ESET NOD32 Antivirus

用户指南

单击此处显示此文档的联机版本

Digital Security
Progress. Protected.

ESET NOD32 Antivirus 由 ESET, spol. s r.o. 开发

有关详细信息，请访问 https://www.eset.com

技术支持https://support.eset.com

修订日期 2024年m月12日

1 ESET NOD32 Antivirus 1
1.1 新功能 1
1.2 我有哪些产品？ 2
1.3 系统要求 3
1.3 过时的 Microsoft Windows 版本 4
1.4 预防 4
1.5 帮助页面 5
2 安装 6
2.1 Live installer 6
2.2 脱机安装 8
2.2 订阅更新 9
2.2 产品升级 10
2.2 订阅降级 11
2.2 产品降级 11
2.3 安装故障排除程序 12
2.4 安装完成后的首次扫描 12
2.5 升级到更新版本 13
2.5 旧版产品自动升级 13
2.5 将安装 ESET NOD32 Antivirus 14
2.5 更改为其他产品线 14
2.5 注册 14
2.5 激活进度 14
2.5 成功激活 14
3 入门 15
3.1 系统托盘图标 15
3.2 键盘快捷键 15
3.3 配置文件 16
3.4 更新 17
4 产品激活 18
4.1 在激活过程中输入激活密钥 19
4.2 用户 ESET HOME 帐户 19
4.3 激活免费试用版 20
4.4 免费 ESET 激活密钥 20
4.5 激活失败 – 常见情况 21
4.6 订阅状态 22
4.6 由于订阅过度使用导致激活失败 22
5 使用 ESET NOD32 Antivirus 23
5.1 概览 24
5.2 计算机扫描 27
5.2 自定义扫描启动程序 28
5.2 扫描进度 30
5.2 计算机扫描日志 32
5.3 更新 33
5.3 对话窗口 – 需要重新启动 36
5.3 如何创建更新任务 36
5.4 工具 37
5.4 日志文件 38
5.4 日志过滤 40
5.4 正在运行的进程 41
5.4 安全报告 43

5.4 ESET SysInspector 44
5.4 计划任务 45
5.4 计划扫描选项 47
5.4 计划任务概述 48
5.4 任务详细信息 48
5.4 任务计时 48
5.4 任务计时 – 一次 48
5.4 任务计时 – 每天 49
5.4 任务计时 – 每周 49
5.4 任务计时 – 由事件触发 49
5.4 跳过的任务 49
5.4 任务详细信息 – 更新 50
5.4 任务详细信息 – 运行应用程序 50
5.4 系统清理器 50
5.4 隔离区 51
5.4 选择样本以供分析 53
5.4 选择样本以供分析 – 可疑文件 54
5.4 选择样本以供分析 – 可疑站点 55
5.4 选择样本以供分析 – 误报文件 55
5.4 选择样本以供分析 – 误报站点 55
5.4 选择样本以供分析 – 其他 55
5.5 设置 55
5.5 计算机防护 56
5.5 检测到渗透 57
5.5 Internet 防护 60
5.5 网络钓鱼防护 61
5.5 导入和导出设置 62
5.6 帮助和支持 63
5.6 关于 ESET NOD32 Antivirus 64
5.6 ESET 新闻 64
5.6 提交系统配置数据 65
5.6 技术支持 66
5.7 ESET HOME 帐户 66
5.7 连接到 ESET HOME 67
5.7 登录到 ESET HOME 68
5.7 登录失败 – 常见错误 69
5.7 在 ESET HOME 中添加设备 70
6 高级设置 70
6.1 检测引擎 71
6.1 排除 71
6.1 性能排除 72
6.1 添加或编辑性能排除 73
6.1 路径排除格式 74
6.1 检测排除 75
6.1 添加或编辑检测排除 76
6.1 创建检测排除向导 78
6.1 检测引擎高级选项 78
6.1 网络通信扫描程序 78
6.1 基于云的防护 79
6.1 基于云的防护的排除过滤器 81
6.1 恶意软件扫描 81

6.1 扫描配置文件 82
6.1 扫描目标 82
6.1 空闲状态下扫描 83
6.1 空闲状态检测 83
6.1 开机扫描 83
6.1 自动启动文件检查 84
6.1 可移动磁盘 84
6.1 文档防护 85
6.1 HIPS – 主机入侵防御系统 86
6.1 HIPS 排除 88
6.1 HIPS 高级设置 88
6.1 始终允许加载驱动程序 88
6.1 HIPS 交互窗口 88
6.1 学习模式已结束 89
6.1 检测到潜在的勒索软件行为 90
6.1 HIPS 规则管理 90
6.1 HIPS 规则设置 91
6.1 为 HIPS 添加应用程序/注册表路径 93
6.2 更新 94
6.2 更新回滚 95
6.2 回滚时间间隔 97
6.2 产品更新 97
6.2 连接选项 97
6.3 保护 98
6.3 文件系统实时防护 101
6.3 进程排除 102
6.3 添加或编辑进程排除 103
6.3 何时修改实时防护配置 103
6.3 检查实时防护 103
6.3 实时防护不工作时如何应对 104
6.3 SSL/TLS 104
6.3 应用程序扫描规则 106
6.3 证书规则 107
6.3 加密的网络通信 107
6.3 电子邮件客户端防护 108
6.3 邮件传输防护 108
6.3 排除的应用程序 109
6.3 排除的 IP 110
6.3 邮箱防护 111
6.3 集成 112
6.3 Microsoft Outlook 工具栏 112
6.3 确认对话框 112
6.3 重新扫描邮件 112
6.3 响应 113
6.3 ThreatSense 113
6.3 Web 访问保护 116
6.3 排除的应用程序 118
6.3 排除的 IP 119
6.3 URL 列表管理 120
6.3 地址列表 121
6.3 创建新的地址列表 122

6.3 如何添加 URL 掩码 123
6.3 HTTP(S) 通信扫描 123
6.3 ThreatSense 123
6.3 设备控制 126
6.3 设备控制规则编辑器 127
6.3 已检测的设备 128
6.3 添加设备控制规则 128
6.3 设备组 130
6.3 ThreatSense 131
6.3 清除级别 134
6.3 不扫描的文件扩展名 134
6.3 其他 ThreatSense 参数 135
6.4 工具 135
6.4 Microsoft Windows® 更新 135
6.4 对话窗口 – 系统更新 136
6.4 更新信息 136
6.4 ESET CMD 136
6.4 日志文件 138
6.4 游戏模式 138
6.4 诊断 139
6.4 技术支持 140
6.5 连接 140
6.6 用户界面 141
6.6 用户界面元素 141
6.6 访问设置 142
6.6 高级设置的密码 143
6.6 屏幕阅读器支持 143
6.7 通知 144
6.7 对话窗口 – 应用程序状态 144
6.7 桌面通知 145
6.7 桌面通知列表 146
6.7 交互警报 147
6.7 确认消息 148
6.7 转发 150
6.8 隐私设置 152
6.8 恢复为默认设置 152
6.8 恢复当前部分中的所有设置 152
6.8 保存配置时出错 153
6.9 命令行扫描程序 153
7 常见问题解答 155
7.1 如何更新 ESET NOD32 Antivirus 156
7.2 如何从 PC 中删除病毒 156
7.3 如何在计划任务中创建新任务 157
7.4 如何计划每周计算机扫描 157
7.5 如何解锁高级设置 158
7.6 如何通过 ESET HOME 解决产品停用 158
7.6 产品已停用，设备已断开连接 159
7.6 产品未激活 159
8.1 客户体验改进计划 159
8.2 最终用户许可协议 160
8.3 隐私策略 167

ESET NOD32 Antivirus

ESET NOD32 Antivirus 代表了真正集成计算机安全的新方法。最新版本的 ESET LiveGrid® 扫描引擎提高了速度和精确性，以保护您的计算机安全。 由此形成了一个能够对可能威胁您的计算机的攻击和恶意软件持续保持警戒状态的智能系统。

ESET NOD32 Antivirus 是结合了最高防护与最少系统占用的完整安全解决方案。我们的先进技术使用人工智能来防止病毒、间谍软件、木马、蠕虫、广告软件Rootkit 和其他威胁的渗透，且不会妨碍系统性能或中断计算机的运行。

功能和优点

重新设计的用户界面	此版本中的用户界面已基于可用性测试结果进行了大量重新设计和简化。已仔细检查所有 GUI 用词和通知，并且该界面现在支持从右到左的语言，例如希伯来语和阿拉伯语。在线帮助现在集成到 ESET NOD32 Antivirus 中，并提供动态更新支持内容。
深色模式	一个扩展，有助于快速将屏幕切换到深色主题。可以在用户界面元素中选择您首选的颜色方案。
病毒和间谍软件防护	主动检测和清除更多已知和未知病毒、蠕虫、木马和 Rootkit即使是前所未见的恶意软件，高级启发式扫描也可对其进行标志，从而防止未知威胁并在恶意软件产生危害之前使其失效Web 访问保护和网络钓鱼防护可监视 Web 浏览器和远程服务器之间的通信（包括 SSL电子邮件客户端防护可控制通过 POP3(S) 和 IMAP(S) 协议接收的电子邮件通信。
定期更新	定期更新检测引擎（之前称为“病毒库”）和程序模块是确保计算机保持最高安全级别的最佳方法。
ESET LiveGrid®（云端信誉）	用户可以直接从 ESET NOD32 Antivirus 检查运行进程和文件的信誉。
设备控制	自动扫描所有 USB 盘、内存卡和 CD/DVD将根据磁盘的类型、制造商、大小和其他特性阻止可移动磁盘。
HIPS 功能	您可以更详细地自定义系统的行为；为系统注册表、活动进程和程序指定规则以及微调您的安全状态。
游戏模式	推迟所有弹出窗口、更新或其他系统占用量大的活动，以为游戏或其他全屏活动保留系统资源。

订阅必须处于活动状态ESET NOD32 Antivirus 的功能才能运行。我们建议您在 ESET NOD32 Antivirus 的订阅到期前几周续订订阅。

新功能

ESET NOD32 Antivirus 17.1 中的新功能

- 小幅改进网络检查器
- 修复了微小错误并进行了其他方面的改进

要禁用**新功能通知**，请执行以下操作：
1. 打开高级设置 > **通知** > **桌面通知**
2. 单击**桌面通知**旁边的**编辑**
3. 取消选中**显示新功能通知**复选框，然后单击**确定**
有关通知的详细信息，请参见通知部分。

有关 ESET NOD32 Antivirus 中更改的详细列表，请参阅 ESET NOD32 Antivirus 更改日志

我有哪些产品？

ESET 在新产品中提供多层安全性，从强大而快速的病毒防护解决方案到具有最少系统占用的一体式安全解决方案：

- **ESET NOD32 Antivirus**
- **ESET Internet Security**
- **ESET Smart Security Premium**
- **ESET Security Ultimate**

若要确定您安装了哪个产品，请打开主程序窗口，您将在窗口顶部看到产品的名称（请参阅知识库文章）

下表详细介绍了每个特定产品中提供的功能。

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
检测引擎	✔	✔	✔	✔
高级机器学习	✔	✔	✔	✔
漏洞利用阻止程序	✔	✔	✔	✔
基于脚本的攻击防护	✔	✔	✔	✔
网络钓鱼防护	✔	✔	✔	✔
Web 访问保护	✔	✔	✔	✔
HIPS（包括勒索软件防护）	✔	✔	✔	✔
反垃圾邮件		✔	✔	✔
防火墙		✔	✔	✔
网络检查器		✔	✔	✔
网络摄像机防护		✔	✔	✔
网络攻击防护		✔	✔	✔
僵尸网络防护		✔	✔	✔
安全银行业务和浏览		✔	✔	✔
浏览器隐私政策和安全性		✔	✔	✔
家长控制		✔	✔	✔
防盗		✔	✔	✔
Password Manager			✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

可能并未针对您的语言/地区提供上述某些产品。

系统要求

若要使 ESET NOD32 Antivirus 发挥最佳性能，您的系统应满足以下硬件和软件要求：

支持的处理器

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

支持的操作系统

Microsoft® Windows® 11

Microsoft® Windows® 10

必须在所有 Windows 操作系统上安装对 Azure 代码签名的支持，才能安装或升级于 2023 年 7 月之后发布的 ESET 产品。更多信息

请始终尝试保持操作系统为最新版本。

ESET NOD32 Antivirus 功能要求

查看下表中特定 ESET NOD32 Antivirus 功能的系统要求：

功能	要求
Intel® Threat Detection Technology	查看支持的处理器
透明背景	Windows 10 版本 RS4 及更高版本。
专用清理器	非基于 ARM64 的处理器。
系统清理器	非基于 ARM64 的处理器。
漏洞利用阻止程序	非基于 ARM64 的处理器。
深度行为检测	非基于 ARM64 的处理器。

其他

需要 Internet 连接才能使激活和 ESET NOD32 Antivirus 更新正常运行。

在单个设备上同时运行的两个病毒防护程序不可避免地会导致系统资源冲突，例如减慢系统运行速度使其不可操作。

过时的 Microsoft Windows 版本

问题

- 您要在装有 Windows 7、Windows 8 (8.1) 或 Windows Home Server 2011 的计算机上安装最新版本的 ESET NOD32 Antivirus
- ESET NOD32 Antivirus 在安装期间显示错误**操作系统已过时**

详细信息

最新版本的 ESET NOD32 Antivirus需要 Windows 10 或 Windows 11 操作系统。

解决方案

有以下解决方案可供使用：

升级到 Windows 10 或 Windows 11

升级过程相对容易，并且在许多情况下，可以完成升级而不会丢失文件。在升级到 Windows 10 之前：

1. 备份重要数据
2. 阅读 Microsoft 的升级到 Windows 10 常见问题解答或升级到 Windows 11 常见问题解答，然后更新 Windows 操作系统。

安装 ESET NOD32 Antivirus 版本 16.0

如果无法升级 Windows，请安装 ESET NOD32 Antivirus 版本 16.0。有关详细信息，请参阅 ESET NOD32 Antivirus 版本 16.0 联机帮助。

预防

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

定期更新

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

下载安全补丁

恶意软件的作者通常利用各种系统漏洞，以提高恶意代码的传播效果。出于这种考虑，软件公司密切关注其应用程序中出现的任何漏洞，并且定期发布可消除潜在威胁的安全更新的原因。安全更新发布后需立即

下载，这非常重要Microsoft Windows 和 Web 浏览器（例如Internet Explorer程序是安全更新定期发布的两个程序示例。

备份重要数据

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

定期扫描计算机、查找病毒

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

遵循基本安全规则

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

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

帮助页面

欢迎使用 ESET NOD32 Antivirus 用户指南。此处提供的信息将为您介绍本产品，并帮助您使计算机更安全。

入门

在使用 ESET NOD32 Antivirus 之前，可以了解使用计算机时可能会遇到的各类检测和远程攻击。我们还编译了 ESET NOD32 Antivirus 中引入的一列新功能

从安装 ESET NOD32 Antivirus 开始。如果已安装 ESET NOD32 Antivirus请参阅使用 ESET NOD32 Antivirus

如何使用 ESET NOD32 Antivirus 帮助页面

联机帮助分为几个章节和子章节。在 ESET NOD32 Antivirus 中，按 **F1** 可查看有关当前已打开窗口的信息。

此程序允许您通过关键字搜索某个帮助主题，或者通过键入字词或短语来搜索内容。这两种方法的区别在于，关键字可能与文本中不包含该特定关键字的帮助页面在逻辑上相关。按字词和短语搜索将搜索所有页面的内容，并仅显示实际文字中包含所搜索字词的页面。

为了保持一致和避免混淆，本指南中使用的术语基于 ESET NOD32 Antivirus 用户界面。我们还使用了一组统一的符号来强调特别有用或非常重要的主题。

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

此信息需要您的注意，我们鼓励您不要跳过此内容。通常，它将提供非关键但重要的信息。

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

这是一个用例或实用示例，旨在帮助您了解如何使用某个功能或特性。

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

联机帮助是帮助内容的主要来源。当已连接 Internet 时，将自动显示最新的联机帮助版本。

安装

有多种方法可用于在您的计算机上安装 ESET NOD32 Antivirus 安装方法稍有差异，具体取决于国家/地区以及分发方式：

- Live 安装程序 – 已从 ESET 网站下载或 CD/DVD 该安装包通用于所有语言（请选择相应语言）。该 Live 安装程序文件较小，将自动下载安装 ESET NOD32 Antivirus 所需的其他文件。

- 脱机安装 – 使用 .exe 文件（文件大小超过 Live 安装程序），不需要连接 Internet 也不需要其他文件来完成安装。

在您安装 ESET NOD32 Antivirus 之前，确保您的计算机上没有安装其他病毒防护程序。如果在一台计算机上安装两个或更多病毒防护解决方案，可能彼此冲突。建议您卸载系统上的任何其他病毒防护程序。请参见 ESET 知识库文章，了解常见病毒防护软件的卸载工具列表（提供英语和多个其他语言版本）。

Live installer

已下载 Live 安装程序安装包后，双击安装文件并遵循安装向导中的分步说明操作。

您必须连接到 Internet 才可进行此类安装。

1. 从下拉菜单中选择适当语言，然后单击**继续**。

> 如果要安装的版本比以前的版本更高，并且设置受密码保护，请键入密码。可以在访问设置中配置设置密码。

2. 选择您对以下功能的偏好、阅读最终用户许可协议和隐私政策，然后单击**继续**或单击**全部允许并继续**以启用所有功能：

- ESET LiveGrid® 反馈系统
- 潜在不受欢迎的应用程序
- 客户体验改进计划

> 通过单击**继续**或**全部允许并继续**，即表示您同意最终用户许可协议并确认隐私政策。

3. 要使用 ESET HOME 激活、管理和查看设备的安全性，请将设备连接到 ESET HOME 帐户。单击**跳过登录**以继续，无需连接到 ESET HOME。您以后可以将设备连接到您的 ESET HOME 帐户。

4. 如果继续而不连接到 ESET HOME，请选择一个激活选项。如果您基于以前的版本安装较新的版本，将自动输入**激活密钥**。

5. 安装向导会基于您的订阅确定安装哪个 ESET 产品。将始终预选择安全功能最多的版本。如果要安装其他版本的 ESET 产品，则单击**更改产品**。单击**继续**以开始安装过程。可能需要一些时间。

> 如果在过去卸载的 ESET 产品中存在任何残留数据（文件或文件夹），系统会提示您允许将其删除。单击**安装**以继续。

6. 单击**完成**以退出安装向导。

安装故障排除程序

安装并激活产品后，模块开始下载。正在初始化防护，某些功能可能无法完全正常工作，除非下载完成。

脱机安装

使用下面的脱机安装程序 (.exe) 下载并安装 ESET Windows 家庭版产品。选择要下载的 ESET 家庭版产品（32 位、64 位或 ARM）

ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
64 位下载 32 位下载 ARM 下载	64 位下载 32 位下载 ARM 下载	64 位下载 32 位下载 ARM 下载	64 位下载 32 位下载 ARM 下载

如果您的 Internet 连接处于活动状态，请使用 Live 安装程序安装 ESET 产品

启动脱机安装程序 (.exe) 后，“安装向导”会引导您完成安装过程。

1. 从下拉菜单中选择适当语言，然后单击**继续**。

如果要安装的版本比以前的版本更高，并且设置受密码保护，请键入密码。可以在访问设置中配置设置密码。

2. 选择您对以下功能的偏好、阅读最终用户许可协议和隐私政策，然后单击**继续**或单击**全部允许并继续**以启用所有功能：

- ESET LiveGrid® 反馈系统
- 潜在不受欢迎的应用程序
- 客户体验改进计划

通过单击**继续**或**全部允许并继续**，即表示您同意最终用户许可协议并确认隐私政策。

3. 单击**跳过登录**。当已连接 Internet 时，可以将设备连接到 ESET HOME 帐户。

4. 单击**跳过激活**。必须在安装之后激活 ESET NOD32 Antivirus才能完全起作用。产品激活需要 Internet 连接处于活动状态。

5. “安装向导”会基于下载的脱机安装程序显示将安装哪个 ESET 产品。单击**继续**以开始安装过程。可能需要一些时间。

如果在过去卸载的 ESET 产品中存在任何残留数据（文件或文件夹），系统会提示您允许将其删除。单击**安装**以继续。

6. 单击**完成**以退出安装向导。

安装故障排除程序

订阅更新

当用于激活 ESET 产品的订阅发生更改时，将出现此通知窗口。更改后的订阅让您可以激活安全功能较多的产品。如果未执行任何更改ESET NOD32 Antivirus 将显示一次警报窗口，称为**更改为功能较多的产品**。

是（建议） – 将自动安装安全功能更多的产品。

不，谢谢 – 不进行任何更改，并且通知将永久消失。

要以后更改产品，请参阅我们的 ESET 知识库文章。有关 ESET 订阅的详细信息，请参阅订阅常见问题解答。

下表详细介绍了每个特定产品中提供的功能。

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
检测引擎	✔	✔	✔	✔
高级机器学习	✔	✔	✔	✔
漏洞利用阻止程序	✔	✔	✔	✔
基于脚本的攻击防护	✔	✔	✔	✔
网络钓鱼防护	✔	✔	✔	✔
Web 访问保护	✔	✔	✔	✔
HIPS包括勒索软件防护）	✔	✔	✔	✔
反垃圾邮件		✔	✔	✔
防火墙		✔	✔	✔
网络检查器		✔	✔	✔
网络摄像机防护		✔	✔	✔
网络攻击防护		✔	✔	✔
僵尸网络防护		✔	✔	✔
安全银行业务和浏览		✔	✔	✔
浏览器隐私政策和安全性		✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
家长控制		✔	✔	✔
防盗		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

产品升级

您已下载默认安装程序并决定要将产品更改为激活状态，或者您希望将已安装的产品更改为安全功能更多的产品。

在安装期间更改产品

下表详细介绍了每个特定产品中提供的功能。

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
检测引擎	✔	✔	✔	✔
高级机器学习	✔	✔	✔	✔
漏洞利用阻止程序	✔	✔	✔	✔
基于脚本的攻击防护	✔	✔	✔	✔
网络钓鱼防护	✔	✔	✔	✔
Web 访问保护	✔	✔	✔	✔
HIPS（包括勒索软件防护）	✔	✔	✔	✔
反垃圾邮件		✔	✔	✔
防火墙		✔	✔	✔
网络检查器		✔	✔	✔
网络摄像机防护		✔	✔	✔
网络攻击防护		✔	✔	✔
僵尸网络防护		✔	✔	✔
安全银行业务和浏览		✔	✔	✔
浏览器隐私政策和安全性		✔	✔	✔
家长控制		✔	✔	✔
防盗		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

订阅降级

当用于激活 ESET 产品的订阅发生更改时，将出现此对话窗口。更改后的订阅只能用于安全功能较少的其他 ESET 产品。产品已自动更改，以防止保护丢失。

有关 ESET 订阅的详细信息，请参阅订阅常见问题解答

下表详细介绍了每个特定产品中提供的功能。

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
检测引擎	✔	✔	✔	✔
高级机器学习	✔	✔	✔	✔
漏洞利用阻止程序	✔	✔	✔	✔
基于脚本的攻击防护	✔	✔	✔	✔
网络钓鱼防护	✔	✔	✔	✔
Web 访问保护	✔	✔	✔	✔
HIPS包括勒索软件防护）	✔	✔	✔	✔
反垃圾邮件		✔	✔	✔
防火墙		✔	✔	✔
网络检查器		✔	✔	✔
网络摄像机防护		✔	✔	✔
网络攻击防护		✔	✔	✔
僵尸网络防护		✔	✔	✔
安全银行业务和浏览		✔	✔	✔
浏览器隐私政策和安全性		✔	✔	✔
家长控制		✔	✔	✔
防盗		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

产品降级

您当前安装的产品的安全功能超出您要激活的产品。

下表详细介绍了每个特定产品中提供的功能。

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
检测引擎	✔	✔	✔	✔
高级机器学习	✔	✔	✔	✔

	ESET NOD32 Antivirus	ESET Internet Security	ESET Smart Security Premium	ESET Security Ultimate
漏洞利用阻止程序	✔	✔	✔	✔
基于脚本的攻击防护	✔	✔	✔	✔
网络钓鱼防护	✔	✔	✔	✔
Web 访问保护	✔	✔	✔	✔
HIPS（包括勒索软件防护）	✔	✔	✔	✔
反垃圾邮件		✔	✔	✔
防火墙		✔	✔	✔
网络检查器		✔	✔	✔
网络摄像机防护		✔	✔	✔
网络攻击防护		✔	✔	✔
僵尸网络防护		✔	✔	✔
安全银行业务和浏览		✔	✔	✔
浏览器隐私政策和安全性		✔	✔	✔
家长控制		✔	✔	✔
防盗		✔	✔	✔
Password Manager			✔	✔
ESET Secure Data			✔	✔
ESET LiveGuard			✔	✔
VPN				✔
Identity Protection				✔

安装故障排除程序

如果在安装期间发生问题，安装向导将提供可解决此问题的故障排除程序（如果可能）。

单击**运行故障排除程序**以启动故障排除程序。故障排除程序完成后，按照建议的解决方案操作。

如果问题持续存在，请参见常见安装错误和解决方案列表。

安装完成后的首次扫描

安装 ESET NOD32 Antivirus 后，计算机扫描将在首次成功更新之后自动启动，以检查是否存在恶意代码。

您也可以单击**计算机扫描**>**扫描计算机**来从主程序窗口手动启动计算机扫描。有关计算机扫描的更多信息，请参见计算机扫描。

升级到更新版本

发布 ESET NOD32 Antivirus 的新版本，是为了实施改进或修复程序模块的自动更新无法解决的问题。有多种方法可以升级到更高版本：

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，以确保所有可能的系统配置都能够工作。如果发布后需要立刻升级到更新版本，请使用以下方法之一。
确保已在**高级设置** > 更新 > **配置文件** > **更新**中启用了**应用程序功能更新**。

2. 在主程序窗口的**更新**部分中，通过单击**检查更新**，进行手动升级。

3. 手动（通过以前的版本来下载并安装更新版本。

有关其他信息和图文并茂说明，请参阅：

- 更新 ESET 产品 – 检查最新产品模块
- 什么是不同的 ESET 产品更新和发布类型？

旧版产品自动升级

您的 ESET 产品版本已不再受支持，该产品已升级到最新版本。

常见安装问题

每个新版本的 ESET 产品都具有许多错误修复和改进功能。具有 ESET 产品有效订阅的现有客户可以免费升级到最新版本的同一产品。

若要完成安装：

1. 单击**接受并继续**接受最终用户许可协议并确认隐私政策。如果您不同意最终用户许可协议，请单击**卸载**。无法恢复到以前的版本。

2. 单击**全部允许并继续**以允许 ESET LiveGrid® 反馈系统和客户体验改进计划；如果您不想参与，请单击**继续**。

3. 在使用激活密钥激活新的 ESET 产品后，“概述”页面即会显示。如果未找到您的订阅信息，请继续使用免费试用版。如果在以前产品中使用的订阅无效，请激活您的 ESET 产品。

4. 需要重新启动设备才能完成安装。

将安装 ESET NOD32 Antivirus

可以显示此对话窗口：

- 在安装过程中 – 单击**继续**以安装 ESET NOD32 Antivirus。
- 在 ESET NOD32 Antivirus 中更改订阅时 – 单击**激活**以更改订阅并激活 ESET NOD32 Antivirus。

通过使用**更改产品**选项，可以根据 ESET 订阅在各个 ESET Windows 家庭版产品间切换。请参阅我有哪些产品？获取详细信息。

更改为其他产品线

根据 ESET 订阅，可以在各个 ESET Windows 家庭版产品间切换。请参阅我有哪些产品？获取详细信息。

注册

请通过填写包含在注册表中的字段并单击**激活**来注册您的订阅。括号中标记为必需的字段为必填字段。此信息将仅用于与您的 ESET 订阅相关的事项。

激活进度

请等待几秒钟，以待激活过程完成（所需时间可能会因 Internet 连接速度或计算机而异）。

成功激活

激活过程完成。

模块更新将在几秒后开始。ESET NOD32 Antivirus 的定期更新将立即开始。

首次扫描将在模块更新后的 20 分钟内自动开始。

如果产品未与 ESET HOME 关联，激活过程可能会中断。请登录您的 ESET HOME 或创建一个帐户。

入门指南

本章提供对 ESET NOD32 Antivirus 及其基本设置的初步概述。

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 – 显示禁用检测引擎的确认对话框，这些防护通过控制文件、Web 和电子邮件通信来保护系统免受恶意系统攻击。通过**时间间隔**下拉菜单，可以指定将禁用防护的时长。

高级设置 – 打开 ESET NOD32 Antivirus 高级设置。要从主程序窗口打开“高级设置”，请按键盘上的 F5 键或依次单击**设置 > 高级设置**。

日志文件 – 日志文件包含已发生的重要程序事件的信息，并提供检测的概要信息。

打开 ESET NOD32 Antivirus – 打开 ESET NOD32 Antivirus 主程序窗口。

重置窗口布局 – 将 ESET NOD32 Antivirus 的窗口重置为其默认大小和屏幕位置。

颜色模式 – 打开用户界面设置，在其中可以更改 GUI 的颜色。

检查更新 – 启动模块或产品更新，以确保您受到保护。ESET NOD32 Antivirus 会每天自动检查更新数次。

关于 – 提供系统信息、有关已安装的 ESET NOD32 Antivirus 版本的详细信息、已安装的程序模块以及有关操作系统和系统资源的信息。

键盘快捷键

为了在 ESET NOD32 Antivirus 中更好地导航，可以使用以下键盘快捷键：

键盘快捷键	操作
F1	打开帮助页面
F5	打开“高级设置”
向上箭头/向下箭头	在下拉菜单项中导航
TAB	移动到窗口中的下一个 GUI 元素

键盘快捷键	操作
Shift+TAB	移动到窗口中的上一个 GUI 元素
ESC	关闭活动对话窗口
Ctrl+U	显示有关 ESET 订阅和计算机的信息（技术支持详细信息）
Ctrl+R	将产品窗口重置为其默认大小和屏幕位置
ALT + 左箭头键	向后导航
ALT + 右箭头键	向前导航
ALT+Home	返航

还可以使用鼠标按钮向后或向前导航。

配置文件

配置文件管理器用在 ESET NOD32 Antivirus 中的两个地方 – 在**手动扫描**部分和**更新**部分中。

计算机扫描

ESET NOD32 Antivirus 中有 4 个预定义的扫描配置文件：

- **智能扫描** – 这是默认的高级扫描配置文件。智能扫描配置文件使用智能优化技术，该技术会排除先前扫描中发现是干净且自该扫描以来未进行过修改的文件。这样可以缩短扫描时间，并且对系统安全性的影响最小。
- **右键菜单扫描** – 可以从右键菜单启动对任何文件的手动扫描。右键菜单扫描配置文件让您可以定义在采用此方法触发扫描时将使用的扫描配置。
- **深入扫描** – 默认情况下，全面扫描配置文件不使用智能优化，因此不会使用此配置文件排除扫描任何文件。
- **计算机扫描** – 这是标准计算机扫描中使用的默认配置文件。

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

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

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

更新

更新设置中的配置文件编辑器使您能够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。

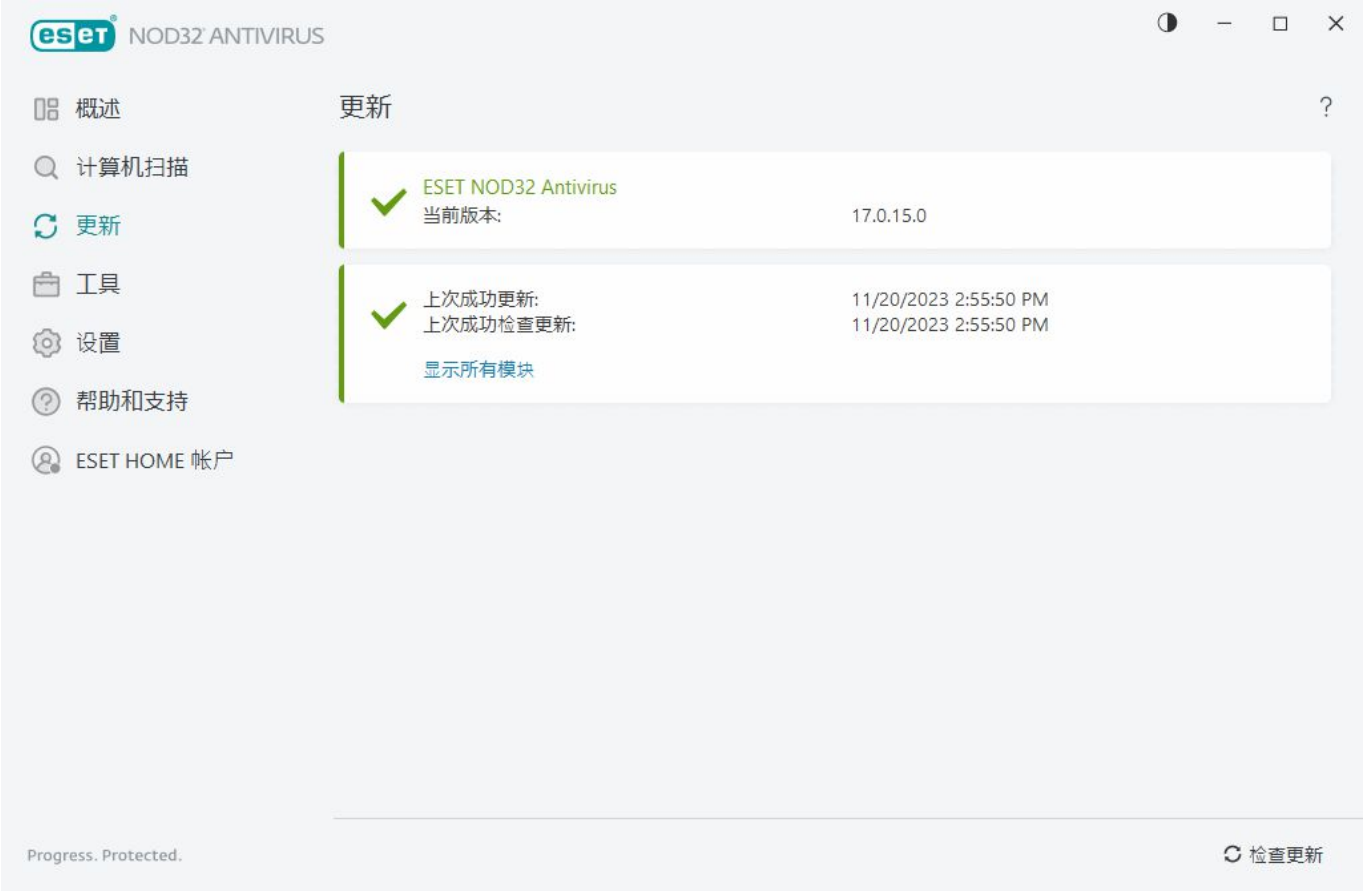
配置文件列表 – 新建或删除现有更新配置文件。

更新

定期更新 ESET NOD32 Antivirus 是确保计算机的最高安全级别的最佳方法。更新模块可确保程序模块和系统组件始终为最新。

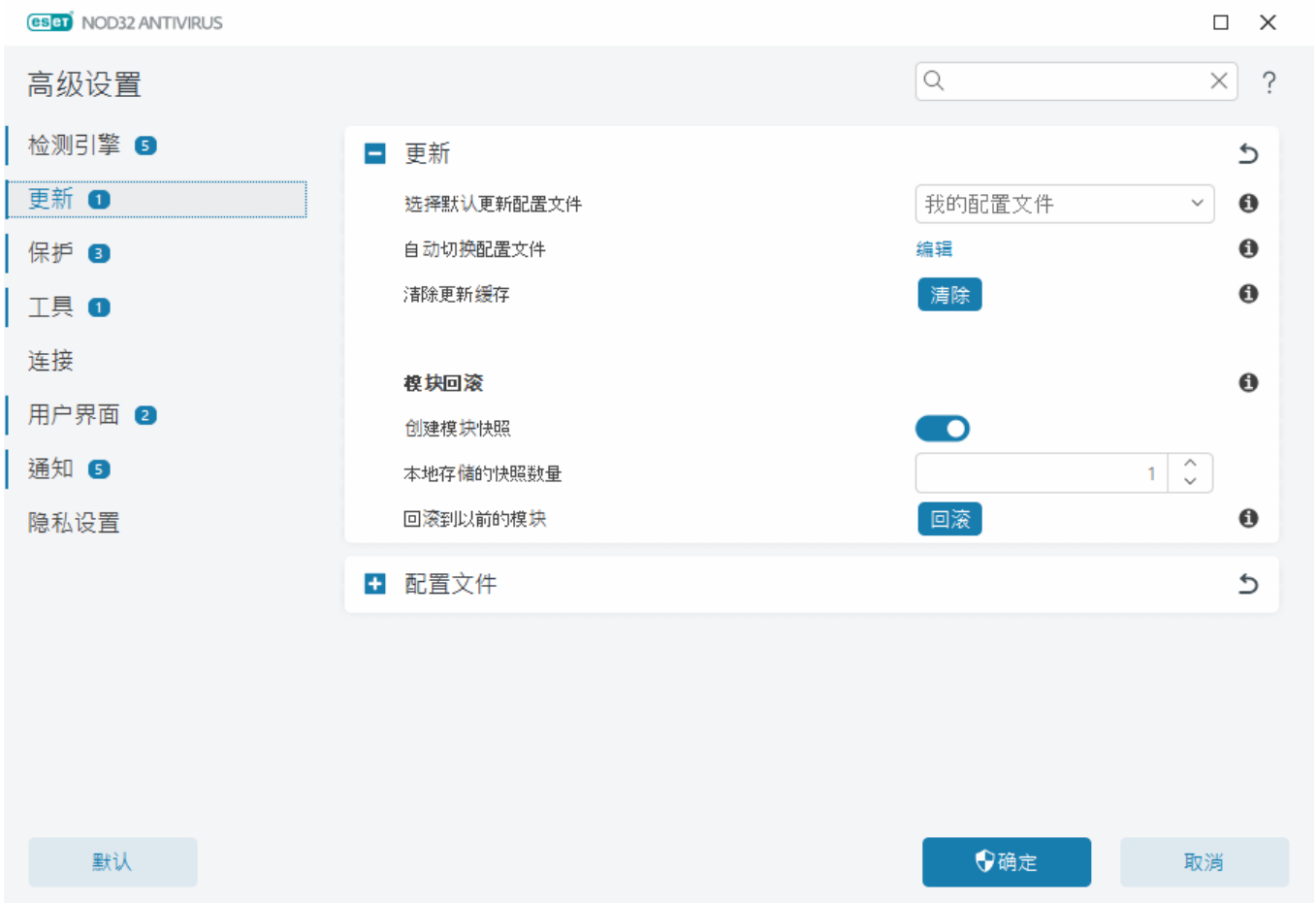
通过在主程序窗口中单击**更新**，可以查看当前更新状态，包括上一次成功更新的日期和时间以及是否需要更新。

除了自动更新之外，还可以单击**检查更新**来触发手动更新。



高级设置 > **更新**包含其他更新选项，如更新模式、代理服务器访问和 LAN 连接。

如果您遇到更新问题，请单击**清除**以清除临时更新缓存。如果仍无法更新程序模块，请参阅“模块更新失败”消息的故障排除部分。



产品激活

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/地区和分发方式（CD/DVD、ESET 网页等）而不同：

- 如果您购买了本产品的零售版或收到了内含订阅详细信息的电子邮件，则通过单击**使用购买的激活密钥**来激活产品。若要成功激活，必须输入提供的激活密钥。激活密钥 – 遵循 XXXX-XXXX-XXXX-XXXX-XXXX 或 XXXX-XXXXXXXX 格式的唯一字符串，用于标识订阅所有者和激活订阅。激活密钥通常位于产品包装的内部或背面。

- 在选择使用 ESET HOME 帐户后，将要求您登录到您的 ESET HOME 帐户。

- 如果您想在购买前先评估 ESET NOD32 Antivirus，则选择免费试用。输入电子邮件地址和国家/地区以在有限时间内激活 ESET NOD32 Antivirus。您的免费试用版将通过电子邮件发送给您。每个客户只能激活一次免费试用版。

- 如果您没有订阅并且想购买一个，请单击**购买订阅**。这会将您重定向到当地的 ESET 经销商网站。ESET Windows 家庭版产品订阅不是免费的。

您可以随时更改产品订阅。为此，请在主程序窗口中依次单击**帮助和支持 > 更改订阅**。您将看到 ESET 支持用来识别您的订阅的公共 ID。

⚠ 产品激活失败？

在激活过程中输入激活密钥

自动更新对您的安全很重要。ESET NOD32 Antivirus 将仅在激活后才接收更新。

当输入您的**激活密钥**时，请务必按照其写入形式准确键入它。您的激活密钥是采用 XXXX-XXXX-XXXX-XXXX-XXXX 格式的唯一字符串，用于标识订阅所有者和激活订阅。

我们建议您从您的注册电子邮件复制并粘贴激活密钥，以确保准确性。

如果您未在安装后输入您的激活密钥，将不会激活您的产品。可以在主程序窗口 > **帮助和支持** > **激活订阅**中激活 ESET NOD32 Antivirus。

ESET Windows 家庭版产品订阅不是免费的。

用户 ESET HOME 帐户

将设备连接到 ESET HOME，以查看和管理所有已激活的 ESET 订阅和设备。可以续订、升级或延期订阅，还可以查看重要的订阅详细信息。在 ESET HOME 管理门户或移动应用程序中，可以添加其他订阅、将产品下载到设备、检查产品的安全状态或通过电子邮件共享订阅。有关详细信息，请访问 ESET HOME 联机帮助。

在选择**使用 ESET HOME 帐户**作为激活方法之后，或在安装过程中连接到 ESET HOME 帐户时：

1. 登录到 ESET HOME 帐户。

> 如果您没有 ESET HOME 帐户，则单击**创建帐户**以注册或查看ESET HOME联机帮助中的说明。
> 如果您忘记了密码，则单击**我忘记了密码**，然后按照屏幕上的步骤进行操作，或查看ESET HOME联机帮助中的说明。

2. 为将在所有 ESET HOME 服务中使用的设备设置**设备名称**，然后单击**继续**。

3. 选择要激活的订阅或添加新订阅。单击**继续**以激活 ESET NOD32 Antivirus。

激活免费试用版

要激活 ESET NOD32 Antivirus 试用版，请在**电子邮件地址**和**确认电子邮件地址**字段中输入有效的电子邮件地址。激活后，将生成 ESET 订阅，并将其发送到您的电子邮件。此电子邮件地址还将用于产品到期通知和其他与 ESET 的通信。该免费试用版只能激活一次。

从**国家或地区**下拉菜单中选择国家或地区以向当地经销商注册 ESET NOD32 Antivirus。该经销商将为您提供技术支持。

免费 ESET 激活密钥

ESET NOD32 Antivirus 订阅不是免费的。

ESET 激活密钥是由 ESET 提供的、短划线分隔的、独一无二的字母数字序列，允许按照最终用户许可协议

合法使用 ESET NOD32 Antivirus每个最终用户仅在根据 ESET 授予的许可数量享有 ESET NOD32 Antivirus 使用权的情况下，方可使用激活密钥。激活密钥被视为机密，不能共享；但是，您可以使用 ESET HOME 共享订阅

Internet 上有一些来源可能会为您提供“免费”ESET 激活密钥，但请记住：

- 单击“免费 ESET 订阅”广告可能会危害您的计算机或设备，并可能导致感染恶意软件。恶意软件可能隐藏在非官方的 Web 内容（例如，视频）、显示广告以根据您的访问赚钱的网站等中。通常，这些都是陷阱。
- ESET 可以并且确实会禁用盗版订阅。
- 拥有盗版激活密钥违反最终用户许可协议，必须接受该协议才能安装 ESET NOD32 Antivirus
- 仅通过官方渠道购买 ESET 订阅，如 www.eset.comESET 分包商或分销商（请勿从非官方第三方网站购买订阅（如 eBay或从第三方购买共享订阅）。
- 下载 ESET NOD32 Antivirus 是免费的，但在安装期间激活需要有效的 ESET 激活密钥（可以下载并安装该产品，但在不激活的情况下，它不会工作）。
- 请勿在 Internet 或社交媒体上共享您的订阅（它可能会广泛传播）。

要识别和举报盗版 ESET 订阅，请访问我们的知识库文章以获取有关说明。

如果不确定是否要购买 ESET 安全产品，可以先使用试用版，然后再做决定：

1. 使用免费试用版激活 ESET NOD32 Antivirus
2. 参与 ESET Beta 计划
3. 安装 ESET Mobile Security（如果使用的是 Android 移动设备），它是免费增值的。

要获得折扣/延长许可证，请续订 ESET

激活失败 – 常见情况

如果激活 ESET NOD32 Antivirus 不成功，则最常见的情况包括：

- 激活密钥已在使用中
- 您输入的激活密钥无效。
- 激活表单中的信息丢失或无效。
- 无法与激活服务器通信。
- 未与 ESET 激活服务器连接或禁止与其连接

验证您输入的激活密钥是否正确且 Internet 连接是否处于活动状态。尝试再次激活 ESET NOD32 Antivirus如果使用 ESET HOME 帐户来激活，则参阅 ESET HOME 订阅和订阅管理 – 联机帮助

如果收到特定错误（例如，“订阅已暂停”或“订阅已过度使用”），请按照订阅状态中的说明操作。

如果仍然无法激活 ESET NOD32 Antivirus，则 ESET 激活故障排除程序将就激活和许可引导您浏览常见问题、错误和问题（仅以英语和其他几种语言提供）。

订阅状态

您的订阅可以具有不同的状态。您可以在 ESET HOME 中查找您的订阅状态。要将订阅添加到 ESET HOME 帐户，请参阅添加订阅。

如果您没有 ESET HOME 帐户，可以创建新的 ESET HOME 帐户。

如果订阅状态并非处于**活动**状态，则您会在激活时收到错误或在主程序窗口中收到通知。

要禁用订阅状态通知，请打开高级设置 > **通知** > **应用程序状态**。单击**应用程序状态**旁边的**编辑**、展开**许可**，然后取消选中要禁用的通知旁边的复选框。禁用通知并不能解决问题。

请参阅下表中针对不同订阅状态的说明和建议解决方案：

订阅状态	说明	解决方案
活动	订阅有效，无需您交互。ESET NOD32 Antivirus 可以激活，然后可以在主程序窗口 > **帮助和支持**中查找订阅详细信息。	
已过度使用	使用此订阅的设备超过了允许的数量。您会收到激活错误。	有关详细信息，请参阅由于订阅过度使用导致激活失败。
已挂起	由于付款出现问题，您的订阅已暂停。要使用订阅，请确保您在 ESET HOME 中的付款详细信息是最新的，或与订阅分销商联系。您可能会在激活期间或主程序窗口中收到此错误。	已安装的产品 – 如果您有 ESET HOME 帐户，则在主程序窗口中显示的通知中，单击**管理 ESET HOME 中的订阅**。然后查看付款详细信息。否则，请联系您的订阅分销商。 激活错误 – 如果您有 ESET HOME 帐户，则在激活错误窗口中，单击**打开 ESET HOME**，然后查看付款详细信息。否则，请联系您的订阅分销商。
已到期	您的订阅已到期，无法使用此订阅来激活 ESET NOD32 Antivirus。您可能会在激活期间或主程序窗口中收到此错误。如果已安装 ESET NOD32 Antivirus，则您的计算机不受保护且不会更新。	已安装的产品 – 在主程序窗口中显示的通知中，单击**续订订阅**，然后按照如何续订订阅？中的说明操作，或者单击**激活产品**，然后选择激活方法。 激活错误 – 在激活错误窗口中，单击**续订订阅**，然后按照如何续订订阅？中的说明操作，或者键入新的或续订的激活密钥，然后单击**续订订阅**。
已取消	ESET 或您的订阅分销商已取消您的订阅。	如果您收到错误：订阅已取消（在主程序窗口中或在激活期间收到），而您的订阅正常工作，请联系您的订阅分销商。

