户服务部门。

提交隔离区中的文件

如果您隔离的可疑文件程序未检测到，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，请将文件发送到 ESET 的病毒实验室。要提交隔离区中的文件，右键单击该文件并从右键菜单中选择提交要分析的文件。

4.4.9 提交文件以供分析

使用文件提交对话框可将文件发送到 ESET 以供分析，该对话框可在工具 > 提交文件以供分析中找到。如果您在计算机上发现了行为可疑的文件，可将其提交给 ESET 的病毒实验室以供分析。如果文件被证实是一个恶意应用程序，则以后的更新中将增加对它的检测。

此外，也可以通过电子邮件提交文件。如果您选用此方式，则使用 WinRAR/ZIP 压缩文件、用密码 Infected 保护压缩文件并发送至 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文件的信息（比如下载此文件的网站名）。

注意：向 ESET 提交文件前，确保其满足以下一个或多个标准：

- 未检测到文件。
- 将文件错误检测为威胁。

除非需要更多信息供分析，否则您不会收到回信。

从提交文件的理由下拉菜单选择最适合您的邮件的描述：

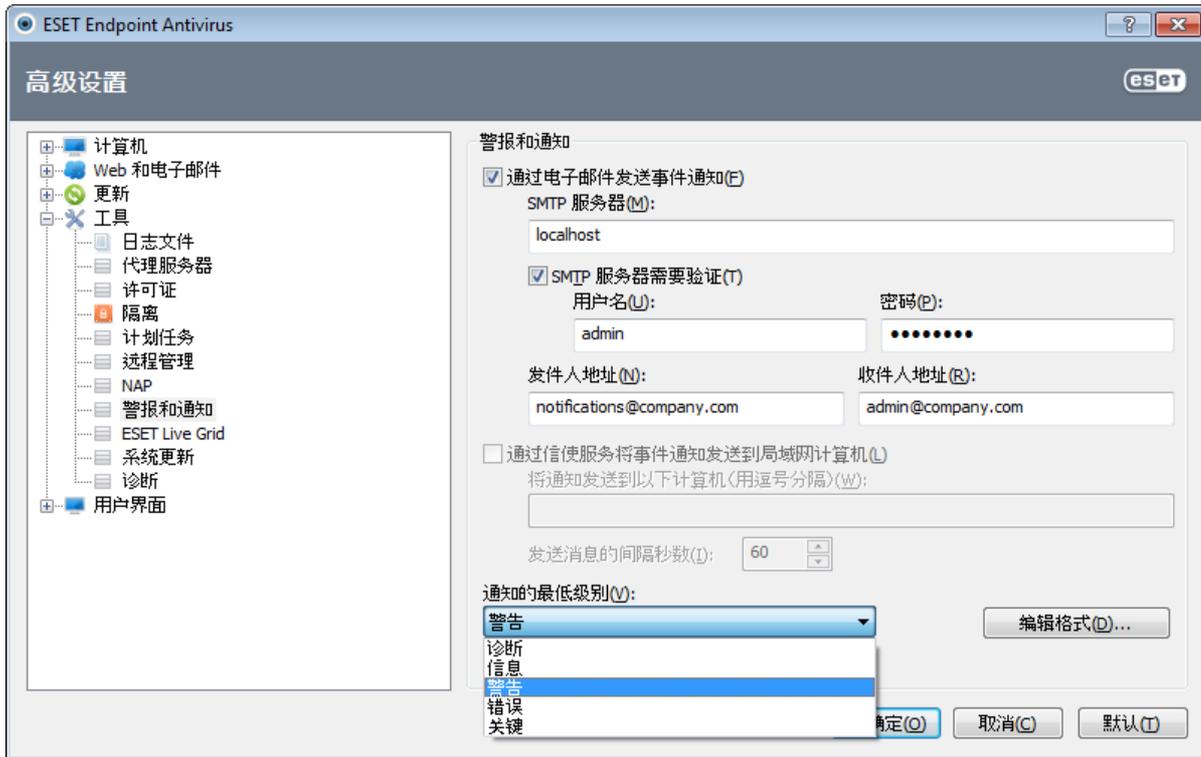
- 可疑文件，
- 误报（文件检测为感染，但并未感染），
- 以及其他。

文件 - 您想要提交的文件的路径。

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，如果需要更多信息供分析时可能会使用该邮件与您联系。可选择是否输入联系人电子邮件。除非需要更多信息，否则您不会收到 ESET 的回信。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。

4.4.10 警报和通知

ESET Endpoint Antivirus 支持发生具有所选级别的事件时发送电子邮件。单击通过电子邮件发送事件通知复选框启用此功能并激活电子邮件通知。



SMTP 服务器 - 用于发送通知的 SMTP 服务器。

注意： ESET Endpoint Antivirus 不支持采用 SSL/TLS 加密的 SMTP 服务器。

SMTP 服务器需要验证 - 如果 SMTP 服务器需要验证，则需在字段中填写有效的用户名和密码，这样才能访问 SMTP 服务器。

发件人地址 - 该字段用于指定发件人地址，发件人地址会在通知电子邮件的标题中显示。

收件人地址 - 该字段用于指定收件人地址，收件人地址会在通知电子邮件的标题中显示。

通过信使服务将事件通知发送到局域网计算机 - 选中此复选框可通过 Windows 信使服务将消息发送给 LAN 计算机。

将通知发送给以下计算机（由逗号分隔） - 输入通过 Windows 信使服务接收通知的计算机名称。

发送消息的间隔秒数 - 要更改（通过 LAN 发送的）通知的时间间隔，请输入希望的时长（以秒计）。

通知的最低级别 - 指定要发送的通知的最低级别。

编辑格式... - 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 信使服务）完成。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，可能需要更改消息格式 - 单击[编辑格式...](#)。

4.4.10.1 邮件格式

这里可以设置远程计算机上显示的事件邮件格式。

威胁警报和通知邮件有预定义的默认格式。我们建议您不要更改该格式。不过在某些情况下（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。

在邮件中，关键字（用 % 符号隔开的字符串）由指定的实际信息替换。可用关键字包括：

- %TimeStamp% - 事件的日期和时间。
- %Scanner% - 相关模块。
- %ComputerName% - 发生警告的计算机的名称。
- %ProgramName% - 产生警报的程序。
- %InfectedObject% - 被感染文件、邮件等的名称。
- %VirusName% - 感染标识。
- %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。

使用本地字母字符 - 根据 Windows 区域设置（例如 windows-1250）将电子邮件转换为 ANSI 字符编码。如果保留此复选框未选中，将转换邮件并以 ACSII 7 位编码（例如“á”将更改为“a”，未知符号改为“？”）。

使用本地字符编码 - 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（áéú）。

4.4.11 系统更新

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 - 不提供系统更新供下载。
- 可选更新 - 将提供标记为低优先级及更高优先级的更新供下载。
- 建议的更新 - 将提供标记为常用及更高优先级的更新供下载。
- 重要更新 - 将提供标记为重要及更高优先级的更新供下载。
- 关键更新 - 仅提供关键更新供下载。

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。

4.4.12 诊断

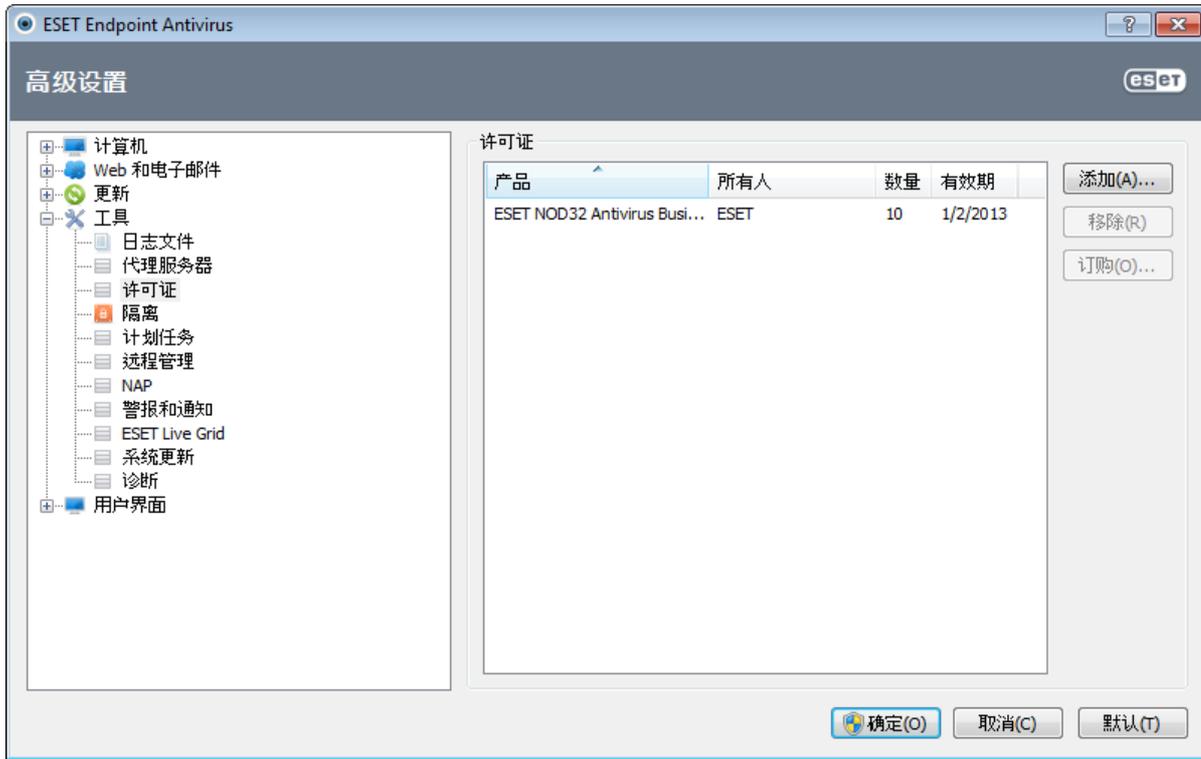
诊断提供 ESET 进程（比如 ekm）的应用程序崩溃转储。如果应用程序崩溃，将生成一个转储。这能够帮助开发人员调试和修复各种 ESET Endpoint Antivirus 问题。有两种转储类型可用：

- 完整的内存转储 - 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。
- 迷你转储 - 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。然而，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。
- 选择不生成内存转储（默认）来禁用此功能。

目标目录 - 在崩溃期间将生成转储的目录。单击打开文件夹...在新 Windows 资源管理器窗口中打开此目录。

4.4.13 许可证

许可证分支可用于管理 ESET Endpoint Antivirus 和其他 ESET 产品（例如 ESET Remote Administrator 等）的许可证密钥。在购买后，许可证密钥会随同用户名和密码一起提供给您。要添加/删除许可证密钥，请单击许可证管理器（许可证）窗口的相应按钮。单击工具 > 许可证可从高级设置树中访问许可证管理器。



