ESET Endpoint Antivirus for macOS

用户指南

单击此处显示此文档的联机版本

Digital Security
Progress. Protected.

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

有关更多信息，请访问 www.eset.com

客户服务www.eset.com/support

修订日期 2021年m月5日

ESET Endpoint Antivirus for macOS

ESET Endpoint Antivirus for macOS 6 代表了真正集成计算机安全的新方法。最新版本的 ThreatSense® 扫描引擎 可利用速度和精确度来使您的计算机保持安全。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 Endpoint Antivirus for macOS 6 是我们结合最高防护与最少系统占用的长期努力而开发出的完整安全解决方案。基于人工智能的高级技术能够主动消除病毒、间谍软件、木马、蠕虫、广告软件Rootkit 和其他基于 Internet 攻击的渗透，而不会妨碍系统性能或中断您的计算机。

本产品主要设计用于小型商业/企业环境中的工作站。它可以与 ESET PROTECT以前称为 ESET Security Management Center结合使用，从而让您可以轻松管理任意数量的客户端工作站、应用策略与规则、监视检测以及从任何联网计算机远程管理更改。

版本 6 中的新功能

ESET Endpoint Antivirus for macOS 的图形用户界面已完全重新设计，以提供更好的可见性和更直观的用户体验。版本 6 所包含的许多改进的其中几处如下所示：

- ESET Enterprise Inspector - 从 ESET Endpoint Antivirus for macOS 版本 6.9 开始ESET Endpoint Antivirus for macOS 可以与 ESET Enterprise Inspector 连接ESET Enterprise Inspector (EEI) 是一个全面的端点检测和响应系统，包括的功能如：事件检测、事件管理和响应、数据收集、攻击检测指示、异常检测、行为检测、策略违反。有关 ESET Enterprise Inspector 及其安装和功能的详细信息，请参阅 ESET Enterprise Inspector 帮助
- **64 位结构支持**
- **Web 访问保护** – 监控 Web 浏览器与远程服务器之间的通信
- **电子邮件防护** – 提供对通过 POP3 和 IMAP 协议接收的电子邮件通信的控制
- **网络钓鱼防护** – 通过限制访问冒充合法网站的恶意网站，可防范尝试获取密码和其他敏感信息的行为
- **设备控制** – 允许您扫描、阻止或调整扩展的过滤器和/或权限，并定义用户是否能够访问和使用外部设备。此功能在产品版本 6.1 和更高版本中可用。
- **演示模式** – 此选项允许您在后台运行 ESET Endpoint Antivirus for macOS 并禁止弹出窗口和计划任务
- **共享的本地缓存** – 可提高虚拟化环境中的扫描速度

系统要求

要使 ESET Endpoint Antivirus for macOS 实现最佳性能，系统应满足以下硬件和软件要求：

	系统要求：
处理器结构	Intel 64-bit

操作系统	macOS 10.12 及更高版本 macOS Server 10.12 及更高版本
内存	300 MB
可用磁盘空间	200 MB

除了支持现有 Intel 之外，ESET Endpoint Antivirus for macOS 版本 6.10.900.0 及更高版本还支持使用 Rosetta 2 的 Apple M1 芯片

介绍 ESET PROTECT

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

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

ESET PROTECT 由以下组件组成：

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

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

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

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

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

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

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

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

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

- ESET PROTECT 虚拟服务器代理主机 - ESET PROTECT 的组件，可虚拟化服务器代理实体，以允许管理无服务器代理的虚拟机。该解决方案支持自动化、动态组使用和与物理计算机上的 ESET Management 服务

器代理相同级别的任务管理。虚拟服务器代理可收集虚拟机的信息，并将它发送到 ESET PROTECT 服务器。

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

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

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

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

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

有关详细信息，请参阅 ESET PROTECT 联机用户指南

介绍 ESET PROTECT CLOUD

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

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

远程安装

安装前

- macOS 10.15 及更早版本

在 macOS 10.13 及更高版本上安装 ESET Endpoint Antivirus for macOS 之前，建议您允许 ESET 内核扩展，在 macOS 10.14 及更高版本上还要允许目标计算机上的完全磁盘访问。如果这些选项在安装之后允许，用户将收到**系统扩展遭到阻止**和**您的计算机受到部分保护**，直到允许 ESET 内核扩展和完全磁盘访问。要远程允许 ESET 内核扩展和全盘访问，您的计算机必须在 MDM（移动设备管理）服务器（例如 Jamf）中进行注册。

启用 ESET 系统扩展

要远程启用您设备上的内核扩展，请下载 .plist 配置文件。使用所选择的 UUID 生成器生成两个 UUID，然后使用文本编辑器将字符串替换已下载配置文件中的相应文本，即 `insert your UUID 1 here` 和 `insert your UUID 2 here`。使用 MDM 服务器部署 `.plist` 配置文件。您的计算机必须在 MDM 服务器中注册，才能将配置文件部署到目标计算机。

启用全盘访问

在 macOS 10.14 上，您将在安装后收到来自 ESET Endpoint Antivirus for macOS 的**您的计算机受到部分保护**通知。要访问所有 ESET Endpoint Antivirus for macOS 功能并阻止通知显示，您需要在安装产品之前允许对 ESET Endpoint Antivirus for macOS 的**完全磁盘访问**。要远程允许**完全磁盘访问**，请执行以下操作：

- 下载 .plist 配置文件。 使用您选择的 UUID 生成器生成两个 UUID，然后使用文本编辑器以字符串替代已下载配置文件中的文本 `insert your UUID 1 here` 和 `insert your UUID 2 here`。使用 MDM 服务器部署 .plist 配置文件。您的计算机需要在 MDM 服务器中注册，才能将配置文件部署到目标计算机。

- macOS Big Sur (11)

在 macOS Big Sur 上安装 ESET Endpoint Antivirus for macOS 之前，必须在目标计算机上启用以下设置：
oESET 系统扩展
如果在安装之前未启用 ESET 系统扩展，用户会收到**系统扩展已阻止**通知，直到启用 ESET 系统扩展。
o全盘访问
如果在安装之前未启用全盘访问，用户会收到**您的计算机受到部分保护**通知，直到启用全盘访问。
oWeb 访问保护
要使 Web 访问保护正常工作，必须将 Web 访问保护配置添加到系统设置。
如果 Web 访问保护配置在安装 ESET Endpoint Antivirus for macOS 之后丢失，用户会收到**"ESET Endpoint Antivirus for macOS" 想要过滤网络内容**。当他们收到此通知时，单击**允许**。如果他们单击**不允许**Web 访问保护将不会起作用。
要远程启用上述 ESET 设置，您的计算机必须在 MDM移动设备管理）服务器（例如 Jamf中进行注册。

启用 ESET 系统扩展

要在设备上远程启用系统扩展，请在安装之前执行以下操作之一：
o下载 .plist 配置文件。使用 MDM 服务部署 .plist 配置文件。
o使用以下设置在 MDM 中创建自己的配置文件：

团队标识符（TeamID）	P8DQRXPVLP
捆绑标识符（BundleID）	com.eset.endpoint com.eset.network com.eset.firewall com.eset.devices

启用全盘访问

要在远程启用全盘访问，请在安装之前执行以下操作之一：
o下载 .plist 配置文件。 使用 MDM 服务部署 .plist 配置文件。
o使用以下设置创建自己的配置文件：

ESET Endpoint Antivirus	
标识符	com.eset.eea.6
标识符类型	bundleID
代码要求	identifier "com.eset.eea.6" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
应用或服务	SystemPolicyAllFiles
访问	Allow
ESET Endpoint Antivirus 和 ESET Endpoint Security	
标识符	com.eset.devices
标识符类型	bundleID
代码要求	identifier "com.eset.devices" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
应用或服务	SystemPolicyAllFiles
访问	Allow
ESET Endpoint Antivirus 和 ESET Endpoint Security	
标识符	com.eset.endpoint
标识符类型	bundleID
代码要求	identifier "com.eset.endpoint" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
应用或服务	SystemPolicyAllFiles
访问	Allow

Web 访问保护

要远程将 Web 访问保护配置添加到系统设置，请在安装之前执行以下操作之一：
o下载 .plist 配置文件。使用 MDM 服务器部署 .plist 配置文件。您的计算机必须在 MDM 服务器中进行注册，才能将配置文件部署到目标计算机。
o要创建自己的配置文件，请使用以下设置创建 VPN 类型配置文件：

VPN 类型	VPN
连接类型	Custom SSL
自定义 SSL VPN 的标识符	com.eset.sysext.manager
服务器	localhost
提供商捆绑标识符	com.eset.network
用户身份验证	证书
提供商类型	App-proxy
提供商指定要求	identifier "com.eset.network" and anchor apple generic and certificate 1[field.1.2.840.113635.100.6.2.6] /* exists */ and certificate leaf[field.1.2.840.113635.100.6.1.13] /* exists */ and certificate leaf[subject.OU] = P8DQRXPVLP
启用 VPN On Demand	
手动规则配置 XML	<array> <dict> <key>Action</key> <string>Connect</string> </dict> </array>
空闲计时器	请勿断开连接
代理设置	手动

代理服务器和端口	localhost : 57856

在远程允许全盘访问和系统扩展后，在**系统首选项 > 安全和隐私**中，这些设置可能显示为处于禁用状态。如果 ESET Endpoint Antivirus for macOS 不显示任何警告，则全盘访问和系统扩展处于允许状态，而无论其在**系统首选项 > 安全和隐私**中的状态为何。

安装

在安装之前，可以创建包含 ESET Endpoint Antivirus for macOS 预设配置的远程安装包，稍后可以使用所选的 ESET PROTECT 或 MDM 进行部署。

创建远程安装包。通过使用 ESET 管理系统创建软件安装任务，来远程安装 ESET Endpoint Antivirus for macOS

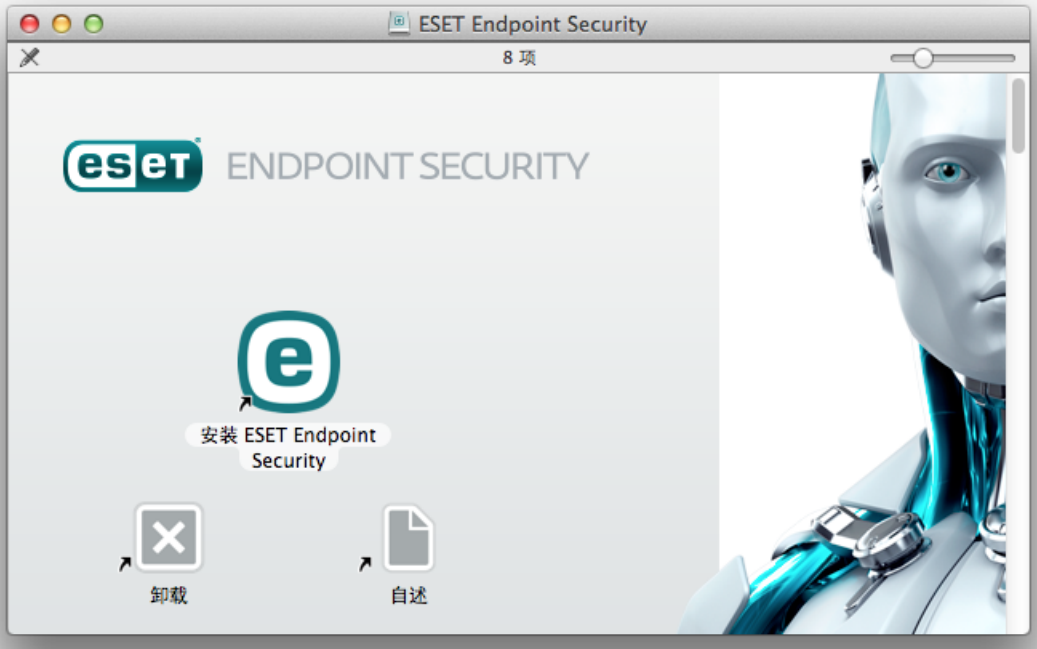
- 软件安装任务 ESET PROTECT
- 软件安装任务 ESET Security Management Center

创建远程安装包

为 Apple Remote Desktop 安装创建安装包

1. 从 ESET 网站下载标准安装包：
ESET Endpoint Antivirus for macOS

2. 要启动 ESET Endpoint Antivirus for macOS 安装程序，请双击下载的文件。



1. 单击**安装**ESET Endpoint Antivirus for macOS

2. 出现提示时，单击**允许**以授权安装程序确定是否可以安装该软件。

3. 单击**继续**。如果要创建远程安装包，将不会安装 ESET Endpoint Antivirus for macOS。

4. 查看系统要求，然后单击**继续**。

5. 阅读 ESET 软件许可协议，然后依次单击**继续** → **同意**（如果同意）。

6. 在**安装模式**步骤中，选择**远程**。

7. 选择要安装的产品组件。默认情况下，所有组件都处于选中状态。单击**继续**。

8. 在**代理服务器**步骤中，选择与 Internet 连接匹配的选项。如果不确定，则使用默认系统设置。单击**下一步**。如果使用的是代理服务器，则在下一步中，系统会提示您输入代理服务器地址、用户名和密码。