由于订阅过度使用导致激活失败

问题

- 您的订阅可能被过度使用或滥用
- 由于订阅过度使用导致激活失败

解决方案

使用此订阅的设备超过了此订阅所允许的数量。您可能是软件盗版或假冒的受害者。此订阅无法用于激活任何其他 ESET 产品。如果允许您在 ESET HOME 帐户中管理订阅或者从合法来源购买了订阅，可以直接解决此问题。如果您还没有帐户，请创建一个。

如果您是订阅所有者而且没有提示您输入电子邮件地址：

1. 要管理 ESET 订阅，请打开 Web 浏览器并导航到 https://home.eset.com。访问 ESET License Manager 然后删除或停用席位。有关详细信息，请参阅订阅过度使用时该怎么办

2. 要识别和举报盗版 ESET 订阅，请访问我们的“识别和举报盗版 ESET 订阅”文章以获取有关说明。

3. 如果不确定，请单击“**后退**”并发送电子邮件至 ESET 技术支持

如果您不是订阅所有者，请联系此订阅的所有者，并提供因订阅过度使用而无法激活 ESET 产品的信息。该所有者可以在 ESET HOME 门户中解决该问题。

如果提示您确认电子邮件地址（仅几种情况），请输入最初用于购买或激活 ESET NOD32 Antivirus 的电子邮件地址。

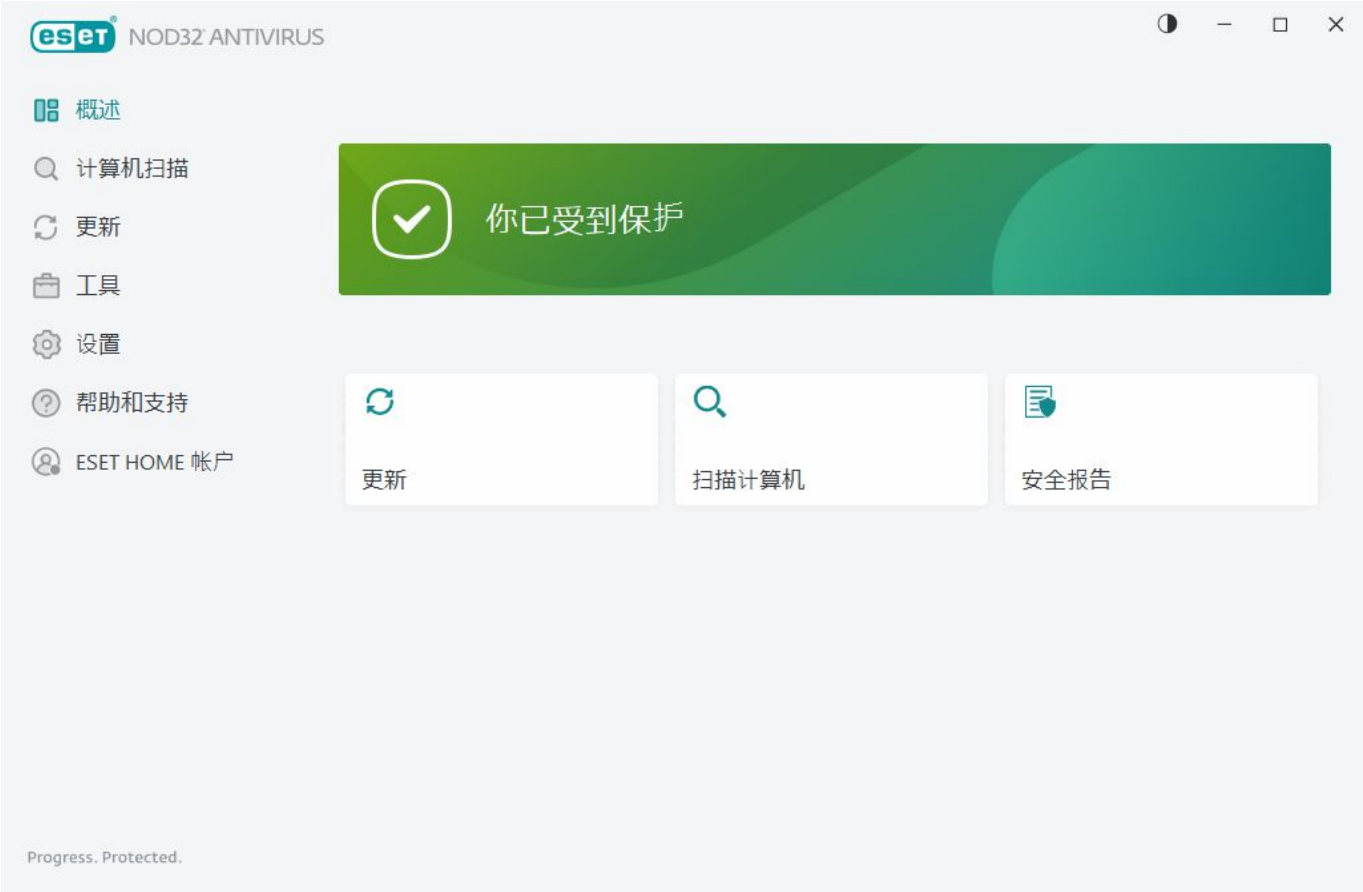
使用 ESET NOD32 Antivirus

ESET NOD32 Antivirus 主程序窗口会分为两个部分。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。

> **图文并茂说明**
> 请参阅打开 ESET Windows 产品的主程序窗口，获取以英语和其他几种语言提供的图文并茂说明。

可以在主程序窗口的右上角，选择 ESET NOD32 Antivirus GUI 的颜色方案。单击**最小化**图标旁边的**颜色方案**图标（该图标会根据当前选定的颜色方案发生变化），然后从下拉菜单中选择颜色方案：

- **与系统颜色相同** – 根据操作系统设置来设置 ESET NOD32 Antivirus 的颜色方案。
- **深色** - ESET NOD32 Antivirus 将应用深色方案（深色模式）。
- **浅色** - ESET NOD32 Antivirus 将应用标准的浅色方案。



主菜单选项：

概述 – 提供有关 ESET NOD32 Antivirus 的防护状态的信息。

计算机扫描 – 配置并启动对计算机的扫描或创建自定义扫描。

更新 – 显示有关模块和检测引擎更新的信息。

工具 – 提供对功能的访问，这些功能有助于简化程序管理并为高级用户提供其他选项。

设置 – 提供 ESET NOD32 Antivirus 防护功能（计算机防护和 Internet 防护）的配置选项和对高级设置的访问。

帮助和支持 – 显示有关订阅的信息、已安装的 ESET 产品以及指向联机帮助、ESET 知识库和技术支持的链接。

ESET HOME 帐户 - 将设备连接到 ESET HOME 或查看 ESET HOME 帐户连接状态。使用 ESET HOME 来查看和管理您的激活的 ESET 订阅和设备。

概览

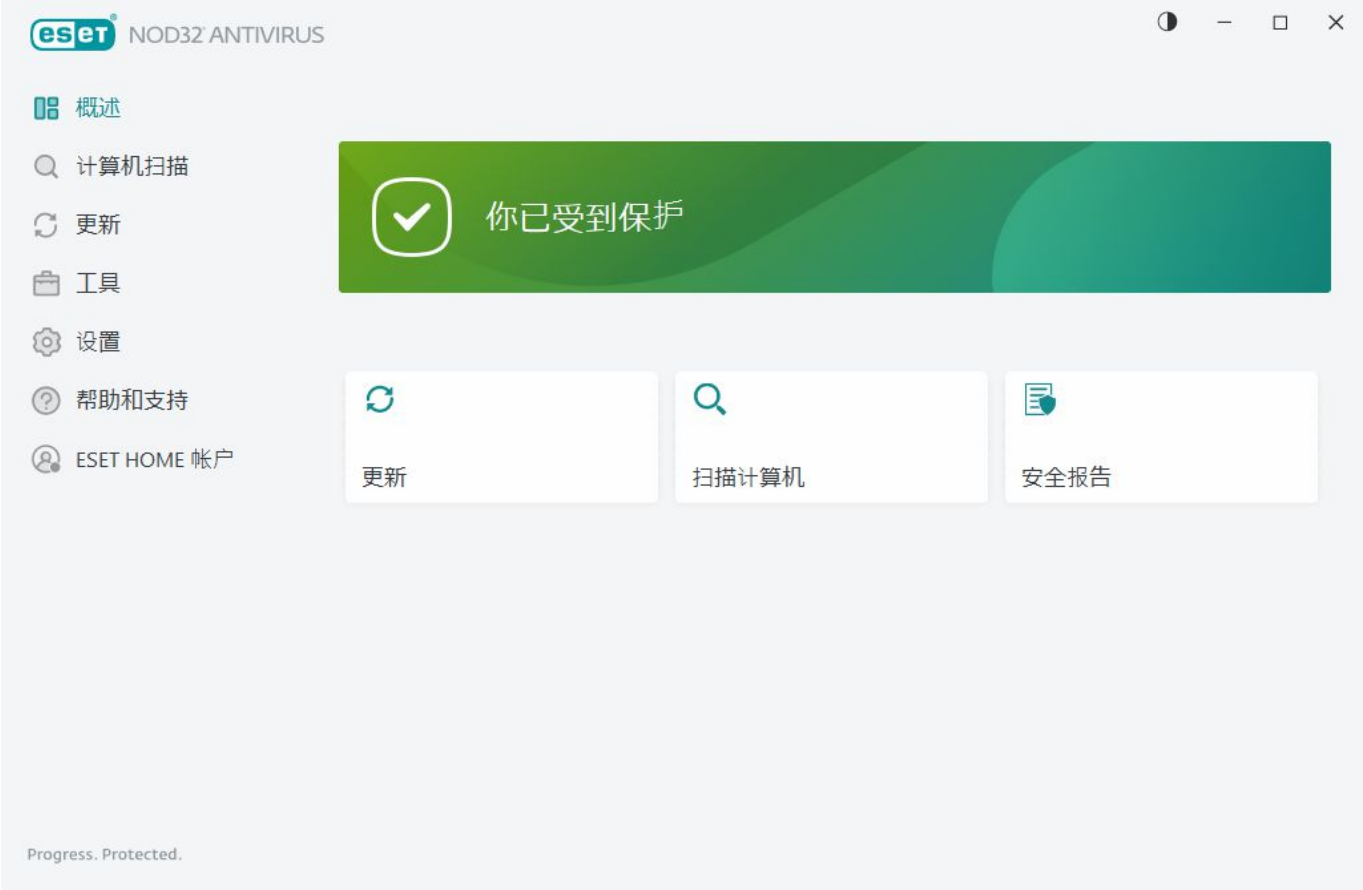
概述窗口显示有关计算机当前防护的信息，以及指向 ESET NOD32 Antivirus 中安全功能的快速链接。

概述窗口显示通知，其中包含的详细信息和建议解决方案可用于提高 ESET NOD32 Antivirus 的安全性、打开其他功能或确保提供最大程度的防护。如果有更多通知，则单击 **x 更多通知**以全部展开。

更新 – 打开更新页面，并检查更新。

扫描计算机 – 打开计算机扫描页面，并开始标准计算机扫描。

安全报告 – 打开安全报告



绿色图标和绿色**您已受保护**状态表示已确保最高防护。

程序工作不正常时如何应对

如果主动防护模块正常工作，其防护状态图标将为绿色。红色惊叹号或橙色通知图标表明无法确保提供最大程度的防护。有关每个模块防护状态的其他信息以及如何恢复完全防护的建议解决方案会在**概述**窗口中以通知形式显示。若要更改各个模块的状态，请单击**设置**并选择所需模块。

红色图标和红色**安全警报**状态表示出现严重问题。有几种原因可能显示此状态，例如：

- **产品未激活**或**订阅已过期** – 此问题由红色防护状态图标表示。订阅过期后该程序将无法更新。按照警报窗口中的说明续订订阅。
- **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。
- **文件系统实时防护已禁用** – 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**启用文件系统实时防护**重新启用该功能。
- **已禁用病毒和间谍软件防护** – 单击**启用病毒和间谍软件防护**，可以重新启用病毒和间谍软件防护。

橙色图标表示防护受到限制。例如，程序更新有问题或者订阅将要过期。有几种原因可能显示此状态，例如：

- **游戏模式处于活动状态** – 启用游戏模式将存在潜在安全风险。启用此功能会禁用所有通知/警报窗口，并停止所有计划任务。
- **您的订阅即将到期/您的订阅今天到期** – 这由在系统时钟的旁边显示感叹号的防护状态图标来指示。订阅过期后，程序将无法更新，防护状态图标将变为红色。

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

计算机扫描

手动扫描程序是病毒防护解决方案的一个重要组成部分。它可以扫描计算机上的文件和文件夹。从安全角度说，计算机扫描应作为日常安全手段的一部分定期执行，而不应仅在怀疑有渗透时执行，这一点非常重要。我们建议您定期执行系统的全面扫描以检测病毒，这些病毒在写入到磁盘时无法由文件系统实时防护捕获。如果文件系统实时防护此时处于禁用状态、检测引擎未更新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**和**扫描计算机**可快速扫描系统，而无需指定扫描参数。**自定义扫描**（在“高级扫描”下）让您可以从为特定目标位置设计的预定义扫描配置文件中进行选择，以及选择特定扫描目标。

请参见扫描进度以了解有关扫描进程的更多信息。

默认情况下，ESET NOD32 Antivirus 会尝试自动清除或删除在计算机扫描期间发现的检测。在某些情况下，如果无法执行任何操作，您会收到一条交互警报并且必须选择一个清除操作（例如，删除或忽略）。要更改清除级别并获取更多详细信息，请参阅清除。要查看以前的扫描，请参阅日志文件。

扫描计算机

扫描计算机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。**扫描计算机**的优势是便于操作，而无需详细的扫描配置。此扫描会检查本地驱动器上的所有文件并自动清除或删除检测到的渗透。清除级别被自动设置为默认值。有关清除类型的更详细信息，请参阅清除。

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。

以下扫描选项在**高级扫描**下提供：

自定义扫描

自定义扫描允许您指定扫描参数，如扫描目标和扫描方法等。**自定义扫描**的优点是可以详细配置参数。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。

可移动磁盘扫描

与**扫描计算机**类似 – 快速启动对当前连接到计算机的可移动磁盘（例如CD/DVD/USB）的扫描。这在将 USB 闪存驱动器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**、从**扫描目标**下拉菜单中选择**可移动磁盘**，然后单击**扫描**。

重复上次扫描

允许您使用运行时的相同设置快速启动之前执行的扫描。

扫描后的操作下拉菜单让您可以设置扫描完成后要自动执行的操作：

- **无操作** – 扫描完成后，不执行任何操作。
- **关机** – 扫描完成后关闭计算机。
- **需要时重新启动** – 仅当需要完成清除检测到的威胁时，计算机才会重新启动。
- **重新启动** – 扫描完成后，关闭所有打开的程序并重新启动计算机。
- **需要时强制重新启动** – 仅当需要完成清除检测到的威胁时，计算机才会强制重新启动。
- **强制重新启动** – 扫描完成后，强制关闭所有打开的程序而不等待用户交互，然后重新启动计算机。
- **睡眠** – 保存会话并使计算机处于低能耗状态，以便用户快速恢复工作。
- **休眠** – 获取在 RAM 上运行的所有内容并将其移动到硬盘上的特定文件。您的计算机将关闭，但在下次启动时将恢复到之前的状态。

> 根据您计算机的电源和使操作系统进入睡眠状态设置或计算机/笔记本电脑功能，可以使用**睡眠**或**休眠**操作。请记住，睡眠中的计算机仍是一台正在运行的计算机。当计算机依赖电池供电时，它仍在运行基本功能且仍在耗电。若要在办公室外移动办公时延长电池使用时间，建议您使用“休眠”选项。

选定操作将在所有正在运行的扫描完成后开始。当选择**关机**或**重新启动**时，将显示一个 30 秒倒计时的确认对话窗口（单击**取消**可停用请求的操作）。

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

自定义扫描启动程序

可以使用“自定义扫描”来扫描系统内存、网络或磁盘的特定部分（而不是整个磁盘）。要执行此操作，请依次单击**高级扫描 > 自定义扫描**，然后从文件夹（树）结构中选择特定目标。

可以从**配置文件**下拉菜单中选择要在扫描特定目标时使用的配置文件。默认的配置文件为**智能扫描**。另外有三个预定义的扫描配置文件：名为**全面扫描**、**右键菜单扫描**和**计算机扫描**。这些扫描配置文件使用不同的 ThreatSense 参数。可用选项在高级设置 > **检测引擎** > **恶意软件扫描** > **手动扫描** > ThreatSense 中进行了介绍。

文件夹（树）结构还包含特定扫描目标。

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

要快速导航到扫描目标（文件或文件夹），请在树形结构下方的文本字段中键入其路径。该路径区分大小写。要将目标包括在扫描中，请在树形结构中选中其复选框。

> **如何计划每周计算机扫描**
> 要计划定期任务，请参阅如何计划每周计算机扫描

可以在高级设置 > **检测引擎** > **恶意软件扫描** > **手动扫描** > **ThreatSense** > **清除**中，配置扫描的清除参数。要运行扫描但不进行清除操作，请单击**高级设置**，然后选择**扫描但不清除**。扫描历史记录将保存到扫描日志。

当选中**忽略排除**时，带有之前已排除扩展名的文件也将进行扫描，没有任何例外。

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您要扫描的文件，则使用此选项。如果当前用户无法以管理员身份调用 UAC 操作，则此按钮不可用。

通过单击显示日志，您可以在扫描完成时查看计算机扫描日志。

扫描进度

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

某些文件（比如受密码保护的文件或仅由系统使用的文件（通常为 *pagefile.sys* 和某些日志文件））无法扫描很正常。可以在我们的知识库文章中找到更多详细信息。

如何计划每周计算机扫描
要计划定期任务，请参阅如何计划每周计算机扫描

扫描进度 – 进度条显示正在运行的扫描的状态。

目标 – 当前扫描的对象的名称及其位置。

检测发生 – 显示在扫描期间扫描的文件、发现的威胁和清除的威胁的总数。

单击“更多信息”以显示以下信息：

- **用户** – 已启动扫描的用户帐户的名称。
- **扫描的对象** – 已扫描对象的数量。
- **持续时间** – 已用时间。

暂停图标 – 暂停扫描。

继续图标 – 当扫描进度暂停时显示此选项。单击该图标可继续扫描。

停止图标 – 终止扫描。

单击**打开扫描窗口**以打开计算机扫描日志，其中包含有关扫描的更多详细信息。

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。

单击放大镜或箭头以显示有关当前正在运行的扫描的详细信息。可以通过单击**扫描计算机**或依次单击**高级扫描 > 自定义扫描**，来运行另一个并行扫描。

扫描后的操作下拉菜单让您可以设置扫描完成后要自动执行的操作：

- **无操作** – 扫描完成后，不执行任何操作。
- **关机** – 扫描完成后关闭计算机。
- **需要时重新启动** – 仅当需要完成清除检测到的威胁时，计算机才会重新启动。
- **重新启动** – 扫描完成后，关闭所有打开的程序并重新启动计算机。
- **需要时强制重新启动** – 仅当需要完成清除检测到的威胁时，计算机才会强制重新启动。
- **强制重新启动** – 扫描完成后，强制关闭所有打开的程序而不等待用户交互，然后重新启动计算机。
- **睡眠** – 保存会话并使计算机处于低能耗状态，以便用户快速恢复工作。
- **休眠** – 获取在 RAM 上运行的所有内容并将其移动到硬盘上的特定文件。您的计算机将关闭，但在下次启动时将恢复到之前的状态。

根据您计算机的电源和使操作系统进入睡眠状态设置或计算机/笔记本电脑功能，可以使用**睡眠**或**休眠**操作。请记住，睡眠中的计算机仍是一台正在运行的计算机。当计算机依赖电池供电时，它仍在运行基本功能且仍在耗电。若要在办公室外移动办公时延长电池使用时间，建议您使用“休眠”选项。

选定操作将在所有正在运行的扫描完成后开始。当选择**关机**或**重新启动**时，将显示一个 30 秒倒计时的确认对话窗口（单击**取消**可停用请求的操作）。

计算机扫描日志

可以在日志文件中，查看与特定扫描相关的详细信息。扫描日志包含以下信息：

- 检测引擎的版本
- 开始日期和时间
- 已扫描的磁盘、文件夹和文件列表
- 计划扫描名称（仅限计划扫描）
- 已启动扫描的用户。
- 扫描状态
- 已扫描的对象数
- 已找到的检测数
- 完成时间
- 总扫描时间

> 如果先前执行的同一个计划任务仍在运行，则会跳过计划计算机扫描任务的新开始。跳过的计划扫描任务将创建已扫描对象为 0 的计算机扫描日志，并且状态为**扫描因上一个扫描仍在运行而未启动**。

要查找以前的扫描日志，请在主程序窗口中选择**工具 > 日志文件**。在下拉菜单中，选择**计算机扫描**并双击所需的记录。

若要了解有关“无法打开”、“打开错误”和/或“压缩文件已损坏”记录的详细信息，请参阅我们的 ESET 知识库文章

单击滑块图标 **过滤**以打开日志过滤窗口，在其中可以通过定义自定义条件来缩小搜索范围。要查看上下文菜单，请右键单击特定的日志条目：

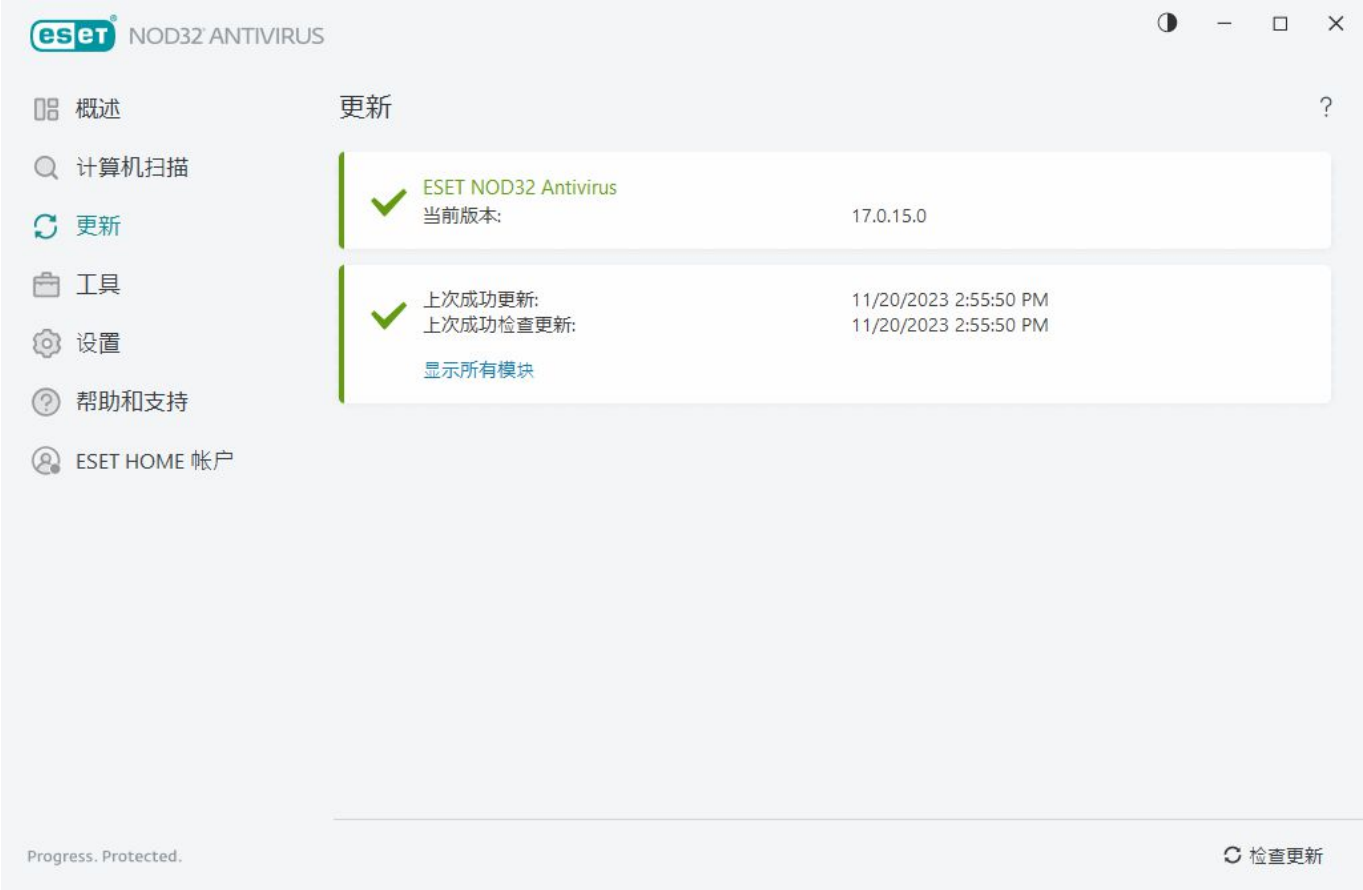
操作	使用情况
过滤相同记录	激活日志过滤。日志将仅显示与选定记录相同类型的记录。
过滤	此选项将打开日志过滤窗口，并允许您为特定日志条目定义标准。快捷方式：Ctrl+Shift+F
启用过滤器	激活过滤器设置。如果首次激活过滤器，则必须定义设置，并打开日志过滤窗口。
禁用过滤器	关闭过滤器（与单击底部的开关相同）。
复制	将突出显示的记录复制到剪切板。快捷方式：Ctrl+C
全部复制	复制窗口中的所有记录。
导出	将突出显示的记录导出到剪切板以导出为 XML 文件。
全部导出	此选项将窗口中的所有记录导出为 XML 文件。
检测说明	将打开 ESET 威胁百科全书，其中包含有关已亮显渗透的危险和症状的详细信息。

更新

定期更新 ESET NOD32 Antivirus 是确保计算机的最高安全级别的最佳方法。更新模块可确保程序模块和系统组件始终为最新。

通过在主程序窗口中单击**更新**，可以查看当前更新状态，包括上一次成功更新的日期和时间以及是否需要更新。

除了自动更新之外，还可以单击**检查更新**来触发手动更新。定期更新程序模块和组件是全面防范恶意代码的重要组成部分。请注意产品模块配置和操作。必须使用激活密钥激活产品，才可接收到更新。如果在安装期间未执行此操作，则需要激活 ESET NOD32 Antivirus，才能访问 ESET 更新服务器。在购买 ESET NOD32 Antivirus 后，ESET 已通过电子邮件向您发送激活密钥。



当前版本 – 显示您安装的当前产品版本的版本号。

上次成功更新 – 显示最近一次成功更新的日期。如果未看到最近的日期，则您的产品模块可能不是最新的。

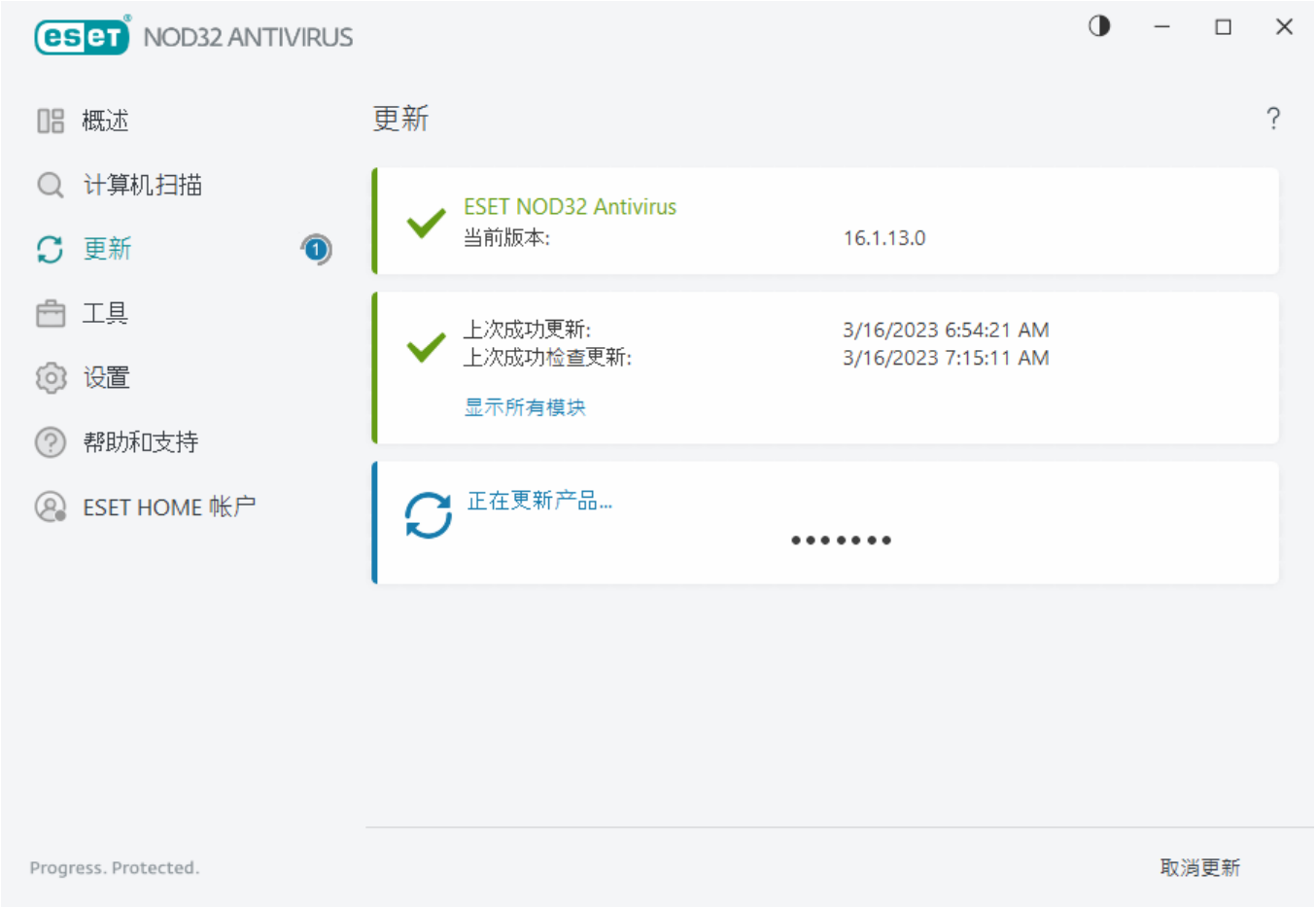
上次成功检查更新 – 显示上次成功检查更新的日期。

显示所有模块 – 显示已安装程序模块的列表。

单击**检查更新**以检查 ESET NOD32 Antivirus 的最新可用版本。

更新过程

单击**检查更新**后，即开始下载。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**。



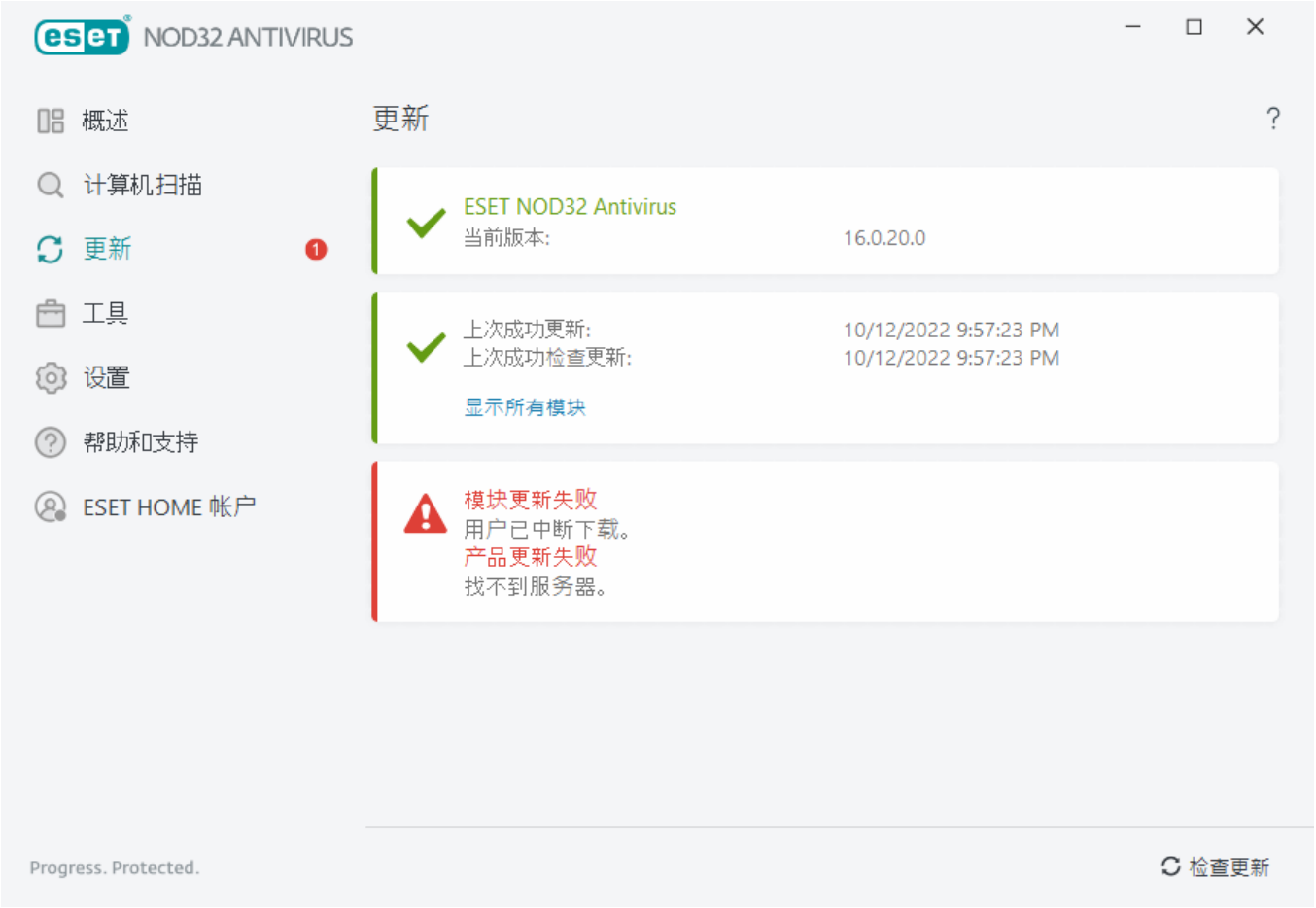
一般情况下，将在**更新**窗口中看到表示程序处于最新状态的绿色对号标记。如果未看到绿色对勾标记，则表示程序已过时且易受感染。请尽快更新程序模块。

更新失败

如果收到模块更新失败的消息，可能的原因如下所示：

1. **订阅无效** – 用于激活的订阅无效或已到期。在主程序窗口中，依次单击**帮助和支持 > 更改订阅**，然后激活产品。

2. **下载更新文件时出错** – 此错误可能由不正确的 Internet 连接设置导致。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。



必须在 ESET NOD32 Antivirus 成功更新到较新产品版本后重新启动计算机，以确保所有程序模块已正确更新。无需在常规模块更新后重新启动计算机。

有关详细信息，请访问“模块更新失败”消息的疑难解答

对话窗口 – 需要重新启动

将 ESET NOD32 Antivirus 更新为新版本后，需要重新启动计算机。发布新版本的 ESET NOD32 Antivirus 是为了实施改进或修复程序模块的自动更新无法解决的问题。

新版本的 ESET NOD32 Antivirus 可以根据程序更新设置自动安装，也可以基于较旧版本通过下载并安装新版本来手动安装。

单击**立即重新启动**以重新启动计算机。如果您打算稍后重新启动计算机，请单击**稍后提醒我**。稍后，可以从主程序窗口的**概述**部分手动重新启动计算机。

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，以下更新任务在 ESET NOD32 Antivirus 中处于激活状态：

- **定期自动更新**

- **用户登录后自动更新**

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

工具

工具菜单会包括提供其他安全性和帮助的功能，可用于简化 ESET NOD32 Antivirus 管理。以下工具可用：

 日志文件

 运行进程（如果 ESET LiveGrid® 已在 ESET NOD32 Antivirus 中启用）

 安全报告

 ESET SysInspector

 计划任务

 系统清理器

 提交样本以供分析（可能不可用，具体取决于 ESET LiveGrid® 配置）。

 隔离区

日志文件

日志文件包含关于已发生的重要程序事件的信息，并提供检测到的威胁的概述。日志记录是系统分析、威胁检测以及故障排除的重要部分。日志记录在后台主动执行，无需用户交互。对信息的记录是根据当前日志级别设置进行的。可以直接从 ESET NOD32 Antivirus 环境中查看文本消息和日志，还可以压缩日志。

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

- **检测** – 此日志提供有关由 ESET NOD32 Antivirus 检测到的检测和渗透的详细信息。日志信息包括检测时间、扫描程序类型、对象类型、对象位置、检测名称、执行的操作、检测到渗透时登录用户的名称、哈希以及首次发生的时间。未清除的渗透始终以浅红色背景的红色文字进行标记。已清除的渗透以白色背景的黄色文字进行标记。未清除的 PUA 或潜在不安全的应用程序以白色背景的黄色文字进行标记。

- **事件** - ESET NOD32 Antivirus 执行的所有重要操作都记录在事件日志中。事件日志包含有关程序中发生的事件和错误的信息。它为系统管理员和用户解决问题而设计。通常这里找到的信息可以帮助您找到程序中所发生问题的解决方案。

- **计算机扫描** – 所有以前的扫描结果都显示在此窗口中。每一行对应一个计算机控件。双击任意条目可查看选定扫描的详细信息。

- **HIPS** – 包含特定 HIPS 规则的记录，这些规则被标记为用于进行记录。该协议显示触发操作的应用程序、结果（规则被允许还是被禁止）和规则名称。

- **过滤的网站** – 如果要查看由 Web 访问保护阻止的网站列表，则此列表很有用。 每个日志都包含时间、URL 地址、用户和创建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。只有具有相应设备控制规则的设备将记录到日志文件。如果规则不匹配连接的设备，则不会创建所连接设备的日志条目。您还可以查看设备类型、序列号、供应商名称和磁盘大小（如果可用）等详细信息。

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

单击 **过滤**可打开日志过滤窗口，您可以在该窗口中定义过滤条件。

右键单击指定的记录来打开右键菜单。右键菜单中提供以下选项：

- **显示** – 在新窗口中显示有关选中日志的更多详细信息。
- **过滤相同记录** – 激活此过滤器后，您将仅看到相同类型的记录（诊断、警告...）。
- **过滤** – 在单击此选项后，日志过滤窗口将允许您为特定日志条目定义过滤条件。
- **启用过滤器** – 激活过滤器设置。
- **禁用过滤器** – 清除所有过滤器设置（如上文所述）。
- **复制/全部复制** – 复制有关窗口中选定记录的信息。
- **复制单元格** – 复制右键单击的单元格的内容。
- **删除/全部删除** – 删除选定记录或所有显示的记录。此操作需要管理员权限。
- **导出/全部导出** – 导出有关选定记录或格式为 XML 的所有记录的信息。
- **查找/查找下一个/查找上一个** – 在单击此选项后，可以使用日志过滤窗口来定义过滤条件，以亮显特定条目。
- **检测说明** – 将打开 ESET 威胁百科全书，其中包含有关已记录渗透的危险和症状的详细信息。
- **创建排除** – 使用向导创建新的检测排除（不适用于恶意软件检测）。
- **添加到浏览器防护允许列表** – 打开浏览器防护允许列表窗口并将项目添加到列表中。

日志过滤

单击 **过滤**（在**工具 > 日志文件**）可定义过滤条件。

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

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

查找下一个

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

在列中搜索

选择搜索时要考虑使用的列。可以选中一个或多个要用于搜索的列。

记录类型

从下拉菜单中选择一个或多个日志记录类型：

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

时段

定义想要显示其结果的时段。

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

全字匹配

如果要搜索全字以得到更精确的结果，则使用此复选框。

区分大小写

如果在过滤时使用大写字母或小写字母对您而言很重要，则启用此选项。完成配置过滤/搜索选项后，单击**确定**以显示过滤的日志记录，或单击**“查找”**以开始搜索。从当前位置（亮显的记录）开始，按从上到下的顺序搜索日志文件。搜索会在找到第一条相应记录时停止。按 **F3** 可搜索下一条记录，或单击右键并选择**查找**以优化搜索选项。

正在运行的进程

运行进程显示计算机上运行的程序或进程，并保持 ESET 立刻持续获知新入侵ESET NOD32 Antivirus 提供有关运行的进程的详细信息，使用 ESET LiveGrid® 技术保护用户。

信誉 – 在大多数情况下，ESET NOD32 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，从而将风险级别指定给对象（文件、进程、注册表项等）。基于这些启发式扫描，会向对象指定风险级别，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。若要打开任务管理器，右键单击任务栏中的空白区域，然后单击**任务管理器**，或者按键盘上的 **Ctrl+Shift+Esc**。

标记为良好（绿色）的已知应用程序肯定干净（在白名单中列出），将不进行扫描以提高性能。

PID – 进程标识符编号可用作各种函数调用中的参数，如调整进程的优先级。

用户数 – 使用给定应用程序的用户数量。此信息由 ESET LiveGrid® 技术收集。

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

标记为未知（橙色）的应用程序不一定是恶意软件。通常它是一个较新的应用程序。如果您对文件不确定，可以通过提交文件以供分析，将文件提交到 ESET 研究实验室。如果文件被证实是一个恶意应用程序，则以后的更新中将增加它的检测。

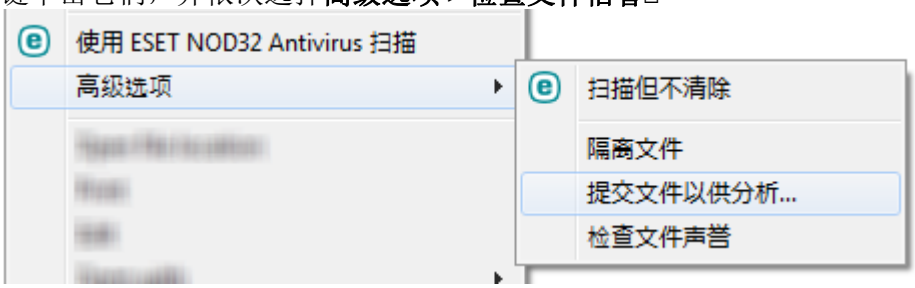
应用程序名称 – 程序或进程的给定名称。

单击某个应用程序可显示该应用程序的以下详细信息：

- **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/修改时间** – 创建（修改）的日期和时间。

还可以检查不充当正在运行的程序/进程的文件的信誉。若要执行此操作，请在文件资源管理器中右键单击它们，并依次选择**高级选项 > 检查文件信誉**。



安全报告

此功能可提供以下类别统计信息的概述：

- **已阻止的网页** – 显示已阻止网页的数量（PUA 的黑名单 URL、网络钓鱼、受攻击的路由器、IP 或证书）。
- **已检测到的被感染电子邮件对象** – 显示已检测到的被感染电子邮件对象的数量。
- **已检测到的 PUA** – 显示潜在不受欢迎的应用程序 (PUA) 的数量。
- **已扫描的文档** – 显示已扫描的文档对象的数量。
- **已扫描的应用程序** – 显示已扫描的可执行文件对象的数量。
- **已扫描的其他对象** – 显示其他已扫描的对象的数量。
- **已扫描的网页对象** – 显示已扫描的网页对象的数量。
- **已扫描的电子邮件对象** – 显示已扫描的电子邮件对象的数量。

这些类别的顺序取决于从最高到最低的数值。不会显示值为零的类别。单击**显示更多**可展开并显示隐藏的类别。

在功能启用后，不会再在安全报告中显示为不起作用。

单击右上角的齿轮⚙，即可**启用/禁用安全报告通知**，或者选择是否显示最后 30 天的数据（自产品激活以后）。如果 ESET NOD32 Antivirus 安装的天数不足 30 天，那么仅可选择完成安装之后算起的天数。默认情况下，设置的时间段为 30 天。

重置数据会清除所有统计信息，并删除安全报告的现有数据。除非在**高级设置** > 通知 > **交互警报** > **确认消息** > **编辑**中取消选中**重置统计前先询问**选项，否则需要确认此操作。

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。要了解如何使用 ESET SysInspector请参阅 ESET SysInspector 联机帮助

ESET SysInspector 窗口显示有关日志的以下信息：

- **时间** – 日志创建时间。
- **注释** – 简短注释。
- **用户** – 创建日志的用户的姓名。
- **状态** – 日志创建的状态。

可用操作包括：

- **显示** – 在 ESET SysInspector 中打开选定日志。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**
- **创建** – 创建新日志。请在生成 ESET SysInspector**已创建**状态）之前稍作等待，然后再尝试访问日志。日志保存在 C:\ProgramData\ESET\ESET Security\SysInspector 中。

- **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）。
- **创建** – 创建新日志。请在生成 ESET SysInspector 已**创建**状态）之前稍作等待，然后再尝试访问日志。
- **删除** – 删除列表中选定的日志。
- **全部删除** – 删除所有日志。
- **导出** – 将日志导出为 .xml 文件或压缩的 .xml

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。

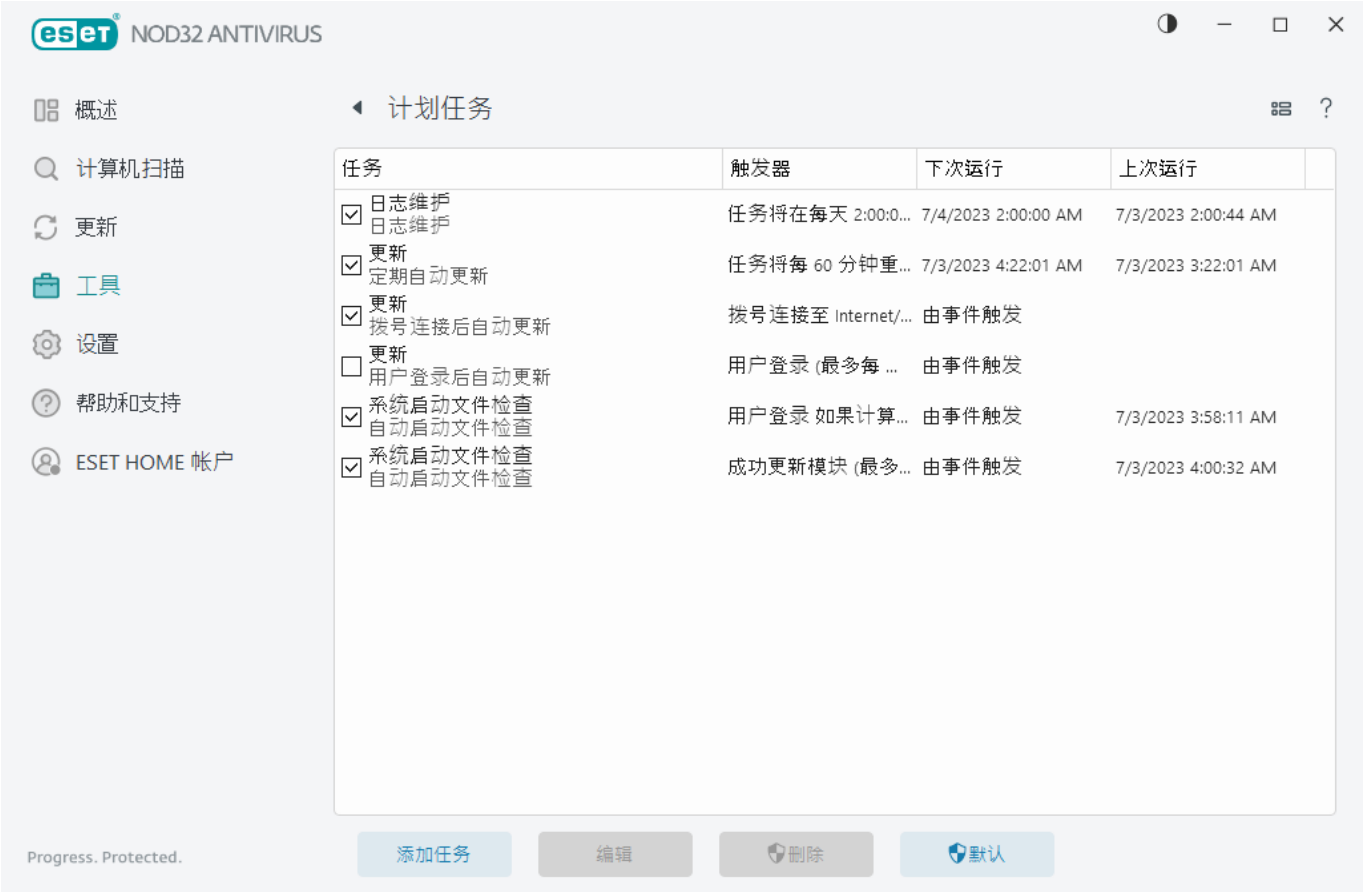
可从 ESET NOD32 Antivirus 主程序窗口中访问计划任务，方法是依次单击**工具 > 计划任务**。**计划任务**包含所有计划任务和配置属性（如预定义的日期、时间和使用的扫描配置文件）的列表。