许可证密钥是一个文本文件，其中包含有关所购买产品的信息：所有者、许可证号以及到期日期。

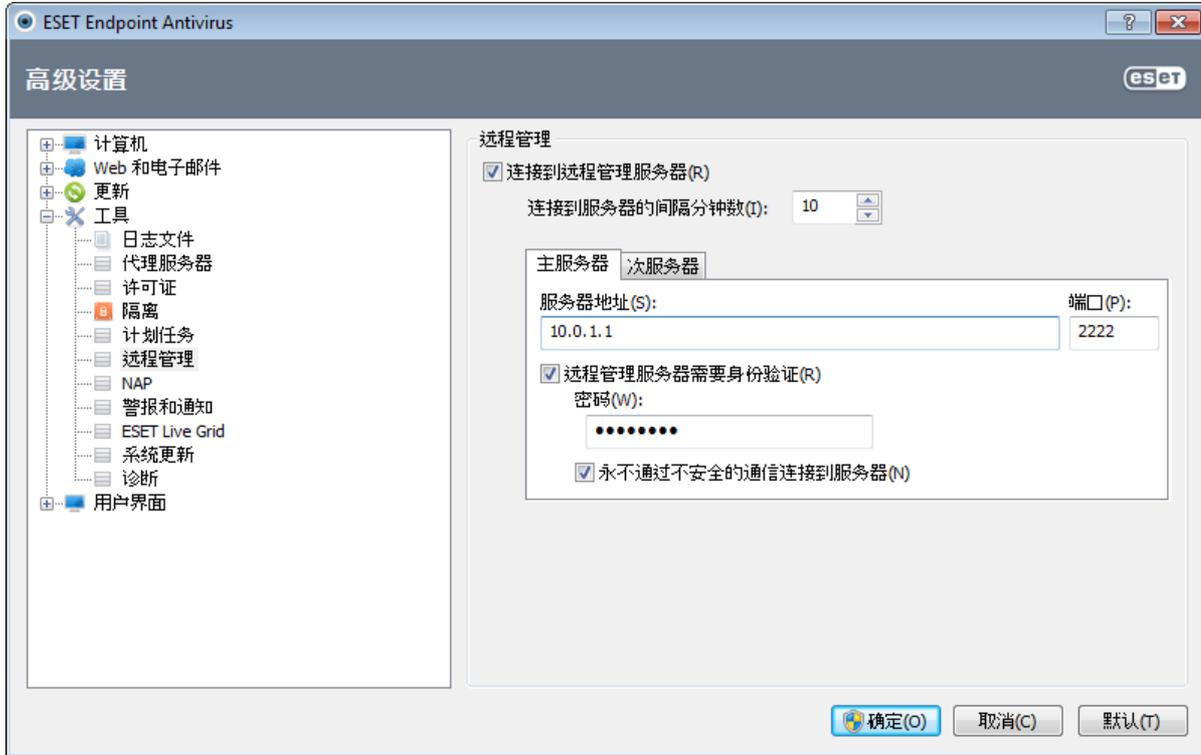
许可证管理器窗口允许您使用添加... 按钮上载和查看许可证密钥的内容 - 其中包含的信息显示在管理器中。要从列表中删除许可证文件，请选中文件然后单击删除。

如果许可证密钥已过期，而您有意续订，请单击订购... 按钮，程序将把您重定向到我们的在线商店。

4.4.14 远程管理

ESET Remote Administrator (ERA) 是用于管理安全策略和获得全面网络安全概览的强大工具。它对大型网络特别有用。ERA 不仅可提高安全级别，还可在客户端工作站上管理 ESET Endpoint Antivirus 时提供方便性。您可以安装、配置、查看日志、计划更新任务、扫描任务等。ESET Remote Administrator (ERAS) 与 ESET 安全产品之间的通信需要对两端都进行正确的配置。

远程管理设置选项可在 ESET Endpoint Antivirus 程序主窗口中找到。单击设置 > 进入高级设置... > 工具 > 远程管理。



通过选择连接到远程管理服务器选项激活远程管理。然后即可访问下述其他选项：

连接到服务器的间隔分钟数 - 这表示 ESET 安全产品连接 ERAS (以发送数据) 的频率。

主服务器, 次服务器 - 通常, 仅需要配置主服务器。如果在网络上运行多个 ERA 服务器, 则可以选择添加另一个次 ERA 服务器连接。它将用作备选解决方案。这样, 如果主服务器不可访问时, ESET 安全解决方案将自动联系次 ERA 服务器。同时, 将尝试重新建立与主服务器的连接。再次激活此连接后, ESET 安全解决方案将切换回主服务器。配置两个远程管理服务器配置文件最适用于通过笔记本电脑从本地网络和外部网络连接的移动客户端。

服务器地址 - 指定运行 ERAS 的服务器的 DNS 名称或 IP 地址。

端口 - 该字段包括用于连接的预定义服务器端口。建议您保留默认端口设置 2222。

服务器连接间隔 (分钟) - 该选项指定 ESET Endpoint Antivirus 将连接到 ERA Server 的频率。如果它被设置为 0, 将每 5 秒钟提交一次信息。

Remote Administrator 服务器需要验证 - 如果需要, 允许输入密码以连接到 ERA Server。

永不通过不安全的通信连接到服务器 - 选中此选项可禁用 ERA 服务器的连接, 尽管已启用未经验证的访问 (参见 ERA Console > 服务器选项 > 安全 > 启用客户端的未经验证访问)。

单击确定, 确认更改并应用设置。ESET Endpoint Antivirus 将使用这些设置来连接到 ERA Server。

4.5 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[图形](#)工具，您可以调整程序的视觉外观和使用的效果。

通过配置[警报和通知](#)，您可以更改检测到的威胁警报和系统通知的行为。可自定义这些设置以满足您的需求。

如果您选择不显示某些通知，它们将显示在[隐藏的通知窗口](#)区域中。您可以在这里检查它们的状态，显示更多细节或将它们从此窗口中删除。

为提供您的安全软件的最大安全性，您可以使用[访问设置](#)工具通过密码保护设置，以避免未经授权更改。

右键单击选中的对象后，就会显示[上下文菜单](#)。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。

4.5.1 图形

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 > 图形分支访问这些配置选项。

在用户界面元素部分，如果图形元素会使计算机性能下降、或引起其他问题，则应禁用图形用户界面选项。对于有视觉障碍的用户可能需要关闭图形界面，因为用于阅读屏幕上显示的文本的特殊应用程序可能与图形界面发生冲突。

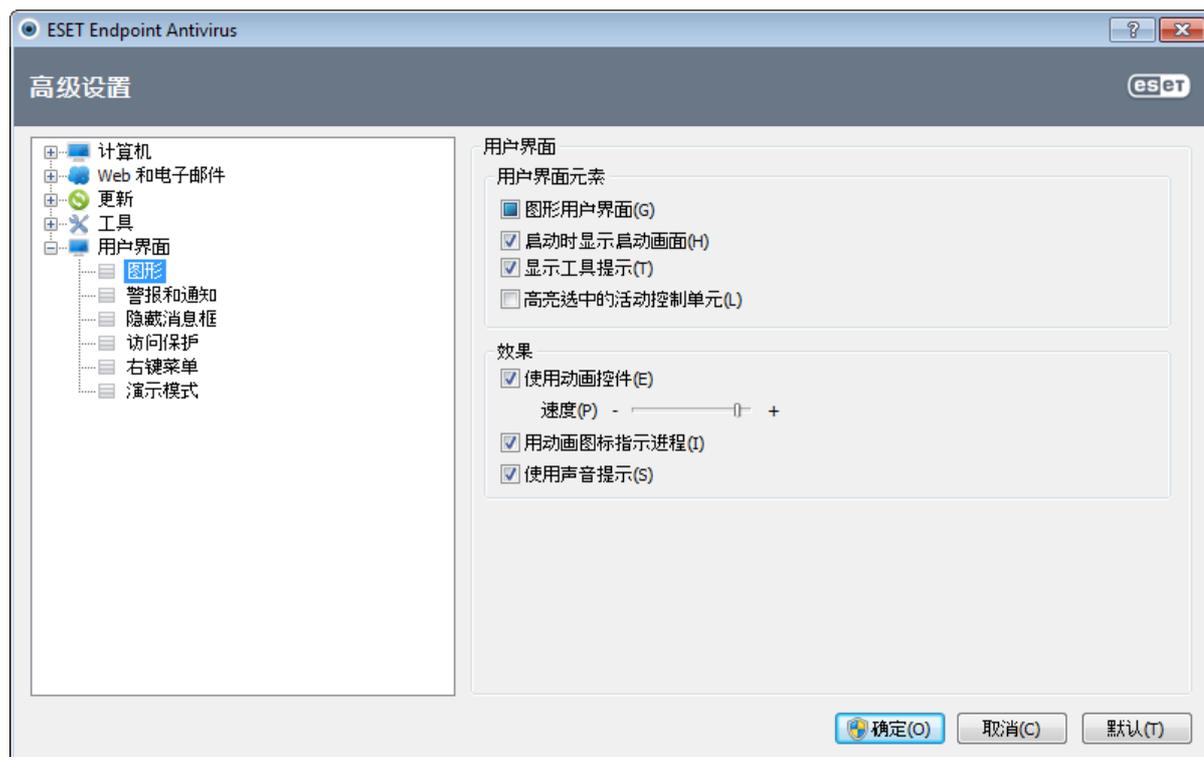
如果希望停用 ESET Endpoint Antivirus 启动画面，则取消选择启动时显示启动画面选项。

如果启用显示工具提示选项，则在光标置于任何选项上时，系统将显示该选项的简短说明。选择活动控件元素选项可使系统突出显示当前在鼠标光标活动区域的任何元素。突出显示的元素将在鼠标单击后被启用。