9. 选择谁可以修改程序配置。只有特权用户和组才能更改它。默认情况下，将“管理员”组选择为特权组。选中**显示所有用户**或**显示所有组**复选框，即可显示所有虚拟用户和组（例如程序和进程）。

10. 在目标计算机上启用 ESET LiveGrid（如果适用）。

11. 在目标计算机上启用潜在的不受欢迎应用程序检测（如果适用）。

12. 选择防火墙模式：
自动模式 – 默认模式。此模式适用于喜欢轻松方便地使用防火墙而无需定义规则的用户。自动模式允许给定系统的标准出站通信，并阻止来自网络端的所有非主动发起的连接。您也可以添加自定义、用户定义的规则。

交互模式 – 允许您构建用于防火墙的自定义配置。当检测到通信且没有任何现有规则适用于该通信时，将显示报告未知连接的对话窗口。对话窗口中还提供允许或拒绝该通信的选项，并且可以将允许或拒绝的决定记忆为防火墙的新规则。如果您选择创建新规则，今后所有此类连接都将根据该规则被允许或阻止。

13. 将安装文件保存在计算机上。如果以前在默认位置创建过安装文件，则必须先更改目标文件夹位置或删除以前的文件，然后才能继续操作。这样就完成了远程安装的第一阶段。本地安装程序将退出，并在所选的目标文件夹中创建远程安装文件。

远程安装文件如下所示：

- *esets_setup.dat* – 在“安装程序的设置”部分中输入的设置数据
- *program_components.dat* – 所选程序组件的设置信息。（该文件是可选的。不选择安装某些 ESET Endpoint Antivirus for macOS 组件时，将不会创建该文件。）
- *esets_remote_install.pkg* – 远程安装包
- *esets_remote_uninstall.sh* – 远程卸载脚本

安装 Apple Remote Desktop

1. 打开 Apple Remote Desktop，然后连接到目标计算机。有关详细信息，请访问 Apple Remote Desktop 文档。

2. 在 Apple Remote Desktop 中，使用**复制文件或文件夹**将以下文件复制到目标计算机上的 */tmp* 文件夹：

如果要安装所有组件，请复制以下内容：
- *esets_setup.dat*

如果并不安装所有产品组件，请复制以下内容：

- *esets_setup.dat*
- *product_components.dat*

3. 使用**安装程序包**命令将 *esets_remote_install.pkg* 安装到目标计算机上。

远程卸载 Apple Remote Desktop

1. 打开 Apple Remote Desktop然后连接到目标计算机。有关详细信息，请访问 Apple Remote Desktop 文档

2. 在 Apple Remote Desktop 中，使用**复制文件或文件夹**将 *esets_remote_uninstall.sh* 脚本复制到目标计算机上的 */tmp* 文件夹。

3. 在 Apple Remote Desktop 中，使用以下**发送 UNIX shell 命令**到目标计算机：

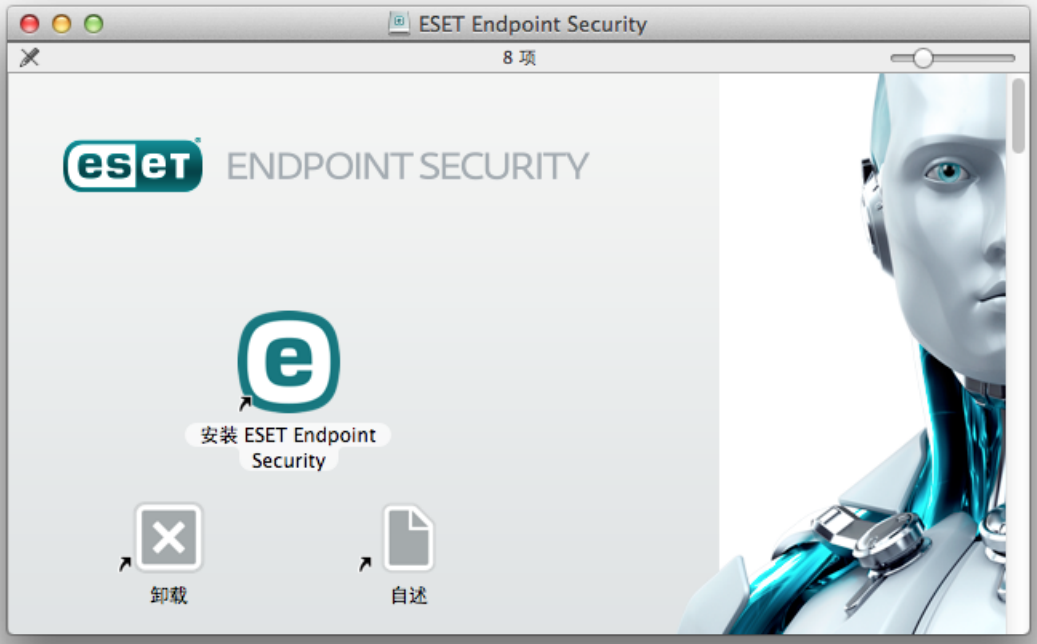
```
/tmp/esets_remote_uninstall.sh
```

卸载过程完成后，控制台将显示在目标计算机上的 Apple Remote Desktop 中。

安装

安装向导将引导您完成基本设置。有关详细指南，请访问我们的安装知识库文章.

1. 要启动 ESET Endpoint Antivirus for macOS 安装程序，请双击下载的文件。



1. 要开始安装，请单击**安装** ESET Endpoint Antivirus for macOS

从 .pkg 文件安装

在安装和启动适用于 macOS 的 ESET 产品时，Mac 计算机上需要能够访问 Internet，才能允许 Apple 验证 ESET 系统扩展公证。

2. 出现提示时，单击**允许**以授权安装程序确定是否可以安装该软件。

3. 如果尚未从计算机中删除诸如病毒防护、间谍软件防护或防火墙之类的任何现有安全应用程序，请进行删除。如果未安装其他安全应用程序，则单击**继续**。

4. 查看系统要求，然后单击**继续**。

5. 阅读 ESET 软件许可协议，然后依次单击**继续** → **同意**（如果同意）。

6. 选择合适的安装类型。

- 典型安装
- 自定义安装
- 远程安装

版本升级

在安装的初始阶段，安装程序将自动在线检查是否有最新的产品版本。如果找到较新的版本，您可以选择下载最新版本，然后再继续安装过程。

典型安装

典型安装模式包括适合于大多数用户的配置选项。这些设置可提供最高安全性和最出色的系统性能。典型安装是默认选项，建议对特定设置没有特别要求的用户使用此选项。

1. 在 **ESET LiveGrid** 窗口中，请选择您的首选选项，然后单击**继续**。如果稍后决定要更改此设置，将能够使用 **LiveGrid 设置**来执行此操作。有关 ESET LiveGrid 的详细信息，请访问我们的词汇表。
2.在**潜在不受欢迎的应用程序**窗口中，选择您的首选选项（请参阅什么是潜在不受欢迎的应用程序？），然后单击**继续**。如果稍后决定要更改此设置，请使用**高级设置**。

3. 单击**安装**。如果系统提示您输入 macOS 密码，请输入该密码，然后单击**安装软件**。

在安装 ESET Endpoint Antivirus for macOS 后：

macOS Big Sur (11)

1. 允许系统扩展。

2. 允许完全磁盘访问。

3. 允许 ESET 添加代理配置。您将收到以下通知：“ESET Endpoint Antivirus for macOS”**想要过滤网络内容**。当收到此通知时，请单击**允许**。如果单击**不允许**，则“Web 访问保护”将不起作用。

macOS 10.15 及更早版本

1. 在 macOS 10.13 及更高版本上，您将收到来自系统的**系统扩展遭到阻止**通知以及来自 ESET Endpoint Antivirus for macOS 的**您的计算机未受到保护**通知。若要访问所有 ESET Endpoint Antivirus for macOS 功能，需要在您设备上允许内核扩展。若要允许您设备上的内核扩展，请导航到**系统首选项 > 安全和隐私**，然后单击**允许**以允许开发者 **ESET, spol. s.r.o.** 开发的系统软件。有关更多详细信息，请访问我们的知识库文章
2. 在 macOS 10.14 及更高版本上，您将收到来自 ESET Endpoint Antivirus for macOS 的**您的计算机受到部分保护**通知。若要访问所有 ESET Endpoint Antivirus for macOS 功能，您需要允许对 ESET Endpoint Antivirus for macOS 的**完全磁盘访问**。依次单击**打开系统首选项 > 安全和隐私**。转到**隐私**选项卡，然后选择**完全磁盘访问**选项。单击锁定图标以启用编辑。单击加号图标，然后选择 ESET Endpoint Antivirus for macOS 应用程序。您的计算机将显示一条重新启动计算机的通知。单击**稍后**。请勿立即重新启动您的计算机。在 ESET Endpoint Antivirus for macOS 通知窗口中单击**再次启动**或重新启动计算机。有关更多详细信息，请访问我们的知识库文章

在安装 ESET Endpoint Antivirus for macOS 后，您应执行计算机扫描以查看是否有恶意代码。在主程序窗口中，依次单击**计算机扫描 > 智能扫描**。有关手动计算机扫描的详细信息，请参阅手动计算机扫描部分。

自定义安装

自定义安装模式是为想要在安装过程中修改高级设置的有经验的用户设计的。

- **程序组件**

  ESET Endpoint Antivirus for macOS 允许您在不安装其某些核心组件（例如 Web 和电子邮件防护）的情况下安装产品。 取消选中产品组件旁边的复选框以从安装中删除它。

- **代理服务器**

  如果使用的是代理服务器，则选择**我使用代理服务器**来定义其参数。在下一个窗口中，请在**地址**字段中输入代理服务器的 IP 地址或 URL在**端口**字段中，指定代理服务器接受连接的端口（3128 为默认值）。如果代理服务器要求验证，则输入有效的**用户名**和**密码**，以便授权访问代理服务器。如果不使用代理服务器，则选择**我不使用代理服务器**。如果不确定是否使用代理服务器，可以通过选择**使用系统设置（建议）**来使用当前的系统设置。

- **权限**

  可以定义授权用户或组，它们能够编辑程序设置。在左侧的用户列表中，选择用户并将其**添加**到**授权用户**列表。要显示所有系统用户，请选择**显示所有用户**。如果您将授权用户列表保留为空，则所有用户均会被视为授权用户。

- **ESET LiveGrid®**

  有关 ESET LiveGrid 的详细信息，请访问我们的词汇表

- **潜在不受欢迎的应用程序**

  有关潜在不受欢迎的应用程序的详细信息，请访问我们的词汇表

在安装 ESET Endpoint Antivirus for macOS 后：

macOS Big Sur (11)

1. 允许系统扩展
2. 允许完全磁盘访问
3. 允许 ESET 添加代理配置。您将收到以下通知：“ESET Endpoint Antivirus for macOS”想要过滤网络内容。

当收到此通知时，请单击**允许**。如果单击**不允许**，则“Web 访问保护”将不起作用。

macOS 10.15 及更早版本

1. 在 macOS 10.13 及更高版本及更高版本上，您将收到来自系统的**系统扩展遭到阻止**通知以及来自 ESET Endpoint Antivirus for macOS 的**您的计算机未受到保护**通知。若要访问所有 ESET Endpoint Antivirus for macOS 功能，需要在您设备上允许内核扩展。若要允许您设备上的内核扩展，请导航到**系统首选项 > 安全和隐私**，然后单击**允许**以允许开发者 **ESET, spol. s.r.o.** 开发的系统软件。有关更多详细信息，请访问我们的知识库文章
2. 在 macOS 10.14 及更高版本上，您将收到来自 ESET Endpoint Antivirus for macOS 的**您的计算机受到部分保护**通知。若要访问所有 ESET Endpoint Antivirus for macOS 功能，您需要允许对 ESET Endpoint Antivirus for macOS 的**完全磁盘访问**。依次单击**打开系统首选项 > 安全和隐私**。转到**隐私**选项卡，然后选择**完全磁盘访问**选项。单击锁定图标以启用编辑。单击加号图标，然后选择 ESET Endpoint Antivirus for macOS 应用程序。您的计算机将显示一条重新启动计算机的通知。单击**稍后**。请勿立即重新启动您的计算机。在 ESET Endpoint Antivirus for macOS 通知窗口中单击**再次启动**或重新启动计算机。有关更多详细信息，请访问我们的知识库文章

在安装 ESET Endpoint Antivirus for macOS 后，您应执行计算机扫描以查看是否有恶意代码。在主程序窗口中，依次单击**计算机扫描 > 智能扫描**。有关手动计算机扫描的详细信息，请参阅手动计算机扫描部分。