任务计划用于计划以下任务： 更新模块、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**）。可以通过单击**默认**将计划任务的列表恢复为默认并删除所有更改。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**
- **用户登录后自动更新**
- **自动启动文件检查**（用户登录后）
- **自动启动文件检查**（成功更新检测引擎后）

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**。



添加新任务

1. 单击窗口底部的**添加任务**。

2. 输入任务的名称。

3. 从下拉菜单中选择所需任务：

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

4. 启用**已启用**旁边的开关以激活该任务（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）、单击**下一步**，然后选择以下计时选项之一：

- **一次** – 任务将在预定义的日期和时间执行。
- **重复** – 任务将以指定的时间间隔执行。

- **每天** – 任务将在每天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**
- **如果自上次运行之后经过的时间超过(小时)，则立即运行** – 表示自任务首次跳过运行之后经过的时间。如果超过此时间，将立即运行该任务。在下面使用微调器设置时间。

要查看计划任务，请右键单击任务，然后单击**显示任务详细信息**。

计划扫描选项

在此窗口中，可以为计划的计算机扫描任务指定高级选项。

要运行扫描但不进行清除操作，请单击**高级设置**，然后选择**扫描但不清除**。扫描历史记录将保存到扫描日志。

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。

扫描后的操作下拉菜单让您可以设置扫描完成后要自动执行的操作：

- **无操作** – 扫描完成后，不执行任何操作。
- **关机** – 扫描完成后关闭计算机。
- **需要时重新启动** – 仅当需要完成清除检测到的威胁时，计算机才会重新启动。
- **重新启动** – 扫描完成后，关闭所有打开的程序并重新启动计算机。
- **需要时强制重新启动** – 仅当需要完成清除检测到的威胁时，计算机才会强制重新启动。
- **强制重新启动** – 扫描完成后，强制关闭所有打开的程序而不等待用户交互，然后重新启动计算机。
- **睡眠** – 保存会话并使计算机处于低能耗状态，以便用户快速恢复工作。
- **休眠** – 获取在 RAM 上运行的所有内容并将其移动到硬盘上的特定文件。您的计算机将关闭，但在下次启动时将恢复到之前的状态。

> 根据您计算机的电源和使操作系统进入睡眠状态设置或计算机/笔记本电脑功能，可以使用**睡眠**或**休眠**操作。请记住，睡眠中的计算机仍是一台正在运行的计算机。当计算机依赖电池供电时，它仍在运行基本功能且仍在耗电。若要在办公室外移动办公时延长电池使用时间，建议您使用“休眠”选项。

选定操作将在所有正在运行的扫描完成后开始。当选择**关机**或**重新启动**时，将显示一个 30 秒倒计时的确认对话窗口（单击**取消**可停用请求的操作）。

选择**扫描无法取消**，以让非特权用户无法停止扫描后执行的操作。

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

另请参阅扫描进度

计划任务概述

当您双击自定义任务，或者右键单击自定义计划任务并单击**显示任务详细信息**时，该对话窗口将显示有关所选计划任务的详细信息。

任务详细信息

键入**任务名称**、选中其中一个**任务类型**选项，然后单击**下一步**

- **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。

任务计时

任务将以指定的时间间隔重复执行。选择以下计时选项之一：

- **一次** – 任务将仅在预定义的日期和时间执行一次。
- **重复** – 任务将以指定的时间间隔（以小时为单位）执行。
- **每天** – 任务将在每天的指定时间运行。
- **每周** – 任务将在每周所选星期和时间运行一次或多次。
- **由事件触发** – 任务将在指定事件后执行。

靠电池供电时跳过任务 – 如果在任务应该启动时您的计算机正靠电池供电，则任务将不会启动。这也适用于依赖 UPS 运行的计算机。

任务计时 – 一次

任务执行 – 指定的任务仅在指定的日期和时间运行一次。

任务计时 – 每天

任务将在每天的指定时间运行。

任务计时 – 每周

任务将在每周选定的这一天和时间重复运行。

任务计时 – 由事件触发

任务将由以下任一事件触发：

- **每次计算机启动**
- **每天计算机第一次启动时**
- **拨号连接至 Internet/VPN**
- **成功更新模块**
- **成功更新产品**
- **用户登录**
- **威胁检测**

计划由事件触发任务时，可以指定两次任务完成之间的最小间隔。例如，如果您每天多次登录计算机，可以选择 24 小时，这样仅在当天首次登录时执行任务，然后在第二天执行任务。

跳过的任务

当计算机靠电池供电或断电时，可以跳过任务。从这些选项之一选择任务应在何时运行，然后单击**下一步**。

- **在下一个计划时间** – 如果计算机在下一个计划时间打开，则运行任务。
- **尽快** – 任务将在计算机打开时运行。
- **如果自上次计划运行之后经过的时间超过(小时)，则立即运行** – 表示自任务首次跳过运行之后经过的时间。如果超过此时间，将立即运行该任务。

> ✓ 如果自上次计划运行之后经过的时间超过(小时)，则立即运行 – 示例
> 示例任务设置为每小时重复运行。选择**如果自上次计划运行之后经过的时间超过(小时)，则立即运行**选项，并将超过时间设置为两小时。任务在 13:00 开始运行；完成后，计算机会进入睡眠状态：
> • 计算机在 15:30 唤醒。任务首次跳过运行的时间为 14:00。从 14:00 开始，时间仅过去 1.5 小时，因此任务将在 16:00 开始运行。
> • 计算机在 16:30 唤醒。任务首次跳过运行的时间为 14:00。从 14:00 开始，时间已过去两个半小时，因此任务将立即运行。

任务详细信息 – 更新

如果您希望从两个更新服务器更新程序，则有必要创建两个不同的更新配置文件。如果第一个更新配置文件无法下载更新文件，则程序会自动切换到备用更新配置文件。这适用于一般从本地局域网更新服务器进行更新但其所有者经常通过其他网络连接到 Internet 的设备，例如，笔记本电脑。因此，如果第一个配置文件出现故障，第二个配置文件将从 ESET 的更新服务器上自动下载更新文件。

任务详细信息 – 运行应用程序

此任务安排外部应用程序的执行。

可执行文件 – 从目录树中选择可执行文件，单击**...**选项或手动输入路径。

工作文件夹 – 定义外部应用程序的工作目录。选定**可执行文件**的所有临时文件将在此目录中创建。

参数 – 应用程序的命令行参数（可选）。

单击**完成**以应用此任务。

系统清理器

系统清理器是一个工具，有助于在清除威胁后将计算机恢复为可用状态。恶意软件可能会禁用系统实用工具，如注册表编辑器、任务管理器或 Windows 更新。一次单击，系统清理器即可恢复给定系统的默认值和设置。

系统清理器报告来自五个设置类别的问题：

- **安全设置：** 可能导致计算机漏洞增加的设置更改，例如 Windows 更新。
- **系统设置：** 可能更改计算机行为的系统设置更改，例如文件关联
- **系统外观：** 影响系统外观的设置，例如桌面壁纸
- **已禁用功能：** 可能已禁用的重要功能和应用程序
- **Windows 系统还原** Windows 系统还原功能的设置，允许您将系统还原到以前的状态

在以下情况下，可以请求系统清理：

- 发现威胁时
- 用户单击**重置**时

您可以查看更改，并在需要时重置设置。

仅具有管理员权限的用户可以在系统清理器中执行上述操作。

隔离区

隔离区的主要功能是安全地存储报告的对象（例如恶意软件、被感染的文件或潜在不受欢迎的应用程序）。

可从 ESET NOD32 Antivirus 主程序窗口中访问隔离区，方法是依次单击**工具 > 隔离**。

可在表格中查看储存在隔离区文件夹中的文件，该表格中将显示以下内容：

- 隔离的日期和时间、
- 文件原始位置的路径、
- 文件大小（字节数）、
- 原因（例如，用户添加的对象）、
- 以及许多检测（例如，同一文件的重复检测，或者如果该文件是包含多个渗透的压缩文件）。

隔离文件

ESET NOD32 Antivirus 会自动隔离已删除的文件（如果尚未在警告窗口中取消该选项）。

如果其他文件出现以下情况，还应隔离这些文件：

a.无法清除、

b.如果不安全或建议删除、

c.如果它们由 ESET NOD32 Antivirus 误检测到、

d.或者，如果文件行为可疑但未被保护检测到。

要隔离文件，有多个选项可供使用：

a.使用拖放功能手动隔离文件，方法是单击文件、长按鼠标按钮的同时将鼠标指针移动到标记区域，然后释放它。在此之后，应用程序会移动到前台。

b.右键单击文件 > 依次单击**高级选项 > 隔离文件**。

c.在**隔离区**窗口中，单击**移至隔离区**。

d.还可以使用右键菜单达到此目的；在**隔离区**窗口中右键单击，然后选择**隔离**。

从隔离恢复

隔离的文件还可以恢复到其原始位置：

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

从隔离区中删除

右键单击给定项并选择**从隔离区中删除**，或者选择要删除的项并在键盘上按 **Delete** 键。如果要选择并删除隔离区中的所有项目，可以在键盘上按 **Ctrl + A**，然后按 **Delete**。删除的项将从设备和隔离区中永久删除。

提交隔离区中的文件

如果程序未检测到您隔离的可疑文件，或文件被错误地确认为被感染（如启发式扫描代码分析所做的评估）并被隔离，请将该样本发送到 ESET 研究实验室进行分析。要提交文件，请右键单击该文件并从右键菜单中选择**提交供分析**。

检测说明

右键单击一个条目，然后单击**检测说明**以打开 ESET 威胁百科全书（其中包含有关已记录渗透的危险和症状的详细信息）。

> 图文并茂说明
> 以下 ESET 知识库文章可能仅提供英文版：
> - 在 ESET NOD32 Antivirus 中恢复隔离的文件
> - 在 ESET NOD32 Antivirus 中删除隔离的文件
> - 我的 ESET 产品向我发送检测通知，我该怎么办？

隔离失败

无法将特定文件移至隔离区的原因如下所示：

- **您没有读取权限** – 这意味着您无法查看文件的内容。
- **您没有写入权限** – 这意味着您无法修改文件的内容，即添加新内容或删除现有内容。
- **文件(您正尝试隔离)过大** – 您需要减小文件大小。

当您收到错误消息“隔离失败”时，请单击**更多信息**。将显示隔离错误列表窗口，并且您会看到文件的名称及该文件无法隔离的原因。

选择样本以供分析

如果在计算机上发现可疑文件或在 Internet 上发现可疑站点，可以将它提交给 ESET 研究实验室以供分析（根据 ESET LiveGrid® 的配置，也许无法提交）。

将样本提交至 ESET 之前

除非样本至少满足以下条件之一，否则请勿提交该样本：

- ESET 产品并未检测到样本
- 将样本错误检测为威胁
- 我们不接受个人文件（希望由 ESET 扫描以查找恶意软件）作为样本（ESET 研究实验室不会为用户手动执行扫描）
- 使用描述性主题行，并尽可能多地包含有关文件的信息（例如，屏幕截图或下载该文件的网站）

可以使用以下方法之一将样本提交（文件或网站）发送到 ESET 以供分析：

1. 使用产品中的样本提交表单。它位于**工具 > 提交样本以供分析**。提交样本的最大大小为 256 MB。

2. 此外，也可以通过电子邮件提交文件。如果您选用此方式，请使用 WinRAR/WinZIP 压缩文件，用密码“infected”保护压缩文件，然后将它发送至 samples@eset.com。

3. 要报告垃圾邮件或垃圾邮件误报，请参阅我们的 ESET 知识库文章。

在**选择样本以供分析**表单中，从**提交样本的理由**下拉菜单中选择最适合您邮件目的的描述：

- 可疑文件
- 可疑站点（被任何恶意软件感染的网站），
- 误报站点
- 误报文件（文件检测为感染，但并未感染），
- 其他

文件/站点 – 您想要提交的文件或网站的路径。

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

您可能不会收到 ESET 的回复

除非需要您提供更多信息，否则您不会收到 ESET 的回复。由于我们的服务器每天都会收到数以万计的文件，因此不可能对所有提交一一回复。
如果样本被证实是一个恶意应用程序或网站，则以后的 ESET 更新中将增加对它的检测。

选择样本以供分析 – 可疑文件

观察到的恶意软件感染迹象和症状 – 输入在您的计算机上观察到的可疑文件行为的描述。

文件来源(URL 地址或供应商) – 请键入文件出处（来源）以及您是如何遇到该文件的。

注释和其他信息 – 您可以在这里添加有助于处理可疑文件的其他信息或描述。

第一个参数（**观察到的恶意软件感染迹象和症状**）必填，此外提供其他信息将对我们实验室的识别过程和样本处理提供极大帮助。

选择样本以供分析 – 可疑站点

请从**网站问题**下拉菜单选择以下内容之一：

- **被感染** – 包含由各种方法分发的病毒或其他恶意软件的网站。
- **网络钓鱼** – 用于获取敏感数据（如银行帐号PIN 码等）的访问权限。请阅读词汇表中关于此类攻击的更多信息。
- **欺诈** – 恶作剧或欺诈性网站，尤其是为了快速获利。
- 如果上述选项与您要提交的站点不符，请选择**其他**

注释和其他信息 – 可以键入有助于分析可疑网站的其他信息或描述。

选择样本以供分析 – 误报文件

我们请求您提交已检测为感染但却未感染的文件，以便改进病毒和间谍软件防护引擎并为其他用户提供防护。当文件模式匹配检测引擎中包含的同一模式时，可能会发生误报 (FP)

应用程序名称和版本 – 程序标题及其版本（例如，编号、别名或代码名称）。

文件来源(URL 地址或供应商) – 请输入文件出处（来源），并注明您是如何遇到该文件的。

应用程序用途 – 一般应用程序描述、应用程序类型（例如浏览器、媒体播放器...）及其功能。

注释和其他信息 – 您可以在这里添加有助于处理可疑文件的其他信息或描述。

> 前三个参数是必填的，以识别合法应用程序并将它与恶意代码区分开来。通过提供其他信息，您将对我们实验室的识别过程和样本的处理提供极大帮助。

选择样本以供分析 – 误报站点

我们请求您提交已检测为感染、欺诈或网络钓鱼但实际是误报的站点。当文件模式匹配检测引擎中包含的同一模式时，可能会发生误报 (FP)请提供该网站以帮助我们改进病毒和网络钓鱼防护引擎，并帮助为其他用户提供防护。

备注和附加信息 – 可以在此处添加有助于处理可疑网站的附加信息或描述。

选择样本以供分析 – 其他

如果文件无法被归类为**可疑文件**或**误报**，请使用此表格。

提交文件的原因 – 请输入详细描述和发送文件的原因。

设置

可以在主程序窗口 > **设置**中，找到可用的保护功能组。

设置菜单分为以下各组：

计算机防护

Internet 防护

在设置窗口的底部还提供了其他选项。单击高级设置以为每个模块设置更详细的参数。通过导入/导出设置使用 .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。

计算机防护

在主程序窗口 > **设置**中单击**计算机防护**，以查看所有防护模块的概述：

- 文件系统实时防护 – 在计算机上打开、创建或运行所有文件时，都将扫描文件是否带有恶意代码。
- 设备控制 – 此模块允许您扫描、阻止或调整扩展的过滤器/权限，并选择用户如何访问和使用给定设备 (CD/DVD/USB...)
- HIPS - HIPS 系统监视操作系统内的事件，并按照自定义的规则集进行响应。
- 游戏模式 – 启用或禁用游戏模式。启用游戏模式后您将收到警告消息（潜在安全风险），主窗口将变为橙色。

要暂停或禁用个别防护模块，请单击开关图标

⚠ 关闭防护模块可能会降低对您计算机的防护级别。

单击防护模块旁边的齿轮图标 ，以访问该模块的高级设置。

对于**文件系统实时防护**，请单击齿轮图标 ，然后从以下选项中进行选择：

- **配置** - 将打开文件系统实时防护高级设置
- **编辑排除** – 将打开排除设置窗口，以便可以排除扫描文件和文件夹。

暂停病毒和间谍软件防护 – 禁用所有病毒和间谍软件防护模块。禁用防护时，将打开一个窗口，以确定使用**时间间隔**下拉菜单禁用防护的时长。仅在您是有经验的用户或 ESET 技术支持的指示下使用。

检测到渗透

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

标准行为

作为 ESET NOD32 Antivirus 处理威胁的常见示例，可以使用以下功能检测渗透：

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

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

扫描计算机以查找被感染的文件

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：

1.打开 ESET NOD32 Antivirus 并单击**计算机扫描**。

2.单击**扫描计算机**（有关详细信息，请参阅计算机扫描。

3.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。

清除和删除

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

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

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

从隔离恢复

可从 ESET NOD32 Antivirus 主程序窗口中访问隔离区，方法是依次单击**工具** > **隔离**。

隔离的文件还可以恢复到其原始位置：

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

多个威胁

如果在计算机扫描期间没有清除任何被感染文件（或清除级别设置为**不清除**），则会出现一个警报窗口，提示您为这些文件选择相应操作。为文件选择相应操作（分别为列表中的每个文件设置操作），然后单击**完成**。

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。

Internet 防护

Internet 连接是个人计算机的一项标准功能。不幸地是，它也成为传输恶意代码的主要媒介。打开主程序窗口 > **设置** > **Internet 防护**，以配置 ESET NOD32 Antivirus 中将增强 Internet 防护的功能。

要暂停或禁用个别防护模块，请单击开关图标 

⚠ 关闭防护模块可能会降低对您计算机的防护级别。

单击防护模块旁边的齿轮图标 ⚙，以访问该模块的高级设置。

Web 访问保护会扫描 HTTP/HTTPS 通信，以查找恶意软件和网络钓鱼。仅应出于故障排除目的而关闭 Web 访问保护。

网络钓鱼防护允许您阻止散布网络钓鱼内容的已知网页。强烈建议您保持启用网络钓鱼防护。

报告网络钓鱼站点 – 向 ESET 报告网络钓鱼/恶意网站以进行分析。

向 ESET 提交网站前，确保其满足以下一个或多个标准：
- 未检测到该网站。
- 该网站被错误地检测为威胁。在此情况下，您可以报告错误阻止的页面

电子邮件客户端防护可控制通过 POP3(S) 和 IMAP(S) 协议接收的电子邮件通信。使用电子邮件客户端的插件程序，ESET NOD32 Antivirus 可控制电子邮件客户端的所有通信。

网络钓鱼防护

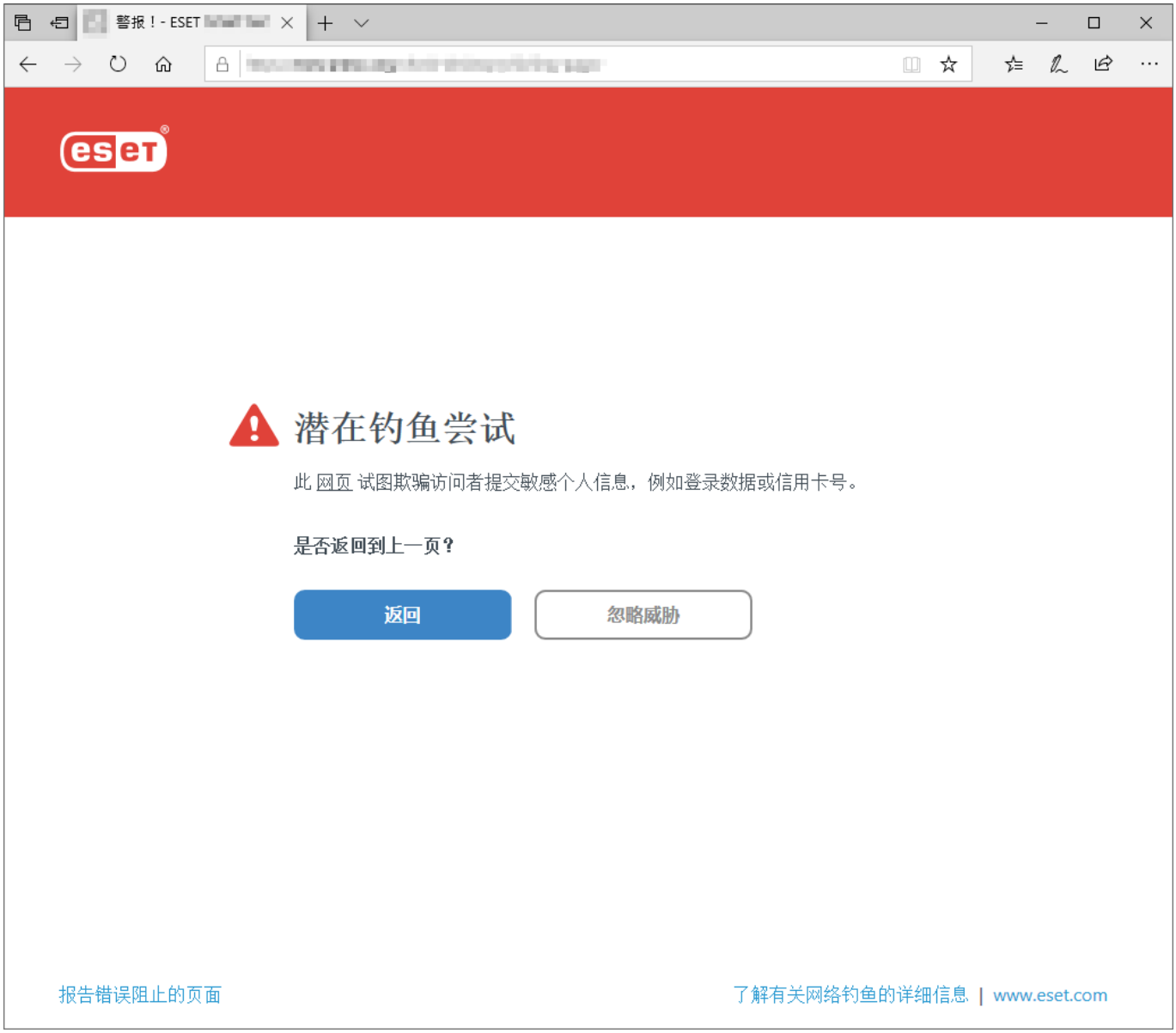
网络钓鱼是一种利用社交工程（操纵用户以获取机密信息）的犯罪活动。网络钓鱼会用于访问敏感数据，例如银行帐号，PIN 等。有关详细信息，请参阅词汇表，ESET NOD32 Antivirus 包括网络钓鱼防护，可阻止分发此类内容的已知网页。

默认情况下，网络钓鱼防护处于启用状态。可以在高级设置 > **保护** > **Web 访问保护**中配置此设置。

有关 ESET NOD32 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，您的 Web 浏览器会显示以下对话框。如果您仍需要访问该网站，请单击**忽略威胁**（不建议）



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，请使用URL 地址管理工具。在高级设置 > **保护** > **Web 访问保护** > **URL 地址管理** > **地址列表** > **编辑**中，将要编辑的网站添加到该列表。

报告网络钓鱼站点

通过**报告错误阻止的页面**链接，可以报告被错误地检测为威胁的网站。

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，引导您访问它的网站，您是如何了解到它的等等）。

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 NOD32 Antivirus.xml 配置文件。

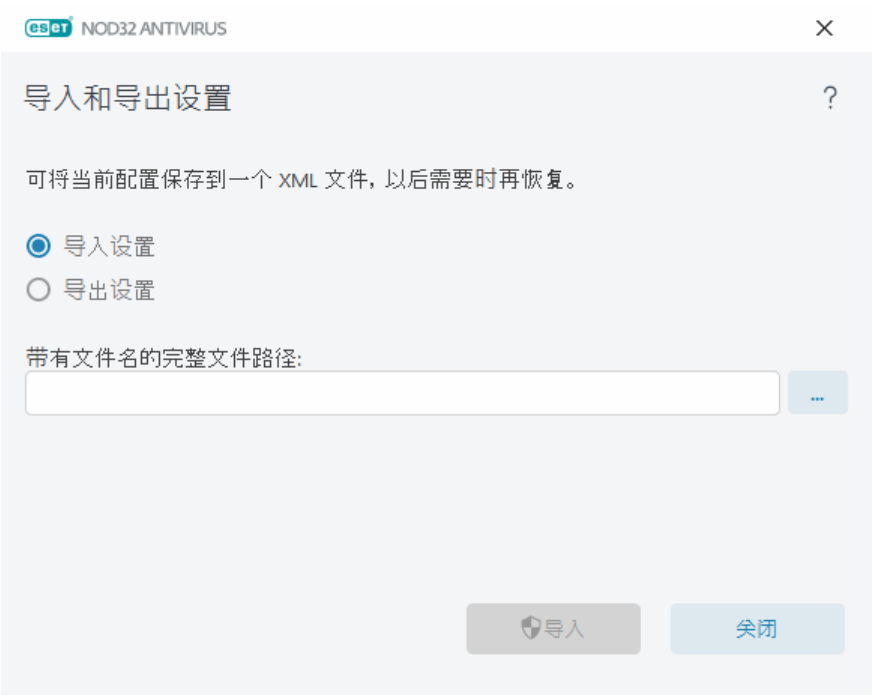
图文并茂说明
有关以英语和其他几种语言提供的图文并茂说明，请参阅使用 .xml 文件导入或导出 ESET 配置设置

当需要备份 ESET NOD32 Antivirus 的当前配置以备日后使用时，导入和导出配置文件将十分有用。当要在多个系统上使用首选配置时，导出设置选项也很便利。可以导入 .xml 文件，来传输这些设置。

要导入配置，请在主程序窗口中，依次单击**设置 > 导入/导出设置**，然后选择**导入设置**。键入配置文件名，或单击 **...** 按钮来浏览要导入的配置文件。

要导出配置，请在主程序窗口中，依次单击**设置 > 导入/导出设置**。选择**导出设置**，键入带有名称的完整文件路径。单击 **...** 以导航到计算机上的某个位置来保存配置文件。

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会遇到错误。



帮助和支持

单击主程序窗口中的**帮助和支持**以显示支持信息和疑难解答工具，可帮助您解决可能遇到的问题。

订阅

- 订阅疑难解答 – 单击此链接以查找激活或订阅更改问题的解决方案。
- 更改订阅 – 单击以启动激活窗口并激活您的产品。如果设备已连接到 ESET HOME，请从 ESET HOME 帐户中选择一个订阅，或者添加一个新许可证。

已安装的产品

- 新功能 – 单击以打开有关新功能和改进功能的信息窗口。
- 关于 ESET NOD32 Antivirus – 显示有关 ESET NOD32 Antivirus 副本的信息。
- 产品疑难解答产品疑难解答 – 单击此链接以查找大多数常见问题的解决方案。
- **更改产品** – 单击以查看是否可以使用当前订阅将 ESET NOD32 Antivirus 更改为其他产品系列

帮助页面 – 单击此链接以启动 ESET NOD32 Antivirus 帮助页面。

技术支持

知识库 - ESET 知识库包含对大多数常见问题的解答以及各种问题的建议解决方案。知识库由 ESET 专业技术人员定期更新，它已成为解决各类问题的最强大工具。

关于 ESET NOD32 Antivirus

此窗口提供有关 ESET NOD32 Antivirus 的已安装版本和您计算机的详细信息。

单击**显示模块**，以查看有关已加载的程序模块列表的信息。

- 可以单击**复制**将有关模块的信息复制到剪贴板。这在排除故障或联系技术支持时可能有用。
- 在模块窗口中，单击**检测引擎**以打开 ESET 病毒雷达，其中包含有关每个 ESET 检测引擎版本的信息。

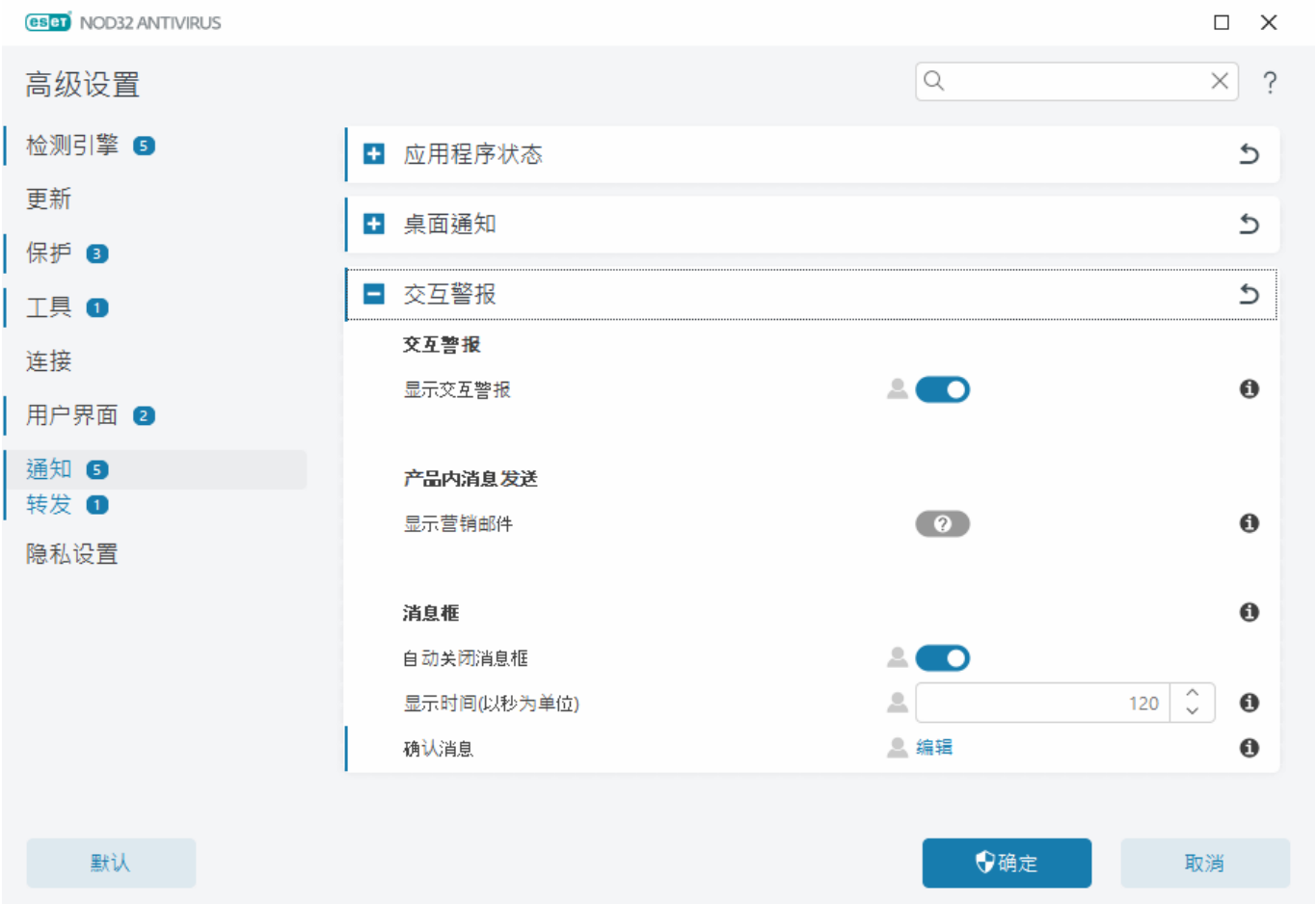
ESET 新闻

在此窗口中ESET NOD32 Antivirus 会定期向您发送 ESET 新闻的通知。

产品内消息旨在向用户发送有关 ESET 新闻和其他通信的通知。发送市场营销消息需要用户同意。因此，默认情况下营销邮件不会发送给用户（显示为问号）。启用此选项，即表示您同意接收 ESET 市场营销消息。如果您对接收 ESET 市场营销材料不感兴趣，则禁用**显示市场营销消息**选项。

要启用或禁用通过通知接收市场营销消息，请按照以下说明进行操作。

1. 打开“高级设置”。
2. 单击**通知** > **交互警报**。
3. 修改**显示市场营销消息**选项。



提交系统配置数据

为了尽可能快速准确地提供支持。ESET 需要有关 ESET NOD32 Antivirus 配置的信息、详细的系统信息以及关于正在运行的进程（ESET SysInspector 日志文件）和注册表数据的信息。ESET 将仅使用此数据来为客户提供技术帮助。

在提交 Web 表单后，您的系统配置数据会发送给 ESET。如果希望记住对此过程执行的该操作，请选择**始终提交此信息**。提交 Web 表单（在不发送任何数据的情况下），单击**不提交数据**并继续。

可以在高级设置 > **工具** > **诊断** > 技术支持中，配置系统配置数据的提交。

如果您决定提交系统配置数据，则需要填写并提交 Web 表单。否则，将不会创建您的票证，并且您的系统数据会丢失。如果无法提交系统配置数据，则填写 Web 表单并等待技术支持的指示。

技术支持

在主程序窗口中，依次单击**帮助和支持** > **技术支持**。

联系技术支持

请求支持 – 如果找不到问题的答案，可以使用位于 ESET 网站上的该表单，来快速联系 ESET 技术支持部门。根据您的设置，在填写 Web 表单之前将显示提交系统配置数据窗口。

获取技术支持信息

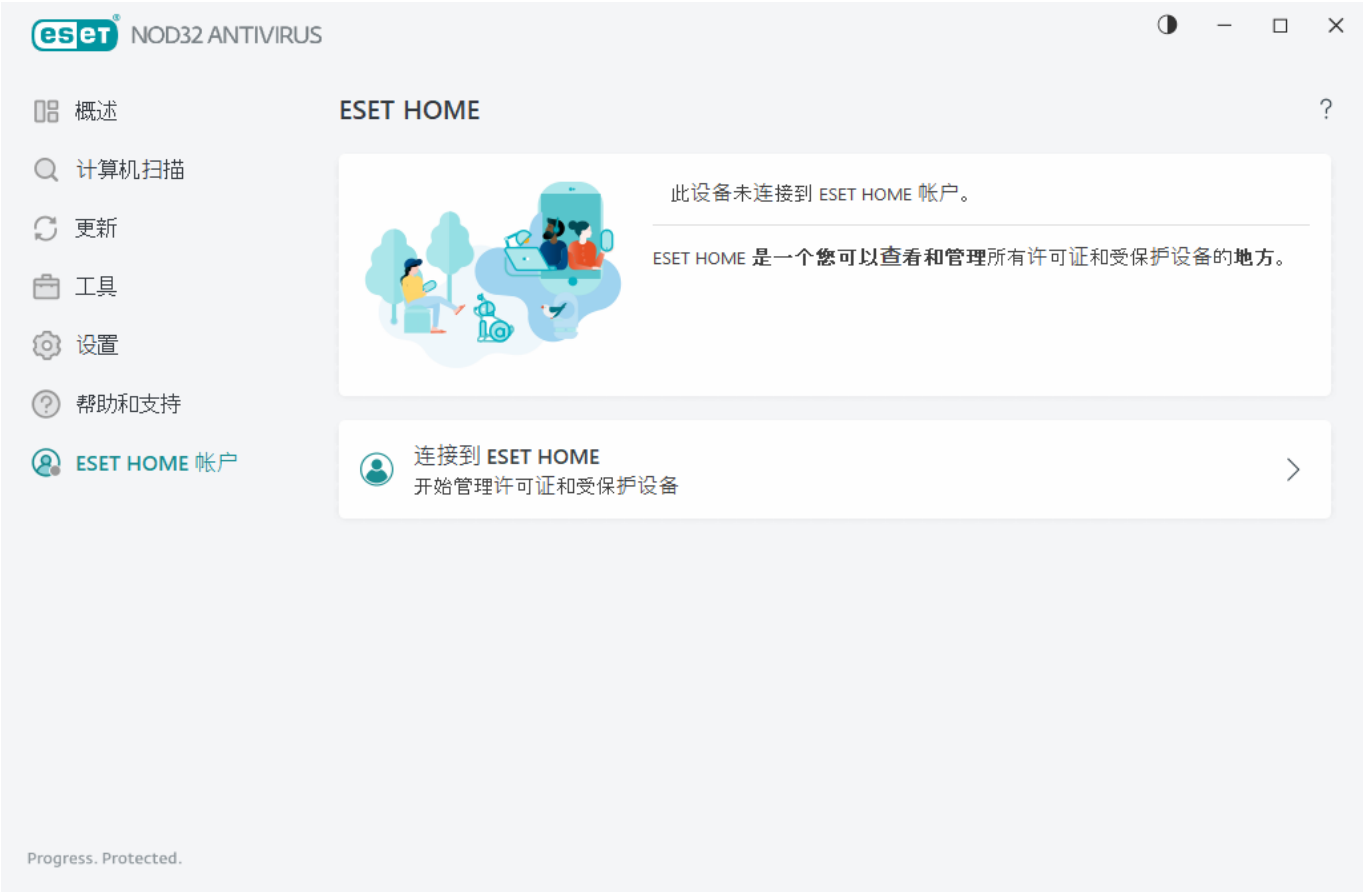
技术支持详细信息 – 当出现提示时，可以复制信息并将其发送给 ESET 技术支持（例如，订阅详细信息、产品名称、产品版本、操作系统和计算机信息）。

ESET Log Collector – 链接到 ESET 知识库文章，可以在其中下载 ESET Log Collector。它是一种从计算机自动收集信息和日志以帮助更快速地解决问题的应用程序。有关详细信息，请参阅 ESET Log Collector 联机用户手册。

启用高级日志记录以为所有可用功能创建高级日志，从而帮助开发人员诊断并解决问题。日志记录的最低级别设置为**诊断**级别。高级日志记录将在两小时后自动禁用，除非通过单击**停止高级日志记录**提前将其停止。创建所有日志后，会显示通知窗口，从而可直接访问含有已创建日志的“诊断”文件夹。

ESET HOME 帐户

可以在主程序窗口 > **ESET HOME 帐户**中查看 ESET HOME 帐户连接状态。



此设备未连接到 ESET HOME 帐户

单击连接到 ESET HOME，以将设备连接到 ESET HOME 并管理订阅和受保护的设备。可以续订、升级或延期订阅，还可以查看重要的许可证详细信息。在 ESET HOME 管理门户或移动应用程序中，可以添加其他订阅、将产品下载到设备、检查产品的安全状态或通过电子邮件共享订阅。有关详细信息，请访问 ESET HOME 联机帮助。

此设备已连接到 ESET HOME 帐户

可以使用 ESET HOME 门户或移动应用程序远程管理设备的安全性。单击 **App Store** 或 **Google Play** 以显示可以使用移动手机扫描的二维码，来从 App Store 或 Google Play 下载 ESET HOME 移动应用程序。

ESET HOME 帐户 – 您的 ESET HOME 帐户名称。

设备名称 – 此设备在 ESET HOME 帐户中显示的名称。

打开 ESET HOME – 打开 ESET HOME 管理门户。

要将设备与 ESET HOME 帐户断开连接，请依次单击**与 ESET HOME 断开连接** > **断开连接**。用于激活的订阅仍会处于有效状态，并且您的设备会受保护。

连接到 ESET HOME

将设备连接到 ESET HOME，以查看和管理所有已激活的 ESET 订阅和设备。可以续订、升级或延期订阅，还可以查看重要的订阅详细信息。在 ESET HOME 管理门户或移动应用程序中，可以添加其他订阅、将产品下载到设备、检查产品的安全状态或通过电子邮件共享订阅。有关详细信息，请访问 ESET HOME 联机帮助。

将设备连接到 ESET HOME:

如果要在安装期间或选择**使用 ESET HOME 帐户**作为激活方法时连接到 ESET HOME，请按照使用 ESET HOME 帐户主题中的说明进行操作。

如果已安装 ESET NOD32 Antivirus 并使用在 ESET HOME 帐户中添加的订阅激活，即可使用 ESET HOME 门户将设备连接到 ESET HOME，按照 ESET HOME 联机帮助指南中的说明操作，并在 ESET NOD32 Antivirus 中允许连接。

1. 在主程序窗口中，依次单击 **ESET HOME 帐户** > **连接到 ESET HOME**，或在**将此设备连接到 ESET HOME 帐户**通知中单击**连接到 ESET HOME**。

2. 登录到 ESET HOME 帐户。

如果您没有 ESET HOME 帐户，则单击**创建帐户**以注册或查看ESET HOME联机帮助中的说明。

如果您忘记了密码，则单击**我忘记了密码**，然后按照屏幕上的步骤进行操作，或查看ESET HOME联机帮助中的说明。

3. 设置**设备名称**，然后单击**继续**。

4. 成功连接后，将显示详细信息窗口。单击**完成**。

登录到 ESET HOME

有几种方法可以登录到 ESET HOME 帐户：

- **使用 ESET HOME 电子邮件地址和密码** – 键入用于创建 ESET HOME 帐户的**电子邮件地址**和**密码**，然后单击**登录**。

• **使用 Google 帐户/AppleID** – 单击**继续使用 Google** 或**继续使用 Apple**，然后登录到相应帐户。成功登录后，您将重定向到 ESET HOME 确认网页。要继续，请切换回 ESET 产品窗口。有关 Google 帐户/AppleID 登录的详细信息，请参阅 ESET HOME 联机帮助中的说明。

• **扫描二维码** – 单击**扫描二维码**以显示二维码。打开 ESET HOME 移动应用程序并扫描二维码，或将设备相机指向二维码。有关详细信息，请参阅 ESET HOME 联机帮助中的说明。

如果您没有 ESET HOME 帐户，则单击**创建帐户**以注册或查看ESET HOME联机帮助中的说明。
如果您忘记了密码，则单击**我忘记了密码**，然后按照屏幕上的步骤进行操作，或查看ESET HOME联机帮助中的说明。

登录失败 – 常见错误

登录失败 – 常见错误

无法找到与输入的电子邮件地址匹配的帐户

您输入的电子邮件地址不匹配任何 ESET HOME 帐户。单击**返回**，然后键入正确的电子邮件地址和密码。

要登录，必须创建一个 ESET HOME 帐户。如果您没有 ESET HOME 帐户，请单击**返回** > **创建帐户**或参阅创建新的 ESET HOME 帐户

用户名和密码不匹配。

键入的密码与输入的电子邮件地址不匹配。单击**返回**，键入正确的密码并验证键入的电子邮件地址是否正确。如果仍然无法登录，请单击**后退** > **忘记密码**以重置密码，并按照屏幕上的步骤操作，或参阅我忘记了我的 ESET HOME 密码

所选登录选项与您的帐户不匹配

您的帐户已链接到您的社交媒体帐户。若要登录到 ESET HOME，请单击**继续使用 Google** 或**继续使用 Apple**，然后登录到相应的帐户。成功登录后，您将重定向到 ESET HOME 确认网页。您可以将社交媒体帐户与 ESET HOME 门户上的 ESET HOME 帐户断开连接。

密码错误

如果您的 ESET NOD32 Antivirus 已连接到 ESET HOME 并且需要登录才能进行更改（例如，禁用 Anti-Theft），而且您输入的密码与您的帐户不匹配，则会发生此错误。单击**返回**，然后键入正确的密码。如果仍然无法登录，请单击**后退** > **忘记密码**以重置密码，并按照屏幕上的步骤操作，或参阅我忘记了我的 ESET HOME 密码。

在 ESET HOME 中添加设备

如果已安装 ESET NOD32 Antivirus 并使用在 ESET HOME 帐户中添加的订阅激活，即可使用 ESET HOME 门户将设备连接到 ESET HOME。

1. 向您的设备发送连接请求。

2. ESET NOD32 Antivirus 将显示**将此设备连接到 ESET HOME 帐户**对话框窗口以及 ESET HOME 帐户名称。单击**允许**，以将该设备连接到提及的 ESET HOME 帐户。

如果没有交互，将在大约 30 分钟后自动取消该连接请求。

高级设置

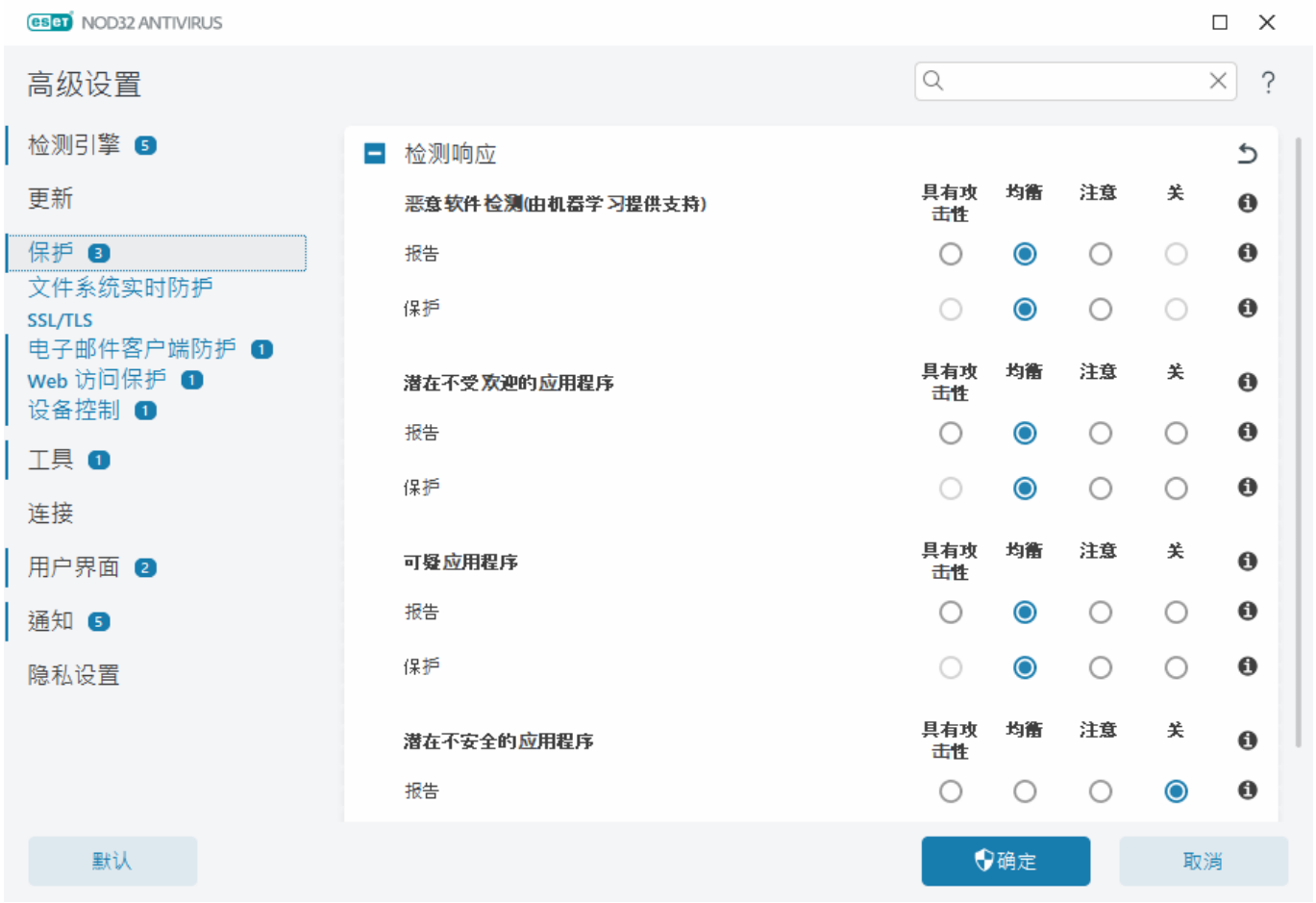
通过高级设置，可以根据自己的需求配置详细的 ESET NOD32 Antivirus 设置。

