ENDPOINT ANTIVIRUS
FOR WINDOWS

用户指南

Microsoft® Windows® 10/8.1/8/7/Vista
单击此处以下载本文档的最新版本

ENJOY SAFER TECHNOLOGY™

ESET ENDPOINT ANTIVIRUS 7

ESET Endpoint Antivirus 由 ESET, spol. s r. o. 开发
有关更多信息，请访问 www.eset.com。

全球客户支持 www.eset.com/support

修订日期 2018/8/16

目录

目录

1. ESET Endpoint Antivirus 7

ESET Endpoint Antivirus 7 代表了真正集成计算机安全的新方法。最新版本的 ThreatSense® 扫描引擎提高了速度和精确性，以便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 7 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 7 主要设计用于小型商业环境中的工作站。在企业环境中将 ESET Endpoint Antivirus 与 ESET Remote Administrator 结合使用，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、监视检测以及从任何联网计算机远程配置客户端。

1.1 系统需求

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

支持的处理器：

- 32 位 (x86) 或 64 位 (x64) 处理器，1 GHz 或更高

操作系统： Microsoft® Windows® 10/8.1/8/7/Vista

?安装了受所选 ESET 产品版本支持的操作系统和必需 Service Pack
?满足安装在计算机上的操作系统和其他软件的系统要求
- 0.3 GB 的可用系统内存（请参阅注释 1）
  1 GB 的可用磁盘空间（请参阅注释 2）
?最小显示器分辨率 1024x768
?产品更新的 Internet 连接或到源的局域网连接（请参阅注释 3）

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

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

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攻击 .要提供最大保护和便利，正确使用病毒防护解决方案和遵守一些有用规则非常重要：

定期更新

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

下载安全补丁

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

备份重要数据

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

定期扫描计算机、查找病毒

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

遵循基本安全规则

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

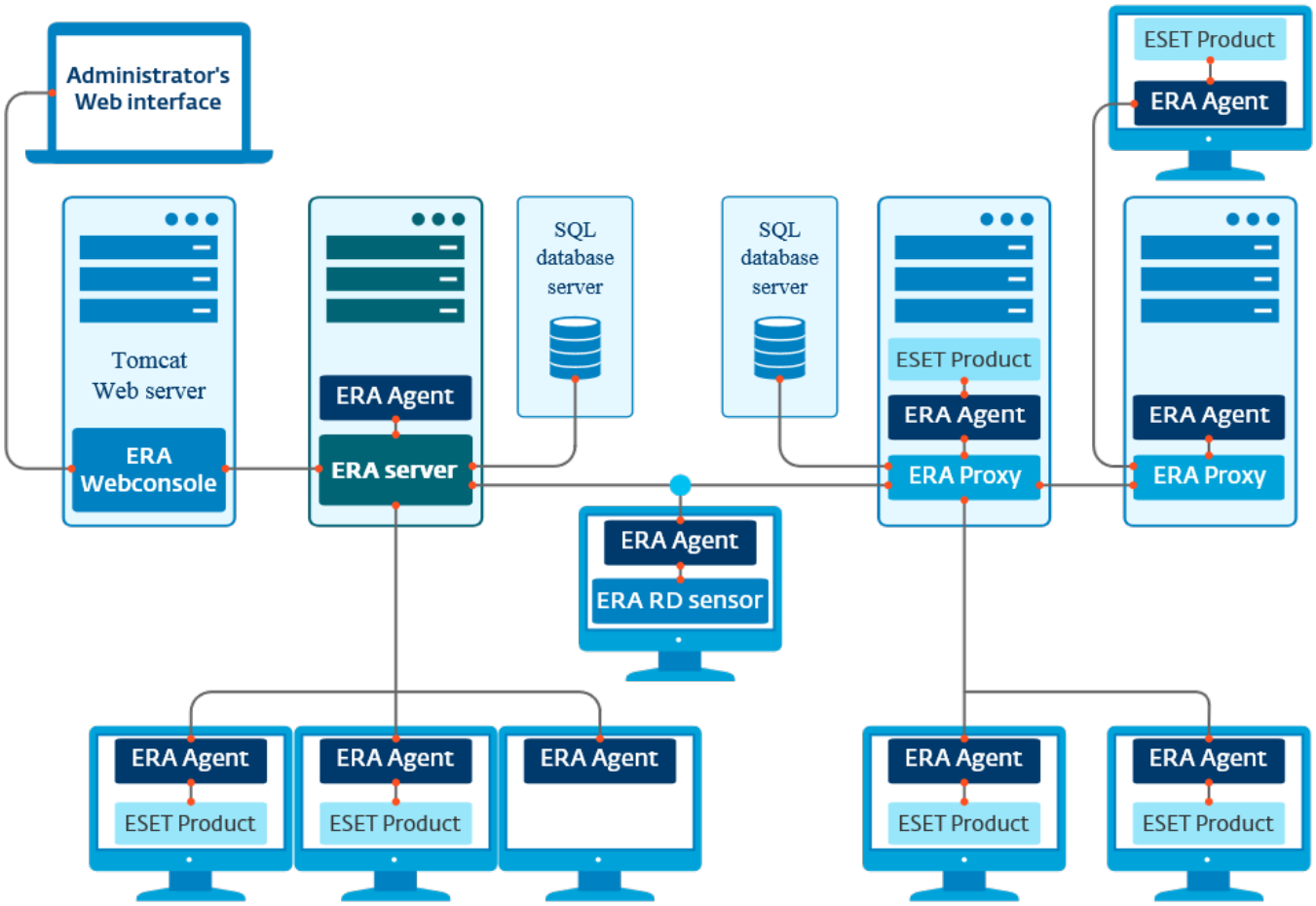
- 不访问带有多个弹出窗口和闪烁广告的可疑网站。
- 谨慎安装免费软件、代码包等。只使用安全的程序，只访问安全的 Internet 网站。
- 谨慎打开电子邮件附件，尤其是批量发送的邮件和来自陌生发件人的邮件。
- 不要使用管理员帐户执行计算机的日常工作。

2. 面向通过 ESET Remote Administrator 连接的用户的文档

ESET Remote Administrator (ERA) 是一个应用程序，它允许您从一个中心位置管理网络环境中的 ESET 产品。此 ESET Remote Administrator 任务管理系统允许您在远程计算机上安装 ESET 安全解决方案并且快速响应新问题和威胁。ESET Remote Administrator 自身不提供对恶意代码的防护，它依赖于每个客户端上是否存在 ESET 安全解决方案。

ESET 安全解决方案支持包括多个平台类型的网络。您的网络可以包括当前可在移动设备（手机和平板电脑）上运行的 Microsoft 操作系统、基于 Linux 的操作系统、Mac OS 操作系统的组合。

下图描绘了由 ERA 托管的 ESET 安全解决方案保护的示例网络架构：



注意
有关详细信息，请参阅 ESET Remote Administrator 联机帮助。

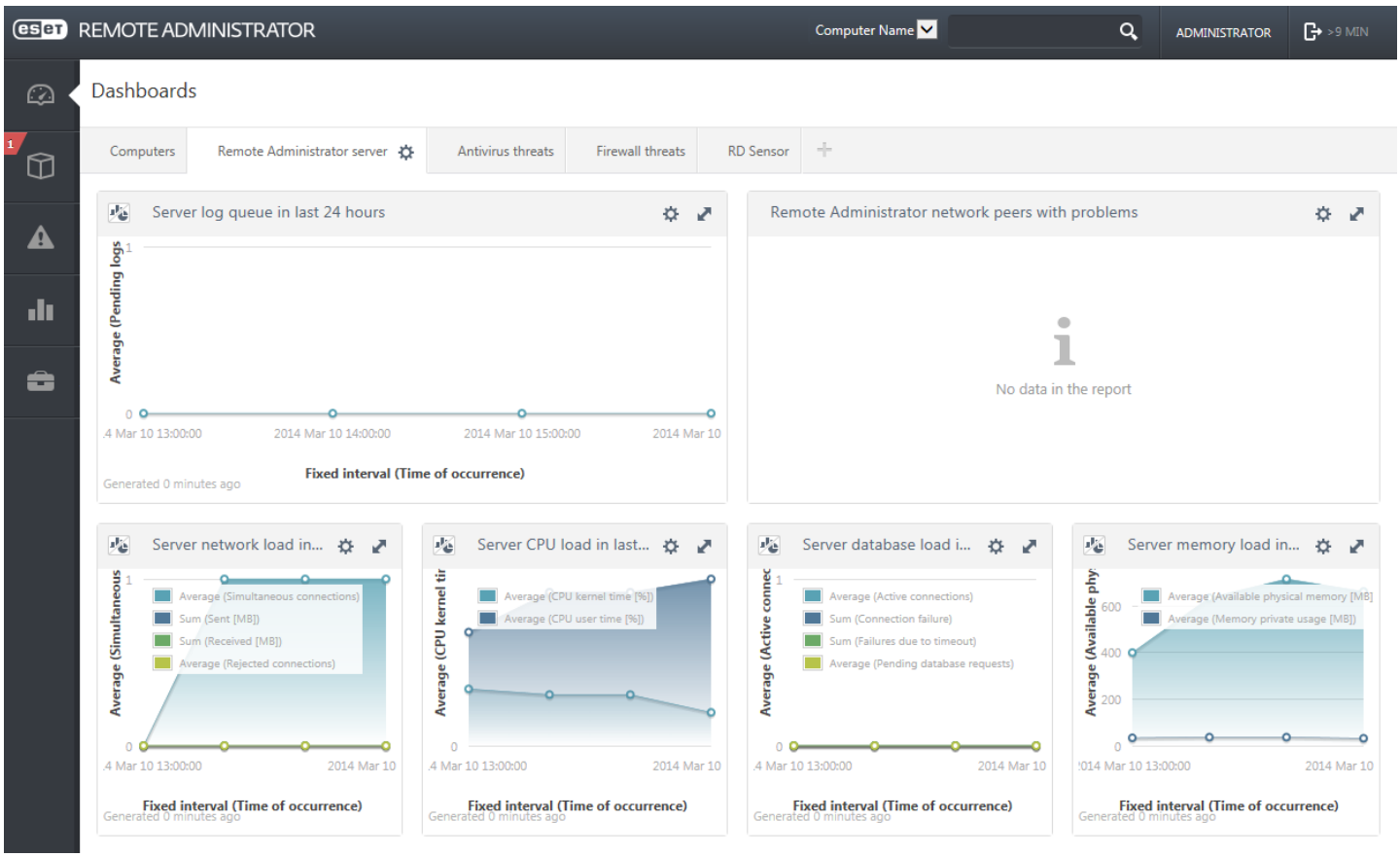
2.1 ESET Remote Administrator Server

ESET Remote Administrator Server 是 ESET Remote Administrator 的一个主要组件。它是可执行应用程序，用于处理从连接到服务器（通过 ERA 服务器代理）的客户端接收的所有数据。ERA 服务器代理将有助于客户端和服务器之间的通信。数据（客户端日志、配置、服务器代理复制等）将存储在数据库中。若要正确处理数据，则 ERA Server 需要稳定地连接到数据库服务器。我们建议将 ERA Server 和您的数据库安装在不同的服务器上以优化性能。必须将装有 ERA Server 的计算机配置为接受所有已通过证书验证的服务器代理 代理 RD Sensor 连接。安装后，您可以打开连接到 ERA Server 的 ERA Web 控制台（如示意图中所示）。在您的网络内管理 ESET 安全解决方案时，所有的 ERA Server 操作都将通过 Web 控制台执行。

2.2 Web 控制台

ERA Web 控制台是一个基于 Web 的用户界面，它可以显示来自 ERA 服务器的数据并允许您在网络中管理 ESET 安全解决方案。可以使用浏览器访问 Web 控制台。它将显示您网络上的客户端状态的概述，并可用于将 ESET 解决方案远程部署到未托管的计算机。您可以选择使 Web 服务器可通过 Internet 进行访问，以允许几乎可以从任何地点或设备使用 ESET Remote Administrator。

下面是 Web 控制台的面板：



快速搜索工具位于 Web 控制台的顶部。从下拉菜单中选择**计算机名称**？**IPv4/IPv6 地址**或**威胁名称**、在文本字段内键入搜索字符串，然后单击放大镜符号或按 **Enter** 以进行搜索。您将重定向到用于显示搜索结果的**组**部分。

注意
有关详细信息，请参阅 ESET Remote Administrator 联机帮助。

2.3 代理

ERA 代理是 ESET Remote Administrator 的另一个组成部分，它有两种用途。在具有许多客户端（例如，10,000 个客户端或更多）的中型网络或企业网络中，您可以使用 ERA 代理在多个 ERA 代理之间分发负载，从而提高主 ERA 服务器的效率。ERA 代理的另一个优点在于，当您要连接到易出故障的远程分支机构时，可以使用它。这意味着每个客户端上的 ERA 服务器代理不会通过 ERA 代理（位于与分支机构相同的本地网络上）直接连接到主 ERA 服务器。此配置释放了指向分支机构的链接。ERA 代理接受来自所有本地 ERA 服务器代理的连接，然后编译来自它们的数据并将其上载到主 ERA 服务器（或其他 ERA 代理）。这可让您的网络在不影响网络和数据库查询性能的情况下容纳更多客户端。

ERA 代理可能会连接到其他 ERA 代理，然后连接到主 ERA 服务器，具体取决于您的网络配置。

为保证 ERA 代理的正常运行，安装 ERA 代理的主机上必须装有 ESET 服务器代理，且必须连接到您网络中较高级别的 ERA 服务器或较高级别的 ERA 代理（如果存在）。

2.4 服务器代理

ERA 服务器代理是 ESET Remote Administrator 产品的重要部分。客户端计算机上的 ESET 安全解决方案（例如 ESET Endpoint Security）通过该代理与 ERA 服务器通信。此通信允许您从一个中心位置管理所有远程客户端上的 ESET 安全解决方案。服务器代理从客户端收集信息并将它发送到服务器。在服务器将任务发送到客户端后，该任务将发送到与客户端通信的服务器代理。所有网络通信均在服务器代理和 ERA 网络的上半部分（服务器和代理）之间进行。

ESET 服务器代理使用以下三种方法之一来连接服务器：

1. 客户端的服务器代理直接连接到服务器。
2. 客户端的服务器代理通过连接到服务器的代理进行连接。
3. 客户端的服务器代理通过多个代理连接到服务器。

ESET 服务器代理与安装在客户端上的 ESET 解决方案通信、从该客户端上的程序收集信息，并将从服务器接收的配置信息传递给客户端。

注意
ESET 代理有自己的服务器代理，它可以处理客户端、其他代理和服务器之间的所有通信任务。

2.5 RD Sensor

RD (Rogue Detection) Sensor 是 ESET Remote Administrator 的一部分，旨在查找您网络上的计算机。它提供了向 ESET Remote Administrator 添加新计算机的简便方法，使您无需手动查找和添加它们。在您网络上找到的每台计算机都将在 Web 控制台中显示，并且将添加到默认的**全部**组中。在此处，您可以对单个客户端计算机采取进一步的操作。

RD Sensor 是一个被动的侦听器，用于检测网络上存在的计算机并将有关它们的信息发送到 ERA Server。ERA 服务器将评估在网络上发现的计算机是否处于未知状态，或者是否已被托管。

3. 单独使用 ESET Endpoint Antivirus

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

3.1 通过 ESET AV Remover 安装

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

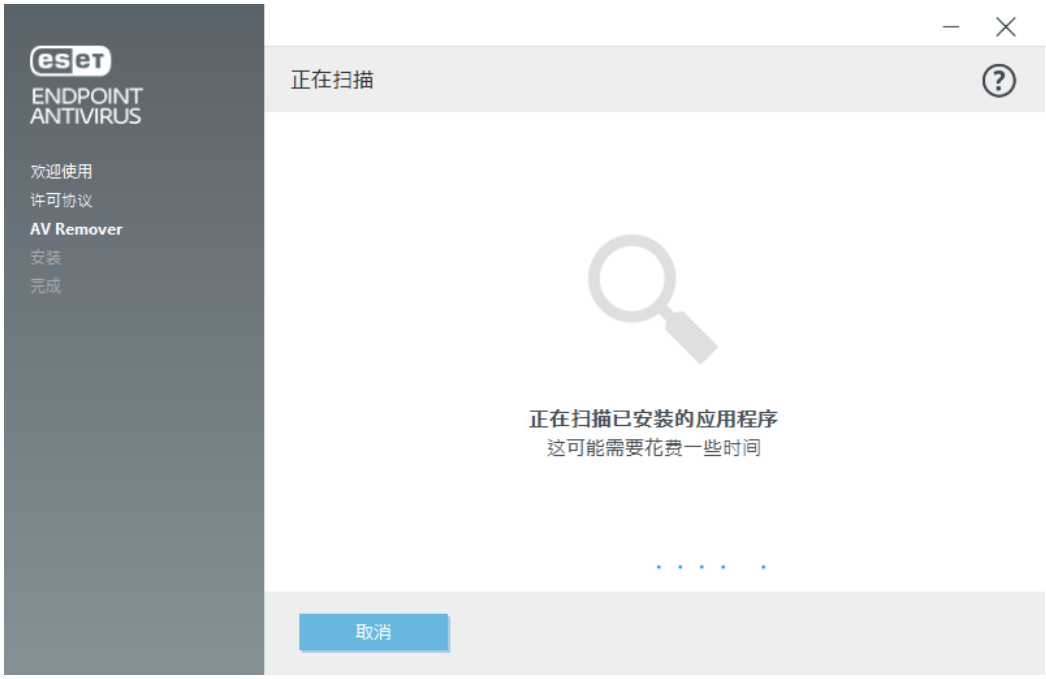
3.1.1 ESET AV Remover

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

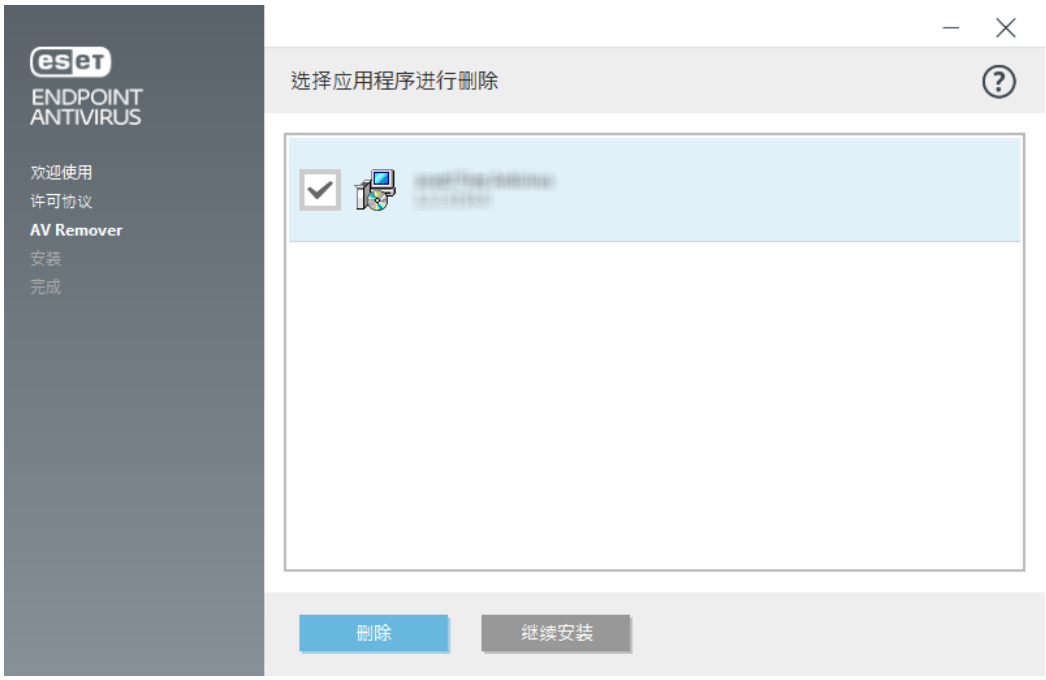
1. 若要查看 ESET AV Remover 可以删除的病毒防护软件的列表，请访问 ESET 知识库文章。 下载 ESET AV Remover 独立工具。

2. 阅读最终用户许可协议并单击**接受**，以确认接受。 单击**拒绝**将终止在计算机上删除现有安全应用程序。

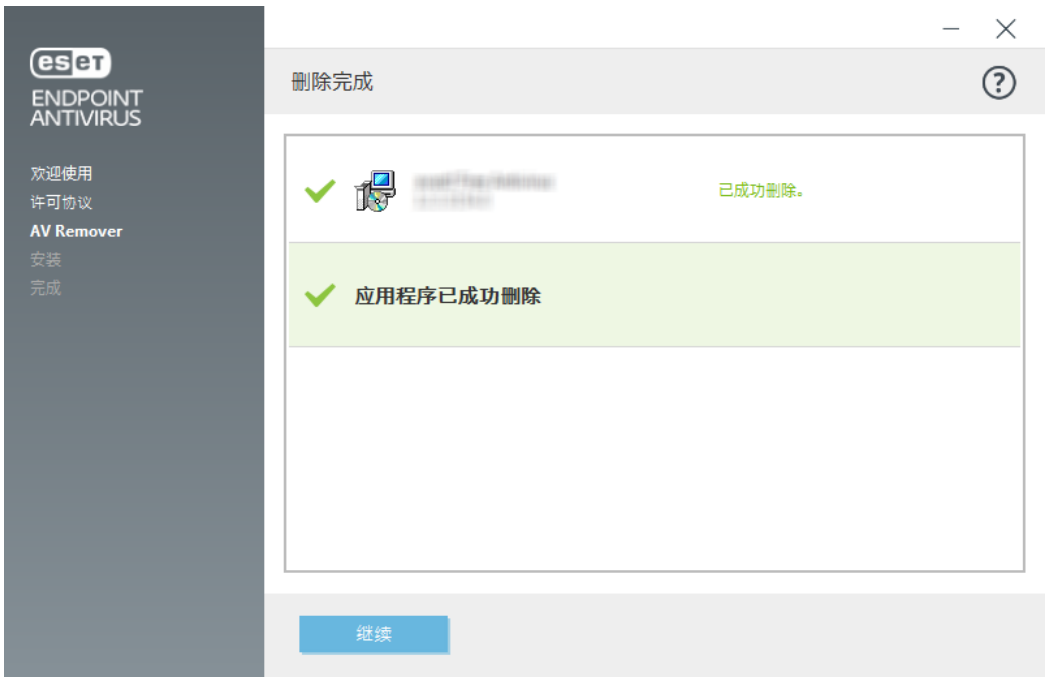
3. ESET AV Remover 将开始在系统中搜索病毒防护软件。



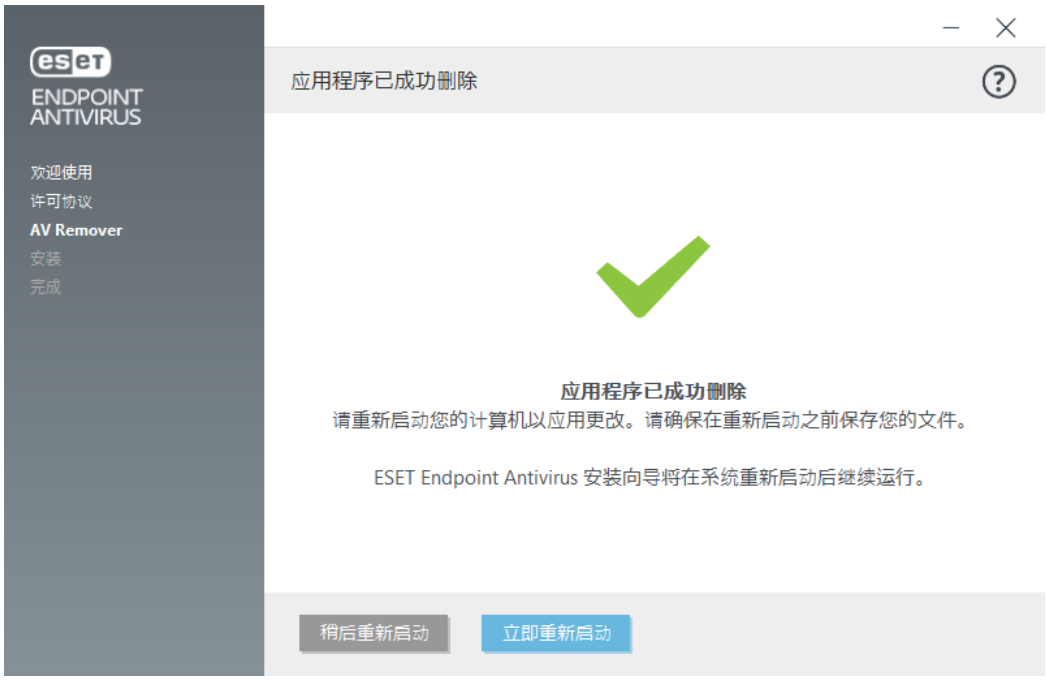
4. 选择任何列出的病毒防护应用程序并单击 删除 ”。 删除可能需要花费一点时间。



5. 成功删除后，请单击**继续**。



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



3.1.2 使用 ESET AV Remover 卸载因出现错误而终止

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

当卸载安全产品失败或仅部分卸载了它的一些组件时，系统将提示您**重新启动并重新扫描**。 重新启动后确认 UAC 并继续扫描和卸载过程。

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

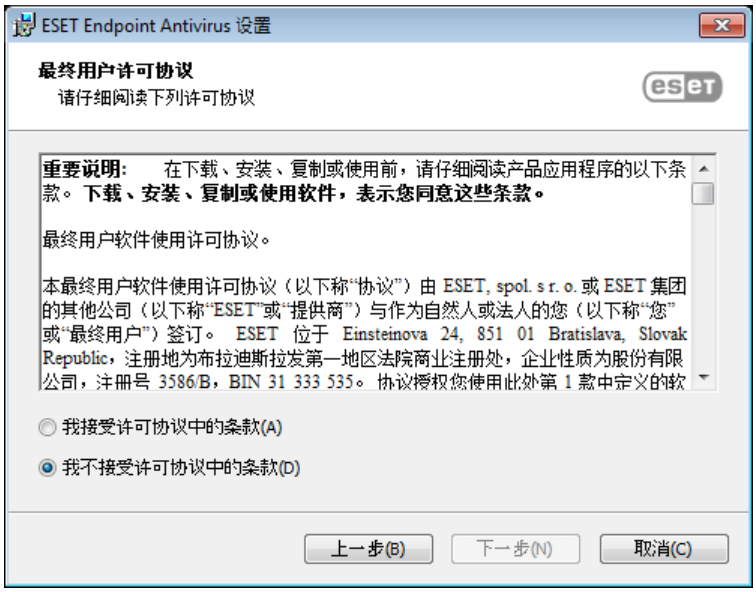
3.2 安装

启动安装程序后，安装向导将指导您完成安装过程。

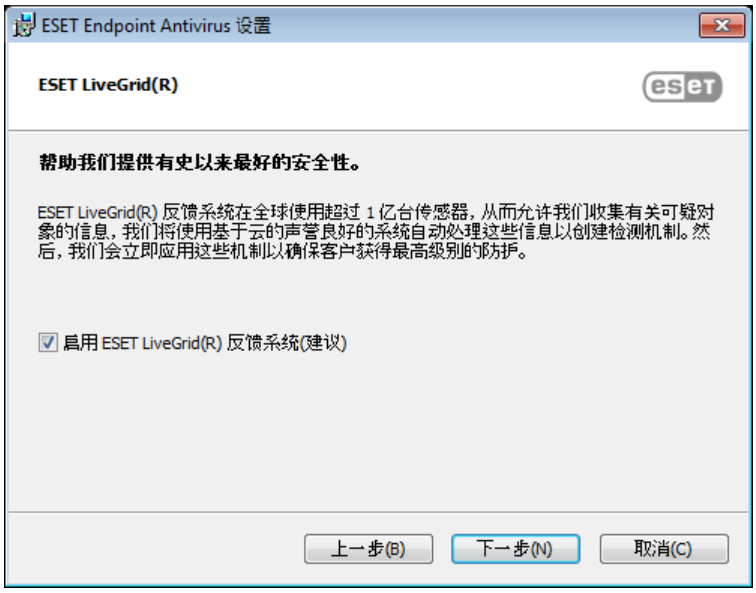
重要信息

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

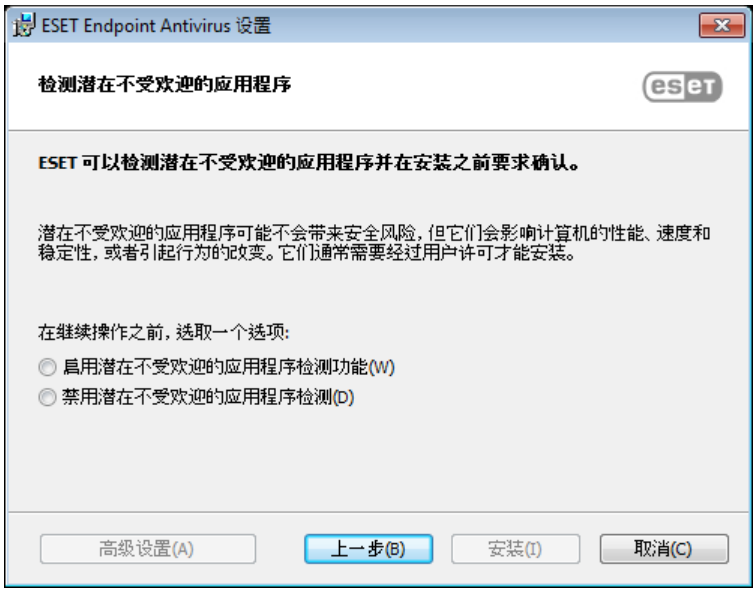
在下一步中将显示最终用户许可证协议。请阅读并单击**接受**以确认接受最终用户许可证协议。在接受条款后单击**下一步**以继续安装。



在选择 我接受 ...并单击**下一步**后，将提示您启用 ESET LiveGrid® 反馈系统。ESET LiveGrid® 帮助您确保将新渗透不断地及时通知给 ESET，这使我们可以更好地保护客户。该系统允许向 ESET 病毒实验室提交新的威胁，这些威胁将在实验室进行分析、处理并添加到检测引擎中。



安装过程的下一步是配置对潜在的不受欢迎应用程序的检测，这些应用程序不一定是恶意的，但通常可对操作系统行为产生负面影响。有关更多详细信息，请参阅潜在不受欢迎的应用程序一章。您可以通过单击**高级设置**访问其他设置（例如，在特定文件夹中安装您的 ESET 产品或在安装后启动自动扫描）。



最后一步是通过单击**安装**确认安装。

3.2.1 高级安装

高级安装允许您自定义在执行典型安装时不可用的大量安装参数。

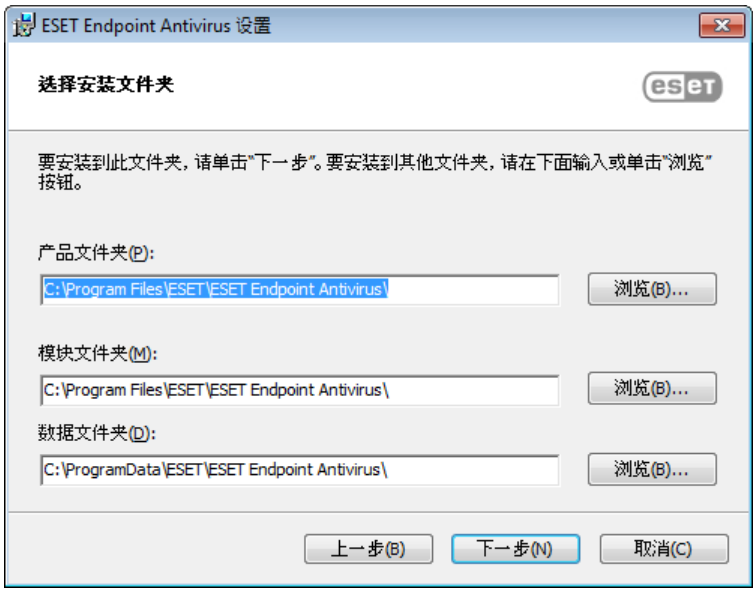
在选择对潜在的不受欢迎应用程序的检测首选项并单击**高级设置**后，将提示您选择安装产品文件夹的位置。默认情况下，程序将安装到以下目录：

C:\Program Files\ESET\ESET Endpoint Antivirus

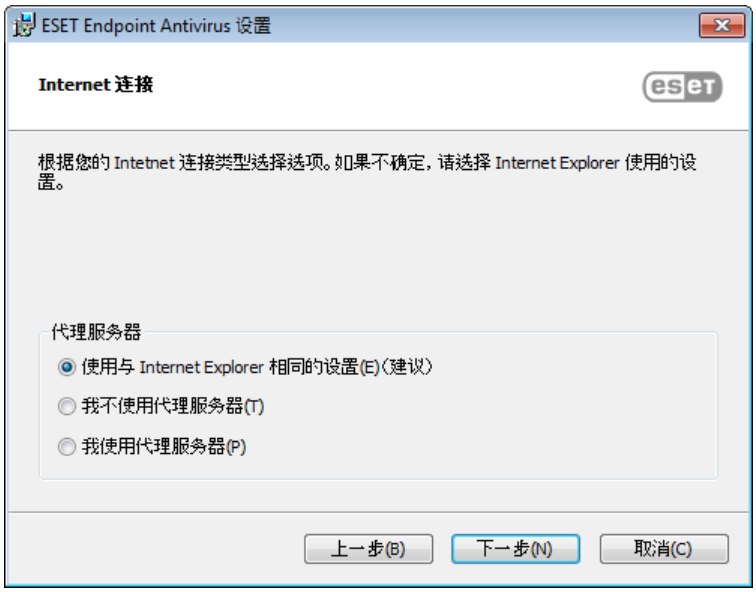
您可以指定程序模块和数据的位置。默认情况下，它们将分别安装到以下目录：

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

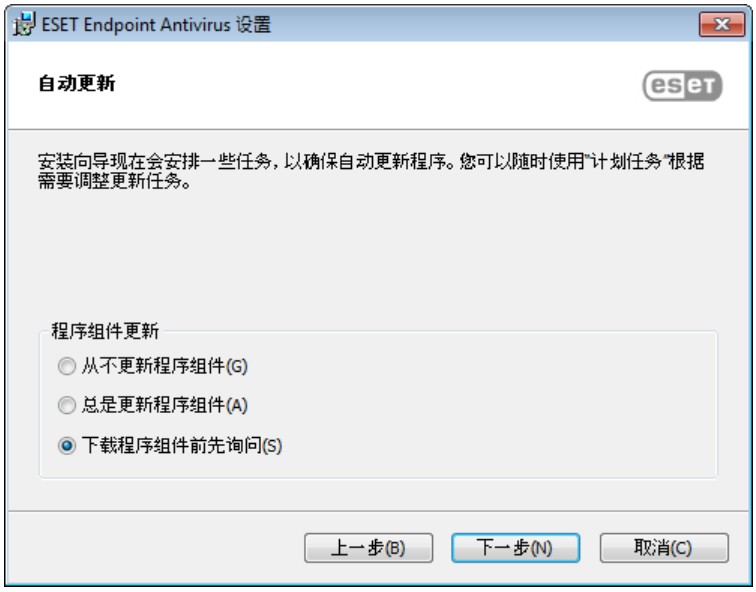
单击**浏览…**以更改这些位置（不建议）。



要配置您的代理服务器设置，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。如果不确定是否使用代理服务器连接到 Internet，请选择**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**。有关更多信息，请参见代理服务器。

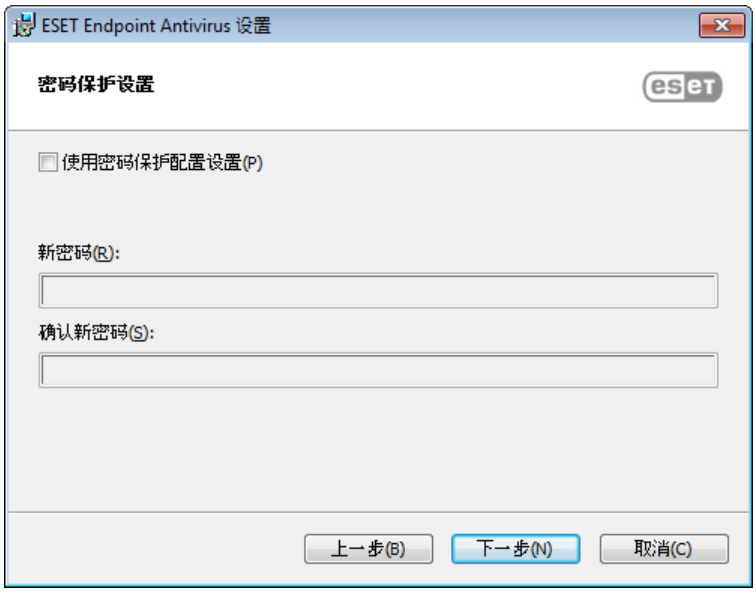


自定义安装允许您定义如何在系统上处理自动程序更新。单击**更改 ..**以访问高级设置。



如果您不想更新程序组件，请选择**从不更新程序组件**。选择**下载程序组件前询问**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升级，请选择**始终更新程序组件**。

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**，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。