本地允许系统扩展

在 macOS 11 (Big Sur) 中，内核扩展已替换为系统扩展。需要用户事先批准，才能加载新的第三方系统扩展。

在安装 macOS Big Sur (11) 及更高版本的 ESET Endpoint Antivirus for macOS 后，您将收到来自系统的“系统扩展遭到阻止”通知，以及来自 ESET Endpoint Antivirus for macOS 的“您的计算机不受保护”通知。要访问 ESET Endpoint Antivirus for macOS 的所有功能，必须允许设备上的系统扩展。

从以前的 macOS 升级到 Big Sur
如果已安装 ESET Endpoint Antivirus for macOS 并且将升级到 macOS Big Sur则需要在升级后手动允许 ESET 内核扩展。需要物理访问客户端计算机 – 如果远程访问，“允许”按钮处于禁用状态。

在 macOS Big Sur 或更高版本上安装 ESET 产品时，必须手动允许 ESET 系统扩展。需要物理访问客户端计算机 – 远程访问时，该选项处于禁用状态。

手动允许系统扩展

1. 在其中一个警报对话框中，单击**打开系统首选项**或**打开安全首选项**
2. 单击左下角的锁定图标，以允许在该设置窗口中进行更改。
3. 使用 Touch ID 或单击**使用密码**并键入用户名和密码，然后单击**解锁**
4. 单击**详细信息**
5. 选择全部三个 ESET Endpoint Antivirus for macOS**.app** 选项。
6. 单击**确定**

有关详细的分步指南，请访问我们的知识库文章。（知识库文章并非以所有语言提供。）

本地允许全盘访问

在 macOS 10.14 上，您将收到来自 ESET Endpoint Antivirus for macOS 的**您的计算机受到部分保护**通知。要访问 ESET Endpoint Antivirus for macOS 的所有功能，必须允许**全盘访问** ESET Endpoint Antivirus for macOS。

1. 在警报对话框窗口中，单击**打开系统首选项**。
2. 单击左下角的锁定图标，以允许在该设置窗口中进行更改。
3. 使用 Touch ID 或单击**使用密码**并键入用户名和密码，然后单击**解锁**。
4. 从列表中选择 ESET Endpoint Antivirus for macOS**.app**。
5. 将显示“重新启动 ESET Endpoint Antivirus for macOS”通知。单击“稍后”。
6. 从列表中选择 ESET **文件系统实时防护**。

> **ESET 文件系统实时防护不存在**
> 如果列表中不存在**文件系统实时防护**选项，则需要允许 ESET 产品的系统扩展。

7. 在 ESET Endpoint Antivirus for macOS 警报对话框窗口中再次单击“启动”，或者重新启动计算机。有关更多详细信息，请访问我们的知识库文章。

产品激活

完成安装后，将提示您激活您的产品。 有多个可使用的激活方法。 特定激活方法的可用性可能有所不同，具体取决于国家/地区以及产品的分发方式（CD/DVD、ESET 网页等）。

若要从程序直接激活您的 ESET Endpoint Antivirus for macOS 副本，请单击位于 macOS 菜单栏（屏幕顶部）中的 ESET Endpoint Antivirus for macOS 图标  ，然后单击**产品激活**。 您还可以从主菜单中的**帮助** > **管理许可证**或**防护状态** > **激活产品**下激活您的产品。

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

- **使用许可证密钥激活** – 采用 XXXX-XXXX-XXXX-XXXX-XXXX 格式的唯一字符串，用于标识许可证所有者和激活许可证。 在购买完成后收到的邮件中或在盒装产品中随附的许可证卡片上，您可以找到您的许可证密钥。
- **安全管理员** – 使用凭证（电子邮件地址 + 密码）在 ESET License Administrator 门户上创建的帐户。此方法允许您在一个位置管理多个许可证。
- **脱机许可证** – 将传输到 ESET 产品以提供许可证信息的自动生成的文件。 您的脱机许可证文件从 ESET License Administrator 门户生成，并在应用程序无法连接到许可证颁发机构的环境中使用。

如果您的计算机是托管网络的成员，并且管理员计划使用 ESET Remote Administrator 激活您的产品，还可以在以后激活此客户端。

> **静默激活**
> ESET Remote Administrator 能够使用管理员提供的许可证静默激活客户端计算机。

ESET Endpoint Antivirus for macOS 版本 6.3.85.0（或更高版本）可向您提供使用终端激活产品的选项。 若要执行此操作，请发出以下命令：

```
sudo ./esets_daemon --wait-respond --activate key=XXXX-XXXX-XXXX-XXXX-XXXX
```

将 XXXX-XXXX-XXXX-XXXX-XXXX 替换为已用于激活 ESET Endpoint Antivirus for macOS 或在 ESET License Administrator 中注册的许可证密钥。 该命令将返回“正常”状态或一个错误（如果激活失败）。

卸载

有多种启动 ESET Endpoint Antivirus for macOS 卸载程序的方法：

- 打开 ESET Endpoint Antivirus for macOS 安装文件（*.dmg*），然后双击**卸载**

- 启动 **Finder**、打开硬盘驱动器上的**应用程序**文件夹、按住 CTRL 键并单击 **ESET Endpoint Antivirus for macOS** 图标，然后选择**显示程序包内容**。打开 **Contents > Helpers** 文件夹，然后双击 **Uninstaller** 图标。

卸载
在卸载过程中，需要多次插入管理员密码，才能完全卸载 ESET Endpoint Antivirus for macOS

基本概述

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

可从主菜单访问以下部分：

- **防护状态** – 提供有关您的计算机Web 和邮件防护的防护状态信息。
- **计算机扫描** – 此部分允许您配置和启动手动计算机扫描
- **更新** – 显示有关模块更新的信息。
- **设置** – 选择此部分可以对您的计算机的安全级别进行调整。
- **工具** – 提供对日志文件计划任务隔离区正在运行的进程和其他程序功能的访问。
- **帮助** – 显示对帮助文件Internet 知识库、支持请求表单和附加程序信息的访问。

键盘快捷键

使用 ESET Endpoint Antivirus for macOS 时可用的键盘快捷键包括：

- *cmd+,* – 显示 ESET Endpoint Antivirus for macOS 首选项；
- *cmd+O* – 将 ESET Endpoint Antivirus for macOS 主 GUI 窗口调整为默认大小，并将其移动到屏幕的中心；
- *cmd+Q* – 隐藏 ESET Endpoint Antivirus for macOS 主 GUI 窗口。您可以通过单击 macOS 菜单栏（屏幕顶部）中的 ESET Endpoint Antivirus for macOS 图标 打开它。
- *cmd+W* – 关闭 ESET Endpoint Antivirus for macOS 主 GUI 窗口。

下列键盘快捷方式仅在启用了**使用标准菜单设置 > 进入应用程序首选项. . . > 界面**下）时有效：

- *cmd+alt+L* – 打开**日志文件**部分；

- *cmd+alt+S* – 打开**计划任务**部分；
- *cmd+alt+Q* – 打开**隔离区**部分。

检查系统操作

若要查看您的防护状态，请从主菜单单击**防护状态**。有关 ESET Endpoint Antivirus for macOS 模块的操作的状态摘要将显示在主窗口中。

程序工作不正常时如何应对

当模块正常工作时，将显示一个绿色的复选标记图标。当模块不正常工作时，将显示一个红色的感叹号或橙色的通知图标。将在主程序窗口中显示与模块有关的附加信息和用于解决问题的建议的解决方案。若要更改各个模块的状态，请单击各通知消息下方的蓝色链接。

如果使用建议的解决方案无法解决问题，您可以在 ESET 知识库中搜索解决方案或联系 ESET 客户服务。客户服务将快速回复您的问题并帮助您解决任何有关 ESET Endpoint Antivirus for macOS 的问题。

计算机防护

您可以在**设置** > **计算机**下找到计算机配置。它显示**文件系统实时防护**的状态。若要关闭各个模块，请将所需模块切换至**禁用**。注意，这可能会降低对您的计算机的保护级别。若要访问每个模块的详细设置，请单击**设置**。

病毒和间谍软件防护

病毒防护通过修改可能导致潜在威胁的文件防止恶意系统攻击。如果检测到带有恶意代码的威胁，则病毒防护模块可以通过阻止它，然后将其清除、删除或移至隔离区，来消除威胁。

常规

在**常规**部分（**设置 > 进入应用程序首选项. . . > 常规**）中，您可以启用以下类型的应用程序的检测功能：

- **潜在的不受欢迎应用程序** – 这些应用程序未必是恶意的，但可能会对计算机的性能产生不利影响。此类应用程序通常会在安装前提请用户同意。如果计算机上安装了这类程序，系统运行（与这些应用程序安装前的行为方式相比）会有所不同。最显著的变化包括会出现不受欢迎的弹出窗口、启动和运行隐藏进程、系统资源消耗增加、更改搜索结果以及应用程序与远程服务器的通信。

- **潜在的不安全应用程序** – 这些应用程序是指合法的商业软件，如果在未经用户同意的情况下安装了它们，可能会被攻击者滥用。其中包括远程访问工具等程序，因此该选项默认情况下为禁用状态。

- **可疑应用程序** – 这些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。加壳程序是一个运行时自解压的可执行文件，可将多种恶意软件包含在单个包中。最常见的加壳程序包括UPXPE_CompactPKLite 和 ASPack当使用不同的加壳程序进行压缩时，相同的恶意软件的检测方式可能会有所不同。此外，加壳程序还能使其“签名”随着时间发生变异，从而使恶意软件更加难以检测和移除。

若要设置文件系统或 Web 和邮件排除，请单击**设置**

排除

在**排除**部分中，您可以将特定文件/文件夹、应用程序或 IP/IPv6 地址排除在扫描之外。

文件系统选项卡中列出的文件和文件夹将排除在所有扫描程序之外：启动、实时和手动（计算机扫描）。

- **路径** – 被排除文件和文件夹的路径

- **威胁** – 如果已排除文件旁有一个威胁的名称，则表示该文件仅对该威胁排除，并不是全部排除。如果该文件稍后被其他恶意软件感染，病毒防护模块将会检测到该文件。

-  – 创建新排除。输入对象的路径（也可以使用通配符 * 和 ?）或从树结构选择文件夹或文件。

-  – 删除选择的条目

- **默认** – 将排除回滚到上次保存的状态。

在 **Web 和邮件**选项卡中，您可以将特定**应用程序**或 **IP/IPv6 地址**排除在协议扫描之外。

启动防护

启动文件检查会在系统启动时自动扫描文件。默认情况下，此扫描会作为计划任务在用户登录后或在模块成功更新后定期运行。若要修改适用于启动扫描的 ThreatSense 引擎参数设置，请单击**设置**。可以通过阅

读本节了解有关 ThreatSense 引擎设置的详细信息。

文件系统实时防护

文件系统实时防护检查所有类型的介质，并根据各种事件触发扫描。使用 ThreatSense 技术（如 ThreatSense 引擎参数设置中所述），文件系统实时防护对于新创建的文件和现有文件可能有所不同。可以更精确地控制新创建的文件。

默认情况下，所有文件都会在**文件打开**、**文件创建**或**文件执行**时扫描。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。实时防护在系统启动时启动，并提供不间断的扫描。在特殊情况下（例如，如果与其他实时扫描程序发生冲突），可通过单击位于菜单栏（屏幕顶部）中的 ESET Endpoint Antivirus for macOS 图标 ，然后选择**禁用文件系统实时防护**来终止实时防护。也可以从主程序窗口禁用文件系统实时防护（单击**设置 > 计算机**并将**文件系统实时防护**切换到**禁用**）。

以下介质类型可能会从 Real-time 扫描程序中排除：

- **本地驱动器** – 系统硬盘驱动器
- **可移动磁盘** - CD、DVD、USB 磁盘、蓝牙设备等
- **网络媒体** – 所有映射的驱动器

建议您使用默认设置并且仅在特殊情况（例如，当扫描某些媒体使数据传输速度显著降低时）下对扫描排除进行修改。

要修改文件系统实时防护的高级设置，请转至**设置 > 进入应用程序首选项...**（或按 *cmd+,*）> **实时防护**并单击**高级选项**旁边的**设置...**（如高级扫描选项中所述）。

高级选项

在此窗口中，您可以定义哪些对象类型由 ThreatSense 引擎扫描。若要了解有关**自解压文件**、**加壳程序**和**高级启发式扫描**的详细信息，请参阅 ThreatSense 引擎参数设置。

不建议在**默认压缩文件设置**部分中进行更改，除非需要解决特定问题，因为较高的压缩嵌套值可能阻碍系统性能。

用于已执行文件的 ThreatSense 参数 – 默认情况下，在执行文件时将使用**高级启发式扫描**。强烈建议您使智能优化和 ESET LiveGrid® 保持启用状态以减轻对系统性能的影响。