要打开“高级设置”，请打开主程序窗口，然后按键盘上的 **F5** 键，或依次单击**设置** > **高级设置**。

根据您的访问设置，系统可能会提示您键入密码以打开“高级设置”。

在“高级设置”中，可以配置以下设置：

- 检测引擎
- 更新
- 保护
- 工具
- 连接
- 用户界面
- 通知
- 隐私设置



检测引擎

高级设置 > **检测引擎**使您能够配置以下选项：

- 排除
- 高级选项
- 网络通信扫描程序

排除

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

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

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

请勿与其他类型的排除混淆：

- 进程排除 – 归因于排除的应用程序进程的所有文件操作都会被排除扫描（可能需要提高备份速度和服务可用性）。

- 排除的文件扩展名
- HIPS 排除
- 基于云的防护的排除过滤器

性能排除

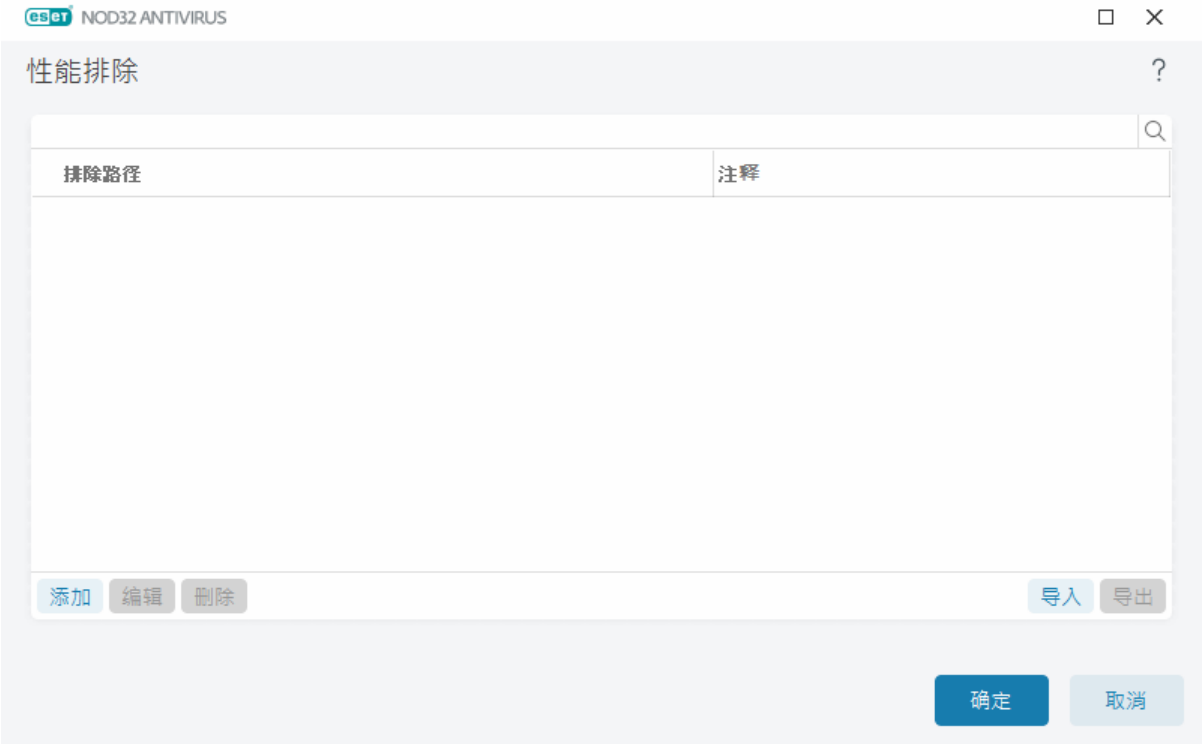
性能排除允许您排除扫描文件和文件夹。

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

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

请勿混淆检测排除排除的文件扩展名HIPS 排除或进程排除

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



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

控件元素

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

添加或编辑性能排除

此对话框窗口不包括此计算机的特定路径（文件或目录）。

选择路径或手动输入
要选择合适的路径，请在**路径**字段中单击 **...**
手动键入时，请参阅下面的多个排除格式示例

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

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

D????.exe（问号将替换缺少/未知的字符）

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

排除中的系统变量

您可以使用类似 %PROGRAMFILES% 的系统变量来定义扫描排除。

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

展开受支持系统变量的列表

在路径排除格式中可以使用以下变量：

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

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

不支持路径中间的通配符

在路径中间使用通配符（例如，*C:\Tools*\Data\file.dat*）可能起作用，但为了性能排除而不正式支持。

当使用检测排除时，不限制在路径中间使用通配符。

排除顺序

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

路径排除格式

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

排除格式

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

D????.exe（问号将替换缺少/未知的字符）

示例：

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

排除中的系统变量

您可以使用类似 %PROGRAMFILES% 的系统变量来定义扫描排除。

• 在添加到排除时，要使用此系统变量排除 Program Files 文件夹，请使用路径 *%PROGRAMFILES%**（记住在路径末尾添加反斜杠和星号）。

• 要排除 *%PROGRAMFILES%* 子目录中的所有文件和文件夹，请使用路径 *%PROGRAMFILES%\Excluded_Directory**

展开受支持系统变量的列表

在路径排除格式中可以使用以下变量：

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

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

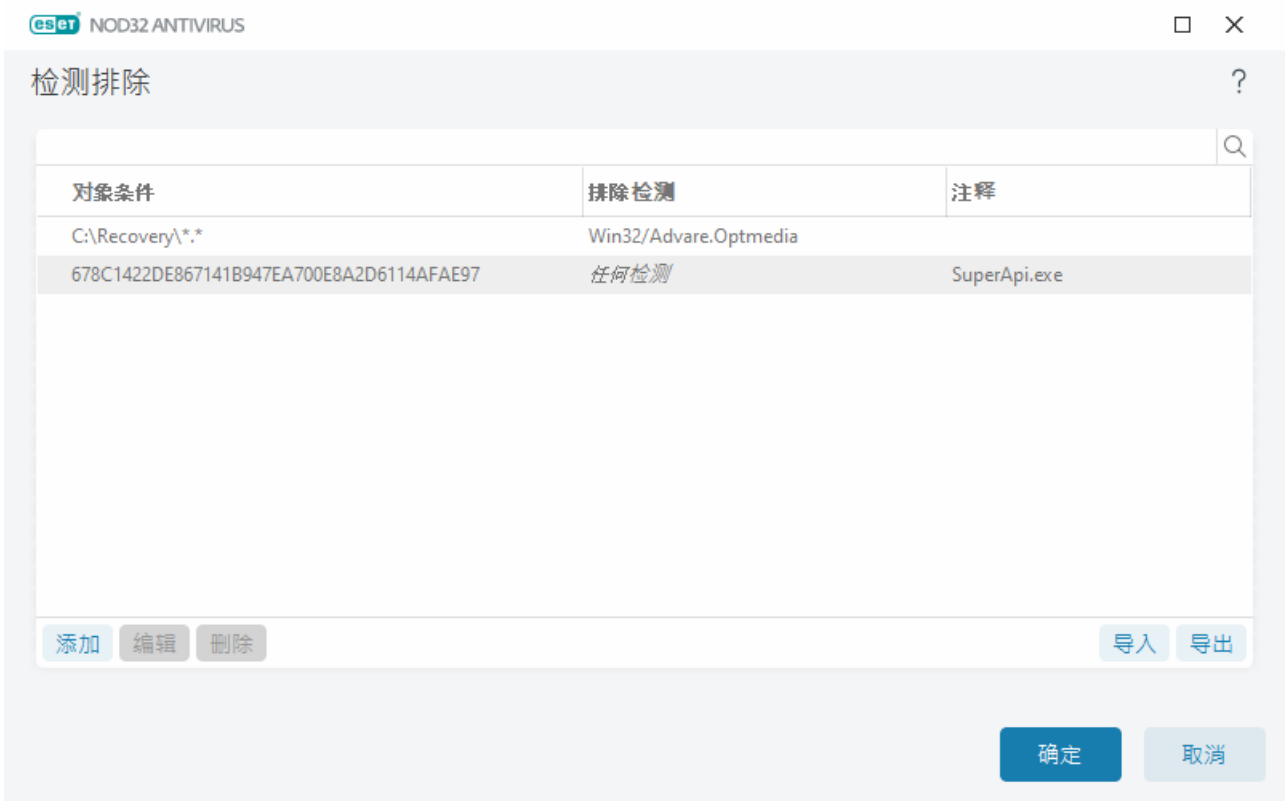
检测排除

“检测排除”让您可以通过过滤检测名称、对象路径或其哈希，来排除检测对象。

检测排除如何工作

检测排除不会像性能排除那样排除扫描文件和文件夹。检测排除仅在检测引擎检测到对象并且排除列表中存在合适规则时才会排除对象。

例如（参见下图中的第一行），当某个对象检测为 Win32/Adware.Optmedia 并且检测到文件为 *C:\Recovery\file.exe* 时。在第二行上，尽管有检测名称，但具有合适 SHA-1 哈希的每个文件将始终被排除。



要确保检测到所有威胁，建议您仅在绝对必要时才创建检测排除。

要将文件和文件夹添加到排除列表，请打开高级设置 > **检测引擎** > **排除** > **检测排除** > **编辑**。

请勿混淆性能排除、排除的文件扩展名、HIPS 排除或进程排除。

要从检测引擎中排除对象（按其检测名称或哈希），请单击**添加**。

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

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

检测排除对象标准

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

添加或编辑检测排除

排除检测

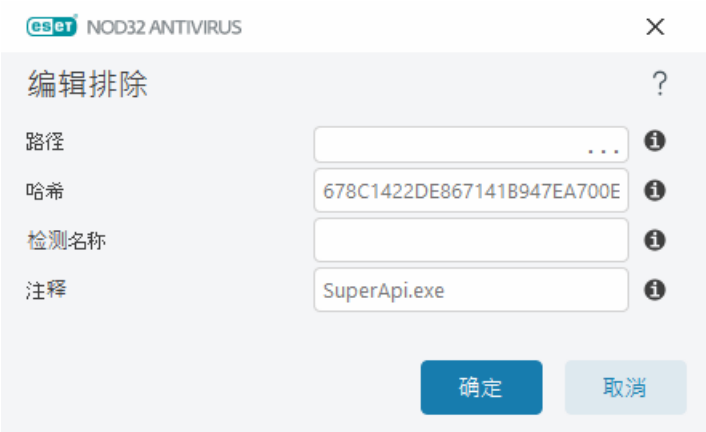
应提供有效的 ESET 检测名称。要查找有效的检测名称，请参见日志文件，然后从日志文件下拉菜单中选择**检测**。当在 ESET NOD32 Antivirus 中检测到误报样本时，这将很有用。对真正渗透的排除是非常危险的，考虑通过单击**路径掩码**中的 **...** 仅排除受影响的文件/目录，并/或在临时时期进行排除。排除还应用于潜在不受欢迎的应用程序、潜在不安全的应用程序和可疑应用程序。

另请参阅路径排除格式

请参阅以下检测排除示例

排除哈希

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



按检测名称排除

要按检测名称排除特定检测，请输入有效的检测名称：
Win32/Adware.Optmedia
当您从 ESET NOD32 Antivirus 警报窗口排除检测时，也可以使用以下格式：
@NAME=Win32/Adware.Optmedia@TYPE=ApplicUnwnt
@NAME=Win32/TrojanDownloader.Delf.QQI@TYPE=Trojan
@NAME=Win32/Bagle.D@TYPE=worm

控件元素

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

创建检测排除向导

还可以从日志文件上下文菜单创建检测排除（不适用于恶意软件检测）：

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

要根据**排除标准**排除一个或多个检测，请单击**更改标准**：

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

建议选项是根据检测类型而预先选择的。

可以选择添加**注释**，然后再单击**创建排除**。

检测引擎高级选项

启用通过 AMSI 的高级扫描是 Microsoft Antimalware Scan Interface 工具，允许扫描 PowerShell 脚本、Windows Script Host 执行的脚本和使用 AMSI SDK 扫描的数据。

网络通信扫描程序

网络通信扫描程序会为应用程序协议提供恶意软件防护，该扫描程序集成了多种高级恶意软件扫描技术。无论 Internet 浏览器或电子邮件客户端如何，网络通信扫描程序都会自动扫描 HTTP(S)、POP3(S) 和 IMAP(S) 协议。可以在高级设置 > **检测引擎** > **网络通信扫描程序**中，启用/禁用网络通信扫描程序。

启用网络通信扫描程序 – 如果禁用此选项，则不会扫描 HTTP(S)、POP3(S) 和 IMAP(S) 协议。请注意，以下 ESET NOD32 Antivirus 功能需要启用网络通信扫描程序：

- Web 访问保护
- SSL/TLS
- 网络钓鱼防护
- 电子邮件客户端防护

基于云的防护

ESET LiveGrid®建立在 ESET ThreatSense.Net 高级早期预警系统之上）利用 ESET 用户在世界各地提交并发送给 ESET 研究实验室的数据。通过提供可疑样本和元数据ESET LiveGrid® 让我们能够立即对客户的需求作出反应，并使 ESET 能够持续应对最新威胁。

以下选项可用：

启用 ESET LiveGrid® 信誉系统

ESET LiveGrid® 信誉系统提供基于云的白名单和黑名单。

可以直接从程序界面或右键菜单通过 ESET LiveGrid® 提供的额外信息，来检查正在运行的进程和文件的信誉。

启用 ESET LiveGrid® 反馈系统

除了 ESET LiveGrid® 信誉系统之外ESET LiveGrid® 反馈系统还会收集有关涉及新检测到威胁的计算机信息。这些信息可能包括：

- 出现威胁的文件的样本或副本
- 文件路径
- 文件名
- 日期和时间
- 威胁在计算机上出现的过程
- 有关计算机操作系统的信息

默认情况下ESET NOD32 Antivirus 配置为提交可疑文件到 ESET 病毒实验室，以供详细分析。始终排除具有特定扩展名的文件（例如 *.doc* 或 *.xls*）。如果有您或贵组织希望避免发送的特定文件，还可以添加其他扩展名。

阅读隐私政策中有关发送相关数据的详细信息。

可以选择不启用 ESET LiveGrid®

您不会失去软件中的任何功能；但在某些情况下，在启用 ESET LiveGrid® 后，ESET NOD32 Antivirus 可以更快地响应新威胁。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 ESETESET发送完当前所有信息后，将不会再创建任何数据包。

请阅读词汇表中有关 ESET LiveGrid® 的更多信息。
有关如何在 ESET NOD32 Antivirus 中启用或禁用 ESET LiveGrid®请参阅我们以英语和其他几种语言提供的图文并茂说明

高级设置中基于云的防护配置

要访问 ESET LiveGrid® 的设置，请打开高级设置 > **检测引擎** > **基于云的防护**。

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

- **启用 ESET LiveGrid® 反馈系统** – 将相关提交数据（在下面的**样本提交**部分中描述）以及崩溃报告和统计信息发送到 ESET 研究实验室以供进一步分析。

- **提交崩溃报告和诊断数据** – 提交 ESET LiveGrid® 相关的诊断数据，例如崩溃报告和模块内存转储。我们建议将其保持为启用状态以帮助 ESET 诊断问题、改进产品和确保对最终用户的更好保护。

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

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

提交样本

手动提交样本 – 让您可以从上下文菜单、隔离或工具将样本手动提交给 ESET。

自动提交已检测的样本

选择将哪类样本提交给 ESET 以供分析，并用于改进以后的检测（最大样本大小默认为 64 MB）。以下选项可用：

- **所有已检测的样本** – 由检测引擎检测的所有对象（包括在扫描程序设置中启用的潜在不受欢迎的应用程序）。

- **除文档外的所有样本** – 除**文档**外的所有检测的对象（见下文）。

- **不提交** – 检测的对象不会发送给 ESET。

自动提交可疑样本

如果检测引擎未检测到这些样本，还会将这些样本发送给 ESET。例如，差点错过检测的样本，或者某个 ESET NOD32 Antivirus 防护模块认为这些样本可疑或其行为不明确（最大样本大小默认为 64 MB）。

- **可执行文件** – 包括可执行文件，如 .exe, .dll, .sys。

- **压缩文件** – 包括诸如 .zip, .rar, .7z, .arch, .arj, .bzip, .gzip, .ace, .arc, .cab 等压缩文件类型。

- **脚本** – 包括诸如 .bat, .cmd, .hta, .js, .vbs, .ps1 等脚本文件类型。

- **其他** – 包括诸如 .jar, .reg, .msi, .sfw, .lnk 等文件类型。

- **可能的垃圾电子邮件** – 允许向 ESET 发送可能的垃圾邮件部分或整个可能的垃圾电子邮件以及附件，以供进一步分析。启用此选项可改进垃圾邮件的全局检测，包括为您改进将来的垃圾邮件检测。

- **文档** – 包括具有或没有活动内容的 Microsoft Office 或 PDF 文档。

展开所有包含的文档文件类型列表

ACCDB, ACCDT, DOC, DOC_OLD, DOC_XML, DOCM, DOCX, DWFX, EPS, IWORK_NUMBERS, IWORK_PAGES, MDB, MPP, ODB, ODF, ODG, ODP, ODS, ODT, OLE2, OLE2_ENCRYPTED, OLE2_MACRO, OLE2_PROTECTED, ONE, ONEPKG, PDF, PPT, PPT_XML, PPTM, PPTX, PS, PSD, RTF, SYLK, THMX, VSD, VSD_XML, WPC, WPS, XLS, XLS_XML, XLSB, XLSM, XLSX, XPS

排除

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

要排除从 download.domain.com 下载的文件，请导航到高级设置 > **检测引擎** > **基于云的保护** > **提交样本**，然后单击**排除**旁边的**编辑**。添加 .download.domain.com

最大样本大小(MB) – 定义自动提交的样本的最大大小1-64 MB

基于云的防护的排除过滤器

排除过滤器允许您不提交某些文件或文件夹样本。列出的文件即使包含可疑代码也不会发送给 ESET 实验室以供分析。默认情况下常见文件类型（例如 doc 等）均被排除。

此功能对将可能包含机密信息的文件（例如文档或电子表格）排除在外很有用。

要排除从 download.domain.com 下载的文件，请依次单击高级设置 > **检测引擎** > **基于云的防护** > **提交样本** > **排除**，然后添加排除 *download.domain.com*

恶意软件扫描

可从高级设置 > **检测引擎** > **恶意软件扫描**访问**恶意软件扫描**部分，并允许您为扫描配置文件配置扫描参数。

手动扫描

选定的配置文件 – 手动扫描程序使用的一组特定参数。若要创建新配置文件，请单击**配置文件列表**旁边的**编辑**。有关更多详细信息，请参阅扫描配置文件

在选择扫描配置文件后，可以配置以下选项：

扫描目标 – 如果要扫描特定目标或一组目标，请单击**扫描目标**旁边的**编辑**，然后从文件夹（树）结构中选择一个选项。有关更多详细信息，请参阅扫描目标

手动和机器学习保护 – 可以为每个扫描配置文件配置报告和保护级别。默认情况下，扫描配置文件使用与在文件系统实时防护中定义的相同设置。禁用**使用实时防护设置**旁边的开关，以配置自定义报告和保护级别。有关报告和保护级别的详细说明，请参阅保护

ThreatSense – 高级设置选项，如要控制的文件扩展名和使用的检测方法。有关详细信息，请参阅 ThreatSense

扫描配置文件

ESET NOD32 Antivirus 中有 4 个预定义的扫描配置文件：

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

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

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

- **计算机扫描** – 这是标准计算机扫描中使用的默认配置文件。

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

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

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

扫描目标

扫描目标下拉菜单让您可以选择预定义的扫描目标。

- **按配置文件设置** – 选择由选定的扫描配置文件指定的目标。
- **可移动磁盘** – 选择磁盘、USB 存储设备和 CD/DVD。

- **本地驱动器** – 选择所有系统硬盘。

- **网络驱动器** – 选择所有映射的网络驱动器。

- **自定义选择** – 取消之前所有的选择。

文件夹（树）结构还包含特定扫描目标。

- **系统内存** – 扫描当前由系统内存使用的所有进程和数据。

- **引导区/UEFI** – 扫描引导区和 UEFI 以查找是否存在恶意软件。在词汇表中阅读有关 UEFI 扫描程序的更多信息。

- **WMI 数据库** – 扫描整个 Windows Management Instrumentation (WMI) 数据库、所有命名空间、所有类实例和所有属性。搜索对被感染文件或嵌入为数据的恶意软件的引用。

- **系统注册表** – 扫描整个系统注册表、所有注册表项和子项。搜索对被感染文件或嵌入为数据的恶

意软件的引用。清除检测时，引用会保留在注册表中，以确保不会丢失重要数据。

要快速导航到扫描目标（文件或文件夹），请在树形结构下方的文本字段中键入其路径。该路径区分大小写。要将目标包括在扫描中，请在树形结构中选中其复选框。

空闲状态下扫描

可以在高级设置 > **检测引擎** > **恶意软件扫描** > **空闲状态扫描**中，启用处于空闲状态的扫描程序。

空闲状态下扫描

启用**启用空闲状态下扫描**旁边的开关，以启用此功能。当计算机处于空闲状态时，将在所有本地驱动器上执行静默计算机扫描。

默认情况下，当计算机（笔记本）使用电池电量运行时，系统不会运行处于空闲状态的扫描程序。可以通过在“高级设置”中启用**计算机使用蓄电池供电时仍然运行扫描**旁边的滑块，来覆盖此设置。

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

空闲状态检测

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

ThreatSense – 高级设置选项，如要控制的文件扩展名和使用的检测方法。有关详细信息，请参阅 ThreatSense。

空闲状态检测

可以在高级设置 > **检测引擎** > **恶意软件扫描** > **空闲状态下扫描** > **空闲状态下检测**中，配置空闲状态下检测设置。这些设置为以下情况下的空闲状态下扫描指定触发器：

- **关闭屏幕或屏幕保护程序**
- **计算机锁定**
- **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。

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检测引擎更新期间执行。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。要修改其设置，请导航到**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。有关计划任务创建和管理的详细说明，请参见创建新任务。

ThreatSense – 高级设置选项，如要控制的文件扩展名和使用的检测方法。有关详细信息，请参阅 ThreatSense。

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）。

要扫描的文件列表对于上面的每个组都是固定的。如果为系统启动时运行的文件选择较低的扫描深度，则未扫描的文件将在打开或执行时进行扫描。

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。

可移动磁盘

将可移动磁盘 (CD/DVD/USB/...) 插入计算机时，ESET NOD32 Antivirus 会自动对其进行扫描。如果计算机管理员希望防止用户使用带有不请自来内容的可移动磁盘，此模块可能很有用。

在插入可移动磁盘并在高级设置 > **检测引擎** > **恶意软件扫描** > **可移动磁盘**中设置**显示扫描选项**后，将显示以下对话框：

用于此对话框的选项：

- **立即扫描** – 这将触发对可移动磁盘的扫描。
- **不扫描** – 将不会扫描可移动磁盘。
- **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 NOD32 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。

要访问可移动磁盘扫描的设置，请打开高级设置 > **检测引擎** > **恶意软件扫描** > **可移动磁盘**。

插入可移动磁盘后要采取的操作 – 选择将可移动磁盘设备 (CD/DVD/USB) 插入到计算机时将执行的默认操作。选择在将可移动磁盘插入计算机时的所需操作：

- **不扫描** – 将不执行任何操作，并且不打开**检测到新设备**窗口。
- **自动设备扫描** – 将执行已插入可移动磁盘设备的计算机扫描。
- **显示扫描选项** – 打开**可移动磁盘**设置部分。

文档防护

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

要激活文档防护，请打开高级设置 > **检测引擎** > **恶意软件扫描** > **文档防护**，然后单击**启用文档防护**旁边的开关。

ThreatSense – 高级设置选项，如要控制的文件扩展名和使用的检测方法。有关详细信息，请参阅 ThreatSense。

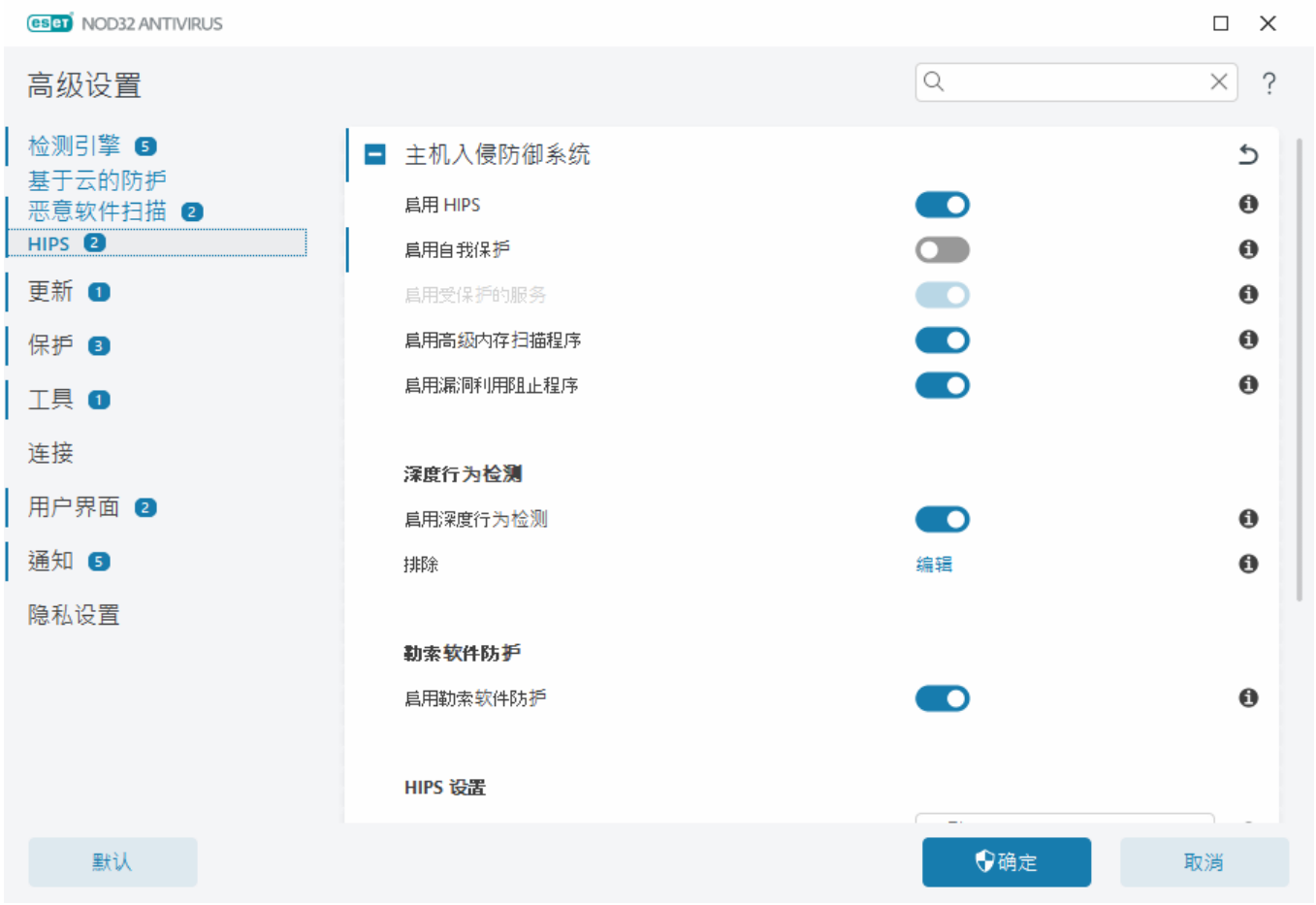
> 此功能由使用 Microsoft Antivirus API 例如 Microsoft Office 2000 及更高版本或 Microsoft Internet Explorer 5.0 及更高版本）的应用程序激活。

HIPS – 主机入侵防御系统

⚠ 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。

可以在高级设置 > **检测引擎** > **HIPS** > **HIPS** 中，配置 HIPS 设置。HIPS 状态（已启用/已禁用）显示在 ESET NOD32 Antivirus 的主程序窗口 > **设置** > **计算机保护**中。



主机入侵防御系统

启用 HIPS – 在 ESET NOD32 Antivirus 中，默认启用 HIPS。关闭 HIPS 会禁用其余 HIPS 功能（如漏洞利用阻止程序）。

启用自我防御 - ESET NOD32 Antivirus 使用内置的**自我防御**技术作为 HIPS 的一部分，来防止恶意软件损坏或禁用病毒和间谍软件防护。自我保护可保护关键系统及 ESET 的进程、注册表项和文件免于遭篡改。

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

启用高级内存扫描程序 – 与漏洞利用阻止程序结合使用以增强对恶意软件的防范，后者旨在通过迷惑或加密方法来逃过反恶意软件产品的检测。默认情况下，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。

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

深度行为检测

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

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

勒索软件防护

启用勒索软件防护是作为 HIPS 功能的一部分工作的另一层保护。必须启用 ESET LiveGrid® 信誉系统才能使勒索软件防护工作。请阅读有关此类防护的更多信息

启用 Intel® Threat Detection Technology – 利用独特的 Intel CPU 遥测技术来帮助检测勒索软件攻击，以提高检测效率、降低误报警报以及扩展可见性来捕获高级规避技术。查看支持的处理器

HIPS 设置

可以使用以下模式之一执行**过滤模式**

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

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

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

HIPS 排除

排除使您能够从 HIPS 深度行为检测排除进程。

要编辑 HIPS 排除，请打开高级设置 > **检测引擎** > **HIPS** > **HIPS** > **排除** > **编辑**

请勿混淆排除的文件扩展名检测排除性能排除或进程排除

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

HIPS 高级设置

以下选项用于调试和分析应用程序的行为：

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

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

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

始终允许加载驱动程序

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

添加 – 添加新驱动程序。

编辑 – 编辑选定的驱动程序。

删除 – 从列表中删除驱动程序。

重置 – 重新加载一组系统驱动程序。

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

安装后，驱动程序列表会为空ESET NOD32 Antivirus 会随时间推移自动填写该列表。

HIPS 交互窗口

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

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

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

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

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

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

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

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

循环显示 HIPS 通知？
要停止显示通知，请在高级设置 > **检测引擎** > **HIPS** > **HIPS** 中，将过滤模式更改为**自动**

学习模式已结束

学习模式会自动创建并保存规则。您可以在 HIPS 规则设置中检查所有已创建的规则。此模式非常适合用于 HIPS 的初始配置，但只能保持较短时间。不需要用户交互，因为 ESET NOD32 Antivirus 会根据预先定义的参数保存规则。在创建了操作系统中运行的所需进程的所有规则后，切换到**交互式**或**基于策略的模式**，以避免安全风险。

如果您不想更改设置，可以推迟此决定。

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。可以选择**拒绝**或**允许**操作。

单击**详细信息**可查看特定检测参数。该对话框窗口让您可以**提交以供分析**或**从检测中排除**。

必须启用 ESET LiveGrid®才能使勒索软件防护正常工作。

HIPS 规则管理

用户定义和从 HIPS 系统自动添加的规则列表。有关规则创建和 HIPS 操作的更多详细信息，请参阅 HIPS 规则设置。另请参阅 HIPS 的一般原则。

列

规则 – 用户定义的或自动选择的规则名称。

已启用 – 如果要将规则保留在列表中但不想使用，请禁用该滑块。

操作 – 该规则指定条件正确的情况下应执行的一项操作：**允许**、**阻止**或**询问**。

源 – 仅当事件由应用程序触发时才使用该规则。

目标 – 仅当操作与特定文件、应用程序或注册表项相关时才使用该规则。

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

通知 – 如果触发事件，右下角会显示一个小通知窗口。

控件元素

添加 – 创建一个新规则。

编辑 – 使您能够编辑选定的条目。

删除 – 删除选定条目。

HIPS 规则的优先级

没有使用最上/最下按钮调整 HIPS 规则优先级的选项。

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

编辑 HIPS 规则

首先查看 HIPS 规则管理

规则名称 – 用户定义的或自动选择的规则名称。

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

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

已启用 – 如果要将规则保留在列表中但不应用它，请禁用该开关。

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

通知用户 – 如果触发事件，右下角会显示一个小通知窗口。

该规则包含以下部分，它们描述了触发使用此规则的条件：

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

目标文件 – 仅当操作与此目标相关时才使用该规则。从下拉菜单中选择**特定文件**，然后单击**添加**以添加新文件或文件夹，或者可以从下拉菜单中选择**所有文件**以添加所有文件。

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

注册表条目 – 仅当操作与此目标相关时才使用该规则。从下拉菜单中选择**特定条目**，并单击**添加**以手动键入它，或者可以单击**打开注册表编辑器**以从注册表中选择某项。此外，可以从下拉菜单中选择**所有项**以添加所有应用程序。

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

重要操作的说明：

文件操作

- **删除文件** – 应用程序要求获得删除目标文件的权限。
- **写入到文件** – 应用程序要求获得写入目标文件的权限。
- **直接访问磁盘** – 应用程序尝试以绕过常见 Windows 过程的非标准方式读取或写入磁盘。这可能导致修改文件而不应用相应规则。尝试回避检测的恶意软件、尝试精确复制磁盘的备份软件或者尝试重新组织磁盘卷的分区管理器都可能导致此操作。
- **安装全局挂钩** – 指从 MSDN 库调用 SetWindowsHookEx 函数。
- **加载驱动程序** – 在系统上安装和加载驱动程序。

应用程序操作

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

注册表操作

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

在输入目标时，可以使用带有某些限制的通配符。注册表路径中可以使用 *（星号）符号代替特定键。例如，*HKEY_USERS*\software* 可以表示 *HKEY_USER\.default\software*，但不是 *HKEY_USERS\S-1-2-21-2928335913-73762274-491795397-7895\.default\software*。*HKEY_LOCAL_MACHINE\system\ControlSet** 不是有效的注册表项路径。注册表键路径具有 *，表示“此路径，或在该符号后的任意级别的任意路径”。这是为文件目标使用通配符的唯一方式。首先，将评估路径的特定部分，然后是通配符符号（*）后的路径。

如果创建了太笼统的规则，将会显示关于此类规则的警告。

在以下示例中，我们将演示如何限制不需要的特定应用程序行为：

1. 命名规则，并从**操作**下拉菜单中选择**阻止**（或**询问**，如果想要稍后选择）。
2. 启用**通知用户**旁边的滑块以在每次应用规则时显示通知。
3. 在**操作影响**部分中，为将应用的规则选择至少一项操作。

4. 单击**下一步**。

5. 在**源应用程序**窗口中，从下拉菜单中选择**特定应用程序**，以将新规则应用于尝试在指定的应用程序上执行任何选定的应用程序操作的所有应用程序。

6. 单击**添加**，单击 **...** 以选择特定应用程序的路径，然后按**确定**。添加更多应用程序（如果需要）。例如： *C:\Program Files (x86)\Untrusted application\application.exe*

7. 选择**写入文件**操作。

8. 从下拉菜单中选择**所有文件**。这将阻止上一步中选定应用程序写入任何文件的任何尝试。

9. 单击**完成**保存新规则。

为 HIPS 添加应用程序/注册表路径

通过单击**...**选项，选择文件应用程序路径。如果选择了文件夹，则位于此位置的所有应用程序都将包括在内。

打开注册表编辑器选项将启动 Windows 注册表编辑器 (regedit)。当添加注册表路径时，将正确的位置输入到**值**字段中。

以下是文件或注册表路径的示例：

- *C:\Program Files\Internet Explorer\iexplore.exe*

- *HKEY_LOCAL_MACHINE\system\ControlSet*

更新

在高级设置 > **更新**中，提供了更新设置选项。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。

更新

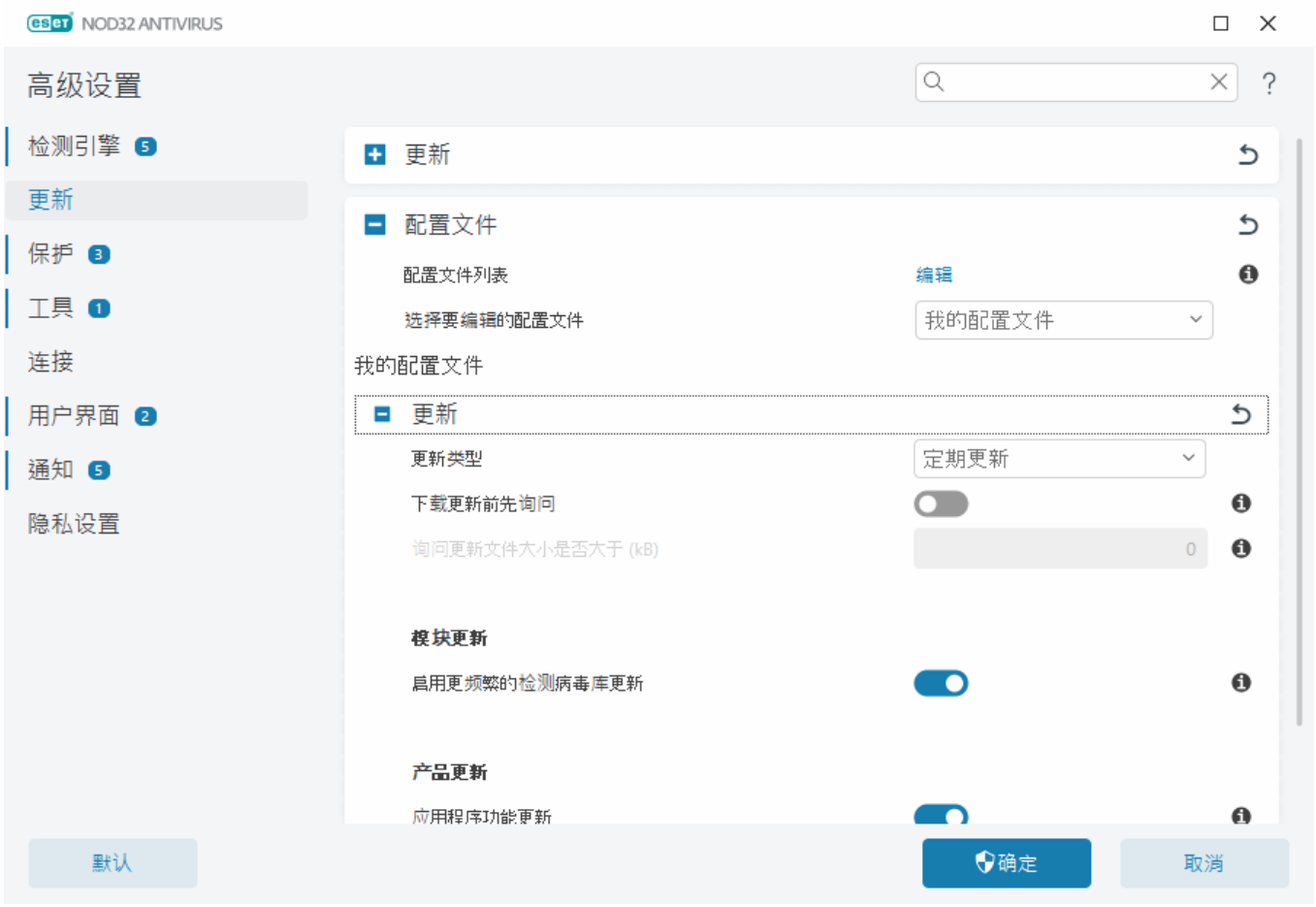
当前使用的更新配置文件显示在**选择默认更新配置文件**下拉菜单中。

若要创建新的配置文件，请参阅更新配置文件部分。

如果在尝试下载检测引擎和模块更新时遇到问题，请单击**清除更新缓存**旁边的**清除**，以清除临时更新文件/缓存。

模块回滚

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



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

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

选择要编辑的配置文件下拉菜单显示当前选定的配置文件，默认设置为**我的配置文件**。若要创建新的配置文件，请单击**配置文件列表**旁边的**编辑**，输入您自己的**配置文件名称**，然后单击**添加**。

更新

默认情况下，**更新类型**设置为**定期更新**，以确保更新文件将以最小的网络流量从ESET服务器自动进行下载。预发布更新（**预发布更新**选项）是已经经过内部彻底测试的更新，将很快公开提供。您可以通过获得最新检测方法和修补程序，从启用预发布更新中获益。但是，预发布更新可能并不始终稳定，不得在需要最大程度可用性和稳定性的生产服务器和工作站上使用。

下载更新前询问 – 程序将显示一条通知，可以在其中选择确认还是拒绝更新文件下载。

询问更新文件大小是否大于(kB) – 如果更新文件大小大于指定的值，程序将显示确认对话框。如果更新文件大小设置为 0 kB，则程序将始终显示确认对话框。

模块更新

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

产品更新

应用程序功能更新 – 自动安装新版本的 ESET NOD32 Antivirus。

连接选项

若要使用代理服务器下载更新，请参阅连接选项部分。

更新回滚

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

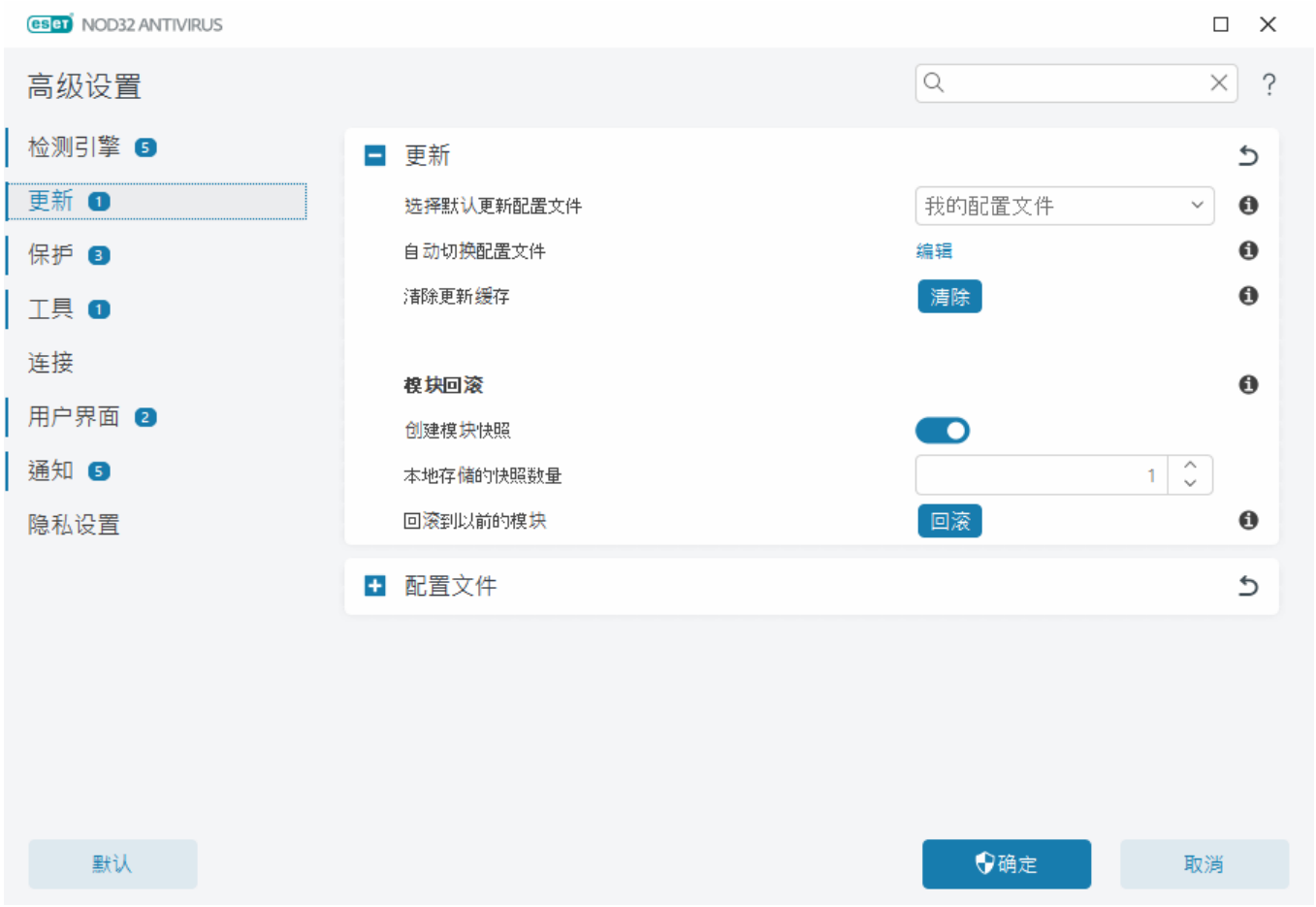
ESET NOD32 Antivirus 会记录检测引擎和程序模块的快照，以用于回滚功能。要创建病毒库快照，请保持**创建模块快照**处于启用状态。如果**创建模块快照**已启用，则会在第一次更新期间创建第一个快照。将在 48 小时后创建下一个快照。**本地存储的快照数量**字段定义了存储的先前检测引擎快照的数量。

> 当达到最大快照数量（例如，三个）时，最旧的快照将每 48 小时替换为新的快照。ESET NOD32 Antivirus 会将检测引擎和程序模块更新版本回滚至最旧的快照。

如果在高级设置 > **更新** > **更新**中单击**回滚**，则必须从**持续时间**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长。

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。由于此选项存在潜在安全风险，因此 ESET 不建议选择它。

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



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

回滚时间间隔

如果在高级设置 > **更新** > **更新**中单击**回滚**，则必须从**持续时间**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长。

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。由于此选项存在潜在安全风险，因此 ESET 不建议选择它。

产品更新

通过**产品更新**部分，可以自动安装可用的新功能更新。

应用程序功能更新会引入新功能，或更改以前版本中已经存在的功能。可以无需用户介入而自动执行更新，也可以选择获取通知。在应用程序功能更新安装完毕后，可能需要重新启动计算机。

应用程序功能更新 – 启用后，将自动执行应用程序功能更新。

连接选项

要访问特定更新配置文件的代理服务器设置选项，请打开高级设置 > **更新** > **配置文件** > **更新** > **连接选项**。单击**代理模式**下拉菜单，然后选择以下三个选项之一：

- 不使用代理服务器
- 通过代理服务器连接
- 使用全局代理服务器设置

选择**使用全局代理服务器设置**，以使用在高级设置 > **连接** > **代理服务器**中已指定的代理服务器配置。

选择**不使用代理服务器**可指定不使用代理服务器来更新 ESET NOD32 Antivirus。

在以下情况下应选择**通过代理服务器连接**选项：

- 将使用不同于在高级设置 > **连接**中定义的代理服务器来更新 ESET NOD32 Antivirus。在此配置中，应在**代理服务器**地址中指定新代理的信息、通信**端口**（默认为 3128）以及代理服务器的**用户名**和**密码**（如果需要）。

- 代理服务器设置不会全局设置，但 ESET NOD32 Antivirus 将连接到代理服务器以进行更新。

- 您的计算机通过代理服务器连接到 Internet。这些设置是在安装程序时从 Internet Explorer 获取的，但是如果设置发生更改（例如，如果您更改 ISP）。请确保在此窗口中列出的代理设置正确。否则程序将无法连接到更新服务器。

代理服务器的默认设置为**使用全局代理服务器设置**。

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

此部分中的**用户名**和**密码**字段特定于代理服务器。仅当访问代理服务器需要用户名和密码时，才填写这些字段。仅当知道需要密码才能通过代理服务器访问 Internet 时，才应该填写这些字段。

保护

保护功能通过控制文件、电子邮件和 Internet 通信来防范恶意系统攻击。例如，如果检测到归类为恶意软件的对象，将开始消除。保护功能可以通过阻止它，然后清除、删除或将其移至隔离区来消除威胁。