要降低或提高动画效果的速度，请选择使用动画控件选项，并将速度滑块移动到左侧或右侧。

要启用动画图标以显示各个操作的进度，请选择用动画图标指示进度选项。

如果想要程序在发生重要事件时发出声音，请选中使用声音信号选项。请注意，该声音仅在计算机扫描正在运行或已完成时发出。



4.5.2 警报和通知

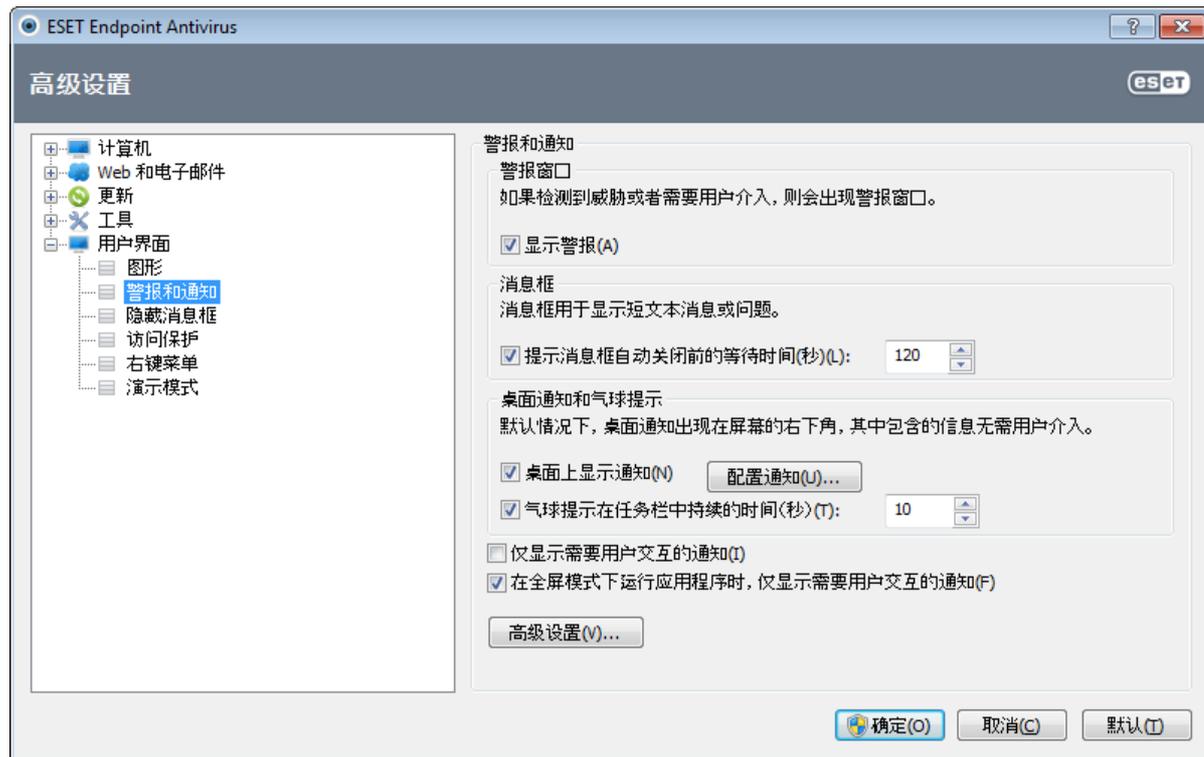
警报和通知部分（在用户界面下）允许您配置如何由 ESET Endpoint Antivirus 处理威胁警报和系统通知（比如成功更新消息）。您还可以设置显示时间和系统托盘透明度级别（仅适用于支持系统托盘通知的系统）。

第一项是显示警报。禁用该选项将取消所有警报窗口，这只适用于少数特定情况。对于大多数用户，我们建议保留该选项的默认设置（启用）。

要在一段时间后自动关闭弹出窗口，请选择提示消息框自动关闭前的等待时间（以秒计）选项。如果未手动关闭，警报窗口会在超过指定时限后自动关闭。

桌面通知和气球提示仅作为信息提示方式，不提供也不需要用户交互。它们显示在屏幕右下角的通知区域。要启用桌面通知，请选择在桌面上显示通知选项。可通过单击配置通知...按钮更改通知显示时间和窗口透明度等更多详细选项。要预览通知情况，请单击预览按钮。

要配置气球提示显示时间，请参见气球提示在任务栏中持续的时间（以秒计）选项，并在相邻字段中输入所需间隔。



仅显示需要用户交互的通知选项允许您切换无需用户交互的警报和通知。选择在全屏模式下运行应用程序时，仅显示需要用户交互的通知以抑制所有非交互通知。

单击高级设置...以进入其他警报和通知设置选项。

4.5.2.1 高级设置

从要显示事件的最低级别下拉菜单中，可以选择要显示的警报和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（启动病毒防护出错等）。

此部分的最后一项功能是在多用户环境中配置通知目标。对于多用户系统，在以下用户的屏幕上显示通知字段在允许多个用户同时连接的系统上指定一个接收系统和其他通知的用户。正常情况下应该是系统或网络管理员。假如所有系统通知都发给管理员，该选项对终端服务器特别有用。

4.5.3 隐藏的通知窗口

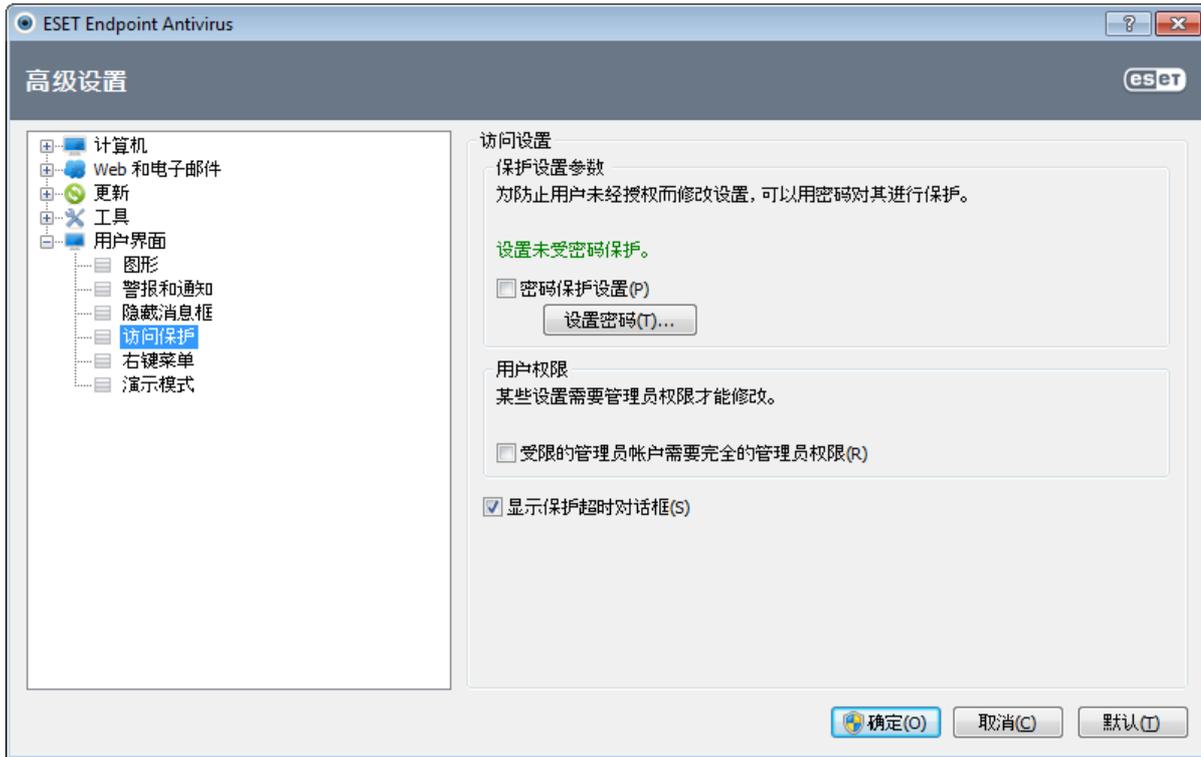
如果对先前显示的任何通知窗口（警报）选中了不再显示此消息选项，则它会出现在隐藏的通知窗口列表中。立即自动执行的操作会显示在标题为确认的列中。

显示 - 显示当前未显示和为其配置了自动操作的通知窗口预览。

删除 - 从隐藏的消息框列表中删除项目。从列表中删除的所有通知窗口都将再次显示。

4.5.4 访问设置

为最大限度地保护系统安全，必须正确配置 ESET Endpoint Antivirus。任何未经授权的更改都可能导致重要数据的丢失。此选项位于高级设置树的用户界面下的访问设置子菜单中。要避免未经授权的更改，可用密码保护 ESET Endpoint Antivirus 的设置参数。



密码保护设置 - 锁定/解锁程序的设置参数。选中或取消选中该复选框以打开密码设置窗口。

要设置或更改密码以保护设置参数，请单击设置密码....

受限的管理员帐户需要完全的管理员权限 - 选中此选项，可在修改某些系统参数（类似于 Windows Vista 中的 UAC）时提示当前用户（如果他或她没有管理员权限）输入管理员用户名和密码。修改包括禁用保护模块。

显示保护超时对话框 - 如果选中此选项，将在您从程序菜单或通过 ESET Endpoint Antivirus > 设置部分暂时禁用保护时提示您。暂时禁用保护窗口中的时间间隔下拉菜单代表所有选定保护部分被禁用的时段。

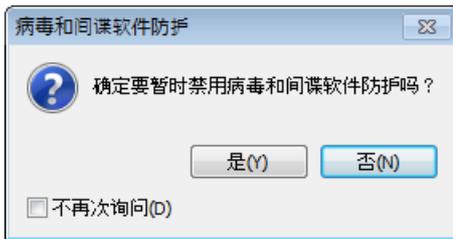
4.5.5 程序菜单

在主程序菜单中，可以访问一些最重要的设置选项和功能。

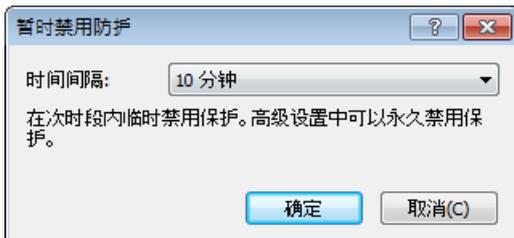


常用 - 显示最常用的 ESET Endpoint Antivirus 部分。您可以从程序菜单快速访问这些常用部分。

暂时禁用防护 - 显示禁用[病毒和间谍软件防护](#)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恶意系统攻击。选择下次不再询问复选框可在将来避免显示此消息。



时间间隔 下拉菜单表示将为其禁用病毒和间谍软件防护的时段。



高级设置... - 选择此选项以进入高级设置树。还有其它方法来打开它，例如按 F5 键或导航到设置 > 进入高级设置...