增加网络卷兼容性 – 当通过网络访问文件时，此选项可提高性能。如果您在访问网络驱动器时遇到运行缓慢的情况，应启用该选项。此功能将在 OS X 10.10 及更高版本上使用系统文件协调器。请注意并非所有应用程序都支持文件协调器，例如 Microsoft Word 2011 不支持它，而 Word 2016 则支持它。

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。修改实时防护参数时要小心。建议您仅在特定情况下修改这些参数。例如，与某个应用程序或另一个病毒防护程序的实时扫描程序发生冲突时。

安装 ESET Endpoint Antivirus for macOS 后，所有设置都会得到优化，以便为用户提供最高级别的系统安全性。若要恢复默认设置，请单击**默认**按钮，它位于**实时防护**窗口（**设置 > 进入应用程序首选项... > 实时防护**）的左下角。

检查实时防护

若要验证实时防护是否工作以及是否在检测病毒，请使用测试文件 eicar.com。此测试文件是一个可供所有病毒防护程序检测的特殊无害文件。此文件由 EICAR 协会（欧洲计算机病毒防护研究协会）创建，用于测试病毒防护程序的功能。

若要在不使用 ESET Security Management Center 的情况下检查实时防护的状态，请使用**终端**远程连接到客户端计算机并执行以下命令：

```
/Applications/.esets/Contents/MacOS/esets_daemon --status
```

实时扫描程序的状态将显示为 `RTPStatus=Enabled` 或 `RTPStatus=Disabled`。

终端 BASH 的输出包含以下状态：

- 客户端计算机上安装的 ESET Endpoint Antivirus for macOS 版本
- 检测引擎的日期和版本
- 更新服务器的路径

> **终端用法**
> 仅推荐高级用户使用“终端”实用程序。

实时防护不工作时如何应对

在本章中，我们将介绍使用实时防护时可能出现的问题场景，以及如何解决这些问题。

实时防护被禁用

如果用户无意中禁用了实时防护，则需要重新启用它。要重新启用实时防护，请在主菜单中单击**设置 > 计算机**并将**文件系统实时防护**切换到**已启用**。或者，您可以在**实时防护**下的“应用程序首选项”窗口中，选择**启用文件系统实时防护**，来启用文件系统实时防护。

实时防护功能不检测和清除威胁

请确保您的计算机上没有安装其他病毒防护程序。如果同时启用两种实时防护，它们可能互相冲突。建议您卸载系统上可能存在的任何其他病毒防护程序。

实时防护不启动

如果系统启动时实时防护未启动，可能是因为与其他程序发生冲突。如果遇到此问题，请联系 ESET 客户服务。

手动计算机扫描

如果您怀疑计算机受到感染（行为不正常），请运行**智能扫描**，以检查计算机中是否存在渗透。为了得到最大防护，计算机扫描应作为日常安全手段的一部分定期运行，而不应仅在怀疑有威胁时运行。定期扫描能够检测到渗透，这些渗透在保存到磁盘时未被实时扫描程序发现。如果计算机被感染时实时扫描程序已被禁用，或者模块过期，就会出现这种情况。

我们建议您每月至少运行一次手动计算机扫描。在**工具 > 计划任务**中，可以将扫描配置为计划任务。

您也可以将所选文件和文件夹从桌面或 **Finder** 窗口拖放到 ESET Endpoint Antivirus for macOS 主屏幕、平台图标、菜单栏图标 ⓔ（屏幕顶部）或应用程序图标（位于 */Applications* 文件夹中）。

扫描类型

可使用两种类型的手动计算机扫描。**智能扫描**快速扫描系统，无需进一步配置扫描参数。**自定义扫描**允许您选择任意预定义的扫描配置文件以及选择特定扫描目标。

智能扫描

智能扫描允许您快速启动计算机扫描和清除被感染文件，而无需用户干预。其主要优势在于操作方便，没有复杂的扫描配置。智能扫描检查所有文件夹中的所有文件并自动清除或删除检测到的渗透。清除级别被自动设置为默认值。有关清除类型的更详细信息，请参见清除。

自定义扫描

自定义扫描允许您指定扫描参数，例如扫描目标和扫描方法。 运行自定义扫描的优点在于能够详细配置扫描参数。 不同的配置可以另存为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。

若要选择扫描目标，请依次选择**计算机扫描** > **自定义扫描**，然后从树结构中选择特定的**扫描目标**。 也可以通过输入要包括的文件夹或文件路径，更精确地指定扫描目标。 如果您仅想扫描系统而不进行附加的清除操作，则选择**扫描但不清除**。 此外，还可以通过依次单击**设置...** > **清除**，从三种清除级别中进行选择。

> **自定义扫描**
> 仅建议具有病毒防护程序使用经验的高级用户使用自定义扫描来执行计算机扫描。

扫描目标

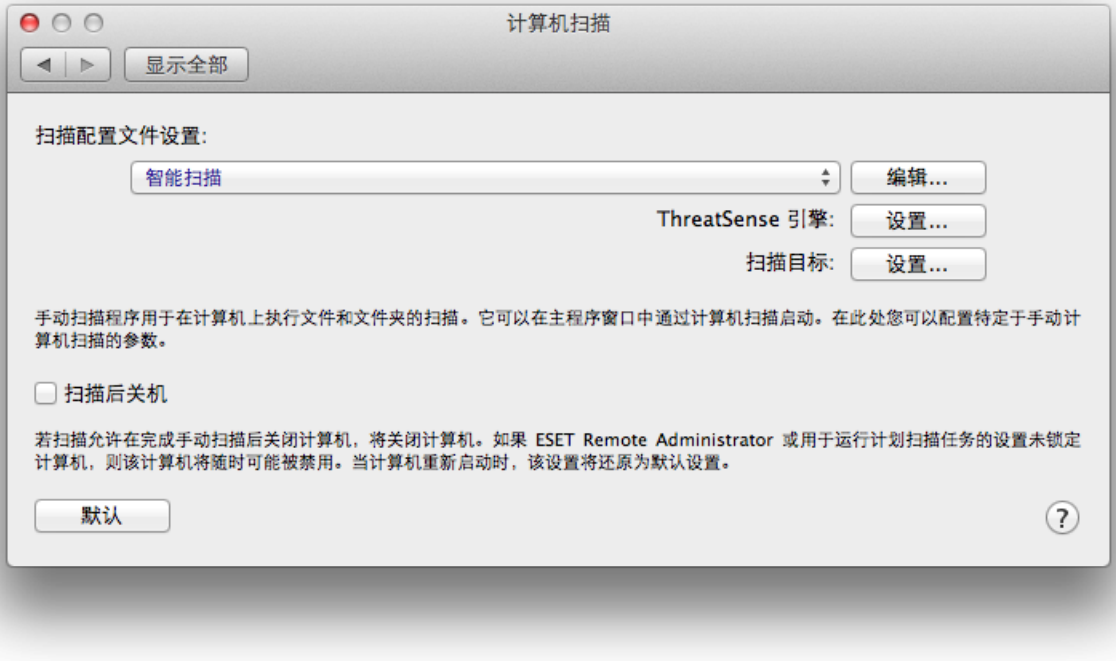
扫描目标树结构允许您选择要进行病毒扫描的文件和文件夹。也可以根据配置文件的设置选择文件夹。

还可以通过输入要扫描的文件或文件夹路径，更精确地定义扫描目标。通过选中与给定文件或文件夹相对应的复选框，从列有计算机上所有可用文件夹的树结构中选择目标。

扫描配置文件

可以保存您的首选扫描设置以用于将来的扫描。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，请从主菜单单击**设置** > **进入应用程序首选项...**（或按 *cmd+,*）> **计算机扫描**并单击当前配置文件列表旁边的**编辑...**



为了帮助您创建满足需求的扫描配置文件，请参阅 ThreatSense 引擎参数设置部分，查看扫描设置中每个参数的描述。

示例

假设您想要创建自己的扫描配置文件而且智能扫描配置部分适用，但您不想要扫描加壳程序或潜在的不安全应用程序，并且还想要应用严格清除。在**手动扫描程序配置文件列表**窗口中，键入配置文件名称、单击**添加**按钮，然后通过单击**确定**进行确认。通过使用 **ThreatSense 引擎**和**扫描目标**设置调整参数以使其满足您的需求。

如果您想要在手动扫描完成后关闭操作系统并关闭计算机，请使用**扫描后关机**选项。

ThreatSense 引擎参数设置

ThreatSense 是 ESET 的专利技术，包含多种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，它还可在新威胁开始传播的较早阶段提供防护。它采用了多种方法（代码分析、代码仿真、一般的识别码等），可显著提高系统安全性。扫描引擎可同时控制多个数据流，最大限度地提高效率和检测速度。ThreatSense 技术还可成功阻止 Rootkit。

ThreatSense 技术设置选项允许您指定若干扫描参数：

- 要扫描的文件类型和扩展名
- 不同检测方法的组合
- 清除级别等

若要进入设置窗口，请依次单击**“设置”>“进入应用程序首选项...”**（或按 *cmd+,*），然后单击 ThreatSense 引擎**设置**按钮，该按钮位于**启动防护**、**实时防护**和**计算机扫描**模块中，所有这些模块都使用 ThreatSense 技术（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：

- **启动防护** – 自动启动文件检查
- **实时防护** – 文件系统实时防护
- **计算机扫描** – 手动计算机扫描
- **Web 访问防护**
- **电子邮件防护**

ThreatSense 参数已针对每个模块进行了特定优化，对其进行修改可能会显著影响系统操作。例如，将设置更改为始终扫描加壳程序，或在文件系统实时防护模块中启用高级启发式扫描，可能会造成系统性能下降。因此，建议您保留所有模块（“计算机扫描”除外）的默认 ThreatSense 参数不变。

对象

对象部分允许您定义将扫描渗透的文件。

- **符号链接** –（仅计算机扫描）扫描文件，这些文件包含被当作某个文件或目录的路径的文本字符串。

- **电子邮件文件** –（在实时防护中不可用）扫描电子邮件文件。

- **邮箱** –（在实时防护中不可用）扫描系统中的用户邮箱。误用此选项可能导致与电子邮件客户端的冲突。要更多了解有关此选项的优缺点，请阅读以下知识库文章。

- **压缩文件** –（在实时防护中不可用）扫描压缩文件（.rar、.zip、.arj、.tar 等）中被压缩的文件。

- **自解压文件** –（在实时防护中不可用）扫描包含在自解压文件中的文件。

- **加壳程序** – 和标准压缩类型不同，加壳程序在内存中解压。选中此选项后，还会扫描标准静态加壳程序（UPX、yoda、ASPack、FGS 等）。

选项

在**选项**部分，可以选择在系统扫描期间所用的方法。可用选项包括：

- **启发式扫描** – 启发式扫描使用一种可分析程序（恶意）活动的算法。启发式扫描检测的主要优点是能够检测到以前不存在的新恶意软件。

- **高级启发式扫描** – 高级启发式扫描具有一种独特的由 ESET 开发的启发式扫描算法，它使用高级编程语言编写而成，针对检测计算机蠕虫和木马进行优化。有了高级启发式扫描，程序的检测能力显著提高。

清除

清除设置确定扫描程序清除被感染文件的方式。 共有 3 个清除级别：

- **不清除** – 被感染文件不会被自动清除。 程序会显示一个警告窗口，并允许您选择操作。

- **标准清除** – 程序将尝试自动清除或删除被感染的文件。 如果无法自动选择正确操作，程序将提供一组后续操作选择。 如果无法完成预定义操作，也将显示后续操作选择。

- **严格清除** – 程序将清除或删除所有被感染文件（包括压缩文件）。 唯一例外的是系统文件。 如果无法清除文件，则您将收到一条通知，要求您选择要采取的操作类型。

> **标准清除模式 – 压缩文件清除**
> 在默认标准清除模式下，仅当压缩文件中的所有文件都被感染时，才会删除整个压缩文件。 如果压缩文件包含合法文件以及被感染的文件，则不删除。 如果在严格清除模式下检测到被感染的压缩文件，即使其中包含干净的文件，也会删除整个压缩文件。

排除

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

默认情况下，扫描所有文件，无论其扩展名是什么。可将任何扩展名添加到不扫描的文件列表中。使用 + 和 − 按钮，可以启用或禁用对特定扩展名的扫描。

如果扫描特定文件类型会妨碍程序正常工作，有时候需要不扫描这些文件。例如，建议排除 *log*、*cfg* 和 *tmp* 文件。用于输入文件扩展名的正确格式是：

log

cfg

tmp

限制

限制部分允许您指定要扫描的对象的最大大小和嵌套压缩文件的层数：

- **最大大小：**定义要扫描的对象的最大大小。病毒防护模块仅将扫描小于指定大小的对象。不建议更改默认值，因为通常无需修改它。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。
- **最长扫描时间：**定义为扫描对象分配的最长时间。如果已在此处输入用户定义的值，则时间用完后病毒防护模块将停止扫描对象，不管扫描是否完成。
- **最大嵌套层数：**指定压缩文件扫描的最大深度。不建议更改默认值 10；因为通常情况下无需修改它。如果扫描因嵌套压缩文件的数量而提前终止，则压缩文件仍将处于未选中状态。
- **最大文件大小：**此选项允许您指定要扫描的压缩文件（当解压缩时）中所包含文件的最大文件大小。如果因此限制而提前终止扫描，则压缩文件仍将处于未选中状态。