要详细地配置保护功能，请打开高级设置 > **保护**。

应该仅由有经验的用户来更改保护。对设置的错误配置可能会导致系统不稳定。

在本部分中：

- 检测响应
- 报告设置
- 防护设置

检测响应

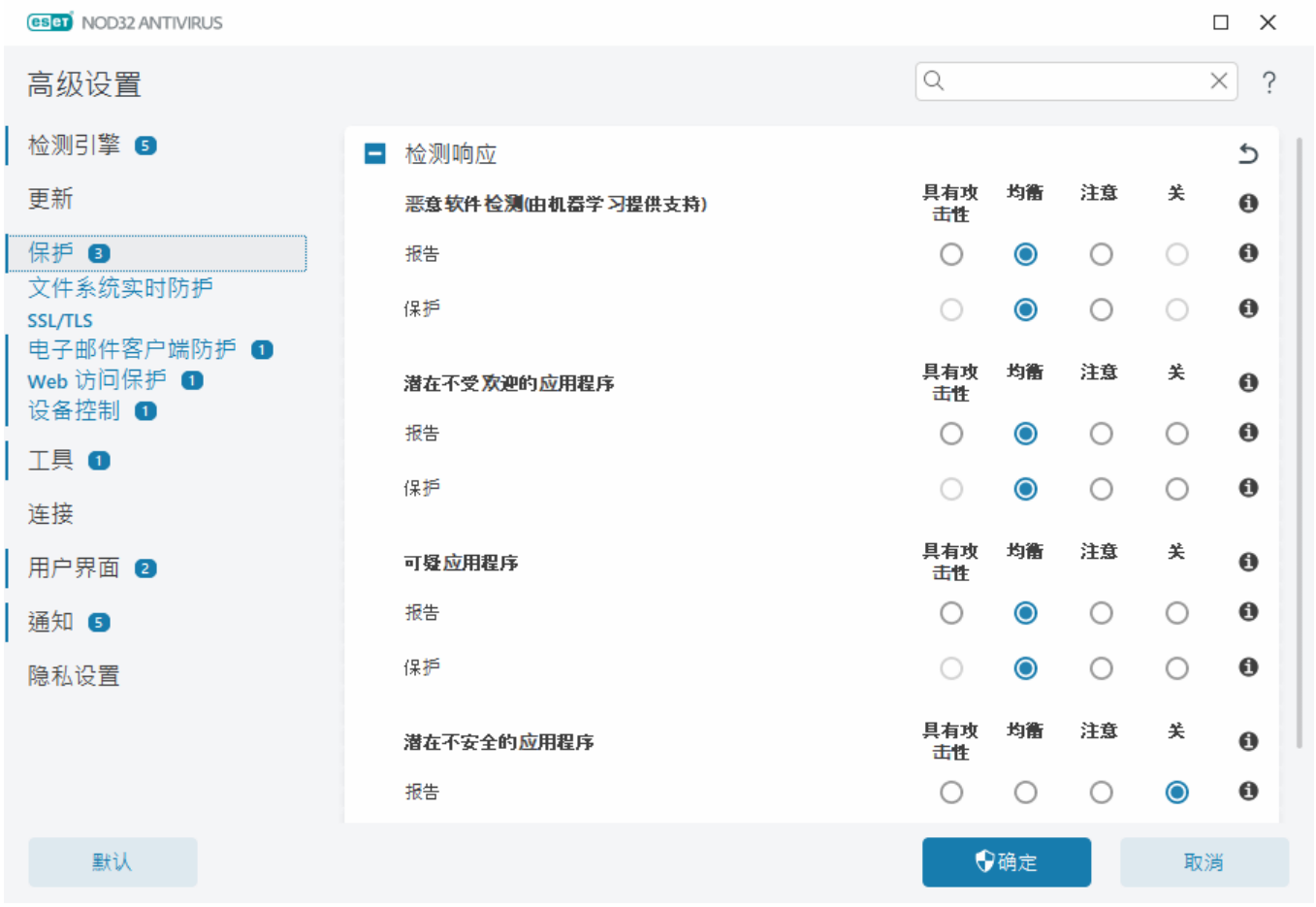
检测响应使您能够为以下类别配置报告和保护级别：

- **恶意软件检测（由机器学习提供支持）** – 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。但是，术语“病毒”经常被误用。“恶意软件”（恶意的软件）是更准确的术语。恶意软件检测由结合了机器学习组件的检测引擎模块执行。请在词汇表中阅读有关这些类型的应用程序的更多信息。

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

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



改进的防护

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

报告设置

当发生检测时（例如，发现威胁和归类为恶意软件），信息将记录到检测日志，如果在 ESET NOD32 Antivirus 中进行了配置，将发生桌面通知。

为每个类别（作为“CATEGORY”引用）配置报告阈值：

1.恶意软件检测

2.潜在不受欢迎的应用程序

3.潜在不安全

4.可疑应用程序

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

为 CATEGORY 报告修改阈值（或级别）前阅读以下内容：

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

ESET NOD32 Antivirus 防护模块的可用性

对于选定的CATEGORY阈值，防护模块的可用性（已启用或已禁用）如下：

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

*不建议。

确定产品版本、程序模块版本和内部版本日期

1. 单击**帮助和支持** > **关于 ESET NOD32 Antivirus**。
2. 在**关于**屏幕中，文本的第一行显示 ESET 产品的版本号。
3. 单击**已安装的组件**以访问关于特定模块的信息。

要点

为环境设置适当阈值的几项要点：

- 为大多数设置建议**均衡**阈值。
- 更高的报告阈值，更高的检测率，但错误识别对象的机会更高。
- 从真实世界角度来看，不能保证 100% 的检测率和 0% 的机会来避免错误地将干净对象归类为恶意软件。
- 保持 ESET NOD32 Antivirus 及其模块最新，以最大程度地保持性能、检测率的准确性与误报对象数量之间的平衡。

防护设置

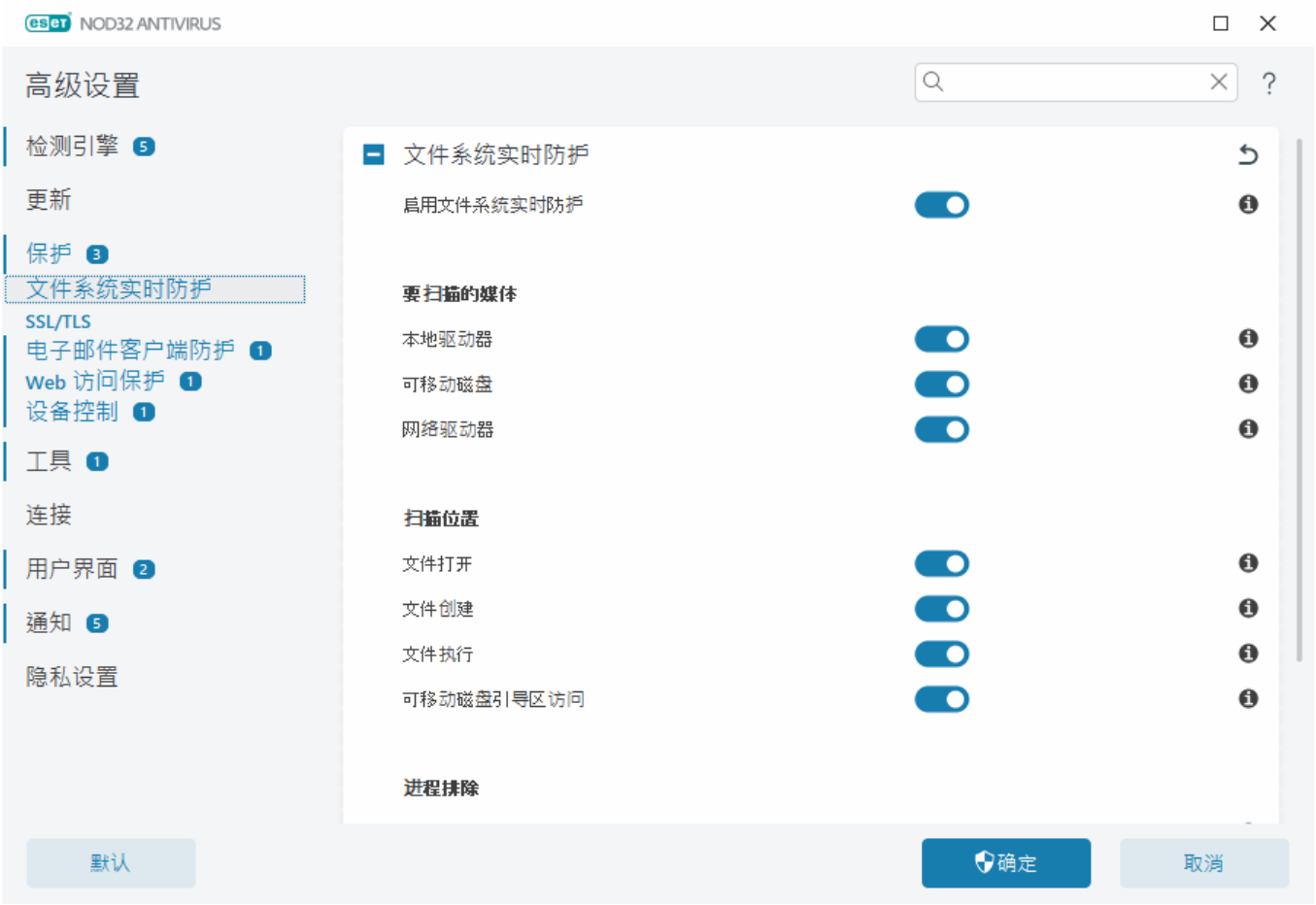
如果报告归类为 CATEGORY 的对象，程序会阻止该对象，然后对它清除、删除或将其移动到隔离区。

为 CATEGORY 保护修改阈值（或级别）前阅读以下内容：

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

文件系统实时防护

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



默认情况下，文件系统实时防护在系统启动时启动，并提供不间断的扫描。不建议您在高级设置 > **保护** > **文件系统实时防护** > **文件系统实时防护**中，禁用**启用文件系统实时防护**。

要扫描的介质

默认情况下，所有类型的介质均可扫描以检查是否存在潜在威胁：

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

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

扫描位置

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

- **文件打开** – 打开文件时扫描。
- **文件创建** – 扫描创建或修改的文件。
- **文件执行** – 执行或运行文件时扫描。
- **可移动磁盘引导区访问** – 将包含引导区的可移动磁盘插入设备时，系统将立即扫描引导区。此选项不会启动可移动磁盘文件扫描。可移动磁盘文件扫描功能位于**要扫描的磁盘** > **可移动磁盘**。为了使**可移动磁盘引导区访问**能够正常工作，请在 ThreatSense 中保持启用**引导区/UEFI**

进程排除

请参阅进程排除

ThreatSense

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 中所述），文件系统实时防护可以配置为以不同于现有文件的方式处理新创建的文件。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）。在每次检测引擎更新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，请打开高级设置 > **保护** > **文件系统实时防护**。依次单击 **ThreatSense** > **其他**，然后选中或取消选中**启用智能优化**

文件系统实时防护还允许您配置其他 ThreatSense 参数

进程排除

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

请勿混淆排除的文件扩展名HIPS 排除检测排除或性能排除

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

可以在高级设置 > **保护** > **文件系统实时防护** > **文件系统实时防护** > **进程排除**中，将可执行文件添加到已排除进程的列表中。

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

单击**编辑**以打开**进程排除**管理窗口，可以在其中添加排除并浏览至将从扫描中排除的可执行文件（例如 *Backup-tool.exe*）。
在将 *.exe* 文件添加到排除中后，ESET NOD32 Antivirus 不会监控此进程的活动，也不会对此进程执行的任何文件操作进行扫描。

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

还可以在排除中**编辑**现有进程或**删除**它们。

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

添加或编辑进程排除

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

通过单击 ...，选择例外应用程序的文件路径（例如 *C:\Program Files\Firefox\Firefox.exe*）。请勿键入应用程序的名称。
在将 *.exe* 文件添加到排除中后，ESET NOD32 Antivirus 不会监控此进程的活动，也不会对此进程执行的任何文件操作进行扫描。

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

还可以在排除中**编辑**现有进程或**删除**它们。

何时修改实时防护配置

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

安装 ESET NOD32 Antivirus 后，所有设置都会得到优化以便为用户提供最高级别的系统安全性。要恢复默认设置，请依次单击高级设置 > **保护** > **检测响应**旁边的 。

检查实时防护

要验证实时防护是否工作并是否在检测病毒，请使用来自 *www.eicar.com* 的测试文件。此测试文件是一个可供所有病毒防护程序检测的无害文件。此文件由 EICAR 公司 (European Institute for Computer Antivirus Research) 创建，用于测试病毒防护程序的功能。

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

实时防护不工作时如何应对

在本章中，我们将介绍使用实时防护时可能出现的问题，以及如何排除这些故障。

实时防护被禁用

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

如果实时防护未能在系统启动时启动，通常是因为**启用文件系统实时防护**处于禁用状态。要确保此选项已启用，请打开高级设置 > **保护** > **文件系统实时防护**。

如果实时防护功能不检测和清除渗透

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

实时防护不启动

如果系统启动时实时防护未启动（且**启用文件系统实时防护**已经启用），可能是因为与其他程序发生冲突。要解决此问题，请创建 ESET SysInspector 日志并将其提交给 ESET 技术支持以供分析。

SSL/TLS

ESET NOD32 Antivirus 可以检查使用 SSL 协议的通信威胁。可以使用各种过滤模式检查证书受信任、证书未知或证书被从 SSL 保护通信检查中排除的 SSL 保护通信。要编辑 SSL/TLS 设置，请打开高级设置 > **保护** > **SSL/TLS**。

启用 SSL/TLS – 如果已禁用，则 ESET NOD32 Antivirus 不会扫描基于 SSL/TLS 的通信。

SSL/TLS 模式在以下选项中可用：

过滤模式	说明
自动	默认模式将仅扫描适当的应用程序，例如 Web 浏览器和电子邮件客户端。可以通过选择扫描通信的应用程序来覆盖它。
交互	如果您输入一个受 SSL 保护的新站点（使用未知证书），会显示操作选择对话框。此模式允许您创建将不扫描的 SSL 证书/应用程序列表。
基于策略	选择此选项可扫描所有受 SSL 保护的通信，除了由排除在检查之外的证书保护的通信。如果使用未知的、签署的证书建立了新通信，不会提示您，且通信将自动被过滤。使用标记为“受信任”的不受信任的证书访问服务器（该证书在“受信任的证书”列表中）时，允许与服务器进行通信，并过滤通信通道内容。

应用程序扫描规则 – 允许您自定义特定应用程序的 ESET NOD32 Antivirus 行为。

证书规则 – 允许您自定义特定 SSL 证书的 ESET NOD32 Antivirus 行为。

不扫描受 ESET 信任的域的通信 – 启用后，受信任域的通信将排除扫描⍰ESET 管理的内置白名单确定域的可信度。

将 ESET 根证书集成到受支持的应用程序中 – 要使 SSL 通信在您的浏览器/电子邮件客户端正常工作，请将 ESET 根证书添加到已知根证书（发布者）的列表中。启用后⍰ESET NOD32 Antivirus 会自动将 ESET SSL Filter CA 证书添加到已知浏览器（例如 Opera⍰⍰对于使用系统证书存储的浏览器，将自动添加该证书。例如⍰Firefox 自动配置为信任系统证书存储中的根颁发机构。

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。

无法建立证书信任时的操作 – 在某些情况下，无法使用受信任的根证书颁发机构 (TRCA) 存储来验证网站证书（例如，已到期的证书、不受信任的证书、对特定域无效的证书或可以解析但未正确对证书进行签名的签名）。合法网站将始终使用受信任的证书。如果它们没有提供受信任的证书，则可能意味着攻击者正在解密您的通信，或者网站遇到技术问题。

如果**询问证书有效性**处于选中状态（默认处于选中状态），则在建立加密通信时，系统会提示您选择一个操作。将显示一个操作选择对话框，可以在其中将证书标记为受信任或已排除。如果证书不存在于 TRCA 列表中，则窗口为红色。如果证书在 TRCA 列表中，则窗口将为绿色

可以选择**阻止使用该证书的通信**，以始终终止与使用不受信任的证书的站点进行加密连接。

阻止已过时的 SSL2 加密的通信 – 将自动阻止使用早期版本的 SSL 协议的通信。

适用于损坏证书的操作 – 损坏的证书意味着证书使用的格式无法由 ESET NOD32 Antivirus 识别，或收到时已损坏（例如，被随机数据覆盖）。在这种情况下，建议您将**阻止使用该证书的通信**保持处于选中状态。如果**询问证书有效性**处于选中状态，则在建立加密通信时，系统会提示用户选择一个操作。

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

应用程序扫描规则

可以使用**应用程序扫描规则**来自定义特定应用程序的 ESET NOD32 Antivirus 行为，并记住 **SSL/TLS 模式**处于**交互模式**下所选的操作。可以在高级设置 > **保护** > **SSL/TLS** > **应用程序扫描规则** > **编辑**中，查看和编辑该列表。

应用程序扫描规则窗口包括：

列

应用程序 – 从目录树中选择可执行文件，单击**...**选项或手动输入路径。

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 – 选择要配置的应用程序，然后单击**编辑**

删除 – 选择要删除的应用程序，然后单击**删除**

导入/导出 – 通过文件导入应用程序，或将当前应用程序列表保存到文件。

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**

证书规则

可以使用**证书规则**来自定义特定 SSL 证书的 ESET NOD32 Antivirus 行为，并记住 **SSL/TLS 模式**处于**交互模式**下所选的操作。可以在高级设置 > **保护** > **SSL/TLS** > **证书规则** > **编辑**中，查看和编辑该列表。

证书规则窗口包括：

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 – 添加新证书并调整其访问和扫描选项的相关设置。

编辑 – 选择您希望配置的证书，然后单击**编辑**。

删除 – 选择要删除的证书，然后单击**删除**。

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

加密的网络通信

如果您的系统配置为使用 SSL/TLS 扫描，则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 NOD32 Antivirus 配置为在此类情况下询问用户（默认情况下，无法验证的证书为“是”，无效的证书为“否”），将显示一个对话框询问您**允许**还是**阻止**该连接。如果证书不在 Trusted Root Certification Authorities store (TRCA) 中，则认为它不受信任。

其次，如果 **SSL/TLS 模式**设置为**交互模式**，则每个网站的对话框都将询问是要**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 NOD32 Antivirus 必须**忽略**该通信以保持应用程序正常工作。

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

在这两种情况下，用户可以选择记住选中的操作。保存的操作存储在证书规则中。

电子邮件客户端防护

要配置电子邮件客户端防护，请打开高级设置 > **保护** > **电子邮件客户端防护**，然后从以下配置选项中进行选择：

- 邮件传输防护
- 邮箱防护
- ThreatSense

邮件传输防护

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

无论使用何种电子邮件客户端，ESET NOD32 Antivirus 均提供对这些协议的保护，无需重新配置电子邮件客户端。默认情况下，将扫描通过 POP3 和 IMAP 协议的所有通信，无论默认的 POP3/IMAP 端口号是什么。不会扫描 MAPI 协议。但与 Microsoft Exchange 服务器的通信可以由电子邮件客户端（例如 Microsoft Outlook 中的集成模块扫描。

> ESET NOD32 Antivirus 还支持扫描 IMAPS (585, 993) 和 POP3S (995) 协议，这些协议使用加密通道在服务器和客户端之间传输信息。ESET NOD32 Antivirus 利用 SSL（安全套接字层）和 TLS（传输层安全）协议检查通信。
> 默认情况下，将扫描加密通信。要查看扫描程序设置，请打开高级设置 > **保护** > SSL/TLS

要配置邮件传输防护，请打开高级设置 > **保护** > **电子邮件客户端防护** > **邮件传输防护**。

启用邮件传输防护 – 启用后，ESET NOD32 Antivirus 将扫描邮件传输通信。

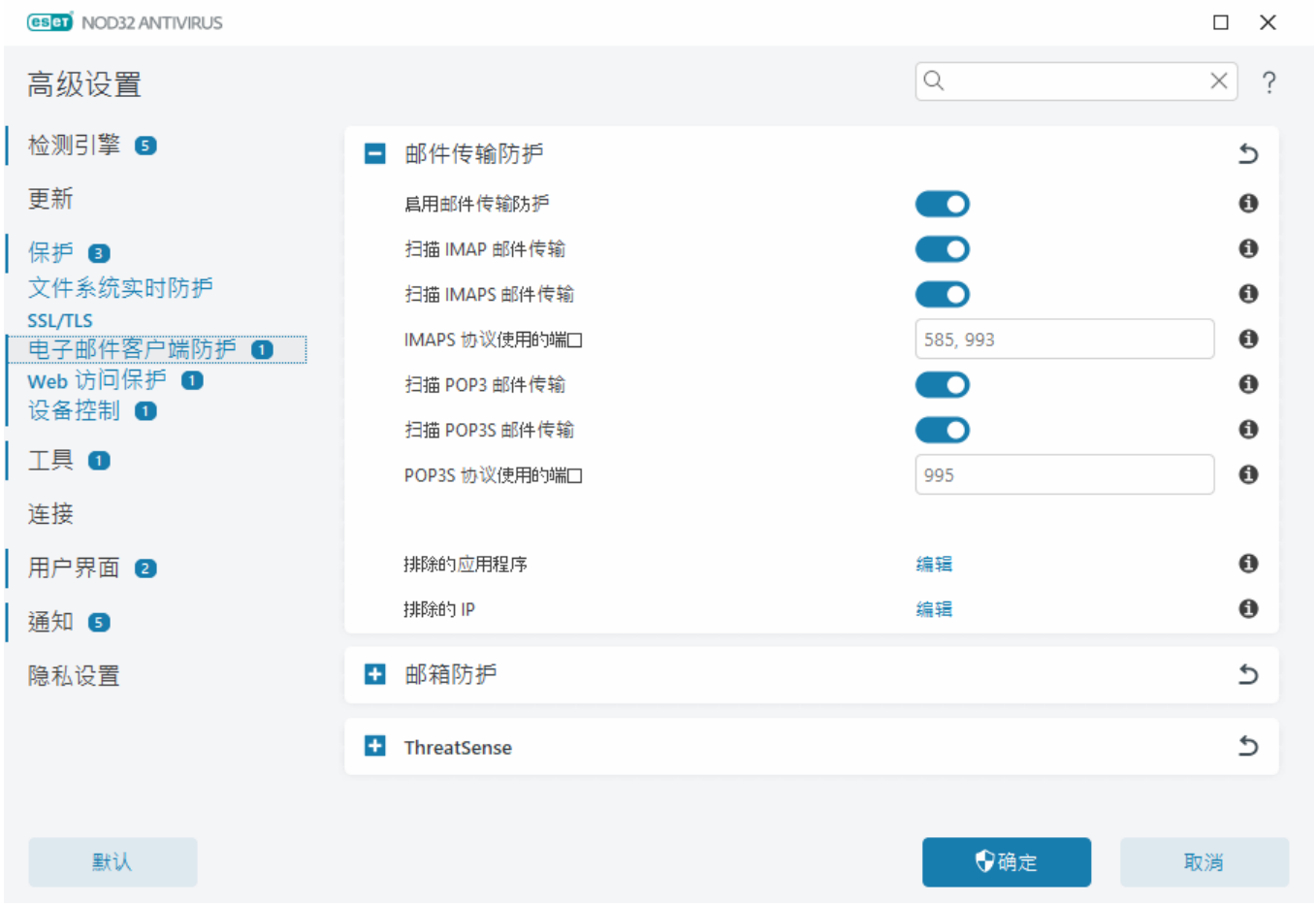
可以通过单击以下选项旁边的开关来选择将扫描的邮件传输协议（默认情况下，扫描所有协议处于启用状态）：

- **扫描 IMAP 邮件传输**
- **扫描 IMAPS 邮件传输**
- **扫描 POP3 邮件传输**
- **扫描 POP3S 邮件传输**

默认情况下，ESET NOD32 Antivirus 将扫描标准端口上的 IMAPS 和 POP3S 通信。要为 IMAPS 和 POP3S 协议添加自定义端口，请将它们添加到 **IMAPS 协议使用的端口**或 **POP3S 协议使用的端口**旁边的文本字段中。多个端口号必须使用逗号分隔。

排除的应用程序 – 使您能够将特定应用程序排除由邮件传输防护进行扫描。当 Web 访问保护导致出现兼容性问题时很有用。

排除的 IP – 使您能够将特定远程地址排除由邮件传输防护进行扫描。当 Web 访问保护导致出现兼容性问题时很有用。



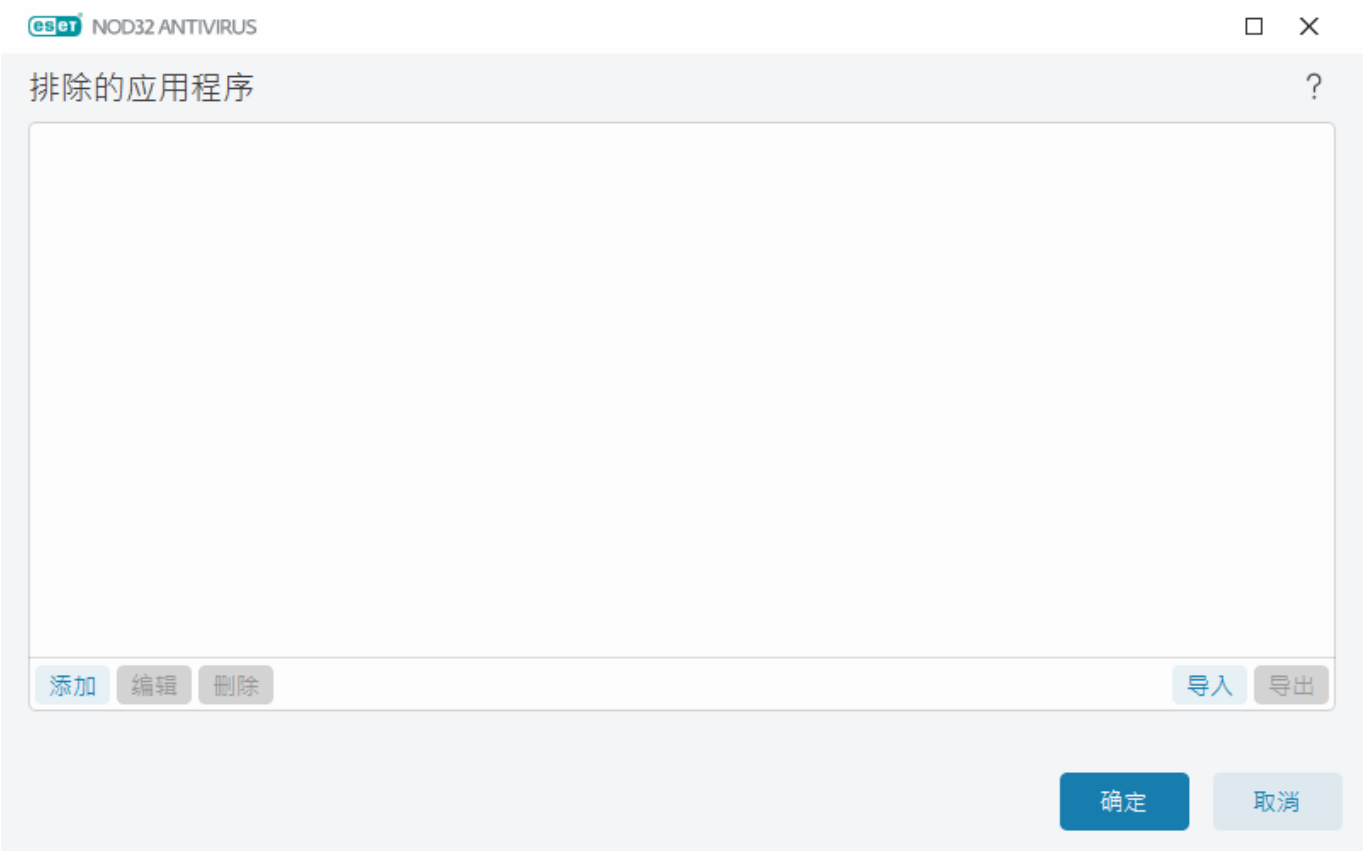
排除的应用程序

要排除扫描特定应用程序的通信，请将这些应用程序添加到列表中。将不检查选定应用程序的 HTTP(S)/POP3(S)/IMAP(S) 通信是否存在威胁。建议您仅将该操作用于在扫描通信时无法正常工作的应用程序。

当单击**添加**时，将在此处自动显示正在运行的应用程序和服务。单击 **...**，然后导航到要手动添加排除的应用程序。

编辑 – 编辑列表中的选定条目。

删除 – 删除列表中的选定条目。



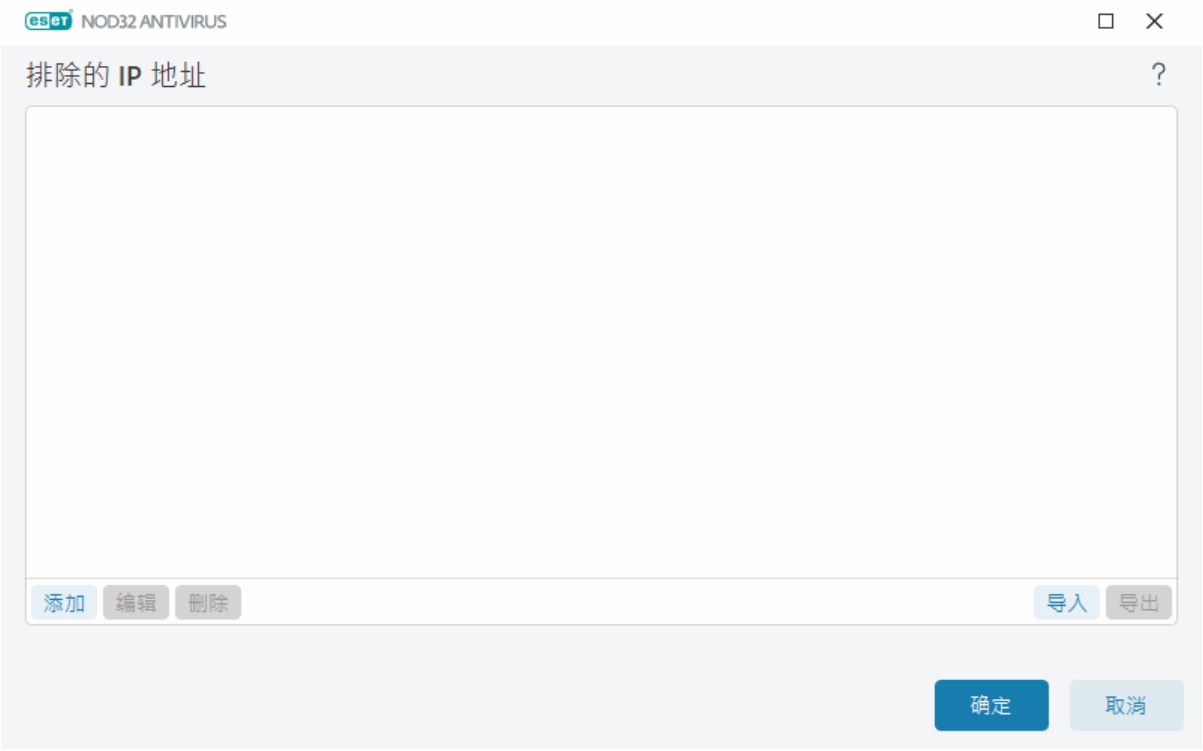
排除的 IP

列表中的条目将排除扫描。将不检查往返选定地址的 HTTP(S)/POP3(S)/IMAP(S) 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。

单击**添加**，以排除远程点的 IP 地址/地址范围/子网。

单击**编辑**，以更改选定的 IP 地址。

单击**删除**，以将选定条目从列表中删除。



IP 地址示例

添加 IPv4 地址：

单个地址 – 添加单个计算机的 IP 地址（例如，*192.168.0.10*）

地址范围 – 键入开始和结束 IP 地址，以指定多台计算机的 IP 范围（例如，*192.168.0.1-192.168.0.99*）

子网 – 子网（一组计算机）由 IP 地址和掩码定义。例如，255.255.255.0 是 192.168.1.0 子网的网络掩码。要排除整个子网，请键入 *192.168.1.0/24*

添加 IPv6 地址：

单个地址 – 添加单台计算机的 IP 地址（例如，*2001:718:1c01:16:214:22ff:fec9:ca5*）

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

邮箱防护

ESET NOD32 Antivirus 与邮箱的集成会提高针对电子邮件中恶意代码的主动防护级别。

要配置邮箱防护，请打开高级设置 > **保护** > **电子邮件客户端防护** > **邮箱防护**

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

选择要扫描的电子邮件：

- **已接收的电子邮件**
- **已发送的电子邮件**
- **已阅读的电子邮件**
- **已修改的电子邮件**

我们建议您将**通过客户端插件启用电子邮件保护**保持为启用。即使集成未启用或不起作用，电子邮件通信仍受邮件传输防护IMAP/IMAPS 和 POP3/POP3S保护。

附件处理优化 – 如果优化处于禁用状态，则会立即扫描所有附件。您可能会遇到电子邮件客户端性能下降。

集成 – 使您能够将邮箱防护集成到电子邮件客户端中。有关详细信息，请参阅集成。

响应 – 使您能够自定义垃圾邮件的处理方式。有关详细信息，请参阅响应。

集成

ESET NOD32 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 NOD32 Antivirus 中启用集成。当集成到电子邮件客户端时ESET NOD32 Antivirus 工具栏将直接插入电子邮件客户端，从而提供更高效的电子邮件防护。要编辑集成设置，请打开高级设置 > **保护** > **电子邮件客户端防护** > **邮箱防护** > **集成**。

集成到 Microsoft Outlook – Microsoft Outlook 是当前唯一受支持的电子邮件客户端。电子邮件防护以插件形式运行。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。有关受支持的 Microsoft Outlook 版本的完整列表，请参阅此 ESET 知识库文章。

高级电子邮件客户端处理 – 处理额外的 Outlook Messaging API (MAPI) 事件：对象已修改（`fnevObjectModified`）和对象已创建（`fnevObjectCreated`）。如果使用电子邮件客户端时遇到系统运行缓慢的情况，请禁用此选项。

Microsoft Outlook 工具栏

Microsoft Outlook 防护以插件模块形式运行。在安装 ESET NOD32 Antivirus 后，包含病毒防护的此工具栏选项会添加到 Microsoft Outlook。

ESET NOD32 Antivirus – 双击图标以打开 ESET NOD32 Antivirus 的主窗口。

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

扫描程序设置 – 显示邮箱保护设置选项。

确认对话框

此通知用于验证用户是否确实想执行所选操作，这将消除可能发生的错误。

另一方面，该对话框也提供禁用确认的选项。

重新扫描邮件

ESET NOD32 Antivirus 工具栏与电子邮件客户端集成在一起，使用户能指定若干电子邮件检查选项。**重新扫描邮件**选项提供两种扫描模式：

当前文件夹中的所有邮件 – 扫描当前显示的文件夹中的邮件。

仅选定的邮件 – 仅扫描由用户标记的邮件。

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

响应

根据邮件扫描结果ESET NOD32 Antivirus 可以移动扫描的邮件或向主题添加自定义文本。可以在高级设置 > **保护 > 电子邮件客户端防护 > 邮箱防护 > 响应**中，配置这些设置。

如果存在包含检测的邮件，则在默认情况下ESET NOD32 Antivirus 会尝试清除该邮件。如果无法清除邮件，则可以选择**无法清除时可采取的操作**

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

文件夹 – 指定希望将检测到的受感染电子邮件移到的自定义文件夹。

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

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

更新已接收和已阅读电子邮件的主题/更新已发送邮件的主题 – 启用此选项，可以将下面指定的自定义文本添加到邮件中。

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

ThreatSense

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

ThreatSense 引擎设置选项允许指定若干扫描参数：

- 要扫描的文件类型和扩展名
- 不同检测方法的组合
- 清除级别等

要进入设置窗口，请在高级设置中单击 **ThreatSense**，以显示任何使用 ThreatSense 技术的模块（见下文）。

不同的安全情形可能要求不同的配置。考虑到这一点，可针对下列防护模块对 ThreatSense 进行单独配置：

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

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

要扫描的对象

此部分使您可以定义要扫描的计算机组件和文件，以查找渗透。

系统内存 – 扫描攻击系统的系统内存的威胁。

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

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

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

自解压文件 – 自解压文件 (SFX) 是可提取自身的压缩文件。

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

扫描选项

选择在扫描系统中的渗透时所用的方法。以下选项可用：

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

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

清除

清理设置决定在清除对象时 ESET NOD32 Antivirus 的行为。共有 4 个清理级别：

ThreatSense 具有以下消除（即清除）级别：

ESET NOD32 Antivirus 中的修复

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

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 设置的此部分允许您定义要扫描的文件类型。

其他

当为手动计算机扫描配置 ThreatSense 引擎参数时，**其他**部分中的以下选项也可用：

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

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

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

启用智能优化 – 启用智能优化后，最优化的设置将用于确保最高效的扫描级别，同时保持最高的扫描速度。各种保护模块将进行智能化扫描，以便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，则在执行扫描时将仅在特定模块的 ThreatSense 核心中应用用户定义的设置。

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

限制

限制部分允许您指定要扫描的对象的最大大小和嵌套压缩文件的层数：

对象设置

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

对象的最长扫描时间(秒) – 定义扫描容器对象（例如 RAR/ZIP 压缩文件或附带多个附件的电子邮件）中文

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

压缩文件扫描设置

压缩文件嵌套层数 – 指定压缩文件扫描的最大深度。默认值：10

压缩文件中文件的最大大小 – 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。最大值为 **3 GB**

> 不建议更改默认值，正常情况下应该没有修改它的理由。

Web 访问保护

Web 访问保护允许您配置高级 Internet 防护模块设置。在高级设置 > **保护** > **Web 访问保护** > **Web 访问保护**中，提供了以下选项：

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

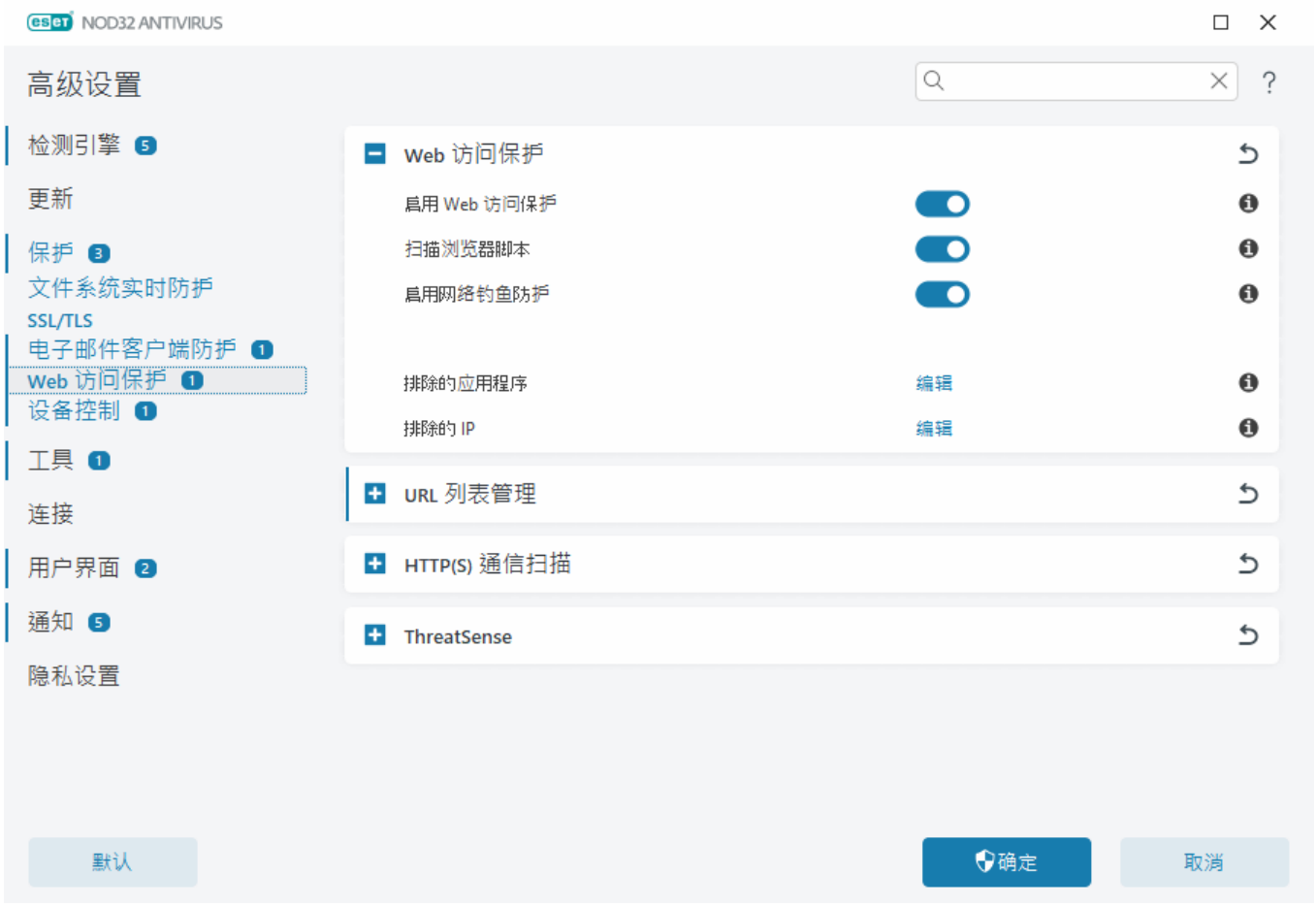
> 强烈建议您保持启用“Web 访问保护”，并在默认情况下不排除任何应用程序或 IP 地址。

扫描浏览器脚本 – 启用后，检测引擎会检查 Web 浏览器执行的所有 JavaScript 程序。

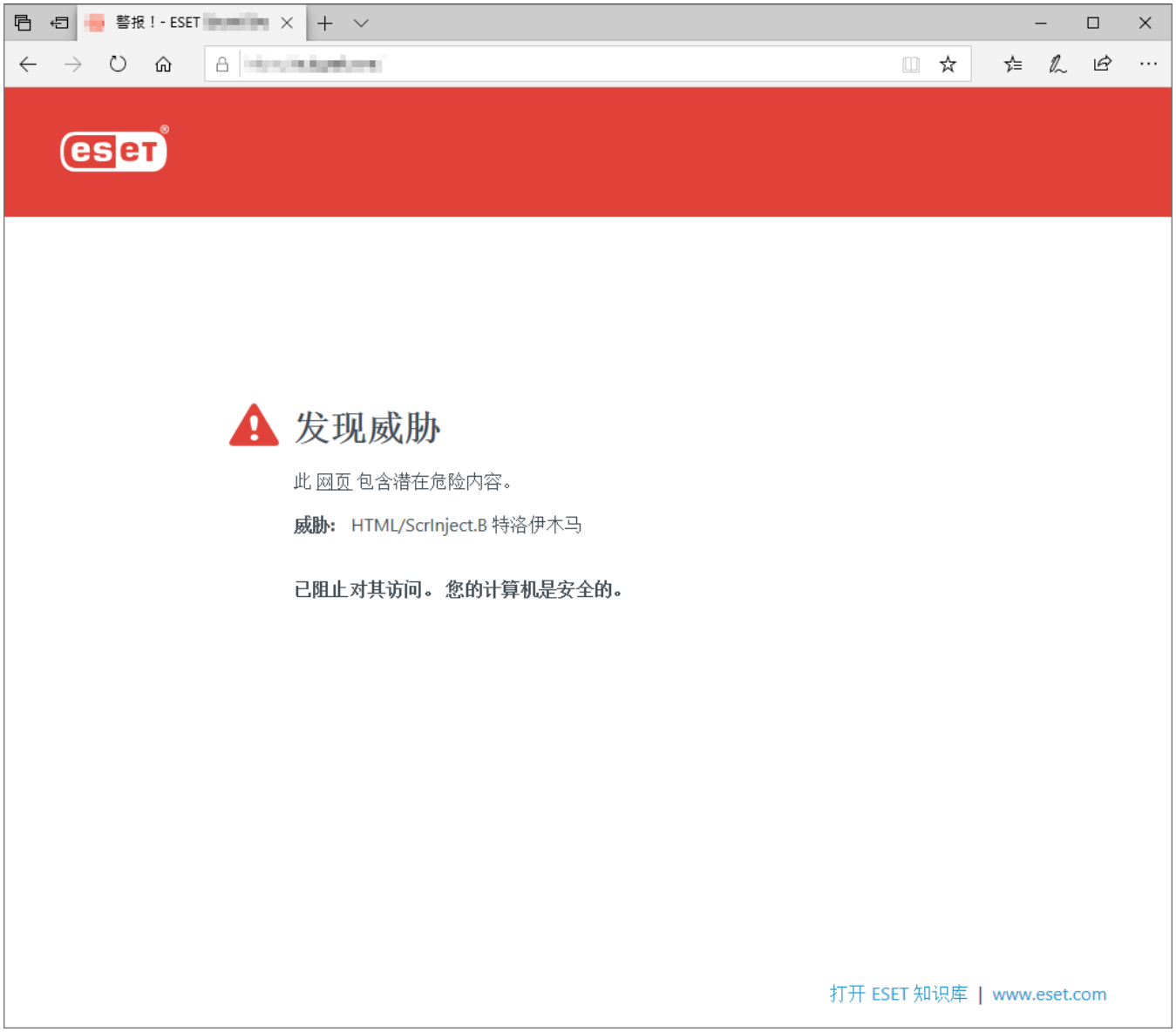
启用网络钓鱼防护 – 启用后，将阻止网络钓鱼网页。有关详细信息，请参阅网络钓鱼防护

排除的应用程序 – 使您能够将特定应用程序排除由 Web 访问保护进行扫描。当 Web 访问保护导致出现兼容性问题时很有用。

排除的 IP – 使您能够将特定远程地址排除由 Web 访问保护进行扫描。当 Web 访问保护导致出现兼容性问题时很有用。



当网站被阻止时Web 访问保护将在浏览器中显示以下消息：



图文并茂说明

以下 ESET 知识库文章可能仅提供英文版：

- 排除安全网站不受 Web 访问保护阻止
- 使用 ESET NOD32 Antivirus 阻止网站

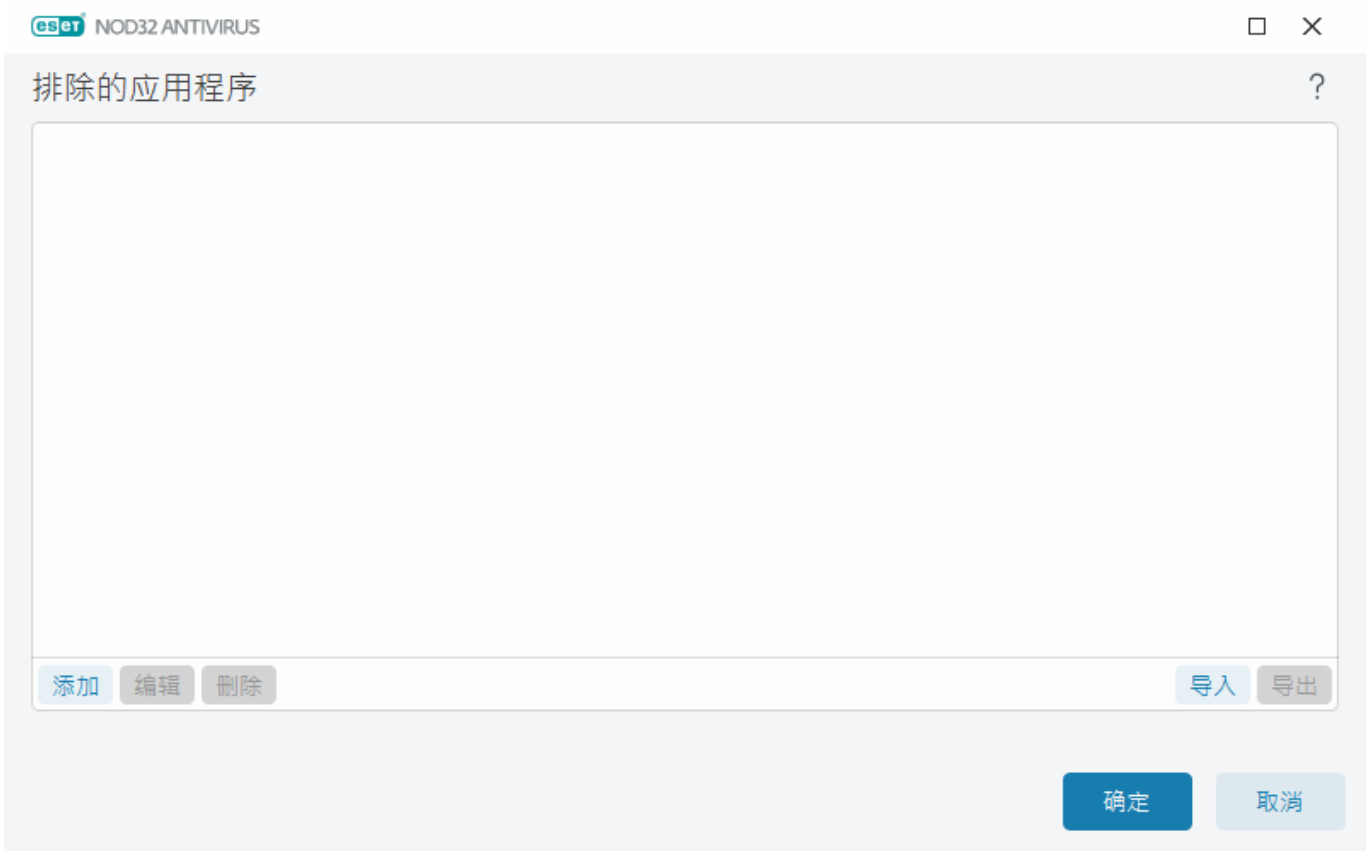
排除的应用程序

要排除扫描特定应用程序的通信，请将这些应用程序添加到列表中。将不检查选定应用程序的 HTTP(S)/POP3(S)/IMAP(S) 通信是否存在威胁。建议您仅将该操作用于在扫描通信时无法正常工作的应用程序。