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，并提供检测到的威胁的概要信息。

重置窗口布局 - 将 ESET Endpoint Antivirus 的窗口重置为其默认大小和屏幕位置。

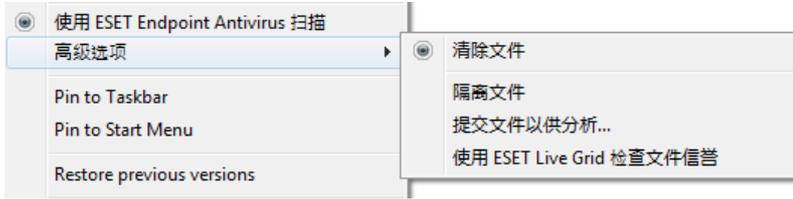
关于 - 提供系统信息、有关已安装的 ESET Endpoint Antivirus 版本以及安装的程序模块的详细信息。这里还可以找到许可证到期日期。在窗口底部，可以找到关于操作系统和系统资源的信息。

4.5.6 右键菜单

右键单击选中的对象后，就会显示右键菜单。该菜单会列出对此对象执行操作的所有可用选项。

可以将 ESET Endpoint Antivirus 控件元素集成到右键菜单中。在高级设置树的用户界面 > 右键菜单部分中提供了此功能的更详细的设置选项。

集成到右键菜单 - 将 ESET Endpoint Antivirus 控件元素集成到右键菜单中。



菜单类型下拉菜单中提供了下列选项：

- 完全（首选扫描） - 启动所有右键菜单选项；主菜单将显示使用 **ESET Endpoint Antivirus** 扫描选项。
- 完全（首选清除） - 启动所有右键菜单选项；主菜单将显示使用 **ESET Endpoint Antivirus** 清除选项。
- 仅扫描 - 右键菜单中将仅显示使用 **ESET Endpoint Antivirus** 扫描选项。
- 仅清除 - 右键菜单中将仅显示使用 **ESET Endpoint Antivirus** 清除选项。

4.5.7 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。启用此功能后，将禁用所有弹出窗口，同时完全停止计划任务活动。系统保护仍在后台运行，但是不需要任何用户交互。

您可以在主菜单中启用或禁用演示模式，方法是单击设置 > 计算机，然后单击演示模式下的启用，方法是展开用户界面，单击演示模式并选中启用游戏模式旁边的复选框。启用演示模式 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，演示模式已启用，以橙色显示。

选中以全屏模式运行应用程序时自动启用演示模式复选框后，将在您启动全屏应用程序后启动演示模式，并在您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直接启动演示模式尤为有用。

您还可以选中复选框自动禁用演示模式前等待的时间以定义时间量（默认值为 1 分钟）。仅当在特定时间段需要演示模式并且希望之后自动禁用时，可以使用此功能。

5. 高级用户

5.1 代理服务器设置

在大型 LAN 网络中，计算机可通过代理服务器连接到 Internet。如果是这样，则需要定义以下设置。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。

要指定此级别的代理服务器设置，请选中使用代理服务器复选框，然后将代理服务器地址和代理服务器的端口号输入代理服务器字段以及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复选框，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按钮，自动检测和填充代理服务器设置。将复制在 Internet Explorer 中指定的参数。

注意：此功能不检索验证数据（用户名和密码），它必须由您提供。

代理服务器设置也可以在高级更新设置中建立（高级设置树的更新分支）。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，因为他们经常从不同位置接收病毒库更新。有关此设置的更多信息，请参见[高级更新设置](#)部分。

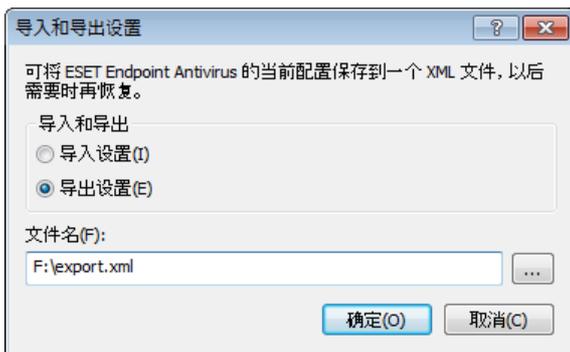
5.2 导入和导出设置

ESET Endpoint Antivirus 的导入和导出配置可在设置下找到。

导入和导出都使用 .xml 文件类型。如果需要备份 ESET Endpoint Antivirus 的当前配置以便在将来使用，导入和导出会很有用。对于想要在多个系统上使用其首选 ESET Endpoint Antivirus 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 文件来传输想要的设置。

导入配置非常简单。在主程序窗口中，单击设置 > 导入和导出设置...，然后选择导入设置选项。输入配置文件的路径，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，单击设置 > 导入和导出设置... 选择导出设置选项，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。



5.3 键盘快捷方式

使用 ESET Endpoint Antivirus 时可用的快捷方式有：

Ctrl+G	禁用产品中的 GUI
Ctrl+I	打开 ESET SysInspector 页面
Ctrl+L	打开日志文件页面
Ctrl+S	打开计划任务页面
Ctrl+Q	打开隔离区页面
Ctrl+U	打开可设置用户名和密码的对话框
Ctrl+R	将窗口重置为其默认大小和屏幕位置。

可以使用以下键盘快捷方式来更好地在 ESET 安全产品中导航：

F1	打开帮助页面
F5	打开高级设置
向上/向下键	在产品中的项目之间导航
*	展开 高级设置 树节点
-	折叠 高级设置 树节点
TAB	在窗口中移动光标
Esc	关闭活动对话框

5.4 命令行

可通过命令行启动 ESET Endpoint Antivirus 的病毒防护模块 –手动（使用 `eccls` 命令）或使用批处理（`bat`）文件启动。
ESET 命令行扫描程序用法：

```
eccls [选项...] 文件..
```

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

<code>/base-dir=FOLDER</code>	从“文件夹 加载模块
<code>/quar-dir=FOLDER</code>	隔离“文件夹”
<code>/exclude=MASK</code>	不扫描与掩码匹配的文件
<code>/subdir</code>	扫描子文件夹（默认）
<code>/no-subdir</code>	不扫描子文件夹
<code>/max-subdir-level=LEVEL</code>	要扫描的文件夹中的最大子文件夹层数
<code>/symlink</code>	跟踪符号链接（默认）
<code>/no-symlink</code>	跳过符号链接
<code>/ads</code>	扫描 ADS（默认）
<code>/no-ads</code>	不扫描 ADS
<code>/log-file=FILE</code>	将结果记录到“文件”
<code>/log-rewrite</code>	覆盖结果文件（默认 - 附加）
<code>/log-console</code>	将结果记录到控制台（默认）
<code>/no-log-console</code>	不将结果记录到控制台
<code>/log-all</code>	同时记录清除文件
<code>/no-log-all</code>	不记录干净的文件（默认）
<code>/aind</code>	显示活动指示器
<code>/auto</code>	扫描并自动清除所有本地磁盘中的病毒

扫描程序选项

<code>/files</code>	扫描文件（默认）
<code>/no-files</code>	不扫描文件
<code>/memory</code>	扫描内存
<code>/boots</code>	扫描引导区
<code>/no-boots</code>	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=SIZE	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=LEVEL	要扫描的压缩档（嵌套压缩档）中的最大子压缩档层数
/scan-timeout=LIMIT	扫描压缩文件超时时间（秒）
/max-arch-size=SIZE	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=SIZE	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
/adware	扫描广告软件/间谍软件/危险软件（默认）
/no-adware	不扫描广告软件/间谍软件/危险软件
/unsafe	扫描潜在的不安全应用程序
/no-unsafe	不扫描可能不安全的程序（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）
/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=EXTENSIONS	仅扫描具有指定“扩展名”的文件（用冒号分隔）
/ext-exclude=EXTENSIONS	不扫描具有指定“扩展名”的文件（用冒号分隔）
/clean-mode=MODE	对被感染的对象使用清除“模式”。
	可用选项：none、standard（默认）、strict、rigorous、delete
/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	保存上一个访问时间戳

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

注意：退出代码大于 100 表示未扫描文件，该文件可能被感染。

5.5 ESET SysInspector

5.5.1 ESET SysInspector 介绍

ESET SysInspector 是彻底检查您的计算机并全面显示所收集数据的应用程序。安装的驱动程序和应用程序、网络连接或重要注册表项等信息有助于调查因软件或硬件不兼容或恶意软件感染引起的可疑系统行为。

有两种方式可用来访问 ESET SysInspector：从 ESET Security 解决方案中的集成版本或从 ESET 网站免费下载单机版本 (SysInspector.exe)。两种版本的功能一致且有相同的程序控件。唯一的区别是管理输出的方式不同。无论独立的还是集成的版本都允许您将系统快照输出为 .xml 文件并保存至磁盘。但是，集成的版本还允许您直接在工具 > ESET SysInspector 中存储系统快照 (ESET Remote Administrator 除外)。

ESET SysInspector 扫描计算机时需要一些时间。可能花费 10 秒到几分钟，这取决于硬件配置、操作系统和计算机上安装的应用程序数量。

5.5.1.1 启动 ESET SysInspector

若要启动 ESET SysInspector，只需运行从 ESET 网站下载的 SysInspector.exe 可执行文件。

应用程序检查您的系统时，可能需要几分钟，请稍作等待，具体取决于要收集的硬件和数据。

5.5.2 用户界面和应用程序的使用

为了方便使用，主窗口被划分为四个主要部分 - 主窗口顶端的程序控件，左侧的导航窗口，位于右中位置说明窗口以及位于右下位置详细信息窗口。日志状态部分列出了日志的基本参数 (过滤器使用、过滤器类型以及日志是否为比较结果等)。

进程	路径	PID	用户名
进程信息			
System Idle Process		0	
System		4	
smss.exe		260	
csrss.exe		360	
csrss.exe		412	
wininit.exe		420	
winlogon.exe		468	
services.exe		516	
lsass.exe		524	
lsm.exe		532	
svchost.exe		632	
svchost.exe		716	

属性	值
SHA1	A81B48A5D6A06543ED36B7E6EA75C5E52B79DD37
最后写入时间	2009/07/14 03:14
创建时间	2009/07/14 01:11
文件大小	69632
文件说明	Windows Session Manager
公司名称	Microsoft Corporation
文件版本	6.1.7600.16395 (x-ww-090713-1250)

5.5.2.1 程序控件

本部分包含 ESET SysInspector 中所有可用程序控件的说明。

文件

单击文件即可存储当前的日志状态以供将来研究使用，或者打开一个先前存储的日志。对于发布用途，我们建议生成适合发送的日志。这种形式的日志会省略敏感信息（当前用户名、计算机名称、域名、当前用户权限、环境变量等）。

注意： 只需将先前存储的 ESET SysInspector 报告拖放至主窗口，即可将其打开。

树

允许您展开或关闭所有节点，并将选定部分导出到服务脚本中。

名单

包含使您能在程序内更方便地导航的功能，以及诸如在线查找信息等各种其他功能。

帮助

包含应用程序及其功能的相关信息。

详细信息

此设置影响主窗口中显示的信息，使信息更容易使用。在 **基本** 模式下，您可以访问查找系统常见解决方法所需的信息。在 **中等** 模式下，程序显示较少使用的详细信息。在 **完整** 模式下，ESET SysInspector 显示解决非常具体问题所需的信息。