其他

启用智能优化

在启用了智能优化的情况下，对设置进行了优化，以便在不影响扫描速度的情况下确保最高效的扫描级别。各种防护模块利用不同的扫描方法进行智能扫描。智能优化在该产品中未严格定义。ESET 开发团队不断进行新更改，然后将这些更改通过定期更新集成到 ESET Endpoint Antivirus for macOS。如果禁用了智能优化，则在执行扫描时仅应用特定模块的 ThreatSense 核心中用户定义的设置。

扫描交换数据流（仅手动扫描程序）

文件系统使用的交换数据流（资源/数据派生）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。

检测到渗透

渗透可通过各种渠道进入系统：网页、共享文件夹、电子邮件或可移动计算机设备。USB。外部磁盘。CD。DVD 等）。

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，建议您遵循以下步骤：

1. 单击**“计算机扫描”**。
2. 单击**智能扫描**（更多信息，请参见智能扫描部分）。
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恶意软件。

以下为 ESET Endpoint Antivirus for macOS 如何处理渗透的一般示例，假设使用默认清除级别的实时文件系统监视程序检测到了渗透。实时防护将尝试清除或删除该文件。如果实时防护模块没有预定义操作，程序将显示一个警报窗口，要求您从中选择一个选项。一般会有**清除**、**删除**和**不操作**等选项。建议您不要选择**不操作**，因为这样被感染文件将保持其被感染状态。只有当您确信该文件无害，只是检测失误所致时，才可以使用此选项。

清除和删除
如果文件遭到了病毒攻击（该病毒在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，以便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。

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

Web 和电子邮件防护

若要从主菜单中访问 Web 和邮件防护，请单击**设置** > **Web 和邮件**。在此处，您还可以通过单击**设置**访问每个模块的详细设置。

> **扫描例外**
> ESET Endpoint Antivirus for macOS 不会扫描加密协议 HTTPS、POP3S 和 IMAPS。

- **Web 访问防护** – 监视 Web 浏览器和远程服务器之间的 HTTP 通信。
- **电子邮件客户端防护** – 提供对通过 POP3 和 IMAP 协议接收的电子邮件通信的控制。
- **网络钓鱼防护** – 阻止来自网站或域的潜在钓鱼攻击。

Web 访问保护

Web 访问保护监视 Web 浏览器和远程服务器之间的通信是否遵从 HTTP（超文本传输协议）规则。

Web 过滤可通过定义 HTTP 通信的端口号和/或 URL 地址来实现。

端口

在**端口**选项卡中，您可以定义用于 HTTP 通信的端口号。默认情况下，预定义的端口号为 80、8080 和 3128。

URL 列表

URL 列表部分使您能够指定要阻止、允许或不进行检查的 HTTP 地址。您将无法访问阻止的地址列表中的网站。无需进行恶意代码扫描，即可访问排除的地址列表中的网站。

若要仅允许访问**允许的 URL**列表中列出的 URL，请选择**限制 URL 地址**。

若要激活列表，请选择列表名称旁的**已启用**。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**接收通知**。

在建立 URL 列表时，可使用特殊符号 *（星号）和 ?（问号）。星号可以替代任意字符串，而问号可以替代任意符号。指定排除的地址时，请务必谨慎，因为此列表只应包含信任的和安全的地址。同样，必须确保在此列表中正确使用符号 * 和 ?。

电子邮件防护

电子邮件防护可提供对通过 POP3 和 IMAP 协议接收的电子邮件通信的控制。检查传入邮件时，ESET Endpoint Antivirus for macOS 使用 ThreatSense 扫描引擎内包含的高级扫描方法，POP3 和 IMAP 协议通信的扫描将在使用任何电子邮件客户端时进行。

ThreatSense 引擎：设置 – 高级病毒扫描程序设置使您能够配置扫描目标、检测方法等。单击**设置**将显示详细的扫描程序设置窗口。

将标记消息附加到电子邮件脚注 – 在扫描某个电子邮件后，包含扫描结果的通知可能会被附加到邮件。不可完全依赖标记消息，因为标记可能会在有问题的 HTML 消息中被遗漏且可能由某些病毒伪造。可用选项包括：

- **从不** – 将不添加任何标记消息
- **仅对被感染的电子邮件** – 仅将包含恶意软件的邮件标记为已检查
- **对所有扫描的电子邮件** - ESET Endpoint Antivirus for macOS 将向所有扫描过的电子邮件附加标记消息

在已接收并阅读的被感染电子邮件主题中添加注释 – 如果想要电子邮件防护在被感染的电子邮件中包含病毒警告，请选中此复选框。此功能允许您对被感染的电子邮件进行简单过滤。它还为收件人提高了可信度级别，如果检测到了渗透，它将提供有关给定电子邮件或发件人的威胁级别的有价值信息。

添加到被感染电子邮件主题中的模板 – 编辑此模板以修改被感染电子邮件的主题前缀格式。

- %avstatus% - 添加电子邮件感染状态（例如：清除、感染等）
- %virus% - 添加威胁的名称
- %product% - 添加您的 ESET 产品的名称（此例中 - ESET Endpoint Antivirus for macOS）
- %product_url% - 添加 ESET 网站链接 (www.eset.com)

在此窗口的下半部分，您还可以启用/禁用对通过 POP3 和 IMAP 协议接收的电子邮件通信的检查。要了解详细信息，请参阅以下主题：

- POP3 协议检查
- IMAP 协议检查

POP3 协议检查

POP3 协议是在电子邮件客户端应用程序中接收电子邮件通信时使用最广泛的协议。无论您使用哪种电子邮件客户端，ESET Endpoint Antivirus for macOS 均针对此协议提供防护。

提供此控制的防护模块将在系统启动时自动启动，并随后在内存中保持启用。请确保该模块处于启用状态，以使协议过滤正常工作；将自动执行 POP3 协议检查，无需重新配置电子邮件客户端。默认情况下，将扫描端口 110 上的所有通信，但如果有必要，可以添加其他通信端口。端口号必须以逗号分隔。

如果已选中**启用 POP3 协议检查**，将监视所有 POP3 通信中是否存在恶意软件。

IMAP 协议检查

Internet 消息访问协议 (IMAP) 是另一个用于电子邮件检索的 Internet 协议。与 POP3 相比，IMAP 具有一些优势，比如多个客户端可同时连接到同一邮箱，并保留邮件状态信息，如邮件是否已读、已回复或已删除。ESET Endpoint Antivirus for macOS 为此协议提供保护，无论使用哪种电子邮件客户端。

提供此控制的防护模块将在系统启动时自动启动，并随后在内存中保持启用。请确保 IMAP 协议检查处于启用状态，以使模块正常工作。IMAP协议控制是自动执行的，无需重新配置电子邮件客户端。默认情况下，将扫描端口 143 上的所有通信，但如果有必要，可以添加其他通信端口。端口号必须以逗号分隔。

如果已选中**启用 IMAP 协议检查**，将监视所有 IMAP 通信中是否存在恶意软件。

网络钓鱼防护

术语网络钓鱼定义了使用社交工程（操纵用户以获取保密信息）的犯罪行为。网络钓鱼通常用于获取对敏感数据的访问权限，例如银行帐号、信用卡号或 PIN 码或者用户名和密码。

建议您保持启用网络钓鱼防护（**设置 > 进入应用程序首选项. . . > 网络钓鱼防护**）。将阻止所有来自危险网站或域的潜在网络钓鱼攻击，并且将显示警告通知，以告知您此类攻击。

设备控制

ESET Endpoint Antivirus for macOS 允许您扫描、阻止或调整扩展的过滤器和权限，并定义用户是否可以访问和使用给定存储设备。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。

> **macOS 11 及更高版本上的设备控制**
> 在 macOS 11 及更高版本上安装的 ESET Endpoint Antivirus for macOS 仅会扫描存储设备。（例如 USB 驱动器、CD/DVD...）

macOS 10.15 及较旧版本上支持的外部设备：

- 磁盘存储（HDD、USB 闪存驱动器）
- CD/DVD
- USB 打印机
- 刻录设备

- 串行端口
- 网络
- 便携式设备

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。

设备控制日志记录了所有触发设备控制的事件。从 ESET Endpoint Antivirus for macOS 主程序窗口的**工具** > 日志文件可以查看日志条目。

规则编辑器

在**设置** > **输入应用程序首选项. . .** > **设备控制**中可以修改设备控制设置选项。

单击**启用设备控制**可激活 ESET Endpoint Antivirus for macOS 中的设备控制功能。 在启用设备控制后，即可管理并编辑设备控制规则。 选中规则名称旁边的复制框可启用/禁用规则。

使用  或者  按钮来添加或删除规则。 按优先级顺序列出规则，优先级越高越靠近顶端。 若要重新排列顺序，将规则拖放到其新位置，或者单击  并选择其中的一个选项。

ESET Endpoint Antivirus for macOS 自动检测所有当前插入的设备及其参数（设备类型、供应商、型号和序列号）。 单击**填充**选项，选择该设备，然后单击**继续**来创建规则，而不是手动创建规则。

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

名称
在**名称**字段中输入规则说明以更好识别。 **规则已启用**复选框可禁用或启用此规则 – 如果不想要永久删除规则，该选项非常有用。

设备类型
从下拉菜单中选择外部设备类型。 可从操作系统中收集设备类型信息。 存储设备包括通过 USB 或 FireWire 连接的外部磁盘或传统存储卡读卡器。 成像设备示例包括扫描仪或照相机。 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：

读/写 – 将允许对设备的完全访问权限

只读 – 将仅允许对设备进行读取访问

阻止 – 将阻止对设备的访问

标准类型
选择**设备组**或**设备**。 下面显示的其他参数可用于微调规则，并根据设备定制规则。

供应商 – 按供应商名称或 ID 过滤

型号 – 设备的给定名称

序列号 – 外部设备通常具有自己的序列号。 如果是 CD/DVD，这是给定介质的序列号，而不是 CD/DVD 驱动器

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

> **提示**
> 若要查看设备信息，请为该类型的设备创建规则，然后将设备连接到您的计算机。 在连接设备后，设备详细信息就会显示在设备控制日志中。

日志记录严重级别

始终 – 记录所有事件

诊断 – 记录微调程序所需的信息

信息 – 记录信息性消息以及以上所有记录

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
通过将用户添加到用户列表，即可将规则限制为特定用户或用户组：

编辑... – 打开**标识编辑器**，可以在其中选择用户或组。 若要定义用户列表，请从左侧的**用户**列表中选择用户，然后单击**添加**。 若要删除用户，请从**选择用户**列表中选择他们的名称，然后单击**删除**。 若要显示所有系统用户，请选择**显示所有用户**。 如果列表为空，将允许所有用户

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

工具

工具菜单包括帮助简化程序管理的模块，并为高级用户提供附加选项。

日志文件

日志文件包含所有已发生的重要程序事件的信息，并提供检测到的威胁的概要信息。日志记录是系统分析、威胁检测以及故障排除的必要工具。日志记录在后台主动执行，无需用户交互。对信息的记录是根据当前日志级别设置进行的。可以直接从 ESET Endpoint Antivirus for macOS 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 ESET Endpoint Antivirus for macOS 主菜单中访问，方法是单击**工具 > 日志文件**。使用窗口顶部的“日志”下拉菜单选择所需日志类型。可用日志包括：

1. **检测到的威胁** – 与渗透检测相关的所有事件的信息。

2. **事件** - ESET Endpoint Antivirus for macOS 执行的所有重要操作都记录在事件日志中。

3. **计算机扫描** – 所有已完成的扫描的结果都显示在此窗口中。双击任意条目以查看指定电脑扫描的详细信息。

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

5. **已过滤的网站** – 如果您想要查看已由 Web 访问保护阻止的网站列表，则此列表很有用。. 在这些日志中，您可以查看时间、URL、状态、IP 地址、用户和打开了到特定网站的连接的应用程序。

右键单击任意日志文件，然后单击**复制**以将该日志文件的内容复制到剪贴板。

日志维护

可从主程序窗口访问 ESET Endpoint Antivirus for macOS 的日志记录配置。依次单击**设置 > 进入应用程序首选项 > 工具 > 日志文件**。您可以为日志文件指定以下选项：

- **自动删除旧日志记录** – 自动删除指定天数以前的日志条目。
- **自动优化日志文件** – 如果未用记录百分比超过指定值，则启用日志文件的自动碎片整理。

图形用户界面、威胁和事件消息上显示的所有相关信息都可以采用人类可阅读的文本格式（如纯文本或 CSV、用逗号分隔的值）存储。如果您要使这些文件可使用第三方工具处理，请选中**启用日志记录到文本文件**旁的复选框。