当单击**添加**时，将在此处自动显示正在运行的应用程序和服务。单击 **...**，然后导航到要手动添加排除的应用程序。

编辑 – 编辑列表中的选定条目。

删除 – 删除列表中的选定条目。



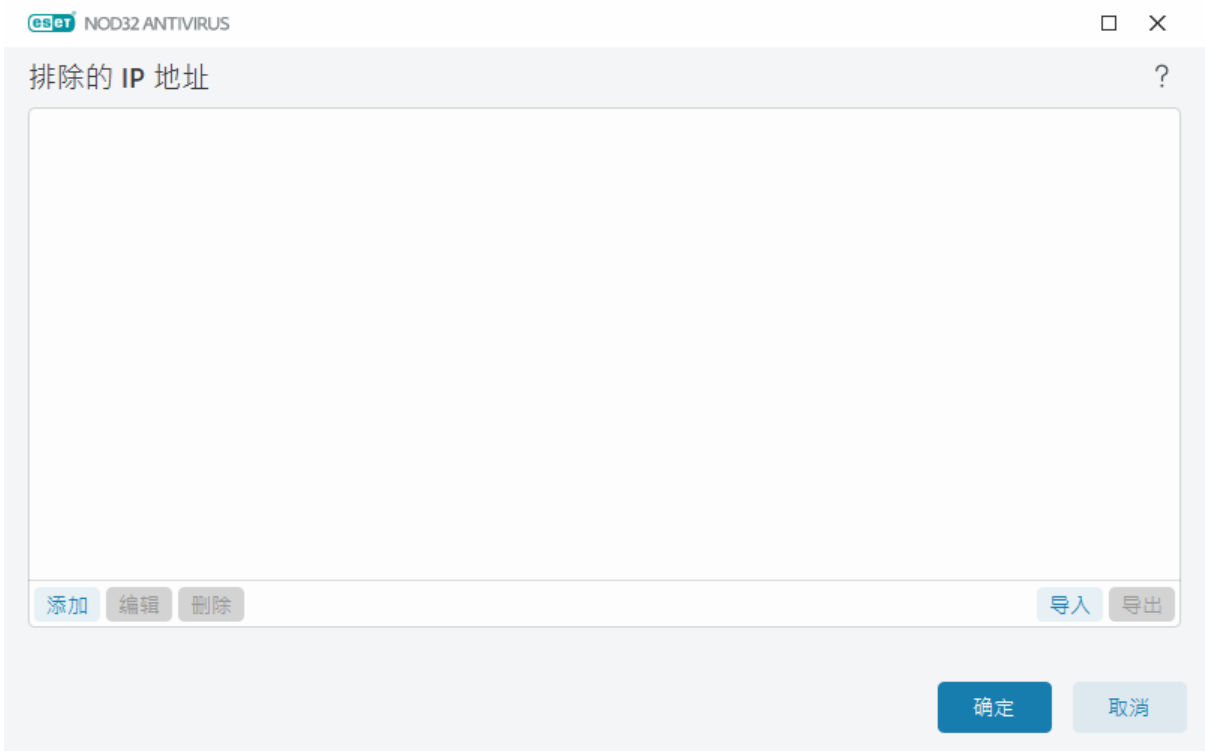
排除的 IP

列表中的条目将排除扫描。将不检查往返选定地址的 HTTP(S)/POP3(S)/IMAP(S) 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。

单击**添加**，以排除远程点的 IP 地址/地址范围/子网。

单击**编辑**，以更改选定的 IP 地址。

单击**删除**，以将选定条目从列表中删除。



IP 地址示例

添加 IPv4 地址：

单个地址 – 添加单个计算机的 IP 地址（例如，*192.168.0.10*）

地址范围 – 键入开始和结束 IP 地址，以指定多台计算机的 IP 范围（例如，*192.168.0.1-192.168.0.99*）

子网 – 子网（一组计算机）由 IP 地址和掩码定义。例如，255.255.255.0 是 192.168.1.0 子网的网络掩码。要排除整个子网，请键入 *192.168.1.0/24*

添加 IPv6 地址：

单个地址 – 添加单台计算机的 IP 地址（例如，*2001:718:1c01:16:214:22ff:fec9:ca5*）

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

URL 列表管理

高级设置 > **保护** > **Web 访问保护**中的 **URL 列表管理**使您能够指定要阻止、允许或排除内容扫描的 HTTP 地址。

如果要过滤 HTTP 以外的 HTTPS 地址，则必须启用 SSL/TLS。否则，将仅添加您访问过的 HTTPS 站点的域，而不会添加完整 URL。

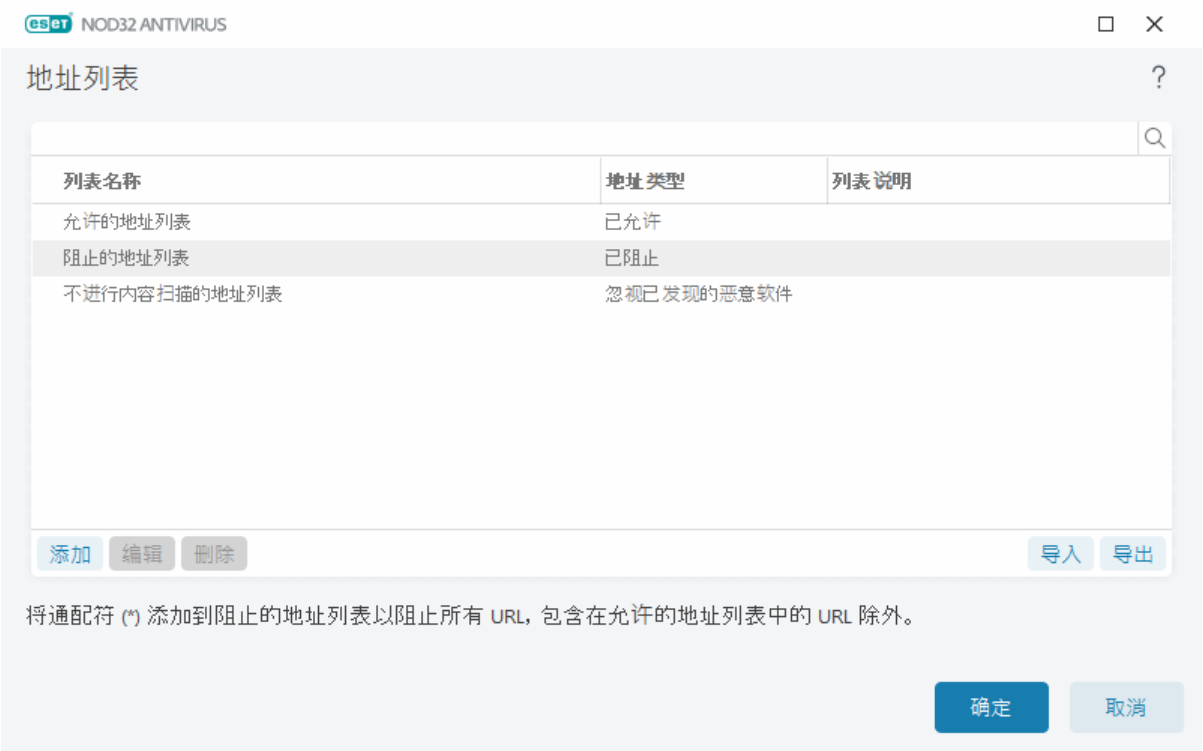
将不能访问**阻止的地址列表**中的网站，除非它们还包含在**允许的地址列表**中。在访问时，不会针对**不进行内容扫描的地址列表**中的网站进行扫描以查找恶意代码。

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

特殊符号 *（星号）和 ？（问号）可用于列表。星号可以替代任意字符串，而问号可以替代任意符号。在指定排除的地址时要特别小心，因为该列表应该仅包含受信任的安全地址。同样，必须确保在此列表中正确使用符号 * 和 ?。有关如何安全匹配包括所有子域的整个域，请参阅添加 HTTP 地址/域掩码。若要启用某个列表，请选择**启用列表**。如果您希望在输入来自当前列表的地址时收到通知，请选择**应用时发送通知**。

受 ESET 信任的地址

如果已为 SSL/TLS 启用**不扫描受 ESET 信任的域的通信**，则 URL 列表管理配置将不会影响由 ESET 管理的白名单上的域。



控件元素

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

编辑 – 修改现有列表。使用此项添加或删除地址。

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

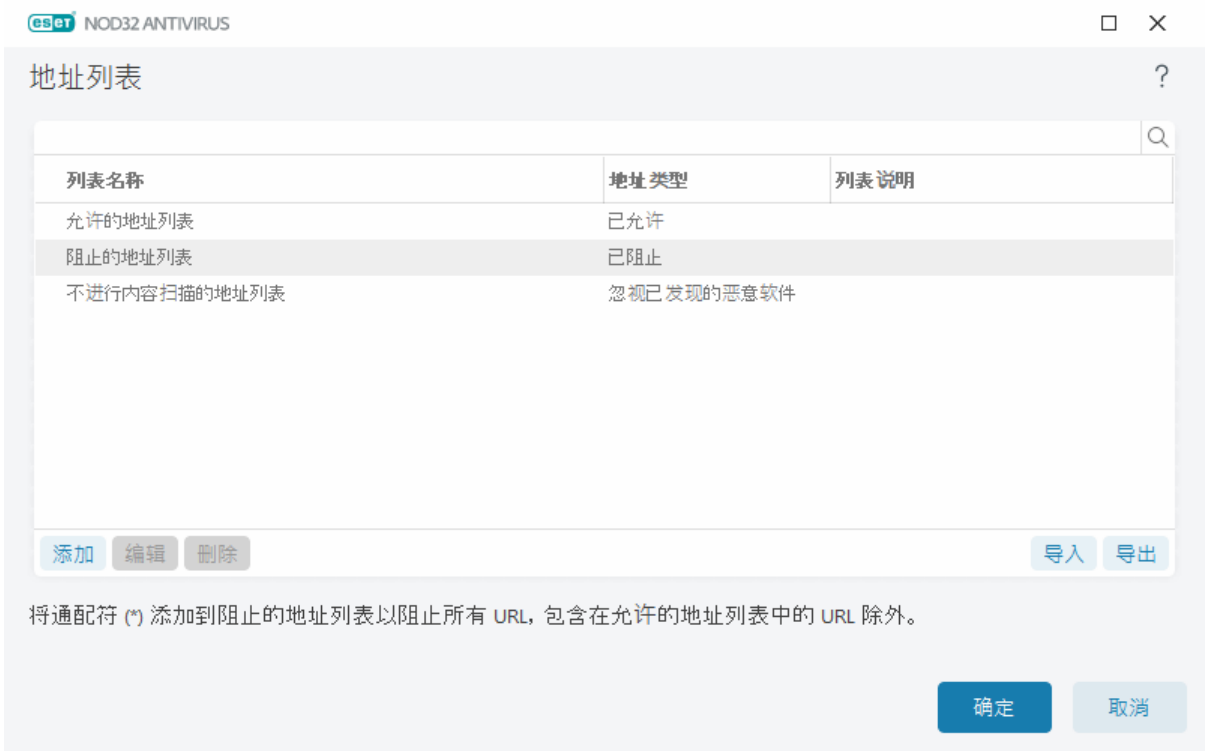
地址列表

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

默认情况下，有以下三种列表可供使用：

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

单击**添加**以创建新的列表。若要删除选定列表，请单击**删除**。



> **图文并茂说明**
> 以下 ESET 知识库文章可能仅提供英文版：
> • 排除安全网站不受 Web 访问保护阻止
> • 使用 ESET Windows 家庭产品阻止网站

有关详细信息，请参阅 URL 列表管理。

创建新的地址列表

通过此对话窗口，可以配置一个新的将阻止、允许或排除检查的 URL 地址/掩码列表。

可以配置以下选项：

地址列表类型 – 提供三种列表类型：

- **忽视已发现的恶意软件** – 不会对已添加至此列表的任何地址执行恶意代码检查。
- **已阻止** – 将阻止访问此列表中指定的地址。
- **已允许** – 将允许访问此列表中指定的地址。允许此列表中的地址，即使它们与阻止地址列表匹配。

列表名称 – 指定列表的名称。当编辑其中一个预定义列表时，此字段将不可用。

列表说明 – 键入列表的简短说明（可选）。当编辑其中一个预定义列表时不可用。

要激活列表，请选中该列表旁边的**激活列表**。如果您希望在访问网站时收到使用特定列表的通知，请选择**应用时通知**。例如，您会在阻止或允许网站时收到通知，因为它包含在阻止或允许的地址列表中。该通知会包含列表的名称。

日志记录严重级别 – 有关访问网站时所使用的特定列表的信息可以写入日志文件。

控件元素

添加 – 将新 URL 地址添加到列表（输入带有分隔符的多个值）。

编辑 – 修改列表中的现有地址。仅适用于使用**添加**创建的地址。

删除 – 删除列表中的现有地址。仅适用于使用**添加**创建的地址。

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

如何添加 URL 掩码

在输入需要的地址/域掩码之前，请参考此对话框中的说明。

ESET NOD32 Antivirus 允许用户阻止对指定网站的访问，并阻止 Internet 浏览器显示其内容。除此之外，它还允许用户指定应从检查中排除的地址。如果用户不知道远程服务器的完整名称，或想要指定整组远程服务器，可以使用所谓的掩码来标识这样的组。掩码包括符号“?”和“*”：

- 使用 ? 来替代一个符号
- 使用 * 来替代一个文本字符串。

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

若在域名的开头处使用，将特殊处理以“*.”开头的序列。首先，在本例中，* 通配符不匹配斜杠字符（“/”）。这是为了避免绕过掩码，例如掩码 **.domain.com* 将不匹配 *http://anydomain.com/anypath#.domain.com*（此类后缀可以附加到任何 URL，不会影响下载）。第二，在此特殊案例中，“*.”还将匹配一个空字符串。此操作将允许使用单个掩码匹配包括任何子域的整个域。例如，掩码 **.domain.com* 还匹配 *http://domain.com*。使用 **domain.com* 是不正确的，因为它还会匹配 *http://anotherdomain.com*。

HTTP(S) 通信扫描

默认情况下，ESET NOD32 Antivirus 配置为扫描 Internet 浏览器和其他应用程序使用的 HTTP 和 HTTPS 通信。仅当在使用第三方软件时遇到问题并想要知道问题是否是由 ESET NOD32 Antivirus 引起时，才应禁用通信扫描。

启用 HTTP 通信扫描 – 将始终监控所有应用程序的所有端口上的 HTTP 通信。

启用 HTTPS 通信扫描 - HTTPS 通信使用加密通道来在服务器和客户端之间传输信息。ESET NOD32 Antivirus 利用 SSL（安全套接字层）和 TLS（传输层安全）协议来检查通信。无论操作系统版本如何，该程序将仅扫描在**HTTPS 协议使用的端口**中定义的端口上的通信（可以将端口添加到预定义的 443 和 0-65535）。

ThreatSense

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

ThreatSense 引擎设置选项允许指定若干扫描参数：

- 要扫描的文件类型和扩展名
- 不同检测方法的组合
- 清除级别等

要进入设置窗口，请在高级设置中单击 **ThreatSense**，以显示任何使用 ThreatSense 技术的模块（见下文）。不同的安全情形可能要求不同的配置。考虑到这一点，可针对下列防护模块对 ThreatSense 进行单独配置：

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

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

要扫描的对象

此部分使您可以定义要扫描的计算机组件和文件，以查找渗透。

系统内存 – 扫描攻击系统的系统内存的威胁。

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

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

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

自解压文件 – 自解压文件 (SFX) 是可提取自身的压缩文件。

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

扫描选项

选择在扫描系统中的渗透时所用的方法。以下选项可用：

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

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

清除

清理设置决定在清除对象时 ESET NOD32 Antivirus 的行为。共有 4 个清理级别：

ThreatSense 具有以下消除（即清除）级别：

ESET NOD32 Antivirus 中的修复

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

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 设置的此部分允许您定义要扫描的文件类型。

其他

当为手动计算机扫描配置 ThreatSense 引擎参数时，**其他**部分中的以下选项也可用：

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

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

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

启用智能优化 – 启用智能优化后，最优化的设置将用于确保最高效的扫描级别，同时保持最高的扫描速度。各种保护模块将进行智能化扫描，以便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，则在执行扫描时将仅在特定模块的 ThreatSense 核心中应用用户定义的设置。

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

限制

限制部分允许您指定要扫描的对象的最大大小和嵌套压缩文件的层数：

对象设置

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

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

压缩文件扫描设置

压缩文件嵌套层数 – 指定压缩文件扫描的最大深度。默认值：10

压缩文件中文件的最大大小 – 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。最大值为 **3 GB**

> 不建议更改默认值，正常情况下应该没有修改它的理由。

设备控制

ESET NOD32 Antivirus 提供自动设备CD/DVD/USB/等）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。如果计算机管理员要阻止使用包含不请自来的内容的设备，则此模块将很有用。

支持的外部设备：

- 磁盘存储HDDUSB 可移动磁盘）
- CD/DVD
- USB 打印机
- FireWire 存储
- Bluetooth 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（电池供电设备，如媒体播放器、智能手机、即插即用设备等）
- 所有设备类型

可以在高级设置 > **保护** > **设备控制**中修改设备控制设置选项。

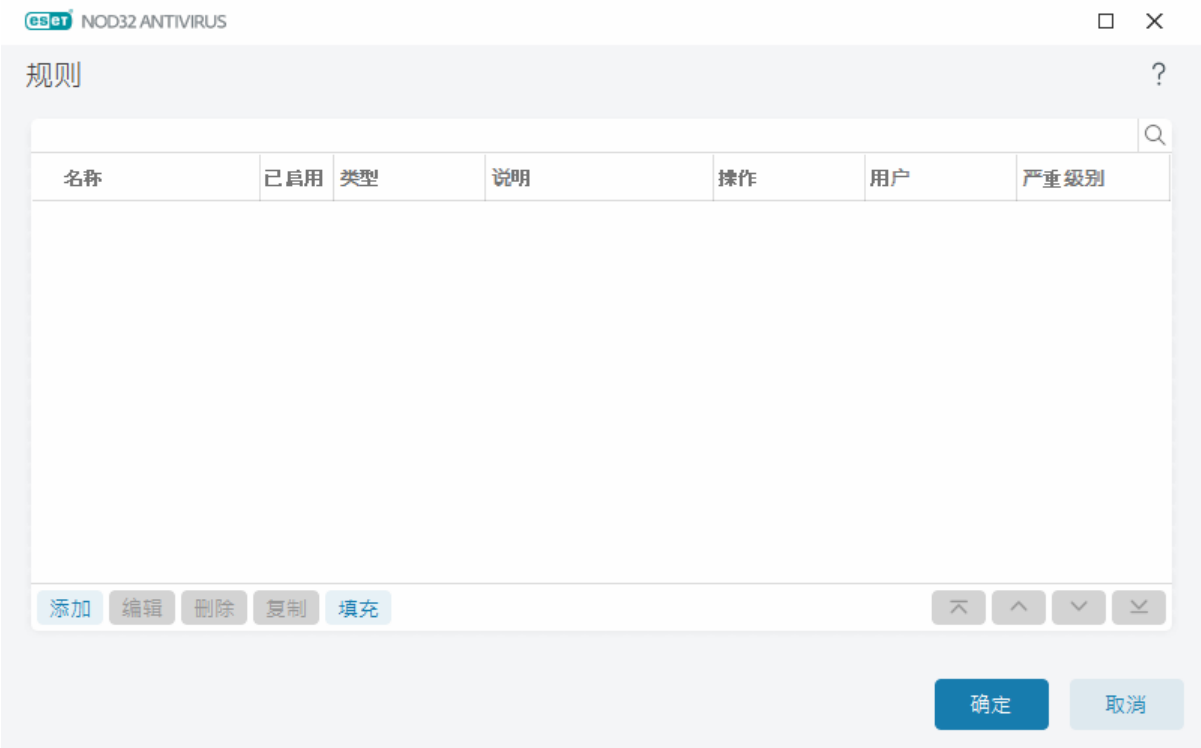
单击**启用设备控制**开关，以在 ESET NOD32 Antivirus 中启用“设备控制”功能；必须重新启动计算机，才能使此更改生效。在启用设备控制后，可以在规则编辑器窗口中定义**规则**。

> 您可以针对应用的不同规则来创建不同的设备组。也可以仅创建一组将应用**允许**或**写入阻止**操作规则的设备。这确保了在未标识的设备连接到计算机时设备控制会阻止它们。

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

设备控制规则编辑器

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

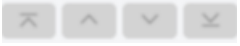


可以按用户或用户组并根据可以在规则配置指定的其他设备参数，来允许或阻止特定设备。规则列表包含规则的多个说明，例如名称、外部设备类型、将外部设备连接到计算机后执行的操作以及日志严重级别。另请参阅添加设备控制规则。

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

按住 **CTRL** 并单击，可以选择多个规则和对所有所选规则应用操作，例如删除或上下移动列表。**启用**复选框可禁用或启用规则；在您希望保留规则时，这会很有用。

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。

可以在主程序窗口 > **工具** > 日志文件中，查看日志条目。

设备控制日志记录了所有出现的已触发的设备控制。

已检测的设备

填充按钮提供了当前所有已连接设备的概述，其中包括以下信息：设备类型、设备供应商、型号以及序列号（如果有）。如果要查看所有隐藏的设备，请选择**显示隐藏的设备**。

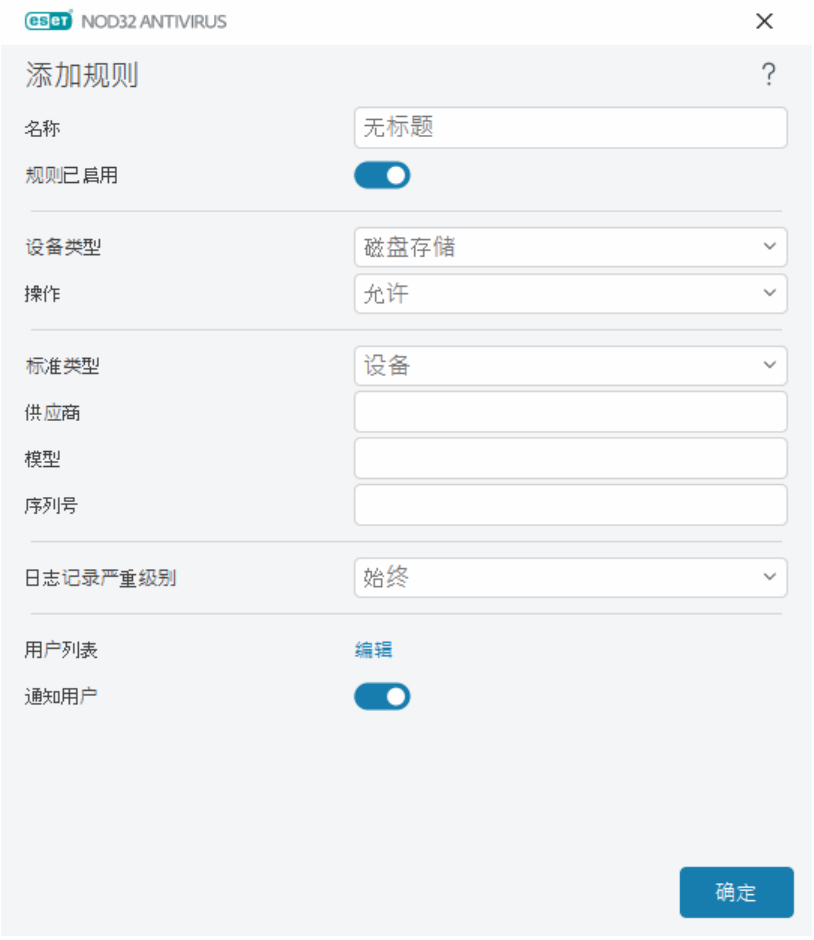
从检测到的设备列表中选择一个设备，然后单击**确定**以添加设备控制规则以及预定义的信息（所有设置都可以调整）。

在低电量（睡眠）模式下运行的设备会标有警告图标 。要启用**确定**按钮并为此设备添加规则，请执行以下操作：

- 重新连接设备
- 使用该设备（例如，在 Windows 中启动“相机”应用程序来唤醒网络摄像头）

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采取的操作。



在**名称**字段中输入规则说明，以便更好地识别。单击**已启用规则**旁边的滑块，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。

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。

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：

- **允许** – 将允许对设备的完全访问权限。
- **阻止** – 将阻止对设备的访问。
- **写入阻止** – 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，并且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**写入阻止**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不同设备的规则。所有参数都区分大小写并支持通配符（*、?）：

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

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区分大小写并支持通配符（问号 (?) 代表单个字符，而星号 (*) 代表字符串中的零个或多个字符）。

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

日志记录严重级别

ESET NOD32 Antivirus 将所有重要事件保存到日志文件中，用户可通过主菜单直接查看日志文件。 依次单击**工具 > 日志文件**，然后从**日志**下拉菜单中选择**设备控制**。

- **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。

- **无** – 不记录任何日志。

用户列表

通过将规则添加到用户列表并单击**用户列表**旁边的**编辑**，即可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。

> **用户列表限制**
> 无法为具有特定设备类型的规则定义用户列表：
> - USB 打印机
> - 蓝牙设备
> - 智能卡读卡器
> - 刻录设备
> - 调制解调器
> - LPT/COM 端口

通知用户 – 如果插入受现有规则阻止的设备，将会显示一个通知窗口。

设备组

> ⚠ 连接到计算机的设备可能会带来安全风险。

“设备组”窗口分为两个部分。该窗口右侧包含属于各个组的设备列表，而该窗口左侧包含已创建的组。选择一个组以在右侧窗格中显示设备。

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

控件元素

添加 – 可以通过键入组名称添加组，也可以将设备添加到现有组，具体取决于在窗口的哪个部分单击了按钮。

编辑 – 让您可以修改选定组的名称或设备的参数（供应商、型号和序列号）。

删除 – 删除选定组或设备，具体取决于您在窗口的哪一部分上单击了该按钮。

导入 – 从文本文件导入设备列表。从文本文件导入设备需要正确的格式设置：

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

> ✓ 以下是文本文件内容的示例：
> ```
> Kingston,DT 101 G2,001CCE0DGRFC0371
> 04081-0009432,USB2.0 HD WebCam,20090101
> ```

导出 – 将设备列表导出到文件。

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

添加设备

在右侧窗口中单击**添加**，以将设备添加到现有组。下面显示的其他参数可用于微调不同设备的规则。所有参数都区分大小写并支持通配符（*、?）：

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

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区分大小写并支持通配符（问号 [?] 代表单个字符，而星号 [*] 代表字符串中的零个或多个字符）。

单击**确定**可保存更改。单击**取消**可离开**设备组**窗口，但不会保存更改。

在创建设备组后，必须为已创建的设备组添加新的设备控制规则，然后选择要采取的操作。

注意，不是所有操作（权限）都可用于所有设备类型。如果设备是存储类型的设备，则所有四个操作均可用。对于非存储设备，仅三个操作可用（例如，**写入阻止**操作对蓝牙不可用；因此，只能对蓝牙设备执行允许、阻止或警告操作）。

ThreatSense

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

ThreatSense 引擎设置选项允许指定若干扫描参数：

- 要扫描的文件类型和扩展名
- 不同检测方法的组合
- 清除级别等

要进入设置窗口，请在高级设置中单击 **ThreatSense**，以显示任何使用 ThreatSense 技术的模块（见下文）。不同的安全情形可能要求不同的配置。考虑到这一点，可针对下列防护模块对 ThreatSense 进行单独配置：

- 文件系统实时防护
- 空闲状态下扫描
- 开机扫描
- 文档防护

- 电子邮件客户端防护
- Web 访问保护
- 计算机扫描

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

要扫描的对象

此部分使您可以定义要扫描的计算机组件和文件，以查找渗透。

系统内存 – 扫描攻击系统的系统内存的威胁。

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

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

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

自解压文件 – 自解压文件 (SFX) 是可提取自身的压缩文件。

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

扫描选项

选择在扫描系统中的渗透时所用的方法。以下选项可用：

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

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

清除

清理设置决定在清除对象时 ESET NOD32 Antivirus 的行为。共有 4 个清理级别：

ThreatSense 具有以下消除（即清除）级别：

ESET NOD32 Antivirus 中的修复

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

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

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 设置的此部分允许您定义要扫描的文件类型。

其他

当为手动计算机扫描配置 ThreatSense 引擎参数时，**其他**部分中的以下选项也可用：

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

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

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

启用智能优化 – 启用智能优化后，最优化的设置将用于确保最高效的扫描级别，同时保持最高的扫描速度。各种保护模块将进行智能化扫描，以便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，则在执行扫描时将仅在特定模块的 ThreatSense 核心中应用用户定义的设置。

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

限制

限制部分允许您指定要扫描的对象的最大大小和嵌套压缩文件的层数：

对象设置

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

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

压缩文件扫描设置

压缩文件嵌套层数 – 指定压缩文件扫描的最大深度。默认值：10

压缩文件中文件的最大大小 – 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。最大值为 **3 GB**

> 不建议更改默认值，正常情况下应该没有修改它的理由。

清除级别

要更改所需保护模块的清除级别设置，请展开 **ThreatSense**（例如，**文件系统实时防护**），然后从下拉菜单中选择**清除级别**

ThreatSense 具有以下消除（即清除）级别：

ESET NOD32 Antivirus 中的修复

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

不扫描的文件扩展名

排除的文件扩展名是 ThreatSense 的一部分。要配置排除的文件扩展名，请在高级设置中，为任何使用 ThreatSense 技术的模块单击 **ThreatSense**

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 设置的此部分允许您定义要扫描的文件类型。

> 请勿混淆进程排除HIPS 排除或文件/文件夹排除

默认情况下，扫描所有文件。可将任何扩展名添加到不扫描的文件列表中。

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

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

要在 Windows 操作系统中查看文件的具体扩展名（如果有），必须在 **Windows 资源管理器** > **查看**（选项卡）中选中**文件名扩展名**复选框。

其他 ThreatSense 参数

要编辑这些设置，请打开高级设置 > **保护** > **文件系统实时防护** > **其他 ThreatSense 参数**

用于新创建文件和新修改文件的其他 ThreatSense 参数

新建或修改的文件被感染的可能性高于现有文件。出于此原因，该程序将使用其他扫描参数检查这些文件。ESET NOD32 Antivirus 会将高级启发式扫描（可在发布检测引擎更新之前检测新威胁）与基于病毒库的扫描方法结合使用。

除了新建文件，系统还会扫描**自解压存档** (.sfx) 和**运行时加壳程序**（内部压缩的可执行文件）。默认情况下，对存档的扫描可深达第 10 个嵌套层，而且不论其实际大小如何都会进行检查。要修改存档扫描设置，请取消选中**默认的存档扫描设置**。

用于已执行文件的其他 ThreatSense 参数

执行文件时采用高级启发式扫描 – 默认情况下，执行文件时将使用高级启发式扫描。启用后，强烈建议您保持智能优化和 ESET LiveGrid® 的启用状态以降低对系统性能的影响。

执行可移动磁盘上的文件时采用高级启发式扫描 – 高级启发式扫描将模拟虚拟环境中的代码并在允许从可移动磁盘运行该代码之前评估其行为。

工具

可以在高级设置 > **工具**中，为提供额外安全性并有助于简化 ESET NOD32 Antivirus 管理的功能配置高级设置。

- Microsoft Windows® 更新
- ESET CMD
- 日志文件
- 游戏模式
- 诊断

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，即时安装可用的 Microsoft Windows 更新很重要。ESET NOD32 Antivirus 会根据在高级设置 > **工具**中指定的级别，来通知您错过的更新。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。

对话窗口 – 系统更新

如果有操作系统的更新，ESET NOD32 Antivirus 会在主程序窗口 > **概述**中显示通知。单击**更多信息**以打开系统更新窗口。

系统更新窗口显示随时可以下载和安装的可用更新的列表。更新类型显示在更新名称旁边。

双击任意更新行可显示带有其他信息的更新信息窗口。

单击**运行系统更新**，以下载并安装所有列出的操作系统更新。

更新信息

系统更新窗口显示随时可以下载和安装的可用更新的列表。更新优先级显示在更新名称旁。

单击**运行系统更新**可以开始下载和安装操作系统更新。

右键单击任意更新行，然后单击**显示信息**以显示一个带有其他信息的新窗口。

ESET CMD

该功能支持高级 ecmd 命令。它允许您使用命令行 (ecmd.exe) 导出和导入设置。到目前为止，只可以使用 GUI 导出设置，ESET NOD32 Antivirus 配置可以导出为 *.xml* 文件。

启用 ESET CMD 后，有两种授权方法可用：

- **无** – 无授权。不建议您使用此方法，因为它允许导入任何未签名的配置，这可能存在风险。
- **高级设置密码** – 需要密码才可从 .xml 文件导入配置，此文件必须已签名（请参阅下面的签名 .xml 配置文件）。可以导入新配置之前，必须提供访问设置中指定的密码。如果未启用访问设置、密码不匹配或 .xml 配置文件未签名，将不会导入配置。

ESET CMD 启用后，可使用命令行导入或导出 ESET NOD32 Antivirus 配置。可以手动执行上述操作，也可以创建用于自动执行的脚本。

若要使用高级 ecmd 命令，您需要具有管理员权限才可以运行这些命令，或者使用**以管理员身份运行**打开 Windows 命令提示符 (cmd)，否则，您会收到 **Error executing command** 消息。此外，导出配置时，目标文件夹必须已存在，ESET CMD 设置关闭时，导出命令仍可正常工作。

导出设置命令：
`ecmd /getcfg c:\config\settings.xml`

导入设置命令：
`ecmd /setcfg c:\config\settings.xml`

高级 ecmd 命令只可以本地运行。

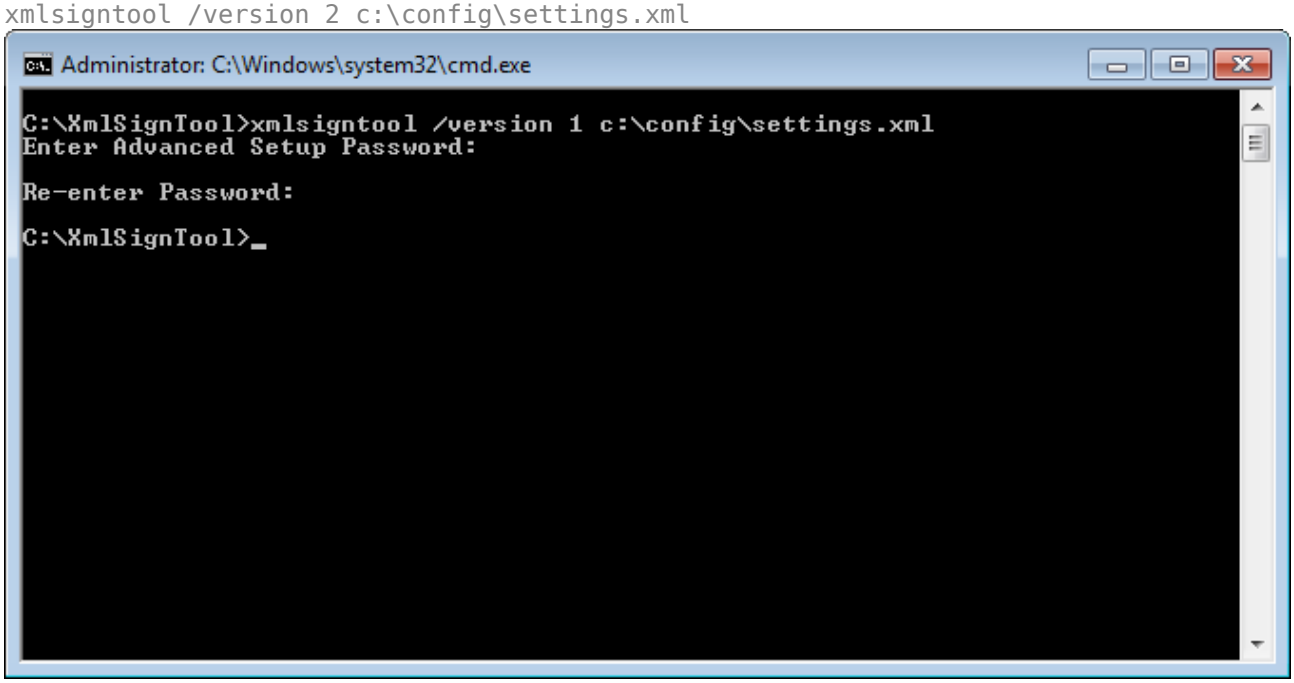
对 *.xml* 配置文件签名：

1. 下载 XmlSignTool 可执行文件。
2. 使用**以管理员身份运行**打开 Windows 命令提示符 (cmd)。
3. 导航到 `xmlsigntool.exe` 的保存位置。
4. 执行对 *.xml* 配置文件进行签名的命令，用法：`xmlsigntool /version 1|2 <xml_file_path>`

`/version` 参数的值取决于您的 ESET NOD32 Antivirus 的版本。为早于 11.1 版本的 ESET NOD32 Antivirus 使用 `/version 1`。为当前版本的 ESET NOD32 Antivirus 使用 `/version 2`。

5. 根据 XmlSignTool 的提示，键入两遍高级设置密码。您的 *.xml* 配置文件现已完成签名，可以用于使用 ESET CMD 以及密码授权方法导入 ESET NOD32 Antivirus 的另一个实例。

对导出的配置文件进行签名的命令：
`xmlsigntool /version 2 c:\config\settings.xml`



如果访问设置密码更改，并且想要导入之前使用旧密码签名的配置，需要重新使用当前密码对 *.xml* 配置文件进行签名。这使您在导入之前无需在另一台运行 ESET NOD32 Antivirus 的计算机上导出旧版本配置文件，即可使用该配置文件。

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

日志文件

可以在高级设置 > **工具** > **日志文件**中，查找 ESET NOD32 Antivirus 的日志记录配置。日志部分用来定义如何管理日志。程序自动删除旧的日志以节省硬盘空间。您可以为日志文件指定以下选项：

日志记录的最低级别 – 指定要记录的事件的最低级别：

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

当选择诊断级别时，将记录所有受阻止的连接。

自动删除早于以下天数的记录字段中指定天数以前的日志条目将自动删除。

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

单击**优化**以开始日志文件的碎片整理。在此过程中会删除所有空日志条目，这将提高性能和日志处理速度。尤其在日志包含大量条目数时，可以感受到这种提高。

启用文本协议支持采用不同于日志文件的其他文件格式存储日志：

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

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

游戏模式

游戏模式是为那些需要不中断使用其软件、不希望被通知/警报窗口打扰，并希望最大程度地降低 CPU 使用的用户提供的功能。游戏模式还可以用于不能被病毒防护活动中断的演示。启用此功能后，将禁用所有弹出窗口，同时完全停止计划任务的活动。系统保护仍在后台运行，但是不需要任何用户交互。

可以在主程序窗口中的**设置** > **计算机防护**下，通过单击 旁边的 或 来启用或禁用游戏模式。启用游戏模式会存在潜在安全风险，因此任务栏上的防护状态图标将变为橙色，并显示一条警告。您还会在主程序窗口中看到该警告，在其中会看到橙色的**游戏模式处于活动状态**

在**高级设置** > 工具 > **游戏模式**下激活**以全屏模式运行应用程序时自动启用游戏模式**，以便当您启动全屏应用程序时立即启动游戏模式，并在您退出应用程序时立即停止该模式。

激活**自动禁用游戏模式前等待的时间**可定义自动禁用游戏模式前的时间量。

诊断

诊断提供 ESET 进程（如 ekrn）的应用程序崩溃转储。如果应用程序崩溃，将生成一个转储。这能够帮助开发人员调试和修复各种 ESET NOD32 Antivirus 问题。

单击**转储类型**旁的下拉菜单，并选择以下三个可用选项之一：

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

目标目录 - 在崩溃期间将生成转储的目录。

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

创建诊断转储 - 单击**创建**以在**目标目录**中创建诊断转储文件。

高级日志记录

启用营销邮件中的高级日志记录 - 记录产品内与营销邮件有关的所有事件。

启用计算机扫描程序高级日志记录 - 记录“计算机扫描”扫描文件和文件夹时发生的所有事件。

启用设备控制高级日志记录 - 记录设备控制中发生的所有事件。这可以帮助开发人员诊断和修复与设备控制有关的问题。

启用 Direct Cloud 高级日志记录 - 记录在 ESET LiveGrid® 中发生的所有事件。这可以帮助开发人员诊断和修复与 ESET LiveGrid® 相关的问题。

启用文档防护高级日志记录 - 记录在文档防护中发生的所有事件，以便诊断和解决问题。

启用电子邮件客户端防护高级日志记录 - 记录在电子邮件客户端防护和电子邮件客户端插件中发生的所有事件，以便诊断和解决问题。

启用内核高级日志记录 - 记录在 ESET 内核 (ekrn) 中发生的所有事件。

启用许可高级日志记录 - 记录与 ESET 激活或 ESET License Manager 服务器之间的所有产品通信。

启用内存跟踪 - 记录有助于开发人员诊断内存泄漏的所有事件。

启用网络通信扫描程序高级日志记录 - 以 PCAP 格式记录通过网络通信扫描程序的所有数据，来帮助开发人员诊断和修复与网络通信扫描程序有关的问题。

启用操作系统高级日志记录 - 记录有关操作系统的其他信息，例如正在运行的进程CPU 活动和磁盘操作。

这可以帮助开发人员诊断并修复与操作系统上运行的 ESET 产品有关的问题。

启用推送邮件高级日志记录 – 记录在推送邮件过程中发生的所有事件。

启用文件系统实时防护高级日志记录 – 记录“文件系统实时防护”扫描文件和文件夹时发生的所有事件。

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

日志文件位于 *C:\ProgramData\ESET\ESET Security\Diagnostics*

技术支持

从 ESET NOD32 Antivirus 联系 ESET 技术支持时，可以提交系统配置数据。从**提交系统配置数据**下拉菜单中选择**始终提交**以自动提交数据，或者选择**提交前询问**以在提交数据前进行提示。

连接

在特定网络中，代理服务器可以协调您的计算机与 Internet 之间的通信。如果您正在使用代理服务器，则需要定义以下设置。否则 ESET NOD32 Antivirus 及其模块无法自动更新。在 ESET NOD32 Antivirus 中，代理服务器设置在高级设置的两个不同部分中可用。

可以在高级设置 > **连接** > **代理服务器**中配置全局代理服务器设置。在此级别指定的代理服务器定义了所有 ESET NOD32 Antivirus 的全局代理服务器设置。此处的参数将用于需要连接到 Internet 的所有模块。

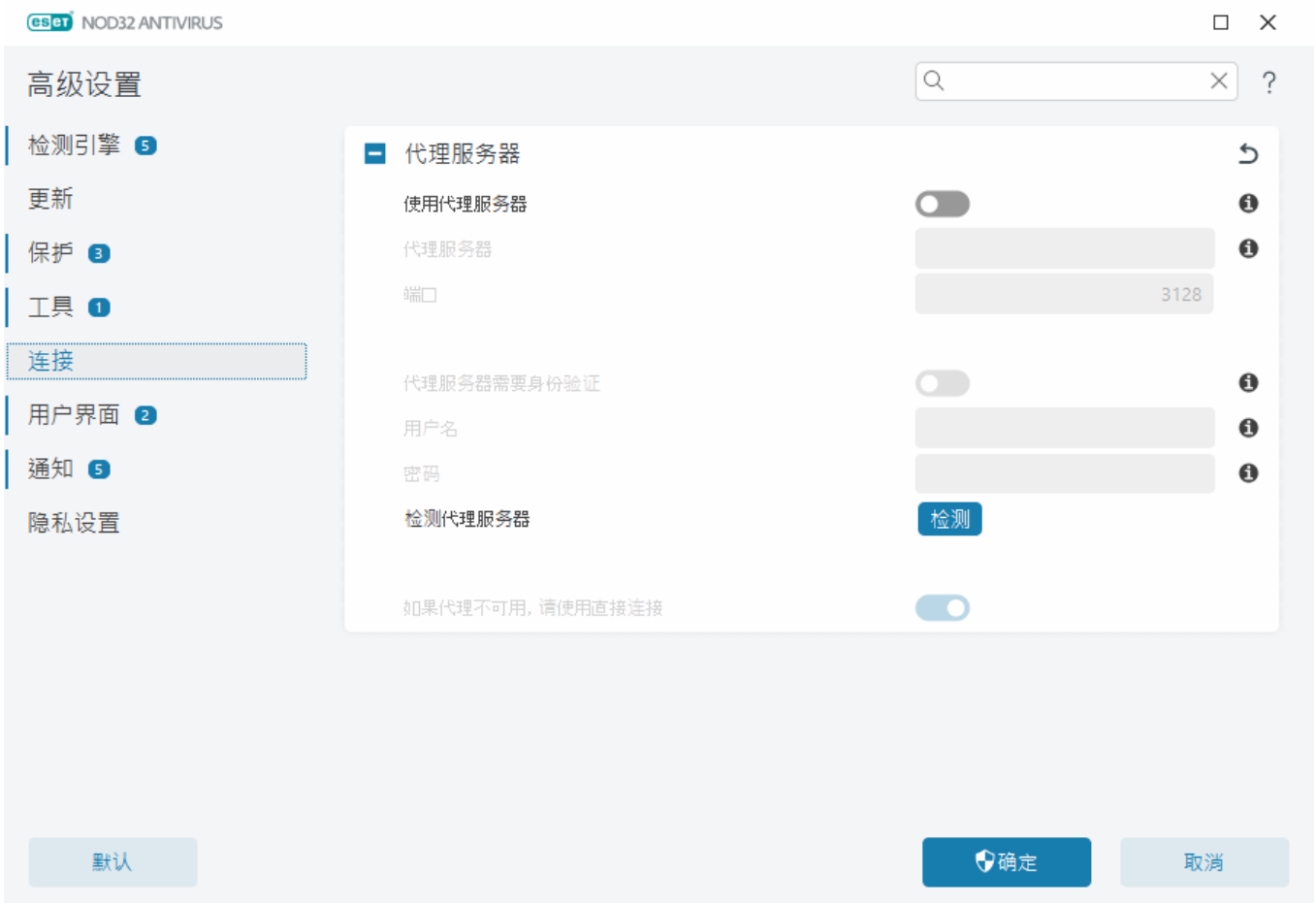
要指定全局代理服务器设置，请启用**使用代理服务器**，然后键入**代理服务器**地址以及代理服务器的**端口**号。

如果与代理服务器的通信需要身份验证，请选中**代理服务器需要身份验证**，然后在相应字段中键入有效的**用户名**和**密码**。单击**检测代理服务器**，以自动检测并填充代理服务器设置 ESET NOD32 Antivirus 将复制在 Internet Explorer 或 Google Chrome 的 Internet 选项中指定的参数。

您必须在**代理服务器**设置中输入用户名和密码。

如果代理不可用，则使用直接连接 – 如果 ESET NOD32 Antivirus 配置为通过代理连接且代理不可用 ESET NOD32 Antivirus 将绕过代理并直接与 ESET 服务器通信。