项目过滤

项目过滤是查找系统中可疑文件或注册表项的最佳方式。通过调整滑块，您可以按风险级别来过滤项目。如果将滑块设定到最左侧（风险级别 1），则会显示所有项目。而将滑块移至右侧，程序将会滤除危险程度低于当前风险级别的所有项目，只显示比显示级别更可疑的项目。若将滑块移至最右侧，程序将仅显示已知的有害项目。

所有标记为风险 6 至 9 的项目可能具有安全风险。如果您未使用 ESET 的安全解决方案，我们建议您在 ESET SysInspector 找到任何此类项目后，使用 [ESET Online Scanner](#) 来扫描您的系统。ESET Online Scanner 是免费服务。

注意： 将项目颜色与风险级别滑块上的颜色进行比较，可以迅速确定项目的风险级别。

搜索

搜索用于通过项目名称或部分名称来快速查找特定项目。搜索请求的结果将会显示在 **说明** 窗口中。

返回

通过单击后退或前进箭头，您可以在说明窗口中返回先前显示的信息。您可以使用 Backspace 和空格键而不是单击后退和前进。

状态部分

显示导航窗口中的当前节点。

重要信息： 突出显示为红色的项目为未知项目，这也正是程序将其标记为潜在危险项目的原因。项目为红色并不一定就意味着您可以将文件删除。删除前，请确保文件确实是危险的或是不需要的。

5.5.2.2 ESET SysInspector 导航

ESET SysInspector 将各种类型的信息划分到一些称为节点的基本部分中。如果可用，您可以通过扩展各个节点到其子节点中来查找其他详细信息。若要打开或折叠某节点，双击节点的名称或单击  或该节点名称旁边的 。当在 导航 窗口中浏览节点和子节点的树结构时，您可能在 说明 窗口中找到有关每个节点的各种详细信息。如果在说明窗口中浏览项目，有关每个项目的其他详细信息可能会显示在详细信息窗口中。

下面是 导航 窗口中主要节点的说明，以及 说明 和 详细信息 窗口中的相关信息。

运行进程

该节点包含生成日志时运行的应用程序和进程的相关信息。在说明窗口中，您可以找到有关每个进程的其他详细信息，例如由进程使用的动态库及其在系统中的位置、应用程序供应商的名称、文件的风险级别。

详细信息窗口包含说明窗口中选定项目的其他信息，例如文件大小或其 Hash 信息。

注意： 操作系统包含若干重要内核组件，它们会全天候运行并为其他用户应用程序提供基本和关键功能。在某些情况下，此类进程会显示在 ESET SysInspector 工具中，文件路径以 \??\ 开头。这些符号为这些进程提供预启动优化；它们对系统是安全的。

网络连接

说明窗口包含进程和应用程序的列表，这些进程和应用程序使用在导航窗口中选择的协议（TCP 或 UDP）的网络以及应用程序连接到的远程地址进行通讯。您还可以检查 DNS 服务器的 IP 地址。

详细信息窗口包含说明窗口中选定项目的其他信息，例如文件大小或其 Hash 信息。

重要注册表项

包含通常与各种系统问题相关的一系列选定注册表项，例如指定启动程序、浏览器帮助程序对象 (BHO) 等的注册表项。

在 说明 窗口中，可以找到哪些文件与特定注册表项相关。您可以在详细信息窗口中查看其他详细信息。

服务

说明 窗口包含注册为 Windows Services 的文件列表。在 详细信息 窗口中可以检查服务的启动设置方法以及文件的特定详细信息。

驱动程序

系统中安装的驱动程序列表。

关键文件

说明窗口显示与 Microsoft Windows 操作系统相关的关键文件的内容。

系统计划任务

包含 Windows 计划任务在指定时间/间隔触发的任务列表。

系统信息

包含有关硬件和软件的详细信息以及有关设置环境变量、用户权限和系统事件日志的信息。

文件详细信息

重要系统文件和 Program Files 文件夹中文件的列表。特定于文件的其他信息可以在说明和详细信息窗口中找到。

关于

关于 ESET SysInspector 版本和程序模块列表的信息。

5.5.2.2.1 键盘快捷方式

使用 ESET SysInspector 时可用的快捷键有：

文件

Ctrl+O 打开现有日志
Ctrl+S 保存已创建的日志

生成

Ctrl+G 生成标准计算机状态快照
Ctrl+H 生成计算机状态快照并记录日志敏感信息

项目过滤

1, O 良好，显示风险级别为 1-9 的项目
2 良好，显示风险级别为 2-9 的项目
3 良好，显示风险级别为 3-9 的项目
4, U 未知，显示风险级别为 4-9 的项目
5 未知，显示风险级别为 5-9 的项目
6 未知，显示风险级别为 6-9 的项目
7, B 危险，显示风险级别为 7-9 的项目
8 危险，显示风险级别为 8-9 的项目
9 危险，显示风险级别为 9 的项目
- 降低风险级别
+ 提高风险级别
Ctrl+9 过滤模式，相等或更高级别
Ctrl+0 过滤模式，仅相等级别

查看

Ctrl+5 按供应商查看，所有供应商
Ctrl+6 按供应商查看，仅 Microsoft
Ctrl+7 按供应商查看，所有其他供应商
Ctrl+3 显示完整的详细信息
Ctrl+2 显示中等详细信息
Ctrl+1 基本显示
BackSpace 后退一步
空格 前进一步
Ctrl+W 扩展树
Ctrl+Q 折叠树

其他控件

Ctrl+T 在搜索结果中选择后，转至项目的原始位置
Ctrl+P 显示项目的基本信息
Ctrl+A 显示项目的完整信息
Ctrl+C 复制当前项目的树
Ctrl+X 复制项目
Ctrl+B 在 Internet 上查找选定文件的相关信息
Ctrl+L 打开选定文件所在的文件夹
Ctrl+R 在注册表编辑器中打开相应注册表项
Ctrl+Z 复制文件路径（如果该项目与文件相关）
Ctrl+F 切换至搜索字段
Ctrl+D 关闭搜索结果
Ctrl+E 运行服务脚本

比较

Ctrl+Alt+O	打开原始/比较日志
Ctrl+Alt+R	取消比较
Ctrl+Alt+1	显示所有项目
Ctrl+Alt+2	仅显示已添加的项目，日志将显示当前日志中的项目
Ctrl+Alt+3	仅显示已删除的项目，日志将显示以前的日志中的项目
Ctrl+Alt+4	仅显示已替换的项目（含文件）
Ctrl+Alt+5	仅显示日志之间的差异
Ctrl+Alt+C	显示比较
Ctrl+Alt+N	显示当前日志
Ctrl+Alt+P	打开以前的日志

其他

F1	查看帮助
Alt+F4	关闭程序
Alt+Shift+F4	关闭程序而不询问
Ctrl+I	日志统计信息

5.5.2.3 比较

比较功能允许用户比较两个现有日志。该功能的输出结果是一组这两个日志并不共有的项目。如果您想跟踪系统中的变化，则这是比较合适的，它是检测恶意代码活动的有用工具。

在启动之后，应用程序会创建新日志并显示在新窗口中。导航至文件 > 保存日志，将日志保存到文件。稍后可打开并查看日志文件。若要打开现有日志，请使用文件 > 打开日志。在主程序窗口中，ESET SysInspector 始终一次显示一个日志。

比较两个日志的好处是可以查看当前活跃日志和文件中保存的日志。若要比较日志，请使用文件 > 比较日志选项，并选择选择文件。将在主程序窗口中比较活动日志与选定日志。比较日志将仅显示这两个日志之间的区别。

注意：如果比较两个日志文件，请选择文件 > 保存日志，并将其另存为 ZIP 文件，则会保存这两个文件。如果稍后打开此类文件，将自动比较包含的日志。

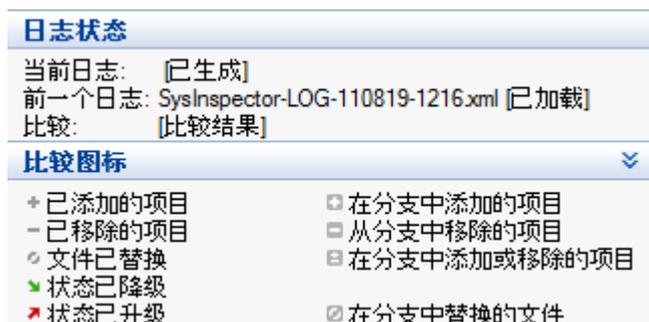
在显示项目的旁边，ESET SysInspector 将显示标识所比较日志之间的差别的标记。

由 - 标记的项目只能在活动日志中找到，并不显示在打开的比较日志中。由 + 标记的项目仅显示在打开的日志中，并不显示在活动日志中。

所有标记的说明可显示在项目旁边：

- + 以前日志中没有出现的新值
- 包含新值的树结构部分
- - 仅在以前日志中出现的已删除的值
- 包含已删除的值的树结构部分
- 值/文件已经更改
- 包含已修改的值/文件的树结构部分
- 风险级别已经降低/上一个日志中更高
- 风险级别已经提高/上一个日志中更低

左下角显示的说明部分介绍了所有标记，还显示了所比较的日志的名称。



任何比较日志都可以保存到文件并在稍后打开。

示例

生成记录有关系统原始信息的日志，并保存到名为 previous.xml 的文件。对系统进行更改之后，打开 ESET SysInspector 并使其生成新日志。将其保存到名为 current.xml 的文件。

为了跟踪这两个日志之间的更改，请浏览至文件 > 比较日志。该程序将创建比较日志，显示日志之间的差别。

如果使用以下命令行选项，也可得到相同的结果：

```
SysInspector.exe current.xml previous.xml
```

5.5.3 命令行参数

ESET SysInspector 支持从命令行使用这些参数生成报告：

/gen	直接从命令行生成日志，而无需运行 GUI
/privacy	生成不包含敏感信息的日志
/zip	以压缩文件的形式直接在磁盘上存储生成的日志
/silent	不显示日志生成进度条
/help, /?	显示有关命令行参数的信息

示例

若要将特定日志直接加载到浏览器中，请使用：SysInspector.exe "c:\clientlog.xml"

若要在当前位置中生成日志，请使用：SysInspector.exe /gen

若要在特定文件夹中生成日志，请使用：SysInspector.exe /gen="c:\folder\"

若要在特定文件/位置中生成日志，请使用：SysInspector.exe /gen="c:\folder\mynewlog.xml"

若要直接在压缩文件中生成不包含敏感信息的日志，请使用：SysInspector.exe /gen="c:\mynewlog.zip" /privacy /zip

若要比较两个日志，请使用：SysInspector.exe "current.xml" "original.xml"

注意：如果文件/文件夹的名称包含间隔，则应放在引号内。

5.5.4 服务脚本

服务脚本轻松移除系统中有害的对象，帮助使用 ESET SysInspector 的客户。

服务脚本允许用户导出整个 ESET SysInspector 日志或其选定部分。导出后，您可以标记不需要的对象以便删除。然后运行修改后的日志来删除标记的对象。

服务脚本适用于之前有过系统问题诊断经验的用户。不符合资格的修改可能导致操作系统损坏。

示例

如果您怀疑计算机受到未被病毒防护程序检测到的病毒感染，请按下面的逐步说明执行操作：

- 运行 ESET SysInspector 来生成一个新的系统快照。
- 在左侧（在树结构中）部分中选择第一个项目，按下 Shift 键并选择最后一个项目，以标记所有项目。
- 右键单击选定对象，选择导出选定部分到服务脚本右键菜单选项。
- 选定的对象将被导出为新日志。
- 以下是整个过程中最关键的步骤：打开新日志，并将您想要删除的所有对象的 - 属性更改为 +。请确保您没有标记任何重要操作系统文件/对象。
- 打开 ESET SysInspector，单击文件 > 运行服务脚本并输入脚本路径。
- 单击确定运行脚本。

5.5.4.1 生成服务脚本

若要生成脚本，请右键单击 ESET SysInspector 主窗口菜单树（左侧窗口）中的任何项目。从右键菜单中选择导出所有部分到服务脚本选项或导出选定部分到服务脚本选项。

注意：比较两个日志时不能导出服务脚本。

5.5.4.2 服务脚本结构

在脚本标题的第一行中，可以找到关于引擎版本 (ev)、GUI 版本 (gv) 和日志版本 (lv) 的信息。您可以使用此数据跟踪生成脚本的 .xml 文件中的可能更改，并防止执行期间出现任何不一致情况。此部分脚本不应被更改。

文件的其余部分分为各节，可以编辑其中的项目（表示项目这些将由脚本处理）。通过将项目前的“#”字符替换为“+”字符，标记要处理的项目。脚本中的各节通过空行彼此分隔。每一节都带有编号和标题。

01) Running processes (运行进程)

本节包含系统中运行的所有进程列表。每个进程由 UNC 路径，进而由星号 (*) 中的 CRC 16 哈希代码标识。

示例：

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

在此示例中，选择进程 module32.exe（以“+”符号标记）；执行脚本时进程将结束。

02) Loaded modules (加载的模块)

本节列出当前使用的系统模块。

示例：

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khhbkb.dll
- c:\windows\system32\advapi32.dll
[...]
```

在此示例中，模块 khbkb.dll 由“+”标记。脚本运行时，将使用该模块识别进程并结束它们。

03) TCP connections (TCP 连接)

本节包含现有 TCP 连接的信息。

示例：

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner:
System
[...]
```

脚本运行时，将查找标记 TCP 连接中套接字的所有者，并停止套接字以释放系统资源。

04) UDP endpoints (UDP 端点)

本节包含现有 UDP 端点的信息。

示例：

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

脚本运行时，将隔离标记的 UDP 端点处套接字的所有者，并停止套接字。

05) DNS server entries (DNS 服务器条目)

本节包含当前 DNS 服务器配置的信息。

示例：

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

运行脚本时将删除标记的 DNS 服务器条目。

06) Important registry entries (重要注册表项)

本节包含重要注册表项的信息。

示例：

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
  HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
  HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

脚本执行时，标记项将被删除、减小至 0 字节或重置为默认值。应用于特定项的操作取决于项类别和特定注册表中的键值。

07) Services (服务)

本节列出系统中注册的服务。

示例：

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running,
startup: Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running,
startup: Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped,
startup: Manual
[...]
```

执行脚本时将停止并卸载标记的服务及其相关服务。

08) Drivers (驱动程序)

本节列出安装的驱动程序。

示例：

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running,
startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

执行脚本时，将停止选定的驱动程序。注意，有些驱动程序不允许停止。

09) Critical files (关键文件)

本节包含对操作系统正常工作至关重要的文件的信息。

示例：

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

选定的项目将被删除或重置为初始值。

5.5.4.3 执行服务脚本

标记所有所需项目，然后保存并关闭脚本。通过选择“文件”菜单中的运行服务脚本选项，直接从 ESET SysInspector 主窗口运行编辑的脚本。打开脚本时，程序将提示您以下消息：确定要运行服务脚本 %Scriptname% 吗？确认您的选择后可能显示另一个警告，通知您尝试运行的服务脚本尚未签名。单击运行启动脚本。

对话框将确认脚本成功执行。

如果只能部分处理脚本，将显示一个具有以下消息的对话框：服务脚本部分运行。是否要查看错误报告？选择是查看列有未执行操作的复杂错误报告。

如果脚本未被识别，将显示具有以下消息的对话框：所选服务脚本未签名。运行未签名和未知脚本可能严重危害您的计算机数据。是否确定要运行该脚本并执行操作？这可能是由脚本不一致引起的（标题损坏、节标题损坏、节之间缺少空行等）。您可以重新打开脚本文件并纠正脚本内的错误或创建新的服务脚本。

5.5.5 常见问题解答

运行 ESET SysInspector 是否需要管理员权限？

运行 ESET SysInspector 不需要管理员权限，但收集到的某些信息只能通过管理员帐户访问。以标准用户或受限制用户的身份运行它，将导致其收集的有关运行环境的信息比较少。

ESET SysInspector 是否创建日志文件？

ESET SysInspector 可以创建计算机配置的日志文件。若要保存某个日志文件，请从主菜单中选择文件 > 保存日志。日志以 XML 格式保存。默认情况下，文件会保存到 %USERPROFILE%\My Documents\ 目录，并使用 "SysInspector-%COMPUTERNAME%-YYMMDD-HHMM.XML" 文件命名约定。如果需要，可以在保存之前更改日志文件的位置和名称。

如何查看 ESET SysInspector 日志文件？

若要查看由 ESET SysInspector 创建的日志文件，请运行该程序并从主菜单中选择文件 > 打开日志。还可以将日志文件拖放到 ESET SysInspector 应用程序上。如果需要频繁查看 ESET SysInspector 日志文件，建议在桌面上创建

SYSINSPECTOR.EXE 文件的快捷方式；然后可以将日志文件拖放到其中以供查看。出于安全原因，Windows Vista/7 可能不允许在安全权限不同的窗口之间进行拖放。

规范是否可用于日志文件格式？SDK 如何？

目前，日志文件规范或 SDK 均不可用，因为程序仍在开发中。程序发布之后，我们可能会根据客户反馈和要求提供这些内容。

ESET SysInspector 如何评估由特定对象产生的风险？

在大多数情况下，ESET SysInspector 使用一系列启发式规则检查每个对象的特性并评估恶意活动的可能性，将风险级别指定给对象（文件、进程、注册表项等）。基于这些启发式扫描，会向对象指派风险级别，级别从 1 - 良好（绿色）到 9 - 危险（红色）。在左侧导航窗格中，根据所包含对象的最高风险级别，各部分有不同的颜色。

风险级别 6- 未知（红色）是否表示对象存在危险？

ESET SysInspector 的评估并不能保证对象是恶意的，这应由安全专家来确定。ESET SysInspector 旨在为安全专家提供快速评估，以使它们了解需要对系统上的哪些对象进行进一步检查，确定其是否有不正常行为。

ESET SysInspector 为什么在运行时连接到 Internet？

与许多应用程序一样，ESET SysInspector 已签署数字签名“证书”，可帮助确保该软件是 ESET 发布的，并且未进行过更改。为了验证证书，操作系统会与证书授权机构通信来验证软件发行者的身份。这是 Microsoft Windows 下通过数字签名的所有程序的正常行为。

什么是反隐藏技术？

防隐匿技术提供了有效的 Rootkit 检测。

如果系统受到行为类似 Rootkit 的恶意代码的攻击，用户将面临数据丢失或被盗的风险。如果没有专用的反 Rootkit 工具，几乎不可能检测到 Rootkit。

为什么有时标记为 ‘Signed by MS’ 的文件同时具有不同的 ‘Company Name’ 条目？

当尝试识别可执行文件的数字签名时，ESET SysInspector 首先查询文件中是否嵌入了数字签名。如果发现数字签名，将使用该信息验证文件。如果未发现数字签名，ESI 则会开始查找包含已处理可执行文件的相关信息的对应 CAT 文件（安全目录 - %systemroot%\system32\catroot）。如果找到相关的 CAT 文件，在可执行文件的验证过程中将应用该 CAT 文件的数字签名。

这就是有时文件标记为 ‘Signed by MS’，但却具有不同 CompanyName 条目的原因。

示例：

Windows 2000 包括 HyperTerminal 应用程序，位于 C:\Program Files\Windows NT 中。主应用程序可执行文件没有进行数字签名，但 ESET SysInspector 将其标记为由 Microsoft 签署的文件。这是因为在 C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat 中有一个引用指向了 C:\Program Files\Windows NT\hypertm.exe（HyperTerminal 应用程序的主要可执行文件），而 sp4.cat 则由 Microsoft 提供了数字签名。

5.5.6 ESET SysInspector 在 ESET Endpoint Antivirus 中使用

要在 ESET Endpoint Antivirus 中打开 ESET SysInspector 部分，单击工具 > ESET SysInspector。ESET SysInspector 窗口中的管理系统与计算机扫描日志或计划任务的管理系统相似。您只需通过一次或两次单击即可访问所有与系统快照有关的操作（创建、查看、比较、删除和导出）。

ESET SysInspector 窗口包含有关已创建快照的基本信息，如创建时间、简短注释、创建快照的用户名称和快照状态等。

若要比对、创建或删除快照，请使用位于 ESET SysInspector 窗口中的快照列表下方的相应按钮。您也可以通过右键菜单来使用这些选项。若要查看选定的系统快照，请使用显示右键菜单选项。若要将选定的快照导出到文件，请在此快照上单击鼠标右键并选择导出...

以下是可用选项的详细描述：

- **比较** - 允许您比较两个现有日志。它适用于您想要在当前日志和较早日志间跟踪更改时。要使此选项可用，您必须选择两个要比较的快照。
- **创建...** - 创建新记录。创建之前，您必须输入与记录有关的简短注释。要了解快照创建过程（当前生成的快照），请参见状态列表。所有完成的快照标记为已创建状态。
- **删除/全部删除** - 删除列表中的条目。
- **导出...** - 将选定的条目保存在 XML 文件中（也可保存为压缩文件）。

5.6 ESET SysRescue

ESET SysRescue 是一种实用程序，使您能够创建包含一个 ESET Security 解决方案的可引导磁盘 - 它可以是 ESET NOD32 Antivirus、ESET Smart Security 或者甚至一些面向服务器的产品。ESET SysRescue 的主要优点是 ESET Security 解决方案独立于主机操作系统运行，而它具有直接访问磁盘和整个文件系统的权限。凭借此功能，您可以删除那些通常无法删除的渗透，例如在操作系统运行时等。

5.6.1 最低要求

ESET SysRescue 在 Microsoft Windows 预安装环境 (Windows PE) 版本 2.x（基于 Windows Vista）中工作。

Windows PE 是 Windows 自动安装套件 (Windows AIK) 的一部分，因此，必须在创建 ESET SysRescue 之前安装 Windows AIK (<http://go.eset.eu/AIK>)。由于支持 32 位版本 Windows PE，在 64 位系统上创建 ESET SysRescue 时需要使用 32 位 ESET Security 解决方案。ESET SysRescue 支持 Windows AIK 1.1 及更高版本。

注意：由于 Windows AIK 的大小超过 1 GB，需要高速 Internet 连接才能顺利下载。

ESET SysRescue 在 ESET Security 解决方案 4.0 及更高版本中可用。

支持的操作系统

- Windows 7
- Windows Vista
- Windows Vista Service Pack 1
- Windows Vista Service Pack 2
- Windows Server 2008
- Windows Server 2003 Service Pack 1 with KB926044
- Windows Server 2003 Service Pack 2
- Windows XP Service Pack 2 with KB926044
- Windows XP Service Pack 3

5.6.2 如何创建急救光盘

若要启动 ESET SysRescue 向导，请单击开始 > 程序 > ESET > ESET Endpoint Antivirus > ESET SysRescue。

首先，该向导会检查是否有 Windows AIK 和引导介质创建的合适设备。如果没有在计算机上安装 Windows AIK（或者它已损坏或安装不正确），向导将为您提供选项来安装它，或输入 Windows AIK 文件夹的路径 (<http://go.eset.eu/AIK>)。

注意：由于 Windows AIK 的大小超过 1 GB，需要高速 Internet 连接才能顺利下载。

在[下一步](#)中，选择 ESET SysRescue 将定位到的目标介质。

5.6.3 目标选择

除 CD/DVD/USB 外，您还可以选择在 ISO 文件中保存 ESET SysRescue。稍后可以在 CD/DVD 上刻录 ISO 映像，或以其他方式使用它（例如在诸如 VMware 或 VirtualBox 的虚拟环境中）。

如果选择 USB 作为目标介质，可能无法在某些计算机上进行引导。某些 BIOS 版本可能报告 BIOS - 引导管理器通信问题（例如，在 Windows Vista 上），引导退出并显示以下错误消息：