若要定义日志文件将保存到的目标文件夹，请单击**高级设置**旁的**设置**。

根据在**文本日志文件**:**编辑**下选择的选项，您可以保存写入了以下信息的日志：

- 用户名和密码无效、无法更新模块等事件将写入 *eventslog.txt* 文件
- 由启动扫描程序、实时防护或计算机扫描检测到的威胁将存储在名为 *threatslog.txt* 的文件中
- 所有已完成扫描的结果都将采用 *scanlog.NUMBER.txt* 格式保存
- devctllog.txt 中提到了设备控制所阻止的设备

若要为**默认计算机扫描日志记录**配置过滤器，请单击**编辑**并根据需要选择/取消选择日志类型。可以在日志过滤中找到对这些日志类型的进一步说明。

日志过滤

有关重要系统事件的日志存储信息。日志过滤功能允许您显示有关特定事件的记录。

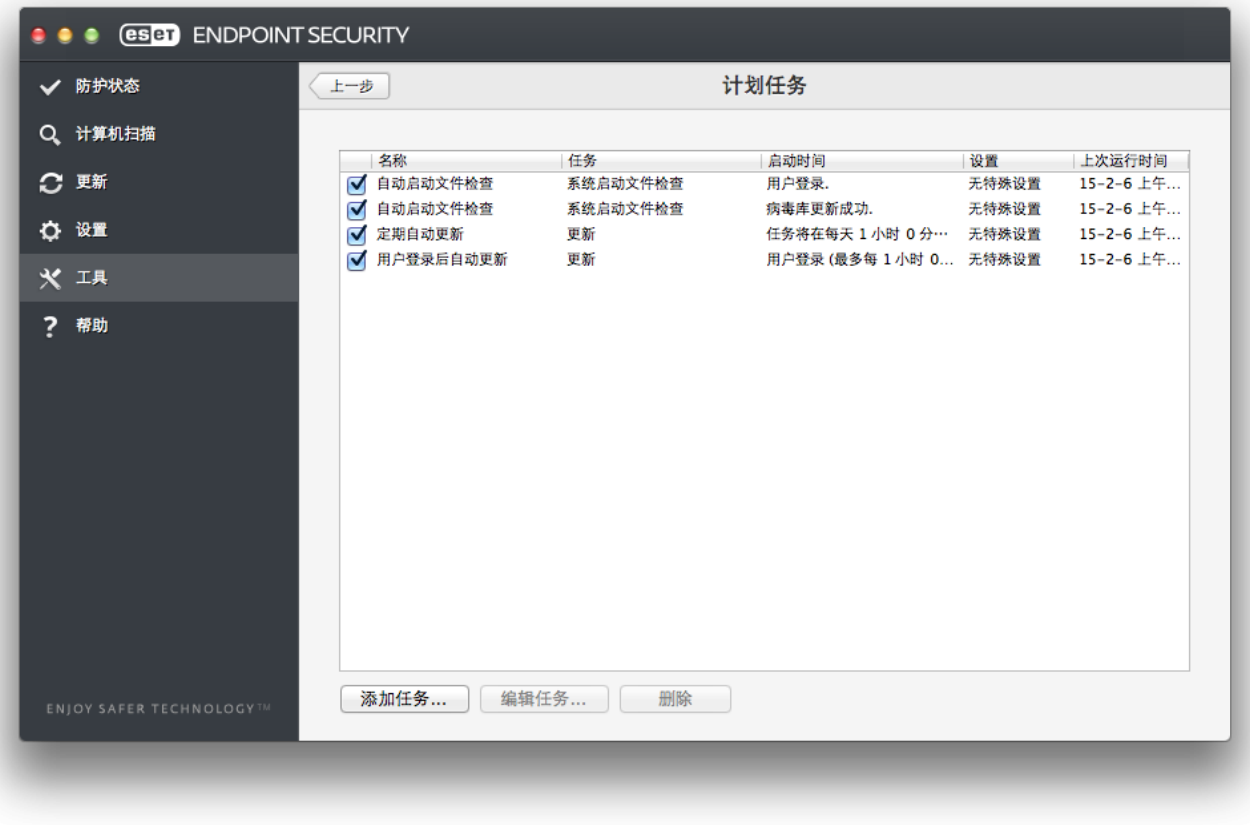
下面列出了最常用的日志类型：

- **严重警告** – 严重系统错误（例如，病毒防护无法启动）

- **错误** – 诸如“下载文件时出错”之类的错误消息和严重错误
- **警告** – 警告消息
- **信息性记录** – 包括成功更新、警报等的信息性消息
- **诊断记录** – 微调程序所需的信息以及上述所有记录。

计划任务

计划任务可以在 ESET Endpoint Antivirus for macOS 主菜单的**工具**下找到。**计划任务**包含所有计划任务和配置属性的列表，如预定义的日期、时间和使用的扫描配置文件。



计划任务管理和启动具有预定义配置和属性的计划任务。配置和属性包含日期和时间等信息以及执行任务期间使用的指定配置文件。

默认情况下，计划任务中显示以下计划任务：

- 日志维护（在计划任务设置中启用**显示系统任务**后）
- 用户登录后启动文件检查
- 成功更新检测模块后启动文件检查
- 定期自动更新
- 用户登录后自动更新

若要编辑现有计划任务的（包括默认和用户定义的）配置，请在按 CTRL 键的同时单击要修改的任务并选择**编辑**，或选择该任务并单击**编辑任务**。

创建新任务

若要在计划任务中创建新任务，请单击**添加任务**，或者按 CTRL 键并单击空白字段，然后从右键菜单中选择**添加**。 共有 4 种类型的计划任务：

- **运行应用程序**
- **更新**
- **手动计算机扫描**
- **系统启动文件检查**

用户定义的任务
默认情况下，应用程序由 ESET 创建的特殊用户（具有限制权限）运行。 若要更改默认用户，请在命令前键入用户名，后跟冒号（:）。 您还可以在此功能中使用**根**用户。

示例： 以用户身份运行任务
在此示例中，我们计划在所选时间以名为 **UserOne** 的用户身份启动“计算器”应用：
1. 在**计划任务**中，选择**添加任务**。
2. 键入任务名称。 选择**运行应用程序**作为**计划任务**。 在**运行任务**窗口中，选择**一次**以运行一次此任务。 单击**下一步**。
3. 单击“浏览”，然后选择“计算器”应用。
4. 在应用程序路径之前键入 **UserOne:**
。UserOne:'/Applications/Calculator.app/Contents/MacOs/Calculator'。。然后单击**下一步**。
5. 选择要执行任务的时间，然后单击**下一步**。
6. 如果任务无法运行，请选择其他选项，然后单击**下一步**。
7. 单击**完成**。
8. ESET 计划任务将于选定的时间启动“计算器”应用。

用户名限制
不能在用户名前使用空格或空格字符。 用户名中也不能使用空格。 而应该使用空白字符。

以目录所有者身份扫描
您可以用目录所有者身份扫描目录：
root:for VOLUME in /Volumes/*; do sudo -u \#`stat -f %u "$VOLUME"` '/Applications/ESET Endpoint Security.app/Contents/MacOS/esets_scan' -f /tmp/scan_log "$VOLUME"; done

您还可以作为当前登录的用户扫描 /tmp 文件夹：
root:sudo -u \#`stat -f %u /dev/console` '/Applications/ESET Endpoint Security.app/Contents/MacOS/esets_scan' /tmp

示例： 更新任务

在此示例中，我们将创建将在指定时间运行的更新任务。

1. 从**计划任务**下拉菜单中选择**更新**。
2. 在**任务名称**字段中键入任务的名称。
3. 从**运行任务**下拉菜单中选择任务频率。 根据所选频率，系统将提示您指定不同的更新参数。 如果选择**用户定义**，系统将提示您以 cron 格式指定日期/时间（请参阅创建用户定义的任务部分以了解更多详细信息）。
4. 在下一步中，选择无法在计划时间执行或完成任务时要使用的其他选项。
5. 单击**完成**。 新的计划任务将添加到当前计划任务列表。

默认情况下，ESET Endpoint Antivirus for macOS 包含配置为确保正确产品功能的预定义计划任务。 这些任务不能进行修改，且默认情况下处于隐藏状态。 若要查看这些任务，请转到主菜单，接着依次单击**设置** > **进入应用程序首选项** > **计划任务**，然后选择**显示系统任务**。

创建用户定义的任务

当您从“运行任务”下拉菜单中选择“用户定义”作为任务类型时，有一些必须定义的特殊参数。

用户定义的任务的日期和时间必须以年扩展 cron 格式输入（空格分隔的 6 个字段组成的字符串）：

分钟(0-59) 小时(0-23) 日期(1-31) 月份(1-12) 年份(1970-2099) 星期几(0-7)(周日 = 0 或 7)

示例：

```
30 6 22 3 2012 4
```

cron 表达式支持以下特殊字符：

- 星号（*）- 表达式将匹配字段的所有值；例如，第 3 个字段（日期）中的星号表示每一天
- 连字符（-）- 定义范围；例如， `3-9`
- 逗号（,）- 分隔列表项；例如，`1,3,7,8`
- 斜杠（/）- 定义范围增量；例如，第 3 个字段（日期）中的 `3-28/5` 表示该月的 3 号，然后每隔 5 天。

不支持日期名称 ((Monday-Sunday)) 和月份名称 ((January-December))。

用户定义的任务

如果定义日期和星期几，则仅当两个字段都匹配时才会执行命令。

LiveGrid®

LiveGrid® 预警系统使 ESET 能够即时并持续地获得有关新渗透的信息。双向 LiveGrid® 预警系统只有一个目的，即加强我们能够提供给您的防护。确保我们在新威胁刚出现时就能够察觉的最好方式是“链接”至尽可能多的客户，并使用他们收集的信息来使我们的检测模块持续保持最新。选择适用于 LiveGrid® 的两个选项之一：

1.您可以选择不启用 LiveGrid® 预警系统。您不会失去软件中的任何功能，但在某些情况下ESET Endpoint Antivirus for macOS 可能会比检测模块更新更快地响应新威胁。

2.您可以配置 LiveGrid® 预警系统，以提交有关新威胁的匿名信息，其中包含新威胁代码。此信息可以发送到 ESET 以供详细分析。研究这些威胁将帮助 ESET 更新其威胁数据库并提高我们的威胁检测能力。

LiveGrid® 预警系统将收集您的计算机上有关新检测到的威胁的信息。这些信息可能包括出现威胁的文件的样本或副本、该文件的路径、文件名、日期和时间、威胁出现在计算机上的过程，以及有关您的计算机操作系统的信息。

虽然这样可能会向 ESET 威胁实验室透露一些有关您或您的计算机的信息（目录路径中的用户名等等），但除了帮助我们对新威胁作出快速反应之外，此信息将不会被用于任何其他用途。

若要从主菜单中访问 LiveGrid® 设置，请单击**设置 > 进入应用程序首选项. . . > LiveGrid®**。选择**启用 ESET LiveGrid® 信誉系统(建议)**以激活 LiveGrid®然后单击**高级选项**旁边的**设置**

可疑文件

默认情况下ESET Endpoint Antivirus for macOS 配置为将可疑文件提交至 ESET 威胁实验室以供详细分析。如果您不希望自动提交这些文件，可取消选择**提交可疑文件设置 > 进入应用程序首选项 > LiveGrid® > 设置**

如果发现可疑文件，可以将其提交到我们的威胁实验室以供分析。 为此，可以从主程序窗口中依次单击**工具 > 提交文件以供分析**。 如果文件是一个恶意应用程序，则以后的更新中将添加对此程序的检测。

提交匿名统计信息 - ESET LiveGrid® 预警系统会收集您的计算机上有关新检测到的威胁的匿名信息。 该信息包括渗透名称、检测的日期和时间ESET 安全产品版本、操作系统版本和位置设置。 这些统计信息通常一天向 ESET 服务器传递一次或两次。

示例： 提交的统计数据包

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"

# language="ENGLISH"

# osver=9.5.0

# engine=5417

# components=2.50.2

# moduleid=0x4e4f4d41

# filesize=28368

# filename=Users/UserOne/Documents/Incoming/rdgFR1463[1].zip
```

排除过滤器 – 此选项允许您从提交队列中排除某些文件类型。 例如，将可能包含机密信息的文件（如文档或电子表格）排除在外可能很有用。 默认情况下，最常见的文件类型均被排除(.doc, .rtf 等）。 您可以将文件类型添加到排除文件列表。

联系人电子邮件(可选) – 在我们需要更多信息用于分析时，将用到您的电子邮件地址。 请注意，除非需要更多信息，否则 ESET 不会与您联系。

隔离

隔离的主要目的是安全存储被感染文件。如果文件出现以下情况，则应该隔离该文件：无法清除、不安全或被建议删除，或被 ESET Endpoint Antivirus for macOS 错误地检测到。

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

可在表格中查看储存在隔离文件夹中的文件，表格中显示隔离的日期和时间、被感染文件原始位置的路径、文件大小（以字节为单位）、隔离它的原因（例如，由用户添加）以及检测到的威胁数量。即使卸载了 ESET Endpoint Antivirus for macOS，隔离文件夹（*/Library/Application Support/Eset/esets/cache/quarantine*）仍将保留在系统中。隔离的文件以安全的加密形式存储，在安装 ESET Endpoint Antivirus for macOS 后可再次恢复。

隔离文件

ESET Endpoint Antivirus for macOS 自动隔离被删除的文件（如果您尚未在警报窗口中取消选择此选项）。在“隔离区”窗口中，您可以单击“隔离区”以将任何文件手动添加到隔离区。您还可以随时按住 Ctrl 键并单击某个文件，然后从右键菜单中选择“服务”>“ESET Endpoint Antivirus for macOS - 将文件添加到隔离区”以将该文件发送到隔离区。

从隔离恢复

隔离的文件还可以恢复到它们的原始位置，若要执行此操作，请选择隔离的文件，然后单击**恢复**。也可以从右键菜单进行恢复，按 CTRL 键并单击“隔离区”窗口中的给定文件，然后单击**恢复**。您可以使用**恢复至**将某个文件恢复到被隔离时所处位置以外的位置。

提交隔离区中的文件

如果您隔离了程序未检测到的可疑文件，或文件被错误地评估为被感染（如启发式扫描代码分析所做的评估）并被隔离，请将该文件发送到 ESET 威胁实验室。若要提交隔离区中的文件，请按 CTRL 键并单击该文件，然后从右键菜单中选择**提交文件以供分析**。

权限

ESET Endpoint Antivirus for macOS 设置对您的组织安全策略非常重要。未经授权的修改可能会破坏系统的稳定性和防护。最终，您可以选择哪些用户具有编辑程序配置的权限。

您可以在**设置 > 进入应用程序首选项 > 用户 > 权限**下配置授权用户。

为最大限度地保障系统安全，必须正确配置程序。未经授权的修改可能导致丢失重要数据。若要设置授权用户列表，请从左侧的**用户**列表选择用户，然后单击**添加**。若要删除用户，请从右侧的**授权用户**列表选择他们的名称，然后单击**删除**。若要显示所有系统用户，请选择**显示所有用户**。

> **空的授权用户列表**
> 如果授权用户列表为空，系统的所有用户都将具有编辑程序设置的权限。

演示模式

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

若要手动启用演示模式，请单击**设置 > 进入应用程序首选项. . . > 演示模式 > 启用演示模式**。

选中**以全屏形式自动启用演示模式**旁的复选框，以在应用程序以全屏模式运行时自动触发演示模式。启用此功能后，每当您启动全屏应用程序时就会启动演示模式，并且将在您退出应用程序后自动停止该模式。这对于开始进行演示时尤其有用。

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

启用演示模式将存在潜在安全风险，因此 ESET Endpoint Antivirus for macOS 防护状态图标将变成橙色，并显示警告。

正在运行的进程

正在运行的进程列表显示您的计算机上正在运行的进程。ESET Endpoint Antivirus for macOS 使用 LiveGrid® 技术提供有关正在运行的进程的详细信息以保护用户。

- **进程** – 当前在您的计算机上运行的进程的名称。您还可以使用活动监视器（位于 */Applications/Utilities* 中）查看正在您的计算机上运行的所有进程。
- **风险级别** – 在大多数情况下，ESET Endpoint Antivirus for macOS 和 ESET LiveGrid® 技术将风险级别指定给对象（文件、进程等）的方法是使用一系列启发式扫描规则检查每个对象的特性，然后评估恶意活动的可能性。根据这些启发式扫描规则，可以为对象指定风险级别。标记为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。这会提高手动扫描和实时扫描的速度。当应用程序被标记为“未知（黄色）”时，它不一定是恶意软件。通常它只是一个较新的应用程序。如果您对某个文件不确定，可以将其提交给 ESET 威胁实验室以供分析。如果文件被证实是一个恶意应用程序，则以后的更新中将增加它的签名。
- **用户数量** – 使用给定应用程序的用户数量。此信息由 ESET LiveGrid® 技术收集。
- **发现时间** – 自应用程序被 ESET LiveGrid® 技术发现以来的时段。
- **应用程序捆绑 ID** – 供应商或应用程序进程的名称。

通过单击给定进程，将在窗口底部显示以下信息：

- **文件** – 计算机上应用程序的位置
- **文件大小** – 磁盘上文件的物理大小
- **文件说明** – 基于操作系统说明的文件特征
- **应用程序捆绑 ID** – 供应商或应用程序进程的名称
- **文件版本** – 来自应用程序发布者的信息

- **产品名称** – 应用程序名称和/或企业名称

用户界面

用户界面配置选项允许您调整工作环境以适应您的需要。可以从主菜单访问这些选项，方法是单击**设置** > **进入应用程序首选项...** > **界面**。

- 若要在系统启动时显示 ESET Endpoint Antivirus for macOS 初始屏幕，请选择**在启动时显示初始屏幕**。

- **当前在平台中的应用程序**允许您在 macOS 平台中显示 ESET Endpoint Antivirus for macOS 图标，并通过按 *cmd+tab* 在 ESET Endpoint Antivirus for macOS 和其他正在运行的应用程序之间进行切换。更改将在您重新启动 ESET Endpoint Antivirus for macOS（通常由计算机重新启动触发）后生效。

- **使用标准菜单**允许您使用特定的键盘快捷方式（请参见键盘快捷方式），并查看 MacOS 菜单栏（屏幕顶部）上的标准菜单项（用户界面、设置和工具）。

- 启用**显示工具提示**，以便在光标置于 ESET Endpoint Antivirus for macOS 中的特定选项上时显示工具提示。

- **显示隐藏文件**允许您查看并选择在**计算机扫描**的**扫描目标**设置中的隐藏文件。

- 默认情况下，ESET Endpoint Antivirus for macOS 图标显示在位于 macOS 菜单栏（屏幕顶部）右侧的菜单栏扩展中。若要禁用此选项，请取消选择**在菜单栏扩展中显示图标**。此更改将在您重新启动 ESET Endpoint Antivirus for macOS（通常由计算机重新启动触发）后生效。

警报和通知

警报和通知部分允许您配置 ESET Endpoint Antivirus for macOS 处理威胁警报、防护状态和系统通知的方式。

禁用**显示警报**将禁用所有警报窗口，而且仅在特定情况下建议启用。对于大多数用户，我们建议保留该选项的默认设置（已启用）。本章将介绍高级选项。

选择**在桌面上显示通知**将使不需要用户交互的警报窗口显示在桌面上（默认情况下，在屏幕的右上角）。通过调整在 X **秒后自动关闭通知**值（默认为 5 秒），可以定义通知显示的时长。

自 ESET Endpoint Antivirus for macOS 版本 6.2 起，您还可以阻止某些**防护状态**显示在程序的主屏幕（**防护状态**窗口）中。若要了解此方面的详细信息，请参阅防护状态。

显示警报

ESET Endpoint Antivirus for macOS 显示警报对话框窗口，向您通知新程序版本、操作系统更新、禁用特定程序组件、删除日志等。您可以通过选择**请勿再次显示该对话框**隐藏各项通知。

对话框列表（在**设置** > **进入应用程序首选项...** > **警报和通知** > **显示警报：设置...** 下找到）显示由 ESET Endpoint Antivirus for macOS 触发的所有警报对话框列表。若要启用或隐藏每个通知，请选中**对话框名称**左侧的复选框。选中复选框时，将始终显示通知并且**显示条件**不应用。如果不希望收到有关列表中特定事件的通知，请取消选中该选项，还可以定义特定操作将执行所依据的**显示条件**。

防护状态

可以更改 ESET Endpoint Antivirus for macOS 的当前防护状态，方法是在**设置 > 进入应用程序首选项. . . > 警报和通知 > 在防护状态屏幕上显示：设置**中激活或取消激活状态。各种程序功能的状态将从 ESET Endpoint Antivirus for macOS 主屏幕（**防护状态**窗口）显示或隐藏。

您可以隐藏以下程序功能的防护状态：

- 网络钓鱼防护
- Web 访问保护
- 电子邮件客户端防护
- 演示模式
- 操作系统更新
- 许可证到期
- 需要重新启动计算机

右键菜单

为了使 ESET Endpoint Antivirus for macOS 功能在右键菜单中可用，请单击**设置 > 进入应用程序首选项 > 右键菜单**，然后选中**集成到右键菜单**旁的复选框。更改将在您注销或重新启动计算机后生效。当您按 CTRL 键并单击任何文件或文件夹时，桌面上和 **Finder** 窗口中将提供右键菜单选项。

更新

定期更新 ESET Endpoint Antivirus for macOS 对于保持最高级别的安全性很有必要。“更新”模块通过下载最新检测模块确保程序始终为最新。

通过从主菜单中单击**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，并查看是否需要更新。若要手动开始更新过程，请单击**更新模块**。

正常情况下，当正常下载更新时，如果您的模块已是最新的，将在“更新”窗口中显示消息无需进行更新 – 所安装的模块为当前版本。如果模块无法更新，建议您检查更新设置 – 此错误的最常见原因是错误地输入了许可证数据或错误地配置了连接设置。

更新窗口还包含检测引擎版本号。此数值指示将链接到显示检测引擎更新信息的 ESET 网站。

更新设置

更新设置部分可指定更新源信息，例如更新服务器和这些服务器的验证数据。 默认情况下，**更新服务器**下拉菜单设置为**自动选择**，以确保更新文件将以最小的网络流量从 ESET 服务器自动下载。

可在**更新服务器**下拉菜单中访问可用更新服务器列表。 若要添加新的更新服务器，请单击**编辑**，在**更新服务器**输入字段中输入新服务器的地址，然后单击**添加**。

ESET Endpoint Antivirus for macOS 允许您设置备用或故障转移更新服务器。 **主**服务器可以是镜像服务器，**辅助**服务器可以是标准 ESET 更新服务器。 辅助服务器必须与主服务器不同，否则将不会使用它。 如果不指定辅助更新服务器、用户名和密码，故障转移更新功能将不起作用。 还可以选择“自动选择”并在相应字段中输入用户名和密码，以使 ESET Endpoint Antivirus for macOS 自动选择要使用的最佳更新服务器。

代理模式允许您使用代理服务器更新检测模块（例如，本地 HTTP 代理）。 服务器可以与适用于需要连接的所有程序功能的全局代理服务器相同，也可以与全局代理服务器不同。 全局代理服务器设置应当已在安装期间或在代理服务器设置中进行定义。

若要将客户端配置为仅从代理服务器下载更新：

1. 从下拉菜单中选择**通过代理服务器连接**。
2. 单击**检测**以让 ESET Endpoint Antivirus for macOS 填写 IP 地址和端口号（**3128** 为默认值）。
3. 如果与代理服务器的通信需要验证，请将有效**用户名**和**密码**输入到相应字段中。

ESET Endpoint Antivirus for macOS 从 macOS 系统首选项中检测到代理设置。 这些设置均可在 macOS 的 > **系统首选项** > **网络** > **高级** > **代理**下进行配置。

如果您启用**如果 HTTP 代理不可用，请使用直接连接**，ESET Endpoint Antivirus for macOS 将自动尝试连接到更新服务器，无需使用代理。 对于使用 MacBooks 的移动用户，建议选择此选项。

如果您在尝试下载检测模块更新时遇到困难，请单击清除**更新缓存**以删除临时更新文件。

高级选项

若要在每次成功更新后禁用通知显示，请选择**不显示关于成功更新的通知**。

启用“预发布更新”以下载正在完成最终测试的开发模块。 预发布更新通常包含产品问题的修复。 延迟的更新下载将在更新发布后的几小时内进行更新，从而确保您的客户仅在更新经确认没有任何问题后才收到更新。

ESET Endpoint Antivirus for macOS 会记录检测和程序模块的快照，以用于**更新回滚**功能。 使**创建更新文件快照**保持为启用状态，以使 ESET Endpoint Antivirus for macOS 自动记录这些快照。 如果您怀疑新检测模块和/或程序模块的更新不稳定或损坏，可以使用“更新回滚”功能来回滚至以前版本，并禁用更新一段时间。 此外，您可以启用先前禁用的更新（如果曾将其无限期推迟）。 在使用“更新回滚”功能来回滚至以前的更新时，请使用“将暂停时段设置为”下拉菜单来指定您希望暂停更新的时段。 如果您选择除非手动恢复，否则直至吊销也不恢复正常更新。 设置要暂停更新的时间段时须小心。

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

如何创建更新任务

单击“更新”> **更新模块**以手动触发检测模块更新。

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

- **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，请参阅计划任务。

系统更新