单击**安装**以开始安装。

3.3 通过 ERA 进行产品安装（命令行）

以下设置旨在仅与**用户界面的降低**? **基本和无**级别一起使用。请参阅用于相应命令行开关的 **msiexec** 版本的文档。

支持的参数：

APPDIR=<path>
- 路径 -有效的目录路径
- 应用程序安装目录。
- 例如： `ees_nt64_ENU.msi /qn APPDIR=C:\ESET\ ADDLOCAL=DocumentProtection`

APPDATADIR=<path>
- 路径 -有效的目录路径
- 应用程序数据安装目录。

MODULEDIR=<path>
- 路径 -有效的目录路径
- 模块安装目录。

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

规则

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

功能状态

- **强制性** - 将始终安装该功能
- **可选** - 可能会取消安装该功能
- **不可见** - 为了使其他功能正常工作，逻辑功能是强制性的
- **占位符** - 不会对产品造成影响的功能，但必须与子功能一同列出

Endpoint 6.1 的功能树如下：

功能树	功能名称	功能状态
计算机	计算机	必需
计算机 病毒和间谍软件防护	病毒防护	必需
计算机 病毒和间谍软件防护 > 文件系统实时防护	RealtimeProtection	必需
计算机 病毒和间谍软件防护 > 计算机扫描	扫描	必需
计算机 病毒和间谍软件防护 > 文档防护	文档防护	可选
计算机 设备控制	DeviceControl	可选
网络	网络	占位符
网络 防火墙	防火墙	可选
Web 和电子邮件	WebAndEmail	占位符
Web 和电子邮件 协议过滤	ProtocolFiltering	不可见
Web 和电子邮件 Web 访问保护	WebAccessProtection	可选
Web 和电子邮件 电子邮件客户端访问保护	EmailClientProtection	可选
Web 和电子邮件 电子邮件客户端保护 MailPlugins	MailPlugins	不可见
Web 和电子邮件 电子邮件客户端保护 反垃圾邮件防护	反垃圾邮件	可选
Web 和电子邮件 Web 控制	WebControl	可选
更新镜像	UpdateMirror	可选
Microsoft NAP 支持	MicrosoftNAP	可选

附加规则

- 如果选择安装任意 **WebAndEmail** 功能，则不可见 **ProtocolFiltering** 功能必须显式包含在此列表中。
- 如果选择安装任意 **EmailClientProtection** 子功能，则不可见 **MailPlugins** 功能必须显式包含在此列表中

示例：

```
ees_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,WebAccessProtection,ProtocolFiltering
```

```
ees_nt64_ENU.msi /qn ADDLOCAL=WebAndEmail,EmailClientProtection,Antispam,MailPlugins
```

CFG_ 属性列表：

CFG_POTENTIALLYUNWANTED_ENABLED=1/0
- 0 - 已禁用，1 - 已启用
  PUA

CFG_LIVEGRID_ENABLED=1/0
- 0 - 已禁用，1 - 已启用
  LiveGrid

CFG_EPFW_MODE=0/1/2/3
0 - 自动，1 - 交互，2 - 策略，3 - 学习

CFG_PROXY_ENABLED=0/1
- 0 - 已禁用，1 - 已启用

CFG_PROXY_ADDRESS=<ip>
?代理 IP 地址。

CFG_PROXY_PORT=<port>
?代理端口号。

CFG_PROXY_USERNAME=<user>
?用于身份验证的用户名。

CFG_PROXY_PASSWORD=<pass>
- 用于身份验证的密码。

通过 SCCM 安装，禁用激活对话框：

ACTIVATION_DLG_SUPPRESS=1

- 1 - 已启用（不显示激活对话框）
  0 - 已禁用（显示激活对话框）

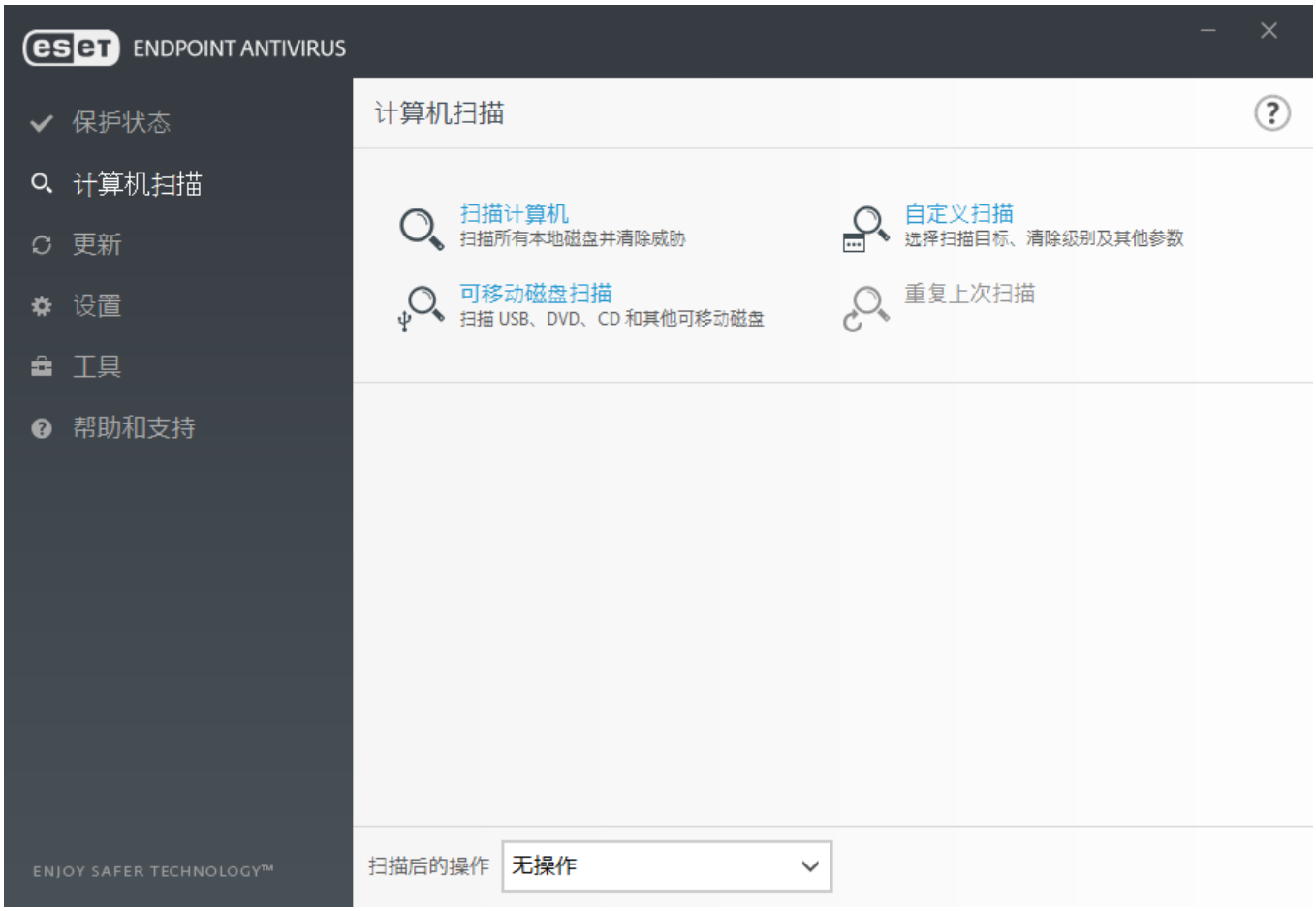
3.4 产品激活

完成安装后，将提示您激活您的产品。

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

3.5 计算机扫描

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



3.6 升级到更新版本

发布 ESET Endpoint Antivirus 的新版本以提供改进功能或修复无法通过程序模块的自动更新来解决的问题。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。
3. 通过 ESET Remote Administrator 在网络环境中使用自动部署手动进行升级。

3.7 入门指南

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

3.7.1 用户界面

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

以下是主菜单中选项的说明：

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

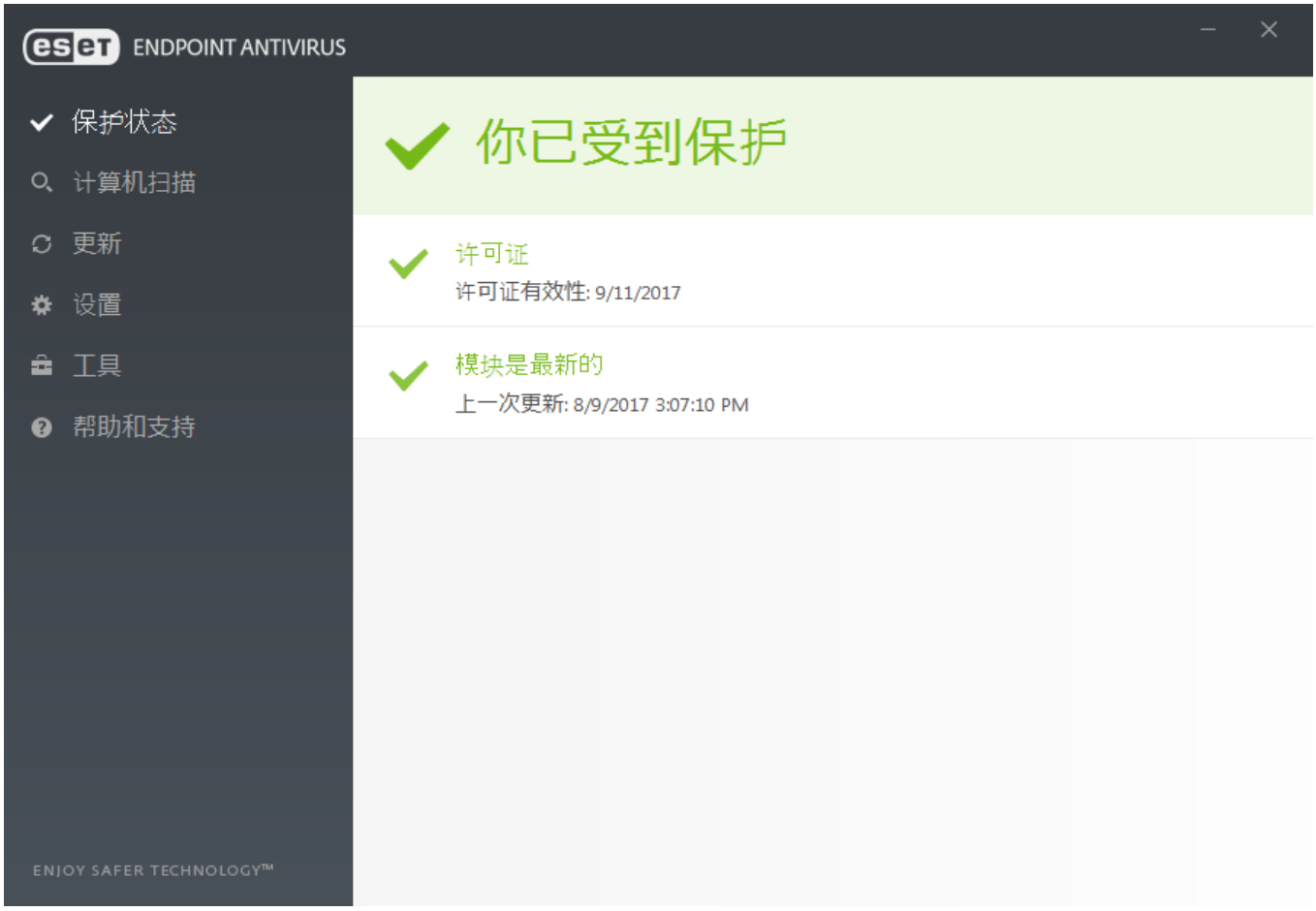
计算机扫描 - 此选项允许您配置和启动智能扫描、自定义扫描或可移动媒体扫描。您还可以重复上次运行的扫描。

更新 - 显示有关检测引擎的信息。

设置 - 选中此选项以调整您的计算机 或者 Web 和电子邮件安全设置。

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

帮助和支持 - 提供对帮助文件、ESET 知识库和 ESET 公司网站的访问权限。还提供用于打开客户服务支持请求的链接、支持工具以及有关产品激活的信息。

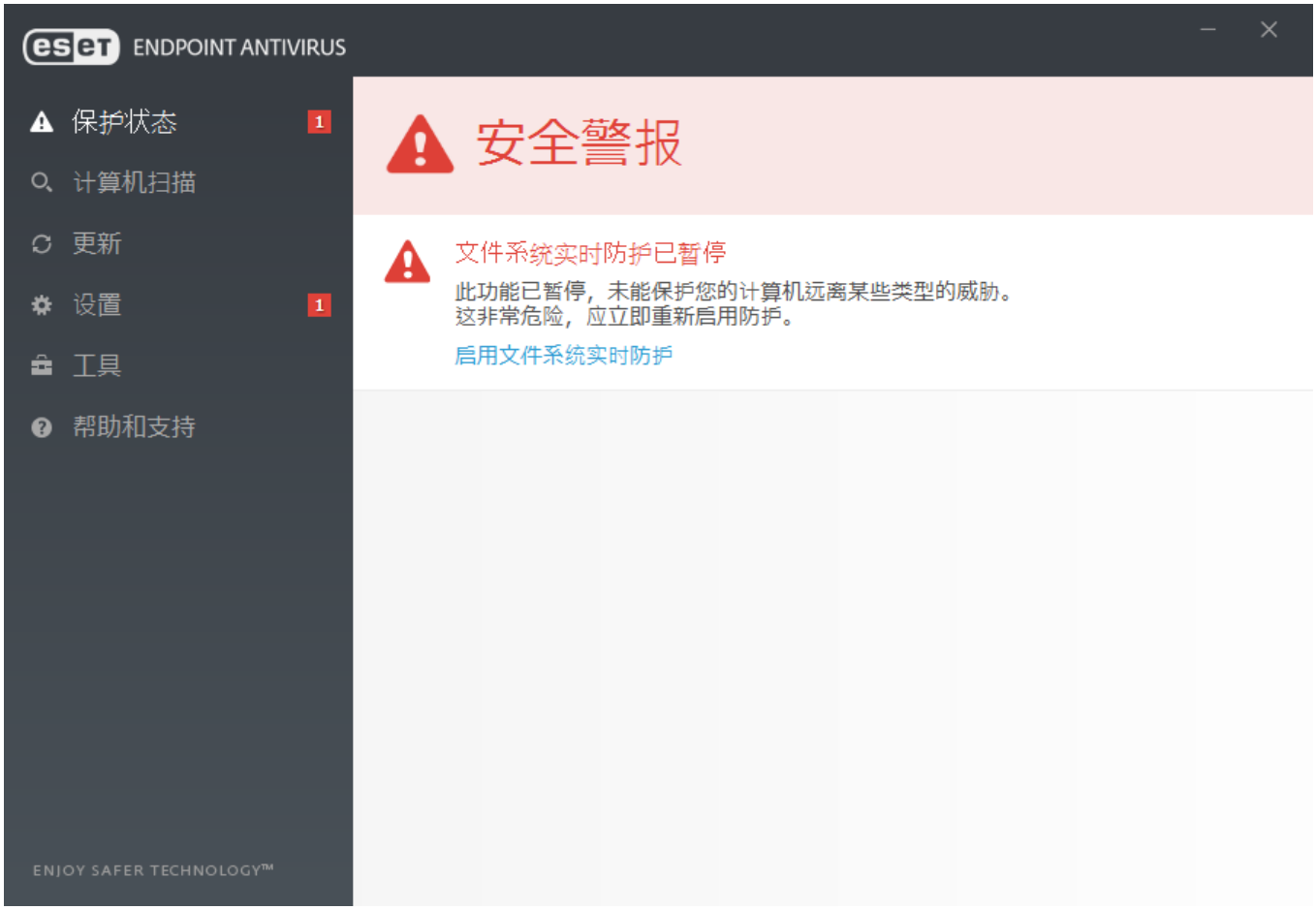


防护状态屏幕可告知您计算机的安全性和当前的防护级别。绿色**最高防护**状态表示已确保最高防护。

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

程序工作不正常时如何应对？

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



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

- **病毒和间谍软件防护已暂停** - 在**防护状态**窗格中，单击**启动所有病毒和间谍软件防护模块**以重新启用病毒和间谍软件防护，或者在主程序窗口的**设置**窗格中，单击**启用病毒和间谍软件防护**。
- **病毒防护不起作用** - 病毒扫描程序初始化失败。大多数 ESET Endpoint Antivirus 模块无法正常工作。
- **网络钓鱼防护不起作用** - 此功能不起作用，因为其他所需程序模块未处于活动状态。
- **检测引擎已过时** – 您正在使用已过时的检测引擎。请更新检测引擎。
- **产品未激活**或**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。
- **主机入侵预防系统 (HIPS) 已禁用** - 从高级设置中禁用 HIPS 会导致出现此问题。您的计算机未针对某些类型的威胁提供防护，应立即通过单击**启用 HIPS** 来重新启用防护。
- **ESET LiveGrid® 已禁用** - 在高级设置中禁用 ESET LiveGrid® 会导致出现此问题。
- **未计划定期更新** - 除非您计划更新任务，否则 ESET Endpoint Antivirus 将不会检查更新或收到重要更新。
- **反隐藏技术已禁用** - 单击**启用反隐藏技术**以重新启用该功能。
- **文件系统实时防护已暂停** - 用户已禁用实时防护。您的计算机未针对威胁提供防护。单击**启用实时防护**重新启用该功能。

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

- **Web 访问保护已禁用** - 单击安全通知以重新启用 Web 访问保护，然后单击**启用 Web 访问保护**。
- **您的许可证即将到期** - 此问题由显示惊叹号的防护状态图标表示。许可证过期后，程序将无法更新，防护状态图标将变为红色。
- **反垃圾邮件防护已暂停** - 单击**启用反垃圾邮件防护**以重新启用该功能。
- **Web 控制已暂停** - 单击**启用 Web 控制**以重新启用该功能。
- **策略覆盖处于活动状态** - 暂时覆盖策略设置的配置，可能直到故障排除结束为止。只有授权用户才可以覆盖策略设置。有关详细信息，请参阅如何使用覆盖模式。
- **设备控制已暂停** - 单击**启用设备控制**以重新启用该功能。

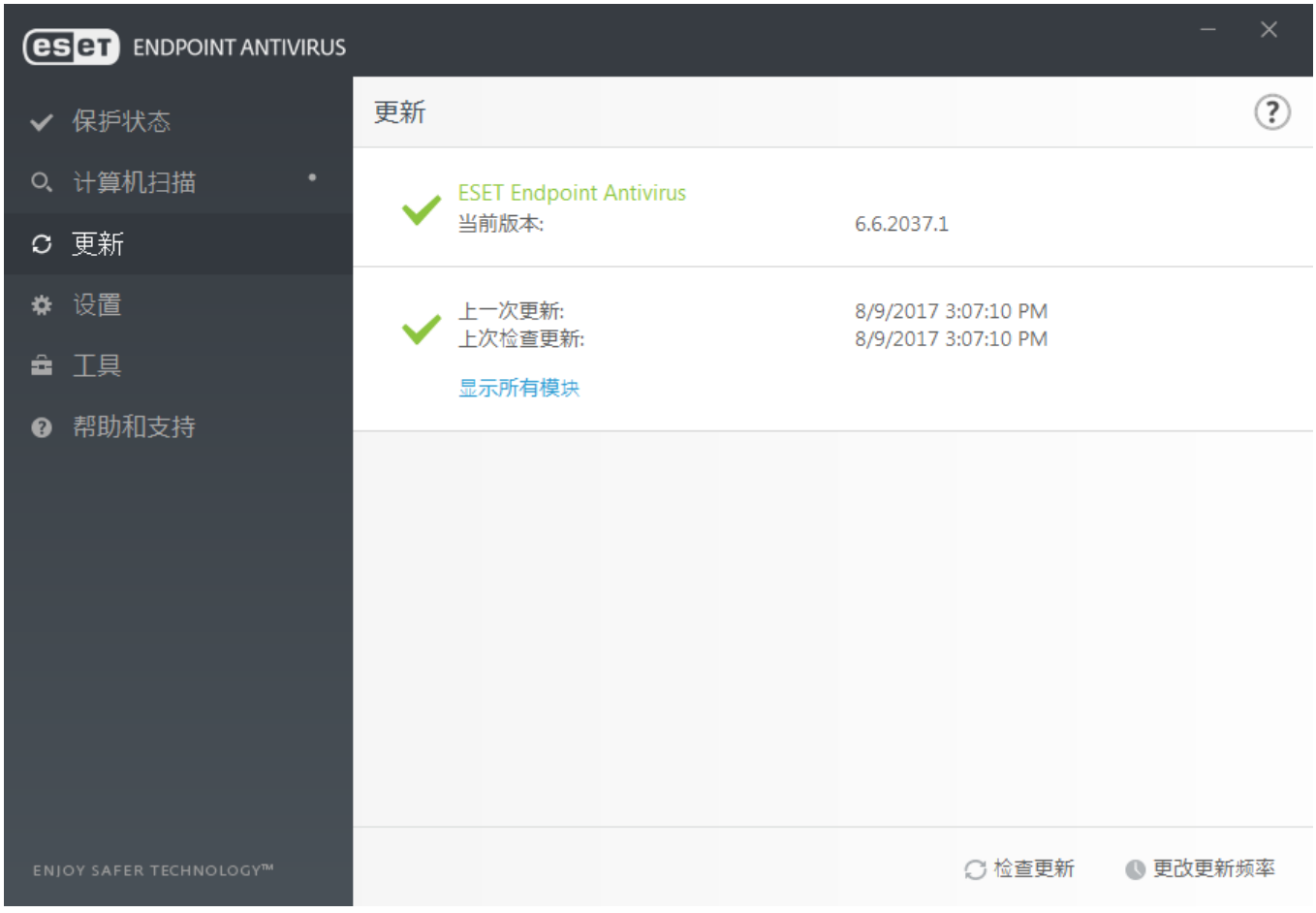
如果使用建议的解决方案无法解决问题，则单击**帮助和支持**以访问帮助文件或搜索 ESET 知识库。如果还需要帮助，可以提交 ESET 客户服务支持请求。ESET 客户服务将快速响应您的问题并帮助找到解决方案。

注意
如果状态属于受 ERA 策略阻止的功能，该链接将处于不可点击状态。

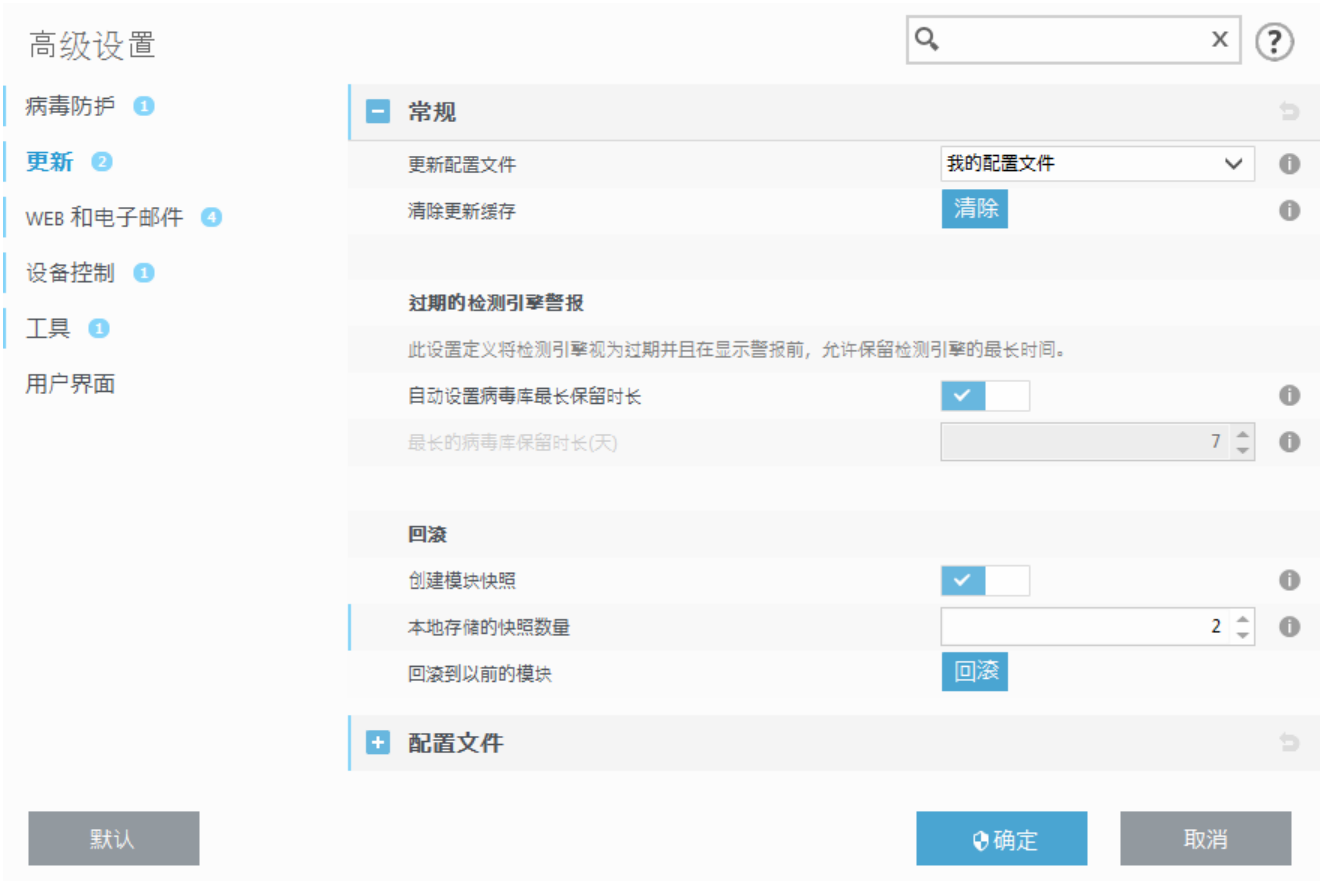
3.7.2 更新设置

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

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



高级设置 窗口（从主菜单中单击**设置** > **高级设置**，或按键盘上的 **F5** 键）包含其他更新选项。若要配置高级更新选项，如更新模式、代理服务器访问、局域网连接和检测引擎副本创建设置，请单击 高级设置 树中的**更新**。如果更新出现了问题，请单击**清除**以清除临时更新缓存。默认情况下，将**更新服务器**菜单设置为 **自动选择**。使用 ESET 服务器时，我们建议您保持选中**自动选择**选项。如果您不希望屏幕右下角的系统托盘通知出现，请选择**禁用显示关于成功更新的通知**。



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

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

3.8 常见问题

本章介绍一些最常见的问题和难题。单击主题标题了解如何解决您的难题：

如何更新 ESET Endpoint Antivirus
如何激活 ESET Endpoint Antivirus
如何使用当前凭据激活新产品
如何从 PC 中删除病毒
如何在计划任务中创建新任务
如何计划扫描任务（每 24 小时）
如何将我的产品连接到 ESET Remote Administrator
如何配置镜像

如果问题没有包括在上面列出的帮助页面中，则尝试在 ESET Endpoint Antivirus 帮助页面中按描述问题的关键字或短语搜索。

如果您无法在帮助页面中找到您的难题或问题的解决方案，请访问 ESET 知识库，此处提供常见问题的解答。

如何删除 Sirefef (ZeroAccess) 木马？
更新镜像故障排除检查列表
应打开我的第三方防火墙上的哪些地址和端口以便 ESET 产品提供完整功能？

如有必要，您可以联系我们的在线技术支持中心咨询您的问题或难题。可以在主程序窗口的**帮助和支持**窗格中找到我们的在线联系表格。

3.8.1 如何更新 ESET Endpoint Antivirus

可以通过手动或自动方式更新 ESET Endpoint Antivirus。若要触发更新，请单击主菜单中的**更新**部分中的**立即更新**。

默认安装设置会创建每小时执行的自动更新任务。若要更改时间间隔，请导航至**工具** > **计划任务**（有关计划任务的更多信息，请单击此处）。

3.8.2 如何激活 ESET Endpoint Antivirus

完成安装后，将提示您激活您的产品。

有几种激活产品的方法。激活窗口中特定激活方案的可用性可能根据国家/地区以及分发方式（CD/DVD、ESET 网页等）而不同。

要在程序中直接激活您的 ESET Endpoint Antivirus 副本，请单击系统托盘图标 并从菜单中选择**激活产品许可证**。您还可以在主菜单中的**帮助与支持** > **激活产品**或**保护状态** > **激活产品**下激活您的产品。

您可以使用以下任一方法来激活 ESET Endpoint Antivirus：

- **许可证密钥** - 采用 XXXX-XXXX-XXXX-XXXX-XXXX 格式的唯一字符串，用于标识许可证所有者和激活许可证。
- **安全管理员** - 使用凭据（电子邮件地址 +密码）在 ESET 许可证管理员门户网站上创建的帐户。此方法允许您在一个位置管理多个许可证。
- **脱机许可证** - 将传输到 ESET 产品以提供许可证信息的自动生成的文件。如果许可证允许您下载可用于执行脱机激活的脱机许可证文件 (.lf)。将从可用许可证的总数中减去脱机许可证的数量。有关生成脱机文件的更多详细信息，请参阅 ESET License Administrator 用户指南。

如果您的计算机是托管网络的成员，请单击**稍后激活**，您的管理员将通过 ESET Remote Administrator 执行远程激活。如果您希望稍后激活此客户端，也可以使用此选项。

如果您拥有用户名和密码但是不知道如何激活 ESET Endpoint Antivirus，请单击**我有用户名和密码，该怎样操作**。您将重定向到 ESET License Administrator，在那里您可以将凭据转换为许可证密钥。

您可以随时更改您的产品许可证。为此，请在主程序窗口中依次单击**帮助和支持** > **管理许可证**。您将看到 ESET 支持用来识别您的许可证的公共许可证 ID。用于注册计算机的用户名存储在**关于**部分中，您可以通过右键单击系统托盘图标 来查看它。

注意
ESET Remote Administrator 能够使用管理员提供的许可证静默激活客户端计算机。有关执行此操作的说明，请参阅 ESET Remote Administrator 用户指南。

3.8.3 如何使用当前凭据激活新产品

如果您已具有用户名和密码并且希望收到一个许可证密钥，请访问 ESET 许可证管理员门户网站，在此处您可以将自己的凭据转换为新的许可证密钥。

3.8.4 如何从 PC 中删除病毒

如果您的计算机显示感染恶意软件的迹象，例如速度变慢，常常停止响应，我们建议您执行以下操作：

1. 在主程序窗口中，单击**计算机扫描**。
2. 单击**智能扫描**以开始扫描您的系统。
3. 扫描完成后，查看日志中扫描文件、被感染文件和已清除文件的数量。
4. 如果您希望仅扫描磁盘的特定部分，请单击**自定义扫描**，然后选择要进行病毒扫描的目标。

有关其他信息，请参阅我们定期更新的 ESET 知识库文章。

3.8.5 如何在计划任务中创建新任务

要在**工具** > **计划任务**中创建新任务，请单击**添加任务**或右键单击并从右键菜单中选择**添加 ...**。共有 5 种类型的计划任务：

- **运行外部应用程序** - 计划外部应用程序的执行。
- **日志维护** - 日志文件中仍会包含已删除记录的残余信息。此任务定期优化日志文件中的记录以提高工作效率。
- **系统启动文件检查** - 检查在系统启动或登录时允许运行的文件。
- **创建计算机状态快照** - 创建 ESET SysInspector 计算机快照 -收集有关系统组件的详细信息（例如，驱动程序、应用程序）并评估每个组件的风险级别。
- **手动计算机扫描** - 执行计算机上文件和文件夹的计算机扫描。
- **更新** - 通过更新模块，计划更新任务。

因为**更新**是最常用的计划任务之一，所以下面我们将解释如何添加新的更新任务：

从**计划任务**下拉菜单中选择**更新**。将任务名称输入**任务名称**字段中并单击**下一步**。选择任务执行频率。有以下选项可供使用：**一次**？**重复**？**每天**？**每周**和**由事件触发。在便携式计算机靠电池供电时，**选择**靠电池供电时跳过任务**以最大限度地减少系统资源。将在**任务执行**字段中指定的日期和时间运行该任务。然后，定义无法在计划时间执行或完成任务时要采取的操作。有以下选项可供使用：

- **在下一个计划时间**
- **尽快**
- **如果自上次运行时间之后经过的时间超过指定值，则立即跳过任务**（可使用**自上次运行时间之后经过的时间**滚动框来定义间隔）

在下一步中，显示有关当前计划任务信息的摘要窗口。当您完成更改时，单击**完成**。

将显示一个对话窗口，允许您选择用于计划任务的配置文件。此处，您可以设置主要和替代配置文件。如果任务不能用主要配置文件来完成，则使用替代配置文件。单击**完成**以进行确认，新计划任务将添加到当前计划任务列表中。

3.8.6 如何计划扫描任务（每 24 小时）

要计划定期任务，请打开主程序窗口，然后单击**工具** > **计划任务**。您可以在下面找到关于如何计划每 24 小时扫描一次本地磁盘的任务的简要指南。

要计划扫描任务：

1. 单击主计划任务屏幕中的**添加**。
2. 从下拉菜单中选择**手动计算机扫描**。
3. 输入任务名称，然后选择**重复**。
4. 选择每 24 小时运行一次任务。
5. 选择计划任务执行因任何原因失败时将执行的操作。
6. 检查计划任务的摘要并单击**完成**。
7. 从**目标**下拉菜单中选择**本地驱动器**。
8. 单击**完成**以应用此任务。

3.8.7 如何将 ESET Endpoint Antivirus 连接至 ESET Remote Administrator

当您已在计算机上安装了 ESET Endpoint Antivirus 并且需要通过 ESET Remote Administrator 进行连接时，请确保您同样在客户端工作站上安装了 ERA 服务器代理。ERA 服务器代理是每个与 ERA Server 通信的客户端解决方案的重要部分。ESET Remote Administrator 可以使用 RD Sensor 工具在网络上搜索计算机。RD Sensor 在您的网络上检测到的每台计算机都将在 Web 控制台中显示。

部署代理后，您可以在客户端计算机上执行 ESET 安全产品的远程安装。ESET Remote Administrator 用户指南中描述了远程安装的具体步骤。

3.8.8 如何配置镜像

可对 ESET Endpoint Antivirus 进行配置，以存储检测引擎更新文件副本，并将更新分发到正在运行 ESET Endpoint Security 或 ESET Endpoint Antivirus 的其他工作站。

将 ESET Endpoint Antivirus 配置为镜像服务器，以通过内部 HTTP 服务器提供更新

按 **F5** 以访问 高级设置 并展开**更新** > **基本**。请确保已将**更新服务器**设置为 **自动选择**。从**高级设置** > **基本** > **镜像**选择**创建更新镜像**和**通过内部 HTTP 服务器提供更新文件**。

配置镜像服务器以通过共享网络文件夹提供更新

在本地或网络设备上创建共享文件夹。此文件夹必须能被所有运行 ESET 安全解决方案的用户读取，并且必须可通过本地 SYSTEM 帐户写入。激活**高级设置** > **基本** > **镜像**下的**创建更新镜像**。浏览并选择已创建的共享文件夹。

注意
如果您不希望通过 HTTP 服务器进行更新，请取消**通过内部 HTTP 服务器提供更新文件**。

3.8.9 如何使用 ESET Endpoint Antivirus 升级到 Windows 10

警告
我们强烈建议您先升级到最新版本的 ESET 产品并下载最新的模块更新，然后再升级到 Windows 10。在升级到 Windows 10 期间，此操作可确保您获取最大程度的防护并将保留您的程序设置和许可证信息。

版本 6.x 及更高版本：

单击下方相应的链接下载并安装最新版本，以便为升级到 Microsoft Windows 10 做好准备：

下载 ESET Endpoint Security 6 32 位 下载 ESET Endpoint Antivirus 6 32 位

下载 ESET Endpoint Security 6 64 位 下载 ESET Endpoint Antivirus 6 64 位

版本 5.x 及更早版本：

单击下方相应的链接下载并安装最新版本，以便为升级到 Microsoft Windows 10 做好准备：

下载 ESET Endpoint Security 5 32 位 下载 ESET Endpoint Antivirus 5 32 位

下载 ESET Endpoint Security 5 64 位 下载 ESET Endpoint Antivirus 5 64 位

其他语言版本：

如果您正在查找 ESET Endpoint 产品的其他语言版本，请访问我们的下载页面。

注意
有关 ESET 产品与 Windows 10 兼容性的详细信息。

3.8.10 如何使用覆盖模式

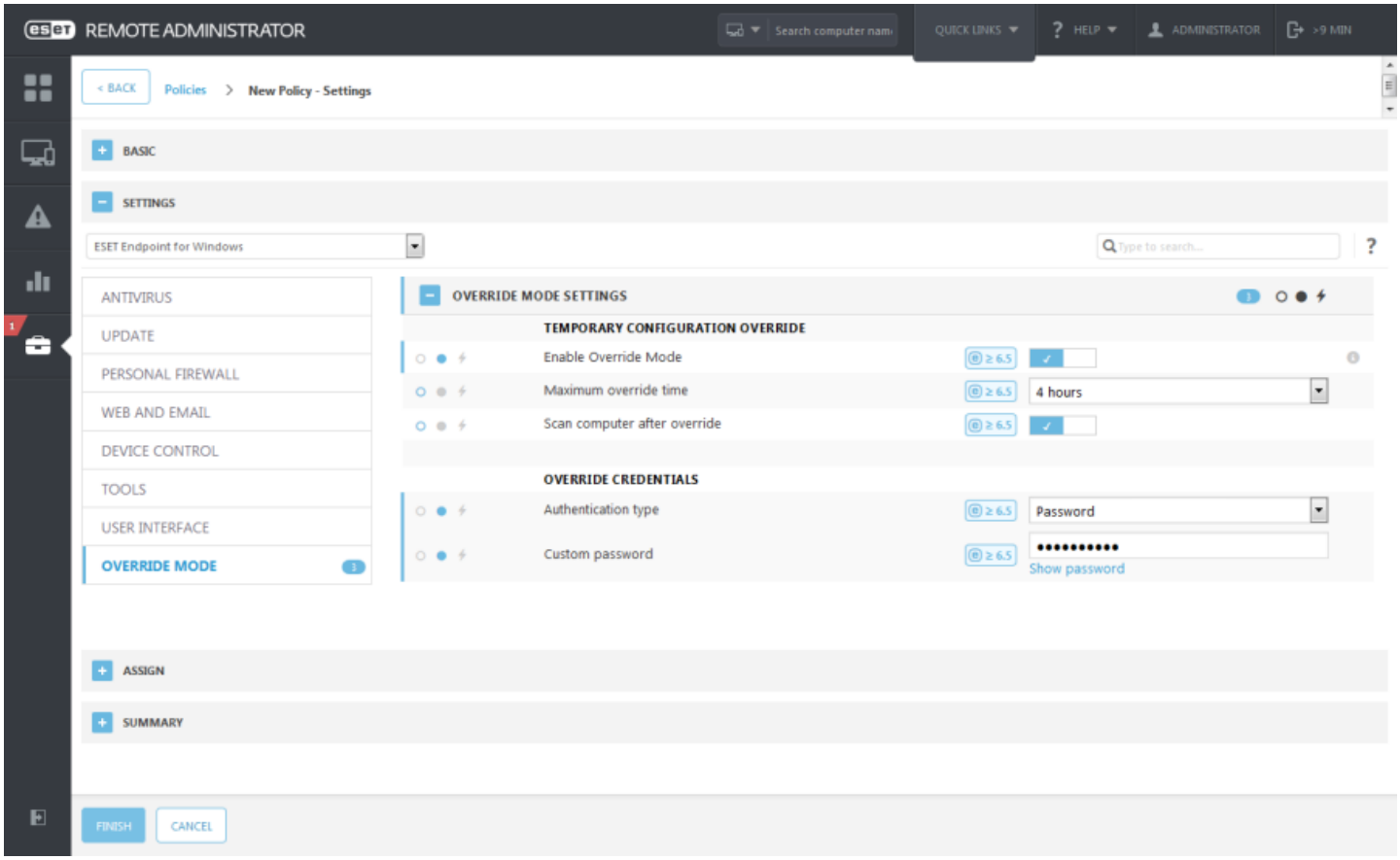
在计算机上已安装适用于 Windows 的 ESET Endpoint 产品（版本 6.5 和更高版本）的用户可以使用覆盖功能。覆盖模式允许客户端计算机级别上的用户更改已安装的 ESET 产品中的设置，即使已对这些设置应用了策略。可以为某些 AD 用户启用覆盖模式，也可以对覆盖模式进行密码保护。启用一次该功能的时长不能超过 4 个小时。

警告
启用覆盖模式后，不能从 ERA Web 控制台停止该模式。仅当覆盖时间过后，或者在客户端上关闭覆盖，才会禁用覆盖。

若要设置**覆盖模式**，请执行以下步骤：

1. 导航到**管理员** > **策略** > **新策略**。
2. 在 **基本**部分中，键入该策略的**名称**和**说明**。
3. 在 **设置**部分中，选择 **ESET Endpoint for Windows**。

4. 单击**覆盖模式**，然后配置覆盖模式的规则。
5. 在 **分配**部分中，选择将应用该策略的计算机或计算机组。
6. 在 **摘要**部分中检查这些设置，然后单击**完成**以应用该策略。



将覆盖策略从 ERA Server 应用到 ERA 服务器代理后，高级设置（位于客户端的 Endpoint 上）中会出现一个覆盖策略按钮。

1. 单击**覆盖策略**。
2. 设置时间并单击**应用**。
3. 允许提升 ESET 应用程序的权限。
4. 输入由策略确定的密码（如果在策略中设置了 Active Directory 用户，则没有密码）。
5. 允许提升 ESET 应用程序的权限。
6. 现在，覆盖模式处于打开状态。
7. 若要结束这一模式，请单击**结束覆盖**。

提示

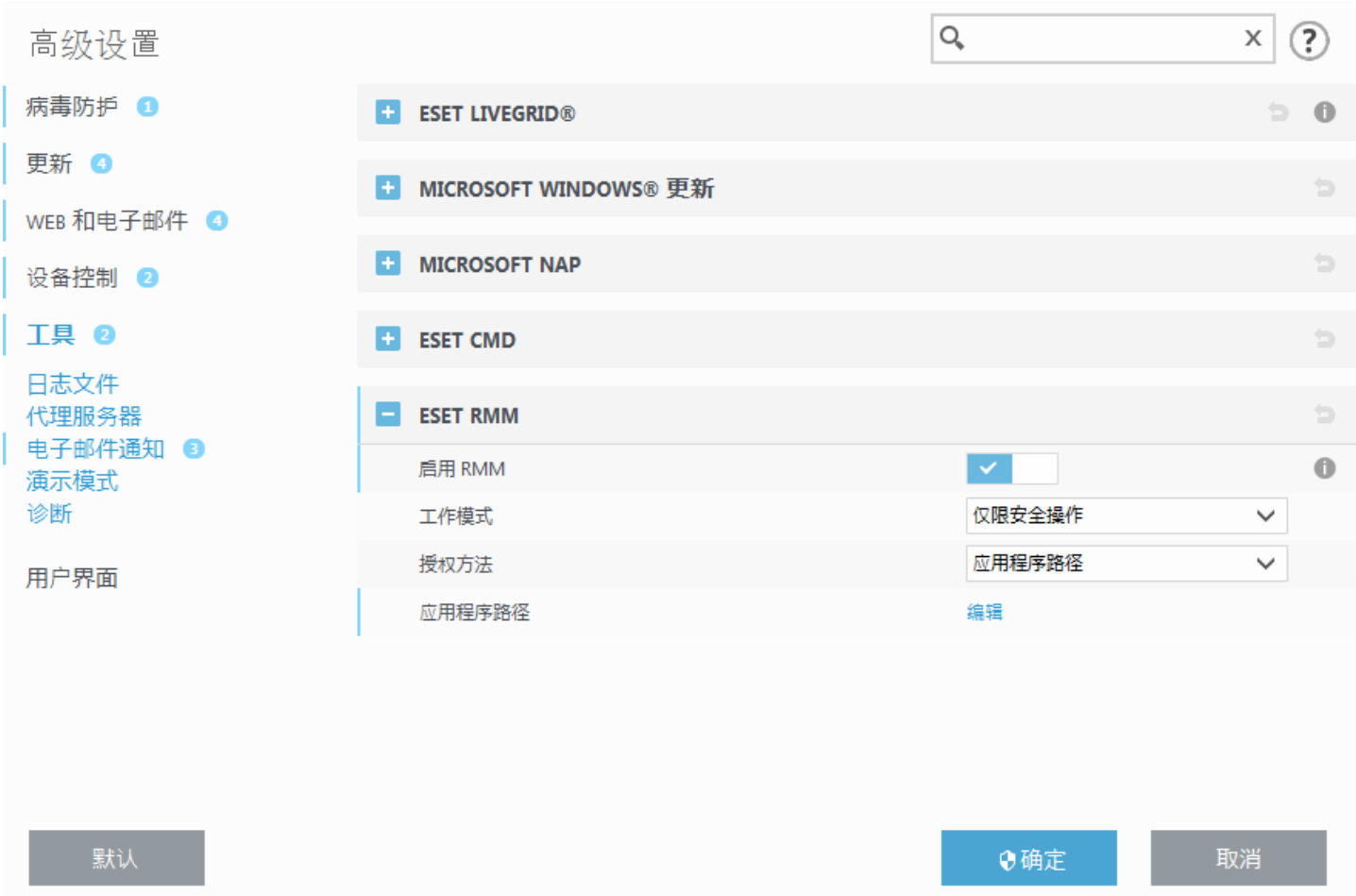
如果 *John* 的计算机上的端点设置阻止了某些重要功能或 Web 访问，管理员可以允许 *John* 覆盖其现有端点策略，然后手动调整其计算机上的设置。之后，ERA 可以请求这些新设置，以便管理员可以基于这些设置创建新策略。

要执行该操作，请遵循以下步骤：

1. 导航到**管理员** > **策略** > **新策略**。
2. 填写**名称**和**说明**字段。在**设置**部分中，选择 **ESET Endpoint for Windows**。
3. 单击**覆盖模式**、启用覆盖模式一个小时，然后选择 *John* 作为 AD 用户。
4. 将策略分配给 *John 的计算机* ，然后单击**完成**以保存策略。
5. *John* 必须在其 ESET Endpoint 上启用**覆盖模式**，并手动在其计算机上更改设置。
6. 在 ERA Web 控制台上，导航到**计算机**、选择 *John 的计算机* ，然后单击**显示详细信息**。
7. 在**配置**部分中，单击**请求配置**，尽快计划从客户端 ASAP 获取配置的客户端任务。
8. 过一会，将显示新配置。单击要保存设置的产品，然后单击**打开配置**。
9. 您可以检查设置，然后单击**转换为策略**。
10. 填写**名称**和**说明**字段。
11. 在**设置**部分中，必要时可修改设置。
12. 在**分配**部分中，可以将该策略分配给 *John 的计算机* （或其他计算机）。
13. 单击**完成**以保存设置。
14. 不再需要覆盖策略后，务必将覆盖策略删除。

3.8.11 如何激活远程监控和管理

远程监控和管理 (RMM) 是使用可供管理服务提供商访问的本地安装的服务器代理监管和控制软件系统（例如桌面、服务器和移动设备上的软件系统）的过程。



默认情况下，ESET RMM 处于禁用状态。若要启用 ESET RMM，请按 **F5** 访问 高级设置 ”，单击**工具**，展开 **ESET RMM** 并打开**启用 RMM** 旁边的开关。

工作模式 –从下拉菜单中选择 RMM 的工作模式。有两种选项可用：**仅安全操作**和**所有操作**。

授权方法 –设置 RMM 授权方法。若要使用授权，在下拉菜单中选择**应用程序路径**，或者选择**无**。

警告
RMM 应始终使用授权以防止恶意软件禁用或规避 ESET Endpoint 防护。

应用程序路径 –如果您选择**应用程序路径**作为授权方法，单击**编辑**以打开**允许的 RMM 应用程序路径**配置窗口。

添加 –创建新的允许的 RMM 应用程序路径。输入路径或单击 **...** 按钮以选择可执行文件。
编辑 - 修改现有的允许的路径。如果可执行文件的位置更改为另一个文件夹，则使用**编辑**。
删除 - 删除现有允许的路径。

默认 ESET Endpoint Antivirus 安装包含位于 Endpoint 应用程序目录（默认路径为 *c:\Program Files\ESET\ESET Security* ）中的 ermm.exe 文件。ermm.exe 与 RMM 插件交换数据，该插件可与链接到 RMM 服务器的 RMM 服务器代理通信。

- ermm.exe –ESET 开发的命令行实用工具，允许管理 Endpoint 产品以及与任何 RMM 插件通信。
- RMM 插件是在 Endpoint 窗口系统上本地运行的第三方应用程序。该插件旨在与特定的 RMM 服务器代理（如 Kaseya ）和 ermm.exe 通信。
- RMM 服务器代理是在 Endpoint 窗口系统上本地运行的第三方应用程序（如来自 Kaseya 的程序）。服务器代理与 RMM 插件和 RMM 服务器通信。
- RMM 服务器在第三方服务器上作为服务运行。RMM 系统由 Kaseya、Labtech、Autotask、Max Focus 和 Solarwinds N-able 支持。

3.9 使用 ESET Endpoint Antivirus

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

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

设置菜单包含以下部分：

- **计算机**
- **Web 和电子邮件**

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、创建或运行所有文件时，都将扫描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。
- **HIPS** - HIPS 系统监视操作系统内发生的事件，并按照自定义的规则集进行响应。
- **演示模式** - 为那些需要不中断其使用软件、不希望被弹出窗口打扰，并希望尽量减少 CPU 使用的用户提供的功能。启用演示模式后您将收到警告消息（潜在安全风险），主程序窗口将变为橙色。
- **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 Rootkit。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** - 如果已启用，将扫描所有通过 HTTP 或 HTTPS 的通信以查看是否有恶意软件。
- **电子邮件客户端防护** - 监视通过 POP3 和 IMAP 协议接收的通信。
- **网络钓鱼防护** - 防止冒充合法网站的非法网站尝试获取密码、银行数据和其他敏感信息，从而为您提供保护。

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

要重新启用已禁用的安全组件的防护，请单击红色开关  以使组件返回其启用状态。

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

注意
计算机重新启动后，以这种方式禁用的所有防护措施都将重新启用。

要访问特定安全组件的详细设置，请单击任意组件旁的齿轮  。

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

有关更详细的选项，请单击**高级设置**或按 **F5**。

3.9.1 计算机

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

单击**文件系统实时防护**旁边的齿轮  并单击**编辑排除**以打开排除设置窗口，此窗口允许您从扫描中排除文件和文件夹。

注意
在您在以下位置启用文档防护状态之前，它可能不可用： **高级设置** (F5) > **病毒防护** > **文档防护**。启用之后，您需要在 设置 窗格 > 计算机 中，通过单击 设备控制 下的**重新启动**来重新启动计算机，或者可以在 防护状态 窗格中通过单击**重新启动计算机**来完成。

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

计算机扫描设置 ...- 单击以调整计算机扫描（手动执行扫描）的参数。

3.9.1.1 检测引擎

病毒防护通过控制文件、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。

若要详细配置病毒防护模块设置，请单击**高级设置**或按 **F5**。

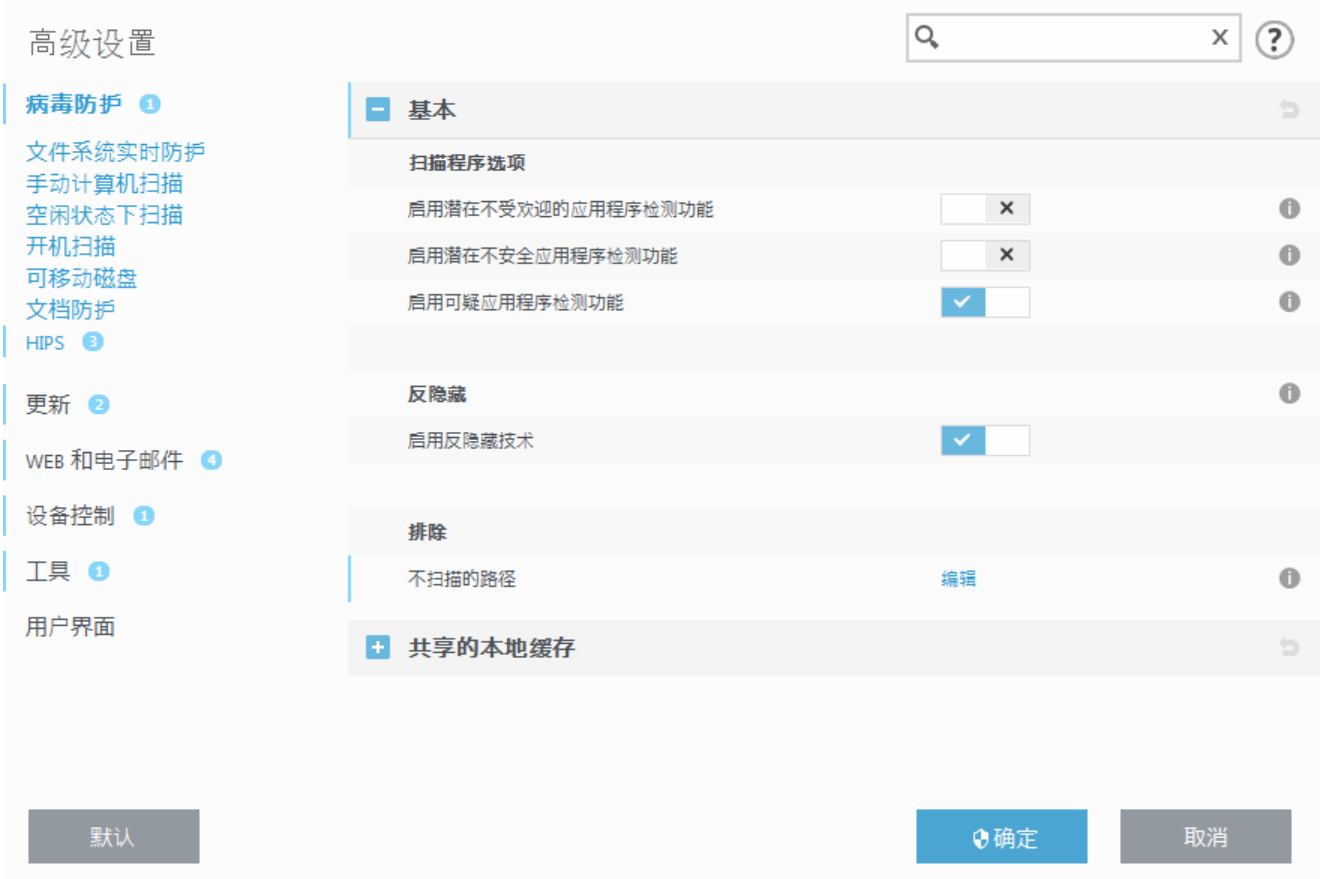
用于所有防护模块（例如文件系统实时防护、Web 访问保护等）的**扫描程序选项**允许您启用或禁用对以下对象的检测：

- **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。
  请阅读词汇表中关于这些类型的应用程序的更多信息。
- **潜在的不安全应用程序**是指有可能被滥用于恶意用途的合法商业软件。潜在的不安全应用程序的示例包括远程访问工具、密码破解应用程序以及按键记录器（记录用户键盘输入信息的程序）等。此选项默认情况下处于禁用状态。
  请阅读词汇表中关于这些类型的应用程序的更多信息。
- **可疑应用程序**包括使用加壳程序或保护程序压缩的程序。这些类型的保护程序通常被恶意软件作者用来逃避检测。

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

使用**排除**可将文件和文件夹排除在扫描之外。要确保对所有对象进行威胁扫描，我们建议您只在绝对有必要时才创建排除。您需要排除某个对象的情况可能包括：在扫描期间会使计算机速度变慢的大型数据库条目扫描，或遇到与扫描冲突的软件。若要从扫描中排除某个对象，请参阅排除。

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



3.9.1.1.1 检测到威胁

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

标准行为

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

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

每个功能使用标准清除级别，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详细信息，请参阅清除。

清除和删除

如果文件系统实时防护没有预定义操作，程序将显示一个警报窗口，提示您从中选择一个选项。一般会有**清除**？**删除**和**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。

多个威胁

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

删除压缩文件中的文件

在默认清除模式下，仅当压缩文件只包含被感染文件而没有干净文件时，才会删除整个压缩文件。换言之，如果还包含无害的干净文件，就不会删除压缩文件。执行严格清除扫描时请小心，严格清除已启用时，即使压缩文件只包含一个被感染文件，无论压缩文件中其他文件的状态如何，都将删除该压缩文件。

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

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

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

3.9.1.2 共享的本地缓存

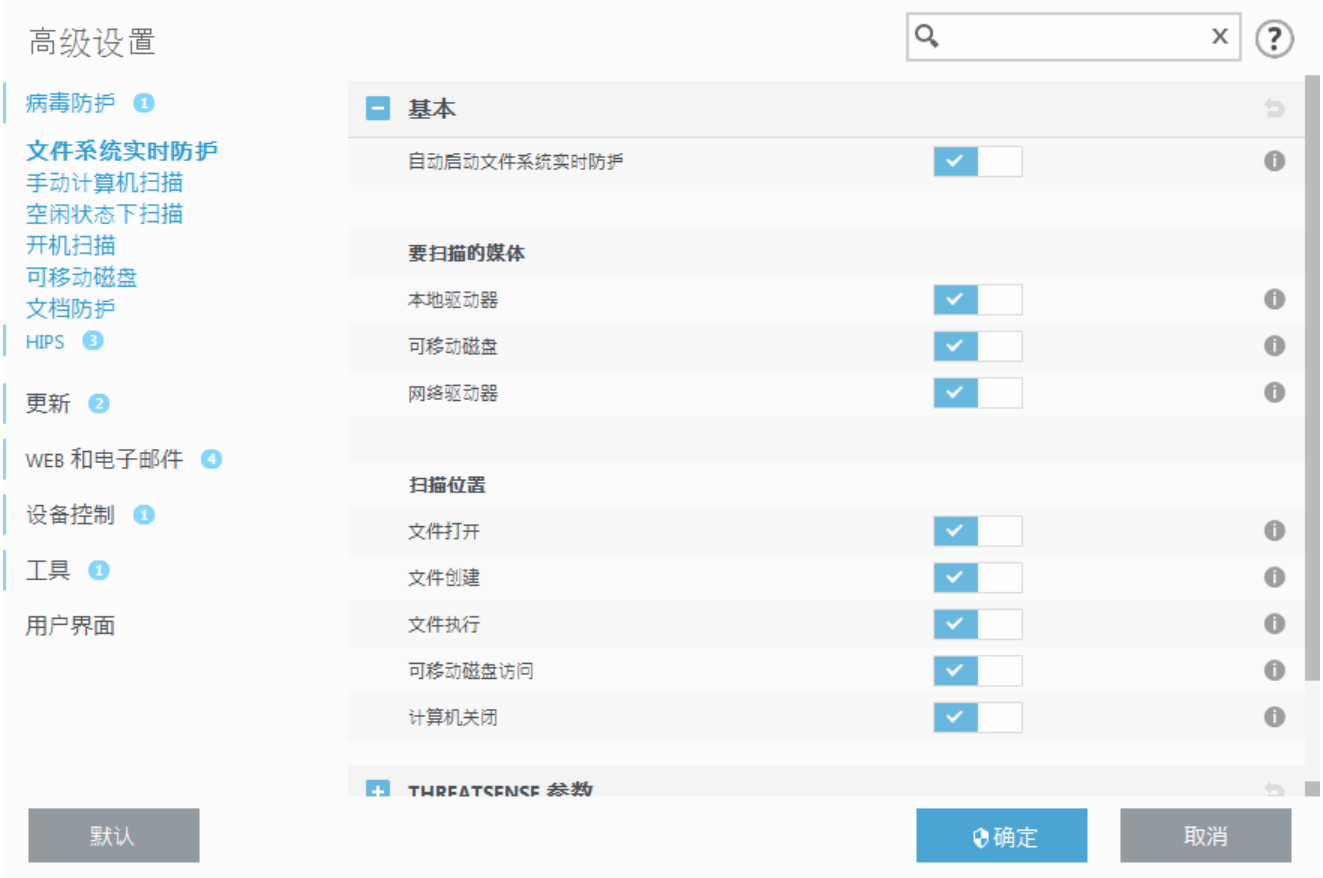
通过消除网络中的重复扫描，共享的本地缓存将在虚拟环境中提高性能。这可确保每个文件仅扫描一次并且存储在共享的缓存中。打开**缓存选项**开关，以将有关扫描网络上的文件和文件夹的信息保存到本地缓存。如果您执行新扫描，ESET Endpoint Antivirus 将搜索该缓存中的已扫描文件。如果文件匹配，将不对其进行扫描。

缓存服务器的设置包含以下内容：

- **主机名** - 缓存所在的计算机的名称或 IP 地址。
- **端口** - 用于通信的端口号（与在共享的本地缓存中设置的端口号相同）。
- **密码** - 指定 ESET 共享的本地缓存密码（如果需要）。

3.9.1.3 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、创建或运行所有文件时，都将扫描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。



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（例如与其他实时扫描程序存在冲突），可以通过在**高级设置**中取消**文件系统实时防护** > **基本**下的**启用文件系统实时防护**，来禁用实时防护。

要扫描的介质

默认情况下，所有类型的介质均可扫描以检查是否存在潜在威胁：

本地驱动器 - 控制所有系统硬盘。
可移动磁盘 - 控制 CD/DVD、USB 存储和蓝牙设备等。
网络驱动器 - 扫描所有映射的驱动器。

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

扫描位置

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

- **打开文件** - 启用或禁用打开文件时的扫描。
- **创建文件** - 启用或禁用创建文件时的扫描。
- **执行文件** - 启用或禁用运行文件时的扫描。
- **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。

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

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

3.9.1.3.1 其他 ThreatSense 参数

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

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

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

3.9.1.3.2 清除级别

实时防护有三种清除级别（要访问清除级别设置，请单击**文件系统实时防护**部分中的 **ThreatSense 引擎参数设置**，然后单击**清除**）。

不清除 - 不会自动清除被感染文件。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。

正常清除 - 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。屏幕右下角的通知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，程序将提供其他后续操作。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，则会删除整个压缩文件。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。

3.9.1.3.3 检查实时防护

要验证实时防护是否工作，是否在检测病毒，请使用测试文件 eicar.com。此测试文件是一个可供所有病毒防护程序检测的无害文件。此文件由 EICAR（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。此文件可从以下网站下载：http://www.eicar.org/download/eicar.com

3.9.1.3.4 何时修改实时防护配置

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

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

3.9.1.3.5 实时防护不工作时如何应对

在本章中，我们将介绍使用实时防护时可能出现的问题，以及如何排除这些故障。

实时防护被禁用

如果用户无意中禁用了实时防护，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**未选中。若要启用此选项，请导航至**高级设置** (**F5**)，然后单击**检测引擎** > **文件系统实时防护**> **基本**。确保**自动启动文件系统实时防护**开关已打开。

如果实时防护功能不检测和清除渗透

请确保您的计算机上未安装任何其他病毒防护程序。如果同时启用两种实时防护，它们可能互相冲突。建议您先卸载系统上的任何其他病毒防护程序，再安装 ESET。

实时防护不启动

如果系统启动时实时防护未启动（且**启用实时文件系统防护**已经启用），可能是因为与其他程序发生冲突。 要获取帮助以解决此问题，请联系 ESET 客户服务。

3.9.1.4 计算机扫描

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

提供两种**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定义特定扫描目标。

请参见扫描进度以了解有关扫描进程的更多信息。

扫描计算机

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

自定义扫描

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

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

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

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

可移动磁盘扫描

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

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

您可以使用**扫描后的操作**下拉菜单选择扫描后要执行的操作（离开、关机和重新启动）。

启用扫描后关机 - 当手动计算机扫描完成时，可按计划关机。确认关机对话窗口将显示 60 秒倒计时。单击**取消**以停用请求的关机操作。

注意
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。

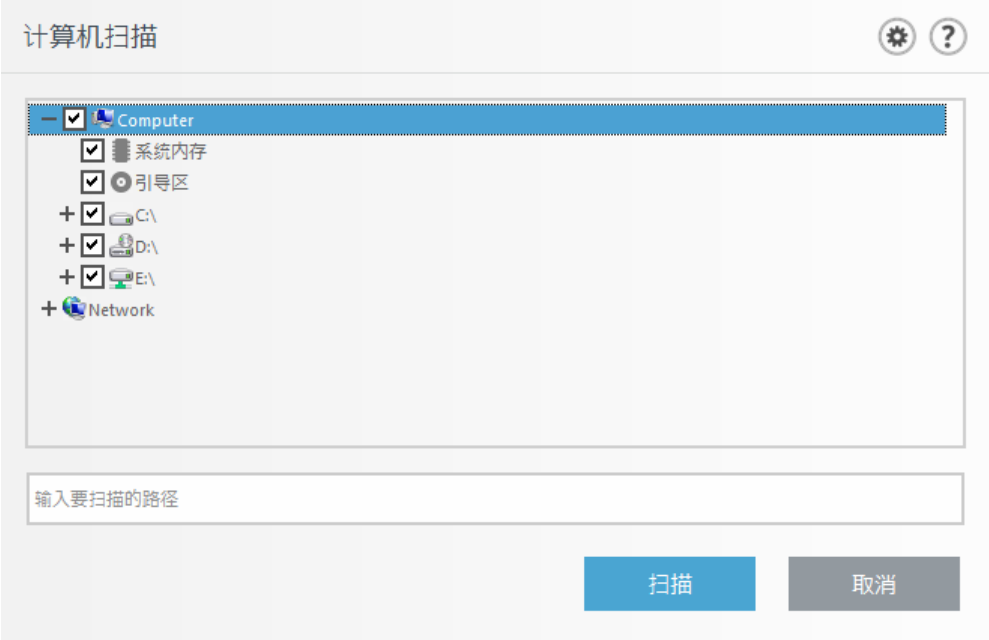
3.9.1.4.1 自定义扫描启动程序

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

扫描目标窗口允许您定义扫描哪些对象（内存、驱动器、扇区、文件和文件夹）中的渗透。从列有计算机上所有可用设备的树结构中选择目标。**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。

若要快速导航到扫描目标或添加目标文件夹或文件，请在文件夹列表下方的空白字段中输入目标目录。仅当树结构中未选择任何目标并且**扫描目标**菜单设置为**未选择**时，才可执行此操作。



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

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

可以从**扫描配置文件**下拉菜单中选择配置文件来用于扫描所选目标。默认配置文件为**智能扫描**。另外有两个预定义的扫描配置文件：名为**全面扫描**和**右键菜单扫描**。这些扫描配置文件使用不同的 ThreatSense 参数。可用选项在**高级设置** > **检测引擎** > **恶意软件扫描** > **手动扫描** > ThreatSense 参数中进行了介绍。

单击**扫描**以使用已设置的自定义参数执行扫描。

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

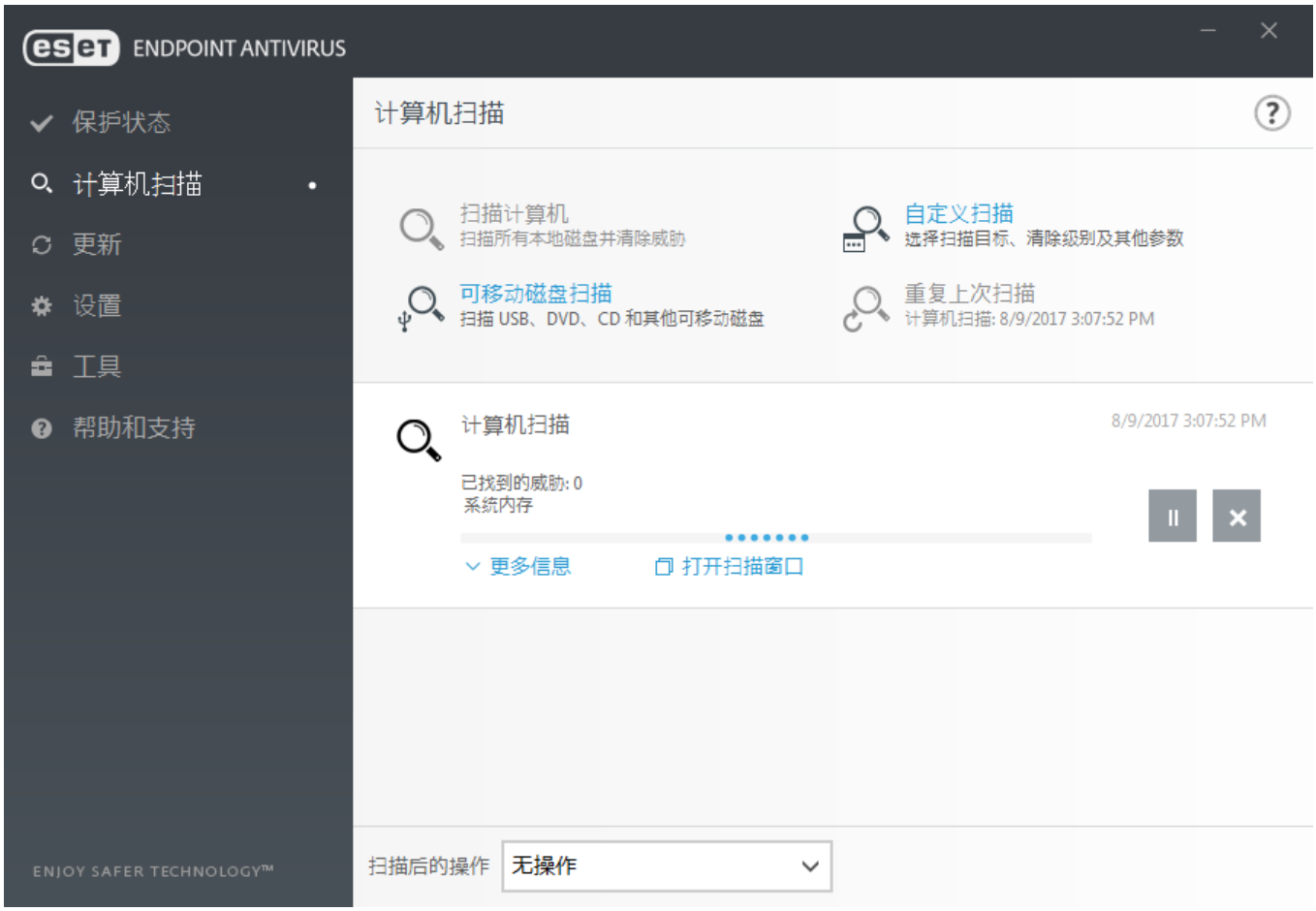
注意
通过单击**显示日志**，您可以在扫描完成时查看计算机扫描日志。

3.9.1.4.2 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状态。扫描进度状态根据扫描对象总数得出。
目标 - 当前扫描的对象的名称及其位置。
已找到的威胁 - 显示在扫描过程中已找到的威胁总数。
暂停 - 暂停扫描。
继续 - 当扫描进度暂停时显示此选项。单击**继续**可继续扫描。
停止 - 终止扫描。
滚动扫描日志 - 如果已启用，扫描日志将随着新条目的添加自动向下滚动，以便显示出最新的条目。



3.9.1.4.3 计算机扫描日志

计算机扫描日志可为您提供关于扫描的常规信息，例如：

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

3.9.1.5 设备控制

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

支持的外部设备：

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

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

打开**集成到系统**旁的开关激活 ESET Endpoint Antivirus 中的设备控制功能；要使此更改生效，需要重新启动计算机。启用设备控制后，**规则**将变为活跃状态，以允许您打开规则编辑器窗口。

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

3.9.1.5.1 设备控制规则编辑器

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

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

复制 - 使用用于其他所选规则的预定义选项创建新规则。

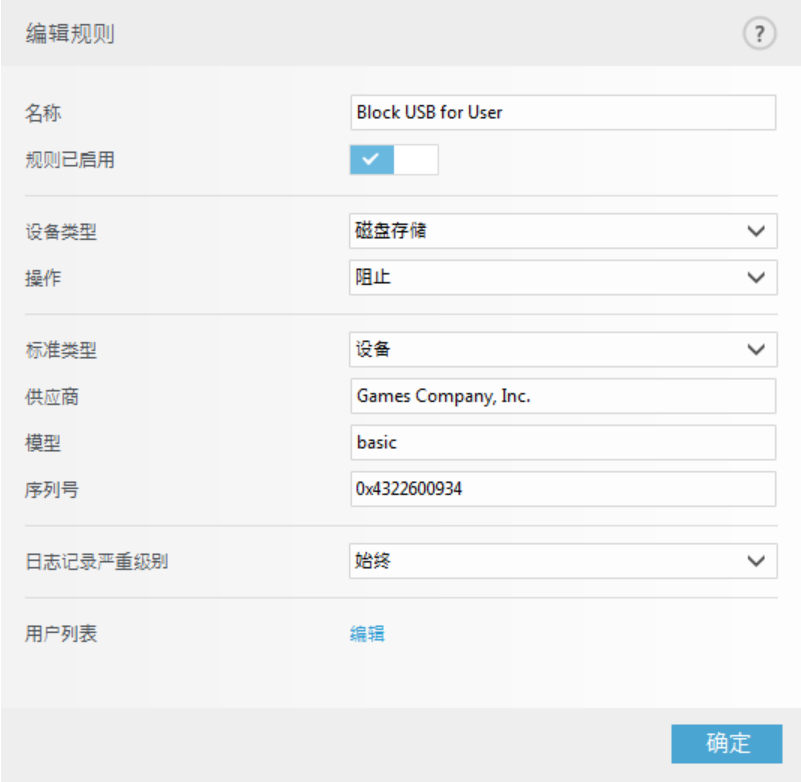
单击**填充**可以为连接到计算机的设备自动填充可移动磁盘设备参数。

按优先级顺序列出规则，具有较高优先级的规则比较靠近顶端。通过单击  **最高** **向上** **向下** **最低**可移动规则，而且还可以单独或成组移动它们。

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

3.9.1.5.2 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。单击**已启用规则**旁的开关以禁用或启用此规则；如果不希望永久删除此规则，这可能会有用。

应用期间 - 允许您在一定时间内应用已创建的规则。在下拉菜单中，选择已创建的时间槽。有关详细信息，请单击此处。

设备类型

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

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

操作

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

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

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

标准类型 - 选择**设备组**或**设备**。

下面显示的其他参数可用于微调规则并根据设备定制。所有参数都不区分大小写：

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

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

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

日志记录严重级别

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

可以通过将规则添加到**用户列表**，来将规则限制为特定用户或用户组：

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

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

3.9.1.6 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。

插入可移动磁盘后要采取的操作 - 选择将可移动磁盘设备插入到计算机 (CD/DVD/USB) 时将执行的默认操作。如果选择了**显示扫描选项**，将显示通知，允许您选择所需操作：

- **不扫描** - 将不执行任何操作，同时将关闭**检测到新设备**窗口。
- **自动设备扫描** - 将执行已插入可移动磁盘设备的手动计算机扫描。
- **显示扫描选项** - 打开可移动磁盘设置部分。

插入可移动磁盘后，将显示以下对话框：

立即扫描 - 这将触发对可移动磁盘的扫描。

稍后扫描 - 将推迟对可移动磁盘的扫描。

设置 - 打开“高级设置”。

始终使用选择的选项 - 选中后，在其他时间插入可移动磁盘时将执行相同的操作。

此外，ESET Endpoint Antivirus 具有设备控制功能，允许您为给定计算机上的外部设备使用定义规则。在设备控制部分可找到设备控制的更多详细信息。

3.9.1.7 空闲状态下扫描

您可以在**病毒防护** > **空闲状态扫描** > **基本**下的高级设置中启用空闲状态扫描程序。将**启用空闲状态扫描**旁边的开关设置为**开**以启用此功能。当计算机处于空闲状态时，会在所有本地驱动器上执行静默的计算机扫描。请参见空闲状态检测触发器，获取触发空闲状态扫描程序必须满足的条件的完整列表。

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

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

当您的计算机处于以下状态时，将运行空闲状态检测：

- 关闭屏幕或屏幕保护程序
- 计算机锁定
- 用户注销

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

3.9.1.8 基于主机的入侵预防系统 (HIPS)

警告

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

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

HIPS 设置可以在**高级设置** (F5) > **病毒防护** > **HIPS** > **基本**中找到。HIPS 状态（已启用 已禁用）显示在**设置** > **计算机**中的 ESET Endpoint Antivirus 主程序窗口内。

ESET Endpoint Antivirus 使用内置的**自我保护**技术作为 HIPS 的一部分，以防止恶意软件损坏或禁用病毒和间谍软件防护。自我保护可保护关键系统及 ESET 的进程、注册表项和文件免于篡改。

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

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

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

可以使用以下四种模式之一执行过滤：

自动模式 - 启用操作（除了保护系统的预定义规则所阻止的操作）。

智能模式 - 仅通知用户极为可疑的事件。

交互模式 - 将提示用户确认操作。

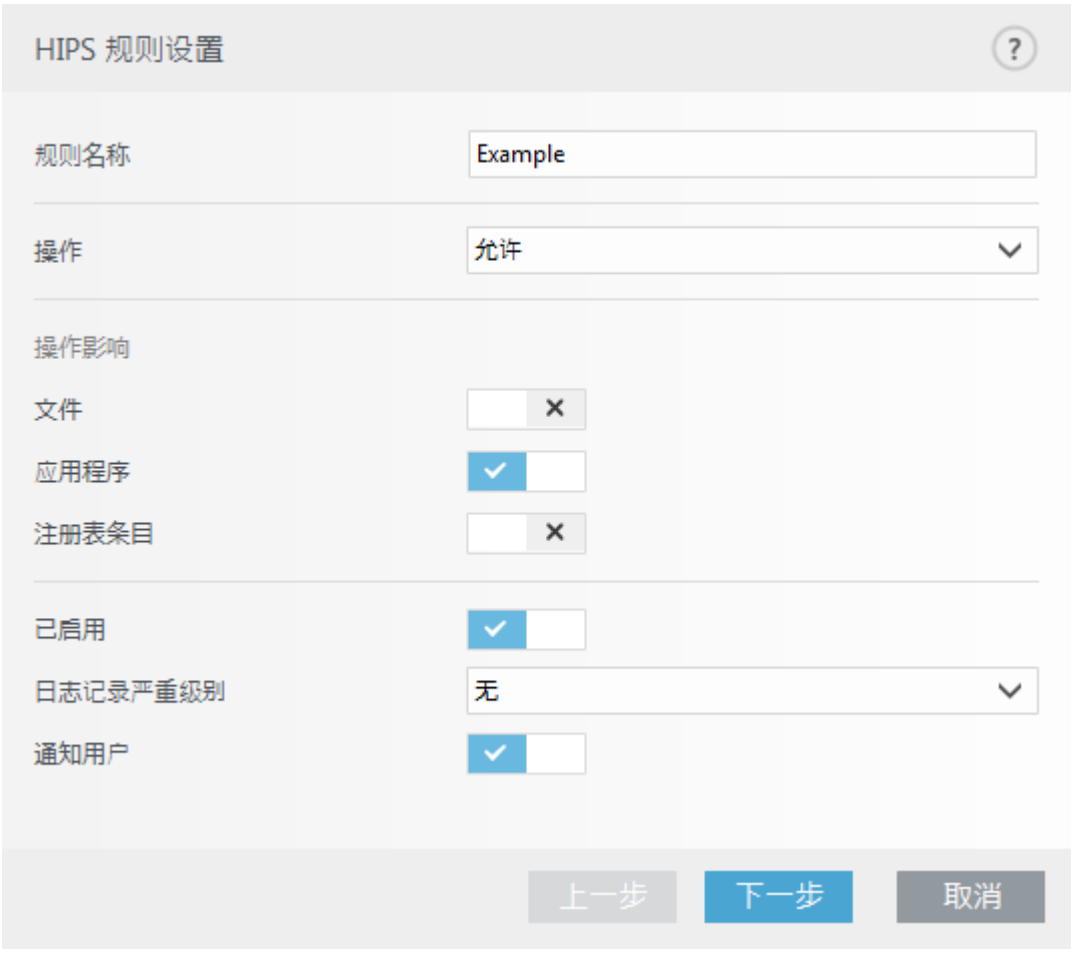
基于策略的模式 - 操作被阻止。

学习模式 - 启用操作，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。当您从 "HIPS 过滤模式 "下拉菜单中选择 "学习模式 "后，**学习模式结束时间**设置将变为可用。选择您想要执行的学习模式的持续时间，最长为 14 天。当指定的持续时间过去后，将会提示您编辑当 HIPS 处于学习模式中时所创建的规则。还可以选择其他过滤模式，或推迟决定并继续使用学习模式。

学习模式到期之后设置的模式 –定义学习模式时间段结束后 ESET Endpoint Antivirus 防火墙将恢复到的过滤模式。

HIPS 系统监控操作系统内的事件，并根据类似于防火墙使用的规则相应地对事件作出反应。单击**编辑**以打开 HIPS 规则管理窗口。在此您可以选择、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. 在**操作影响**部分中，为规则选择至少一项操作。
3. 从下拉菜单中选择**日志记录严重级别**。具有警告严重级别的记录由 Remote Administrator 收集。
4. 选择**通知用户**旁边的滑块以在每次应用规则时显示通知。单击**下一步**。

5. 在**源应用程序**窗口中，从下拉菜单中选择**所有应用程序**，以将新规则应用于尝试执行任何选定操作的所有应用程序。单击**下一步**。
6. 在下面的窗口中，选择**修改其他应用程序的状态**旁边的滑块，并单击**下一步**（所有操作在产品帮助中都有介绍，可按 F1 键进行访问）.
7. 从下拉菜单中选择**特定应用程序**，然后单击**添加**以添加一个或多个要阻止的应用程序。
8. 单击**完成**保存新规则。

3.9.1.8.1 高级设置

以下选项用于调试和分析应用程序的行为：

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

记录所有阻止的操作 - 所有阻止的操作将写入到 HIPS 日志中。

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

有关此帮助页的更新版本，请参阅我们的知识库文章。

3.9.1.8.2 HIPS 交互窗口

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

此对话窗口使您能够基于 HIPS 检测到的任何新操作创建规则，然后定义允许或拒绝此操作的条件。单击**详细信息**可访问具体参数的设置。用这种方式创建的规则被认为等同于手动创建的规则，所以从对话窗口创建的规则可以比触发该对话窗口的规则更笼统。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将使系统在规则或过滤模式发生更改、HIPS 模块更新或系统重启之前始终使用此操作（**允许** 或 **拒绝**）。发生这三项操作中的任意一项后，将删除临时规则。

3.9.1.8.3 检测到潜在的勒索软件行为

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

此对话窗口允许您**提交文件以供分析**或**从检测中排除**。 单击**详细信息**可查看特定的检测参数。

重要信息
必须启用 ESET Live Grid 才能使勒索软件防护正常工作。

3.9.1.9 演示模式

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

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

执行**以全屏模式运行应用程序时自动启用演示模式**时，将在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立即启动演示模式尤为有用。

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

3.9.1.10 开机扫描

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

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

有关计划任务创建和管理的详细说明，请参见创建新任务。

3.9.1.10.1 自动启动文件检查

在创建系统启动文件检查计划任务时，有几个选项可用于调整以下参数：

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

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

还包括两个特定组：

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

上述每个组的要扫描文件列表是固定的。

扫描优先级 - 用于确定何时开始扫描的优先级别：

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

3.9.1.11 文档防护

文档防护功能会在打开 Microsoft Office 文档之前对其进行扫描，还会扫描通过 Internet Explorer 自动下载的文件，如 Microsoft ActiveX 元素。文档防护提供文件系统实时防护之外的另一层防护，可以将其禁用以加强没有运行大容量 Microsoft Office 文档时的系统性能。

集成到系统将启动防护系统。若要修改此选项，请按 F5 打开 高级设置 窗口，并在 高级设置 树中单击**病毒防护** > **文档防护**。

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

3.9.1.12 排除

使用排除可将文件和文件夹排除在扫描之外。要确保对所有对象进行威胁扫描，我们建议您只在绝对有必要时才创建排除。您需要排除某个对象的情况可能包括：在扫描期间会使计算机速度变慢的大型数据库条目扫描，或遇到与扫描冲突的软件（例如备份软件）。

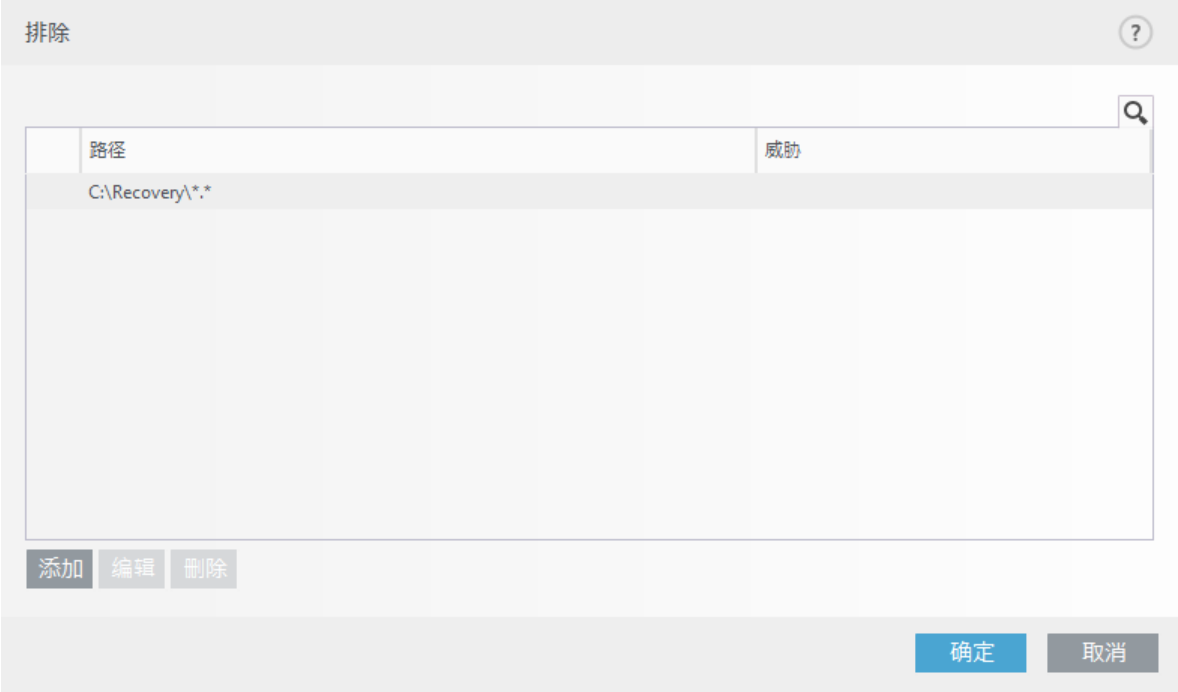
从扫描中排除对象的步骤：

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 (*) 则代表包含零个或更多字符的可变字符串。

示例

- 如果要排除文件夹中的所有文件，则键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）并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。



注意
如果该文件满足不进行扫描的标准，那么文件系统实时防护模块或计算机扫描模块就不会检测到该文件内的威胁。

列

路径 - 已排除文件和文件夹的路径。

威胁 - 如果在已排除文件旁边显示威胁的名称，则表示该文件仅对给定威胁排除。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**），还可以通过依次单击**工具** > **隔离**，然后右键单击隔离文件并从右键菜单中选择**从检测中还原和排除**来创建。

控件元素

添加 - 选择不予检测的对象。

编辑 - 使您能够编辑选定的条目。

删除 - 删除选定的条目。

3.9.1.13 ThreatSense 参数

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。该技术采用代码分析、代码仿真、一般的识别码、病毒库的组合，以显著提高系统安全性。扫描引擎可同时控制多个数据流，最大限度地提高效率和检测速度。ThreatSense 技术还可成功去除 Rootkit。

ThreatSense 引擎设置选项允许您指定若干扫描参数：

- 要扫描的文件类型和扩展名，
- 不同检测方法的组合，
- 清除级别等。

若要进入设置窗口，请单击 **ThreatSense 引擎参数设置**，它位于使用 ThreatSense 技术的任何模块的高级设置窗口中（请参阅下文）。不同的安全情形可能要求不同的配置。考虑到这一点，可针对下列防护模块对 ThreatSense 进行单独配置：

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

ThreatSense 参数已针对每个模块进行了高度优化，对其进行修改可能会明显影响系统操作。例如，将参数更改为始终扫描加壳程序，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。

要扫描的对象

此部分使您可以定义要扫描的计算机组件和文件，以查找渗透。

系统内存 - 扫描攻击系统的系统内存的威胁。

引导区 /UEFI - 扫描引导区和 UEFI 以查找是否存在 Rootkit、Bootkit 和其他恶意软件。有关详细信息，请单击此处。

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），扫描程序能够通过使用代码仿真来识别多种其他类型的加壳程序。

扫描选项

选择在扫描系统中的渗透时所用的方法。有以下选项可供使用：

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

高级启发式扫描 /DNA 病毒库 - 高级启发式扫描包含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。使用高级启发式扫描显著提高了 ESET 产品的威胁检测功能。病毒库可以可靠地检测和识别病毒。利用自动更新系统，可以在发现威胁后的数小时内提供新病毒库。该病毒库的缺点是只能检测到它所知道的病毒（或在这些病毒基础上略做修改的版本）。

潜在的不受欢迎应用程序是一种包含广告软件、将安装工具栏或具有其他不明对象的程序。在某些情况下，用户可能觉得潜在的不受欢迎应用程序的好处多于风险。为此，与其他类型的恶意软件（例如木马程序或蠕虫）相比，ESET 将这些应用程序划分到较低风险类别中。

警告 -发现潜在威胁

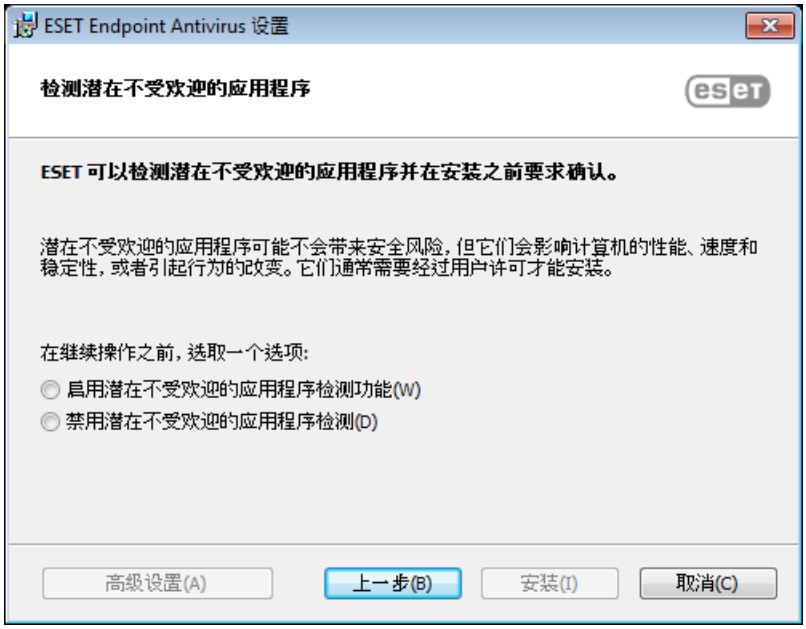
检测到潜在的不受欢迎应用程序后，您将能够确定采取哪种操作：

1. **清除 断开连接**：此选项将终止操作并阻止潜在的威胁进入系统。
2. **不操作**：此选项允许潜在威胁进入系统。
3. 若要使应用程序以后能够在计算机上运行而不受到打扰，请单击**更多信息 显示高级选项**，然后选中**从检测中排除**旁的复选框。

当检测到潜在的不受欢迎应用程序且无法清除时，屏幕右下角将显示消息窗口：**地址已被阻止**。有关此事件的更多信息，请从主菜单导航至**工具** > **日志文件** > **已过滤的网站**。

潜在的不受欢迎应用程序 -设置

安装 ESET 产品时，您可以确定是否启用潜在不受欢迎的应用程序检测，如下所示：

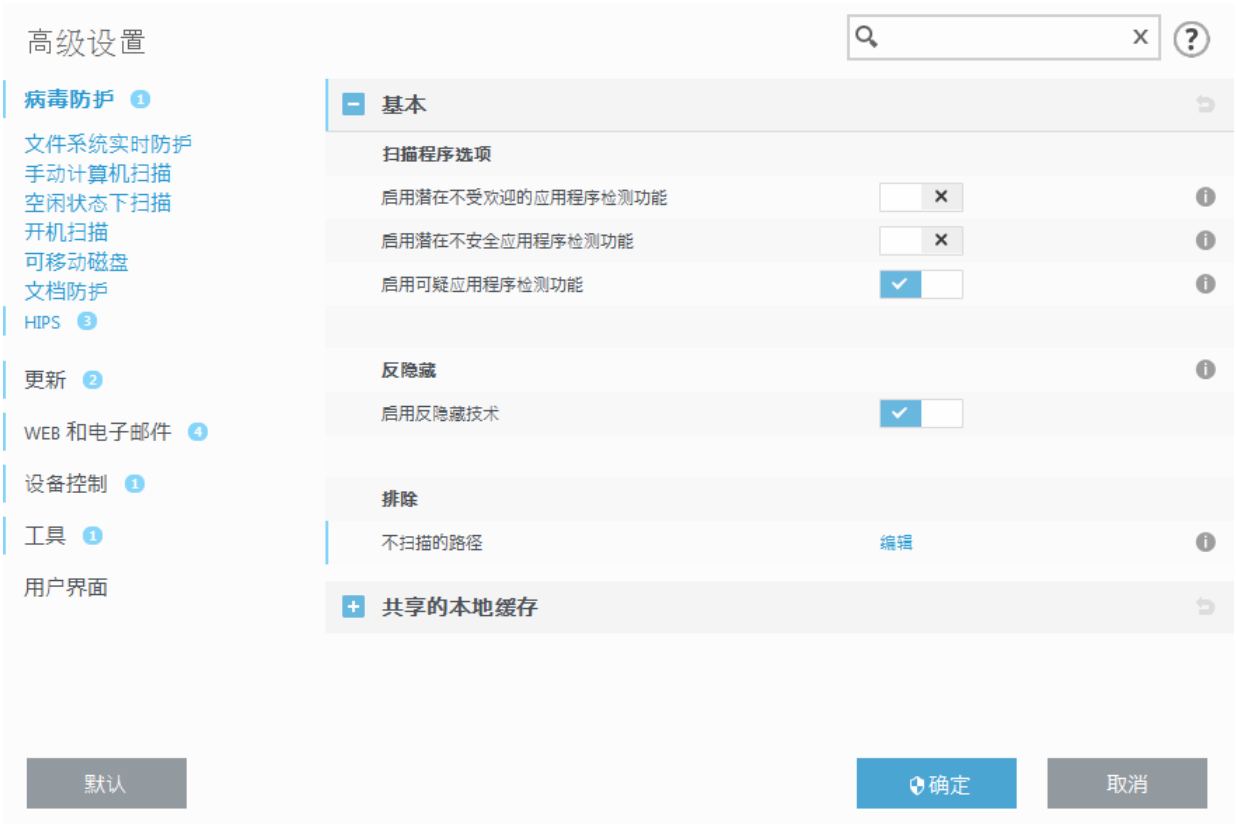


警告

潜在不受欢迎的应用程序可能安装广告软件、工具栏或包含其他不受欢迎和不安全的程序功能。

可随时在程序设置中修改这些设置。若要启用或禁用潜在不受欢迎、不安全或可疑的应用程序检测，请按照以下说明操作：

1. 打开您的 ESET 产品。如何打开我的 ESET 产品？
2. 按 **F5** 键以访问**高级设置**。
3. 单击**病毒防护**并根据您的偏好启用或禁用以下选项：**启用潜在不受欢迎的应用程序检测功能**？**启用潜在不安全应用程序检测功能**和**启用可疑应用程序检测功能**。单击**确定**以确认。



潜在的不受欢迎应用程序 -软件封装程序

软件封装程序是由一些托管文件的网站使用的特殊类型的应用程序修改。它是一种第三方工具，可安装用户想要下载的程序，但会添加附加软件，例如工具栏或广告软件。附加的软件可能还会更改您的 Web 浏览器主页和搜索设置。此外，托管文件的网站通常不会通知软件供应商或下载收件人已进行了修改，并且不会轻易允许取消修改。基于这些原因，ESET 将软件封装程序归类为潜在不受欢迎的应用程序类型，以使用户可以接受或不接受下载。

请参阅此 ESET 知识库文章了解此帮助页的更新版本。

有关详细信息，请单击此处。

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程序，例如远程访问工具、密码破解应用程序以及按键记录器（用于记录用户的每次按键的程序）。此选项默认情况下处于禁用状态。

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 - 不会自动清除被感染文件。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。

正常清除 - 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。屏幕右下角的通知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，程序将提供其他后续操作。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，则会删除整个压缩文件。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。

排除

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

其他

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

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

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

记录所有对象 - 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。

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

限制

限制部分允许您指定要扫描的对象的最大大小和嵌套压缩文件的层数：

对象设置

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

对象的最长扫描时间(秒) - 定义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* 。

压缩文件扫描设置

压缩文件嵌套层数 - 指定压缩文件扫描的最大深度。默认值： *10*.

压缩文件中文件的最大大小 - 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* 。

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。

3.9.1.13.1 排除

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

默认情况下，扫描所有文件。可将任何扩展名添加到不扫描的文件列表中。

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

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。若要将新扩展名添加到列表，请单击**添加**以将该扩展名键入到空白字段中，然后单击**确定**。当您选择**输入多个值**时，您可以添加多个由行、逗号或分号分隔的文件扩展名。启用多项选择时，扩展名将显示在列表中。选择列表中的扩展名，然后单击**删除**可从列表中删除该扩展名。如果您希望编辑选定的扩展名，请单击**编辑**。

可以使用特殊符号 ？（问号）。此 问号表示任意符号。

注意
若要显示 Windows 操作系统中所有文件的扩展名（文件类型），请在**控制面板** > **文件夹选项** > **查看**下取消选中**隐藏已知文件类型的扩展名**。

3.9.2 Web 和电子邮件

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

Internet 连接是个人计算机的一项标准功能。不幸地是，它也成为传输恶意代码的主要媒介。出于此原因，仔细考虑 **Web 访问保护**就变得很重要。

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、IMAP、HTTP 和 MAPI）。

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

禁用 - 单击开关以取消对用于 Web 浏览器和电子邮件客户端的 Web/电子邮件 防护的注册  。

3.9.2.1 协议过滤

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

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

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

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

Web 和电子邮件客户端 - 仅用于 Windows XP 操作系统，允许您选择通过协议过滤为其过滤所有通信的应用程序，不管使用何种端口。

3.9.2.1.1 Web 和电子邮件客户端

注意

从 Windows Vista Service Pack 1 和 Windows Server 2008 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，因此 **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。可以将已使用协议进行通信的应用程序或来自选定路径的应用程序输入到 Web 和电子邮件客户端列表。

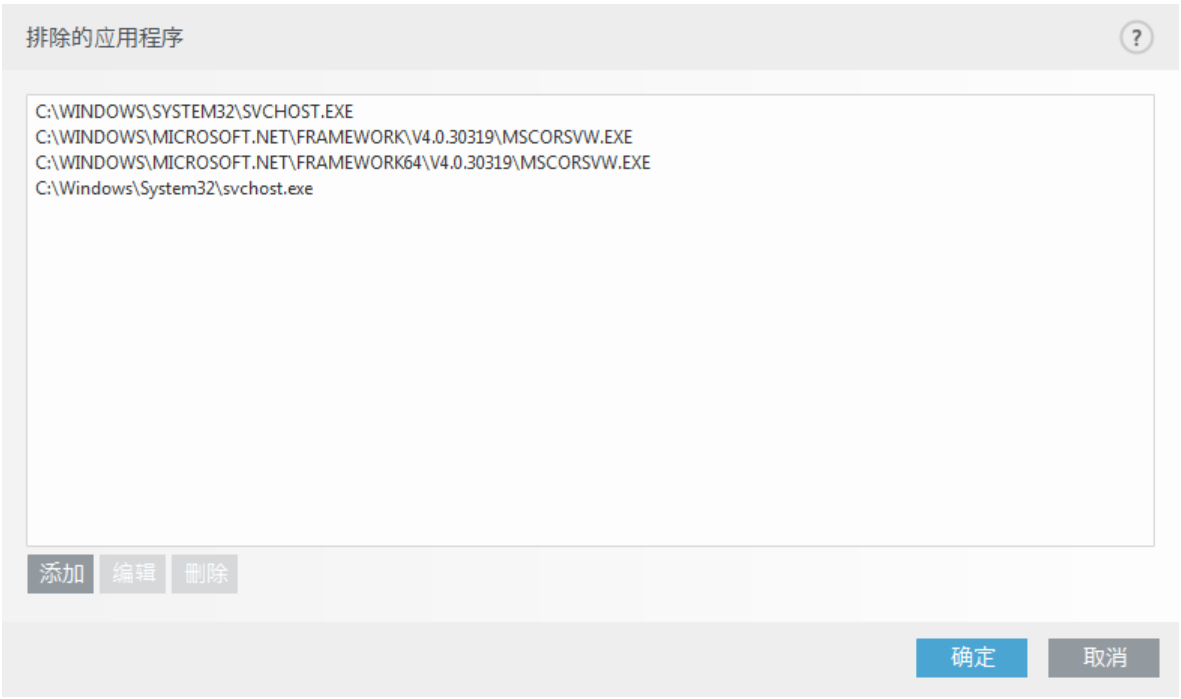
3.9.2.1.2 排除的应用程序

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

单击**添加**后，将自动显示已受协议过滤影响的应用程序和服务。

编辑 - 编辑列表中的选定条目。

删除 - 删除列表中的选定条目。



3.9.2.1.3 排除的 IP 地址

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

添加 - 单击以添加将应用规则的远程点的 IP 地址 /地址范围 /子网。

编辑 - 编辑列表中的选定条目。

删除 - 删除列表中的选定条目。

3.9.2.1.4 SSL/TLS

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

启用 SSL/TLS 协议过滤 - 如果禁用协议过滤，该程序将不会扫描使用 SSL 的通信。

SSL/TLS 协议过滤模式在以下选项中可用：

自动模式 - 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标记为受信任（位于受信任的证书列表上）而用来访问服务器时，会允许对该服务器的通信，也会过滤通信通道的内容。

交互模式 - 如果您输入一个受 SSL 保护的新站点（使用未知证书），将显示操作选择对话框。此模式可用来创建将不扫描的 SSL 证书列表。

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

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

排除使用受信任域的通信 - 域信任由内置白名单确定。

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

根证书

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

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

证书有效性

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

该证书无效或已损坏时 - 这意味着证书已过期或已错误地签名。 在这种情况下，我们建议保持选中**阻止使用该证书的通信**。

3.9.2.1.4.1 加密的 SSL 通信

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

首先，如果网站使用无法验证或无效的证书，而且 ESET Endpoint Antivirus 配置为在此类情况下询问用户（默认情况下，无法验证的证书为 是”，无效的证书为 否”），将显示一个对话框询问您**允许**还是**阻止**该连接。

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

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

3.9.2.1.4.2 已知证书列表

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

已知证书列表窗口包含：

列

名称 - 证书名称。

证书颁发者 - 证书创建者的名称。

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

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

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

控件元素

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

编辑 - 选择您希望配置的证书，然后单击**编辑**。

删除 - 选择您希望删除的证书，然后单击**删除**。

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

3.9.2.1.4.3 SSL/TLS 过滤的应用程序列表

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

SSL/TLS 过滤的应用程序列表窗口包含：

列

应用程序 - 应用程序的名称。

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

控件元素

添加 - 添加过滤的应用程序。

编辑 - 选择您希望配置的证书，然后单击**编辑**。

删除 - 选择要删除的证书，然后单击**删除**。

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

3.9.2.2 电子邮件客户端防护

3.9.2.2.1 电子邮件客户端

ESET Endpoint Antivirus 与电子邮件客户端的集成可提高针对电子邮件中恶意代码的主动防护级别。如果您的电子邮件客户端受支持，则可以在 ESET Endpoint Antivirus 中启用集成。如果激活了集成，则 ESET Endpoint Antivirus 工具栏将直接插入电子邮件客户端（未插入适用于较新版本的 Windows Live Mail 的工具栏），从而提供更高效的电子邮件防护。集成设置位于**设置** > **高级设置** > **Web 和电子邮件** > **电子邮件客户端防护** > **电子邮件客户端**。

电子邮件客户端集成

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

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。

如果使用电子邮件客户端（仅限 MS Outlook）时遇到系统运行缓慢的情况，请启用**禁用对收件箱内容更改的检查**。当从 Kerio Outlook Connector Store 中检索电子邮件时可能会发生这种情况。

要扫描的电子邮件

通过客户端插件启用电子邮件保护 - 在通过电子邮件客户端禁用了电子邮件客户端防护后，仍支持通过协议过滤检查电子邮件客户端。
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。

要对受感染的电子邮件执行的操作

无操作 - 如果已启用，则程序虽能识别感染的附件，但不会对电子邮件采取任何操作。
删除电子邮件 - 程序会通知用户有关渗透的信息并删除邮件。
将电子邮件移到已删除邮件文件夹 - 受感染的电子邮件将自动移至 已删除 邮件文件夹。
将电子邮件移到文件夹 - 受感染的电子邮件将自动移至指定的文件夹。

文件夹 - 指定希望将检测到的受感染电子邮件移到的自定义文件夹。

更新后重新扫描 - 在检测引擎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，电子邮件防护模块会接受其他防护模块的扫描结果（POP3、IMAP 协议扫描）。

注意
我们建议启用选项**通过客户端插件启用电子邮件保护**和**启用通过协议过滤提供电子邮件防护**（高级设置 (F5) > Web 和电子邮件 > 电子邮件客户端防护 > 电子邮件协议）。

3.9.2.2.2 电子邮件协议

IMAP 和 POP3 协议是最广泛地用于在电子邮件客户端应用程序中接收电子邮件通信的协议。无论使用何种电子邮件客户端，ESET Endpoint Antivirus 均提供对这些协议的保护，无需重新配置电子邮件客户端。

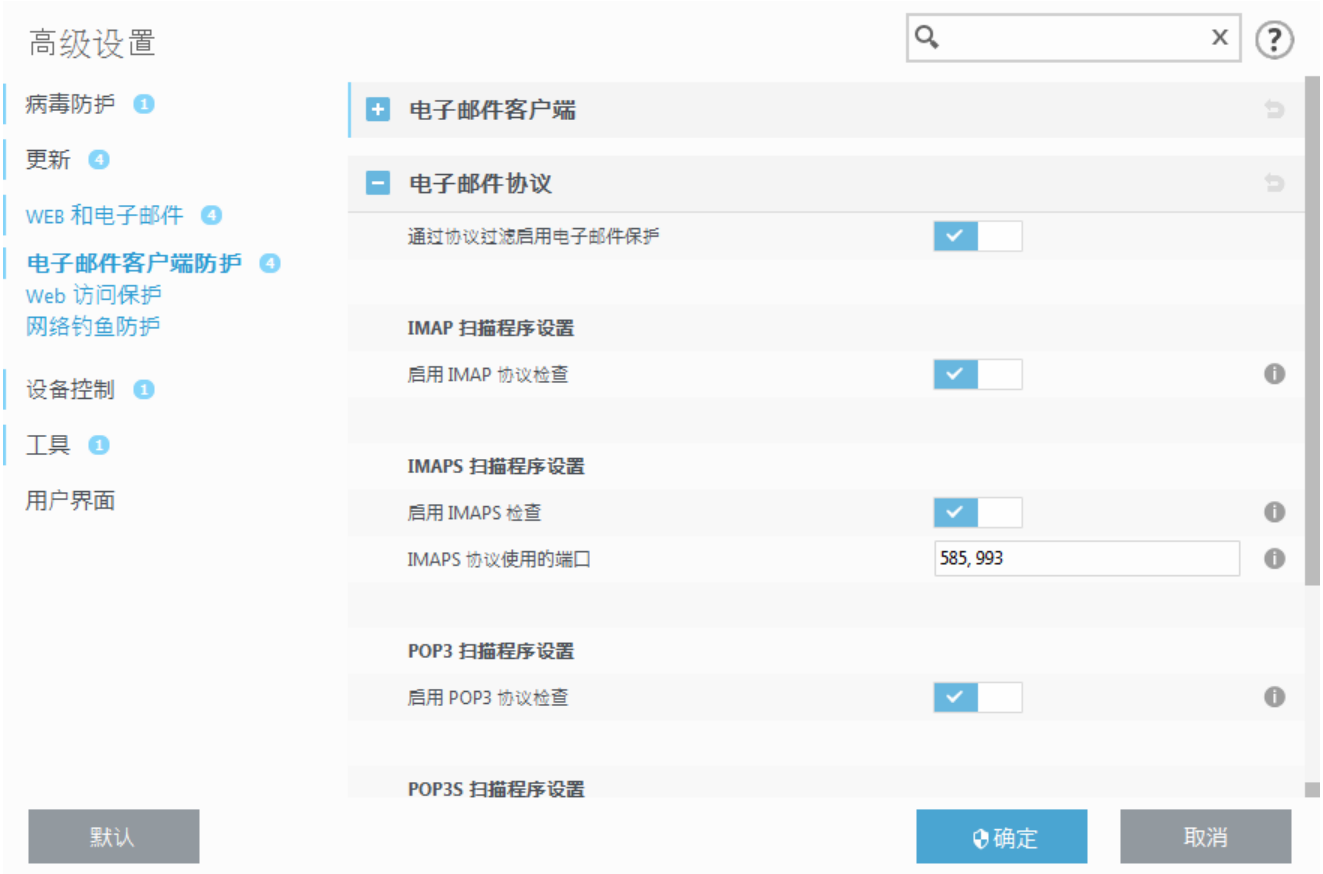
您可以在 高级设置 中配置 IMAP/IMAPS 和 POP3/POP3S 协议检查。若要访问此设置，请依次展开 **Web 和电子邮件** > **电子邮件客户端防护** > **电子邮件协议**。

启用电子邮件协议防护 - 启用电子邮件协议检查。

在 Windows Vista 及更高版本中，将在所有端口上自动检测和扫描 IMAP 和 POP3 协议。在 Windows XP 中，仅针对所有应用程序扫描**由 IMAP/POP3 协议使用的已配置端口**，并且针对标记为 Web 和电子邮件客户端的应用程序扫描所有端口。

ESET Endpoint Antivirus 还支持扫描 IMAPS 和 POP3S 协议，这些协议使用加密通道在服务器和客户端之间传输信息。ESET Endpoint Antivirus 利用 SSL（安全套接字层）和 TLS（传输层安全）协议检查通信。无论操作系统版本如何，该程序将只在 **IMAPS/POP3S 协议使用的端口**中定义的端口上扫描通信。

如果默认设置正在使用中，将不会扫描加密通信。若要启用加密通信扫描，请导航到 高级设置 中的 SSL/TLS、依次单击 **Web 和电子邮件** > **SSL/TLS**，然后选择**启用 SSL/TLS 协议过滤**。



3.9.2.2.3 警报和通知

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 扫描引擎内包含的所有高级扫描方法。这意味着恶意程序检测在与检测引擎匹配之前就已进行。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。

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

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。单击以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**、**在已接收并阅读的被感染电子邮件主题上添加注释**或**在已发送电子邮件上添加标记消息**。请注意，在少数情形下，标记消息可能被有问题的 HTML 邮件忽略，而恶意软件也可能伪造这些消息。可将标记消息添加到已接收 已阅读的电子邮件、已发送的电子邮件或两类邮件中都添加。可用选项包括：

- **从不** - 不添加任何标记消息。
- **仅对被感染的电子邮件** - 仅将包含恶意软件的消息标记为已选中（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。

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

添加到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。

3.9.2.3 Web 访问保护

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

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

我们强烈建议您保持启用 Web 访问保护。在 ESET Endpoint Antivirus 主程序窗口中导航至**设置** > **Web 和电子邮件** > **Web 访问保护**可以访问此选项。

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

- **Web 协议** - 使您可以为大多数 Internet 浏览器使用的这些标准协议配置监视。

- **URL 地址管理** - 使您可以指定要对其阻止、允许或排除检查的 HTTP 地址。
- **ThreatSense 引擎参数设置** - 高级病毒扫描程序设置 -使您能够为 Web 访问保护配置设置，例如要扫描的对象类型（电子邮件、压缩文件等）、检测方法等。

3.9.2.3.1 Web 协议

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

在 Windows Vista 及更高版本中，始终在所有应用程序的所有端口上监视 HTTP 通信。在 Windows XP 中，您可以在**高级设置** (F5) > **Web 和电子邮件** > **Web 访问保护** > **Web 协议** > **HTTP 扫描程序设置**中修改**由 HTTP 协议使用的端口**。在所有应用程序的指定端口上以及标记为 Web 和电子邮件客户端的应用程序的所有端口上监视 HTTP 通信。

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

如果默认设置正在使用中，将不会扫描加密通信。若要启用加密通信扫描，请导航到 高级设置 中的 SSL/TLS、依次单击 **Web 和电子邮件** > **SSL/TLS**，然后选择**启用 SSL/TLS 协议过滤**。

3.9.2.3.2 URL 地址管理

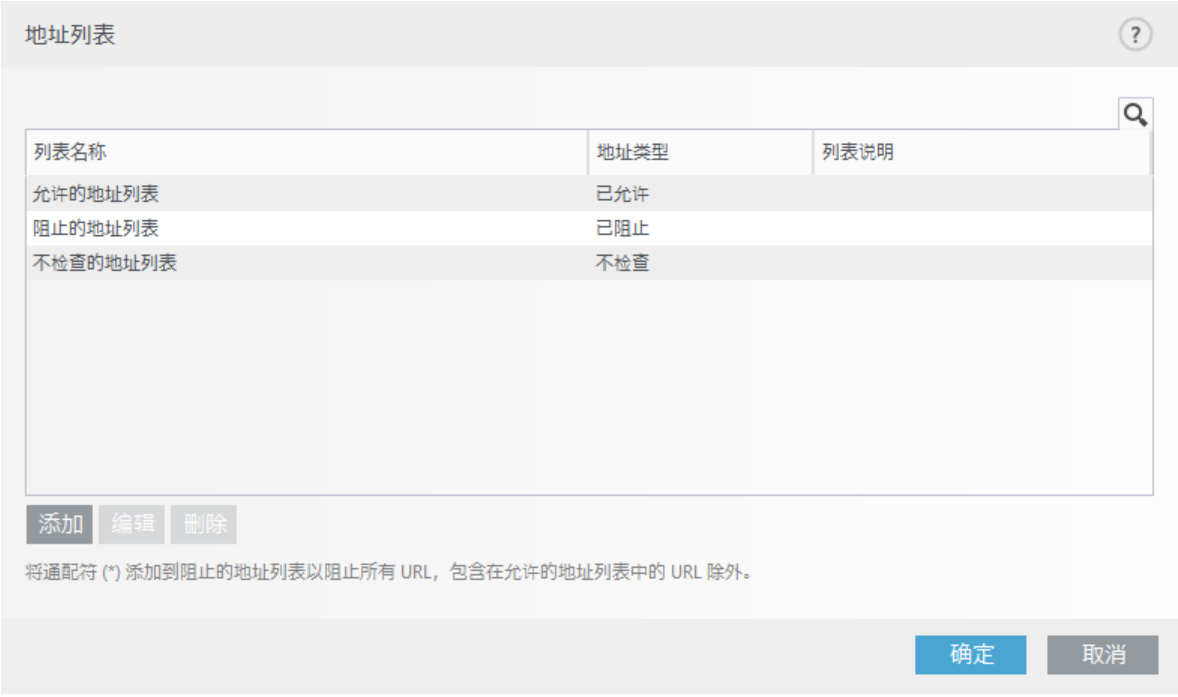
URL 地址管理部分可允许您指定要对其阻止、允许或排除检查的 HTTP 地址。

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

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

在所有列表中，您都可以使用特殊符号 *（星号）和 ？（问号）。星号表示任何数字或字符，而问号表示任一字符。指定排除的地址时，请务必谨慎，因为此列表只应包含信任的和安全的地址。同样，必须确保在此列表中正确使用符号 *和 ?。有关如何安全匹配包括所有子域的整个域，请参阅添加 HTTP 地址 /域掩码。若要激活某个列表，请启用**列出活动**选项。如果您希望在输入来自当前列表的地址时收到通知，请启用**应用时发送通知**。

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



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

编辑 - 修改现有列表。使用此选项从列表中添加或删除地址。

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

3.9.2.4 网络钓鱼防护

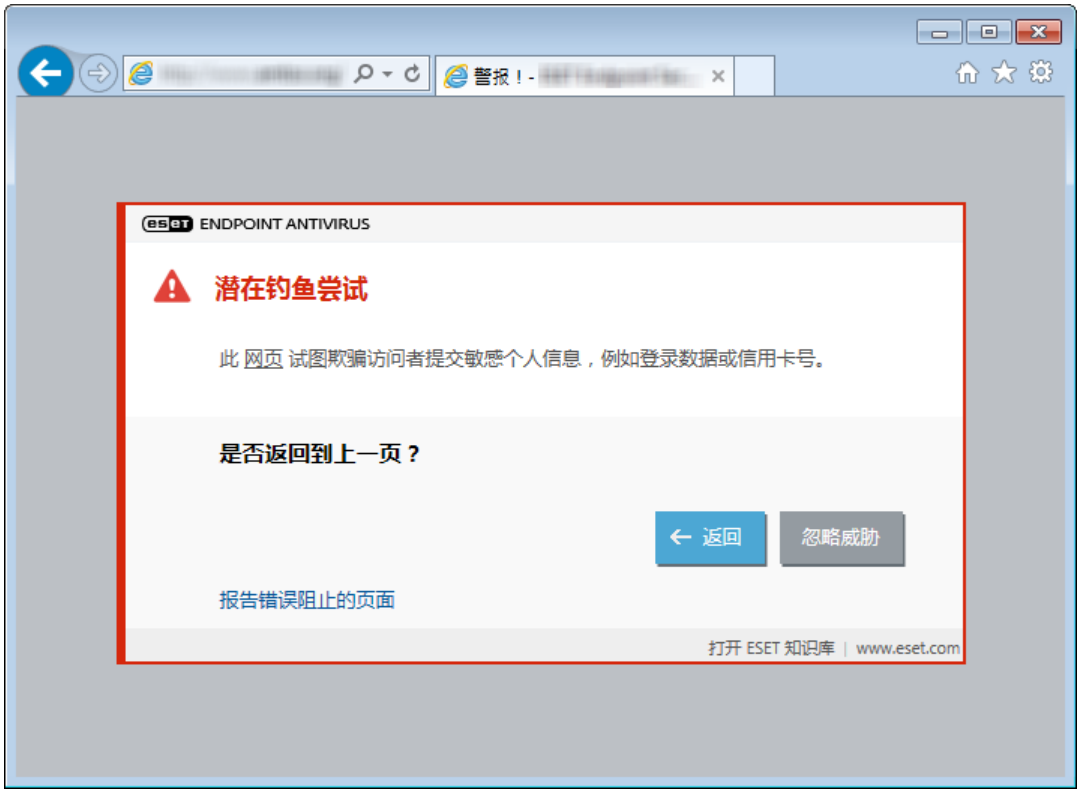
网络钓鱼这一术语是指利用社会工程学（操纵用户以获取机密信息）的一种犯罪活动。网络钓鱼通常用于获取敏感信息（如银行帐号、PIN 码等）的访问权限。在词汇表中阅读此活动的详细信息。ESET Endpoint Antivirus 包括网络钓鱼防护，用于阻止散布此类内容的已知网页。

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

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

访问网络钓鱼网站

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



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

报告网络钓鱼站点

报告链接使您能够向 ESET 报告网络钓鱼 恶意网站以供分析。

注意
向 ESET 提交网站前，确保其满足以下一个或多个标准：

- 未检测到该网站；
- 该网站被错误地检测为威胁。在此情况下，您可以报告误报的网络钓鱼站点。

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

3.9.3 更新程序

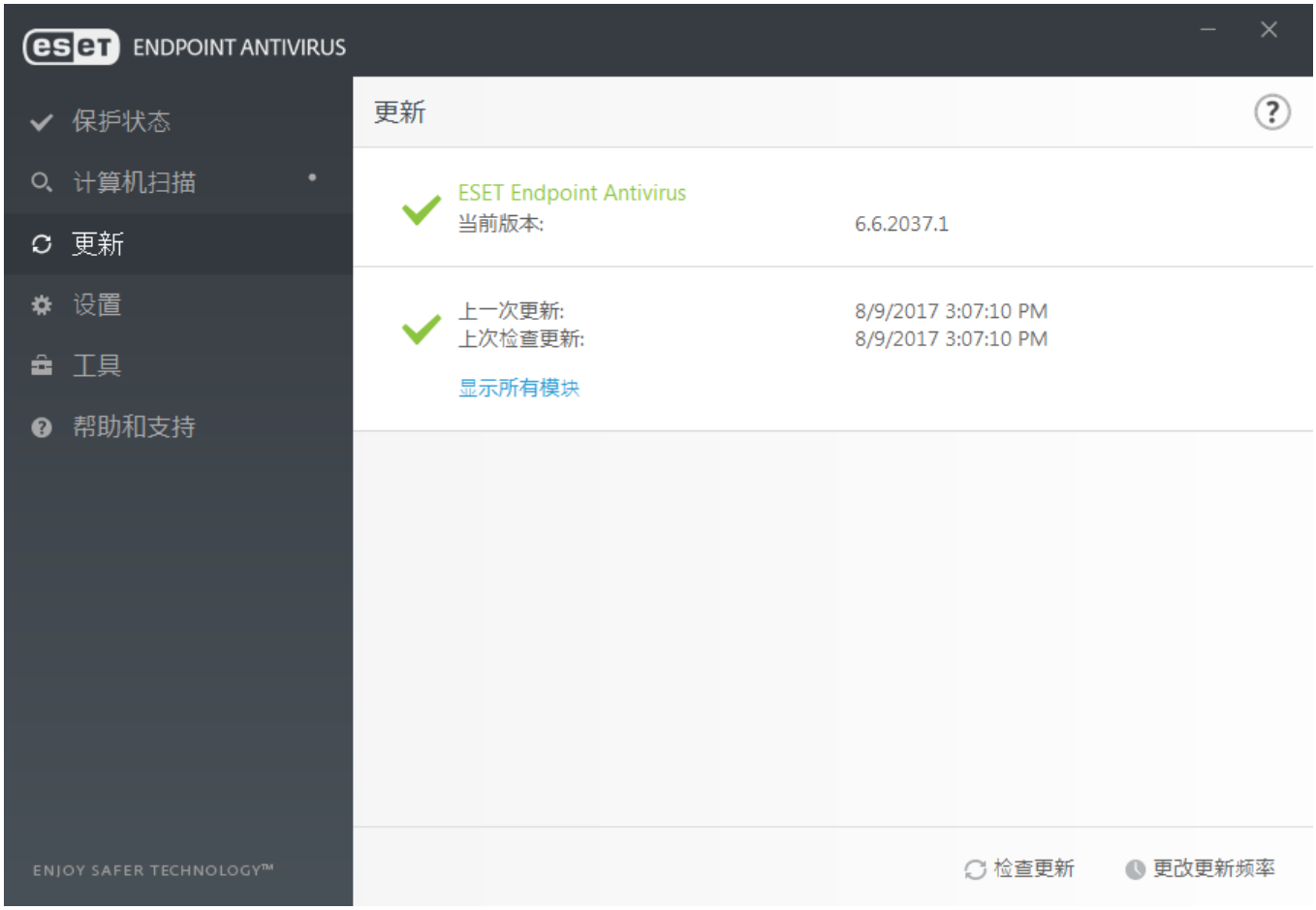
定期更新 ESET Endpoint Antivirus 是获取计算机最高安全级别的最佳方法。更新模块通过两种方式确保程序始终处于最新状态，即更新检测引擎和更新系统组件。

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。您还可以单击**显示所有模块**链接，打开已安装模块列表，查看模块版本和上一次更新。

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

如果您使用脱机许可证文件在没有用户名和密码的情况下激活 ESET Endpoint Antivirus 并尝试更新，则红色信息**检测引擎更新以错误结束**指示您只能从镜像下载更新。

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



当前版本 –ESET Endpoint Antivirus 内部版本编号。

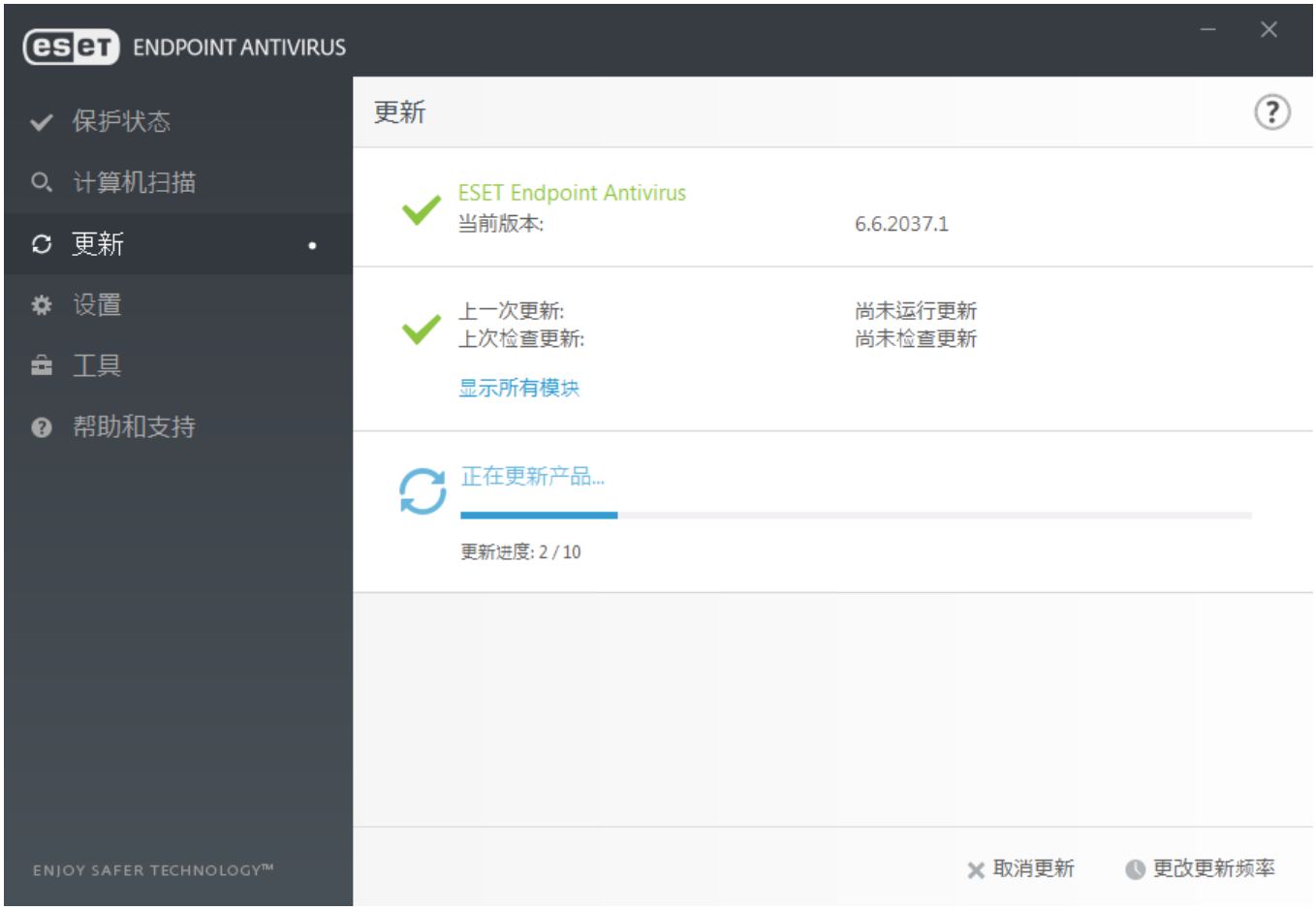
上次更新 - 最近一次更新的日期和时间。确保是最近的日期，表明检测引擎是最新的。

上次检查更新 –上次尝试更新模块的日期和时间。

显示所有模块 –单击该链接以打开已安装模块列表，查看模块版本和上一次更新。

更新过程

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

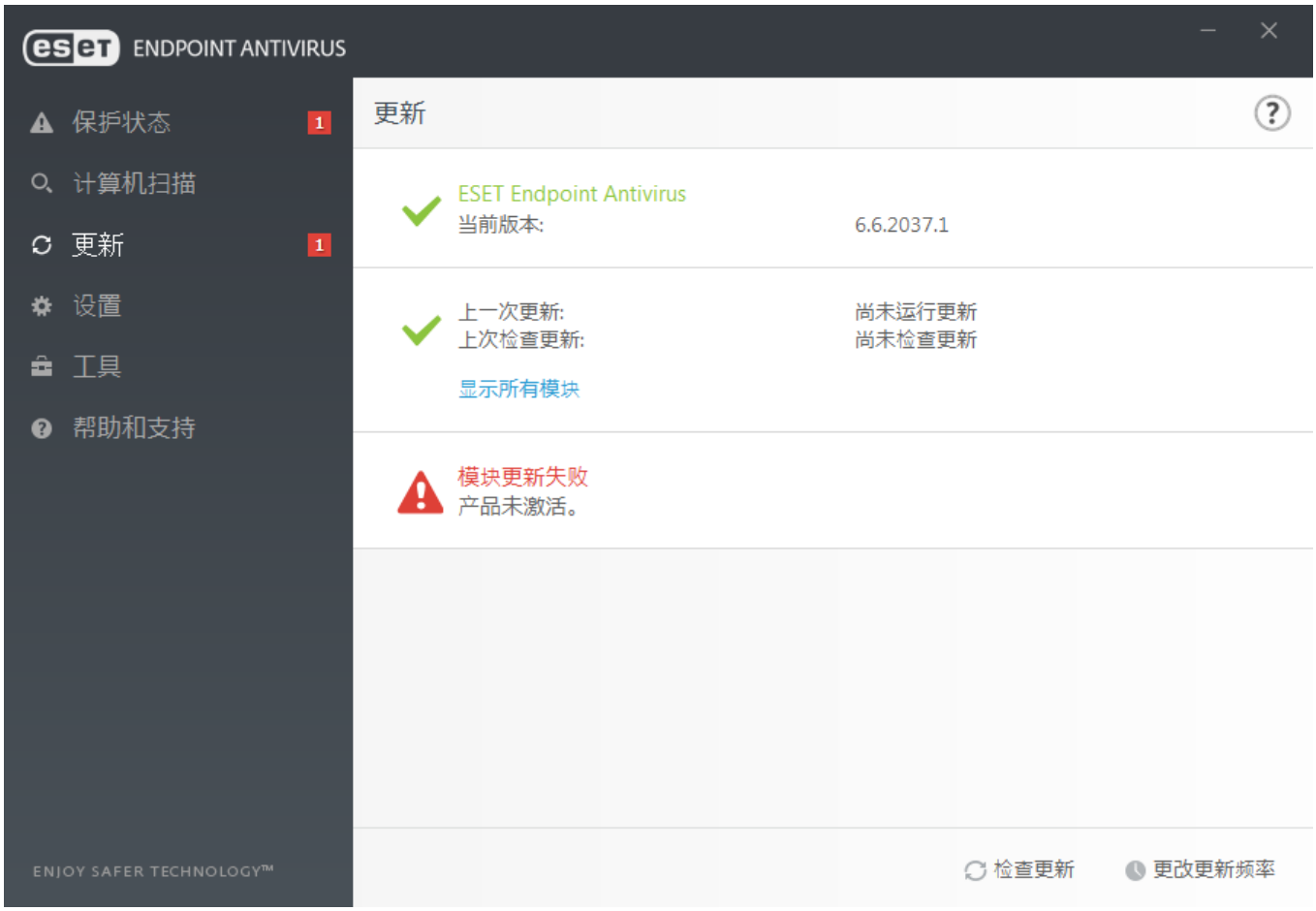


重要信息
在正常情况下，检测引擎每天更新若干次。如果不是这样，则表示程序不是最新的，且更容易被感染。请尽快更新检测引擎。

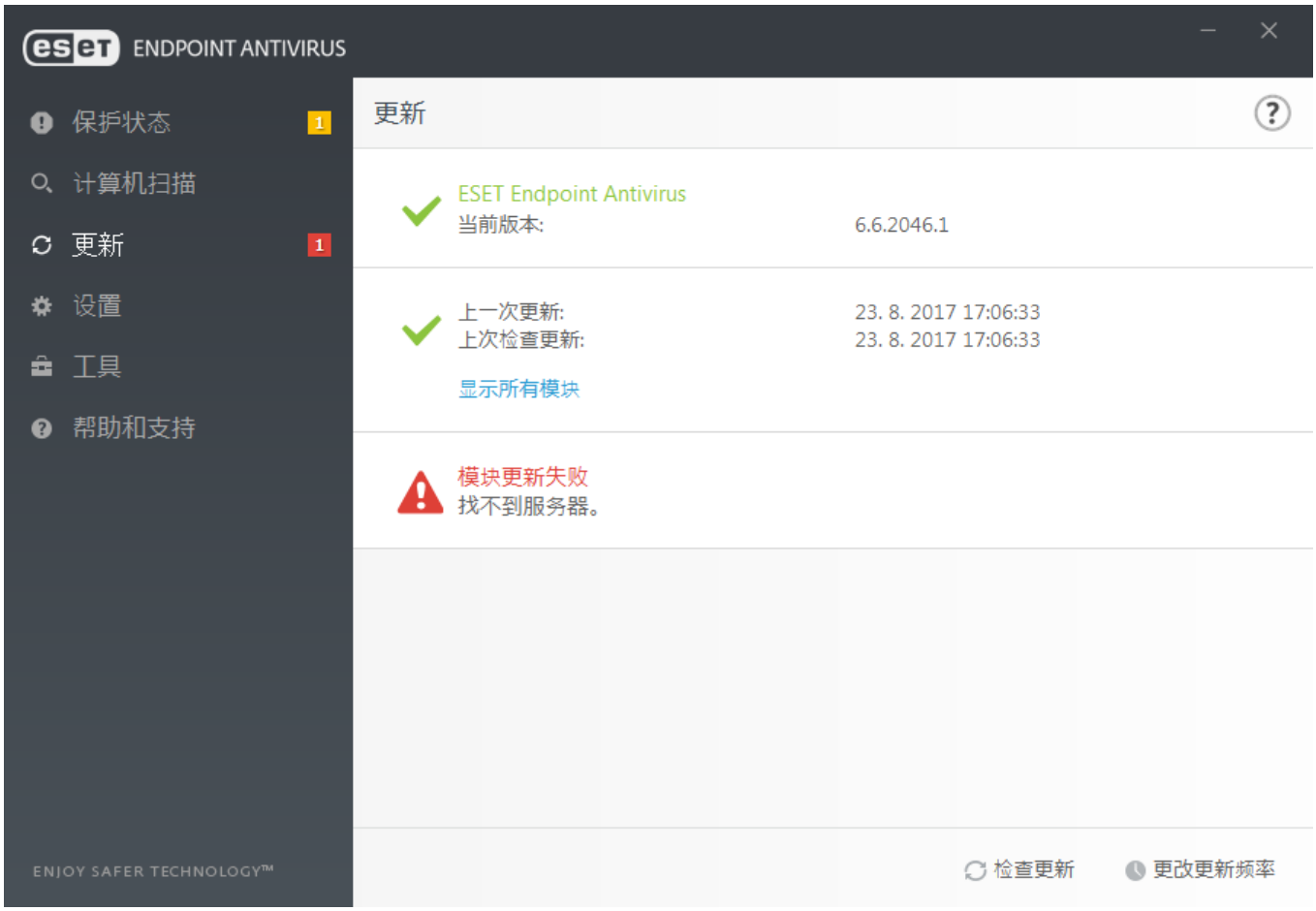
检测引擎已过期 - 此错误将在几次尝试更新检测引擎失败之后显示。建议您检查更新设置。此错误的最常见原因是错误输入了验证数据或错误配置了连接设置。

以前的通知与下列有关不成功更新的两条**检测引擎更新失败**消息相关：

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



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



注意
有关详细信息，请访问此 ESET 知识库文章。

3.9.3.1 更新设置

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

常规

当前使用的更新配置文件显示在**更新配置文件**下拉菜单中。若要创建新配置文件，请导航到**配置文件**选项卡、单击**配置文件列表**旁边的**编辑**、输入您自己的**配置文件名称**，然后单击**添加**。

如果您在尝试下载模块更新时遇到困难，请单击**清除**以清除临时更新文件 *缓存*。

过期的检测引擎警报

自动设置数据库最长保留时长 - 允许设置最长保留时长（以天为单位），在此之后检测引擎将报告为已过期。默认值为 7。

回滚

如果您怀疑检测引擎和 *或*程序模块的新更新不稳定或损坏，可以回滚至以前版本并禁用更新一段时间。此外，您可以启用先前禁用的更新（如果曾将其无限期推迟）。

ESET Endpoint Antivirus 会记录检测引擎和程序模块的快照以用于*回滚*功能。要创建病毒库快照，请保持**创建更新文件快照**开关处于启用状态。**本地存储的快照数量**字段定义了存储的先前病毒库快照的数量。

如果您单击**回滚**（**高级设置** (F5) > **更新** > **常规**），则必须从下拉菜单中选择时间间隔，该间隔表示将暂停检测引擎和程序模块更新的时段。

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

配置文件

若要创建新配置文件，请单击**配置文件列表**旁边的**编辑**，输入您自己的**配置文件名称**，然后单击**添加**。若要编辑已创建的配置文件，请选择已创建的配置文件，然后单击**配置文件列表**旁边的**编辑**。

基本

默认情况下，**更新类型**设置为**定期更新**，以确保更新文件将以最小的网络流量从 ESET 服务器自动进行下载。预发布更新（**预发布更新**选项）是已经经过内部彻底测试的更新，将很快公开提供。您可以通过获得最新检测方法和修补程序，从启用预发布更新中获益。但是，预发布更新可能并不始终稳定，不得在需要最大程度可用性和稳定性的生产服务器和工作站上使用。**延迟更新**允许从提供新版本病毒库的延迟至少 X 小时的特别更新服务器进行更新（即在真实环境中测试并因此视为稳定的数据库）。

禁用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。

从可移动磁盘更新 - 当可移动磁盘包含了创建的镜像时，允许您从该可移动磁盘更新。选中了**自动**后，将在后台运行更新。如果要显示更新对话框，请选中**始终询问**。

默认情况下，**更新服务器**菜单设置为**自动选择**。更新服务器是存储更新的地方。如果使用 ESET 服务器，我们建议您保持选中默认选项。

使用本地 HTTP 服务器（也称为 "镜像"）时，更新服务器应进行如下设置：
http://computer_name_or_its_IP_address:2221

使用启用 SSL 的本地 HTTP 服务器时，更新服务器应进行如下设置：
https://computer_name_or_its_IP_address:2221

使用本地共享文件夹时，更新服务器应进行如下设置：
\\computer_name_or_its_IP_address\shared_folder

从镜像更新

更新服务器的验证基于**许可证密钥**，该密钥在您购买之后生成并发送给您。当使用本地镜像服务器时，您可以先定义凭据，以便客户端在接收更新前登录镜像服务器。默认情况下，无需进行验证并且**用户名**和**密码**字段留空。

3.9.3.1.1 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（这些用户需要备用配置文件以用于定期更改的 Internet 连接属性）尤其有用。

更新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**配置文件列表**旁边的**编辑**，输入您自己的**配置文件名称**，然后单击**添加**。

3.9.3.1.2 更新回滚

如果您单击**回滚**（**高级设置** (F5) > **更新** > **配置文件**），则必须从下拉菜单中选择时间间隔，该间隔表示将暂停检测引擎和程序模块更新的时段。

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

检测引擎版本降级至可用的最旧版本，并作为快照存储在本地计算机文件系统中。

注意
以编号 10646 作为检测引擎的最新版本。10645 和 10643 作为检测引擎快照存储。在下载 10644 之前注意到 10644 现在不可用（例如，因为计算机长时间关闭），并且有更新的更新可用。如果将**本地存储的快照数量**字段设置为 2 并单击**回滚**，检测引擎（包括程序模块）将恢复至版本号 10643。此过程可能需要一些时间。在 ESET Endpoint Antivirus 主程序窗口的更新部分检查检测引擎版本是否已降级。

3.9.3.1.3 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：

- **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。
- **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。
- **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。

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，例如程序更新后自动重新启动服务器可能会造成严重损害。

启用程序组件手动更新 - 默认已禁用。启用并且新版本的 ESET Endpoint Antivirus 可用时，可以在**更新**窗格中检查更新，然后**安装**该新版本。

如果启用了**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 (kB)** 字段中指定的值，程序将显示通知。

3.9.3.1.4 HTTP 服务器

服务器端口 - 默认情况下，服务器端口设置为 2221。

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

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

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 需要填写密码时才填写这些信息。

3.9.3.1.5 连接选项

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

若要配置此类帐户，请在**用以下身份连接到局域网**下拉菜单中选择：

- **系统帐户(默认)**?
- **当前用户**?
- **指定的用户**。

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

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

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

用户名和**密码**设置是可选项。

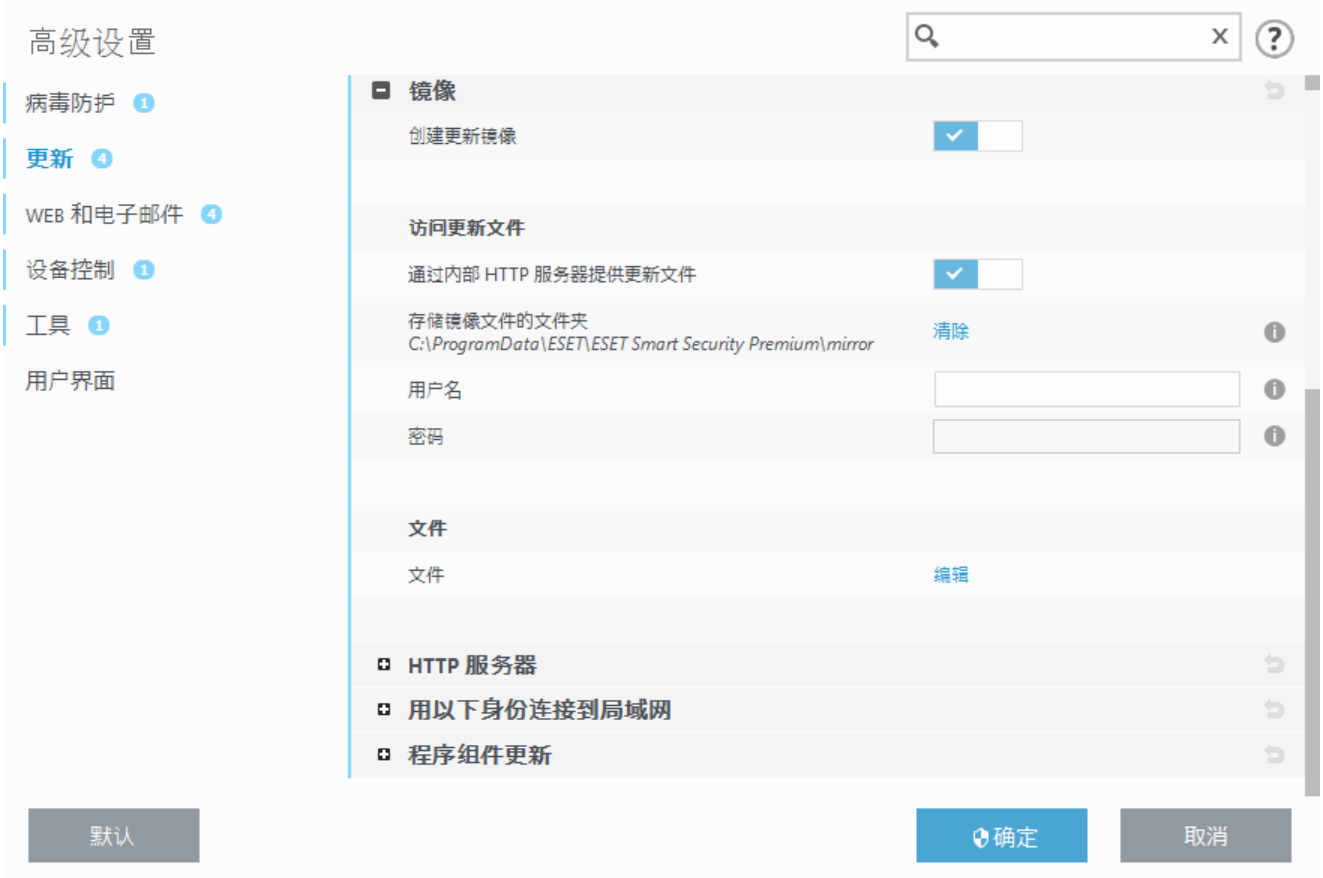
警告
选择**当前用户**或**指定用户**后，如果将程序身份更改为所需用户，可能发生错误。我们建议在主更新设置部分中输入局域网验证数据。在此更新设置部分中，应按如下所示输入验证数据：*domain_name\user*（如果是工作组，请输入 *workgroup_name\name*）和密码。从本地服务器的 HTTP 版本更新时，无需验证。

如果在更新下载后仍与服务器保持连接，则选择**更新后断开与服务器的连接**以强制断开连接。

3.9.3.1.6 更新镜像

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

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



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

访问更新文件

通过内部 HTTP 服务器提供更新文件 - 启用后，通过 HTTP 即可访问更新文件，而无需提供凭据。

> **注意**
> Windows XP 需要 Service Pack 2 或更高版本以使用 HTTP 服务器。

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

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

文件 - 配置镜像后，可指定要下载的更新的语言版本。选定的语言必须受用户配置的镜像服务器支持。

程序组件更新

自动更新组件 - 允许安装新功能并更新现有功能。无需用户介入即可自动执行更新，或者也可以选择收取通知。程序组件更新安装完毕后，可能需要重新启动计算机。

立即更新组件 - 将程序组件更新到最新版本。

3.9.3.1.6.1 从镜像更新

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

使用内部 HTTP 服务器访问镜像

此配置是默认的，在预定义的程序配置中指定。若要允许使用 HTTP 服务器访问镜像，请导航到**高级设置** > **更新** > **配置文件** > **镜像**并选择**创建更新镜像**。

在**HTTP 服务器**部分（**镜像**选项卡内），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。有以下选项可供使用：**无**？**基本**和 **NTLM**。选择**基本**以使用 base64 编码进行基本用户名和密码验证。**NTLM** 选项提供使用安全编码方法的编码。对于验证，将使用在共享更新文件的工作站上创建的用户。默认设置为**无**，此设置授予对更新文件的访问权，无需验证。

警告

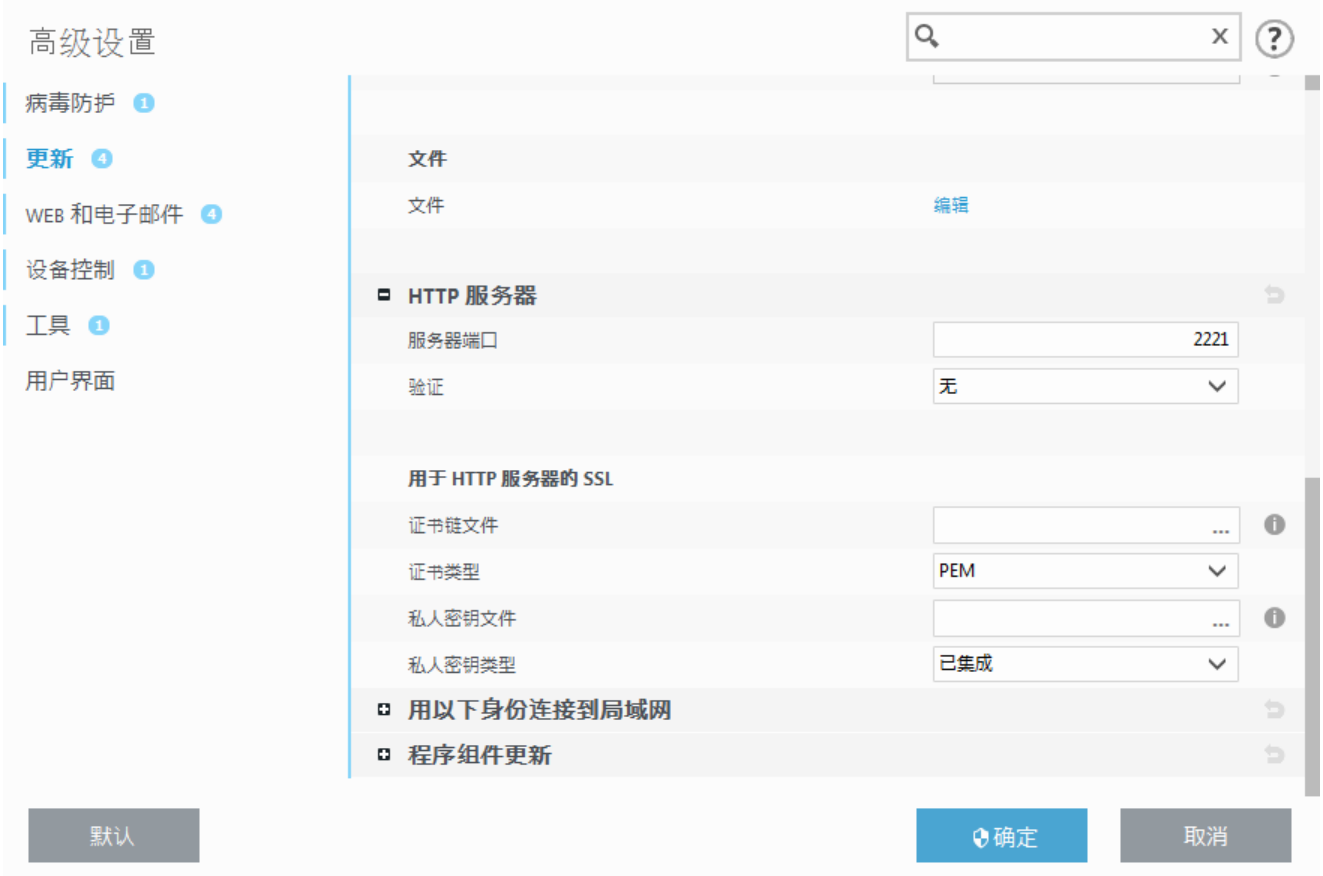
如果您希望允许通过 HTTP 服务器访问更新文件，镜像文件夹必须和创建它的 ESET Endpoint Antivirus 实例位于同一计算机上。

用于 HTTP 服务器的 SSL

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

注意

在几次尝试从镜像更新检测引擎失败之后，将在主菜单的 更新 窗格中显示**用户名和 /或密码无效**错误。我们建议导航到**高级设置** > **更新** > **配置文件** > **镜像**并检查用户名和密码。此错误的最常见原因是错误输入了验证数据。



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

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

通过系统共享访问镜像

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

接下来，继续在**高级设置** > **更新** > **配置文件** > **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**。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)，然后依次单击**更新** > **配置文件** > **用以下身份连接到局域网**。如用以下身份连接到局域网部分所述，此设置和用于更新的设置相同。

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

1. 打开 ESET Endpoint Antivirus **高级设置**，然后依次单击**更新** > **配置文件** > **基本**。
2. 取消**自动选择**，然后采用 *\\UNC\PATH* 格式将新服务器添加到**更新服务器**字段。

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

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。如果激活**程序组件更新**，则无需单击**更新**，因为当文件可用时将自动复制到本地镜像。参见更新模式了解程序组件更新的更多信息。

3.9.3.1.6.2 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限。 所有人 不意味着任何非授权用户，它仅表示文件夹可供所有域用户访问。因此，如果文件夹可供 所有人 访问，仍需要在更新设置部分中输入域用户名和密码。

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

3.9.3.2 如何创建更新任务

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

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

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

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

3.9.4 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（如果 ESET LiveGrid® 已在 ESET Endpoint Antivirus 中启用）
- 计划任务
- 隔离区
- ESET SysInspector

提交样本以供分析 - 允许您提交可疑文件以供 ESET 研究实验室进行分析。单击此选项后显示的对话窗口在提交文件以供分析部分中介绍。

ESET SysRescue - 将您重定向到 ESET SysRescue Live 页面，您可以在其中下载 ESET SysRescue Live 图像或适用于 Microsoft Windows 操作系统的 Live CD/USB Creator。

3.9.4.1 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。日志是系统分析、威胁检测以及故障排除的必要工具。日志记录在后台主动执行，无需用户交互。对信息的记录是根据当前日志级别设置进行的。可直接从 ESET Endpoint Antivirus 环境查看文本消息和日志。还可压缩日志文件。

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

- **检测到的威胁** - 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。它旨在帮助系统管理员和用户解决问题。通常这里找到的信息可以帮助您找到程序中所发生问题的解决方案。
- **计算机扫描** - 所有扫描结果显示在此窗口中。每一行对应一个计算机控件。双击任意条目以查看相应扫描的详细信息。
- **阻止的文件** –包含已阻止且无法访问的文件的记录。该协议显示阻止文件的理由和源模块，以及执行该文件的应用程序和用户。
- **HIPS** - 包含特定规则的记录，这些规则标记为用于记录。该协议显示调用操作的应用程序、结果（无论已允许还是已禁止规则）以及所创建的规则的名称。
- **已过滤的网站** -此列表可用于查看被 Web 访问保护阻止的网站的列表。 在这些日志中，您可以查看时间、URL、用户和打开了到特定网站的连接的应用程序。
- **设备控制** - 包含与计算机连接的可移动磁盘或设备的记录。只有具有设备控制规则的设备才会记录到日志文件。如果规则不匹配连接的设备，则不会创建所连接设备的日志条目。您还可以在这里找到设备类型、序列号、供应商名称和磁盘大小（如果可用）等详细信息。

在每一部分中，显示的信息都可以复制到剪贴板（键盘快捷方式为 **Ctrl + C**），方法是选择条目并单击**复制**。**Ctrl** 和 **Shift** 键可用于选择多个条目。

单击 **过滤**以打开**日志过滤**窗口，您可以在该窗口中定义过滤条件。

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：

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

3.9.4.1.1 在日志中搜索

日志存储重要系统事件的相关信息。日志过滤功能可以显示特定类型事件的记录。

将搜索关键字输入到**查找文本**字段中。如果希望在特定列中搜索关键字，则在**在列中搜索**下拉菜单中更改过滤器。

记录类型 - 从下拉菜单选择一个或多个记录日志类型：

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

时段 - 定义想要显示其结果的时段。

仅全字匹配 - 如果想要搜索特定的全字以得到更精确的结果，则选中此复选框。

区分大小写 - 如果在过滤时使用大写或小写对您很重要，则启用此选项。

向上搜索 - 将首先显示出现在文档中较高处的搜索结果。

3.9.4.2 代理服务器设置

在大型局域网网络中，计算机与 Internet 之间的通信可通过代理服务器进行协调。使用此配置时需要定义以下设置。否则程序将无法自动更新。在 ESET Endpoint Antivirus 中， 高级设置 树中的两个不同部分提供了代理服务器设置。

首先，可以在**高级设置**（在**工具** > **代理服务器**下）中配置代理服务器设置。在此级别指定的代理服务器定义了所有 ESET Endpoint Antivirus 的全局代理服务器设置。此处的参数将用于需要连接到 Internet 的所有模块。

若要指定此级别的代理服务器设置，请选中**使用代理服务器**，然后在**代理服务器**字段输入代理服务器地址以及该代理服务器的**端口**号。

如果与代理服务器的通信需要验证，请选中**代理服务器需要验证**，然后在相应字段中输入有效**用户名**和**密码**。单击**检测**以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
您必须在**代理服务器**设置中输入用户名和密码。

如果代理不可用，请使用直接连接 - 如果将产品配置为利用 HTTP 代理，并且该代理不可访问，该产品将绕过代理，直接与 ESET 服务器通信。

还可以在 高级更新 设置中建立代理服务器设置（通过从**代理模式**下拉菜单中选择**通过代理服务器连接**来选择**高级设置** > **更新** > **配置文件** > **更新** > **连接选项**）。此设置适用于给定更新配置文件，并建议笔记本电脑用户使用，因为他们经常从远程位置接收检测引擎更新。有关此设置的详细信息，请参阅高级更新设置。

3.9.4.3 计划任务

计划任务管理和启动具有预定义配置和属性的计划任务。

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

任务计划用于计划以下任务：检测引擎更新、扫描任务、系统启动文件检查以及日志维护。您可以直接从主 计划任务 窗口中添加或删除任务（单击底部的**添加任务**或**删除**）。在 计划任务 窗口中右键单击任意位置可执行以下操作：显示详细信息、立即执行任务、添加新任务和删除现有任务。使用每个条目开头的复选框来启用 停用任务。

默认情况下，**计划任务**中显示以下计划任务：

- **日志维护**
- **定期自动更新**
- **拨号连接后自动更新**
- **用户登录后自动更新**
- **自动启动文件检查**（用户登录后）
- **自动启动文件检查**（模块更新成功后）

要编辑现有计划任务（包括默认和用户定义的）的配置，请右键单击任务然后单击**编辑 ...**，或选择要修改的任务然后单击**编辑**按钮。

添加新任务

1. 单击窗口底部的**添加任务**。
2. 输入任务的名称。

3. 从下拉菜单中选择所需任务：

- **运行外部应用程序** - 计划外部应用程序的执行。
- **日志维护** - 日志文件中还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。
- **创建计算机扫描** - 创建 ESET SysInspector 计算机快照 -收集有关系统组件的详细信息（例如，驱动程序、应用程序）并评估每个组件的风险级别。
- **手动计算机扫描** - 执行计算机上文件和文件夹的计算机扫描。
- **更新** - 通过更新检测引擎和程序模块，计划更新任务。

4. 如果要激活任务（您可以之后通过选中 取消选中计划任务列表中的复选框来执行此操作），请打开**启用**开关，单击**下一步**并选择其中一个计时选项：

- **一次** - 任务将在预定义的日期和时间执行。
- **重复** - 任务将以指定的时间间隔执行。
- **每天** - 任务将在每天的指定时间重复运行。
- **每周** - 任务将在选定的星期和时间运行。
- **由事件触发** - 任务将在发生指定事件时执行。

5. 在便携式计算机靠电池供电时，选择**靠电池供电时跳过任务**以最大限度地减少系统资源。将在**任务执行**字段中指定的日期和时间运行该任务。如果任务无法在预定义的时间运行，可以指定其再次执行时间：

- **在下一个计划时间**
- **尽快**
- **如果自上次运行时间之后经过的时间超过指定值，则立即跳过任务**（可使用**自上次运行时间之后经过的时间**滚动框来定义间隔）

您可以通过右键单击并单击**显示任务详细信息**来查看计划任务。

3.9.4.4 防护统计

要查看与 ESET Endpoint Antivirus 的防护模块相关的统计数据的图表，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。

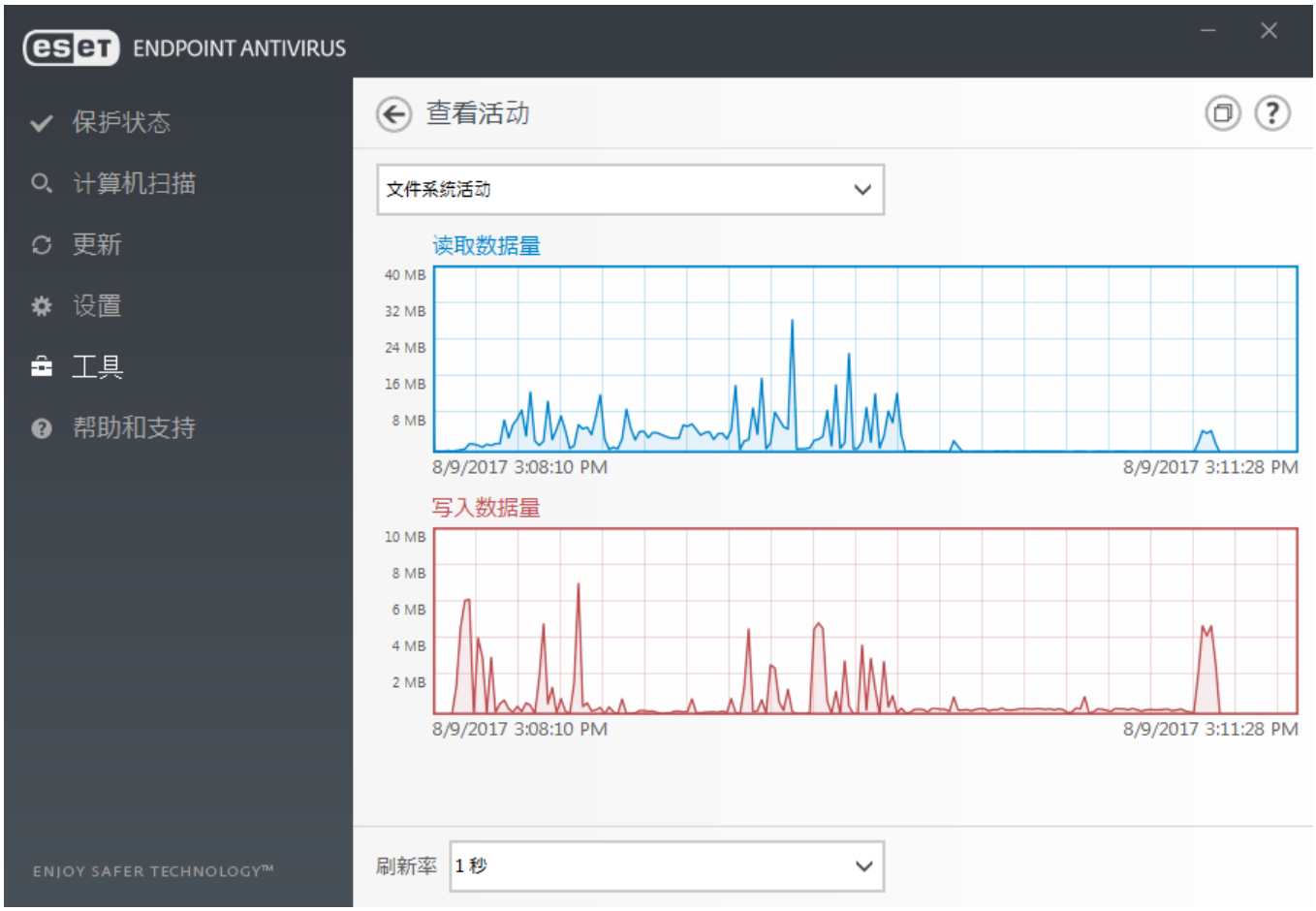
以下统计图表可供使用：

- **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 访问和网络钓鱼防护** - 仅显示 Web 浏览器下载的对象。

在统计图表旁边，您可以看到所有已扫描对象数、被感染对象数、已清除对象数和干净对象数。单击**重置**以清除统计信息，或单击**全部重置**以清除并删除所有现有数据。

3.9.4.5 查看活动

要以图表方式查看当前**文件系统活动**，请单击**工具** > **查看活动**。图表的底部是时间线，用于实时记录选定时间范围内的文件系统活动。若要更改时间范围，请从**刷新率**下拉菜单中进行选择。



有以下选项可供使用：

- **步进:1 秒** - 图表每秒刷新一次，时间线范围为最后 10 分钟。
- **步进:1 分钟(最后 24 小时)** - 图表每分钟刷新一次，时间线范围为最后 24 小时。
- **步进:1 小时(最后一个月)** - 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量（蓝色）和写入的数据量（红色）。两个值均以 KB（千字节） /MB/GB 为单位。如果将鼠标移到图表下方图例中的读取数据或写入数据的上方，图表将仅显示该活动类型的数据。

3.9.4.6 ESET SysInspector

ESET SysInspector 是一个可彻底检查计算机、收集有关系统组件（例如，驱动程序和应用程序、网络连接或重要注册表项）的详细信息以及评估每个组件风险级别的应用程序。该信息有助于确定可能由于软硬件不兼容或恶意感染而导致出现可疑系统行为的原因。

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：

- **打开** - 打开已创建的日志。还可以右键单击给定日志文件，然后在右键菜单中选择**显示**。
- **比较** - 比较两个现有日志。
- **创建 ...**- 创建新日志。请在 ESET SysInspector 完成（日志状态将显示为 "已创建"）之前稍作等待，完成后再尝试访问日志。
- **删除** - 删除列表中选定的日志。

当选中一个或多个日志文件时，右键菜单中的以下项将为可用：

- **显示** - 在 ESET SysInspector 中打开选定日志（相当于双击日志）。
- **比较** - 比较两个现有日志。
- **创建 ...**- 创建新日志。请在 ESET SysInspector 完成（日志状态将显示为 "已创建"）之前稍作等待，完成后再尝试访问日志。
- **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*。

3.9.4.7 ESET LiveGrid®

ESET LiveGrid® 是包含多种基于云的技术的高级预警系统。它帮助基于信誉检测新威胁，并通过白名单提高扫描性能。新威胁信息将实时传输到云，这使 ESET 恶意软件研究实验室能够提供及时的响应，并始终提供持续的防护。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，并从 ESET LiveGrid® 获取其他信息。安装 ESET Endpoint Antivirus 时，请选择以下选项之一：

1. 您可以决定不启用 ESET LiveGrid®。您的软件不会失去任何功能，但在某些情况下，ESET Endpoint Antivirus 可能会比检测引擎更新更慢地响应新威胁。
2. 您可以配置 ESET LiveGrid® 以提交关于新威胁以及检测到的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 LiveGrid® 将收集您的计算机中与新检测到的威胁相关的信息。这些信息可能包括出现威胁的文件的样本或副本、该文件的路径、文件名、日期和时间、威胁出现在计算机上的过程，以及有关您的计算机操作系统的信息。

默认情况下，ESET Endpoint Antivirus 配置为提交可疑文件以供 ESET 病毒实验室详细分析。始终排除具有特定扩展名的文件（例如 *.doc* 或 *.xls*）。如果您或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 LiveGrid® 信誉系统提供了基于云的白名单和黑名单。若要访问 ESET LiveGrid® 的设置，请按 **F5** 以进入 "高级设置"，然后依次展开**工具** > **ESET LiveGrid®**。

启用 ESET LiveGrid® 信誉系统(建议) - ESET LiveGrid® 信誉系统通过将已扫描的文件与云中白名单和黑名单项目数据库进行比较，可提高 ESET 恶意软件防护解决方案的效率。

提交匿名统计 - 允许 ESET 收集有关新检测到的威胁的信息，如威胁名称、检测日期和时间、检测方法和相关联的元数据、产品版本以及配置，其中包括有关您的系统的信息。

提交文件 - 将类似威胁的可疑文件和 / 或具有不正常特征或行为的可疑文件提交给 ESET 以供分析。

选择**启用日志记录**以创建记录文件和统计信息提交的事件日志。这将启用在发送文件或统计信息后记录到事件日志。

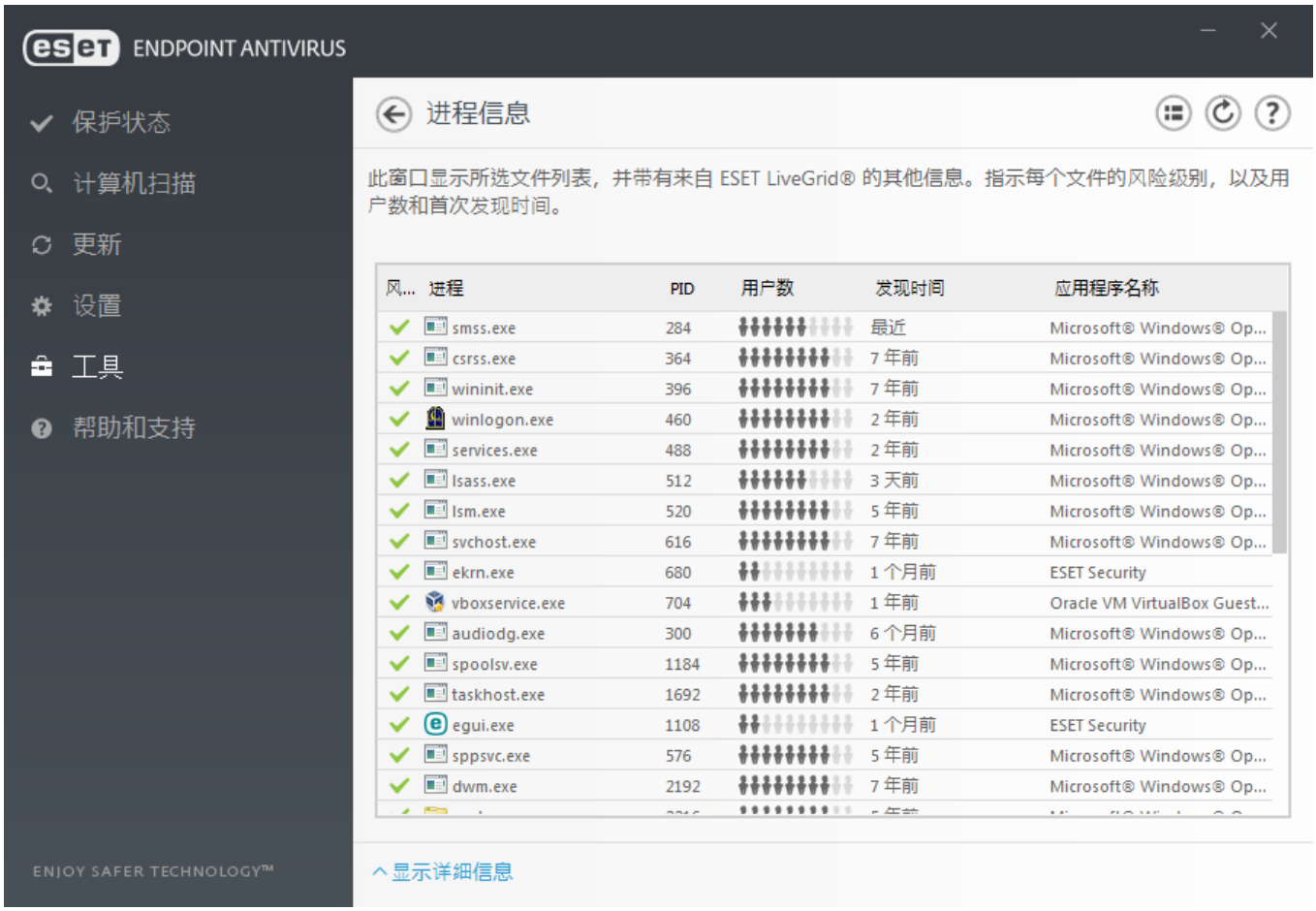
联系人电子邮件(可选) - 您的联系人电子邮件可以与任何可疑文件一起发送，而且可能用于在需要进一步信息以供分析时联系您。请注意，除非需要更多信息，否则 ESET 不会与您联系。

排除 - 排除过滤器允许您不提交某些文件 / 文件夹（例如，排除诸如文档或电子表格等可能包含机密信息的文件会很有用）。列出的文件即使包含可疑代码也不会发送给 ESET 实验室以供分析。默认情况下，最常见的文件类型均会排除（ doc 等）。如果需要，可以添加到排除文件列表。

如果您以前使用过 ESET LiveGrid® 但已禁用它，可能仍会发送数据包。即使已停用，此类数据包也会发送给 ESET。发送完当前所有信息后，将不会再创建任何数据包。

3.9.4.8 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，以通过启用 ESET LiveGrid® 技术来保护用户。



风险级别 - 在大多数情况下，ESET Endpoint Antivirus 和 ESET LiveGrid® 技术使用一系列启发式规则检查每个对象的特性，然后评估恶意活动的可能性，将风险级别指定给对象（文件、过程、注册表项等）。基于这些启发式扫描，会向对象指定风险级别，级别从 1 - 良好（绿色）到 9 - 危险（红色）。

进程 - 当前在计算机上运行的程序或进程的映像名称。要查看计算机上运行的所有进程，还可以使用 Windows 任务管理器。可以通过右键单击任务栏中的空白区域，然后单击任务管理器，或者通过按下键盘上的 **Ctrl**+**Shift**+**Esc** 来打开任务管理器。

PID - 是在 Windows 操作系统中运行的进程的 ID。

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 LiveGrid® 技术收集。

发现时间 - 自应用程序由 ESET LiveGrid® 技术发现以来的时段。

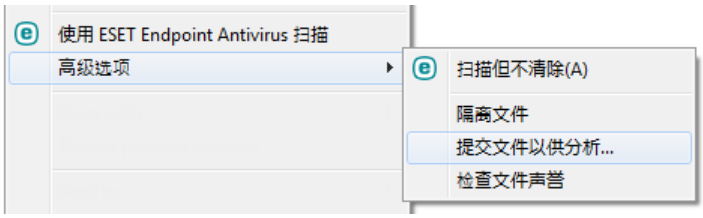
注意
当应用程序被标记为 未知（橙色） 安全级别时，它不一定就是恶意软件。通常它是一个较新的应用程序。如果您对文件不确定，使用提交文件以供分析功能将该文件发送到 ESET 病毒实验室。如果文件被证实是一个恶意应用程序，则以后的检测引擎更新中将增加对它的检测。

应用程序名称 - 程序或进程的给定名称。

通过单击底部的给定应用程序，将在窗口底部显示以下信息：

- **路径** - 计算机上应用程序的位置。
- **大小** - 以 kB（千字节）或 MB（兆字节）为单位的文件大小。
- **说明** - 基于操作系统说明的文件特性。
- **公司** - 供应商或应用程序进程的名称。
- **版本** - 来自应用程序发布者的信息。
- **产品** - 应用程序名称和 /或企业名称。
- **创建日期** - 创建应用程序的日期和时间。
- **修改日期** - 最后一次修改应用程序的日期和时间。

注意
还可以对不充当运行程序 /进程的文件检查信誉 - 标记要检查的文件，右键单击它们，从右键菜单中选择**高级选项** > **使用 ESET LiveGrid® 检查文件信誉**。



3.9.4.9 提交样本以供分析

使用样本提交对话框可将文件或站点发送到 ESET 以供分析，该对话框可在**工具** > **提交样本以供分析**中找到。如果您在计算机上发现了行为可疑的文件或在 Internet 上发现了可疑的站点，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或网站，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 提交样本前，确保其满足以下一个或多个标准：

- 未检测到文件或网站
- 将文件或网站错误地检测为威胁

除非需要更多信息以供分析，否则您不会收到回信。

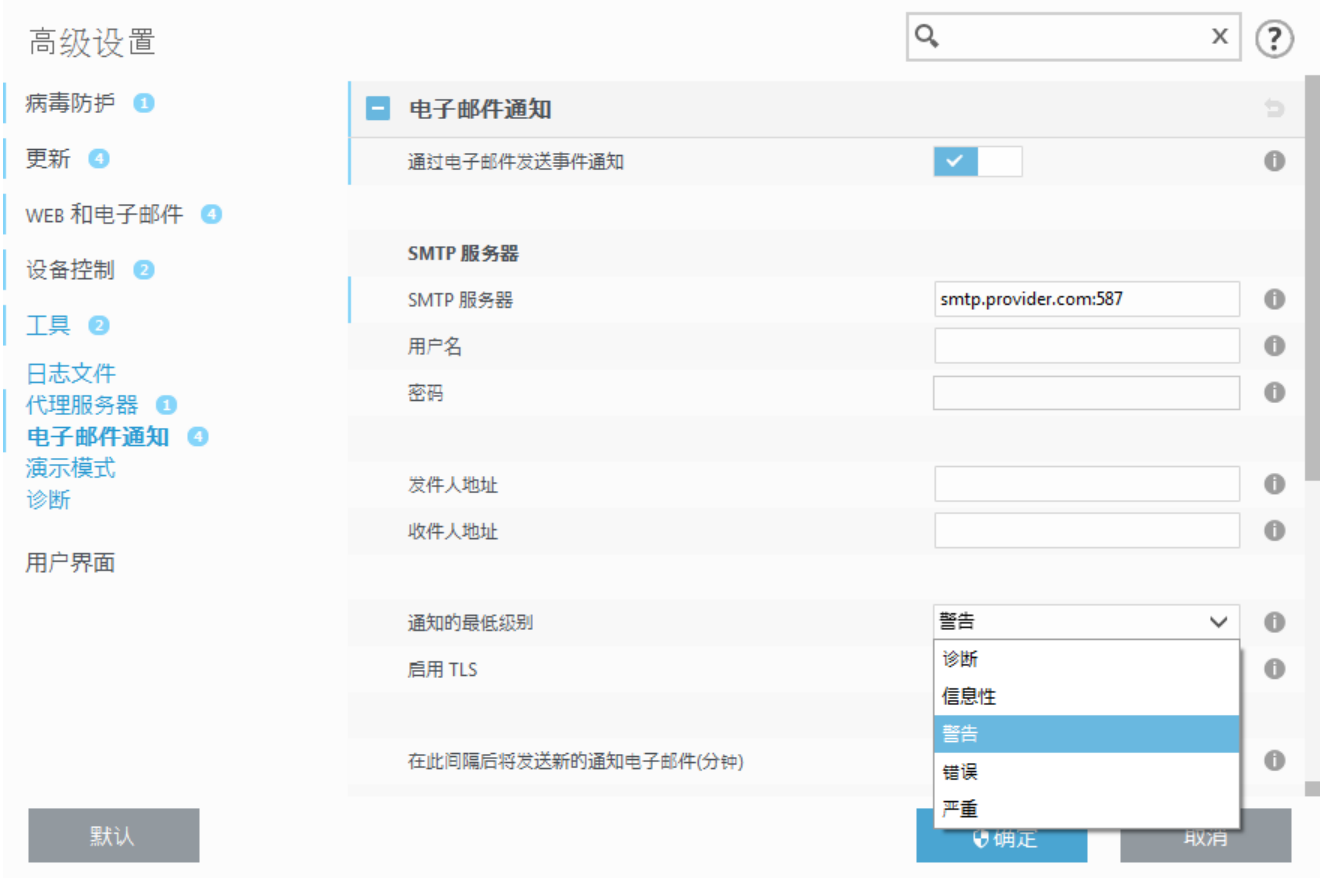
从**提交样本的理由**下拉菜单选择最适合您的邮件的描述：
- **可疑文件**
- **可疑站点**（被任何恶意软件感染的网站），
- **误报文件**（文件检测为感染，但并未感染），
- **误报站点**
- **其他**

文件 /站点 - 您想要提交的文件或网站的路径。

联系人电子邮件 - 此联系人电子邮件随可疑文件一起发送给 ESET，如果需要更多信息以供分析，可能会使用该电子邮件与您联系。可选择是否输入联系人电子邮件。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。

3.9.4.10 电子邮件通知

如果发生具有所选级别的事件，ESET Endpoint Antivirus 可以自动发送通知电子邮件。启用**通过电子邮件发送事件通知**以激活电子邮件通知。



SMTP 服务器

SMTP 服务器 - 用于发送通知的 SMTP 服务器（例如 *smtp.provider.com:587* ，预定义的端口为 25）。

注意
ESET Endpoint Antivirus 支持采用 TLS 加密的 SMTP 服务器。

用户名和**密码** - 如果 SMTP 服务器需要验证，则应在这些字段中填写有效的用户名和密码，以便访问 SMTP 服务器。

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

收件人地址 - 该字段用于指定收件人地址，收件人地址将显示在通知电子邮件的标题中。使用分号 ";" 分隔多个电子邮件地址。

从**通知的最低级别**下拉菜单中，可以选择要发送的通知的起始严重性级别。

- **诊断** - 记录微调程序所需的信息和以上所有记录。
- **信息性** - 记录信息性消息（如非标准的网络事件），其中包括成功更新消息及以上所有记录。
- **警告** - 记录严重错误和警告消息（未正确运行反隐藏技术或者更新失败）。
- **错误** - 将记录错误（未启动文档防护）和严重错误。
- **严重** - 仅记录严重错误（启动病毒防护或被感染的系统时出错）。

启用 TLS - 允许发送 TLS 加密支持的警报和通知消息。

在此间隔后将发送新的通知电子邮件(分钟) - 在此间隔（以分钟为单位）后将新的通知发送到电子邮件。若将该值设置为 0，则将立即发送这些通知。

在单独的电子邮件中发送每个通知 - 启用后，收件人将收到有关每个单独通知的新电子邮件。这可能导致在短时间内收到大量的电子邮件。

邮件格式

程序和远程用户或系统管理员之间的通信通过电子邮件或 LAN 消息（使用 Windows 消息服务）来进行。在大多数情况下，警报消息和通知的默认格式是最适用的。而在某些情况下，您可能需要更改事件消息的消息格式。

事件消息的格式 - 显示在远程计算机上的事件消息的格式。

威胁警告消息的格式 - 威胁警报和通知消息具有预定义的默认格式。 我们建议您不要更改该格式。 但是在某些情况下（例如，如果有自动电子邮件处理系统），可能需要更改邮件格式。

字符集 - 基于 Windows 区域设置（例如，windows-1250）、Unicode (UTF-8)、ACSII 7 位（例如，将 á 更改为 a 以及将未知符号更改为 ?）或 Japanese (ISO-2022-JP) 将电子邮件转换为 ANSI 字符编码。

使用可打印字符引用编码 - 电子邮件源将编码为使用 ASCII 字符的引用可打印 (QP) 格式，可通过 8 位格式电子邮件正确传输特殊国家字符 (áéíóú)。

在消息中，关键字（用 % 符号隔开的字符串）由指定的实际信息替换。以下关键字可用：

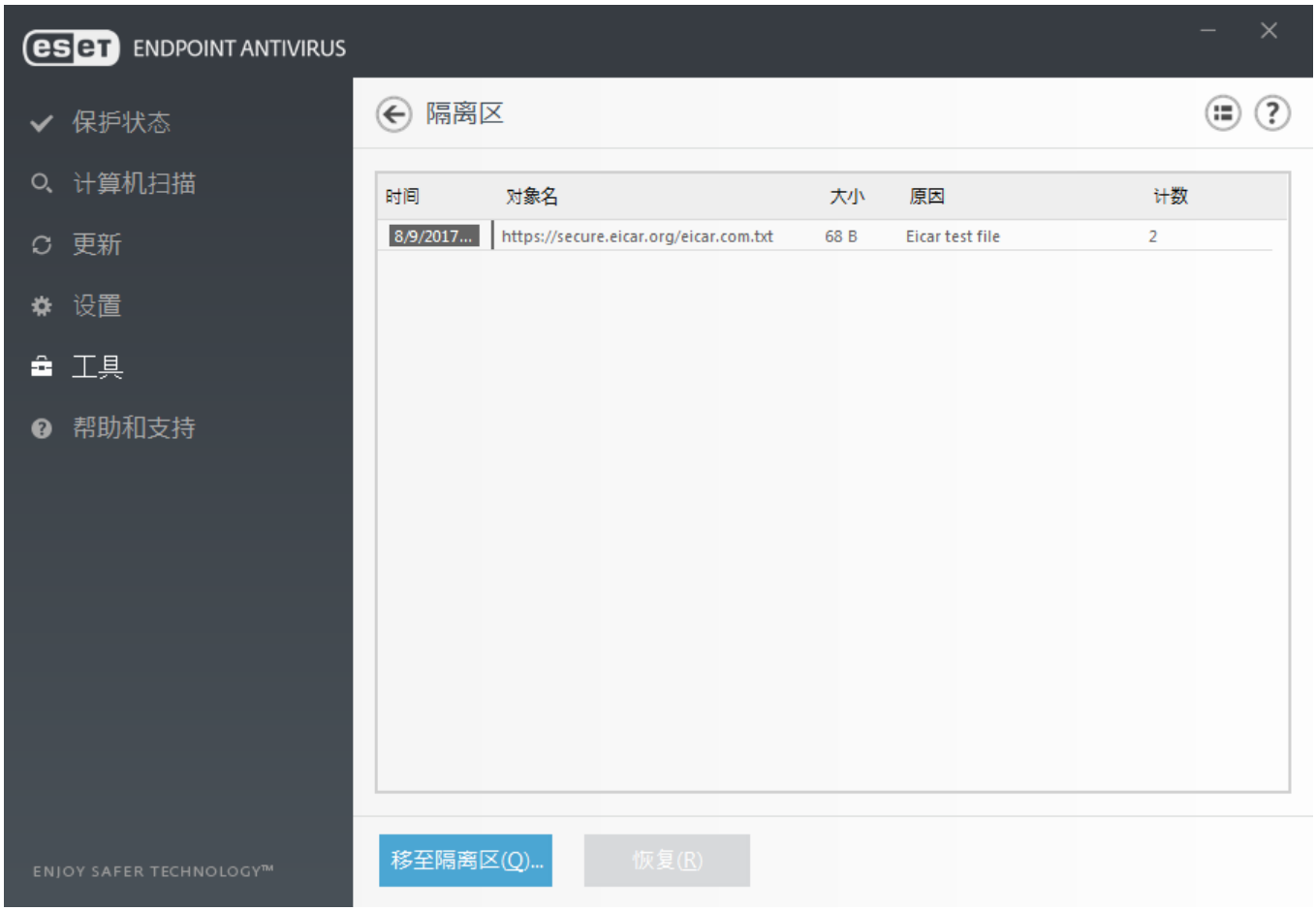
- **%ComputerName%** - 发生警报的计算机的名称。
- **%ProgramName%** - 生成警报的程序。
- **%TimeStamp%** - 事件的日期和时间。
- **%UserName%** - 发生警报的登录用户的名称。
- **%InfectedObject%** - 被感染文件、消息等的名称。
- **%VirusName%** - 感染标识。
- **%ErrorDescription%** - 非病毒事件的说明。
- **%Scanner%** - 相关模块。
- **%Action%** - 针对渗透采取的操作。