还可以在高级设置 > **更新** > **配置文件** > **更新** > **连接选项**中，通过从**代理模式**下拉菜单中选择**通过代理服务器连接**来配置代理服务器设置。此配置仅适用于更新，建议用于从远程位置接收模块更新的笔记本电脑。有关详细信息，请参阅高级更新设置



用户界面

要配置程序的图形用户界面 (GUI) 行为，请打开高级设置 > **用户界面**。

可以在用户界面元素高级设置屏幕中，调整程序的视觉外观和效果。

为了最大程度地提高安全软件的安全性，可以使用访问设置工具来通过密码保护设置，以阻止卸载或任何未经授权的更改。

要配置系统通知、检测警报和应用程序状态的行为，请参阅通知部分。

用户界面元素

可以在高级设置 > **用户界面** > **用户界面元素**中调整 ESET NOD32 Antivirus 工作环境 (GUI)以适配您的需求。

颜色模式 – 从下拉菜单中选择 ESET NOD32 Antivirus GUI 的颜色方案：

- **与系统颜色相同** – 根据操作系统设置来设置 ESET NOD32 Antivirus 的颜色方案。
- **深色** - ESET NOD32 Antivirus 将应用深色方案（深色模式）。
- **浅色** - ESET NOD32 Antivirus 将应用标准的浅色方案。

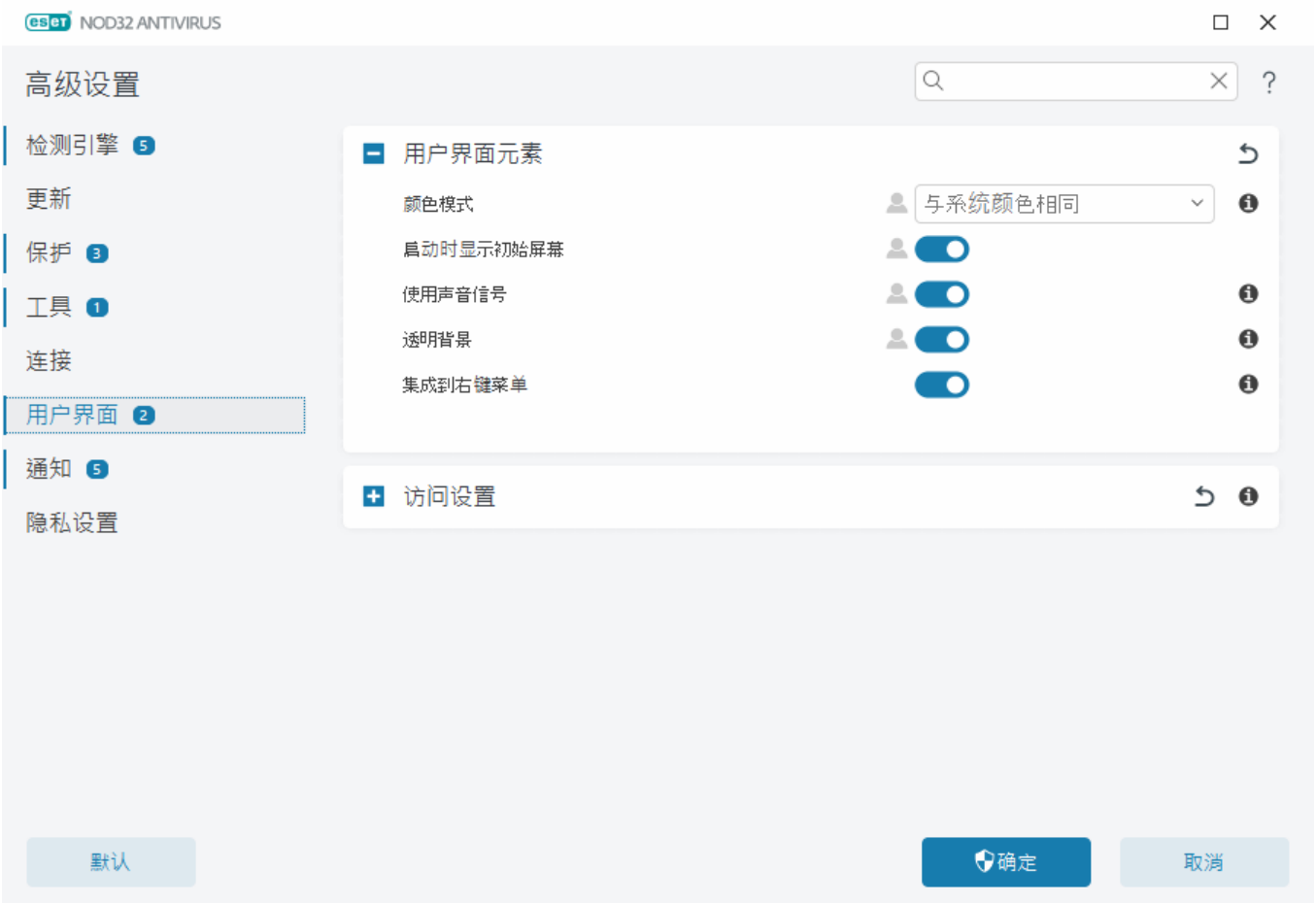
还可以在主程序窗口的右上角，选择 ESET NOD32 Antivirus GUI 的颜色方案。

启动时显示初始屏幕 – 在启动期间显示 ESET NOD32 Antivirus 初始屏幕。

使用声音信号 – 扫描期间发生重要事件时（例如，发现了威胁时或扫描已完成时）， 会播放声音。

透明背景 – 启用 主程序窗口的透明背景效果。透明背景仅适用于最新的 Windows 版本RS4 及更高版本）。

集成到右键菜单 – 将 ESET NOD32 Antivirus 控件元素集成到右键菜单中。



访问设置

ESET NOD32 Antivirus 设置是安全策略的一个重要组成部分。未经授权的修改可能潜在危及系统的稳定和保护。为避免未经授权的修改，可以使用密码保护 ESET NOD32 Antivirus 的设置参数和卸载。可以在高级设置 > **用户界面** > **访问设置**中，配置访问设置。

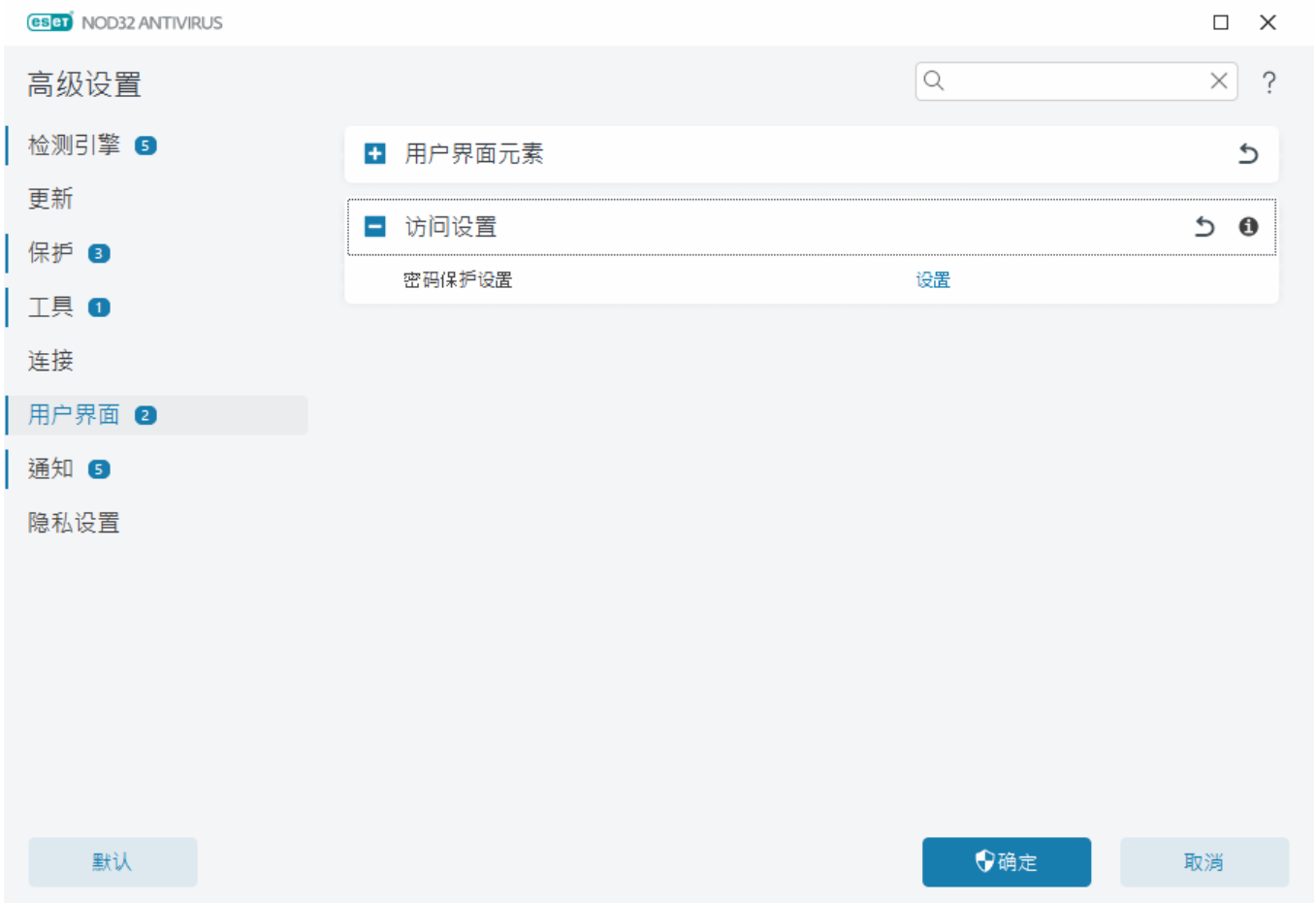
若要设置密码以保护 ESET NOD32 Antivirus 的设置参数和卸载，请单击**密码保护设置**旁边的**设置**

当想要访问受保护的高级设置时，会显示用于输入密码的窗口。如果已忘记或遗失密码，请单击以下**恢复密码**选项，然后输入用于订阅注册的电子邮件地址ESET 会向您发送一封电子邮件，其中内含验证码以及如何重置密码的说明。

- 如何解锁高级设置

若要更改密码，请单击**密码保护设置**旁边的**更改密码**

若要删除密码，请单击**密码保护设置**旁边的**删除**



高级设置的密码

要保护 ESET NOD32 Antivirus 高级设置并避免未经授权的修改，请在**新密码**和**确认密码**字段中键入新密码。单击**确定**。

如果要更改现有密码：

1. 在**旧密码**字段中键入旧密码。
2. 在**新密码**和**确认密码**字段中输入新密码。
3. 单击**确定**。

将需要此密码才能访问“高级设置”。

如果忘记密码，请参阅解锁 ESET HOME 产品中的设置密码。

要恢复丢失的 ESET 激活密钥、订阅的到期日期或 ESET NOD32 Antivirus 的其他订阅信息，请参阅我丢失了激活密钥。

屏幕阅读器支持

ESET NOD32 Antivirus 可以与屏幕阅读器一起使用，以允许视力受损的 ESET 用户浏览产品或配置设置。支持以下屏幕阅读器(JAWS, NVDA, Narrator)。

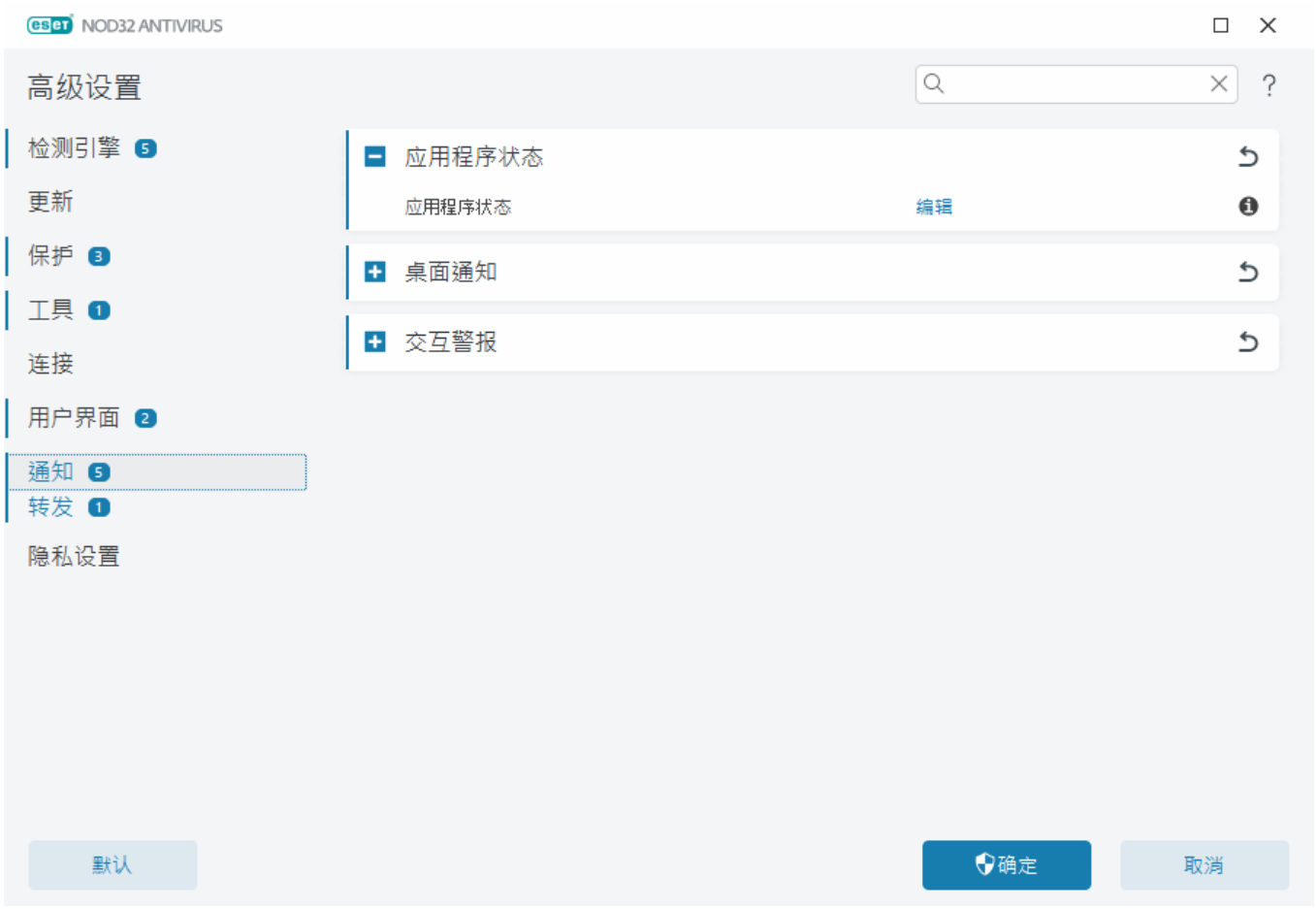
为确保屏幕阅读器软件可以正确访问 ESET NOD32 Antivirus GUI，请按照我们的知识库文章中的说明进行操

作。

通知

要管理 ESET NOD32 Antivirus 通知，请打开高级设置 > **通知**。可以配置以下类型的通知：

- 应用程序状态 – 在主程序窗口 > **概述**中显示的通知。
- 桌面通知 – 系统任务栏旁边的小通知窗口。
- 交互警报 – 需要用户交互的警报窗口和消息框。
- 转发（电子邮件通知） – 电子邮件通知发送到指定的电子邮件地址。



应用程序状态

应用程序状态 – 单击**编辑**，以选择将在主程序窗口 > **概述**中显示的应用程序状态。

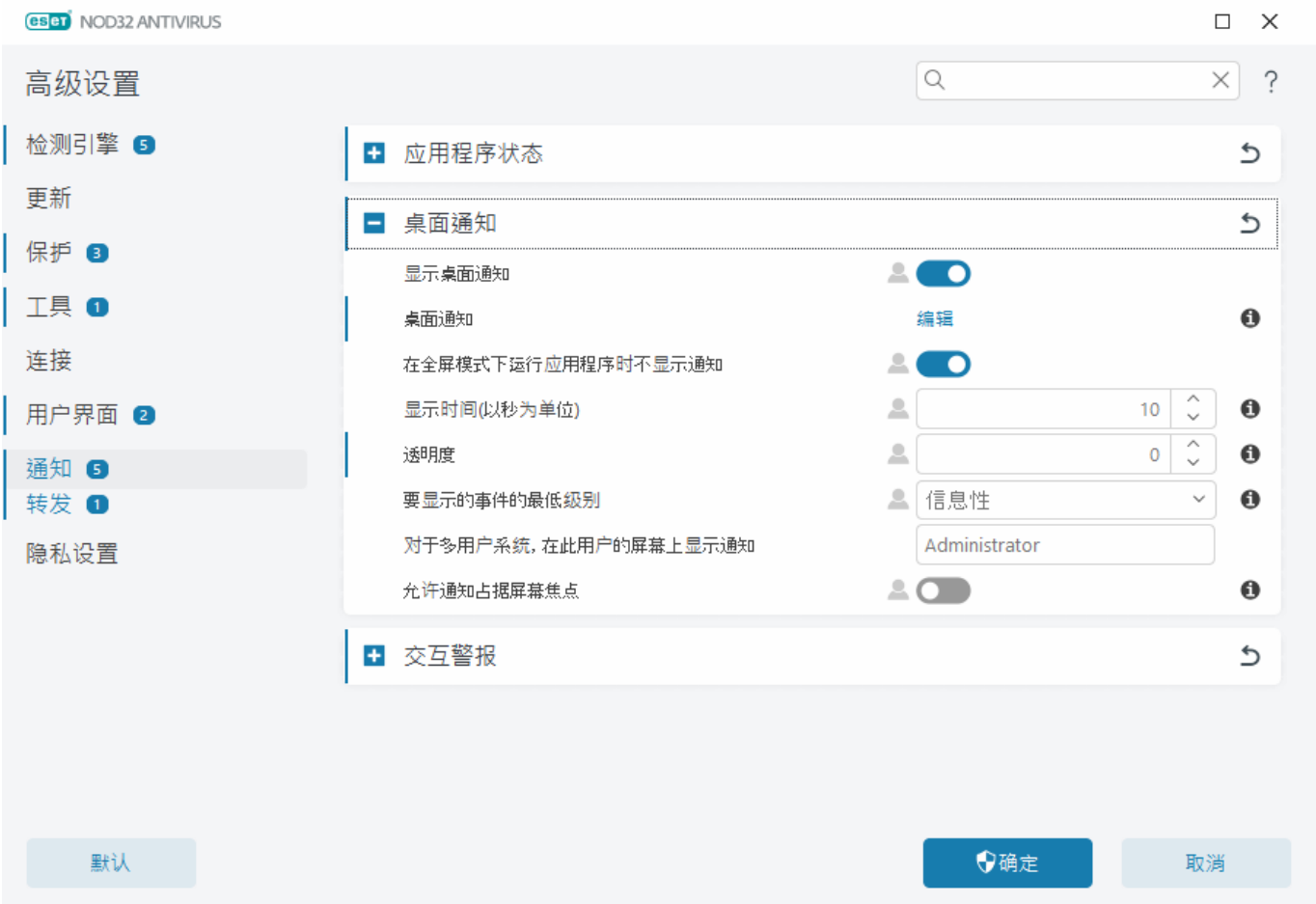
对话窗口 – 应用程序状态

在此对话窗口中，可以选择要显示的应用程序状态。例如，暂停病毒和间谍软件防护或者启用游戏模式的情况。

如果产品未激活或订阅已到期，也会显示应用程序状态。

桌面通知

桌面通知会显示为系统任务栏旁边的小通知窗口。默认情况下，它将显示 10 秒，然后它会慢慢消失。通知包括产品更新成功、已连接新设备、病毒扫描任务完成或找到新威胁。



在桌面上显示通知 – 建议您将此选项保持为启用，以便产品会在发生新事件时给您发送通知。

桌面通知 – 单击**编辑**以启用或禁用特定桌面通知。

在全屏模式下运行应用程序时不显示通知 – 在全屏模式下运行应用程序时，抑制显示所有非交互通知。

显示时间(以秒为单位) – 设置通知显示持续时间。该值必须介于 3-30 秒之间。

透明度 – 设置通知的透明度百分比。支持的范围为 0（不透明）到 80（非常高的透明度）。

要显示事件的最低级别 – 设置显示的起始通知严重性级别。从下拉菜单中，选择以下选项之一：

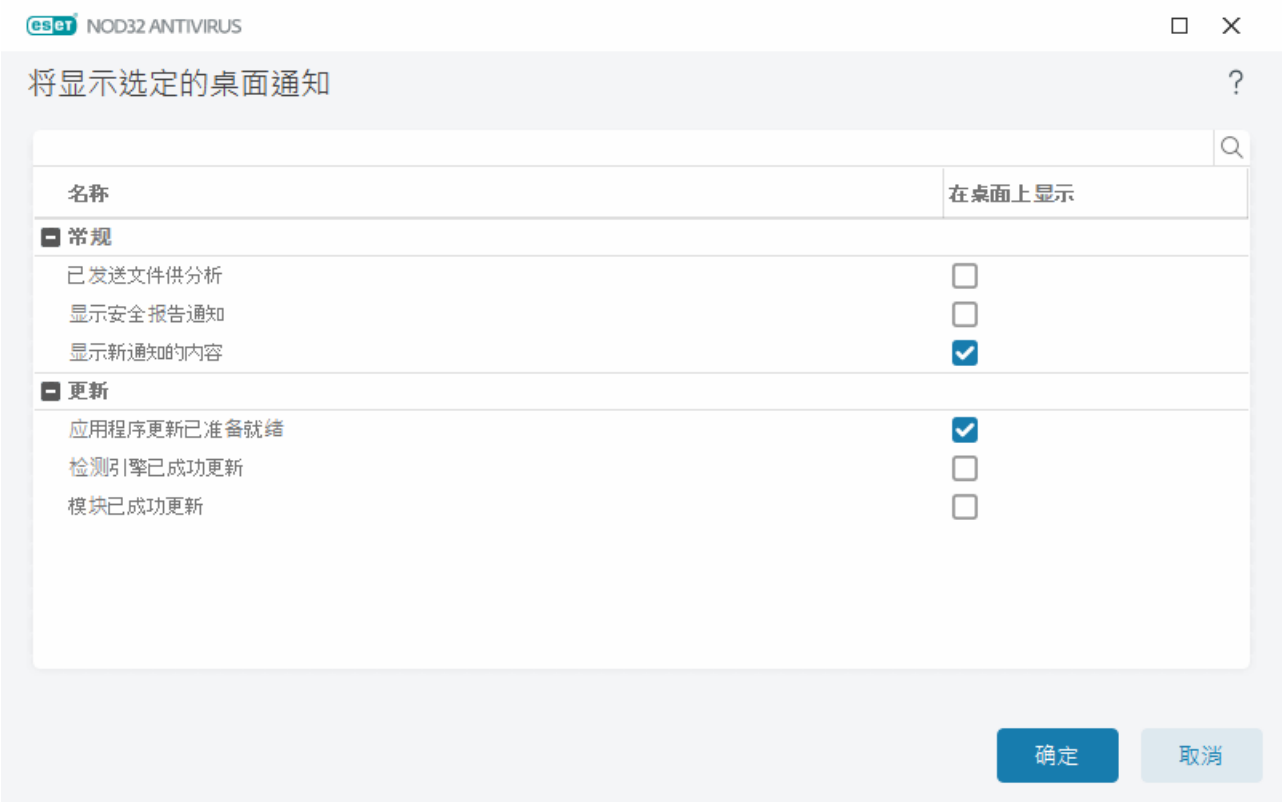
- **诊断** – 显示微调程序所需的信息和以上所有记录。
- **信息性** – 显示信息性消息（如非标准的网络事件），其中包括成功更新消息及以上所有记录。
- **警告** – 显示警告消息、错误和严重错误（例如，更新失败）。
- **错误** – 显示错误（例如，文档防护未启动）和严重错误。
- **严重** – 仅显示严重错误（启动病毒防护时出错或系统被感染等）。

对于多用户系统，在此用户的屏幕上显示通知 – 允许选定帐户接收桌面通知。例如，如果您使用的不是管理员帐户，则键入完整帐户名称，将显示指定帐户的桌面通知。只有一个用户帐户可以接收桌面通知。

允许通知占据屏幕焦点 – 允许通知占据屏幕焦点，并可在 **ALT + Tab** 菜单中进行访问。

桌面通知列表

要调整桌面通知的可见性（在屏幕右下角显示），请打开高级设置 > **通知** > **桌面通知**。单击**桌面通知**旁边的**编辑**，然后选中相应的**显示**复选框。



常规

显示安全报告通知 – 当生成新的安全报告时收到通知。

显示新增功能的通知 – 有关最新产品版本的所有新功能和增强功能的通知。

已发送文件供分析 – 每次 ESET NOD32 Antivirus 发送文件供分析时收到通知。

网络检查器

发送有关新发现的网络设备的通知 – 当有新设备连接到网络时接收通知。

网络防护

网络配置文件已更改 – 网络配置文件发生更改时接收通知。

Wi-Fi 防护警告 – 当您尝试连接到密码较弱或无密码的 Wi-Fi 网络时，会收到通知。

更新

应用程序更新已准备就绪 – 当更新到新版本的 ESET NOD32 Antivirus 准备就绪时收到通知。

检测引擎已成功更新 – 当产品更新检测引擎模块时收到通知。

模块已成功更新 – 当产品更新程序组件时收到通知。

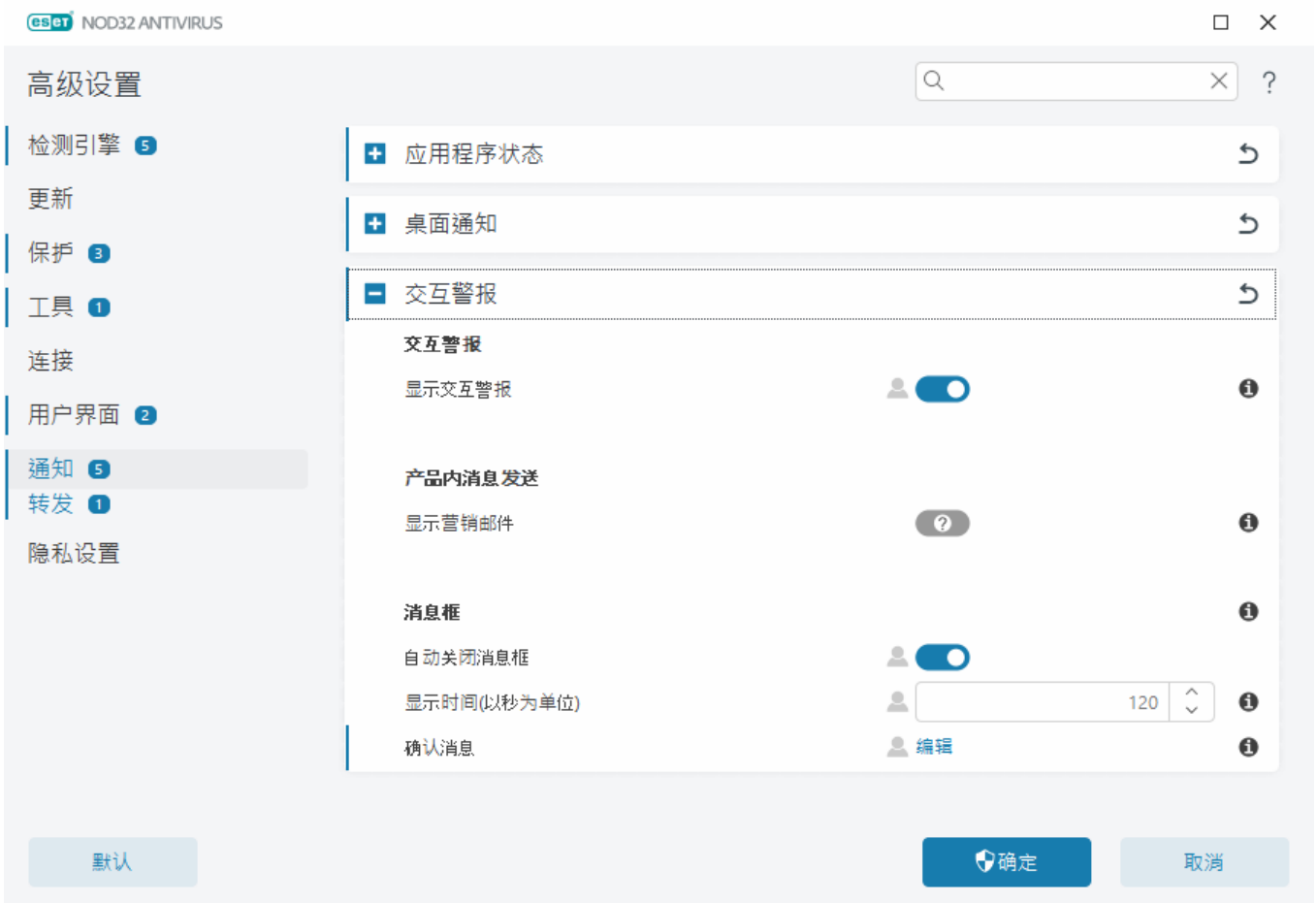
若要设置桌面通知的常规设置，例如消息的显示时长或要显示事件的最低级别，请参阅高级设置 > **通知**中的桌面通知

交互警报

正在查找有关常见警报和通知的信息？

- 发现威胁
- 地址已被阻止
- 产品未激活
- 更改为功能较多的产品
- 更改为功能较少的产品
- 已有可用更新
- 更新信息不一致
- “模块更新失败”消息的疑难解答
- 解决模块更新错误
- 已吊销网站证书

通过**高级设置** > 通知中的**交互警报**部分，可以配置 ESET NOD32 Antivirus 如何处理检测的消息框和交互警报（其中需要由用户做出决定，例如潜在的网络钓鱼网站）。



交互警报

禁用**显示交互警报**将隐藏所有警报窗口和浏览器内的对话框，这只适用于少数特定情况。建议您保持启用此选项。

产品内消息发送

产品内消息旨在向用户发送有关 ESET 新闻和其他通信的通知。发送市场营销消息需要用户同意。因此，默认情况下营销邮件不会发送给用户（显示为问号）。启用此选项，即表示您同意接收 ESET 市场营销消息。如果您对接收 ESET 市场营销材料不感兴趣，则禁用**显示市场营销消息**选项。

消息框

要在一段时间后自动关闭消息框，请选择**自动关闭消息框**。如果未手动关闭它们，则警报窗口会在指定时间过后自动关闭。

显示时间(以秒为单位) - 设置警报显示持续时间。该值必须介于 10-999 秒之间。

确认消息 - 单击**编辑**以显示可以选择是否显示的确认消息列表

确认消息

要调整确认消息，请打开高级设置 > **通知** > **交互警报**，然后单击**确认消息**旁边的**编辑**

该对话窗口将显示在执行任何操作之前 ESET NOD32 Antivirus 显示的确认消息。选中或取消选中每条确认消息旁的复选框以启用或禁用它。

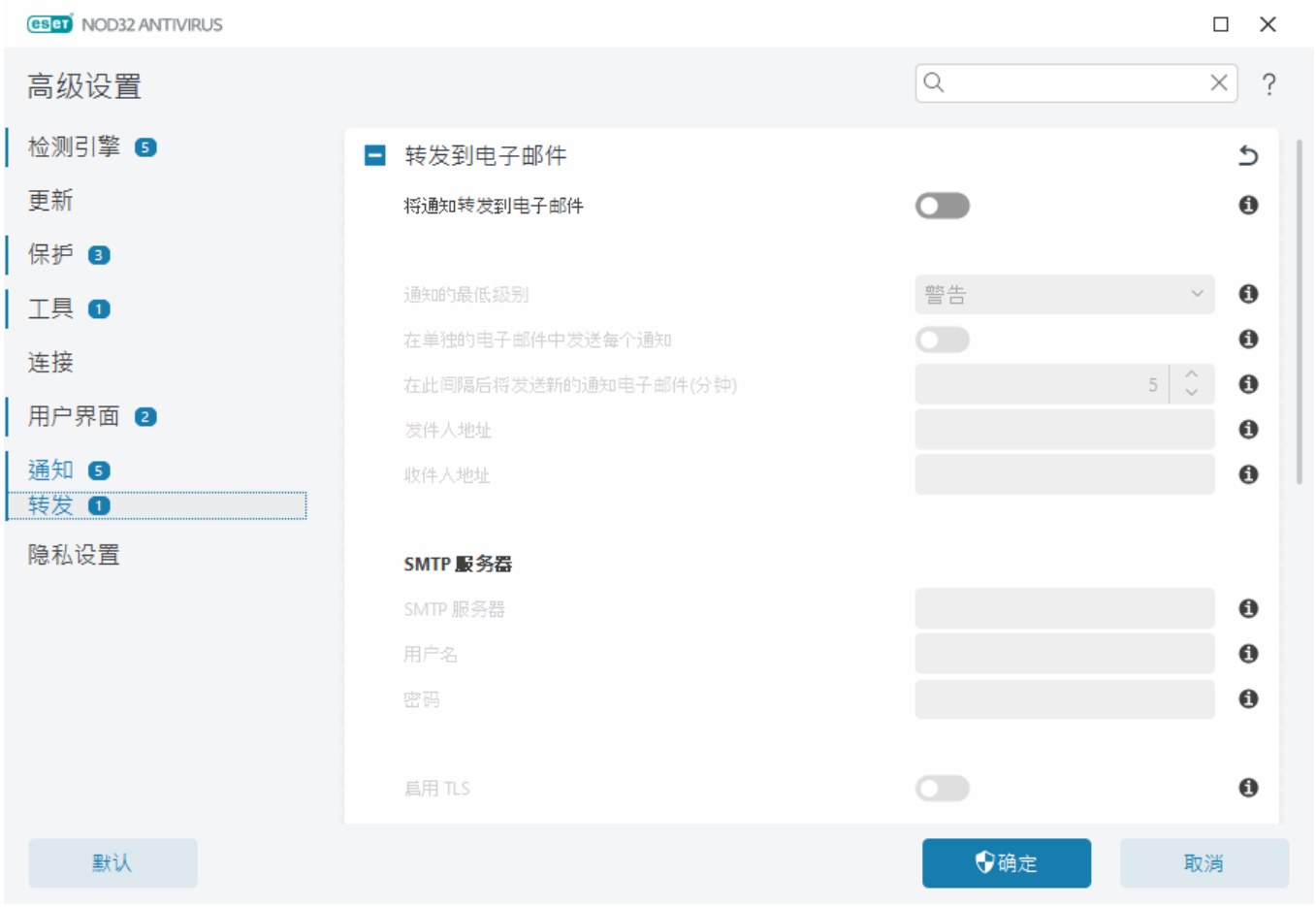
详细了解与确认消息有关的特定功能：

- 删除 ESET SysInspector 日志前询问
- 删除所有 ESET SysInspector 日志前询问
- 从隔离区中删除对象前询问
- 放弃高级设置中的设置前先询问
- 不清除发现的所有威胁之前在警报窗口中询问
- 从日志中删除记录前先询问
- 删除计划任务中的已计划任务前先询问
- 删除所有日志记录前先询问
- 重置统计前先询问
- 从隔离区中恢复对象前先询问
- 从隔离区中恢复对象并且不扫描前先询问
- 执行计划任务中的已计划任务前先询问
- 显示 Outlook Express 和 Windows Mail 电子邮件客户端的产品确认对话框

- 显示 Windows Live Mail 的产品确认对话框
- 显示 Outlook 电子邮件客户端的产品确认对话框

转发

如果发生具有所选级别的事件，ESET NOD32 Antivirus 可以自动发送通知电子邮件。打开高级设置 > **通知** > **转发**，然后启用**将通知转发到电子邮件**以激活电子邮件通知。



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（例如，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（例如，启动病毒防护时出现错误或发现威胁）。

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。这可能会导致在短时间内收到许多电子邮件。

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

发件人地址 – 定义发件人地址，发件人地址将显示在通知电子邮件的标题中。

收件人地址 – 定义收件人地址，收件人地址将显示在通知电子邮件的标题中。支持多个值。使用分号作为分隔符。

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□预定义端口为 25）。

ESET NOD32 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。

启用 TLS – 使用 TLS 加密保护警报和通知。

测试 SMTP 连接 – 测试电子邮件将发送到收件人的电子邮件地址。需要填写 SMTP 服务器、用户名、密码、发件人地址和收件人地址。

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，针对警报消息和通知**使用默认消息格式**是最合适的。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。建议您保留预定义格式。但是在某些情况下（例如，如果有自动电子邮件处理系统），可能需要更改邮件格式。

字符集 – 基于 Windows 区域设置（例如□windows-1250□Unicode (UTF-8)□ACSII 7-bit 或日语 (ISO-2022-JP)□□因此□"á" 将更改为 "a" 以及将未知符号更改为 ″?″。

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

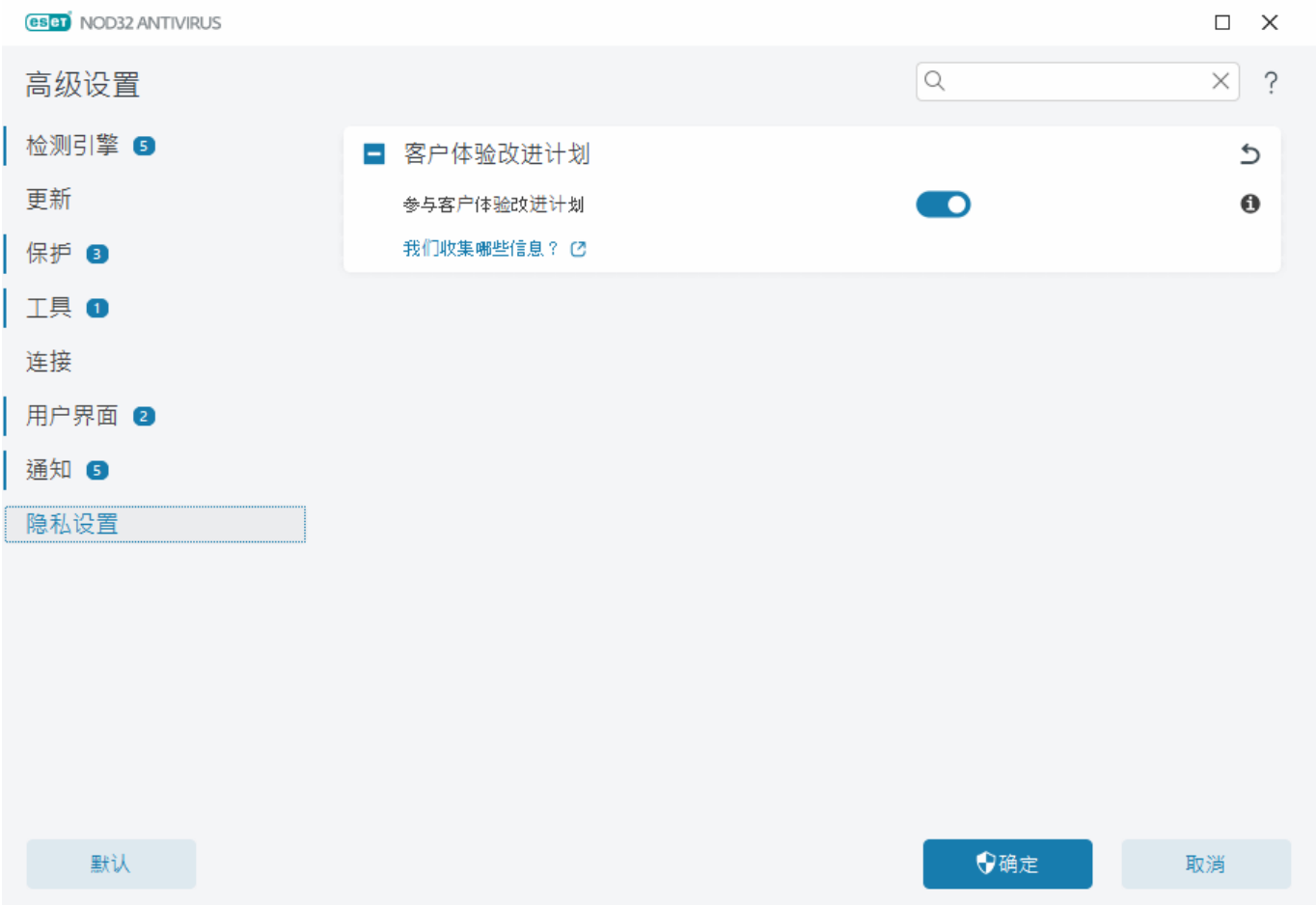
- **%TimeStamp%** – 事件的日期和时间
- **%Scanner%** – 相关模块
- **%ComputerName%** – 发生警报的计算机的名称
- **%ProgramName%** – 生成警报的程序
- **%InfectedObject%** – 被感染文件、邮件等的名称
- **%VirusName%** – 感染标识
- **%Action%** – 针对渗透采取的操作
- **%ErrorDescription%** – 非病毒事件的说明

关键字 **%InfectedObject%** 和 **%VirusName%** 仅用于威胁警告邮件，而 **%ErrorDescription%** 仅用于事件邮

件。

隐私设置

打开高级设置 > **隐私设置**



客户体验改进计划

启用**参与客户体验改进计划**旁边的滑块，以加入客户体验改进计划。加入后，即可向 ESET 提供与使用 ESET 产品有关的匿名信息。收集的数据将帮助我们改进您的体验，绝不会与第三方共享。我们收集哪些信息？

恢复为默认设置

对于所有模块，在“**高级设置**” 中单击默认值可恢复所有程序设置。这将重置为它们在全新安装后所具有的状态。

另请参阅导入和导出设置

恢复当前部分中的所有设置

单击弯曲箭头 ，以将当前部分中的所有设置恢复为 ESET 定义的默认设置。

请注意，单击**恢复为默认值**后，进行过的所有更改都将丢失。

恢复表格内容 – 启用后，已手动或自动添加的规则、任务或配置文件将丢失。

另请参阅导入和导出设置

保存配置时出错

此错误消息表明，这些设置因出现错误而未正确保存。

这通常表示尝试修改程序参数的用户：

- 没有足够的访问权限或没有修改配置文件和系统注册表所需的必要操作系统权限。
  > 要执行所需的修改，系统管理员必须登录。

- 最近已在 HIPS 或防火墙中启用了“学习”模式，并尝试更改“高级”设置。
  > 要保存配置并避免配置冲突，请关闭“高级”设置而不保存，并尝试再次进行所需的更改。

第二种最常见的原因是程序无法再正常工作或者已损坏，从而需要重新安装。

命令行扫描程序

可通过命令行启动 ESET NOD32 Antivirus 的病毒防护模块 – 手动（使用“ecls”命令）或使用批处理“bat”文件启动。

ESET 命令行扫描程序用法：

```
ecls [OPTIONS..] FILES..
```

从命令行运行手动扫描程序时，可使用以下参数和开关：

选项

/base-dir=文件夹	从“文件夹”加载模块
/quar-dir=文件夹	隔离“文件夹”
/exclude=MASK	不扫描与“掩码”匹配的文件
/subdir	扫描子文件夹（默认）
/no-subdir	不扫描子文件夹
/max-subdir-level=级别	要扫描的文件夹中的最大子文件夹层数
/symlink	跟踪符号链接（默认）
/no-symlink	跳过符号链接
/ads	扫描 ADS默认）
/no-ads	不扫描 ADS
/log-file=文件	将结果记录到“文件”
/log-rewrite	覆盖输出文件（默认 – 附加）
/log-console	将结果记录到控制台（默认）
/no-log-console	不将结果记录到控制台
/log-all	同时记录清除文件
/no-log-all	不记录干净的文件（默认）

/aind	显示活动指示器
/auto	扫描并自动清除所有本地磁盘中的病毒

扫描程序选项

/files	扫描文件（默认）
/no-files	不扫描文件
/memory	扫描内存
/boots	扫描引导区
/no-boots	不扫描引导区（默认）
/arch	扫描压缩文件（默认）
/no-arch	不扫描压缩文件
/max-obj-size=大小	仅扫描小于指定“大小”兆字节的文件（默认值 0 = 无限制）
/max-arch-level=级别	要扫描的压缩档（嵌套压缩档）中的最大子压缩档层数
/scan-timeout=限制	扫描压缩文件超时时间（秒）
/max-arch-size=大小	如果压缩文件中的文件小于指定“大小”（默认值 0 = 无限制），则仅扫描这些文件
/max-sfx-size=大小	如果自解压文件中的各个文件小于指定“大小”兆字节（默认值 0 = 无限制），则只扫描这些文件
/mail	扫描电子邮件文件（默认）
/no-mail	不扫描电子邮件文件
/mailbox	扫描邮箱（默认）
/no-mailbox	不扫描邮箱
/sfx	扫描自解压文件（默认）
/no-sfx	不扫描自解压文件
/rtp	扫描加壳程序（默认）
/no-rtp	不扫描加壳程序
/unsafe	扫描潜在的不安全应用程序
/no-unsafe	不扫描可能不安全的应用程序（默认）
/unwanted	扫描潜在的不受欢迎应用程序
/no-unwanted	不扫描潜在不受欢迎的应用程序（默认）
/suspicious	扫描可疑应用程序（默认）
/no-suspicious	不扫描可疑应用程序
/pattern	使用病毒库（默认）
/no-pattern	不使用病毒库
/heur	启用启发式扫描（默认）
/no-heur	禁用启发式扫描
/adv-heur	启用高级启发式扫描（默认）
/no-adv-heur	禁用高级启发式扫描
/ext-exclude=具有指定扩展名的文件	不扫描具有指定“扩展名”的文件（用冒号分隔）

/clean-mode=模式	对被感染的对象使用清除“模式” 以下选项可用： • `none`（默认）- 不会自动进行清除。 • `standard` - ecls.exe 将尝试自动清除或删除被感染的文件。 • `strict` - ecls.exe 将尝试自动清除或删除被感染的文件，且无需用户干预（在删除文件之前，您不会收到提示）。 • `rigorous` - ecls.exe 将在不尝试清除的情况下删除文件，无论文件是什么。 • `delete` - ecls.exe 将在不尝试清除的情况下删除文件，但将避免删除敏感文件，如 Windows 系统文件。
/quarantine	将被感染的文件（若已清除）复制到隔离区 （补充清理时执行的操作）
/no-quarantine	不将被感染的文件复制到隔离区

常规选项

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

退出代码

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

退出代码大于 100 表示未扫描文件，该文件可能被感染。

常见问题解答

可以在下面找到一些最常见的问题和难题。单击主题标题可了解如何解决您的难题：

- 如何更新 ESET NOD32 Antivirus
- ESET NOD32 Antivirus 已检测到威胁
- 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（每周）
- 如何解锁高级设置
- 如何通过 ESET HOME 解决产品停用

如果您的问题未包含在上面的列表中，请尝试搜索 ESET NOD32 Antivirus 联机帮助。

如果在 ESET NOD32 Antivirus 联机帮助中找不到难题/问题的解决方案，则可以访问我们定期更新的在线 ESET 知识库。下面包含了指向我们最受欢迎的知识库文章的链接：

- 如何续订订阅？
- 安装 ESET 产品时，我收到了激活错误消息。它是什么意思？
- 使用激活密钥激活我的 ESET Windows 家庭版产品
- 卸载或重新安装我的 ESET 家庭版产品
- 我收到关于我的 ESET 安装提前结束的消息
- 续订订阅后我应该执行什么操作？（家庭用户）
- 如果我更改了我的电子邮件地址会发送什么情况？
- 将我的 ESET 产品传输到新的计算机或设备
- 如何以安全模式启动 Windows 或在网络中使用安全模式
- 排除阻止安全的网站
- 允许屏幕阅读器软件访问 ESET GUI

如有必要，可以联系我们的技术支持，并提供您的问题或疑问。

如何更新 ESET NOD32 Antivirus

可以通过手动或自动方式更新 ESET NOD32 Antivirus。若要触发更新，请在主程序窗口中单击**更新**，然后单击**检查更新**。

默认安装设置会创建每小时执行一次的自动更新任务。如果需要更改时间间隔，请浏览到**工具** > 计划任务。

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**扫描计算机**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. 如果要扫描磁盘的选定部分，请单击**自定义扫描**，然后选择要在其中扫描病毒的目标。