macOS 系统更新功能是一个重要组件，旨在保护用户免受恶意软件侵害。为了最大程度实现安全性，我们建议您在这些更新可用时立即安装。ESET Endpoint Antivirus for macOS 会根据重要性级别通知您缺少哪些更新。通过使用**操作系统更新**旁的**显示条件**下拉菜单，您可以调整为其在**设置** > **进入应用程序首选项** > **警报和通知** > **设置**中显示通知的更新重要性级别。

- **显示所有更新** – 只要缺少系统更新，就会显示通知

- **仅显示建议的更新** – 仅收到关于建议的更新的通知

如果您不希望收到关于缺少更新的通知，请取消选中**操作系统更新**旁的复选框。

通知窗口将提供可用于 macOS 操作系统的更新概述，以及通过 macOS 本机工具更新的应用程序，即软件更新。您可以从通知窗口直接运行更新，或者可以从 ESET Endpoint Antivirus for macOS 的**主页**部分单击**安装缺少的更新**来运行更新。

通知窗口包含应用程序名称、版本、大小、属性（标记）和其他关于可用更新的信息。**标记**列包含以下信息：

- **[推荐]** – 操作系统制造商建议您安装此更新以提高系统的安全性和稳定性
- **[重新启动]** – 进行以下安装时，需要重新启动计算机
- **[关机]** – 进行以下安装时，需要关机，然后将重新开机

通知窗口将显示由称为“softwareupdate”的命令行工具检索的更新。该工具检索的更新可能不同于“软件更新”应用程序显示的更新。如果要安装“缺少的系统更新”窗口中显示的所有可用更新，以及“软件更新”应用程序未显示的更新，您必须使用“softwareupdate”命令行工具。若要了解关于此工具的详细信息，请通过在**终端**窗口中键入 `man softwareupdate` 来手动读取“softwareupdate”。此建议仅适用于高级用户。

导入和导出设置

若要导入现有配置或导出您的 ESET Endpoint Antivirus for macOS 配置，请单击**设置** > **导入和导出设置**。

如果需要备份 ESET Endpoint Antivirus for macOS 的当前配置以便在将来使用，导入和导出会很有用。导出设置对于想要在多个系统上使用其首选 ESET Endpoint Antivirus for macOS 配置的用户而言，也很便利。您可以轻松地导入配置文件来传输想要的设置。

若要导入某项配置，请选择**导入设置**，然后单击**浏览**以导航至要导入的配置文件。若要导出，请选择**导出**

设置并使用浏览器在计算机上选择要保存配置文件的位置。

代理服务器设置

可在**设置 > 进入应用程序首选项 > 代理服务器**中配置代理服务器设置。在此级别指定代理服务器定义了所有 ESET Endpoint Antivirus for macOS 功能的全局代理服务器设置。此处定义的参数将用于需要连接到 Internet 的所有模块。ESET Endpoint Antivirus for macOS 支持 Basic Access 和 NTLM (NT LAN Manager) 验证。

若要指定此级别的代理设置，请选中**使用代理服务器**，然后在**代理服务器**字段中输入您的代理服务器的 IP 地址或 URL。在“端口”字段中，指定代理服务器接受连接的端口(3128 为默认值）。还可以单击**检测**以让程序同时填写这两个字段。

如果与代理服务器的通信需要验证，请将有效的**用户名**和**密码**输入到各自的字段中。

共享的本地缓存

若要使用共享的本地缓存，请依次单击“设置”>“进入应用程序首选项”>“共享的本地缓存”，然后选中“使用 ESET 共享的本地缓存启用缓存”旁边的复选框。 通过消除网络中的重复扫描，使用此功能可在虚拟化环境中提高性能。 这可确保每个文件仅扫描一次并且存储在共享的缓存中。 启用时，有关您网络上文件和文件夹的扫描信息将保存到本地缓存。 如果您执行新扫描。ESET Endpoint Antivirus for macOS 将搜索该缓存中的已扫描文件。 如果文件匹配，将不对其进行扫描。

共享的本地缓存设置包含以下内容：

- **服务器地址** – 缓存所在的计算机的名称或 IP 地址
- **端口** – 用于通信的端口号(3537 为默认值）
- **密码** – 共享的本地缓存密码（可选）

> **详细说明**
> 有关如何安装和配置 ESET 共享的本地缓存的详细说明，请参考 ESET 共享的本地缓存用户指南。（此指南仅提供英语版本。）

最终用户许可协议

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**.**

最终用户许可协议

本最终用户使用许可协议(以下简称“协议”)由 ESET, spol. s r. o..(以下简称“ESET”或“提供商”)与作为自然人或法人的您(以下简称“您”或“最终用户”)签订。ESET 位于 Einsteinova 24, 85101 Bratislava, Slovak Republic。注册地为布拉迪斯拉发第一地区法院商业注册处，企业性质为股份有限公司，注册号 3586/B。BIN 31333532。协议授权您使用此处条款 1 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。如果您不同意本协议的任意条款和条件，请立刻单击取消选项，取消安装或下载，销毁或将本软件、安装介质、随附文档和购买发票返还至 ESET 或您购买软件的地方。

您同意使用软件表示您已经阅读本协议，您理解并同意遵守本协议的条款。

1.**软件。**本协议中的“软件”是指: (i) 本协议附带的计算机程序及其所有组成部分；(ii) 磁盘、CD-ROM、DVD、电子邮件及任何附件或附带本协议提供的其他介质的所有内容，包括数据承载工具提供、通过电子邮件提供或通过 Internet 下载的对象代码形式的软件；(iii) 任何有关本软件的书面说明材料和任何其他相关文档，包括但不限于所有软件说明、软件规格、软件特点或操作说明、使用软件的操作环境的说明、使用或安装软件的说明，或任何关于如何使用软件的说明(以下称“文档”)；(iv) 软件的副本、软件错误的修复程序、软件的附加程序、软件的扩展、软件的修改版本及软件组件更新(如果有)，关于这一点，提供商根据本协议第 3 条授予您许可。软件将仅以可执行目标代码的形式提供。

2.**安装、计算机和许可证密钥。**数据承载工具上提供、通过电子邮件发送、从 Internet 下载、从提供商服务器下载或从其他来源获得的软件需要安装。文档中指定了安装方式。任何可能对本软件有不利影响的计算机程序或硬件都不能安装在安装本软件的计算机上。计算机是指硬件，包括但不限于个人计算机、笔记本电脑、工作站、掌上电脑、智能电话、手持电子设备或本软件针对其而设计并将于其上安装和/或使用的其他电子设备。任何可能对本软件有不利影响的计算机程序或硬件都不能安装在安装本软件的计算机上。计算机是指硬件，包括但不限于个人计算机、笔记本电脑、工作站、掌上电脑、智能电话、手持电子设备或本软件针对其而设计并将于其上安装和/或使用的其他电子设备。许可证密钥是指唯一的符号、字母、数字或特殊符号的序列，提供给最终用户以允许本软件的合法使用、其特定版本或根据本协议延长许可证的期限。

3.**许可**。如果您同意本条件，同意本协议条款并且遵守此处规定的所有条款和条件，提供商将授予您以下权利（以下简称“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（以下称“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。最终用户只有在由提供商授予的许可证限制下有权使用本软件时，才有权输入软件的许可证密钥。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) **商业版。**必须获得商业版软件才能在邮件服务器、邮件中继器、邮件网关或 Internet 网关上使用软件。

d) **许可条款。**您使用软件的权利将受时间限制。

e) **OEM 软件。**OEM 软件限制为在您获得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、销毁或自行承担费用将软件及所有备份副本返还至 ESET 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软件更新（“更新”），但没有提供更新的义务。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。出于提供更新的目的，需要进行许可证真实性验证，包括有关根据“隐私政策”于其上安装本软件的计算机和/或平台的信息。

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(以下称“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以及本地网络中设备的信息(如设备的类型、供应商、型号和/或名称)(以下称“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。您特此同意接收通知和消息，包括但不限于营销信息。

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。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：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。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。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（以下简称“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（以下称为“出口管制法”），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（以下简称“制裁法”）。

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。

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。如果本协议的各语言版本之间存在差异，则以英文版本为准。本协议只能以书面形式修改，并且必须由提供商授权代表或明确授权执行此操作的人在授权委托书条款下签署此类修改。

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。

EULA ID: BUS-STANDARD-20-01

Privacy Policy

ESET, spol. s r. o.□注册办公室位于斯洛伐克共和国 Einsteinova 24, 851 01 Bratislava□在布拉迪斯拉发第一地区法院商业注册处注册，企业性质为股份有限公司，注册号为 3586/B□业务识别号：31 333 535（简称为“ESET”或“我们”□□ESET 希望在处理个人数据和客户隐私时保持透明。为了达到上述目的，我们发布了此隐私政策，唯一目的是告知我们的客户（“最终用户”或“您”）有关以下主题的信息：

- 个人数据处理、
- 数据机密性、
- 数据主体的权利。

个人数据处理

在我们的产品中实施的由 ESET 提供的服务是根据最终用户许可协议□“EULA”□提供的，但其中一些可能需要特别注意。我们希望为您提供与服务提供有关的数据收集的更多详细信息。我们提供最终用户许可协议和产品文档中所述的各种服务，例如更新/升级服务□ESET LiveGrid®□防止数据滥用、支持等。为了正常运行，我们需要收集以下信息：

- 涵盖涉及安装过程和计算机信息的更新和其他统计数据，包括产品安装所在的平台以及我们产品的操作和功能信息，例如操作系统、硬件信息、安装 ID□许可证 ID□IP 地址□MAC 地址、产品的配置设置。
- 作为 ESET LiveGrid® 信誉系统的一部分、与渗透有关的单向哈希，通过将已扫描的文件与云中白名单和黑名单项目数据库进行比较，可提高我们恶意软件防护解决方案的效率。
- 作为 ESET LiveGrid® 反馈系统的一部分、野生的可疑样本和元数据使 ESET 能够立即应对我们的最终用户的需求，以及使我们持续响应最新的威胁（如果有的话）。我们依赖您向我们发送
  - o渗透，如病毒和其他恶意程序以及可疑程序的潜在样本；有问题、潜在不受欢迎或潜在不安全的对象，如可执行文件、由您报告为垃圾邮件的电子邮件或我们的产品标记的电子邮件；
  - o关于本地网络中的设备的信息，例如设备的类型、供应商、型号和/或名称；
  - o涉及 Internet 使用的信息，例如 IP 地址和地理信息□IP 数据包□URL 和以太网帧；
  - o崩溃转储文件及包含的信息。

我们不希望收集超出此范围的数据，但有时不可避免。意外收集的数据可能包含在恶意软件本身中（在您不知情或未批准的情况下收集）或者作为文件名或 URL 的一部分包含在内，我们不打算将其构成我们系统的一部分，或为了本隐私政策中声明的目的而对其进行处理。

- 出于计费目的、许可证真实性验证以及我们服务的提供，需要提供许可信息（如许可证 ID□和个人资料（如名字、姓氏、地址、电子邮件地址）。
- 支持服务可能需要您的支持请求中包含联系信息和数据。根据您选择与我们联系的渠道，我们可能会收集您的电子邮件地址、电话号码、许可证信息、产品详细信息和支持案例的描述。可能会要求您向我们提供其他信息，以便于提供支持服务。

数据机密

ESET 是一家通过附属实体或合作伙伴（作为我们分销、服务和支持网络的一部分）在全球运营的公司。出于 EULA 的履行（例如，提供服务、支持或计费）考虑，经 ESET 处理的信息可能会在附属实体或合作伙伴之间传输。根据您的位置和选择要使用的服务，欧盟委员会可能会要求我们将您的数据传输到缺乏妥善决策的国家/地区。即使在这种情况下，每一次信息传输都会遵守数据保护法规，并且仅在需要时才会进行传输。必须毫无例外地建立标准合同条款、约束性企业规则或其他适当保护措施。

在根据最终用户许可协议提供服务的同时，我们会尽最大努力防止存储数据超过必要时间。我们的保留期可能长于许可证的有效期，只是让您有时间轻松方便地续订。出于统计目的，可能会进一步处理来自 ESET LiveGrid® 的必要和匿名统计信息和其他数据。

ESET 会实施适当技术和组织措施来确保与潜在风险相称的安全级别。我们会尽最大努力来确保提供处理系统和服务所需的持续机密性、完整性、可用性和灵活性。但当发生导致您的权利和自由遭受威胁的数据泄漏时，我们会随时通知监管机构以及数据主体。作为数据主体，您有权向监管机构提出投诉。

数据主体的权利

ESET 遵守斯洛伐克法律的规定，并且我们受欧盟的数据保护法的约束。在遵守适用数据保护法律规定条件的前提下，您作为数据主体享有以下权利：

- 有权请求访问 ESET 收集的您的个人数据，
- 有权更正可能不准确的个人数据（您也有权补充不完整的个人数据），
- 有权请求清除您的个人数据，
- 有权请求限制处理您的个人数据，
- 有权反对处理
- 还有权提出投诉
- 数据迁移。

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