关键字 **%InfectedObject%** 和 **%VirusName%** 仅用于威胁警告消息，而 **%ErrorDescription%** 仅用于事件消息。

3.9.4.11 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 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禁用该选项）。如果需要，您可以通过单击**隔离**手动隔离任何可疑文件。原文件将从其初始位置删除。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。若要恢复隔离的文件，请在 隔离区 窗口中右键单击该文件，然后在右键菜单中选择**恢复**。如果文件被标记为潜在的不受欢迎应用程序，则**恢复并且不扫描**也将可用。右键菜单还包含**恢复至 ..**选项，使用此选项可将文件恢复到其被删除时所在位置之外的其他位置。

从隔离区中删除 - 右键单击给定项并选择**从隔离区中删除**，或选择想要删除的项，然后在键盘上按 **Delete** 键。还可以选择多个项，然后将它们一起删除。

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

如果程序未检测到您隔离的可疑文件，或文件被错误地检测为威胁并且随后被隔离，请将该文件发送到 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**。

3.9.4.12 Microsoft Windows 更新

Windows 更新功能是防止用户遭受恶意软件攻击的重要组件。出于此原因，即时安装 Microsoft Windows 更新很重要。ESET Endpoint Antivirus 会根据您指定的级别，通知您有关错过的更新。可用级别包括：

- **无更新** - 没有提供可供下载的系统更新。
- **可选更新** - 将提供标记为低优先级及更高优先级的更新以供下载。
- **建议的更新** - 将提供标记为常用及更高优先级的更新以供下载。
- **重要更新** - 将提供标记为重要及更高优先级的更新以供下载。
- **关键更新** - 仅提供关键更新以供下载。

单击**确定**可保存更改。在验证更新服务器的状态后将显示系统更新窗口。因此，在保存更改后系统更新信息可能无法立即使用。

3.9.4.13 ESET CMD

该功能支持高级 ecmd 命令。它允许您使用命令行 (ecmd.exe) 导出和导入设置。到目前为止，只可以使用 GUI 导出和导入设置。ESET Endpoint Antivirus 配置可以导出到 *xml* 文件。

启用 ESET CMD 后，有两种授权方法可用：

- **无** - 无授权。不建议您使用此方法，因为它允许导入任何未签名的配置，这可能存在风险。
- **高级设置密码** - 使用密码保护。从 *xml* 文件导入配置时，此文件必须已签名（请参阅以下 *xml* 配置文件）。此授权方法会在配置导入期间验证密码，以确保它与访问设置中指定的密码相匹配。如果未启用访问设置、密码不匹配或 *xml* 配置文件未签名，将不会导入配置。

ESET CMD 启用后，即可开始使用命令行导出 导入 ESET Endpoint Antivirus 配置。可以手动执行上述操作，也可以创建用于自动执行的脚本。

重要信息
若要使用高级 ecmd 命令，您需要具有管理员权限才可以运行这些命令，或者使用**以管理员身份运行**打开 Windows 命令提示符 (cmd)。否则，您会收到 **Error executing command.** 消息。此外，导出配置时，目标文件夹必须已存在。

注意
高级 ecmd 命令只可以在本地运行。使用 ERA 执行客户端任务**运行命令**将不起作用。

示例
导出设置命令：

```
ecmd /getcfg c:\config\settings.xml
```

导入设置命令：

```
ecmd /setcfg c:\config\settings.xml
```

对 *xml* 配置文件签名：

1. 从 ESET 工具和实用工具下载页面下载 **XmlSignTool**，然后解压缩该工具。为对 eset .*xml* 配置文件进行签名，特意开发了此工具。
2. 使用**以管理员身份运行**打开 Windows 命令提示符 (cmd)。
3. 导航到以下工具所在的位置：`XmlSignTool.exe`.
4. 执行对 *xml* 配置文件进行签名的命令，用法：`XmlSignTool <xml_file_path>`
5. XmlSignTool 要求输入两遍高级设置密码。您的 *xml* 配置文件现已完成签名，可以用于导入带有使用高级设置密码授权方法的 ESET CMD 的 ESET Endpoint Antivirus 的另一个实例。

警告
不建议在未授权的情况下启用 ESET CMD，因为这会允许导入任何未签名的配置。在**高级设置** > **用户界面** > **访问设置**中设置密码，以防止用户未经授权进行修改。

3.9.5 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。

使用用户界面元素工具，您可以调整程序的视觉外观和使用的效果。

为提供您的安全软件的最大安全性，您可以使用访问设置工具来阻止所有未经授权的更改。

通过配置警报和通知，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**用户界面元素** > **应用程序状态**中。您可以在此处检查这些通知的状态，或者可以阻止显示它们。

右键单击选中的对象后，就会显示右键菜单集成。使用此工具将 ESET Endpoint Antivirus 控件元素集成到右键菜单中。

演示模式对于用户来说非常有用，他们希望在不受弹出窗口、计划任务和任何会加重处理器和 RAM 负担组件的影响下使用应用程序。

3.9.5.1 用户界面元素

ESET Endpoint Antivirus 中的用户界面配置选项允许您调整工作环境以符合您的需要。可以从 ESET Endpoint Antivirus 高级设置树的**用户界面** > **用户界面元素**分支访问这些配置选项。

在**用户界面元素**部分中，可以调整工作环境。使用**启动模式**下拉菜单来从以下图形用户界面 (GUI) 启动模式中进行选择：

完整 - 将显示完整 GUI。

最小 - GUI 不可用，仅向用户显示通知。

手动 - 将不显示通知或警报。

静默 - 既不显示 GUI，也不显示通知和警报。此模式在需要保留系统资源的情况下非常有用。静默模式只能由管理员启动。

注意
选择最小 GUI 启动模式且重新启动计算机后，将显示通知，但不显示图形界面。若要还原到完整的图形用户界面模式，请以管理员身份在 开始 菜单中的**所有程序** > **ESET** > ESET Endpoint Antivirus 下运行 GUI，或者通过 ESET Remote Administrator 并使用某个策略来执行此操作。

如果希望停用 ESET Endpoint Antivirus 初始屏幕，则取消选择**启动时显示初始屏幕**。

若要使 ESET Endpoint Antivirus 在扫描期间发生重要事件时（例如，在发现威胁时或已完成扫描时）发出声音，请选中**使用声音信号**。

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

状态

应用程序状态 - 单击**编辑**按钮以管理（禁用）在主菜单的**防护状态**窗格中显示的状态。

许可证信息

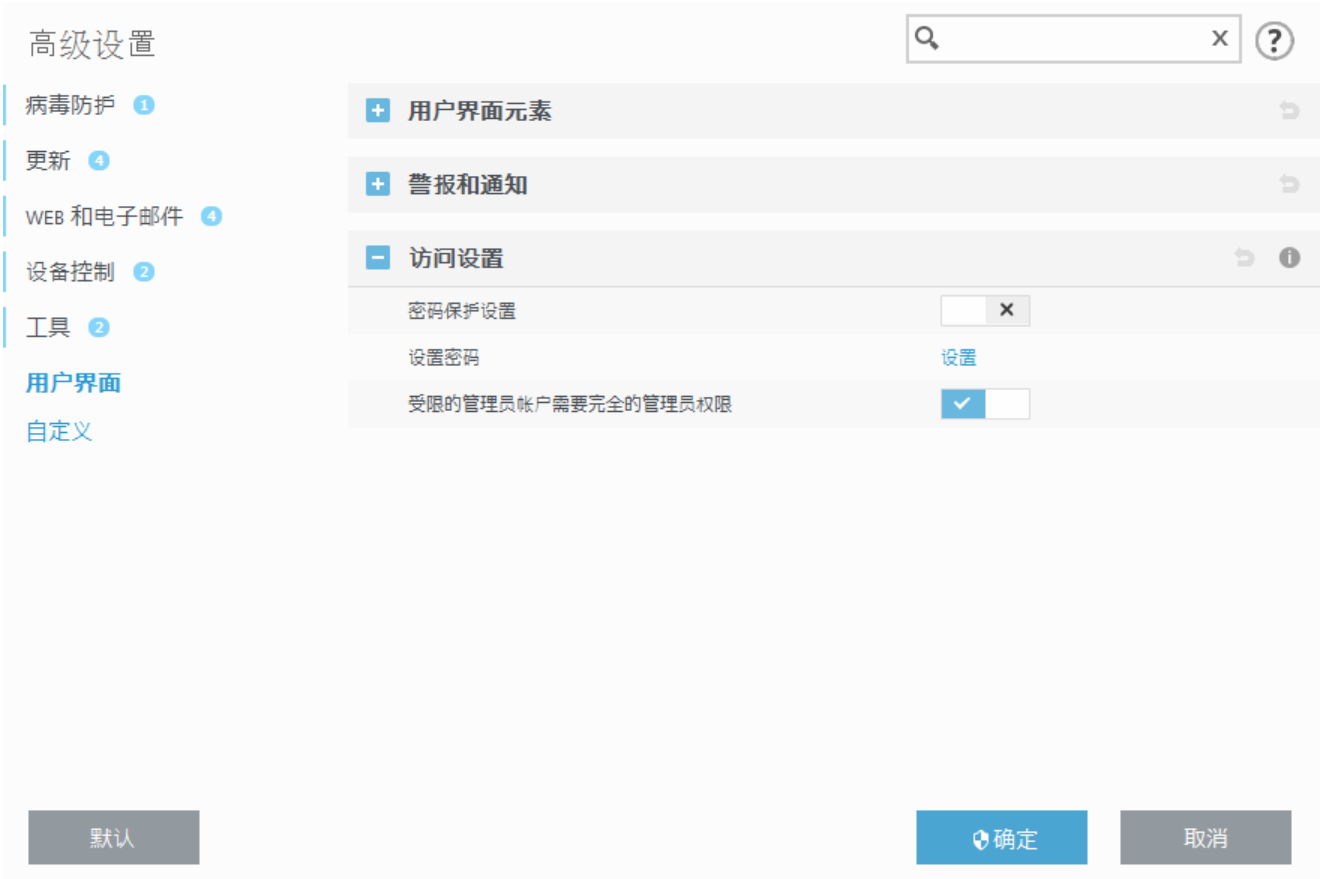
显示许可信息 - 禁用该选项后，将不会在**防护状态**和**帮助和支持**屏幕上显示许可信息。

显示许可证邮件和通知 - 禁用该选项后，仅当许可证到期后才会显示通知和消息。

注意
将应用许可证信息设置，但不适用于 MSP 许可证激活的 ESET Endpoint Antivirus。

3.9.5.2 访问设置

为最大限度地保障系统安全，必须正确配置 ESET Endpoint Antivirus。任何未经授权的更改都可能导致丢失重要数据。为避免进行未经授权的更改，可用密码保护 ESET Endpoint Antivirus 的设置参数。用于保护密码的配置设置位于**用户界面** > **访问设置**下的**高级设置** (F5) 中。



密码保护设置 - 指示密码设置。单击以打开 密码设置 窗口。

若要设置或更改密码以保护设置参数，请单击**设置**。

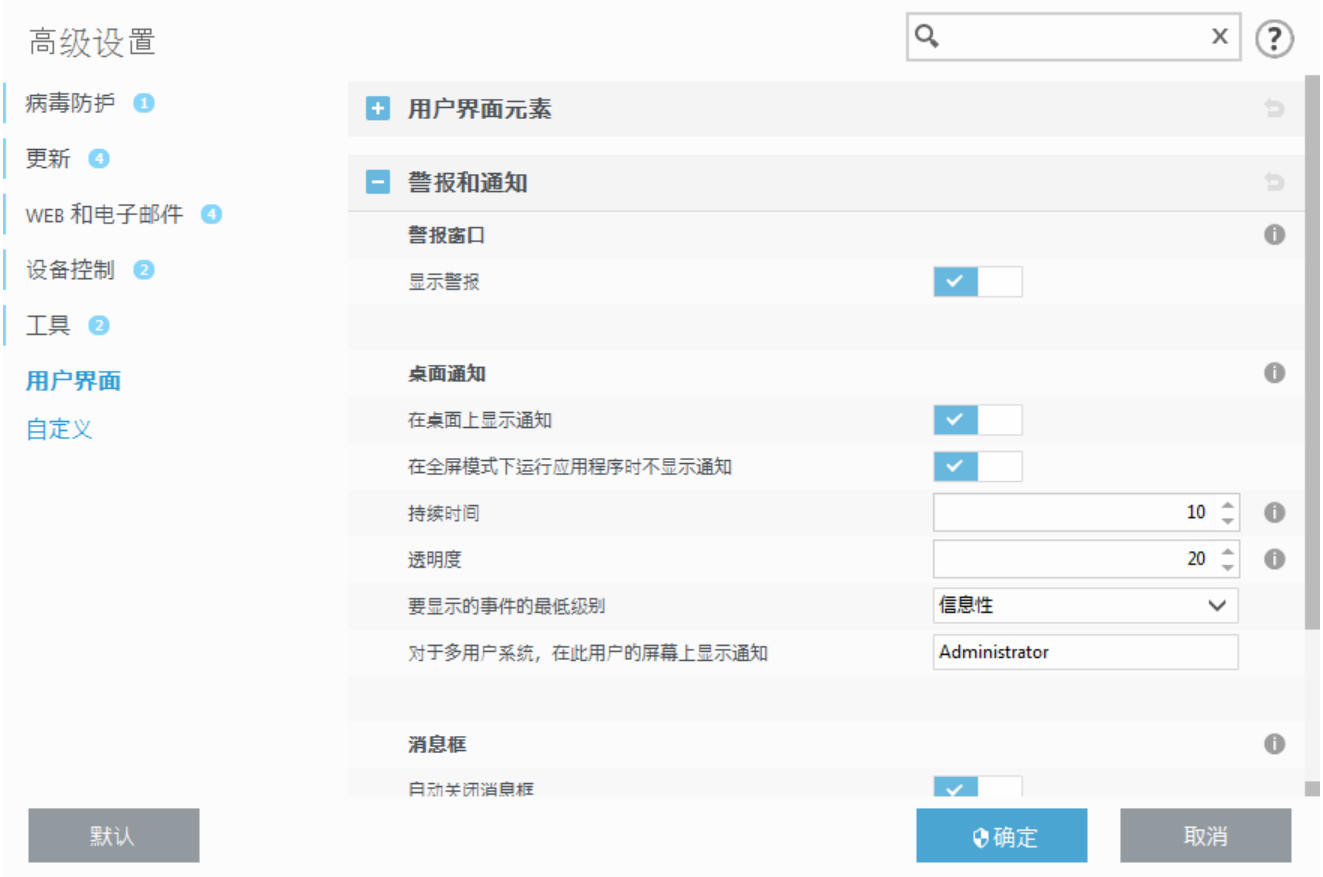
受限的管理员帐户需要完全的管理员权限 - 使此选项保持活动状态，可在修改某些系统参数（类似于 Windows Vista 中的 UAC）时提示当前用户（如果他或她没有管理员权限）输入管理员用户名和密码。 修改包括禁用保护模块。

仅适用于 Windows XP：

需要管理员权限(无 UAC 支持的系统) - 启用此选项后，ESET Endpoint Antivirus 将提示用户提供管理员凭据。

3.9.5.3 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（例如成功更新消息）。您还可以设置显示时间和系统托盘通知透明度（这仅适用于支持系统托盘通知的系统）。



警报窗口

禁用**显示警报**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）。

桌面通知

桌面通知和气球提示仅作为信息提示方式，并且不需要用户交互。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**。打开**在全屏模式下运行应用程序时不显示通知**开关以阻止所有非交互通知。可通过以下方式修改通知显示时间和窗口透明度等更多详细选项。

您可以通过**要显示事件的最低级别**下拉菜单选择要显示的警报和通知的严重性级别。有以下选项可供使用：

- **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允许您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。

消息框

若要在一段时间后自动关闭弹出窗口，请选择**自动关闭消息框**。如果未手动关闭，警报窗口会在超过指定时限后自动关闭。

确认消息 - 向您显示确认消息列表，您可以从中选择是否显示确认消息。

3.9.5.3.1 高级设置冲突错误

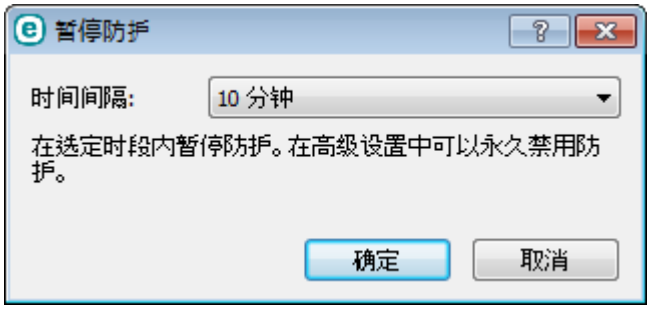
如果某个组件（如 HIPS）和用户同时在交互或学习模式下创建规则，可能会发生此错误。

重要信息
如果您想要创建自己的规则，我们建议将过滤模式更改为默认的**自动模式**。 阅读关于 HIPS 和过滤模式的更多信息。

3.9.5.4 系统托盘图标

可通过右键单击系统托盘图标 使用一些最重要的设置选项和功能。

暂停防护 - 显示禁用病毒和间谍软件防护的确认对话框，这些防护通过控制文件、Web 和电子邮件通信来保护系统免受攻击。



时间间隔下拉菜单表示将为其禁用病毒和间谍软件防护的时段。

高级设置 - 选择此项以进入**高级设置**树。您还可以通过按 F5 键或导航到**设置** > **高级设置**来访问高级设置。

日志文件 - 日志文件包含所有已发生的重要程序事件的信息，并提供检测到的威胁的概要信息。

隐藏 ESET Endpoint Antivirus - 从屏幕隐藏 ESET Endpoint Antivirus 窗口。

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

检查更新 ... –开始更新程序模块，以确保对恶意代码的防护级别。

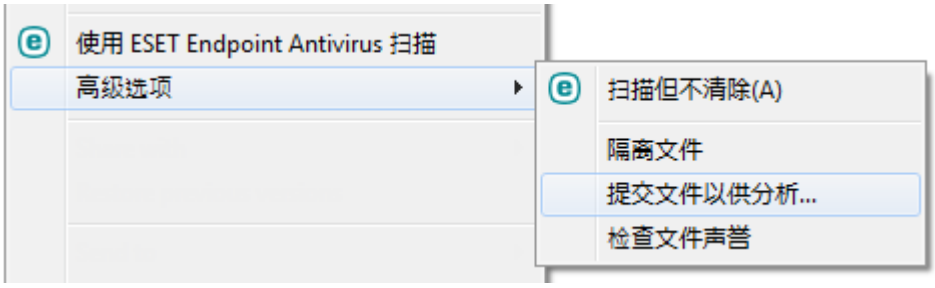
关于 - 提供系统信息、有关已安装的 ESET Endpoint Antivirus 版本和安装的程序模块的详细信息，以及您的许可证到期日期。有关您的操作系统和系统资源的信息可以在页面底部找到。

3.9.5.5 右键菜单

右键单击对象（文件）后，就会显示右键菜单。该菜单将列出您可以在对象上执行的所有操作。

可以将 ESET Endpoint Antivirus 控件元素集成到右键菜单中。此功能的设置选项在**用户界面** > **用户界面元素**下的高级设置树中提供。

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



3.10 高级用户

3.10.1 配置文件管理器

配置文件管理器用在 ESET Endpoint Antivirus 中的两个地方 -在**手动计算机扫描**部分和**更新**部分中。

手动计算机扫描

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

要创建新配置文件，请打开 高级设置 窗口 (F5) 并单击**病毒防护** > **手动计算机扫描**，然后单击**配置文件列表**旁边的**编辑**。列出现有扫描配置文件的**更新配置文件**下拉菜单。为了帮助您创建适合需求的扫描配置文件，请参阅 ThreatSense 引擎参数设置部分，查看扫描设置中每个参数的描述。

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**。在**配置文件管理器**窗口中输入新配置文件的名称并单击**添加**。从**更新配置文件**下拉菜单中选择新的配置文件并调整其余参数以满足要求，单击**确定**以保存新配置文件。

更新

更新设置部分中的配置文件编辑器允许用户创建新的更新配置文件。请只在计算机使用多种方式连接更新服务器时，创建和使用您自己的自定义配置文件（不是默认的**我的配置文件**）。

例如，一台笔记本电脑通常连接的是本地网络中的本地服务器（镜像），但在断开与本地网络的连接时（比如出于商务旅行的需要）可能会使用两种配置文件直接从 ESET 的更新服务器下载更新：第一个连接到本地服务器，另一个连接到 ESET 的服务器。配置完这些配置文件后，浏览到**工具** > **计划任务**，编辑更新任务参数。将其中一个配置文件指定为主配置文件，另一个为次配置文件。

更新配置文件 - 当前使用的更新配置文件。要更改它，请从下拉菜单中选择一个配置文件。

配置文件列表 - 新建或删除现有更新配置文件。

3.10.2 诊断

诊断提供 ESET 进程（比如 *ekrn*）的应用程序崩溃转储。如果应用程序崩溃，将生成一个转储。这能够帮助开发人员调试和修复各种 ESET Endpoint Antivirus 问题。单击**转储类型**旁的下拉菜单并选择以下三个可用选项之一：

- 选择**禁用**（默认）以禁用此功能。
- **小型** - 记录可能有助于识别应用程序意外崩溃原因的最小有用信息集。 此类转储文件在空间有限时有用，但是，因为所包含的信息有限，分析此文件可能无法找到不是由出现问题时正在运行的线程直接导致的错误。
- **完整** - 当应用程序意外停止时记录系统内存的所有内容。 完整的内存转储可能包含在收集内存转储时正在运行进程的数据。

启用协议过滤高级日志记录 - 采用 PCAP 格式记录所有通过协议过滤引擎传递的数据，从而帮助开发人员诊断并修复与协议过滤有关的问题。

启用更新引擎高级日志记录 - 记录更新过程中发生的所有事件。这可以帮助开发人员诊断并修复与更新引擎有关的问题。

启用许可高级日志记录 - 记录所有产品与许可证服务器的通信。

启用反垃圾邮件引擎高级日志记录 - 记录反垃圾邮件扫描期间发生的所有事件。 这可以帮助开发人员诊断和修复与 ESET 反垃圾邮件引擎有关的问题。

启用操作系统高级日志记录 - 将收集有关操作系统的其他信息，比如正在运行的进程、CPU 活动和磁盘操作。这可以帮助开发人员诊断并修复与操作系统上运行的 ESET 产品有关的问题。

可在下面的位置找到日志文件：
C:\ProgramData\ESET\ESET Security\Diagnostics（Windows Vista 和更高版本中）或 *C:\Documents and Settings\All Users\...*（较早版本的 Windows 中）。

目标目录 - 在崩溃期间将生成转储的目录。

打开诊断文件夹 - 单击**打开**以在新的 *Windows 资源管理器* 窗口中打开此目录。

创建诊断转储 - 单击**创建**以在**目标目录**中创建诊断转储文件。

3.10.3 导入和导出设置

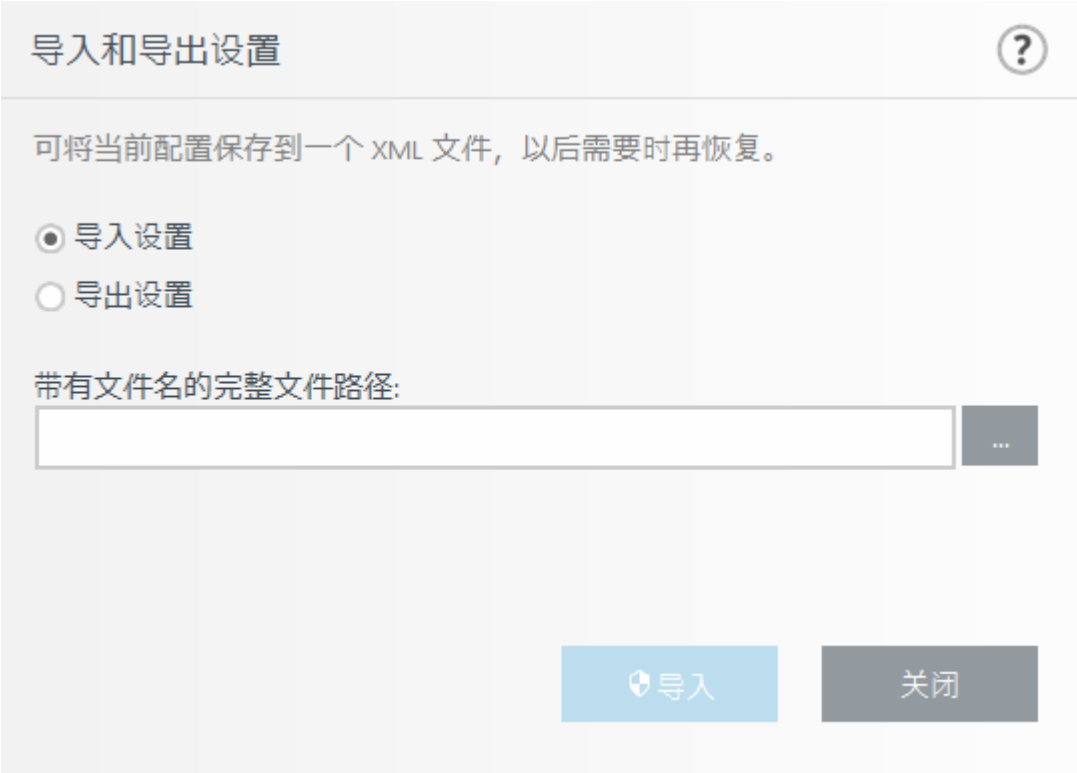
您可以从**设置**菜单导入或导出自定义的 ESET Endpoint Antivirus .xml 配置文件。

当需要备份 ESET Endpoint Antivirus 的当前配置以备日后使用时，配置文件的导入和导出功能十分有用。对于想要在多个系统上使用其首选配置的用户，导出设置选项也很便利，因为他们可以方便地导入 *.xml* 文件来传输这些设置。

导入配置非常简单。在主程序窗口中，依次单击**设置** > **导入 /导出设置**，然后选择**导入设置**。输入配置文件的文件名，或单击**...**按钮来找到想要导入的配置文件。

导出配置的步骤非常相似。在主程序窗口中，依次单击**设置** > **导入 /导出设置**。选择**导出设置**并输入配置文件的文件名（即 *export.xml* ）。使用浏览器在计算机上选择要保存配置文件的位置。

注意
如果您没有足够的权限将导出的文件写入到指定的目录，则在导出设置时可能遇到错误。



3.10.4 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 "ecls "命令）或使用批处理（ "bat "）文件启动。ESET 命令行扫描程序用法：

```
ecls [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

/base-dir=FOLDER	从 "文件夹 "加载模块
/quar-dir=FOLDER	隔离 "文件夹 "
/exclude=MASK	不扫描与 "掩码 "匹配的文件
/subdir	扫描子文件夹（默认）
/no-subdir	不扫描子文件夹
/max-subdir-level=LEVEL	要扫描的文件夹中的最大子文件夹层数
/symlink	跟踪符号链接（默认）
/no-symlink	跳过符号链接
/ads	扫描 ADS（默认）
/no-ads	不扫描 ADS
/log-file=FILE	将结果记录到 "文件 "

/log-rewrite	覆盖输出文件（默认 -附加）
/log-console	将结果记录到控制台（默认）
/no-log-console	不将结果记录到控制台
/log-all	同时记录清除文件
/no-log-all	不记录干净的文件（默认）
/aind	显示活动指示器
/auto	扫描并自动清除所有本地磁盘中的病毒

扫描程序选项

/files	扫描文件（默认）
/no-files	不扫描文件
/memory	扫描内存
/boots	扫描引导区
/no-boots	不扫描引导区（默认）
/arch	扫描压缩文件（默认）
/no-arch	不扫描压缩文件
/max-obj-size=SIZE	仅扫描小于指定 'k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 'k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 'k大小 '兆字节（默认值 0 = 无限制），则只扫描这些文件
/mail	扫描电子邮件文件（默认）
/no-mail	不扫描电子邮件文件
/mailbox	扫描邮箱（默认）
/no-mailbox	不扫描邮箱
/sfx	扫描自解压文件（默认）
/no-sfx	不扫描自解压文件
/rtp	扫描加壳程序（默认）
/no-rtp	不扫描加壳程序
/unsafe	扫描潜在的不安全应用程序
/no-unsafe	不扫描可能不安全的应用程序（默认）
/unwanted	扫描潜在的不受欢迎应用程序
/no-unwanted	不扫描潜在不受欢迎的应用程序（默认）
/suspicious	扫描可疑应用程序（默认）
/no-suspicious	不扫描可疑应用程序
/pattern	使用病毒库（默认）
/no-pattern	不使用病毒库
/heur	启用启发式扫描（默认）
/no-heur	禁用启发式扫描
/adv-heur	启用高级启发式扫描（默认）
/no-adv-heur	禁用高级启发式扫描
/ext=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 '
	有以下选项可供使用： • none - 不会自动进行清除。 • standard（默认） -ecls.exe 将尝试自动清除或删除被感染的文件。 • strict - ecls.exe 将尝试自动清除或删除被感染的文件，而无需用户干预（在删除文件之前，您会收到提示）。 • rigorous - ecls.exe 将在不尝试清除的情况下删除文件，无论文件是什么。 • delete - ecls.exe 将在不尝试清除的情况下删除文件，但将避免删除敏感文件，如 Windows 系统文件。
/quarantine	将被感染的文件（若已清除）复制到隔离区 （补充清理时执行的操作）

/no-quarantine	不将被感染的文件复制到隔离区

常规选项

/help	显示帮助并退出
/version	显示版本信息并退出
/preserve-time	保存上一个访问时戳

退出代码

0	未发现威胁
1	发现威胁并已清除
10	某些文件无法扫描（可能是威胁）
50	发现威胁
100	错误

注意
退出代码大于 100 表示未扫描文件，该文件可能被感染。

3.10.5 空闲状态检测

可以在**高级设置**（在**病毒防护** > **空闲状态扫描** > **空闲状态检测**下）中配置空闲状态检测设置。这些设置为空闲状态下扫描指定了触发器，即出现以下情况时触发扫描：

- 屏幕保护程序正在运行；
- 计算机已锁定；
- 用户注销。

使用每种状态的开关以启用或禁用不同的空闲状态检测触发器。

3.10.6 ESET SysInspector

3.10.6.1 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感染引起的可疑系统行为。

您可以使用两种方法访问 ESET SysInspector：一种是从 ESET Security 解决方案中的集成版访问，另一种是从 ESET 网站免费下载单机版访问。这两个版本的功能一致，且具有相同的程序控件。唯一的区别是管理输出的方式不同。单机版和集成版均允许您将系统快照输出为 *.xml* 文件，并将它们保存到磁盘。但是，集成版还允许您直接将系统快照存储在**工具** > **ESET SysInspector** 中（ESET Remote Administrator 除外）。 有关详细信息，请参见 ESET Endpoint Antivirus 的 ESET SysInspector 部分一节。

ESET SysInspector 扫描您的计算机时，请等待一些时间。它可能要花 10 秒到几分钟的时间，具体取决于您的硬件配置、操作系统和计算机上安装的应用程序的数量。

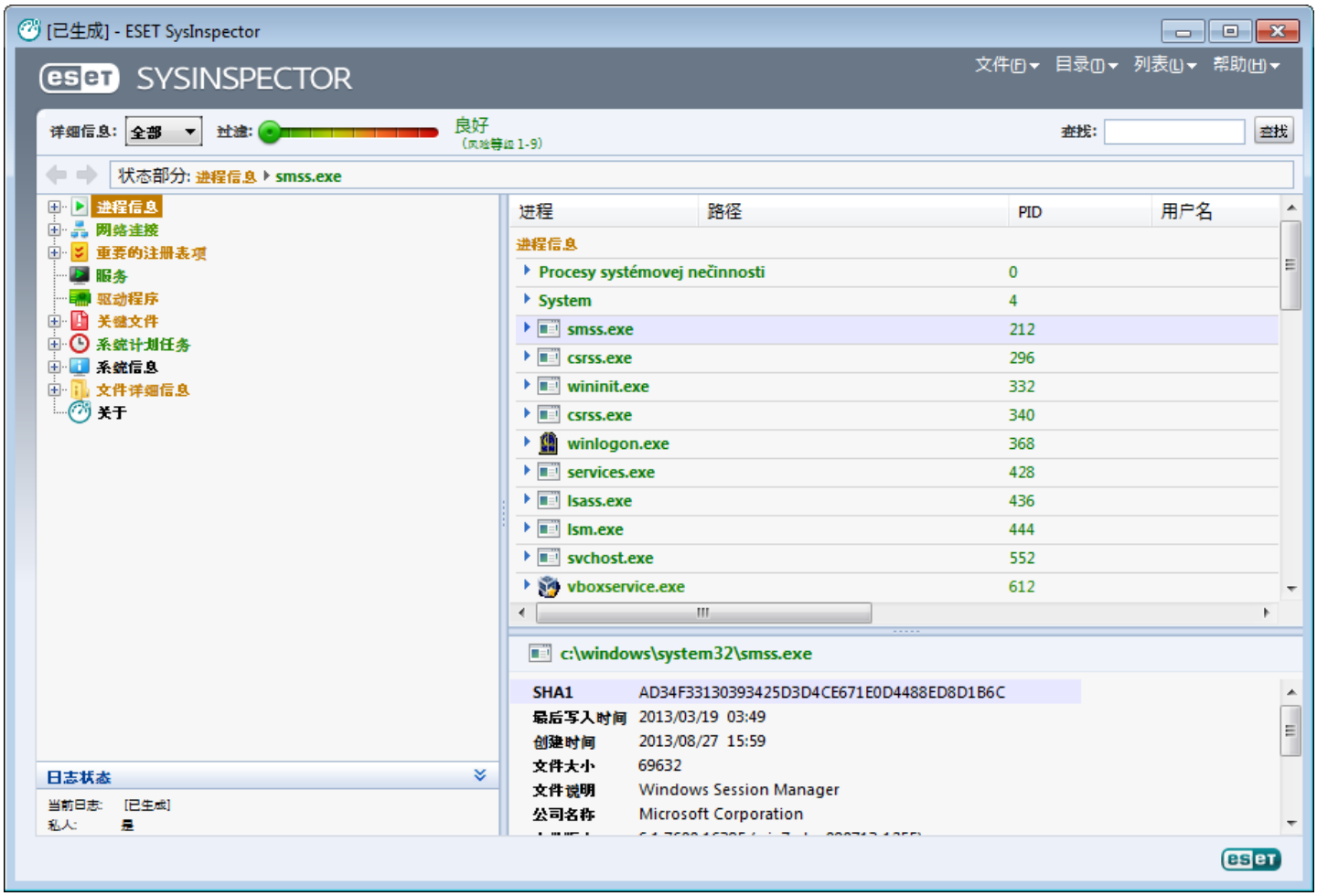
3.10.6.1.1 启动 ESET SysInspector

若要启动 ESET SysInspector，只需运行从 ESET 网站下载的 *SysInspector.exe* 可执行文件。 如果已经安装了一个 ESET Security 解决方案，可以直接从 开始 菜单（依次单击**程序** > **ESET** > **ESET Endpoint Antivirus**）运行 ESET SysInspector。

应用程序检查您的系统时，可能需要几分钟，请稍等。

3.10.6.2 用户界面和应用程序的使用

为了方便使用，主程序窗口被划分为四个主要部分 -主程序窗口顶端的程序控件，左侧的导航窗口，右侧的说明窗口以及位于主程序窗口底部的详细信息窗口。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）。



3.10.6.2.1 程序控件

本部分将涵盖 ESET SysInspector 中所有可用程序控件的说明。

文件

单击 **"文件"** 即可存储当前的系统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
可以将先前存储的 ESET SysInspector 报告拖放至主程序窗口以将其打开。出于安全原因，此功能在 Windows Vista 操作系统中不可用。

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。

列表

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

此设置影响主程序窗口中显示的信息，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问题解决方法所需的信息。在 中等 模式下，该程序将显示较少使用的详细信息。在 全部 模式下，ESET SysInspector 将显示解决具体问题所需的所有信息。

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。如果将滑块完全设定到左侧（风险级别 1），则会显示所有项目。如果将滑块移至右侧，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。如果将滑块完全移至右侧，该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。

比较

比较两个日志时，您可以选择显示所有项目、仅显示已添加的项目、仅显示已删除的项目或仅显示已替换的项目。

查找

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。您可以使用退格键和空格键，来代替单击后退和前进。

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不需要的。

3.10.6.2.2 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，您可以通过将各个节点扩展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该节点名称旁边的 或 。当在 导航 窗口中浏览节点和子节点的树结构时，您可能会在 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

该节点包含生成报告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和文件的风险级别。

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，它们会持续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。这些标记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"窗口中选定的协议（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

包含在特定时间/间隔由 Windows 任务计划触发的任务列表。

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

有关 ESET SysInspector 版本和程序模块列表的信息。

3.10.6.2.2.1 键盘快捷键

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	生成标准的计算机状态快照
Ctrl+H	生成还会记录敏感信息的计算机状态快照

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

3.10.6.2.3 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，这是比较合适的，它是检测恶意代码的有用工具。

在启动之后，应用程序会创建新日志并显示在新窗口中。依次单击**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，请依次单击**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您可以查看当前活动的日志和文件中保存的日志。若要比较日志，请依次单击**文件** > **比较日志**，并选择**选择文件**。将在主程序窗口中比较活动的日志与选定日志。该比较日志将仅显示这两个日志之间的差别。

注意
如果比较两个日志文件，请依次单击**文件** > **保存日志**，将其另存为 ZIP 文件；将保存这两个文件。如果稍后打开此文件，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。

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 并允许其生成新日志。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，请单击**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：

SysIsnpector.exe current.xml previous.xml

3.10.6.3 命令行参数

ESET SysInspector 支持从使用这些参数的命令行生成报告：

/gen	直接从命令行生成日志，而无需运行 GUI
/privacy	生成日志，忽略敏感信息
/zip	以压缩的 zip 文件保存输出日志
/silent	从命令行生成日志时不显示进度窗口
/blank	启动 ESET SysInspector，而无需生成 加载日志

示例

用法：
```
Sysinspector.exe [load.xml] [/gen=save.xml] [/privacy] [/zip] [compareto.xml]
```

若要将特定日志直接加载到浏览器中，请使用：*SysInspector.exe .\clientlog.xml*
若要从命令行生成日志，请使用：*SysInspector.exe /gen=.\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=.\mynewlog.zip /privacy /zip*
若要比较两个日志文件并浏览不同之处，请使用：*SysInspector.exe new.xml old.xml*

注意
如果文件 文件夹的名称包含间隔，则应采用引号。

3.10.6.4 服务脚本

服务脚本是向使用 ESET SysInspector 的客户提供帮助的一款工具，该工具可使用户轻松删除系统中不需要的对象。

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，您可以标记要删除的不需要的对象。然后运行修改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。不合格的修改可能会导致操作系统损坏。

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，请按下面的分步说明执行操作：

1. 运行 ESET SysInspector 来生成一个新的系统快照。
2. 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。
3. 右键单击选定对象，选择**导出选定部分到服务脚本**。
4. 选定的对象将会被导出到新日志中。
5. 这是整个过程中最关键的步骤：打开新的日志，并将您想要删除的所有对象的 -属性更改为 +。请确保您未标记任何重要的操作系统文件 对象。
6. 打开 ESET SysInspector，单击 **"文件 "> "运行服务脚本 "**，然后输入脚本路径。
7. 单击 **"确定 "**运行脚本。

3.10.6.4.1 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（左侧窗格）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**或**导出选定部分到服务脚本**。

注意
比较两个日志时不能导出服务脚本。

3.10.6.4.2 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，并阻止执行时的任何不一致情况。不得修改这部分脚本。

文件的其余部分分为各个部分，可以编辑其中的项目（注意这些将由脚本处理）。将项目前的 "-"字符替换为 "+"字符，标记要处理的项目。脚本中的各部分通过空行彼此分隔。每个部分具有编号和标题。

01) Running processes（运行进程）

此部分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）

此部分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\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

在此示例中，模块 khbekhb.dll 以 "+"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）

此部分包含现有 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）

此部分包含现有 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 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）

此部分包含当前 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）

此部分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）

此部分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）

此部分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，选择的驱动程序将停止。请注意，某些驱动程序不允许自行停止。

09) Critical files（关键文件）

此部分包含有关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
[...]
```

选择的项将被删除或重置为初始值。

3.10.6.4.3 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。

对话框窗口将确认该脚本已成功执行。

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窗口：**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。

如果该脚本未识别，将显示具有以下消息的对话框窗口：**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？**这可能因脚本不一致引起（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。

3.10.6.5 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。要保存某个日志文件，请从主程序窗口中单击**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 "SysInpsector-%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程序窗口中单击**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。

某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，然后将风险级别指定给对象（文件、过程、注册表项等）。根据这些启发式规则，对象被指定的风险级别范围从 "1 - 良好（绿色）" 至 "9 - 危险（红色）"。在左侧导航窗格中，根据其中对象的最高风险级别对各部分进行着色。

危险级别 '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，以使他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由 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。

什么是防隐匿技术？

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。如果没有专用的反 Rootkit 工具，则几乎不可能检测到 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 首先检查文件中是否嵌入了数字签名。如果找到了数字签名，则使用该信息验证文件。如果未找到数字签名，则 ESI 会开始查找对应的 CAT 文件（安全目录 *-%systemroot%\system32\catroot* ），该文件包含有关已处理的可执行文件的信息。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。

这是有时文件标记为 "Signed by MS "，但却具有不同 "CompanyName 条目的原因。

3.10.6.6 ESET Endpoint Antivirus 的 ESET SysInspector 部分

若要在 ESET Endpoint Antivirus 中打开 ESET SysInspector 一节，请单击 **"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。

若要比较、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，请从右键菜单中选择**显示**。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 ...**。

以下是对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。若要了解（当前生成的快照的）快照创建进度，请查看 **"状态 "**列。所有完成的快照都标记为 **"已创建 "**状态。
- **删除 全部删除** - 从该列表中删除条目。
- **导出 ...**- 将选定的条目保存在 XML 文件中（也可保存至压缩文件）。

3.10.7 远程监控和管理

Remote Monitoring and Management (RMM) is the process of supervising and controlling software systems using a locally installed agent that can be accessed by a management service provider. The default ESET Endpoint Antivirus installation contains the file *ermm.exe* located in the Endpoint application within the directory *c:\Program Files\ESET\ESET Security* . *ermm.exe* is a command line utility designed to facilitate the management of endpoint products and communications with any RMM Plugin. *ermm.exe* exchanges data with the RMM Plugin, which communicates with the RMM Agent linked to an RMM Server. By default, the ESET RMM tool is disabled. For more information, see 如何激活远程监控和管理.

The default ESET Endpoint Antivirus installation contains file ermm.exe located in the Endpoint application directory (default path *c:\Program Files\ESET\ESET Security*). ermm.exe exchanges data with the RMM Plugin, which communicates with the RMM Agent that is linked to an RMM Server.

- ermm.exe – command line utility developed by ESET that allows managing of Endpoint products and communication with any RMM Plugin.

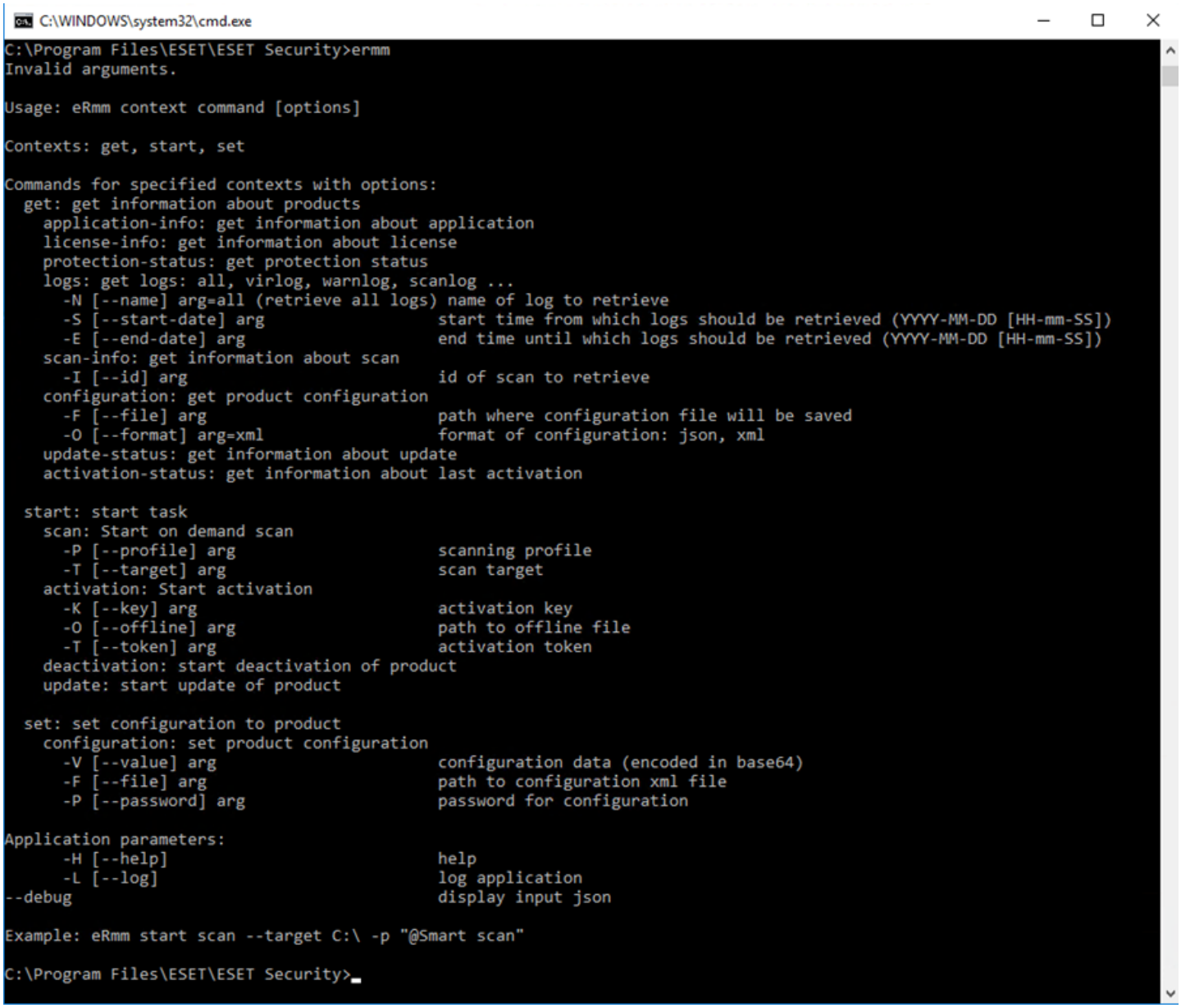
3.10.7.1 RMM 命令行

Remote monitoring management is run using the command line interface. The default ESET Endpoint Antivirus installation contains the file *ermm.exe* located in the Endpoint application within the directory *c:\Program Files\ESET\ESET Security* .

Run the Command Prompt (cmd.exe) as an Administrator and navigate to the mentioned path. (To open Command Prompt, press Windows button + R on your keyboard, type a *cmd.exe* into the Run window and press Enter.)

The command syntax is: `ermm context command [options]`

Also note that the log parameters are case sensitive.



ermm.exe uses three basic contexts: Get, Start and Set. In the table below you can find examples of commands syntax. Click the link in the Command column to see the further options, parameters, and usage examples. After successful execution of command, the output part (result) will be displayed. To see an input part, add parameter `--debug` at the of the command.

Context	Command	Description
get		**Get information about products**

Context	Command	Description
	应用程序信息	Get information about product
	许可证信息	Get information about license
	防护状态	Get protection status
	日志	Get logs
	扫描信息	Get information about running scan
	配置	Get product configuration
	更新状态	Get information about update
	激活状态	Get information about last activation
start		**Start task**
	扫描	Start on demand scan
	激活	Start activation of product
	停用	Start deactivation of product
	更新	Start update of product
set		**Set options for product**
	配置	Set configuration to product

In the output result of every command, the first information displayed is result ID. To understand better the result information, check the table of IDs below.

Error ID	Error	Description
0	Success	
1	Command node not present	"Command" node not present in input json
2	Command not supported	Particular command is not supported
3	General error executing the command	Error during execution of command
4	Task already running	Requested task is already running and has not been started
5	Invalid parameter for command	Bad user input
6	Command not executed because it's disabled	RMM isn't enabled in advanced settings or isn't started as an administrator

3.10.7.2 JSON 命令列表

3.10.7.2.1 获取防护状态

Get the list of application statuses and the global application status

Command line

```
ermm.exe get protection-status
```

Parameters

None

Example

call

```
{
 "command":"get_protection_status",
 "id":1,
 "version":"1"
}
```

result

```
{
 "id":1,
 "result":{
  "statuses":[{
    "id":"EkrnNotActivated",
    "status":2,
    "priority":768,
    "description":"Product not activated"
   }],
```

```
  "status":2,
  "description":"Security alert"
 },
 "error":null
}
```

3.10.7.2.2 获取应用程序信息

Get information about the installed application

Command line

```
ermm.exe get application-info
```

Parameters

None

Example

call

```
{
 "command":"get_application_info",
 "id":1,
 "version":"1"
}
```

result

```
{
  "id":1,
  "result":{
   "description":"ESET Endpoint Antivirus",
   "version":"6.6.2018.0",
   "product":"eea",
   "lang_id":1033,
   "modules":[{
    "id":"SCANNER32",
    "description":"Detection engine",
    "version":"15117",
    "date":"2017-03-20"
   },{
    "id":"PEGASUS32",
    "description":"Rapid Response module",
    "version":"9734",
```

```
 "date":"2017-03-20"
},{
 "id":"LOADER32",
 "description":"Update module",
 "version":"1009",
 "date":"2016-12-05"
},{
 "id":"PERSEUS32",
 "description":"Antivirus and antispyware scanner module",
 "version":"1513",
 "date":"2017-03-06"
},{
 "id":"ADVHEUR32",
 "description":"Advanced heuristics module",
 "version":"1176",
 "date":"2017-01-16"
},{
 "id":"ARCHIVER32",
 "description":"Archive support module",
 "version":"1261",
 "date":"2017-02-22"
},{
 "id":"CLEANER32",
 "description":"Cleaner module",
 "version":"1132",
 "date":"2017-03-15"
},{
 "id":"ANTISTEALTH32",
 "description":"Anti-Stealth support module",
 "version":"1106",
 "date":"2016-10-17"
},{
 "id":"SYSTEMSTATUS32",
 "description":"ESET SysInspector module",
 "version":"1266",
 "date":"2016-12-22"
},{
 "id":"TRANSLATOR32",
 "description":"Translation support module",
 "version":"1588B",
 "date":"2017-03-01"
},{
```

```
    "id":"HIPS32",
    "description":"HIPS support module",
    "version":"1267",
    "date":"2017-02-16"
   },{
    "id":"PROTOSCAN32",
    "description":"Internet protection module",
    "version":"1300",
    "date":"2017-03-03"
   },{
    "id":"DBLITE32",
    "description":"Database module",
    "version":"1088",
    "date":"2017-01-05"
   },{
    "id":"CONFENG32",
    "description":"Configuration module (33)",
    "version":"1496B",
    "date":"2017-03-17"
   },{
    "id":"IRIS32",
    "description":"LiveGrid communication module",
    "version":"1022",
    "date":"2016-04-01"
   },{
    "id":"SAURON32",
    "description":"Rootkit detection and cleaning module",
    "version":"1006",
    "date":"2016-07-15"
   },{
    "id":"SSL32",
    "description":"Cryptographic protocol support module",
    "version":"1009",
    "date":"2016-12-02"
   }
  },
  "error":null
 }
}
```

3.10.7.2.3 获取许可证信息

Get information about the license of the product

Command line

```
ermm.exe get license-info
```

Parameters

None

Example

call

```
{
 "command":"get_license_info",
 "id":1,
 "version":"1"
}
```

result

```
{
 "id":1,
 "result":{
  "type":"NFR",
  "expiration_date":"2020-12-31",
  "expiration_state":"ok",
  "public_id":"3XX-7ED-7XF",
  "seat_id":"6f726793-ae95-4e04-8ac3-e6a20bc620bf",
  "seat_name":"M"
 },
 "error":null
}
```

3.10.7.2.4 获取日志

Get logs of the product

Command line

```
ermm.exe get logs --name warnlog --start-date "2017-04-04 06-00-00" --end-date "2017-04-04 12-00-00"
```

Parameters

Name	Value

name	{ all, virlog, warnlog, scanlog, blocked, hipslog, urllog, devctrllog } : log to retrieve
start-date	start date from which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])
end-date	end time until which logs should be retrieved (YYYY-MM-DD [HH-mm-SS])

Example

call


```
{
 "command":"get_logs",
 "id":1,
 "version":"1",
 "params":{
  "name":"warnlog",
  "start_date":"2017-04-04 06-00-00",
  "end_date":"2017-04-04 12-00-00"
 }
}
```


result


```
{
 "id":1,
 "result":{
  "warnlog":{
   "display_name":"Events",
   "logs":[{
    "Time":"2017-04-04 06-05-59",
    "Severity":"Info",
    "PluginId":"ESET Kernel",
    "Code":"Malware database was successfully updated to version 15198 (20170404).",
    "UserData":""
   },{
    "Time":"2017-04-04 11-12-59",
    "Severity":"Info",
    "PluginId":"ESET Kernel",
    "Code":"Malware database was successfully updated to version 15199 (20170404).",
    "UserData":""
   }]
  }
```

```
 },
 "error":null
}
```

3.10.7.2.5 获取激活状态

Get information about the last activation. Result of status can be { success, error }

Command line

```
ermm.exe get activation-status
```

Parameters

None

Example

call

```
{
 "command":"get_activation_status",
 "id":1,
 "version":"1"
}
```

result

```
{
 "id":1,
 "result":{
  "status":"success"
 },
 "error":null
}
```

3.10.7.2.6 获取扫描信息

Get information about running scan.

Command line

```
ermm.exe get scan-info
```

Parameters

None

Example

call

```
{
 "command":"get_scan_info",
 "id":1,
 "version":"1"
}
```

result

```
{
 "id":1,
 "result":{
  "scan-info":{
 "scans":[{
  "scan_id":65536,
  "timestamp":272,
  "state":"finished",
  "pause_scheduled_allowed":false,
  "pause_time_remain":0,
  "start_time":"2017-06-20T12:20:33Z",
  "elapsed_tickcount":328,
  "exit_code":0,
  "progress_filename":"Operating memory",
  "progress_arch_filename":"",
  "total_object_count":268,
  "infected_object_count":0,
  "cleaned_object_count":0,
  "log_timestamp":268,
  "log_count":0,
  "log_path":"C:\\ProgramData\\ESET\\ESET Security\\Logs\\eScan\\ndl31494.dat",
```

```
  "username":"test-PC\\test",
  "process_id":3616,
  "thread_id":3992,
  "task_type":2
 }],
 "pause_scheduled_active":false
}
 },
 "error":null
}
```

3.10.7.2.7 获取配置

Get the product configuration. Result of status may be { success, error }

Command line

```
ermm.exe get configuration --file C:\tmp\conf.xml --format xml
```

Parameters

Name	Value
file	the path where the configuration file will be saved
format	format of configuration: json, xml. Default format is xml

Example

call

```
{
 "command":"get_configuration",
 "id":1,
 "version":"1",
 "params":{
  "format":"xml",
  "file":"C:\\tmp\\conf.xml"
 }
}
```

result

```
{
 "id":1,
 "result":{
```

```
  "configuration":"PD94bWwgdmVyc2lvbj0iMS4w=="
 },
 "error":null
}
```

3.10.7.2.8 获取更新状态

Get information about the update. Result of status may be { success, error }

Command line

```
ermm.exe get update-status
```

Parameters

None

Example

call

```
{
 "command":"get_update_status",
 "id":1,
 "version":"1"
}
```

result

```
{
 "id":1,
 "result":{
  "last_update_time":"2017-06-20 13-21-37",
  "last_update_result":"error",
  "last_successful_update_time":"2017-06-20 11-21-45"
 },
 "error":null
}
```

3.10.7.2.9 启动扫描

Start scan with the product

Command line

```
ermm.exe start scan --profile "profile name" --target "path"
```

Parameters

Name	Value
profile	Profile name of On-demand computer scan defined in product
target	Path to be scanned

Example

call

```
{
 "command":"start_scan",
 "id":1,
 "version":"1",
 "params":{
  "profile":"Smart scan",
  "target":"c:\\"
 }
}
```

result

```
{
 "id":1,
 "result":{
  "task_id":458752
 },
 "error":null
}
```

3.10.7.2.10 启动激活

Start activation of product

Command line

```
ermm.exe start activation --key "activation key" | --offline "path to offline file" | --token "activation to
```

Parameters

Name	Value
key	Activation key
offline	Path to offline file
token	Activation token

Example

call

```
{
 "command":"start_activation",
 "id":1,
 "version":"1",
 "params":{
  "key":"XXXX-XXXX-XXXX-XXXX-XXXX"
 }
}
```

result

```
{
 "id":1,
 "result":{
 },
 "error":null
}
```

3.10.7.2.11 启动停用

Start deactivation of the product

Command line

```
ermm.exe start deactivation
```

Parameters

None

Example

call

```
{
 "command":"start_deactivation",
 "id":1,
 "version":"1"
}
```

result

```
{
 "id":1,
 "result":{
 },
 "error":null
}
```

3.10.7.2.12 启动更新

Start update of the product. Only one update may be running in the product so in case the update is already running, "Task already running" error code is returned

Command line

```
ermm.exe start update
```

Parameters

None

Example

call

```
{
 "command":"start_update",
```

```
 "id":1,
 "version":"1"
}
```

result

```
{
 "id":1,
 "result":{
 },
  "error":{
   "id":4,
   "text":"Task already running."
  }
}
```

3.10.7.2.13 设置配置

Set configuration to the product. Result of status may be { success, error }

Command line

```
ermm.exe set configuration --file C:\tmp\conf.xml --format xml --password pass
```

Parameters

Name	Value
file	the path where the configuration file will be saved
password	password for configuration
value	configuration data from the argument (encoded in base64)

Example

call

```
{
 "command":"set_configuration",
 "id":1,
 "version":"1",
 "params":{
  "format":"xml",
  "file":"C:\\tmp\\conf.xml",
  "password": "pass"
```

```
 }
}
```

result

```
{
 "id":1,
 "result":{
 },
 "error":null
}
```

3.11 词汇表

3.11.1 威胁类型

渗透是一种试图进入和 /或损坏用户计算机的恶意软件。

3.11.1.1 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的威胁。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。

3.11.1.2 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。

3.11.1.3 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** - 能够从 Internet 下载其他威胁的恶意程序。
- **Dropper** - 能够将其他类型的恶意软件放入所破坏计算机的恶意程序。
- **Backdoor** - 与远程攻击者通信，允许其获得计算机访问权限并控制计算机的恶意程序。
- **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。

3.11.1.4 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. 当它们隐藏自己而不被一般测试检测到时：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。

3.11.1.5 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。

3.11.1.6 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记录程序的列表。

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，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 -它们看上去像间谍软件防护程序，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。

3.11.1.7 加壳程序

加壳程序是一个运行时自解压的可执行文件，可将多种恶意软件合并在单个包中。

常见的加壳程序包括：UPX、PE_Compact、PKLite 和 ASPack。若使用不同的加壳程序进行压缩，相同的恶意软件的检测方式可能会有所不同。此外，加壳程序还能使其 签名 随着时间发生变异，从而使恶意软件更加难以检测和移除。

3.11.1.8 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。

3.11.1.9 潜在的不受欢迎应用程序

潜在的不受欢迎应用程序是一种包含广告软件、将安装工具栏或具有其他不明对象的程序。在某些情况下，用户可能觉得潜在的不受欢迎应用程序的好处多于风险。为此，与其他类型的恶意软件（例如木马程序或蠕虫）相比，ESET 将这些应用程序划分到较低风险类别中。

警告 -发现潜在威胁

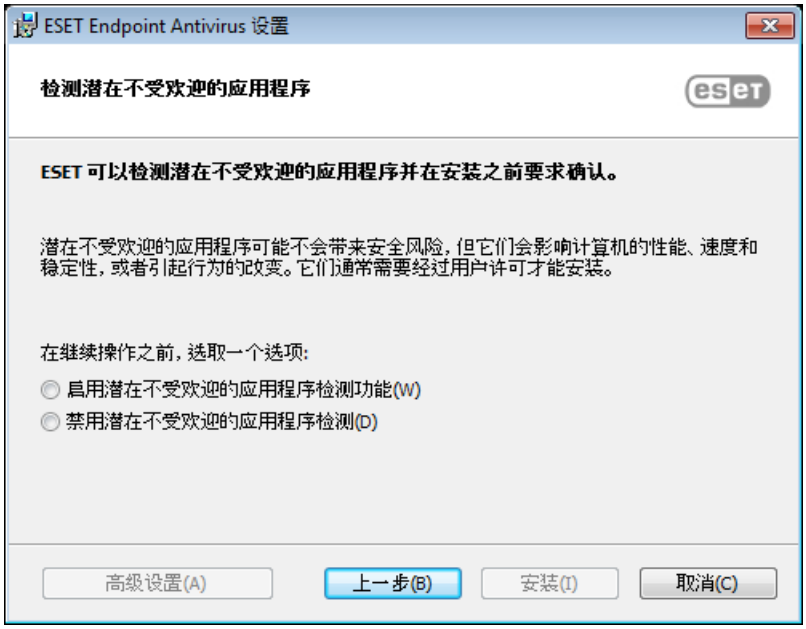
检测到潜在的不受欢迎应用程序后，您将能够确定采取哪种操作：

1. **清除 断开连接**：此选项将终止操作并阻止潜在的威胁进入系统。
2. **不操作**：此选项允许潜在威胁进入系统。
3. 若要使应用程序以后能够在计算机上运行而不受到打扰，请单击**更多信息 显示高级选项**，然后选中**从检测中排除**旁的复选框。

当检测到潜在的不受欢迎应用程序且无法清除时，屏幕右下角将显示消息窗口：**地址已被阻止**。有关此事件的更多信息，请从主菜单导航至**工具** > **日志文件** > **已过滤的网站**。

潜在的不受欢迎应用程序 -设置

安装 ESET 产品时，您可以确定是否启用潜在不受欢迎的应用程序检测，如下所示：

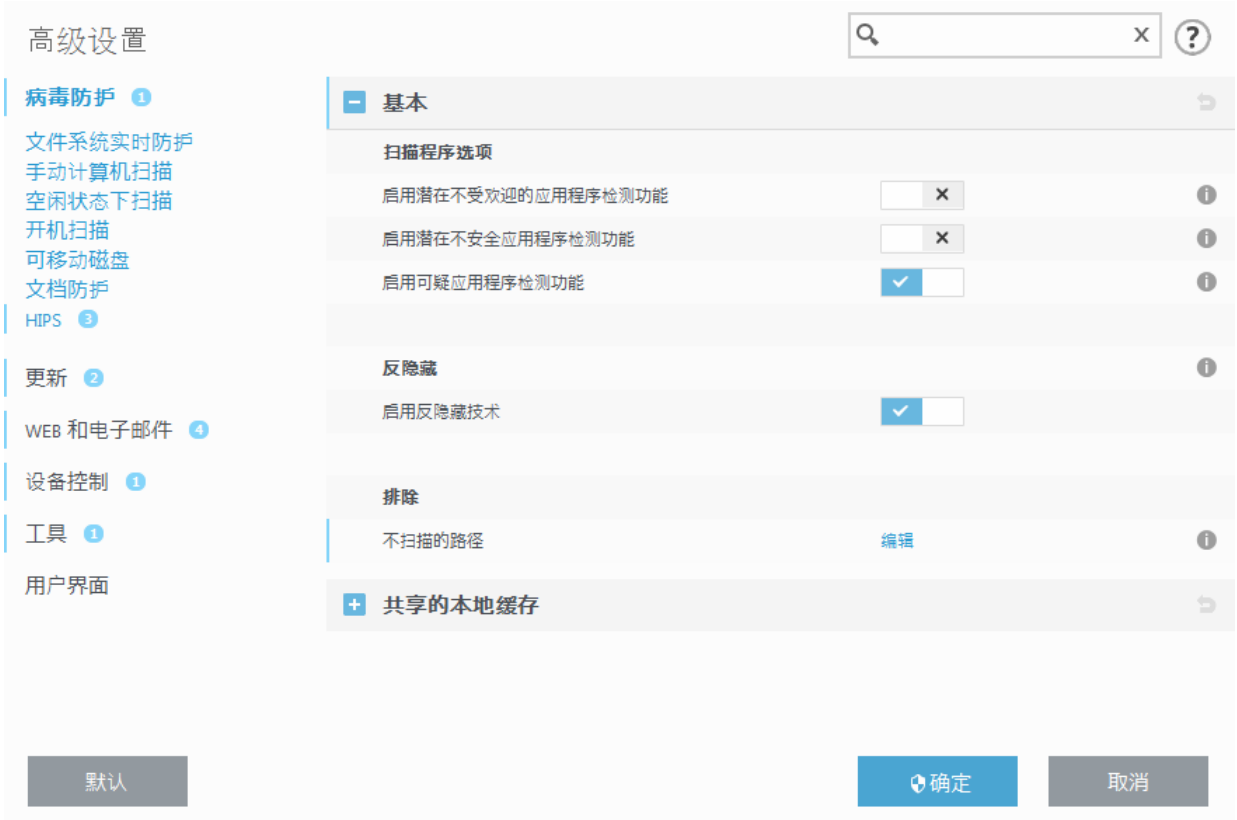


警告

潜在不受欢迎的应用程序可能安装广告软件、工具栏或包含其他不受欢迎和不安全的程序功能。

可随时在程序设置中修改这些设置。若要启用或禁用潜在不受欢迎、不安全或可疑的应用程序检测，请按照以下说明操作：

1. 打开您的 ESET 产品。如何打开我的 ESET 产品？
2. 按 **F5** 键以访问**高级设置**。
3. 单击**病毒防护**并根据您的偏好启用或禁用以下选项：**启用潜在不受欢迎的应用程序检测功能**？**启用潜在不安全应用程序检测功能**和**启用可疑应用程序检测功能**。单击**确定**以确认。



潜在的不受欢迎应用程序 -软件封装程序

软件封装程序是由一些托管文件的网站使用的特殊类型的应用程序修改。它是一种第三方工具，可安装用户想要下载的程序，但会添加附加软件，例如工具栏或广告软件。附加的软件可能还会更改您的 Web 浏览器主页和搜索设置。此外，托管文件的网站通常不会通知软件供应商或下载收件人已进行了修改，并且不会轻易允许取消修改。基于这些原因，ESET 将软件封装程序归类为潜在不受欢迎的应用程序类型，以使用户可以接受或不接受下载。

请参阅此 ESET 知识库文章了解此帮助页的更新版本。

有关详细信息，请单击此处。

3.11.2 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 的迅速发展中起到了至关重要的作用。

不幸地是，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：

- 尽量不要在 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。
- 不时地更改您的电子邮件地址
- 使用反垃圾邮件解决方案

3.11.2.1 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市场营销工具与当前和潜在客户进行有效通信。

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。

3.11.2.2 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。

3.11.2.3 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（例如金融机构、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。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。

3.11.2.4 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。
- 以各种借口（数据验证、财务操作）要求您输入某些个人数据 -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 ‶iagra 拼写成 ‶aigra 等。

3.11.3 ESET 技术

3.11.3.1 漏洞利用阻止程序

漏洞利用阻止程序通常监控可利用的应用程序（浏览器、文档阅读器、电子邮件客户端、Flash、Java 等），并且它不是仅针对特定 CVE 标识符，而是专注于利用技术。该程序触发时，会对进程的行为进行分析：如果行为被认为可疑，可能会立即在计算机上阻止该威胁。

虽然 ESET 的扫描引擎涵盖出现在格式错误的文档文件中的漏洞利用以及网络攻击防护的目标是通信级别，但是漏洞利用阻止程序技术可阻止利用进程本身并记录有关威胁的数据，该数据之后将发送到 ESET LiveGrid® 云系统。该数据将由 ESET 威胁实验室进行处理，并用来更好地保护所有用户，以使他们免受未知威胁和零日攻击（新发布的恶意软件，目前没有预配置的补救措施）的侵害。

3.11.3.2 高级内存扫描程序

高级内存扫描程序与漏洞利用阻止程序结合使用以提供对恶意软件更好的防范，后者旨在通过迷惑和 ⁄或加密方法来逃过反恶意软件产品的检测。为了防止普通的模拟或启发式扫描无法检测出某个威胁，高级内存扫描程序可以在可疑行为和威胁出现在系统内存中时识别可疑行为并扫描威胁。此解决方案对迷惑性极强的恶意软件也非常有效。与漏洞利用阻止程序不同，这是执行后方法，这意味着可能会出现在它检测到威胁之前某些恶意活动已执行的风险。但是在其他检测技术都失效的情况下，该方法可以提供额外一层安全性。

3.11.3.3 ESET LiveGrid®

ESET LiveGrid® 建立在 ThreatSense.Net® 高级早期预警系统之上，并利用 ESET 用户在世界各地提交并发送给 ESET 病毒实验室的数据。通过提供可疑的样本和原始的元数据，ESET LiveGrid® 使我们能够立即对客户的需要作出反应并使 ESET 能够持续应对最新的威胁。ESET 恶意软件研究人员使用该信息生成全球威胁的性质和范围的精确快照，以帮助我们将注意力放在正确的目标上。ESET LiveGrid® 数据在我们设置自动处理优先级时起着重要的作用。

此外，它还实施了一个信誉系统，可帮助提高我们的反恶意软件解决方案的整体效率。在用户系统上检查可执行文件或压缩文件时，系统会首先将其哈希标记与数据库中的白名单和黑名单项进行对比。如果发现它位于白名单中，则检查的文件将被视作未感染并且将被标记，以便从日后的扫描中排除。如果发现它位于黑名单中，将根据威胁的性质采取相应的措施。如果未发现匹配，将彻底扫描文件。基于此次扫描的结果，文件将被分类为威胁或非威胁。此方法对于扫描性能有着极为重要的积极影响。

此信誉系统可以有效地检测恶意软件样本，甚至是在其签名通过检测引擎更新分发到用户之前（每天执行若干次）。

3.11.3.4 Java 漏洞利用阻止程序

Java 漏洞利用阻止程序是现有 ESET 漏洞利用阻止程序防护的扩展。它可以监控 Java 中类似漏洞利用的行为。可以将阻止的样本报告给恶意软件分析人员，以便分析人员创建签名来在不同的层（URL 阻止、文件下载等）上阻止未遂的 Java 漏洞利用。

3.11.3.5 基于脚本的攻击防护

基于脚本的攻击防护包含针对 Web 浏览器中的 javascript 防护和针对 Powershell 中的脚本（wscript.exe 以及 cscript.exe ）的 Antimalware Scan Interface (AMSI) 防护。

警告
必须启用 HIPS 才能使此功能起作用。

基于脚本的攻击防护支持以下 Web 浏览器：

- Mozilla Firefox
- Google Chrome
- Internet Explorer
- Microsoft Edge

注意
由于浏览器的文件签名经常更改，所以 Web 浏览器受支持的的最低版本可能不同。Web 浏览器的最新版本始终受支持。

3.11.3.6 勒索软件防护

勒索软件是一种恶意软件，它会通过锁定系统的屏幕或加密文件来阻止用户访问其系统。勒索软件防护会监视应用程序和进程尝试修改您个人数据的行为。如果某个应用程序的行为被视为恶意，或基于信誉的扫描显示某个应用程序可疑，则会阻止该应用程序，或者会询问用户是要阻止它还是允许它。

重要信息
必须启用 ESET LiveGrid® 才能使勒索软件防护正常工作。

3.11.3.7 DNA 检测

检测类型范围为非常特定的哈希到 ESET DNA 检测，此类检测是恶意行为和恶意软件特征的复杂定义。虽然攻击者可以轻易地修改或篡改恶意代码，但无法轻易更改对象的行为，因而 ESET DNA 检测旨在利用该原则。

我们对代码进行深入分析，然后提取对其行为负责的 基因 ”，从而构建 ESET DNA 检测，此类检测用于评估潜在的可疑代码（不论是在磁盘上还是在正在运行的进程内存中找到代码）。DNA 检测可识别特定已知恶意软件样本、已知恶意软件家族的新变种、甚至以前未见过或未知的恶意软件（包含指示恶意行为的基因）。

3.11.3.8 UEFI 扫描程序

统一可扩展固件接口 (UEFI) 扫描程序是基于主机的入侵防御系统 (HIPS) 的一部分，可保护计算机上的 UEFI。 UEFI 是在启动过程开始时加载到内存中的固件。 该代码存在于焊接在主板上的闪存芯片中。 通过感染它，攻击者可以部署在系统重新安装和重新启动后仍然存在的恶意软件。 反恶意软件解决方案也很容易忽略此类恶意软件，因为大多数反恶意软件不会扫描该层。

将自动启用 UEFI 扫描程序。 也可以在主程序窗口中，通过依次单击**计算机扫描** > **高级扫描** > **自定义扫描**，选择**引导区 /UEFI** 目标，来手动启动计算机扫描。 有关计算机扫描的更多信息，请参阅计算机扫描一节。

如果您的计算机已感染 UEFI 恶意软件，请阅读以下 ESET 知识库文章：
我的计算机感染了 UEFI 恶意软件，我应该怎么做？