```
文件 \boot\bcd  
状态 :0xc000000e  
信息 :尝试读取引导配置数据时发生错误
```

如果出现此消息，建议选择 CD 而不是 USB 介质。

5.6.4 设置

在启动 ESET SysRescue 创建之前，安装向导在 ESET SysRescue 向导的最后一步中显示编译参数。这些设置可通过单击更改...按钮进行修改。可用选项包括：

- [文件夹](#)
- [ESET Antivirus](#)
- [高级](#)
- [Internet 协议](#)
- [可引导 USB 设备](#)（选择目标 USB 设备时）
- [刻录](#)（选择目标 CD/DVD 驱动器时）

如果没有指定 MSI 安装程序包或者计算机上没有安装 ESET Security 解决方案，则创建按钮处于不活动状态。若要选择安装程序包，请单击更改按钮并转到 ESET Antivirus 选项卡。而且，如果没有填写用户名和密码（更改 > ESET Antivirus），创建按钮将灰显。

5.6.4.1 文件夹

临时文件夹是一个用于 ESET SysRescue 编译期间所需文件的工作目录。

ISO 文件夹是在编译完成之后保存生成的 ISO 文件的文件夹。

此选项卡上的列表显示所有本地和映射的网络驱动器以及可用空间。如果某些文件夹所在的驱动器可用空间不足，建议您选择具有更多可用空间的其他驱动器。否则，编译可能会由于可用磁盘空间不足而提前结束。

外部应用程序 - 允许您指定在从 ESET SysRescue 介质引导后将运行或安装的其他程序。

包括外部应用程序 - 允许您将外部程序添加到 ESET SysRescue 编译。

选定文件夹 - 定位所包含的程序将被添加到 ESET SysRescue 磁盘的文件夹。

5.6.4.2 ESET Antivirus

如果是创建 ESET SysRescue CD，则可以选择编译器要使用的两个 ESET 文件源。

ESS/EAV 文件夹 - 计算机上安装 ESET Security 解决方案的文件夹中包含的文件。

MSI 文件 - 使用 MSI 安装程序中包含的文件。

接下来，可以选择更新 (.nup) 文件的位置。通常，应设置默认选项 **ESS/EAV 文件夹/MSI 文件**。在一些情况下，可以选择自定义更新文件夹，例如，使用较旧或较新的病毒库。

您可以使用以下用户名和密码的两个源之一：

安装的 **ESS/EAV** - 用户名和密码从当前安装的 ESET Security 解决方案复制。

来自用户 - 使用相应文本框中输入的用户名和密码。

注意：ESET SysRescue CD 上的 ESET Security 解决方案从 Internet 或运行 ESET SysRescue CD 的计算机上安装的 ESET Security 解决方案更新。

5.6.4.3 高级设置

高级选项卡允许您根据计算机上的内存量优化 ESET SysRescue CD。选择 **576 MB 及更多** 可将 CD 的内容写入操作内存 (RAM)。如果选择少于 **576 MB**，则运行 WinPE 时将永久访问恢复 CD。

在外部驱动程序部分中，可以插入特定硬件（通常为网络适配器）的驱动程序。尽管 WinPE 基于支持多种硬件的 Windows Vista SP1，但有时无法识别硬件。这需要您手动添加驱动程序。有两种方法可将驱动程序引入 ESET SysRescue 编译中 - 手动（添加按钮）和自动（自动搜索按钮）。如果是手动引入，您需要选择相应 .inf 文件的路径（适用的 *.sys 文件也必须在此文件夹中）。如果是自动引入，将自动在给定的计算机的操作系统中查找驱动程序。我们建议仅当使用 ESET SysRescue 的计算机和创建 ESET SysRescue CD 的计算机具有相同网络适配器时，才使用自动引入。在创建 ESET SysRescue 期间，驱动程序会被引入到编译中，因此，用户以后将不需要单独查找它。

5.6.4.4 Internet 协议

本部分允许您配置基本网络信息并在安装 ESET SysRescue 之后设置预定义的连接。

选择自动私人 IP 地址可自动从 DHCP（动态主机配置协议）服务器获取 IP 地址。

或者，此网络连接也可以使用手动指定的 IP 地址（也称为静态 IP 地址）。选择自定义来配置适当的 IP 设置。如果选择此选项，必须指定 IP 地址，而且对于 LAN 和高速 Internet 连接，还要指定子网掩码。在首选 DNS 服务器和备用 DNS 服务器中，键入主要和次要 DNS 服务器地址。

5.6.4.5 可引导 USB 设备

如果已将选定 USB 设备作为目标介质，可以在可引导 USB 设备选项卡上选择可用 USB 设备之一（如果多个 USB 设备）。

选择适当的目标设备，将在该设备上安装 ESET SysRescue。

警告: 在创建 ESET SysRescue 过程中将格式化所选的 USB 设备。设备上的所有数据都将被删除。

如果选择快速格式化选项，格式化将从分区删除所有文件，但不会扫描磁盘是否有坏扇区。如果 USB 设备以前已格式化，而且您确信该设备未损坏，则使用此选项。

5.6.4.6 刻录

如果您已选择 CD/DVD 作为目标介质，可以在刻录选项卡上指定其他刻录参数。

删除 ISO 文件 - 选中该选项以在创建 ESET SysRescue CD 之后删除临时 ISO 文件。

启用删除 - 使您可以选择快速清除和完整清除。

刻录设备 - 选择要用于刻录的驱动器。

警告： 这是默认选项。如果使用可重新写入的 CD/DVD，将擦除 CD/DVD 上的所有数据。

介质部分包含在 CD/DVD 设备中的介质的信息。

刻录速度 - 从下拉菜单中选择所需的速度。在选择刻录速度时，应考虑刻录设备的性能和所用 CD/DVD 的类型。

5.6.5 使用 ESET SysRescue

要使急救 CD/DVD/USB 有效工作，必须从 ESET SysRescue 引导介质启动计算机。可以在 BIOS 中修改引导优先级。或者，您可以在计算机启动过程中使用引导菜单，通常使用 F9 - F12 键之一，具体取决于主板/BIOS 的版本。

从引导介质启动后，ESET Security 解决方案将启动。因为 ESET SysRescue 仅在特定的情况下使用，所以并不需要 ESET Security 标准版本解决方案中的某些防护模块和程序功能；其列表仅限于计算机扫描、更新以及设置中的某些部分。更新病毒库的能力是 ESET SysRescue 的最重要功能，我们建议您在开始计算机扫描前先更新程序。

5.6.5.1 使用 ESET SysRescue

假设网络中的计算机已被病毒感染，病毒修改了可执行文件 (.exe)。ESET Security 解决方案能够清除所有被感染文件，除了 explorer.exe，该文件无法清除，即使是在安全模式下。这是因为 explorer.exe 作为基本 Windows 进程之一，也在安全模式下启动。ESET Security 解决方案无法对该文件执行任何操作，它将保持被感染状态。

在此类情况下，您可以使用 ESET SysRescue 来解决该问题。ESET SysRescue 不需要宿主操作系统的任何组件，因此能够处理（清除、删除）磁盘上的任何文件。

6. 词汇表

6.1 渗透类型

渗透是一种试图进入和/或损坏用户计算机的恶意软件。

6.1.1 病毒

计算机病毒是一段预先附着或追加到计算机上现有文件的恶意代码。计算机病毒之所以用生物学上的“病毒”一词命名，是因为它们使用类似手法在计算机之间传播。对于“病毒”一词，通常错误用于指代任何类型威胁。这种用法正在逐渐改变，而由更为准确的术语“恶意软件”所取代。

计算机病毒主要攻击可执行文件和文档。计算机病毒的工作方式可简述如下：执行被感染文件后，在执行原始应用程序前调用并执行恶意代码。病毒可以感染当前用户具有写入权限的任何文件。

计算机病毒的目的和严重性各有不同。其中有些病毒非常危险，因为它们会故意删除硬盘驱动器上的文件。另一方面，一些病毒不造成任何破坏，它们只是骚扰用户，展示其作者的技术技巧。

如果您的计算机感染病毒而无法清除，请提交至 ESET 实验室寻求帮助。在某些情况下，被感染文件可能被修改至无法清除的程度，必须以干净副本替换文件。

6.1.2 蠕虫

计算机蠕虫是包含可通过网络攻击主机并传播的恶意代码的程序。病毒和蠕虫的基本区别在于蠕虫具有自我传播的能力，它们不依赖主机文件（或引导区）。蠕虫通过联系人列表中的电子邮件地址或利用网络应用程序中的安全漏洞进行传播。

因此，蠕虫的生存能力远超计算机病毒。由于 Internet 的广泛应用，它们可以在发布后数小时甚至数分钟内传播到世界各地。这种独立快速复制的能力使得它们比其他类型恶意软件更加危险。

在系统中激活的蠕虫会带来多种不便：它可以删除文件、降低系统性能，甚至停止程序。计算机蠕虫的特性使其适合作为其他类型渗透的“传输手段”。

如果您的计算机感染了蠕虫，建议您删除被感染文件，因为它们可能包含恶意代码。

6.1.3 木马

过去对计算机木马（特洛伊木马程序）的定义是，试图以有用程序的假面具欺骗用户运行的一类威胁。

由于木马的涵盖范围非常广，因此常被分为许多子类别：

- Downloader - 一种能够从 Internet 下载其他威胁的恶意程序。
- Dropper - 一种能够将其他类型恶意软件放入所破坏的计算机的恶意程序
- Backdoor - 一种与远程攻击者通信，允许其获得系统访问权并控制系统的恶意程序。
- Keylogger -（按键记录程序），一种记录用户键入的每个按键并将信息发送给远程攻击者的程序。
- Dialer - 一种用于连接附加计费号码而不是用户的 Internet 服务提供商的恶意程序。用户几乎无法注意到新连接的创建。Dialer 只能对使用拨号调制解调器（现在已很少使用）的用户造成破坏。

如果计算机上的文件被检测为木马，建议您将其删除，因为它极有可能包含恶意代码。

6.1.4 Rootkit

Rootkit 是一种恶意程序，它能在隐瞒自身存在的同时赋予 Internet 攻击者不受限制的系统访问权。访问系统（通常利用系统漏洞）后，Rootkit 可使用操作系统中的功能避开病毒防护软件的检测：它们能够隐藏进程、文件和 Windows 注册表数据。有鉴于此，几乎无法使用普通测试技术检测到它们。

有两种检测级别可阻止 Rootkit：

1. Rootkit 试图访问系统时。它们还未出现，因此处于不活动状态。大部分病毒防护系统能够清除此级别的 Rootkit（假定系统实际检测到此类文件被感染）。
2. 隐藏自己而不被一般测试检测到它们时。ESET Endpoint Antivirus 用户可以利用反隐藏技术，该技术还能够检测并清除活动的 Rootkit。

6.1.5 广告软件

广告软件是可支持广告宣传的软件的简称。显示广告资料的程序便属于这一类别。广告软件应用程序通常会在 Internet 浏览器中自动打开一个包含广告的新弹出窗口，或者更改浏览器主页。广告软件经常与免费软件程序捆绑在一起，以填补其开发人员开发应用程序（通常为有用程序）的成本。

广告软件本身并不危险 – 用户仅会受到广告的干扰。广告软件的危险在于它也可能执行跟踪功能（和间谍软件一样）。

如果您决定使用免费软件产品，请特别注意安装程序。安装程序大多会通知您将要安装附加的广告软件程序。通常您可以取消它，仅安装不带有广告软件的程序。

如果不安装广告软件，某些程序可能无法安装，或者功能受到限制。这意味着，广告软件可能常常以“合法”方式访问系统，因为用户已同意安装它。在此情况下，应防患于未然。如果计算机上的某个文件被检测为广告软件，我们建议您删除它，因为该软件极有可能包含恶意代码。

6.1.6 间谍软件

此类别包括所有在未经用户同意/了解的情况下发送私人信息的应用程序。间谍软件使用跟踪功能发送各种统计数据，例如所访问网站的列表、用户联系人列表中的电子邮件地址或记录按键的列表。

间谍软件的作者宣称，这些技术旨在更好地了解用户需求和兴趣，从而使广告更有针对性。问题在于，有用和恶意的应用程序之间并没有明显的差别，任何人都无法确保检索到的信息不会被滥用。间谍软件应用程序获得的数据可能包括安全代码、PIN、银行帐号等。程序的作者通常将间谍软件与其免费版本程序捆绑，以获取收益或促使用户购买软件。通常情况下，程序在安装时会告知用户存在间谍软件，以促使其将软件升级为不带间谍软件的付费版本。

比如 P2P（点对点）网络客户端应用程序就是著名的捆绑了间谍软件的免费软件产品。Spyfalcon 或 Spy Sheriff（以及更多）属于特定的间谍软件子类别 – 它们看上去象间谍软件防护程序，实际上其本身就是间谍软件程序。

如果计算机上的某个文件被检测为间谍软件，我们建议您删除它，因为该软件极有可能包含恶意代码。

6.1.7 潜在的不安全应用程序

许多合法程序可用于简化联网计算机的管理。然而，不法之徒可能将其滥用为恶意目的。ESET Endpoint Antivirus 提供检测此类威胁的选项。

潜在的不安全应用程序是指用于商业目的的合法软件。其中包括远程访问工具、密码破解应用程序以及按键记录器（用于记录用户键盘输入信息）等程序。

如果您发现计算机上存在且正在运行潜在的不安全应用程序（而您并没有安装它），请咨询您的网络管理员或删除该应用程序。

6.1.8 潜在的不受欢迎应用程序

潜在的不受欢迎应用程序 (PUA)未必是恶意的，但可能会对计算机性能造成不良影响。此类应用程序通常会在安装前提请用户同意。如果计算机上安装了这类程序，系统运行（与安装前相比）会有所不同。其中最显著的变化是：

- 以前没见过的新窗口（弹出窗口、广告），
- 启动并运行隐藏的进程，
- 系统资源的使用增加，
- 搜索结果发生改变，
- 应用程序会与远程服务器通信。

6.2 电子邮件

电子邮件是一种具有许多优点的现代通信方式。它灵活、快速、直接，在 20 世纪 90 年代初 Internet 的迅速发展起到了至关重要的作用。

不幸的是，由于其高度的匿名性，电子邮件和 Internet 为垃圾邮件等非法活动留下了空间。垃圾邮件包括不请自来的广告、恶作剧和恶意软件的传播。因发送垃圾邮件的成本极低，并且垃圾邮件作者拥有许多用于获取新电子邮件地址的工具，这些因素增加了电子邮件给您带来的不便和危险。此外，垃圾邮件的数量和种类之多使得它难以管理。您使用电子邮件地址的时间越长，该地址进入垃圾邮件引擎数据库的可能性就越大。下面是一些用于预防垃圾邮件的提示：

- 尽量避免在 Internet 上发布您的电子邮件地址
- 仅向信任的个人提供您的电子邮件地址
- 尽量不要使用常用别名 - 使用更复杂的别名，跟踪的可能性将降低
- 不要回复已经进入您的收件箱的垃圾邮件
- 填写 Internet 表单时请小心 - 尤其小心 是，我希望收到信息。 之类的选项
- 使用 专用 电子邮件地址 - 例如，一个用于工作，一个用于和您的朋友通信等等
- 不时地更改您的电子邮件地址
- 使用反垃圾邮件解决方案

6.2.1 广告

Internet 广告是发展最迅速的广告形式之一。其主要营销优势在于成本最低、非常直接；而且，邮件几乎是立刻送达。许多公司使用电子邮件营销工具有效地与现有客户和潜在客户沟通。

这种类型的广告是合法的，因为您可能希望收到关于某些产品的商业信息。但许多公司发送大量不请自来的商业邮件。在这种情况下，电子邮件广告就演变成了垃圾邮件。

大量不请自来的电子邮件就成了问题，而且毫无缓解的迹象。不请自来的电子邮件的作者经常试图将垃圾邮件伪装成合法邮件。

6.2.2 恶作剧

恶作剧是通过 Internet 传播的错误信息。恶作剧通常通过电子邮件或类似 ICQ 和 Skype 的通信工具发送。邮件内容通常是笑话或都市传奇。

计算机病毒恶作剧试图在收件人中产生恐惧、不确定和怀疑情绪 (FUD)，使他们相信有一个 无法检测的病毒 正在删除文件和检索密码，或者对他们的系统执行一些其他有害活动。

一些恶作剧要求收件人将邮件转发给其联系人，从而继续传播恶作剧。恶作剧包括手机恶作剧、请求帮助、他人要求从海外寄钱给您等。通常无法确定创建者的意图。

如果您看到邮件提示您转发给认识的每个人，这很可能是恶作剧。Internet 上的许多网站都可以验证电子邮件是否合法。在转发前，请对您怀疑是恶作剧的任何邮件执行 Internet 搜索。

6.2.3 欺诈

术语 欺诈 定义了一种利用社会工程学技术（为获得机密信息而操控用户）进行犯罪的行为。其目的是获得银行帐号、PIN 码等敏感数据的访问权限。

通常，攻击者通过冒充可信赖的个人或企业（比如金融机构、保险公司）发送电子邮件而获得访问权限。这类电子邮件的外观非常逼真，其中包含的图片和内容可能来自于被仿冒对象的原始来源。信中会以各种借口（数据验证、财务运作等）要求您输入一些个人数据，如银行帐号或用户名和密码等。如果提交，所有这类数据都可能被盗用和滥用。

银行、保险公司和其他合法的公司从来不会要求用户在不请自来的电子邮件中输入用户名和密码。

6.2.4 识别垃圾邮件欺骗

通常，一些标志可以帮助您识别邮箱中的垃圾邮件（不请自来的电子邮件）。如果邮件至少满足以下部分条件，则很可能是垃圾邮件。

- 发件人地址不属于您的联系人列表中的任何人。
- 向您提供大笔金额，但您必须先提供少量金额。
- 信中会以各种借口（数据验证、财务运作等）要求您输入您的一些个人数据，比如银行帐号、用户名和密码等。
- 以外语撰写。
- 要求您购买您不感兴趣的产品。如果您决定购买，请验证邮件发件人是否为可靠供应商（咨询原始产品制造商）。
- 部分词语拼写错误，试图欺骗您的垃圾邮件过滤器。例如，将 Viagra 拼写成 Vaigra 等。