有关其他信息，请参阅：

- ESET 知识库文章
- 隔离区

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。以下选项可用：**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(小时)**滚动框来定义间隔）

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

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

如何计划每周计算机扫描

要计划定期任务，请打开主程序窗口，然后单击**工具 > 计划任务**。下面是介绍如何计划每周扫描一次本地驱动器的任务的简要指南。有关更详细的说明，请参阅我们的知识库文章。

要计划扫描任务：

1. 单击主计划任务屏幕中的**添加**。
2. 输入任务的名称，然后从**任务类型**下拉菜单中选择**手动计算机扫描**。
3. 选择**每周**作为任务频率。
4. 设置将执行任务的日期和时间。

5. 如果计划任务由于任何原因（例如，计算机已关闭）而无法运行，请选择**尽快运行任务**以便在稍后执行任务。

6. 检查计划任务的摘要并单击**完成**。

7. 从**目标**下拉菜单中选择**本地驱动器**。

8. 单击**完成**以应用此任务。

如何解锁受密码保护的高级设置

当要访问受保护的高级设置时，将显示用于输入密码的窗口。如果已忘记或遗失密码，请单击**恢复密码**，然后键入用于订阅注册的电子邮件地址。ESET 会发送一封内含验证码的电子邮件。键入该验证码，然后填写并确认新密码。验证码的有效时间为 7 天。

通过 ESET HOME 帐户恢复密码 – 如果用于激活的订阅与 ESET HOME 帐户关联，则使用此选项。键入用于登录到 ESET HOME 帐户的电子邮件地址。

如果不记得电子邮件地址或恢复密码时遇到困难，请单击**联系技术支持**。您将重定向到 ESET 网站，以便联系我们的技术支持部门。

为技术支持生成代码 – 此选项会生成技术支持代码。复制由技术支持提供的代码，然后单击**我有验证码**。键入该验证码，然后填写并确认新密码。验证码的有效时间为 7 天。

有关详细信息，请参阅在 ESET Windows 家庭版产品中解锁设置密码。

如何通过 ESET HOME 解决产品停用

产品未激活

当订阅所有者从 ESET HOME 门户中停用您的 ESET NOD32 Antivirus 或与您的 ESET HOME 帐户共享的订阅不再共享时，将显示此错误消息。要解决此问题，请执行以下操作：

- 单击**激活**，然后使用激活方法之一来激活 ESET NOD32 Antivirus。
- 联系订阅所有者，并提供您的 ESET NOD32 Antivirus 已由订阅所有者停用或订阅不再与您共享的信息。所有者可以在 ESET HOME 中解决该问题。

产品已停用，设备已断开连接

在从 ESET HOME 帐户中删除设备后，将显示此错误消息。要解决此问题，请执行以下操作：

- 单击**激活**，然后使用激活方法之一来激活 ESET NOD32 Antivirus。
- 联系订阅所有者，并提供您的 ESET NOD32 Antivirus 已停用且设备已与 ESET HOME 断开连接的信息。
- 如果您是订阅所有者且未注意到这些更改，则查看 ESET HOME 活动摘要。如果您发现任何可疑活动，则更改 ESET HOME 帐户密码，并联系 ESET 技术支持。

产品已停用，设备已断开连接

在从 ESET HOME 帐户中删除设备后，将显示此错误消息。要解决此问题，请执行以下操作：

- 单击**激活**，然后使用激活方法之一来激活 ESET NOD32 Antivirus
- 联系订阅所有者，并提供您的 ESET NOD32 Antivirus 已停用且设备已与 ESET HOME 断开连接的信息。
- 如果您是订阅所有者且未注意到这些更改，则查看 ESET HOME 活动摘要。如果您发现任何可疑活动，则更改 ESET HOME 帐户密码，并联系 ESET 技术支持

产品未激活

当订阅所有者从 ESET HOME 门户中停用您的 ESET NOD32 Antivirus 或与您的 ESET HOME 帐户共享的订阅不再共享时，将显示此错误消息。要解决此问题，请执行以下操作：

- 单击**激活**，然后使用激活方法之一来激活 ESET NOD32 Antivirus
- 联系订阅所有者，并提供您的 ESET NOD32 Antivirus 已由订阅所有者停用或订阅不再与您共享的信息。所有者可以在 ESET HOME 中解决该问题。

0

客户体验改进计划

通过加入客户体验改进计划，即可向 ESET 提供与产品使用有关的匿名信息。有关数据处理的详细信息在隐私政策中提供。

您同意

参与此计划是自愿行为，并需要您的同意。加入后，参与者处于被动状态，这意味着您无需采取任何进一步操作。可以随时更改产品设置来撤销同意。这样做将阻止我们进一步处理您的匿名数据。

您可以随时更改产品设置以撤销同意：

- 在 ESET Windows 家庭版产品中更改“客户体验改进计划”设置

我们收集哪些类型的信息？

有关与产品交互的数据

此信息可告知我们有关产品使用情况的更多信息。感谢提供此信息，我们通过该信息可以获取诸如哪些功能最常用、用户修改了哪些设置或用户使用产品所花费的时间之类的信息。

有关设备的数据

我们收集此信息是为了了解我们的产品在何处以及哪些设备上使用。典型示例是设备型号、国家/地区以及操作系统的版本和名称。

错误诊断数据

还会收集有关错误和崩溃情况的信息。例如，发生了何种错误以及哪些操作导致发生该错误。

我们为什么要收集此信息？

此匿名信息使我们可以为您（即我们的用户）改进我们的产品。它帮助我们使产品相关性最高、易于使用并尽可能完美无缺。

谁将控制此信息？

ESET, spol. s r.o. 是该计划中所收集数据的唯一控制者。此信息不会与第三方共享。

最终用户许可协议

自 2021 年 10 月 19 日起生效。

重要说明:在下载、安装、复制或使用前，请仔细阅读产品应用程序的以下条款。**下载、安装、复制或使用本软件即表示您同意这些条款和条件并承认隐私政策** 隐私政策

最终用户许可协议

本最终用户使用许可协议（“协议”）由 ESET, spol. s r. o..(“ESET”或“提供商”）与作为自然人或法人的您（“您”或“最终用户”）签订ESET 位于 Einsteinova 24, 85101 Bratislava, Slovak Republic注册地为布拉迪斯拉发第一地区法院商业注册处，企业性质为股份有限公司，注册号 3586/BBIN 31333532 协议授权您使用此处第 1 条中定义的软件。此处条款 1 中定义的软件可能存储在数据承载工具上、通过电子邮件发送、从 Internet 下载、从提供商的服务器下载或者按照以下指定的条款从其他来源获得。

这不是购买合同，而是关于最终用户权利的协议。无论是此软件的副本，还是经过商业包装的包含此软件的物理介质，亦或根据本协议最终用户有权使用的任何其他副本，所有权均归提供商所有。

在安装、下载、复制或使用软件过程中单击“我接受”或“我接受…”，即表示您同意本协议的条款和条件并确认隐私政策。如果您不同意本协议的任意条款及条件和/或隐私政策，请立刻单击取消选项、取消安装或下载、销毁或退还本软件、安装介质、随附文档和购买发票给提供商或您从中获取软件的渠道。

您同意使用软件表示您已经阅读本协议，您理解并同意遵守本协议的条款。

1.**软件。**本协议中的“软件”是指: (i) 本协议附带的计算机程序及其所有组成部分(ii) 磁盘CD-ROMDVD电子邮件及任何附件或附带本协议提供的其他介质的所有内容，包括数据承载工具提供、通过电子邮件提供或通过 Internet 下载的对象代码形式的软件(iii) 任何有关本软件的书面说明材料和任何其他相关文档，包括但不限于所有软件说明、软件规格、软件特点或操作说明、使用软件的操作环境的说明、使用或安装软件的说明，或任何关于如何使用软件的说明(以下称“文档”)(iv) 软件的副本、软件错误的修复程序、软件的附加程序、软件的扩展、软件的修改版本及软件组件更新(如果有)，关于这一点，提供商根据本协议第 3 条授予您许可。软件将仅以可执行目标代码的形式提供。

2.**安装、计算机和许可证密钥。**数据承载工具上提供、通过电子邮件发送、从 Internet 下载、从提供商服务器下载或从其他来源获得的软件需要安装。文档中指定了安装方式。任何可能对本软件有不利影响的计算机程序或硬件都不能安装在安装本软件的计算机上。计算机是指硬件，包括但不限于个人计算机、笔记本电脑、工作站、掌上电脑、智能电话、手持电子设备或本软件针对其而设计并将于其上安装和/或使用的其他电子设备。任何可能对本软件有不利影响的计算机程序或硬件都不能安装在安装本软件的计算机上。计算机是指硬件，包括但不限于个人计算机、笔记本电脑、工作站、掌上电脑、智能电话、手持电子设备或本软件针对其而设计并将于其上安装和/或使用的其他电子设备。许可证密钥是指唯一的符号、字母、数字或特殊符号的序列，提供给最终用户以允许本软件的合法使用、其特定版本或根据本协议延长许可证

的期限。

3.**许可**。如果您同意本条件，同意本协议条款并且遵守此处规定的所有条款，提供商将授予您以下权利(“许可”)：

a) **安装和使用。**您将具有在计算机硬盘或其他永久介质中安装软件以进行数据存储，在计算机系统内存中安装和存储软件，实施、存储和显示软件的非独占、不可转让的权利。

b) **许可数量规定。**软件的使用权利受最终用户数量约束。一位最终用户指(i) 在一个计算机系统上安装软件；或 (ii) 如果许可约束范围为邮箱数量，则单个用户指的是通过邮件用户代理“MUA”接收电子邮件的计算机用户。如果 MUA 接受电子邮件，然后将其自动分发到多个用户，则最终用户数量应根据收到电子邮件的实际用户数量确定。如果邮件服务器执行邮件网关的功能，则最终用户数量应等于上述网关所服务的邮件服务器用户数量。如果未指定数量的电子邮件地址（例如通过别名）指向一个用户，用户接受这些地址，并且客户端不自动将邮件分发给大量用户，则需要一台计算机的许可证。您不得同时在多台计算机上使用同一许可。仅当最终用户根据限制（因提供商授予的许可证数量而引起）而有权使用本软件时，最终用户才有权输入本软件的许可证密钥。许可证密钥被视为保密信息，除非本协议或提供商允许，否则您不得与第三方共享许可证或允许第三方使用许可证密钥。如果您的许可证密钥被盗用，请立即通知提供商。

c) **家庭版/商业版。**本软件的家庭版应仅在私人和/或非商业环境中专供家庭和家人使用。必须获得本软件的商业版，才能在商业环境中使用，以及将本软件用于邮件服务器、邮件中继、邮件网关或 Internet 网关。

d) **许可条款。**您使用软件的权利将受时间限制。

e) **OEM 软件。**分类为“OEM”的软件应限于在您获得该软件的计算机上使用。不得转移到其他计算机。

f) **NFR/试用软件。**分类为“非转售性”NFR 或试用的软件不得用于付费用途，只能用于演示或测试软件功能。

g)**许可终止。**许可将在授予的期限结束时自动终止。如果不遵守本协议的任何条款，提供商有权撤销协议，不影响提供商在此类不测事件下的任何权利或合法补救措施。如果取消许可，您必须立刻删除、销毁本软件及所有备份副本，或自行承担费用将软件及所有备份副本返还至 ESET 或您购买软件的地方。在许可终止后，提供商有权取消最终用户使用本软件功能（这些功能需要连接到提供商的服务器或第三方服务器）的权利。

4.**具有数据收集和 Internet 连接要求的功能。**要正确操作本软件，需要连接到 Internet并且必须定期连接到提供商服务器或第三方服务器和遵循“隐私政策”的适用的数据收集。以下软件功能要求必须连接到 Internet 和适用的数据收集：

a) **软件更新。**提供商有权时常发布本软件的更新或升级（即“更新”），但没有义务提供更新。此功能在软件标准设置下启用，因此自动安装更新，除非最终用户禁用自动安装更新。为了提供更新，需要进行许可证真实性验证，包括根据“隐私政策”获取其上安装本软件的计算机和/或平台的相关信息。

任何更新的提供可能都要遵循生命周期结束政策（即“EOL 政策”），可通过访问 https://go.eset.com/eol_home 了解该政策。在本软件或其任何功能达到 EOL 政策中定义的生命周期结束日期后，将不会提供任何更新。

b) **将渗透和信息发送给提供商**。本软件包含多项功能，这些功能用于收集计算机病毒和其他恶意计算机程序与可疑对象、问题对象、潜在不受欢迎对象或潜在不安全对象(例如文件URLIP 数据包和以太网帧)的样本(“渗透”)并将其发送给提供商，包括但不限于安装过程、安装本软件的计算机和/或平台的信息，本软件的操作和功能信息(“信息”)。这些信息和渗透可能包含已安装本软件的计算机上的最终用户或其他用户的数据(包括随机或意外获得的个人数据)，以及受附带相关联元数据的渗透影响的文件。

信息和渗透可通过以下软件功能进行收集：

i.LiveGrid 信誉系统功能包括将与渗透有关的单向哈希收集起来并发送给提供商。可在本软件的标准设置下

启用此功能。

ii.LiveGrid 反馈系统功能包括将附带相关元数据的威胁和信息收集起来并发送给提供商。此功能可在本软件的安装过程中由最终用户激活。

提供商将仅使用获得用于分析和检查威胁以及改善软件和许可证真实性验证的“信息”和“威胁”，并将采取合理措施保证所获信息安全。如果您启用本软件的上述功能，则“威胁”和“信息”可由提供商按照“隐私政策”和相关法规收集和处理。您可以随时停用此功能。

就本协议而言，有必要收集、处理和存储数据，使提供商能够根据隐私政策识别您的身份。您特此承认提供商以自有方式检查您是否按照本协议条款使用此软件。您特此承认，就本协议而言，需要通过与提供商计算机系统或作为其分销和支持网络的商业合作伙伴进行软件通信来传输数据，以确保软件功能正常、授权使用软件以及保护提供商的权利。

本协议缔结后，提供商或作为其分销和支持网络的任何商业合作伙伴均有权传输、处理和存储标识您的重要数据，用于计费目的、本协议的履行以及您计算机上通知的传输。

关于隐私、个人数据保护和您作为数据主体所拥有权利的详细信息可以在“隐私政策”（“隐私政策”可在提供商的网站上找到，并可在安装过程中直接访问）中找到。您还可以从软件的帮助部分中访问此信息。

5.**行使最终用户的权利**。您必须亲自或通过员工行使最终用户权利。您只能将软件用于确保操作安全和保护购买了许可证的计算机或计算机系统

6.**权利的限制。**您不得复制、分发、提取组件或创建软件的衍生版本。使用软件时，您必须遵守以下限制：

a) 您可以在永久存储介质上创建一份软件副本作为备份副本，前提是不在任何其他计算机上安装或使用该存档备份副本。创建软件的任何其他副本应视为违反本协议。

b) 您不得以本协议明确提供的方式以外的任何其他方式使用、修改、翻译、复制或转让软件或软件副本的使用权。

c)您不得出售软件、授予从属许可、将软件出租给他人，或从他人租用软件或借出软件用于提供商业服务。

d) 您不得在法律明确禁止此类限制的范围之外以任何其他方式反向工程、反编译、反汇编软件，或试图获得软件的源代码。

e) 您同意使用软件的方式必须符合有关软件使用的相关法律中的所有适用法规，包括但不局限于，符合版权法和其他知识产权中适用的限制。

f) 您同意将只以不会限制其他最终用户获取这些服务的可能性的方式使用该软件及其功能。提供商保留限制向个体最终用户提供的服务范围，以确保最大数量的最终用户能够使用服务的权利。限制服务范围还将意味着完全杜绝在提供商的服务器或与软件的特定功能相关的第三方服务器上使用软件的任何功能和删除数据及信息的可能性。

g) 您同意不从事涉及使用许可证密钥的任何违反本协议条款的活动，或向任何无权使用本软件的人员提供许可证密钥，例如以任何形式转让已使用或未使用的许可证密钥，以及未经授权复制或分发复制或生成的许可证密钥，或从提供商以外的来源获得许可证密钥从而使用本软件。

7.**版权**。软件及所有权利，包括但不局限于所有权和知识产权，归 ESET 和/或其许可提供商所有。它们受国际条约条款以及使用此软件的国家的所有其他适用法律保护。软件的结构、组织和代码均为 ESET 和/或其许可提供商的重要商业机密和保密信息。您不得复制软件，第 6 (a) 款中指定的情况除外。允许按照本协议创建的任何副本必须包含与软件上显示的相同版权和其他所有权声明。如果您反向工程、反编译、反汇编源或试图以违反本协议条款的方式获得软件源代码，则您同意自此类行为开始起获得的任何信息将自动且不可逆地转让给提供商，并全部为提供商所有。

8.**保留权利**。除本协议中未明确授予您作为软件最终用户的权利以外，提供商特此保留所有软件权利。

9.**多个语言版本，双介质软件，多个副本**。如果软件支持多个平台或多种语言，或者如果您获得多个软件副本，则只能将软件用于已购买许可的计算机系统数量和版本。您不得将不使用的软件的任何版本或副本出售、出租、租用、授予从属许可、借出或转让给其他人。

10.**协议开始和终止。**本协议自您同意本协议条款之日起生效。您可以通过永久卸载、销毁或返还（费用自付）软件、所有备份副本以及提供商或其商业合作伙伴提供的所有相关材料来随时终止本协议。您使用软件及其任何功能的权利可能要遵循 EOL 政策。在本软件或其任何功能达到 EOL 政策中定义的生命周期结束日期后，您使用本软件的权利将终止。不考虑本协议终止方式，第 7、8、11、13、19 和 21 款的条款应保持无限期有效。

11.**最终用户声明**。作为最终用户，您了解软件“按原样”提供，不带任何明示或暗示担保，在适用法律允许的最大范围内。提供商、其许可提供商或分支机构或者版权所有者都不得提供任何明示或暗示的陈述或保证，包括但不限于适销性保证、特定用途适用性保证或对软件不侵犯任何第三方专利、版权、商标或其他权利的保证。提供商或任何其他方均不保证软件包含的功能符合您的要求，或软件操作将顺畅无错为实现预期目的而选择此软件以及安装、使用此软件和软件应用结果的全部责任和风险由您承担。

12.**无其他义务**。除本协议特别列出的义务以外，本协议不对提供商及其许可提供商施加任何其他义务。

13.**责任限制**。在适用法律允许的最大范围内，任何情况下提供商、其员工或许可提供商均不对以下损失负责：在适用法律允许的最大范围内，任何情况下提供商、其员工或许可提供商均不对以下损失负责：以任何形式造成的任何赢利、收入或销售额损失，任何数据损失，为获得备用物品或服务支付的额外费用，财产损失、人身伤害，营业中断，商业信息损失，或任何特殊、直接、间接、意外、经济、涵盖、犯罪、特殊或后继损失。无论这些损失是由合约、故意误操作、疏忽或其他责任理论造成，还是因安装、使用或无法使用本软件导致，提供商、其员工或许可提供商均不负责，即使已经通知提供商或其许可提供商或分支机构此类损失的可能。由于某些国家和某些法律不允许免责，但可能允许责任限制，因此提供商、其员工或许可提供商的责任应限制为您购买许可所支付的价格。

14. 本协议中的任何条款均不影响被法律认可具备消费者权利和地位的一方的权利。

15.**技术支持**ESET 或 ESET 委托的第三方将出于自行考量提供技术支持，不具有任何保证或声明。在本软件或其任何功能达到EOL政策中定义的生命周期结束日期后，将不会提供任何技术支持。提供技术支持前，最终用户需要备份所有现有数据、软件和程序工具ESET 和/或 ESET 委托的第三方不承担因提供技术支持导致的数据、财产、软件或硬件破坏或损失或者利润损失ESET 和/或 ESET 委托的第三方保留决定解决问题是否超出技术支持范围的权利ESET 保留出于自行考量拒绝、暂停或终止提供技术支持的权利。出于提供技术支持的目的，可能需要遵循“隐私政策”的许可证信息、信息和其他数据。

16.**转让许可**。除非违背协议条款，否则软件可以在不同计算机系统之间转移。如果不违背协议条款，最终用户仅有权在提供商同意下，将许可及从本协议产生的所有权利转让给其他最终用户，并受以下条款约束(i) 原始最终用户不得保留软件的任何副本(ii) 权利转让必须从原始最终用户转交给新最终用户(iii) 新最终用户必须承担原始最终用户在本协议条款下承担的所有权利和义务(iv) 原始最终用户必须向新最终用户提供文档，证明第 17 款下指定的软件正版性。

17.**证明软件的正版性。**最终用户可以采用以下任意方式证明软件的使用权(i) 通过提供商或提供商指定的第三方发布的许可证书(ii) 通过书面许可协议，如果已缔结此类协议(iii) 通过提交发送给提供商的包含许可详细信息(用户名和密码)的电子邮件。出于证明软件正版性的目的，可能需要遵循“隐私政策”的许可证信息和最终用户身份数据。

18.**政府当局和美国政府许可**。软件提供给政府当局（包括美国政府）时具有本协议介绍的许可权利和限制。

19.**贸易控制合规性**

a) 您将不得直接或间接地向任何人出口、再出口、转让或以其他方式提供该软件，不得以任何方式使用该软件，也不得涉及任何行为，否则可能导致 ESET 或其控股公司、其子公司及其任何控股公司的子公司以及由其控股公司控制的实体（“关联公司”）违反《贸易管制法》或承担《贸易管制法》所规定的不良后果，包括

i. 美国、新加坡、英国、欧盟或其任何成员国的任何政府、州或监管机构、将履行本协议规定义务的国家/地区、成立或运维 ESET 或其任何关联企业的国家/地区颁布或通过的针对出口、再出口或转让商品、软件、技术或服务进行控制、限制或施加许可要求的任何法律，和

ii. 美国、新加坡、英国、欧盟或其任何成员国的任何政府、州或监管机构、将履行本协议规定义务的国家/地区、成立或运维ESET或其任何关联企业的国家/地区实施的任何经济、金融、贸易或其他方式的制裁、限制、禁运、进出口禁令、禁止转移资金或资产或提供服务或其他等效措施。

（上述“i.”和“ii.”部分中提到的法律行为统称为“《贸易管制法》”）。

b) 如果发生以下情况，ESET 有权立即中止或终止这些条款所规定的义务：

i.ESET 合理认为用户已违反或可能违反了本协议第 19 a) 款的规定；或

ii. 最终用户和/或软件受《贸易管制法》约束，因此 ESET 合理认为继续履行本协议所规定的义务可能会导致 ESET 或其关联公司违反《贸易管制法》，或承担《贸易管制法》所规定的不良后果。

c) 本协议无意，也不应理解或解释为诱导或要求任何一方以不遵循《贸易管制法》、受《贸易管制法》处罚或禁止的方式行事或不作为（或者同意行事或不作为）。

20.**通知**。所有通知、返还的软件和文档必须交付给 ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic，但不影响 ESET 根据本协议的第 22 条有权向您传达对本协议、隐私政策、EOL 政策以及文档所做的任何更改，ESET 可能会通过软件向您发送电子邮件、应用内通知，也可能会在我们的网站上发布通信帖子。您同意接收 ESET 以电子形式发送的法律通信，包括有关条款、特殊条款或隐私政策变更的任何通信、任何合同修改/赞同、要约邀请、通知或其他法律通信。此类电子通信应等同于书面形式接收，除非适用法律明确要求采用其他形式的通信。

21.**适用法律**。本协议受斯洛伐克法律管辖，并按斯洛伐克法律解释。最终用户和提供商同意，法律与联合国国际货物销售合同公约之间的冲突原理不适用。您明确同意，与提供商之间发生的任何索赔或争端，或任何方式的与软件使用相关的索赔或争端，其唯一裁决权属于斯洛伐克布拉迪斯拉发第一地区法院，并且您明确同意上述法院作出的裁决。

22.**通用条款**。如果本协议中的任何条款无效或无法执行，将不影响协议其他条款的有效性，按照此处规定的条款这些条款仍然有效且可执行。本协议已以英文履行。如果出于方便目的或任何其他目的而准备了本协议的任何翻译，或者本协议的各语言版本之间存在差异，则以英文版本为准。

ESET 保留随时更改本软件以及出于以下目的修订本协议的条款、其附件、附录、隐私政策、EOL 政策和文档或其任何部分的权利：(i) 反映对本软件或 ESET 开展业务方式的更改；(ii) 出于法律、法规或安全原因，或 (iii) 防止滥用或损害。将通过电子邮件、应用内通知或其他电子方式通知您本协议的任何修订。如果您不同意对本协议的拟议变更，可以在收到变更通知后的 30 内，根据第 10 条终止履行本协议。除非您在该时限内终止履行本协议，否则拟议变更将视为被接受，并自您收到变更通知之日起开始对您生效。

您与提供商签署的本协议是关于本软件的唯一完整协议，它完全取代任何之前的关于软件的表述、讨论、承诺、沟通或广告。

协议附录

连网设备安全评估。适用于“连网设备安全评估”的附加条款如下所示：

本软件包含用于检查最终用户本地网络的安全性和本地网络中设备的安全性的功能，该功能需要本地网络名称和本地网络中设备的相关信息，例如本地网络中设备的状态、类型、名称、IP 地址和 MAC 地址(与许可证信息有关)。该信息还包括路由器设备的无线安全类型和无线加密类型。该功能可能还会提供用于保护本地网络中设备的安全软件解决方案的相关信息。

防止数据滥用。适用于“防止数据滥用”的附加条款如下所示：

该软件具有防止因计算机被盗而导致关键数据丢失或滥用的功能。如果您选择激活此功能，将收集被盗计算机的相关数据并将其发送至 ESET。其中可能包括有关计算机的网络位置、计算机屏幕上显示的内容、计算机的配置和/或连接到计算机的照相机记录的数据。要激活该功能，需要创建 MEC ESET HOME 帐户，该功能可通过此帐户激活计算盗窃事件的数据收集。如果您选择激活软件的这一功能，将收集被盗计算机的相关数据并将其发送至提供商，其中可能包括有关计算机的网络位置、计算机屏幕上显示的内容和计算机配置的数据或连接到计算机的照相机记录的数据(以下简称“数据”)。最终用户有权由此功能获得并通过“ESET HOME 帐户”专门提供的数据用于修整计算机被盗的不利情况。此功能作为唯一目的，提供商可按照“隐私政策”和相关法规处理数据。提供商将允许最终用户在必要时段(不应超过“隐私政策”所规定的保留期限)内访问数据，以达到获取数据所为的目的。对数据滥用的防护应仅用于最终用户拥有合法访问权限的计算机和帐户。任何非法使用会被报告至相关主管部门。提供商将遵守相关法律并在发生滥用时协助执法部门。您同意并确认您有责任保护用于访问 ESET HOME 帐户的密码，并同意不会向任何第三方泄露您的密码。最终用户将对任何使用防止数据滥用功能和 ESET HOME 帐户的活动(授权或未授权)负责。如果 ESET HOME 帐户被盗用，请立即通知提供商。“防止数据滥用”的附加条款应仅适用于 ESET Internet Security 和 ESET Smart Security Premium 最终用户。

ESET Secure Data适用于 ESET Secure Data 的附加条款如下所示：

1. 定义。在 ESET Secure Data 的这些附加条款中，以下字词具有如下相应含义：

a) “信息”使用软件加密或解密的任何信息或数据；

b)产品ESET Secure Data本软件和本文档；

c) “ESET Secure Data”用于加密并解密电子数据的软件；

所有对复数的引用应包括单数，所有对阳性的引用应包括阴性和中性；反之亦然。无具体定义的词语应遵循本协议规定的定义使用。

2. 附加最终用户声明。您承认并接受：

a) 您负责保护、维护和备份信息；

b) 您应该先完全备份您计算机上的所有信息和数据(包括但不限于任何重要的信息和数据)，然后再安装 ESET Secure Data。

c) 您必须确保安全记录用于设置和使用 ESET Secure Data 的任何密码或其他信息，还必须将生成的所有加密密钥、许可证代码、密钥文件和其他数据的副本备份到单独的存储介质；

d) 您对产品的使用负有责任。提供商对因任何未经授权使用或错误使用信息或其他数据的加密或解密而造成的任何损失、索赔或损害不负任何责任，无论信息或其他数据以何种方式存储在何处都是如此；

e) 虽然提供商已采取所有合理措施来确保 ESET Secure Data 的完整性和安全性，但本产品(或其中任一功能)不得在任何依赖自动防故障装置安全级别的领域中使用，也不得在具有潜在危害或危险环境(包括但不限于核设施、飞行器导航、控制或通信系统、武器和防御系统以及生命支持或生命监测系统)中使用；

f) 您作为最终用户，对确保本产品提供的安全级别和加密满足您的要求负有责任；

g) 您对产品或其中任一功能的使用负有责任，包括但不限于确保此类使用遵守斯洛伐克共和国或使用本产品所在的其他国家、地区或州的所有适用法律和法规。您必须确保：在使用本产品之前，您已确认本产品不违反任何政府(斯洛伐克共和国或其他任何国家/地区)的禁令；

h) ESET Secure Data 本软件可以不时地连接提供商服务器以检查许可证信息、可用补丁程序、服务包和其他更新(可以用于改进、维护、修改或增强 ESET Secure Data 的运行)并且可能会根据“隐私政策”发送与其功能有关的常规系统信息。

i) 提供商对因本软件使用期间所生成或存储的密码、设置信息、加密密钥、许可证激活代码和其他数据的丢失、被盗、误用、损坏、损毁或破坏而导致的任何损失、损害、费用或索赔不负任何责任。

ESET Secure Data 的附加条款应仅适用于 ESET Smart Security Premium 最终用户。

Password Manager 软件。适用于“Password Manager 软件”的附加条款如下所示：

1. 附加最终用户声明。您承认并接受您不得：

a) 使用 Password Manager 软件运行可能与人类生命或财产存在利害关系的任何关键任务应用程序。您要明白Password Manager 软件不是针对此类目的设计的，如果本软件在此类情形中运行失败可能会导致死亡、人身伤害或严重的财产损失或环境损害，而提供商对此类后果不负任何责任。

Password Manager 软件未设计、旨在或许可用于要求使用故障安全控制的危险环境，包括但不限于核设施、飞机导航或通信系统、空中交通管制以及生命支持或武器系统的设计、建造、维护或操作。提供商明确否认对适用于此类目的做任何明示或默示保证。

b) 以违反本协议或斯洛伐克共和国(或您所在地司法管辖权)的法律的方式使用 Password Manager 软件。具体而言，您不得使用 Password Manager 软件实施或从事任何违法活动，包括上载含有有害内容或可能用于任何违法活动的内容的数据，或者以任何方式违反法律或侵犯任何第三方权利(包括任何知识产权)，包括但不限于任何试图获取存储(就“Password Manager 软件”的这些附加条款而言，“存储”是指由提供商或提供商和用户以外的第三方出于支持同步和备份用户数据的目的而管理的数据存储空间)中帐户的访问权限，或者试图获取任何其他 Password Manager 软件或存储用户的帐户和数据的访问权限。如果您违反其中任何一项规定，提供商有权立即终止此协议并向您收取任何采取必要补救措施所产生的费用，以及采取任何必要步骤阻止您进一步使用 Password Manager 软件，不会退还任何款项。

2. 责任限制Password Manager 软件“按原样”提供。不提供任何明示或默示担保。使用本软件由您自行承担风险。本产品对任何数据丢失、损坏、服务可用性受限不负任何责任，包括 Password Manager 软件为了数据同步和备份而向外部存储发送的任何数据。使用 Password Manager 软件加密数据并不意味着提供商会对该数据的安全性承担任何责任。您明确同意Password Manager 软件采集、使用、加密、存储、同步或发送的数据还可以存储到第三方服务(仅适用于 Password Manager 的使用，其中同步和备份服务已启用)。如果提供商酌情选择使用此类第三方存储、网站Web 门户、服务器或服务，提供商对此类第三方服务的质量、安全性或可用性不负任何责任；提供商不对以下方面替您承担责任：第三方违反合同或法律义务，使用本软件期间造成的损害、利润损失、金融或非金融损害赔偿或任何其他类型的损失。提供商对使用 Password Manager 采集、使用、加密、存储、同步或发送的任何数据的内容不负任何责任，对存储中的任何数据的内容也不负任何责任。您确认提供商无权访问存储数据的内容，也不会监视它或删除法律上有害的内容。

提供商拥有改进、升级和修复 Password Manager 软件相关的所有权利(“改进”)，即使任何此类改进是基于您以任何方式提交的反馈、想法或建议。您无权获取与此类改进相关的任何补偿，包括任何版税。

提供商实体和许可方不会为您承担因以下方面造成的索赔和债务：由您或第三方使用 Password Manager 软件、使用或停用任何经纪公司或经销商、销售或购买任何安全产品，无论此类索赔和债务是否基于任何法律或公平原则都是如此。

提供商实体和许可方不会替您承担因以下方面所引起的任何直接、附带、特殊、间接或相应损害赔偿：第三方软件、通过 Password Manager 软件访问的任何数据、您使用或者无法使用或访问 Password Manager 软件、通过 Password Manager 软件提供的任何数据，无论此类损害赔偿是否基于任何法律或公平原则都是如此。此条款规定之外的损害赔偿包括但不限于企业利润损失、人身伤害或财产损失、营运中断、企业或个人信息丢失。某些司法管辖区不允许限制附带或相应损害赔偿，则此约束可能不适用于您。在此种情况下，提供商责任范围将依据适用法律降至最低允许程度。

通过 Password Manager 提供的信息(包括股市行情、分析、市场信息、新闻和财务数据)可能会延迟、不准确，或者含有错误或遗漏，提供商实体和许可方对此不承担任何责任。提供商可能会随时更改或中断 Password Manager 软件的任何方面或功能Password Manager 软件中全部或任一功能或技术的使用，而不

会事先通知您。

如果本文中的条款因某些原因而失效，或者提供商被视为要依据适用法律承担损失、损害赔偿等，当事双方同意提供商替您承担的责任仅限于您支付的许可费用总额。

您同意赔偿、捍卫和维护提供商及其员工、子公司、附属公司、品牌重塑和其他合作伙伴免受来自和针对任何和全部第三方(包括设备所有者或其权利受 Password Manager 软件或存储中使用的数据影响的当事方)的索赔、债务、损害赔偿、损失、成本、支出，以及此类当事方可能因您使用 Password Manager 软件而引发的费用。

3.Password Manager 软件中的数据。除非另有指定以及由您明确选定，否则您输入的将保存到 Password Manager软件数据库中的所有数据将以加密格式保存到您的计算机或由您定义的其他存储设备。您要明白：如果删除或损坏任何 Password Manager 软件数据库或其他文件，则其中包含的所有数据将不可逆地丢失，同时您要理解并接受此类丢失的风险。实际上，您的个人数据以加密格式存储在计算机上并不意味着该信息不会被破解主密码，或获取客户定义的激活设备的访问权限以打开数据库的他人盗用或滥用。您负责维护所有访问方法的安全性。

4. 传输个人数据到提供商或存储。如果您选择此操作仅仅是为了确保及时同步和备份数据Password Manager 软件会将 Password Manager 软件数据库中的个人数据(即密码、登录信息、帐户和身份)通过 Internet 传输或发送到存储。数据专门使用加密形式进行传输。使用 Password Manager 软件填写内含密码、登录或其他数据的在线表单可能会将信息通过 Internet 发送到由您指定的网站。该数据传输不由 Password Manager 软件初始化，因此提供商对与各种提供商支持的任何网站的此类交互的安全性不负任何责任。借助 Internet 的任何事务(不论是否结合使用 Password Manager 软件)由您自己掌控并承担风险，同时您自行承担因下载和/或使用任何此类材料或服务而导致您的任何计算机系统损坏或数据丢失。若要最大程度地降低丢失有价值数据的风险，提供商建议客户定期将数据库和其他敏感文件备份到外部驱动器。提供商不会向您提供恢复丢失或损坏数据的任何协助。如果提供商在用户电脑上的文件损坏或删除时提供用户数据库文件的备份服务，则此类备份服务没有任何保证，同时也并不意味着提供商会为您承担任何责任(无论何时)。

使用 Password Manager 软件，即表示您同意本软件可以不时地连接提供商服务器以检查许可证信息、可用补丁程序、服务包和其他更新(可以用于改进、维护、修改或增强 Password Manager 软件的运行)。本软件可能会发送与 Password Manager 软件有关的常规系统信息。

5. 卸载信息和说明。必须先导出任何您想要保留的数据库中的信息，然后再卸载 Password Manager 软件。

“Password Manager 软件”的附加条款应仅适用于 ESET Smart Security Premium 最终用户。

ESET LiveGuard. 适用于 ESET LiveGuard 的附加条款如下所示：

本软件包含对最终用户提交的文件进行额外分析的功能。提供商应仅遵循隐私政策和相关法律规定，来使用最终用户提交的文件和分析结果。

ESET LiveGuard 的附加条款应仅适用于 ESET Smart Security Premium 最终用户。

EULAID: EULA-PRODUCT-LG-EHSW; 3537.0

隐私策略

ESET, spol. s r. o. 作为数据控制者（以下简称“ESET”或“我们”），保护个人数据对于 ESET, spol. s r. o. 而言尤为重要（注册办公室位于 Einsteinova 24, 851 01 Bratislava, Slovak Republic在布拉迪斯拉发第一地区法院商业注册处注册，企业性质为股份有限公司，注册号为 3586/B业务识别号：31333532） 。我们希望遵守依据《欧盟一般数据保护条例“GDPR”作为法律上所规定的透明度要求。为了达到上述目的，我们发布此隐私政策，唯一目的是告知我们的客户（即作为数据主体的“最终用户”或“您”）有关以下个人数据

保护主题的信息：

- 个人数据处理的法律依据、
- 数据共享和机密性、
- 数据安全性、
- 作为数据主体的权利、
- 个人数据的处理
- 联系人信息。

个人数据处理的法律依据

在数据处理方面，我们根据与个人数据保护有关的适用法律框架所用到的法律依据较少ESET 处理个人数据主要是为了履行 最终用户许可协议 “EULA”与最终用户GDPR 第 6 (1) (b) 款），这适用于提供 ESET 产品或服务，除非另有明确说明，例如：

- 合法权益法律依据GDPR 第 6 (1) (f) 款），使我们可以处理有关客户如何使用我们的服务及其满意度的数据，从而为用户提供我们所能提供的最佳保护、支持和体验。甚至营销也被适用法律确认为合法权益，因此我们通常据此与客户沟通营销。
- 同意GDPR 第 6 (1) (a) 款），当我们认为此法律依据是最适合的法律依据或法律所要求时，我们可能会在特定情形下向您提出要求。
- 遵守法律义务GDPR 第 6 (1) (c) 款），例如订立电子通信、发票或账单文件保留的要求。

数据共享和机密性

我们不会与第三方共享您的数据。但是ESET 是一家通过附属公司或合作伙伴（作为我们销售、服务和支持网络的一部分）在全球运营的公司。出于履行最终用户许可协议的目的（例如，提供服务或支持ESET 所处理的许可、计费和技术支持信息可能会在附属公司或合作伙伴之间传输。

ESET 更愿意在欧盟 (EU) 内处理其数据。但是，根据您所在的位置（在欧盟以外使用我们的产品和/或服务）和/或您选择的服务，可能需要将您的数据传输到欧盟以外的国家/地区。例如，我们使用与云计算相关的第三方服务。在这些情况下，我们会仔细选择服务提供商，并确保通过合同以及技术和组织措施提供相应级别的数据保护。通常，我们同意欧盟标准合同条款，并在必要时提供补充合同规定。

对于欧盟以外的一些国家/地区（例如，英国和瑞士），欧盟已确定提供同等级别的数据保护。由于提供同等级别的数据保护，因此向这些国家/地区传输数据不需要任何特殊授权或协议。

数据安全性

ESET 会实施适当技术和组织措施来确保与潜在风险相称的安全级别。我们会尽最大努力来确保处理系统和服务的持续机密性、完整性、可用性和弹性。但当发生导致您的权利和自由遭受威胁的数据泄漏时，我们会随时通知相关监管机构以及作为数据主体的受影响最终用户。

数据主体的权利

每个最终用户的权利都很重要，我们会告知您，所有最终用户（来自任何欧盟或任何非欧盟国家/地区）在 ESET 都享有以下权利。要行使您数据主体的权利，可以通过支持表单或发送电子邮件至 dpo@eset.sk 与我们联系。出于识别目的，我们会要求您提供以下信息：姓名、电子邮件地址以及（如果有）许可证密钥

或客户编号和公司隶属关系。请勿向我们发送任何其他个人数据，例如出生日期。我们想指出的是，为了能够处理您的请求以及出于识别目的，我们将处理您的个人数据。

撤消同意的权利。撤消同意的权利仅适用于基于同意进行处理的情况。如果我们根据您的同意处理您的个人数据，则您有权随时撤消同意，而无需给出理由。撤消您的同意仅对将来处理有效，并不影响撤消之前所处理数据的合法性。

反对权。反对处理的权利适用于基于 ESET 或第三方合法权益的处理。如果我们处理您的个人数据是为了保护合法权益，则您作为数据主体有权随时反对我们所谓的合法权益和对您个人数据的处理。您的反对仅对将来处理有效，并不影响反对之前所处理数据的合法性。如果我们出于直接营销目的处理您的个人数据，则无需给出您的反对理由。这也适用于资料收集，因为它与此类直接营销有关。在所有其他情况下，我们要求您简要告知我们针对 ESET 处理您个人数据的合法权益提出的投诉。

请注意，在某些情况下，尽管您撤消了同意，但我们有权根据其他法律依据进一步处理您的个人数据（例如，为了履行合同）。

访问权。您作为数据主体，有权随时免费获取有关 ESET 存储您数据的信息。

纠正权。如果我们无意中处理了有关您的错误个人数据，您有权更正该数据。

删除权和限制处理权。您作为数据主体，有权要求删除或限制处理您的个人数据。如果我们处理您的个人数据（例如，在您同意的情况下），而您撤消同意并且没有其他法律依据（例如，合同），则我们会立即删除您的个人数据。在我们的保留期结束时，如果不再需要您的个人数据用于为其规定的目的，您的个人数据也会被删除。

如果我们将您的个人数据用于直接营销的唯一目的，而您已撤消同意或反对 ESET 的潜在合法权益，则我们将限制对您个人数据的处理，以便将您的联系方式数据包括在我们的内部黑名单中，从而避免主动联系。否则，将删除您的个人数据。

请注意，我们可能需要存储您的数据，直到立法者或监管机构发布的保留义务和期限到期。保留义务和期限也可能源于斯洛伐克法律。其后，将例行删除相应的数据。

数据迁移。我们很乐意为您（作为数据主体）提供 ESET 采用 xls 格式处理的个人数据。

提出投诉的权利。您作为数据主体，有权随时向监管机构提出投诉。ESET 遵守斯洛伐克法律的规定，并且我们受欧盟的数据保护法的约束。相关数据监管机构是斯洛伐克共和国个人数据保护办公室，具体地址为 Hraničná 12, 82007 Bratislava 27, Slovak Republic。

个人数据的处理

由 ESET 提供并在我们的产品中实现的服务都是依据 最终用户许可协议提供的，但其中一些服务可能需要特别关注。我们希望为您提供与服务提供有关的数据收集的更多详细信息。我们提供最终用户许可协议和产品 文档处理从您或您的产品收集的数据，其中一些数据可能包含个人数据。为了正常运行，我们需要收集以下信息：

许可和计费数据。ESET 会收集和处理姓名、电子邮件地址、许可证密钥以及（如果适用）地址、公司隶属关系和付款数据，以方便许可证激活、许可证密钥交付、到期提醒、支持请求、许可证真实性验证、提供我们的服务和其他通知（包括依据适用法律或在您同意的情况下发送营销邮件。ESET 有法律义务将计费信息保留 10 年，但许可信息将在许可证到期后的 12 个月之内进行匿名化处理。

更新和其他统计信息。处理的信息包括有关安装过程和您计算机的信息（包括安装我们产品的平台）以及有关我们产品的操作和功能的信息，例如操作系统、硬件信息、安装 ID、许可证 ID、IP 地址、MAC 地址、所处理产品的配置设置（出于提供更新和升级服务以及维护、安全性和我们的后端基础架构改进的目的）。

此信息与许可和计费目的所需的识别信息分开存储，因为它不需要用于识别最终用户。保留期最长可达 4

年。

ESET LiveGrid® 信誉系统。与渗透有关的单向哈希是为了 ESET LiveGrid® 信誉系统而处理的，通过将已扫描的文件与云中列入白名单和黑名单的项目数据库进行比较，从而提高我们反恶意软件解决方案的效率。在此过程中不会识别最终用户。

ESET LiveGrid® 反馈系统。作为 ESET LiveGrid® 反馈系统的一部分、野生的可疑样本和元数据使 ESET 能够立即应对我们的最终用户的需求，以及使我们持续响应最新的威胁（如果有的话）。我们依赖您向我们发送

- 渗透，如病毒和其他恶意程序以及可疑程序的潜在样本；有问题、潜在不受欢迎或潜在不安全的对象，如可执行文件、由您报告为垃圾邮件的电子邮件或我们的产品标记的电子邮件；
- 涉及 Internet 使用的信息，例如 IP 地址和地理信息、IP 数据包、URL 和以太网帧；
- 崩溃转储文件及包含的信息。

我们不希望收集超出此范围的数据，但有时不可避免。意外收集的数据可能包含在恶意软件本身中（在您不知情或未批准的情况下收集）或者作为文件名或 URL 的一部分包含在内，我们不打算将其构成我们系统的一部分，或为了本隐私政策中声明的目的而对其进行处理。

通过 ESET LiveGrid® 反馈系统获取和处理的所有信息都应在不识别最终用户身份的情况下使用。

连网设备安全评估。为了提供安全评估功能，我们会处理本地网络名称和您本地网络中设备的相关信息，例如本地网络中设备的状态、类型、名称、IP 地址和 MAC 地址以及许可证信息。该信息还包括路由器设备的无线安全类型和无线加密类型。识别最终用户的许可信息将在许可证到期后的 12 个月之内进行匿名化处理。

技术支持。支持服务可能需要在您的支持请求中包含联系方式和许可信息及数据。根据您选择与我们联系的渠道，我们可能会收集您的电子邮件地址、电话号码、许可证信息、产品详细信息和支持案例的描述。为了便于提供支持服务，可能会要求您提供给我们其他信息。为技术支持而处理的数据存储 4 年。

防止数据滥用。如果最终用户在 https://home.eset.com 上创建 ESET HOME 帐户，并激活与计算机被盗有关的功能，将收集和处理以下信息：位置数据、屏幕截图、计算机的配置数据以及计算机的摄像头记录的数据。收集的数据存储在我们的服务器或我们服务提供商的服务器上，保留期为 3 个月。

Password Manager如果您选择激活 Password Manager 的功能，则与登录详细信息相关的数据将仅以加密形式存储在您的计算机或其他指定设备上。如果激活同步服务，则加密数据会存储在我们的服务器或服务提供商的服务器上，以保护此类服务。ESET 和服务提供商都无权访问该加密数据。只有您拥有解密数据的密钥。停用该功能后，将删除数据。

ESET LiveGuard. 如果您选择激活 ESET LiveGuard 功能，则需要提交样本（例如，最终用户预定义和选择的文件）。为远程分析所选择的样本将上传给 ESET 服务，并且分析结果会发送回您的计算机。任何可疑样本都会根据 ESET LiveGrid® 反馈系统收集的信息进行处理。

客户体验改进计划。如果选择激活 客户体验改进计划 ，则在您同意的情况下，将收集和使用与使用我们产品相关的匿名遥测信息。

请注意，如果使用我们产品和服务的用户不是已购买产品或服务并与我们签订最终用户许可协议的最终用户（例如，最终用户的雇员、家庭成员或最终用户依据最终用户许可协议向其授权使用产品或服务的用户），则 ESET 依据 GDPR 第 6 (1) (f) 款规定的合法权益执行数据处理，以使最终用户授权的用户能够使用我们依据最终用户许可协议提供的产品和服务。

联系人信息

如果您希望行使作为数据主体的权利或有疑问，请发送邮件至：

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk