

# ESET Endpoint Antivirus for macOS

## 用户指南

[单击此处显示此文档的联机版本](#)

版权所有 ©2024, 所有者 ESET, spol. s r.o.

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

有关详细信息, 请访问 <https://www.eset.com>

保留所有权利。未经作者书面许可, 不得以任何形式或任何方式 (电子、机械、影印、录制、扫描或其他方式) 复制、在检索系统中存储或传输本文档的任何部分。

ESET, spol. s r.o. 保留更改任何所述应用程序软件的权利, 恕不另行通知。

技术支持 <https://support.eset.com>

修订日期 2024年m月12日

1 ESET Endpoint Antivirus for macOS	1
2 版本 7 中的新功能	1
2.1 版本 6 与版本 7 比较	2
2.2 设置迁移	5
2.3 更改日志	6
3 系统要求	6
4 升级 ESET Endpoint Antivirus for macOS 版本 6 到版本 7	7
5 安装	9
5 载入	9
5 允许系统扩展	10
5 允许完全磁盘访问	10
5 命令行安装	11
5 安装前设置	12
5 Jamf 安装前设置	15
5 通过 ESET 管理控制台部署	17
5 在哪里可以找到许可证	18
5 本地激活	18
5 通过终端激活	18
5 远程激活	19
6 远程管理端点的文档	19
6.1 ESET PROTECT On-Prem 中的产品配置	20
6.1 检测引擎	20
6.1 文件系统实时防护	21
6.1 基于云的防护	22
6.1 恶意软件扫描	24
6.1 ThreatSense 参数	25
6.1 其他 ThreatSense 参数	27
6.1 清除级别	27
6.1 更新	27
6.1 更新镜像（自定义更新服务器）	28
6.1 网络钓鱼防护	29
6.1 Web 访问保护	30
6.1 电子邮件客户端防护	31
6.1 工具	32
6.1 代理服务器	33
6.1 日志文件	33
6.1 用户界面	34
6.2 ESET PROTECT CLOUD 介绍	35
6.3 ESET PROTECT On-Prem 介绍	35
6.4 通过 MDM 禁用通知	36
7 使用 ESET Endpoint Antivirus for macOS	37
7.1 概述	38
7.2 扫描	39
7.2 自定义扫描	41
7.3 提交样本	42
7.4 保护	42
7.4 计算机	42
7.4 Web 和电子邮件	43
7.5 更新	43
7.6 工具	44

7.6 日志文件 .....	44
7.6 隔离区 .....	45
7.7 帮助 支持 .....	46
7.7 终端实用程序和后台程序 .....	47
7.7 隔离区 .....	47
7.7 配置 .....	49
7.7 事件 .....	49
7.7 通过终端更新检测模块 .....	50
7.7 通过终端手动扫描 .....	51
8 应用程序首选项 .....	53
8.1 检测引擎 .....	54
8.1 性能排除 .....	55
8.1 检测排除 .....	55
8.1 协议排除 .....	55
8.1 基于云的扫描 .....	55
8.1 恶意软件扫描 .....	56
8.2 保护 .....	57
8.2 引擎灵敏度 .....	57
8.2 文件系统防护 .....	57
8.2 Web 访问防护 .....	58
8.2 电子邮件客户端防护 .....	58
8.2 网络钓鱼防护 .....	59
8.3 更新 .....	59
8.3 模块和产品更新 .....	59
8.4 工具 .....	60
8.4 计划任务 .....	60
8.4 日志文件 .....	60
8.4 代理服务器 .....	61
8.5 用户界面 .....	61
8.5 系统集成 .....	61
8.5 应用程序状态 .....	61
9 卸载 .....	62
10 技术支持 .....	63
11 最终用户许可协议 .....	63
12 隐私策略 .....	68

# ESET Endpoint Antivirus for macOS

ESET Endpoint Antivirus for macOS 7 代表了真正集成计算机安全的新方法。最新版本的 ThreatSense® 扫描引擎提高了速度和精确性以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 Endpoint Antivirus for macOS 7 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可主动消除病毒、间谍软件、木马、蠕虫、广告软件、Rootkit 和其他基于 Internet 攻击的渗透，而不会妨碍系统性能或中断您计算机的运行。

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 On-Prem 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 7 中的新功能

ESET Endpoint Antivirus for macOS 版本 7 是我们基于微服务而非单一服务的新一代产品。

- 本机 Apple ARM 芯片支持（从版本 7.1.1700.0 开始）
- 本机 64 位架构
- 提高了性能和稳定性。如果 ESET Endpoint Antivirus for macOS 发生崩溃，它会自动重新启动，而无需通知用户。
- 通过使进程彼此更独立，提高了安全性。
- 新的主程序窗口包括：
  - o 深色模式支持
  - o 本机桌面通知
  - o 禁用 GUI 的选项（适用于最终用户）
- 改进了文件系统实时防护
  - o 最新的本机 64 位扫描引擎
  - o 已针对多核性能进行优化
  - o 本地用户下实时扫描
- 全新的本机图形用户界面
- 通过 ESET PROTECT On-Prem 和 ESET PROTECT CLOUD 扩展了对 ESET LiveGrid 的配置
- 命令行命令与 Linux 平台的统一。
- 保护状态配置
- 支持性能和所有检测排除项（按路径、路径和检测、哈希）

## 版本 6 与版本 7 比较

功能	版本 6	版本 7.3 和 7.4
<b>建筑</b>		
建筑	单个	微服务
架构安全配置文件	主进程在 <b>root</b> 下运行 (所有重要操作均由主进程执行)	每个服务都以尽可能低的权限运行 降低可能的攻击向量 一个服务中的漏洞不会暴露整个应用程序。 崩溃或劫持一个产品进程不会禁用所有防护
架构稳定性配置文件	单个扫描程序中发生的崩溃会导致防护短暂失效 在崩溃时自动重新启动进程	非关键服务崩溃不会导致防护暂停 针对特定任务优化的更简单服务 在崩溃时自动重新启动服务
macOS 支持	10.12 (Sierra) 10.13 (High Sierra) 10.14 (Mojave) 10.15 (Catalina) 11 (Big Sur) 12 (Monterey) 13 (Ventura)	10.15 Catalina <sup>2</sup> 仅限版本 7.3) 11 (Big Sur) 12 (Monterey) 13 (Ventura) 14 (Sonoma)
本机 64 位扫描引擎	x	x
本机 64 位应用程序	x	x
多语言支持	特定语言的安装包	所有语言均在一个程序包内 <sup>2</sup> (GUI 语言与系统一样)
本机 ARM 支持		从版本 7.1.1700.0 开始
Rosetta ARM 支持	x	x
<b>文件系统防护</b>		
对潜在不受欢迎、不安全和可疑的应用程序检测	x	x
性能排除	x	x
按路径和检测排除检测	在 ESET PROTECT On-Prem 中创建检测排除 (扫描文件, 但忽略问题) 后, 它会创建性能排除 (不扫描文件)。	x
按检测排除检测		x
按精确文件 (哈希) 排除检测		x
文件系统实时防护	x	x
增加网络卷兼容性	x	不需要
在登录用户下扫描		x
扫描本地驱动器	x	x
扫描可移动磁盘	x	x

功能	版本 6	版本 7.3 和 7.4
扫描网络驱动器	x	x
打开、创建时扫描	x	x
执行时扫描	x	是，部分打开
进程排除		x
基于云的防护	x	x
ESET LiveGrid© 信誉系统	x	x (已延长)
ESET LiveGrid© 反馈系统	x	x
可发送内容的精细配置		x
恶意软件扫描（手动）	x	x
扫描符号链接	x	x
扫描电子邮件文件	x	x
扫描邮箱	x	x
扫描压缩文件	x	x
扫描自解压文件	x	x
扫描运行时加壳程序	x	x
扫描交换数据流 (ADS)	x	x
启用智能优化	x	x
从扫描中排除系统文件夹	x	不需要
以低优先级运行后台扫描		x
保存上一个访问时戳	x	x
开机扫描	x	
<b>Web 和电子邮件防护</b>		
应用程序排除	x	x
IP 地址排除	x	x
Web 访问保护（HTTP 扫描）	x	x
电子邮件客户端防护	x	x
网络钓鱼防护	x	x
<b>模块更新程序</b>		
自定义主/次更新服务器的代理服务器	x	x
模块回滚	x	x
预发布更新	x	x
延迟的更新	x	x
<b>其他主要功能</b>		
设备控制	x	
防火墙		
Web 控制		
ERMM 支持（用于远程监视和管理集成的命令行界面）	x	
ESET Enterprise Inspector 支持	x	x

功能	版本 6	版本 7.3 和 7.4
<b>其他较小功能</b>		
命令行界面	x	x(与 ESET Endpoint for Linux 统一)
检测日志	x	x
事件日志	x	x
计算机扫描日志	x	x
导入或导出设置	x	x
隔离区	x	x
本地任务计划任务	x	x
代理服务器配置	x	x
演示模式	x	x(系统本机请勿打扰)
<b>用户界面</b>		
日志文件	x	x
检测到的威胁	x	x
事件	x	x
计算机扫描	x	x
设备控制	x	
防火墙	(在 Endpoint Security 中)	
已过滤的网站	x	x
Web 控制	(在 Endpoint Security 中)	
日志过滤	x	x
防护统计	x	x
计划任务	x	x
正在运行的进程	x	
隔离区	x	x
提交文件进行分析	x	x 7.4
防护状态	x	x
手动模块更新	x	x
用户的本地设置/配置	x	x
从 GUI 导入或导出设置	x	
帮助	x	x
全新的本机图形用户界面		x
深色模式支持		x
高分辨率显示支持	x	x
可以为用户禁用 GUI		x
本机通知		x
菜单栏	x	x
可以隐藏菜单栏图标	x	x



功能	版本 6	版本 7.3 和 7.4
右键菜单集成	x	
对 GUI 中显示/报告给 ESET PROTECT On-Prem 或 ESET PROTECT CLOUD 的保护状态精细控制	x	x
系统更新通知	x	x
<b>安装</b>		
本地基于 GUI 的安装	x	x
基于组件的安装	x	
基于组件的远程安装（组件安装需要其他步骤）	x	
静默安装支持（通过 MDM 预批准）	x	x
通过重新安装更新产品	x	x
从 ESET PROTECT On-Prem 或 ESET PROTECT CLOUD 更新产品	x	x
<b>产品激活</b>		
使用许可证密钥激活	x	x
订阅许可证支持	x	x
通过 ESET PROTECT On-Prem 或 ESET PROTECT CLOUD 激活	x	x
使用脱机许可证文件激活	x	x
<b>与 ESET 管理控制台的兼容性</b>		
与 ESET PROTECT CLOUD 的兼容性	x	x
与 ESET PROTECT On-Prem 的兼容性	x	x

## 设置迁移

### 迁移过程

从 7.2 版及更高版本开始，ESET Endpoint Antivirus for macOS 版本 6 中的设置会在升级过程中自动迁移到新版本。

迁移过程完成后，ESET Endpoint Antivirus for macOS 会在主屏幕上显示设置迁移成功的通知：**您的设置已传输到新版本**。



ESET PROTECT On-Prem 和 ESET PROTECT CLOUD 中的策略不会自动迁移，因为版本 6 中存在的所有功能并非都 ESET Endpoint Antivirus for macOS 存在于版本 7 中。升级到版本 7 后，您需要查看现有策略，并根据版本 7 中提供的功能创建新策略。您可以在“策略”主题中找到有关如何创建或删除策略的详细信息：

- [ESET PROTECT On-Prem 中的策略](#)
- [ESET PROTECT CLOUD 中的策略](#)



适用于 ESET Endpoint Antivirus for macOS 版本 6 和版本 7 的 ESET PROTECT On-Prem 和 ESET PROTECT CLOUD 中的策略可以同时处于活动状态。



如果已将 ESET Endpoint Antivirus for macOS 从版本 6 升级到版本 7 或 7.1，仍可以在升级到更高版本后迁移设置。有关说明，请访问 [ESET 知识库迁移文章](#)。

版本 7.X 中可用的所有设置都会从版本 6 迁移，但以下情况除外：

- 权限设置（在版本 7 中不受支持）
- 更新的自定义代理服务器（自定义代理在版本 7 中不受支持）
- 隔离区内容
- 扫描的清除级别
- 手动扫描的目标配置文件

以下功能的设置存储在 .xml 迁移文件中；当这些功能存在于将来版本的 ESET Endpoint Antivirus for macOS 中时，可以加载这些功能：

- 设备控制
- 日志
- Web 访问防护
- 演示模式

## 其他迁移问题


- 自定义扫描配置文件已迁移，可通过 ESET PROTECT On-Prem<sup>®</sup>ESET PROTECT CLOUD 或在[应用程序首选项](#)中进行管理

# 更改日志

## 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	Intel 64-bit <sup>®</sup> Apple ARM 64 位
操作系统	macOS Big Sur (11) 至 macOS Sonoma (14)
内存	300 MB
可用磁盘空间	600 MB

 在安装期间<sup>®</sup>ESET Endpoint Antivirus for macOS 需要一个功能正常的 Internet 连接。

 ESET Endpoint Antivirus for macOS 版本 7.1.1700.0 及更高版本提供对 Apple ARM 芯片的本机支持。

## 升级 ESET Endpoint Antivirus for macOS 版本 6 到版

# 本 7

从 ESET Endpoint Antivirus for macOS 版本 6 升级到版本 7 后，ESET Endpoint Antivirus for macOS 将恢复为默认设置。这包括 ESET 管理控制台中的策略。

ESET Endpoint Antivirus for macOS 版本 7 包含与版本 6 的许多不同之处，并缺少一些功能。在决定升级 ESET Endpoint Antivirus for macOS 之前，建议您阅读[比较版本 6 与版本 7](#) 主题。

- [本地升级](#)
- [通过命令行升级](#)
- [通过 ESET 管理控制台升级](#)
- [设置迁移](#)

## 本地升级

1. [下载最新的 ESET Endpoint Antivirus for macOS 安装文件 \(.dmg\)](#)
2. 打开安装文件 (.dmg)

3. 双击安装 ESET Endpoint Antivirus for macOS 图标 

4. 如果未安装任何其他安全应用程序，则单击继续。如果已安装其他病毒防护应用程序，安装可能会失败。

5. 单击继续，以确认[系统要求](#)

6. 单击同意，以接受[最终用户许可协议](#)和[隐私政策](#)

7. 如果要更改目标文件夹或更改所有用户是否都有权访问 ESET Endpoint Antivirus for macOS，请单击更改安装位置。要开始安装，请单击安装

 [更改安装位置](#)

选择安装目标。选择是要为计算机上的所有用户还是仅为当前用户安装 ESET Endpoint Antivirus for macOS，还可以为 ESET Endpoint Antivirus for macOS 安装选择特定文件夹。选择您的选项并单击继续，以返回到安装类型步骤。

8. 在开始安装时，系统可能会提示您输入管理员密码。

9. 单击关闭以完成安装。

10. 安装后，将显示载入向导，请按照[此处](#)所述的步骤操作，以确保您的计算机受到保护。

## 通过命令行升级

要通过命令行升级 ESET Endpoint Antivirus for macOS 到版本 7，请执行以下操作：

1. 下载 ESET Endpoint Antivirus for macOS 版本 7。

2. 将 .dmg 文件分发给目标计算机。
3. 按照[命令行安装](#)主题中所述，运行安装。

## 通过 ESET PROTECT On-Prem 或 ESET PROTECT CLOUD 升级 ESET Endpoint Antivirus for macOS

在升级之前，必须在 MDM 中的配置文件中进行以下更改：

- 在全盘访问配置文件中


版本 6		版本 7	
标识符	com.eset.eea.6	标识符	com.eset.eea.g2

- 如果在 macOS 12 及更高版本上安装 ESET Endpoint Antivirus for macOS 则需要为 Uninstaller.app 添加全盘访问权限。这是从系统中删除版本 6 并允许将来远程卸载版本 7 所必需的。在全盘访问权限配置文件中，请添加：

macOS 12 Monterey 上的 ESET Endpoint Antivirus 和 ESET Endpoint Security	
标识符	com.eset.app.Uninstaller
标识符类型	bundleID
代码要求	identifier "com.eset.app.Uninstaller" 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

- 在 Web 和电子邮件防护配置文件中

版本 6		版本 7	
自定义 SSL VPN 的标识符	com.eset.sysexm.manager	自定义 SSL VPN 的标识符	com.eset.network.manager

 如果在升级到版本 7 之前删除版本 6 的设置，则用户会收到通知，就好像这些设置未应用一样。建议您为 ESET Endpoint Antivirus for macOS 版本 7 创建一个新的配置文件、将配置文件部署到目标计算机、升级您的 ESET Endpoint Antivirus for macOS 并删除版本 6 的配置文件。还建议确保一台设备上只有一个 ESET Endpoint Antivirus for macOS 的安装策略。当同时使用 ESET PROTECT On-Prem 和 Jamf 时，请确保每个产品都只有一个安装策略。

可以在[安装前设置主题](#)中，找到要下载的 ESET Endpoint Antivirus for macOS 版本 7 的新配置文件。

完成部署新配置文件后，请继续[通过 ESET 管理控制台部署主题](#)中的安装。

# 安装

## 安装方法

安装方法	安装类型	备注
<a href="#">GUI 安装</a>	本地	可以从安装 .dmg 文件在本地安装 ESET Endpoint Antivirus for macOS。在开始安装之前，请关闭所有打开的计算机程序。ESET Endpoint Antivirus for macOS 包含的组件可能会与计算机上已安装的其他病毒防护程序产生冲突。因此，强烈建议您删除所有其他病毒防护程序，以避免出现可能的问题。安装后，将显示载入向导，请按照 <a href="#">此处</a> 所述的步骤操作，以确保您的计算机受到保护。
<a href="#">命令行安装</a>	本地/远程	可以安装 ESET Endpoint Antivirus for macOS 而无需与安装程序的 GUI 交互。也可以使用此方法远程安装 ESET Endpoint Antivirus for macOS。如果要远程安装 ESET Endpoint Antivirus for macOS，建议您在安装前通过 MDM 应用用户同意设置。
ESET PROTECT On-Prem	远程	如果计算机已在 ESET PROTECT On-Prem 中进行注册，则可以创建一个安装任务以在目标计算机上安装 ESET Endpoint Antivirus for macOS。
ESET PROTECT CLOUD	远程	如果计算机已在 ESET PROTECT CLOUD 中进行注册，则可以创建一个安装任务以在目标计算机上安装 ESET Endpoint Antivirus for macOS。



ESET Endpoint Antivirus for macOS 需要用户同意设置才能运行。这些设置需要在安装后手动应用。您的设备必须在 MDM 中进行注册，才能避免将用户同意设置添加给每台计算机。然后将使用 MDM 将配置文件分发给目标计算机。如果在安装之前未应用这些设置，用户会收到多个弹出对话框，敦促他们手动应用用户同意设置。建议您在安装 ESET Endpoint Antivirus for macOS 之前分发配置文件。

## 载入

完成安装 ESET Endpoint Antivirus for macOS 后，**载入向导**即会显示一组屏幕，用于引导您完成建议步骤和强制步骤，以使 ESET Endpoint Antivirus for macOS 完全起作用。

1. 启用**建议的防护设置**、选择首选选项，然后单击**继续**。有关 **ESET LiveGrid®** 或**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](#)。
2. 强制步骤：启用 **ESET 系统扩展**。按照屏幕上的说明操作以继续设置。
3. 强制步骤：允许**代理配置**。在警报窗口中，单击**允许**。
4. 强制步骤：授予 ESET Endpoint Antivirus for macOS **完全磁盘访问权限**。按照屏幕上的说明操作，然后允许完全磁盘访问权限。
5. 接下来，该向导会提示您 **激活 ESET Endpoint Antivirus for macOS**。在[“激活”](#)章节中，可以找到多个激活选项。
6. **允许通知**。建议您允许通知，以及时了解检测到的任何系统威胁。



**正在跳过 ESET Endpoint Antivirus for macOS 载入向导。**  
通过单击**以后设置**，可以跳过强制设置；但请注意，为您提供的防护仅部分起作用。

## 正在重新启动载入向导

- i 打开 **Finder** > 应用程序 > 按住 **Control** 并单击（或右键单击）**ESET Endpoint Antivirus for macOS** 图标 > 从快捷菜单中选择**显示包内容** > 打开 **Contents** > 打开 **Helpers** > **载入**。您还可以按照[手动载入](#)一章手动设置强制安全设置。

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**扫描** > **立刻扫描**。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。

## 允许系统扩展

首次安装 ESET Endpoint Antivirus for macOS 时，必须允许 ESET Endpoint Antivirus for macOS 保护**系统扩展**和**完全磁盘访问**。

### macOS Ventura (13) 及更高版本

1. 打开**系统设置**。
2. 从左侧菜单中选择**隐私和安全**。
3. 向下滚动到**安全**部分，然后单击注意“某些系统软件需要您参与操作才能使用”下的**详细信息**按钮。

如果注意“某些系统软件需要您参与操作才能使用”和**详细信息**按钮不可用，则表示系统扩展先前已允许，无需进行下一步操作。
4. 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**。
5. 通过单击开关，启用 **ESET 文件系统实时防护**和 **ESET Web 和电子邮件防护**。
6. 单击**确定**。
7. 将显示 **ESET Web 和电子邮件防护**警报，提示您**添加代理配置**，请选择**允许**。如果在警报显示时不允许代理配置，则必须重新启动计算机以发出该警报，并可以再次允许代理配置。

### macOS Monterey (12) 及更早版本

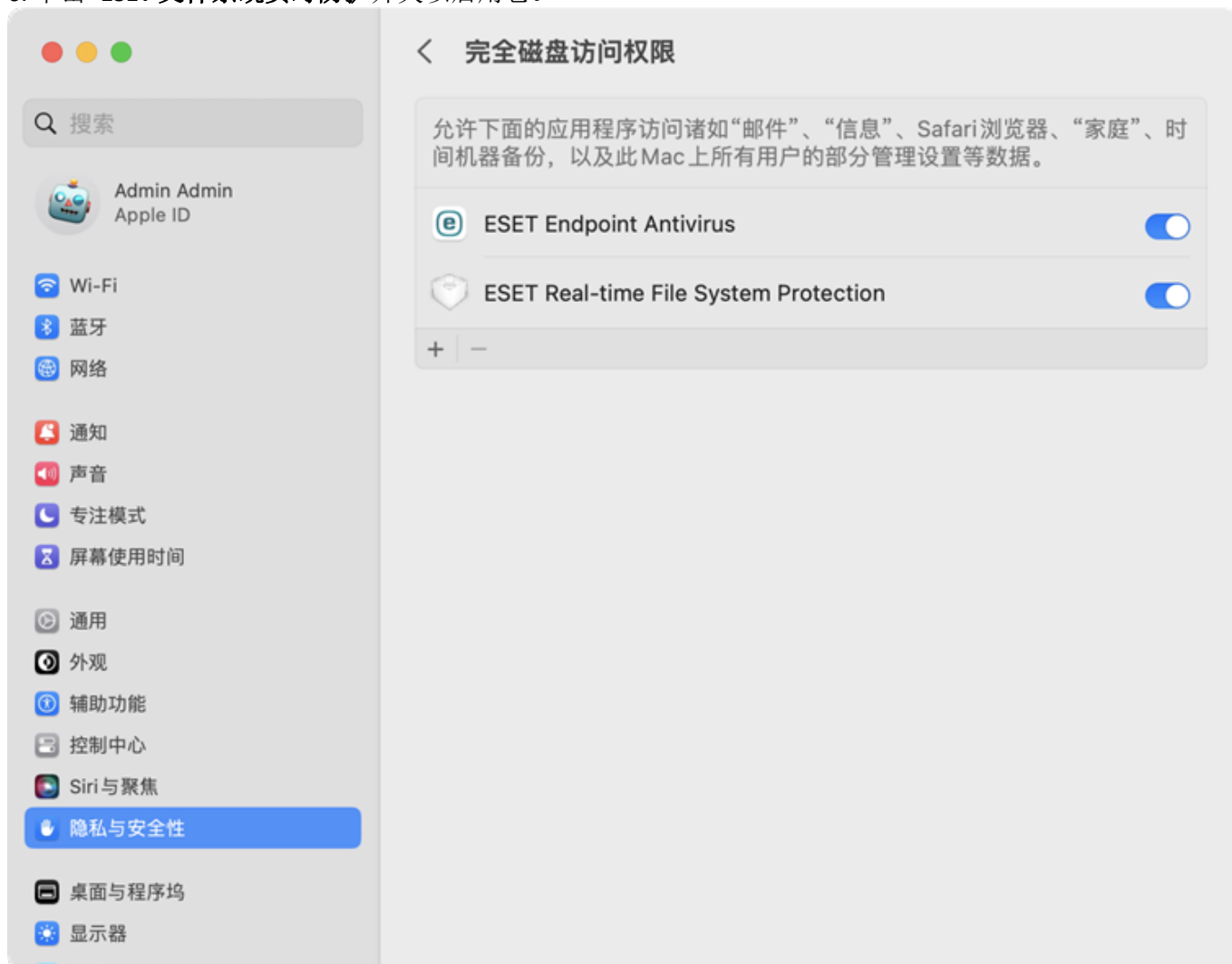
1. 打开**系统偏好设置**。
2. 选择**安全性与隐私**。
3. 单击左下角的锁定图标，以允许在该设置窗口中进行更改。
4. 使用 **Touch ID** 或单击**使用密码**并键入用户名和密码，然后单击**解锁**。
5. 单击**详细信息**。
6. 全选 **ESET Endpoint Antivirus for macOS** 选项。
7. 单击**确定**。

## 允许完全磁盘访问

首次安装 ESET Endpoint Antivirus for macOS 时，必须允许 ESET Endpoint Antivirus for macOS 保护**系统扩展**和**完全磁盘访问**。

### macOS Ventura (13) 及更高版本

1. 打开**系统设置**。
2. 从左侧菜单中选择**隐私和安全**。
3. 单击**完全磁盘访问**选项，然后单击 ESET Endpoint Antivirus for macOS 开关以启用它。
4. 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**。
5. 如果重新启动 ESET Endpoint Antivirus for macOS 提示显示，则单击**稍后**。
6. 单击 **ESET 文件系统实时防护**开关以启用它。



### [macOS Monterey \(12\) 及更早版本](#)

1. 打开**系统偏好设置**。
2. 导航到**隐私**选项卡，然后从左侧菜单中选择**完全磁盘访问权限**。
3. 单击左下角的锁定图标，以允许在该设置窗口中进行更改。
4. 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**。
5. 从列表中选择 **ESET Endpoint Antivirus for macOS**。
6. 将显示“重新启动 ESET Endpoint Antivirus for macOS”通知。单击“**稍后**”。
7. 从列表中选择 **ESET 文件系统实时防护**。

❗ 如果**文件系统实时防护**选项不可用，则必须先按照[此处](#)的步骤操作以允许系统扩展。

8. 在警报对话框窗口中单击**重新启动**以重新启动 ESET Endpoint Antivirus for macOS 来查看您的更改，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](#)。

## 命令行安装

通过命令行安装 ESET Endpoint Antivirus for macOS 来跳过 GUI 安装。如果计算机未在 MDM 中注册，则仍需要在“系统设置”中手动允许 ESET Endpoint Antivirus for macOS 的用户访问权限。



如果您使用命令行安装来远程安装 ESET Endpoint Antivirus for macOS，建议您在安装 ESET Endpoint Antivirus for macOS 之前通过 MDM 分发包含用户同意设置的配置文件。可以在[安装前设置主题](#)中找到配置文件设置。

#### 1. [下载 ESET Endpoint Antivirus for macOS](#)

2. 要装载下载的 .dmg 文件，请双击该文件或使用以下命令行过程：

a. 在终端中，导航到文件的位置。键入：`cd ~/Downloads`  
将 `Downloads` 替换为已下载文件的位置。

b. 键入：`hdiutil attach eea_osx_mlp_0.dmg`  
将 `eea_osx_mlp_0` 替换为您的文件名。

3. 在终端中，键入：`sudo installer -pkg /Volumes/ESET\ Endpoint\ Antivirus/.resources/Installer.pkg -target /`  
可能需要将 `Installer.pkg` 的路径替换为您的 `Installer.pkg` 位置。

4. 安装后，需要在[手动载入](#)中允许 ESET Endpoint Antivirus for macOS 的用户同意设置以允许全面保护。

## 远程安装

### 安装前

ESET Endpoint Antivirus for macOS 需要权限设置，以阻止该产品在设备未在 MDM 中注册的情况下远程完全安装。如果设备已注册在 MDM 中，可以使用 MDM 来通过配置文件分发这些设置。如果您的设备未在 MDM 中注册，则必须在每台计算机上手动允许这些权限设置。

如果使用的是 Jamf，还可以查看我们的 [Jamf 特定指南](#)。

## 设置 ESET Endpoint Antivirus for macOS 的配置文件

在安装 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 和电子邮件防护

要使 Web 和电子邮件防护能够正常工作，必须将 Web 和电子邮件防护配置添加到系统设置。

如果 Web 和电子邮件保护配置在安装 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 和电子邮件保护将不会起作用。

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 负载](#)。使用 .plist 负载，在 MDM 中创建配置文件。

o 使用以下设置，在 MDM 中创建配置文件：

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

## 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 ESET Endpoint Antivirus for macOS 的 .plist 负载文件](#)。使用 .plist 负载，在 MDM 中创建配置文件。

如果设备由 ESET PROTECT On-Prem 或 ESET PROTECT CLOUD 管理，则还需要为 ESET Management Agent 启用完全磁盘访问权限。[下载 ESET Management Agent 的 .plist 负载文件](#)

o 使用以下设置，创建配置文件：

ESET Endpoint Antivirus	
标识符	com.eset.eea.g2
标识符类型	bundleID
代码要求	identifier "com.eset.eea.g2" 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

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

### 在 macOS 12 Monterey 及更高版本上

标识符	com.eset.app.Uninstaller
标识符类型	bundleID
代码要求	identifier "com.eset.app.Uninstaller" 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 Management Agent

标识符	com.eset.remoteadministrator.agent
标识符类型	bundleID
代码要求	identifier "com.eset.remoteadministrator.agent" 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



在远程允许全盘访问和系统扩展后，在系统设置 > 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，而无论其在系统设置 > 安全和隐私中的状态为何。

## Web 和电子邮件防护

要远程将 Web 和电子邮件防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 负载文件](#)。使用 .plist 负载，在 MDM 中创建配置文件。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.network.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	无

卸载 ESET Endpoint Antivirus for macOS 后删除 Web 和电子邮件保护配置。如果需要卸载并安装 ESET Endpoint Antivirus for macOS 则需要在卸载后再次将 Web 和电子邮件保护配置部署到目标计算机。

## Jamf 安装前设置

在 Jamf 主窗口中，依次单击**计算机 > 配置文件**

### Web 和电子邮件防护

要使 Web 和电子邮件防护能够正常工作，必须将 Web 和电子邮件防护配置添加到系统设置。如果 Web 和电子邮件保护配置在安装 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。



Web 访问保护配置会在卸载 ESET Endpoint Antivirus for macOS 后被删除。如果需要卸载并重新安装 ESET Endpoint Antivirus for macOS 则必须将 Web 和电子邮件保护配置重新部署到目标计算机。

在**常规**部分中，请填写：

名称	例如ESET Web 和电子邮件防护
级别	计算机级别
分发方法	通常：自动安装

在 **VPN** 部分中，请填写：

VPN 类型	VPN
连接类型	自定义 SSL
标识符	com.eset.network.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	应用-代理
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
身份证书	无
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	无

---

## 启用 ESET 系统扩展

在**常规**部分中，请填写：

名称	例如 ESET SEXT
级别	计算机级别
分发方法	通常，自动安装

在**系统扩展**部分中，请填写：

显示名称	例如 ESET SEXT
系统扩展类型	允许的系统扩展
团队标识符	P8DQRXPVLP
允许的系统扩展	com.eset.endpoint com.eset.network com.eset.firewall com.eset.devices

---

## 启用全盘访问

在**常规**部分中，请填写：

名称	例如 ESET 全盘访问
级别	计算机级别
分发方法	通常，自动安装

在**隐私首选项策略控制**部分中，请填写：

标识符	com.eset.endpoint
标识符类型	捆绑包标识符
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	系统策略所有文件
访问	允许

标识符	com.eset.devices
标识符类型	捆绑包标识符
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	系统策略所有文件
访问	允许

标识符	com.eset.eea.g2
标识符类型	捆绑包标识符
代码要求	identifier "com.eset.eea.g2" 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	系统策略所有文件
访问	允许

标识符	com.eset.app.Uninstaller
标识符类型	捆绑包标识符
代码要求	identifier "com.eset.app.Uninstaller" 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	系统策略所有文件
访问	允许

⚠ 在远程允许全盘访问和系统扩展后，在系统设置 > 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，而无论其在系统设置 > 安全和隐私中的状态为何。

## 通过 ESET 管理控制台部署

⚠ ESET Endpoint Antivirus for macOS 需要权限设置，以阻止该产品在设备未在 MDM 中注册的情况下远程完全安装。如果设备已注册在 MDM 中，可以使用 MDM 来通过配置文件分发这些设置。如果您的设备未在 MDM 中注册，则必须在每台计算机上手动允许这些权限设置。

### ESET PROTECT On-Prem

在通过 ESET PROTECT On-Prem 部署 ESET Endpoint Antivirus for macOS 之前，您需要将 ESET Management Agent 分发给目标计算机。

1. 要安装 ESET Management Agent，请创建 [Agent Live 安装程序](#)。
2. 下载 macOS Agent Live 安装程序。
3. 从下载的 .tar.gz 压缩文件中提取 .sh 脚本。
4. 在目标计算机上部署并运行 .sh 脚本，以安装服务器代理。如果将 Jamf 用作 MDM，则可以[使用 Jamf 来部署和运行脚本](#)。
5. 在目标计算机上安装服务器代理后，该计算机将在 ESET PROTECT On-Prem 中可见。

要安装 ESET Endpoint Antivirus for macOS，请在 [ESET PROTECT On-Prem 中创建并运行软件安装任务](#)。

## ESET PROTECT CLOUD

可以通过创建 [Live 安装程序](#)，来同时通过 ESET PROTECT CLOUD 和 ESET Management Agent 安装 ESET Endpoint Antivirus for macOS。



如果您拥有与 ESET PROTECT On-Prem 或 ESET PROTECT CLOUD 相连的许可证，则该许可证会自动添加到安装包中，并且 ESET Endpoint Antivirus for macOS 将自动激活。

## 在哪里可以找到许可证

如果您购买了许可证，应该会收到两封从 ESET 发送的电子邮件。第一封电子邮件包含有关 ESET Business Account 门户的信息。第二封电子邮件包含有关您的许可证密钥 (XXXXXX-XXXXX-XXXXX-XXXXX-XXXXX) 公共许可证 ID (xxx-xxx-xxx) 产品名称（或产品列表）以及数量的详细信息。

## 本地激活

1. 打开 ESET Endpoint Antivirus for macOS。
2. 在“产品激活安全警报”中，单击激活对话框。



3. 在激活对话窗口打开后，键入许可证密钥并单击继续。
4. 单击完成。

## 通过终端激活

以特权用户身份使用 `/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/lic` 实用程序，以从终端窗口激活 ESET Endpoint Antivirus for macOS。

语法: /Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/lic [OPTIONS]

#### 示例

以下命令必须以特权用户身份执行。

#### 使用许可证密钥激活



```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/lic -k XXXX-XXXX-XXXX-XXXX-XXXX  
或  
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/lic --key XXXX-XXXX-XXXX-XXXX-XXXX  
其中 XXXX-XXXX-XXXX-XXXX-XXXX 代表您的 ESET Endpoint Antivirus for macOS 许可证密钥。
```

## 远程激活

如果您要通过 ESET PROTECT On-Prem 或 ESET PROTECT CLOUD 安装 ESET Endpoint Antivirus for macOS<sup>®</sup>并且您拥有与 ESET PROTECT On-Prem 或 ESET PROTECT CLOUD 相连的许可证，则该许可证会自动添加到安装包中，并且 ESET Endpoint Antivirus for macOS 将自动激活。

## 使用 ESET PROTECT On-Prem 远程激活 ESET Endpoint Antivirus for macOS

要以后通过 ESET PROTECT On-Prem 或 ESET PROTECT CLOUD 激活 ESET Endpoint Antivirus for macOS<sup>®</sup>请登录到 ESET PROTECT On-Prem Web 控制台，然后[使用产品激活客户端任务<sup>®</sup>](#)

## 远程管理端点的文档

ESET Endpoint Antivirus for macOS 版本 7 可以通过 ESET PROTECT On-Prem 或 ESET PROTECT CLOUD 进行远程管理。可以使用 ESET 远程管理工具来部署 ESET 解决方案、管理任务、强制执行安全策略、监视系统状态以及从一个中心位置快速响应远程计算机上出现的问题或威胁。

## ESET 远程管理工具

可以通过 ESET 管理控制台远程管理 ESET Endpoint Antivirus for macOS<sup>®</sup>

- [ESET PROTECT On-Prem 介绍](#)
- [ESET PROTECT CLOUD 介绍](#)

## 移动设备管理 (MDM)

要远程安装 ESET Endpoint Antivirus for macOS<sup>®</sup>必须在 MDM 中注册您的设备。如果设备未在 MDM 中进行注册，将需要物理访问每台设备才能安装 ESET Endpoint Antivirus for macOS<sup>®</sup>

移动设备管理 (MDM) 解决方案允许管理员部署组织和配置策略、监视设备、安装或卸载应用程序等操作。并非所有 MDM 解决方案都支持 Apple 设备。为了帮助您选择 MDM 解决方案<sup>®</sup>Apple 已创建一个[选择 MDM 解决方案指南](#)。

可以在 [Apple 文档](#)和您 MDM 供应商的特定文档中找到有关 MDM 的更多信息。

需要通过 MDM 完成的 ESET Endpoint Antivirus for macOS 配置包含可用于在任何 MDM 上创建配置文件的[通用可下载负载](#)。如果将 Jamf 用作 MDM<sup>®</sup>还可以使用 [Jamf 特定指南](#) <sup>®</sup>

# ESET PROTECT On-Prem 中的产品配置

要远程配置 ESET Endpoint Antivirus for macOS<sup>®</sup>

1. 在 ESET PROTECT On-Prem 中，依次单击策略 > 新策略，然后为策略键入一个名称。

**i** 要调整现有策略中 ESET Endpoint for macOS (V7+) 的设置，请单击策略列表上要更改的策略，然后依次单击编辑 > 设置<sup>®</sup>

2. 单击设置，然后从下拉菜单中选择 ESET Endpoint for macOS (V7+)<sup>®</sup>
3. 调整所需的设置。
4. 依次单击继续 > 分配，然后选择相应的计算机组。
5. 依次单击确定 > 完成<sup>®</sup>

**i** 要在本地配置 ESET Endpoint Antivirus for macOS<sup>®</sup>请参阅 [应用程序首选项<sup>®</sup>](#)

## 检测引擎

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

要远程配置 ESET Endpoint Antivirus for macOS<sup>®</sup>

1. 在 ESET PROTECT On-Prem 中，依次单击策略 > 新策略，然后为策略键入一个名称。

**i** 要调整现有策略中 ESET Endpoint for macOS (V7+) 的设置，请单击策略列表上要更改的策略，然后依次单击编辑 > 设置<sup>®</sup>

2. 单击设置，然后从下拉菜单中选择 ESET Endpoint for macOS (V7+)<sup>®</sup>
3. 调整所需的设置。
4. 依次单击继续 > 分配，然后选择相应的计算机组。
5. 依次单击确定 > 完成<sup>®</sup>

**i** 要在本地配置 ESET Endpoint Antivirus for macOS<sup>®</sup>请参阅 [应用程序首选项<sup>®</sup>](#)

在检测引擎中，可以配置以下设置：

## 基本

### 扫描程序选项

启用对潜在不受欢迎的应用程序检测 – 请参阅我们词汇表中的[潜在不受欢迎的应用程序<sup>®</sup>](#)

启用对潜在不安全的应用程序检测 – 请参阅我们词汇表中的[潜在不安全的应用程序<sup>®</sup>](#)




启用对可疑应用程序检测 – 可疑应用程序是指使用[加壳程序](#)或保护程序压缩的软件，这些加壳程序或保护程序常用于通过专有的压缩和/或加密方法阻碍反向工程或混淆可执行文件的内容（例如，隐藏恶意软件的存在）。

此类别包括：使用常用于压缩恶意软件的加壳程序或保护程序压缩的所有未知应用程序。

## 排除

性能排除 – 通过排除扫描路径（文件夹），可显著减少在文件系统中扫描来查找恶意软件所需的时间。

要创建排除，请执行以下操作：



1. 单击性能排除旁边的编辑
2. 单击添加，然后定义扫描程序要跳过的路径。（可选）为您的信息添加注释。
3. 依次单击确定 > 保存，以创建排除并关闭对话框。



## 文件系统实时防护



文件系统实时防护控制系统中所有与病毒防护相关的事件。在计算机上打开、创建或运行所有文件时，都会对它们扫描以查找恶意代码。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。

要远程配置 ESET Endpoint Antivirus for macOS

1. 在 ESET PROTECT On-Prem 中，依次单击策略 > 新策略，然后为策略键入一个名称。

 要调整现有策略中 ESET Endpoint for macOS (V7+) 的设置，请单击策略列表中要更改的策略，然后依次单击编辑 > 设置

2. 单击设置，然后从下拉菜单中选择 ESET Endpoint for macOS (V7+)
3. 调整所需的设置。
4. 依次单击继续 > 分配，然后选择相应的计算机组。
5. 依次单击确定 > 完成

 要在本地配置 ESET Endpoint Antivirus for macOS 请参阅 [应用程序首选项!\[\]\(f35e6978c00a4669a23800ac9bf47246\_img.jpg\)](#)

在检测引擎 > 文件系统实时防护中，可以配置以下设置：

## 基本

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。在特殊情况下（例如，如果与另一个实时扫描程序存在冲突），可以通过单击启用文件系统实时防护旁边的滑块来禁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 – 控制所有系统硬盘。

- 可移动磁盘 – 控制 CD/DVD 和 USB 存储和蓝牙设备等。
- 网络驱动器 – 扫描所有映射的驱动器。

ESET 建议您使用默认设置，并仅在特殊情况下（例如，当扫描某些媒体使数据传输速度显著降低时）修改默认设置。

## 扫描位置

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

- 打开文件 – 启用或禁用打开文件时的扫描。
- 创建文件 – 启用或禁用创建文件时的扫描。
- 可移动磁盘访问 – 启用或禁用连接到计算机时对可移动磁盘自动扫描。

## 进程排除

要排除扫描的进程 – 通过排除扫描进程，可显著减少在文件系统中扫描来查找恶意软件所需的时间。

要创建排除，请执行以下操作：

1. 单击要排除扫描的进程旁边的编辑。
2. 单击添加，然后定义可执行文件的路径。
3. 依次单击保存 > 保存，以创建排除并关闭对话框。

## ThreatSense 参数

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 参数](#) 部分中所述），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。

## 基于云的防护

[ESET LiveGrid®](#) 是包含多种基于云的技术的高级预警系统。它有助于根据信誉检测新出现的威胁，并利用白名单提高扫描性能。

默认情况下，ESET Endpoint Antivirus for macOS 配置为提交可疑文件给 ESET 研究实验室以供分析。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。

要远程配置 ESET Endpoint Antivirus for macOS：

1. 在 ESET PROTECT On-Prem 中，依次单击策略 > 新策略，然后为策略键入一个名称。

**i** 要调整现有策略中 ESET Endpoint for macOS (V7+) 的设置，请单击策略列表中要更改的策略，然后依次单击编辑 > 设置。

2. 单击设置，然后从下拉菜单中选择 ESET Endpoint for macOS (V7+)。

3. 调整所需的设置。
4. 依次单击继续 > 分配，然后选择相应的计算机组。
5. 依次单击确定 > 完成。

**i** 要在本地配置 ESET Endpoint Antivirus for macOS 请参阅 [应用程序首选项](#)

在检测引擎 > 基于云的防护中，可以配置以下设置：

## 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

数据将发送给 ESET 病毒实验室以供进一步分析。

提交崩溃报告和诊断数据

提交诸如崩溃报告、模块或内存转储之类的数据。

通过提交匿名使用情况统计信息来帮助改进产品

允许 ESET 收集有关新检测到的威胁的信息，例如威胁名称、检测的日期和时间、检测方法和关联的元数据、扫描的文件（哈希、文件名、文件来源、遥测数据）、阻止的和可疑 URL、产品版本和配置（包括有关您系统的信息）。

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详细信息以供分析时联系您。请注意，除非需要更多信息，否则 ESET 不会与您联系。

## 提交样本

自动提交已检测的样本

根据所选选项，这会将被感染的样本提交给 ESET 研究实验室以供分析，并改进以后的检测。

- 所有已感染的样本
- 除文档外的所有样本
- 不提交

### 自动提交可疑样本

将类似威胁的可疑样本和具有不正常特征或行为的样本提交给 ESET 研究实验室以供分析。

可执行文件 - 包括可执行文件，如 `.exe`, `.dll`, `.sys`

压缩文件 - 包括压缩文件类型: `.zip` `.rar` `.7z` `.arch` `.arj` `.bzip2` `.gzip` `.ace` `.ard` `.cab`

脚本 - 包括脚本文件类型: `.bat` `.cmd` `.hta` `.js` `.vbs` `.ps1`

其他 - 包括文件类型: `.jar` `.reg` `.msi` `.swf` `.lnk`

文档 - 包括在 Microsoft Office 或 Libre Office 或其他 Office 工具中创建的文档, 或具有活动内容的 PDF 文档。

## 排除

单击排除旁边的编辑, 以排除提交特定文件或文件夹。排除的文件不会发送给 ESET 研究实验室, 即使它们包含可疑代码也是如此。

最大样本大小(MB)

定义样本的最大大小。

## 恶意软件扫描

手动扫描程序是病毒防护解决方案的一个重要组成部分, 可用于对计算机上的文件和文件夹执行扫描。从安全角度来说, 计算机扫描应作为日常安全措施的一部分定期执行, 而不应仅在怀疑有渗透时执行, 这一点非常重要。

要远程配置 ESET Endpoint Antivirus for macOS

1. 在 ESET PROTECT On-Prem 中, 依次单击策略 > 新策略, 然后为策略键入一个名称。

**i** 要调整现有策略中 ESET Endpoint for macOS (V7+) 的设置, 请单击策略列表中要更改的策略, 然后依次单击编辑 > 设置

2. 单击设置, 然后从下拉菜单中选择 ESET Endpoint for macOS (V7+)
3. 调整所需的设置。
4. 依次单击继续 > 分配, 然后选择相应的计算机组。
5. 依次单击确定 > 完成

**i** 要在本地配置 ESET Endpoint Antivirus for macOS 请参阅 [应用程序首选项](#)

在检测引擎 > 恶意软件扫描中, 可以为手动扫描配置文件配置选项:

选定的配置文件 - 选择要编辑的配置文件。

配置文件列表 - 要创建新配置文件或删除现有配置文件, 请单击编辑。为配置文件键入一个名称, 然后单击添加。新配置文件将显示在选定的配置文件下拉菜单中, 该菜单会列出现有扫描配置文件。

ThreatSense 参数 - 扫描配置文件配置选项, 例如要控制的文件扩展名、要扫描的对象、使用的检测方法等。有关详细信息, 请参阅 [ThreatSense 参数](#)

# ThreatSense 参数

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

ThreatSense 引擎设置选项允许指定若干扫描参数：

- 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

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
- 恶意软件扫描
- Web 访问保护
- 电子邮件客户端防护

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）。

## 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。

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

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

自解压文件 – 自解压文件 (SFX) 是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（例如 UPX、yoda、ASPack、FSG 之外，扫描程序还可以通过代码仿真来识别其他几种加壳程序。

## 扫描选项

选择在扫描系统中的渗透时所用的方法。有以下选项可供使用：

启发式扫描 – 启发式扫描是一种分析（恶意）程序行为的算法。高级启发式扫描显著提高了对 ESET 产品的威胁检测能力。病毒库可以可靠地检测和识别病毒。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

ThreatSense 参数具有以下清除级别：

清除级别	说明
不清除	最终用户在清除对象时会收到一个交互式窗口，必须选择一个操作（例如，删除或忽略）。此级别专为更高级的用户设计，他们知道发生检测时应采取哪些步骤。
正常清除	清除对象时尝试清除检测，而无需任何最终用户干涉。在某些情况下（例如，包含干净文件和受感染文件的系统文件或存档），如果无法清除检测，则报告对象会在无法清除检测的情况下保留在其原始位置。
严格清除	清除对象时尝试清除检测，而无需任何最终用户干涉。在极少数情况下（例如，系统文件），报告的对象会在无法清除检测的情况下保留在其原始位置。
严格清除	在清除对象时尝试清除检测。在某些情况下，如果不能执行任何操作，则最终用户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）。大多数情况下建议使用此设置。
删除	尝试删除所有被感染文件，而无需任何最终用户干预。

## 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。

## 其他

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

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

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

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

禁用默认对象设置旁边的滑块，以配置以下选项：

最大对象大小 - 定义要扫描对象的最大大小。如果在此输入用户定义的值，时间用完后病毒防护模块将停止扫描对象，而不管扫描是否完成。此选项应仅由具有从扫描中排除大型对象的特定原因的高级用户更改。默认值：无限制




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

## 压缩文件扫描设置

禁用默认存档扫描设置旁边的滑块，以配置以下选项：

压缩文件嵌套层数 – 指定压缩文件扫描的最大深度。默认值：10

压缩文件中文件的最大大小 – 此选项允许您指定要扫描的压缩文件（当解压缩时）中所包含文件的最大文件大小。默认值：无限制

 不建议更改默认值，正常情况下应该没有修改它的理由。

## 其他 ThreatSense 参数

这些设置仅适用于[文件系统实时防护](#)

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 Endpoint Antivirus for macOS 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

## 清除级别

清除级别	说明
不清除	最终用户在清除对象时会收到一个交互式窗口，必须选择一个操作（例如，删除或忽略）。此级别专为更高级的用户设计，他们知道发生检测时应采取哪些步骤。
正常清除	清除对象时尝试清除检测，而无需任何最终用户干涉。在某些情况下（例如，包含干净文件和受感染文件的系统文件或存档），如果无法清除检测，则报告对象会在无法清除检测的情况下保留在其原始位置。
严格清除	清除对象时尝试清除检测，而无需任何最终用户干涉。在极少数情况下（例如，系统文件），报告的对象会在无法清除检测的情况下保留在其原始位置。
严格清除	在清除对象时尝试清除检测。在某些情况下，如果不能执行任何操作，则最终用户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）。大多数情况下建议使用此设置。
删除	尝试删除所有被感染文件，而无需任何最终用户干预。

## 更新

本部分指定更新源信息，例如使用的更新服务器和这些服务器的验证信息。

要远程配置 ESET Endpoint Antivirus for macOS

1. 在 ESET PROTECT On-Prem 中，依次单击策略 > 新策略，然后为策略键入一个名称。

**i** 要调整现有策略中 ESET Endpoint for macOS (V7+) 的设置，请单击策略列表中要更改的策略，然后依次单击编辑 > 设置。

2. 单击设置，然后从下拉菜单中选择 ESET Endpoint for macOS (V7+)。
3. 调整所需的设置。
4. 依次单击继续 > 分配，然后选择相应的计算机组。
5. 依次单击确定 > 完成。

**i** 要在本地配置 ESET Endpoint Antivirus for macOS，请参阅 [应用程序首选项](#)。

在更新中，可以配置以下设置：

## 基本

默认情况下，更新类型为定期更新。这可确保检测病毒库和产品模块通过 [ESET 更新服务器](#) 自动更新。

预发布更新包括即将向公众提供的最新错误修复和检测方法。但是，它们可能并非始终稳定；因此，不建议在生产环境中使用它们。

延迟更新允许延迟至少 X 小时从提供新版本病毒库的特定更新服务器进行更新（即，在真实环境中经过测试并视为稳定的数据库）。

## 模块回滚

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，可以使用 [模块更新回滚的 ESET PROTECT On-Prem 任务](#) 回滚至以前版本并暂时禁用更新。或者，如果在撤消之前已推迟先前禁用的更新，则还可以启用这些更新。

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

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

## 更新镜像（自定义更新服务器）

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

要远程配置 ESET Endpoint Antivirus for macOS：

1. 在 ESET PROTECT On-Prem 中，依次单击策略 > 新策略，然后为策略键入一个名称。

**i** 要调整现有策略中 ESET Endpoint for macOS (V7+) 的设置，请单击策略列表中要更改的策略，然后依次单击编辑 > 设置。

2. 单击设置，然后从下拉菜单中选择 ESET Endpoint for macOS (V7+)。



3. 调整所需的设置。
4. 依次单击继续 > 分配，然后选择相应的计算机组。
5. 依次单击确定 > 完成

**i** 要在本地配置 ESET Endpoint Antivirus for macOS 请参阅 [应用程序首选项](#)

在更新 > 主服务器或次服务器中，可以将 ESET Endpoint Antivirus for macOS 配置为使用更新镜像（自定义更新服务器）：

1. 在基本部分中，禁用自动选择旁边的滑块。
2. 在更新服务器字段中，以下列形式之一键入镜像服务器的 URL 地址：

http://<IP>:<port>

http://<hostname>:<port>

**i** 应使用以下服务器来安装更新：http://update.eset.com/eset\_upd/businessmac/

3. 键入合适的用户名和密码

如果您的网络中有多个可用的镜像服务器，请重复上述步骤来配置次服务器

## 网络钓鱼防护

[网络钓鱼](#)防护是另一层防护，可增强对试图获取密码和其他敏感信息的非法网站的防御。

要远程配置 ESET Endpoint Antivirus for macOS

1. 在 ESET PROTECT On-Prem 中，依次单击策略 > 新策略，然后为策略键入一个名称。

**i** 要调整现有策略中 ESET Endpoint for macOS (V7+) 的设置，请单击策略列表中要更改的策略，然后依次单击编辑 > 设置

2. 单击设置，然后从下拉菜单中选择 ESET Endpoint for macOS (V7+)
3. 调整所需的设置。
4. 依次单击继续 > 分配，然后选择相应的计算机组。
5. 依次单击确定 > 完成

**i** 要在本地配置 ESET Endpoint Antivirus for macOS 请参阅 [应用程序首选项](#)

默认情况下，网络钓鱼防护处于启用状态。要禁用网络钓鱼防护，请导航到 Web 和电子邮件 > 网络钓鱼防护，然后单击启用网络钓鱼防护旁边的滑块。

# 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。

要远程配置 ESET Endpoint Antivirus for macOS

1. 在 ESET PROTECT On-Prem 中，依次单击策略 > 新策略，然后为策略键入一个名称。

**i** 要调整现有策略中 ESET Endpoint for macOS (V7+) 的设置，请单击策略列表中要更改的策略，然后依次单击编辑 > 设置

2. 单击设置，然后从下拉菜单中选择 ESET Endpoint for macOS (V7+)
3. 调整所需的设置。
4. 依次单击继续 > 分配，然后选择相应的计算机组。
5. 依次单击确定 > 完成

**i** 要在本地配置 ESET Endpoint Antivirus for macOS 请参阅 [应用程序首选项](#)

在 Web 和电子邮件 > Web 访问保护中，可以配置以下设置：

## 基本

启用 Web 防护 – 监视 Web 浏览器和远程服务器之间的 HTTP 通信。

## Web 协议

启用 HTTP 协议检查 – 扫描任何应用程序使用的 HTTP 通信。

该程序将仅扫描在 HTTP 协议使用的端口中定义的端口上的流量。如果必要，还可以添加其他通信端口。多个端口号必须使用逗号分隔。

## URL 地址管理

URL 地址管理允许您指定要阻止、允许或排除扫描的 HTTP 地址。将无法访问阻止的地址列表中的网站。忽略发现的恶意软件地址列表中的网站无需扫描恶意代码即可访问。

要仅允许访问允许的地址列表中列出的 URL 请启用限制 URL 地址旁边的滑块。

要激活列表，请启用特定列表名称的列表活动旁边的滑块。要在输入特定列表中的地址时收到通知，请启用应用时通知旁边的滑块。

在创建地址列表时，可以使用特殊符号 \*（星号）和 ? 星号可以替代任意字符串，而问号可以替代任意符号。

指定排除的地址时应特别小心，因为该列表应仅包含受信任的安全地址。同样地，必须确保在此列表中正确使用符号 \* 和 ?。

## ThreatSense 参数

通过使用 ThreatSense 参数，可以指定 Web 访问保护的配置选项，例如要扫描的对象、使用的检测方法等。有关详细信息，请参阅 [ThreatSense 参数](#)。

# 电子邮件客户端防护

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。

要远程配置 ESET Endpoint Antivirus for macOS

1. 在 ESET PROTECT On-Prem 中，依次单击策略 > 新策略，然后为策略键入一个名称。

**i** 要调整现有策略中 ESET Endpoint for macOS (V7+) 的设置，请单击策略列表中要更改的策略，然后依次单击编辑 > 设置。

2. 单击设置，然后从下拉菜单中选择 ESET Endpoint for macOS (V7+)。
3. 调整所需的设置。
4. 依次单击继续 > 分配，然后选择相应的计算机组。
5. 依次单击确定 > 完成。

**i** 要在本地配置 ESET Endpoint Antivirus for macOS 请参阅 [应用程序首选项](#)。

在 Web 和电子邮件 > 电子邮件客户端防护中，可以配置以下设置：

## 基本

ESET Endpoint Antivirus for macOS 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。ESET 建议您将启用电子邮件防护保持处于启用状态。

## 电子邮件协议

IMAP 和 POP3 协议是最广泛地用于在电子邮件客户端应用程序中接收电子邮件通信的协议。Internet 消息访问协议 (IMAP) 是另一种用于电子邮件检索的 Internet 协议。IMAP 在某些方面优于 POP3，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。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。

ESET Endpoint Antivirus for macOS 会为这些协议提供保护，无论使用何种电子邮件客户端，也无需重新配置电子邮件客户端。该程序将仅扫描在 IMAP/POP3 协议使用的端口中定义的端口上的流量。如果必要，还可以添加其他通信端口。多个端口号必须使用逗号分隔。

## ThreatSense 参数

通过使用 ThreatSense 参数，可以指定电子邮件客户端防护的配置选项，例如要扫描的对象、使用的检测方法等。有关详细信息，请参阅 [ThreatSense 参数](#)。

## 警报和通知

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。可以选择在已接收并阅读的电子邮件上添加标记消息。请注意，在有问题的 HTML 邮件或恶意软件伪造的邮件中，可能会省略标记消息。可将标记消息添加到已接收并阅读的电子邮件中。有以下选项可供使用：

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

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

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

## 工具

要远程配置 ESET Endpoint Antivirus for macOS<sup>2</sup>

1. 在 ESET PROTECT On-Prem 中，依次单击策略 > 新策略，然后为策略键入一个名称。

**i** 要调整现有策略中 ESET Endpoint for macOS (V7+) 的设置，请单击策略列表上要更改的策略，然后依次单击编辑 > 设置<sup>2</sup>

2. 单击设置，然后从下拉菜单中选择 ESET Endpoint for macOS (V7+)<sup>2</sup>
3. 调整所需的设置。
4. 依次单击继续 > 分配，然后选择相应的计算机组。
5. 依次单击确定 > 完成<sup>2</sup>

**i** 要在本地配置 ESET Endpoint Antivirus for macOS<sup>2</sup>请参阅 [应用程序首选项<sup>2</sup>](#)

在工具中，可以配置以下设置：

## 计划任务

计划任务管理和启动已预定义配置和属性的手动扫描计划任务。

单击任务旁边的编辑，可查看所有计划任务和配置属性的列表。

要编辑现有计划任务的配置，请选择要修改的任务并单击编辑。要删除任务，请选择任务并单击删除<sup>2</sup>

要添加新任务，请执行以下操作：

1. 单击列表底部的添加<sup>2</sup>

2. 输入任务的名称，并设置任务执行的时间<sup>2</sup>
3. 选择任务将重复运行的日期。单击下一步<sup>2</sup>
4. 选择要在计划扫描中使用的扫描配置文件。要查看和编辑扫描配置文件，请参阅[恶意软件扫描](#)<sup>2</sup>
5. 定义扫描目标，选择是否要清除检测到的项目以及是否希望计划扫描也扫描在[扫描配置文件配置](#)中设置的排除。
6. 依次单击完成 > 保存<sup>2</sup>

## 代理服务器

在大型局域网网络中，代理服务器可以协调您的计算机与 Internet 之间的通信。使用此配置时需要定义以下设置。否则程序将无法自动更新。

要远程配置 ESET Endpoint Antivirus for macOS<sup>2</sup>

1. 在 ESET PROTECT On-Prem 中，依次单击策略 > 新策略，然后为策略键入一个名称。

**i** 要调整现有策略中 ESET Endpoint for macOS (V7+) 的设置，请单击策略列表中要更改的策略，然后依次单击编辑 > 设置<sup>2</sup>

2. 单击设置，然后从下拉菜单中选择 ESET Endpoint for macOS (V7+)<sup>2</sup>
3. 调整所需的设置。
4. 依次单击继续 > 分配，然后选择相应的计算机组。
5. 依次单击确定 > 完成<sup>2</sup>

**i** 要在本地配置 ESET Endpoint Antivirus for macOS<sup>2</sup>请参阅 [应用程序首选项](#)<sup>2</sup>

在工具 > 代理服务器中，可以指定代理服务器设置。需要连接到 Internet 的所有模块将使用此处定义的参数。

要配置代理服务器，请执行以下操作：

1. 启用使用代理服务器，然后在代理服务器字段中输入代理服务器的地址和代理服务器的端口号。
2. 如果与代理服务器通信需要身份验证，请启用代理服务器需要身份验证，然后在相应字段中输入有效的用户名和密码<sup>2</sup>
3. 如果代理无法访问，请启用如果代理不可用，则使用直接连接来绕过代理并与 ESET 服务器直接通信。

## 日志文件

修改 ESET Endpoint Antivirus for macOS 日志记录的配置。可以查看 [ESET PROTECT On-Prem 的日志文件](#)<sup>2</sup>

要远程配置 ESET Endpoint Antivirus for macOS<sup>2</sup>

1. 在 ESET PROTECT On-Prem 中，依次单击策略 > 新策略，然后为策略键入一个名称。

**i** 要调整现有策略中 ESET Endpoint for macOS (V7+) 的设置，请单击策略列表中要更改的策略，然后依次单击编辑 > 设置。

2. 单击设置，然后从下拉菜单中选择 ESET Endpoint for macOS (V7+)。
3. 调整所需的设置。
4. 依次单击继续 > 分配，然后选择相应的计算机组。
5. 依次单击确定 > 完成。

**i** 要在本地配置 ESET Endpoint Antivirus for macOS，请参阅 [应用程序首选项](#)。

在工具 > 日志文件中，可以配置以下设置：

日志记录的最低级别

日志记录级别定义了日志文件包含的详细信息级别。

- 严重警告 – 仅包括严重错误（例如，无法启动病毒防护）。
- 错误 – 除了严重警告，还将记录诸如“下载文件时出现错误”之类的错误。
- 警告 – 除了错误，还将记录严重错误和警告消息。
- 信息记录 – 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。
- 诊断记录 – 包括微调程序所需的信息和以上所有记录。

自动删除几天前的记录 – 将自动删除超过指定天数的日志条目。

自动优化日志文件 – 启用后，如果碎片百分比高于如果未使用的记录数超过(%) 字段中指定的值，将自动对日志文件进行碎片整理。将删除所有空白日志条目，以改善性能并提高日志处理速度。当日志包含大量条目时，可以观察到这种改进。

系统日志工具

[系统日志工具](#)是一个系统日志记录参数，用于对类似的日志消息进行分组。例如，如果配置了守护程序日志（通过系统日志工具守护程序收集日志），则可以转到 `~/log/daemon.log`。随着最近切换到systemd 及其日志，系统日志工具不再那么重要，但仍可用于过滤日志。

## 用户界面

要远程配置 ESET Endpoint Antivirus for macOS

1. 在 ESET PROTECT On-Prem 中，依次单击策略 > 新策略，然后为策略键入一个名称。

**i** 要调整现有策略中 ESET Endpoint for macOS (V7+) 的设置，请单击策略列表中要更改的策略，然后依次单击编辑 > 设置。

2. 单击设置，然后从下拉菜单中选择 ESET Endpoint for macOS (V7+)。
3. 调整所需的设置。



4. 依次单击继续 > 分配，然后选择相应的计算机组。

5. 依次单击确定 > 完成。

**i** 要在本地配置 ESET Endpoint Antivirus for macOS，请参阅 [应用程序首选项](#)。

在用户界面中，可以配置以下设置：

## 用户界面元素

允许用户打开图形用户界面 – 禁用此设置可阻止用户访问 GUI。这在托管环境或需要保留系统资源的情况下可能很有用。

在菜单栏扩展中显示图标 – 禁用此设置可从 macOS 菜单栏的菜单栏扩展（位于屏幕顶部）中删除 ESET Endpoint Antivirus for macOS 图标。

## 通知

在桌面上显示通知 – 桌面通知（例如，成功更新消息、病毒扫描任务完成或发现新威胁）由 macOS 菜单栏旁边的小弹出窗口表示。如果已启用，则 ESET Endpoint Antivirus for macOS 会在发生新事件时通知您。

## 状态

应用程序状态 – 单击编辑以配置哪些应用程序状态将在[防护状态窗口](#)中显示通知，以及哪些应用程序状态将报告给 ESET PROTECT On-Prem Web 控制台。

# ESET PROTECT CLOUD 介绍

ESET PROTECT CLOUD 让您可以在网络环境中从一个中心位置管理工作站和服务器上的 ESET 产品，而无需 ESET PROTECT On-Prem 或 ESET Security Management Center 之类的物理或虚拟服务器。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](#)

# ESET PROTECT On-Prem 介绍

ESET PROTECT On-Prem 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 On-Prem 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 On-Prem 架构和基础结构元素概述](#)、[ESET PROTECT On-Prem Web 控制台快速入门](#)和[支持的桌面设置环境](#)。

ESET PROTECT On-Prem 由以下组件组成：

- [ESET PROTECT On-Prem 服务器](#) - ESET PROTECT On-Prem 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 On-Prem Web 控制台](#) - ESET PROTECT On-Prem Web 控制台是让您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 On-Prem 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 On-Prem

- [ESET Management 服务器代理](#) - ESET Management 服务器代理有助于增强 ESET PROTECT On-Prem 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 On-Prem 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 On-Prem 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 On-Prem 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 On-Prem 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。
- [ESET Bridge](#) - 是可与 ESET PROTECT On-Prem 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 On-Prem 服务器。
- [Mobile Device Connector](#) - 是一个可用于 ESET PROTECT On-Prem 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 On-Prem 虚拟设备](#) - ESET PROTECT On-Prem VA 适用于想要在虚拟环境中运行 ESET PROTECT On-Prem 的用户。
- [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 ESET PROTECT On-Prem 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。有关使用 ESET Business Account 的更多信息，请参阅 ESET Business Account [用户指南](#)
- [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 On-Prem 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 On-Prem 联机用户指南](#)

## 通过 MDM 禁用通知

ESET Endpoint Antivirus for macOS 通知会显示在 ESET 管理控制台中。如果在 ESET 管理控制台中管理 ESET 产品，则不需要接收 ESET Endpoint Antivirus for macOS 通知。

可以通过 MDM 禁用通知。

要创建自己的配置文件，[下载 .plist 负载文件](#)



大多数 MDM 允许附加 .plist 负载或复制/粘贴配置文件中的文件内容。

## Jamf 用户

- 1. 在 Jamf 主窗口中，依次单击**计算机 > 配置文件**
- 2. 在**常规**部分中，请填写：

设置	值
名称	例如ESET 通知
级别	计算机级别
分发方法	通常，自动安装

- 3. 在**通知**部分中，单击**添加+** 并填写：

设置	值
应用程序名称	ESET Endpoint Antivirus for macOS
捆绑包标识符	com.eset.eea.agent
重要警告	禁用
通知	禁用

## 使用 ESET Endpoint Antivirus for macOS

要打开主程序窗口，请单击 macOS 菜单栏（位于屏幕顶部）中显示的 ESET Endpoint Antivirus for macOS 图标 ，然后单击显示 ESET Endpoint Antivirus for macOS

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。



在主菜单中，有以下选项可供使用：

- [概览](#)
- [扫描](#)
- [保护](#)
- [更新](#)
- [工具](#)
- [帮助 支持](#)

要修改 ESET Endpoint Antivirus for macOS 的高级设置，请通过使用 `cmd+,` 来打开**应用程序首选项**，或单击 macOS 菜单栏中的 ESET Endpoint Antivirus for macOS 并选择**首选项**（设置）。如果 ESET Endpoint Antivirus for macOS 是托管的，可以使用 [ESET PROTECT On-Prem](#) 或 [ESET PROTECT CLOUD](#) [配置 ESET Endpoint Antivirus for macOS 设置](#)。

## 概述

单击[主程序窗口中](#)的概述以查看有关计算机当前保护级别的信息。



概述窗口还会显示当前[更新](#)状态，包括上一次成功更新的日期和时间。

ESET Endpoint Antivirus for macOS 可以显示以下防护状态之一：

- 您已受保护🟢标题为绿色 - 提供最大程度的保护
- 需要注意🟡标题为橙色 - ESET Endpoint Antivirus for macOS 要求注意一个不太严重的问题
- 安全警报🔴标题为红色 - 存在严重问题，无法确保最大程度的保护

如果防护状态为需要注意或安全警报，则防护状态窗口会显示通知，其中包含其他信息和建议的解决方案。

如果无法使用建议的解决方案解决问题，可以搜索 [ESET 知识库](#)。如果仍需要帮助，可以[提交 ESET 技术支持请求](#)。

## 扫描

单击[主程序窗口](#)中的**扫描**以在计算机上执行文件和文件夹扫描。


手动扫描程序是病毒防护解决方案的一个重要组成部分，可用于对计算机上的文件和文件夹执行扫描。从安全角度来说，计算机扫描应作为日常安全措施的一部分定期执行，而不应仅在怀疑有渗透时执行，这一点非常重要。

我们建议您对系统执行定期深入扫描，以检测[文件系统实时防护](#)未捕获的病毒。在以下情形下可能会发生这种情况：威胁是在禁用文件系统实时防护时引入的、检测引擎已过时或威胁在保存到磁盘时未被检测到。



### 🔍 扫描计算机

单击立即扫描，以快速启动计算机扫描并清除被感染文件，而无需用户干预。扫描计算机的操作方便，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。

单击箭头图标  以显示**自定义扫描**和**提交样本**选项。

### 🔍 自定义扫描

单击扫描，以打开[自定义扫描窗口](#)。

自定义扫描允许您指定扫描参数，例如扫描目标、扫描配置文件、清除级别和排除。



要添加自定义扫描目标，请执行以下操作：

- 手动拖放文件或文件夹，方法是单击文件或文件夹、按下鼠标按钮的同时将鼠标指针移动到标记区域，然后释放鼠标按钮。
- 单击浏览，然后选择要扫描的文件或文件夹。

单击菜单图标 ，以显示高级扫描选项：

选择扫描配置文件 - 为自定义扫描选择扫描配置文件和[清除级别](#)<sup>②</sup>

**i** 可以使用 [ESET PROTECT On-Prem](#)<sup>②</sup>[ESET PROTECT CLOUD](#) 或在[应用程序首选项](#)中[编辑扫描配置文件](#)<sup>②</sup>

设置排除 - 添加将排除扫描的文件或文件夹。

要使用 **odscan** 实用程序通过终端运行手动扫描，请参阅[通过终端手动扫描](#)主题。

## 提交样本

此选项允许您选择在计算机上找到的可疑行为文件或在线发现的可疑站点，并将其发送到 ESET 研究实验室进行分析。

单击**发送**以指定要发送以进行分析的文件。首先，选择提交原因，然后选择文件。手动拖放文件或文件夹，方法是单击文件或文件夹、按下鼠标按钮的同时将鼠标指针移动到标记区域，然后释放鼠标按钮。有一个选项可以包含您的电子邮件，这使我们能够在需要更多信息时与您联系。如果启用**匿名提交开关**，则不必包含电子邮件。

您提交的样本必须至少满足以下条件之一：

- ESET 产品未检测到该样本。
- 将样本错误检测为威胁

单击**下一步**将转到最后一步，在该步骤中提供有关样本文件的其他信息，例如观察到的恶意软件感染的迹象或症状以及文件来源。提供更多信息将有助于我们的实验室识别和处理样本。

**i** ESET 不接受您的个人文件（您要扫描恶意软件的文件）作为样本。ESET 研究实验室不为用户执行手动扫描。

## 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、扫描配置文件、清除级别和排除。



要添加自定义扫描目标，请执行以下操作：

- 手动拖放文件或文件夹，方法是单击文件或文件夹、按下鼠标按钮的同时将鼠标指针移动到标记区域，然后释放鼠标按钮。
- 单击浏览，然后选择要扫描的文件或文件夹。


单击菜单图标 ，以显示高级扫描选项：

选择扫描配置文件 - 为自定义扫描选择扫描配置文件和[清除级别](#)

**i** 可以使用 [ESET PROTECT On-Prem](#)或[ESET PROTECT CLOUD](#) 或在[应用程序首选项](#)中[编辑扫描配置文件](#)

设置排除 - 添加将排除扫描的文件或文件夹。

# 提交样本

在主应用程序窗口中，选择左侧菜单中的**扫描**，单击箭头图标  以显示**提交样本**选项。


此选项允许您选择在计算机上找到的可疑行为文件或在线发现的可疑站点，并将其发送到 ESET 研究实验室进行分析。

单击**发送**以指定要发送以进行分析的文件。首先，选择提交原因，然后选择文件。手动拖放文件或文件夹，方法是单击文件或文件夹、按下鼠标按钮的同时将鼠标指针移动到标记区域，然后释放鼠标按钮。有一个选项可以包含您的电子邮件，这使我们能够在需要更多信息时与您联系。如果启用**匿名提交**开关，则不必包含电子邮件。

您提交的样本必须至少满足以下条件之一：

- ESET 产品未检测到该样本。
- 将样本错误检测为威胁

单击**下一步**将转到最后一步，在该步骤中提供有关样本文件的其他信息，例如观察到的恶意软件感染的迹象或症状以及文件来源。提供更多信息将有助于我们的实验室识别和处理样本。

 ESET 不接受您的个人文件（您要扫描恶意软件的文件）作为样本。ESET 研究实验室不为用户执行手动扫描。

# 保护

通过主应用程序窗口中的**保护**选项，可以调整对计算机、Web 和电子邮件的保护级别。在[计算机保护](#)和[Web 和电子邮件防护](#)部分中，包含可以启用或禁用的防护模块。强烈建议您使所有模块都保持处于启用状态，以充分利用 ESET Endpoint Antivirus for macOS 并确保计算机安全。

# 计算机

可以在**保护 > 计算机**下，找到计算机保护配置。此窗口会显示**文件系统实时防护**和 **ESET LiveGrid® 信誉系统**模块的状态。建议您使这两个模块都保持处于启用状态，关闭其中任何一个模块都可能会降低计算机的保护。



在**更新**部分中，可以单击开关来启用或禁用**自动更新**功能。当自动更新处于启用状态时，ESET Endpoint Antivirus for macOS 会自动查找最新产品更新并下载它们。

## Web 和电子邮件

要从主菜单访问 Web 和邮件防护，请依次单击**保护 > Web 和电子邮件**。要管理每个模块的更多高级设置，请通过使用 **cmd+,** 来打开**应用程序首选项**，或单击 macOS 菜单栏中的 ESET Endpoint Antivirus for macOS 并选择**首选项**（设置 Web 和电子邮件防护中提供有以下防护模块：

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

## 更新

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

定期更新 ESET Endpoint Antivirus for macOS 是确保计算机的最高安全级别的最佳方法。自动更新可确保程序模块和系统组件始终为最新。除了自动更新，还可以单击检查更新来触发手动更新。如果有可用的产品更新，则会显示有关当前版本和可用版本的信息以及更新大小和发布日期。要继续产品更新，您需要接受**最终用户许可协议**并确认**隐私政策**，可以**接受并立即更新**，也可以**接受并重新启动时更新**。要查看有关各个产品版本的更多详细信息，请单击**查看更改日志**链接。

**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。

**上次检查更新** – 显示上次成功检查更新的日期。



要修改 ESET Endpoint Antivirus for macOS 的**更新**高级设置，请通过使用 `cmd+` 来打开**应用程序首选项**，或单击 macOS 菜单栏中的 ESET Endpoint Antivirus for macOS 并选择**首选项**（设置）。如果 ESET Endpoint Antivirus for macOS 是托管的，则可以远程使用 [ESET PROTECT On-Prem](#) 或 [ESET PROTECT CLOUD](#) **配置高级更新设置**。

要通过终端使用 **upd** 实用程序更新检测模块，请参阅[通过终端更新检测模块](#)主题。

## 工具

**工具**菜单包含的模块可帮助简化程序管理并为高级用户提供更多选项。此菜单包括下列工具：

- [日志文件](#)
- [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。日志记录对于系统分析、威胁检测和故障排除至关重要。日志记录是在后台主动执行的，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 环境和存档日志查看文本消息和日志。

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**。使用窗口右上方的下拉菜单选择所需的日志类型。可用日志包括：

- **检测** – 显示与对渗透检测相关事件的所有信息
- **计算机扫描** – 所有已完成的扫描的结果显示在此日志中；双击任意条目可查看相应手动计算机扫描的详细信息
- **事件** – 此选项用于帮助系统管理员和用户解决问题。ESET Endpoint Antivirus for macOS 执行的所有重要操作都记录在事件日志中
- **阻止的文件** – 包含扫描期间根据 ESET Inspect 配置的阻止文件列表（阻止的哈希）阻止的文件的记录。
- **已过滤的网站** – 显示由“Web 访问保护”阻止的网站的列表。在这些日志中，您可以查看时间、URL、状态、IP 地址、用户和打开了到特定网站的连接的应用程序。
- **已发送的文件** – 包含发送用于分析的样本的记录。



## 隔离区

隔离区安全地存储受感染的文件。如果文件出现以下情况，则应该隔离这些文件：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。

可以在表格中查看储存在隔离区文件夹中的文件，该表格会显示隔离的日期和时间、被感染文件原始位置的路径、大小（字节数）、原因（例如，由用户添加的对象）以及威胁数量（例如，是否为包含多个渗透的压缩文件）。包含隔离文件的隔离区文件夹（`/Library/Application Support/Eset/security/cache/quarantine`）会保留在系统中，即使删除 ESET Endpoint Antivirus for macOS 也是如此。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


## 从隔离区恢复

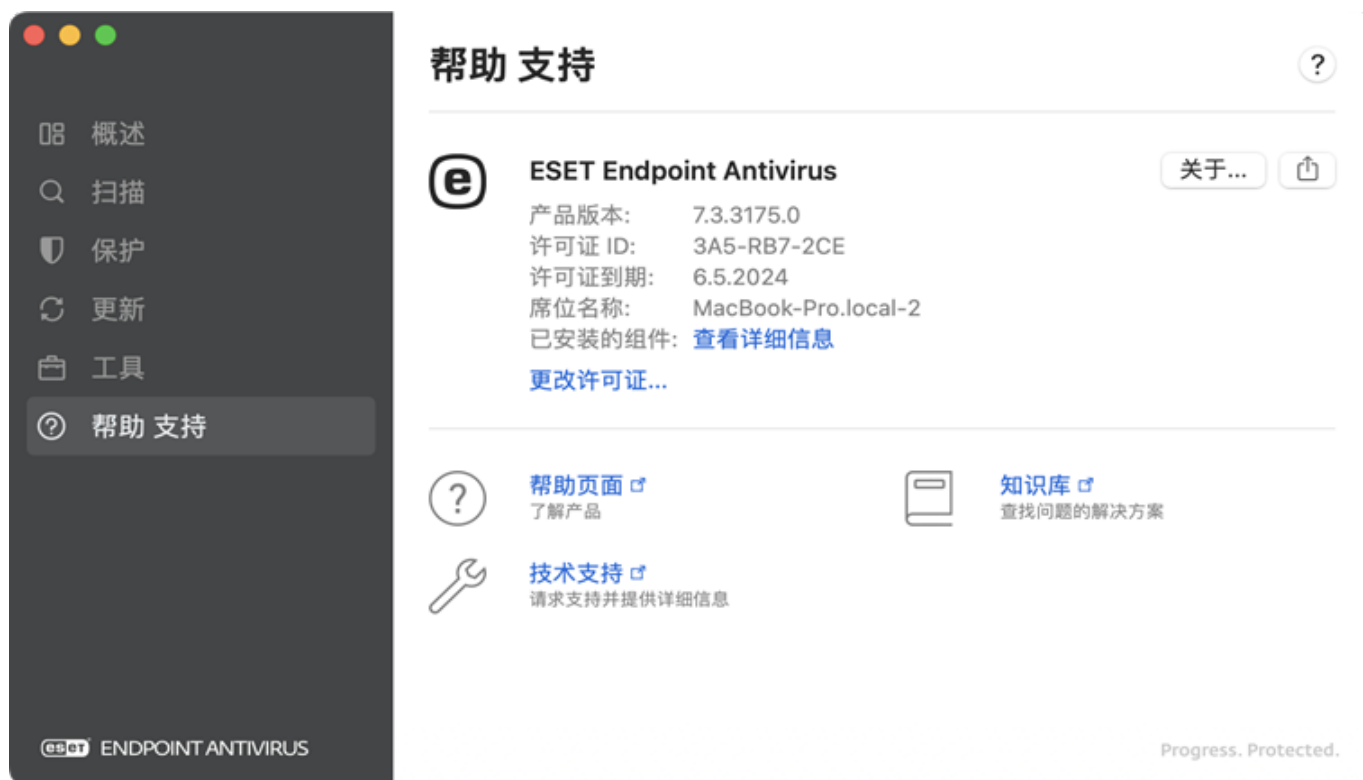
## 提交隔离区中的文件

## 帮助 支持

② **帮助页面** - 单击此链接以启动 ESET Endpoint Antivirus for macOS 帮助页面。

 **技术支持** – 如果使用帮助页面无法解决问题，请联系 [ESET 技术支持](#)。

 **知识库** – 访问 [ESET 知识库](#) 以查找常见问题的解答以及针对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。



## 终端实用程序和后台程序

### 命令行实用程序

- `./lslog` – 日志实用程序使用它来显示 ESET Endpoint Antivirus for macOS 收集的日志。
- `./odscan` – 手动扫描程序，可用于通过终端窗口运行手动扫描。
- `./cfg` – 配置实用程序，可用于导入/导出 ESET Endpoint Antivirus for macOS 设置。
- `./mdm-info` – MDM 信息实用程序，显示用于创建完成[通过 MDM 预安装设置](#)所需配置文件的必要信息。
- `./lic` – 许可实用程序，可用于使用购买的许可证密钥激活 ESET Endpoint Antivirus for macOS 或检查激活状态和许可证有效性。
- `./upd` – 模块更新实用程序，可用于管理模块更新或修改更新设置。
- `./guar` – 隔离区管理实用程序，可用于管理隔离项。

## 隔离区

隔离区安全地存储受感染的文件。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。您可以将隔离的文件提交到 ESET 病毒实验室进

行分析。

## 通过终端管理隔离项

语法: `/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar [OPTIONS]`

选项 - 短格式	选项 - 长格式	说明
-i	--import	将文件导入到隔离
-l	--list	显示隔离区中文件的列表
-r	--restore=id	将 id 标识的隔离项恢复到 --restore-path 定义的路径
-e	--restore-exclude=id	恢复 id 标识并在可排除列中标有“x”的隔离项
-d	--delete=id	删除 id 标识的隔离项
	--restore-path=path	将隔离项恢复到的新路径
-h	--help	显示帮助
-v	--version	显示版本信息并退出

i

恢复

如果命令不是以特权用户身份执行的，则恢复不可用。

## 示例

删除 id 为 “0123456789” 的隔离项：

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar -d 0123456789
```

或

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar --delete=0123456789
```

将 id 为 “9876543210” 的隔离项恢复到登录用户的 *Download* 文件夹，并将其重命名为 *restoredFile.test*：

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar -r 9876543210 --  
restore-path=/Users/$USER/Desktop/restoredFile.test
```

或

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar --  
restore=9876543210 --restore-path=/Users/$USER/Desktop/restoredFile.test
```

将 id 为 “9876543210” 的隔离项（在可排除列中标有 “x” ）恢复到 *Download* 文件夹：

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar -e 9876543210 --
```

```
restore-path=/Users/$USER/Downloads/restoredFile.test
```

或

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar --restore-exclude=9876543210 --restore-path=/Users/$USER/Downloads/restoredFile.test
```

## 通过终端从隔离区恢复文件

- 1. 列出隔离项。  
`/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar -l`
- 2. 查找要恢复的隔离对象的 ID 和名称，然后运行以下命令：  
`/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/quar --restore=ID_OF_OBJECT_TO_RESTORE --restore-`

## 配置

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/cfg --export-xml=/tmp/export.xml
```

### 导入配置

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/cfg --import-xml=/tmp/export.xml
```

### 可用选项

短格式	长格式	说明
	--import-xml	导入设置
	--export-xml	导出设置
-h	--help	显示帮助
-v	--version	显示版本信息

## 事件

在**事件**屏幕中会记录 ESET Endpoint Antivirus for macOS Web 界面中执行的重要操作、失败的 Web 界面登录尝试、通过终端执行的 ESET Endpoint Antivirus for macOS 相关命令以及一些详细信息。

每个记录的操作都包括以下信息：事件发生的时间、组件（如果可用）、事件、用户

## 通过终端显示事件

要通过终端窗口显示**事件**屏幕的内容，请使用 `lslog` 命令行工具。

```
语法：/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/lslog [OPTIONS]
```

选项 - 短格式	选项 - 长格式	说明
-f	--follow	等待新日志并将其附加到输出
-o	--optimize	优化日志。
-c	--csv	以 <b>CSV</b> 格式显示日志
-e	--events	列出事件日志
-u	--urls	列出 <b>URL</b> 日志记录
-n	--sent-files	显示提交供分析的文件列表
-s	--scans	列出手动扫描日志
	--with-log-name	另外显示日志名称列
	--ods-details=log-name	显示日志名称标识的手动扫描的详细信息
	--ods-events=log-name	打印找到的检测和文件，这些检测和文件在日志名称标识的特定手动扫描期间并未进行扫描。
	--ods-detections=log-name	显示日志名称标识的手动扫描的检测
	--ods-notscanned=log-name	显示日志名称标识的手动扫描的未扫描项
-d	--detections	列出检测日志记录
-b	--blocked files	列出阻止的文件日志

## 示例

显示所有事件日志：

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/lslog -e
```

将 CSV 格式的所有事件日志保存到当前用户的文档目录中的文件：

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/lslog -ec > /Users/$USER/Desktop/eventlogs.csv
```

## 通过终端更新检测模块

### 通过终端更新模块

要从终端窗口更新所有产品模块，请执行以下命令：

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/upd -u
```

### 通过终端更新和回滚

选项 - 短格式	选项 - 长格式	说明
-u	--update	更新模块
-c	--cancel	取消下载模块
-e	--resume	取消阻止更新



选项 - 短格式	选项 - 长格式	说明
-r	--rollback=VALUE	回滚至扫描程序模块最旧的快照并阻止 VALUE(以小时为单位)的所有更新。
-l	--list-modules	显示产品模块列表
	--check-app-update	检查存储库中新产品版本的可用性
	--download-app-update	下载新产品版本（如果可用）
	--perform-app-update	下载并安装新产品版本（如果可用）
	--accept-license	接受许可证更改



### upd 限制

upd 实用程序无法用于更改产品配置。

要停止更新 48 小时并回滚到扫描程序模块的最旧快照，请以特权用户身份执行以下命令：

```
sudo /opt/eset/efs/bin/upd --rollback=48
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/upd --rollback=48
```

要恢复扫描程序模块的自动更新，请以特权用户身份执行以下命令：

```
sudo /opt/eset/efs/bin/upd --resume
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/upd --rollback=48
```

要从镜像服务器IP地址“192.168.1.2”、端口“2221”更新，请以特权用户身份执行以下命令：

```
sudo /opt/eset/efs/bin/upd --update --server=192.168.1.2:2221
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/upd --rollback=48
```

## 通过终端手动扫描

语法：/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan [OPTIONS..]

选项 - 短格式	选项 - 长格式	说明
-l	--list	显示当前正在运行的扫描
	--list-profiles	显示所有可用的扫描配置文件
	--all	还显示其他用户执行的扫描（需要根权限）
-r	--resume=session_id	恢复 session_id 标识的先前已暂停扫描
-p	--pause=session_id	暂停 session_id 标识的扫描
-t	--stop=session_id	停止 session_id 标识的扫描
-s	--scan	启动扫描
	--show-scan-info	显示有关已启动扫描的基本信息（包括 log_name
	--profile=PROFILE	使用选定配置文件扫描
	--profile-priority=优先级	任务将以指定的优先级运行。 优先级可以是：正常、较低、最低、空闲
	--readonly	扫描但不清除
	--local	扫描本地驱动器
	--network	扫描网络驱动器
	--removable	扫描可移动磁盘
	--exclude=FILE	跳过选定的文件或目录
	--ignore-exclusions	还扫描排除的路径和扩展名

完成扫描后，该 odscan 实用程序以退出代码而结束。完成扫描后，在终端窗口中执行 `echo $?` 可显示退出代码。

退出代码

退出代码	含义
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

示例

使用“@Smart scan”扫描配置文件，以后台进程的方式对 `/root/` 目录递归运行手动扫描：

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan --scan --profile="@Smart scan" / &
```

使用“@Smart scan”扫描配置文件，对多个目标递归运行手动扫描：

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan --scan --profile="@Smart scan" /Application/ /tmp/ /home/
```

列出所有正在运行的扫描

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan -l
```

暂停会话 ID 为“15”的扫描。每个扫描都有自己启动时生成的唯一 `session-id`

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan -p 15
```

停止会话 ID 为“15”和扫描。每个扫描都有自己启动时生成的唯一 `session-id`

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan -t 15
```

对排除的目录 `/exc_dir` 和排除的文件 `/eicar.com` 运行手动扫描：

```
/Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan --scan --profile="@In-depth scan" --exclude=/exc_dir/ --exclude=/eicar.com /
```

扫描可移动设备的引导区。以特权用户身份执行以下命令。

```
sudo /Applications/ESET\ Endpoint\ Antivirus.app/Contents/MacOS/odscan --scan --  
profile="@In-depth scan" --boot-removable
```

## 应用程序首选项

要修改 ESET Endpoint Antivirus for macOS 的高级设置，请通过使用 `cmd+,` 来打开**应用程序首选项**，或单击 macOS 菜单栏中的 ESET Endpoint Antivirus for macOS 并选择**首选项**（设置）。

您可以为以下类别配置模块设置：

- [检测引擎](#)
- [保护](#)
- [更新](#)
- [工具](#)
- [用户界面](#)





## 检测引擎


检测引擎通过控制文件，来抵御恶意系统攻击。例如，如果检测到归类为恶意软件的对象，将开始清除。检测引擎可以通过先阻止它，然后清理、删除或隔离来消除它。

要修改 ESET Endpoint Antivirus for macOS **检测引擎**高级设置，请通过使用 `cmd+,` 来打开**应用程序首选项**，或单击 macOS 菜单栏中的 ESET Endpoint Antivirus for macOS 并选择**首选项**（设置）。

# 性能排除

在**性能排除**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。通过排除扫描路径（文件夹），可显著减少在文件系统中扫描来查找恶意软件所需的时间。

-  - 创建新排除；输入对象的路径。
-  - 删除选择的条目

 只有在遇到严重的实时防护问题时，才应从扫描中排除文件，因为从扫描中排除文件会降低整体防护。


# 检测排除

检测排除允许您通过过滤检测名称、对象路径或其哈希，来排除清除对象。

设置检测排除时，必须指定特定的排除标准。应提供有效的检测名称或 SHA-1 哈希。要查找有效的检测名称或 SHA-1 哈希，请参见[日志文件](#)，并从日志文件下拉菜单中选择“检测”。当在 ESET Endpoint Antivirus for macOS 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，考虑仅将受影响的文件或目录排除一段临时时间。排除也适用于可能不需要、不安全和可疑的应用程序。

提供有以下类型的排除标准：

- **确切文件** - 基于指定的 SHA-1 哈希排除某个文件，不管文件类型、位置、名称或文件扩展名如何
- **检测** - 按检测名称排除每个文件。
- **路径和检测** - 按检测名称和路径排除每个文件，包括文件名（例如，`file:///Users/documentation/Downloads/eicar_com.zip`）

 仅当检测恶意软件时遇到严重问题时，才应使用检测排除，因为从扫描中排除恶意软件会降低整体保护。

# 协议排除

排除列表中的条目会从协议内容过滤中排除。建议您仅对已知可信的应用程序或地址使用此选项。

# 基于云的扫描

## 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

数据将发送给 ESET 病毒实验室以供进一步分析。

## 提交样本

自动提交已检测的样本：根据所选选项，这会将被感染的样本提交给 ESET 研究实验室以供分析，并改进以后的检测。

- 所有已检测的样本
- 除文档外的所有样本
- 不提交

自动提交可疑样本：将类似威胁的可疑样本和具有不正常特征或行为的样本提交给 ESET 研究实验室以供分析。

- 可执行文件 – 文件类型 `.exe`、`.dll`、`.sys`
- 压缩文件 – 文件类型 `.zip`、`.rar`、`.7z`、`.arch`、`.arj`、`.bzip2`、`.gzip`、`.ace`、`.arc`、`.cab`
- 脚本 – 文件类型 `.bat`、`.cmd`、`.hta`、`.js`、`.vbs`、`.ps1`
- 文档 – 包括在 Microsoft Office、Libre Office 或其他 Office 工具中创建的文档，或具有活动内容的 PDF
- 其他 – 文件类型 `.jar`、`.reg`、`.msi`、`.swf`、`.lnk`

自动提交排除：排除的文件不会发送给 ESET 研究实验室，即使它们包含可疑代码也是如此。

## 提交崩溃报告和诊断数据

提交诸如崩溃报告、模块或内存转储之类的数据。

## 通过提交匿名使用情况统计信息来帮助改进产品



允许 ESET 收集有关新检测到的威胁的信息，例如威胁名称、检测的日期和时间、检测方法和关联的元数据、扫描的文件（哈希、文件名、文件来源、遥测数据）、阻止的和可疑 URL、产品版本和配置，包括系统信息。

## 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详细信息以供分析时联系您。除非需要更多信息，否则 ESET 不会与您联系。

## 恶意软件扫描

手动扫描程序是病毒防护解决方案的一个重要组成部分，可用于对计算机上的文件和文件夹执行扫描。从安全角度来说，计算机扫描应作为日常安全措施的一部分定期执行，而不应仅在怀疑有渗透时执行。在 **恶意软件扫描** 部分中，可以为手动扫描配置文件配置选项：

**配置文件列表** – 要创建新的配置文件列表或删除现有配置文件列表，请选择  或 。添加新配置文件列表时，请键入该配置文件的名称，然后单击“确定”。新配置文件将显示在选定的配置文件下拉菜单中，该菜单会列出现有扫描配置文件。

**ThreatSense 参数** – 扫描配置文件配置选项，例如要控制的文件扩展名、要扫描的对象、使用的检测方法

等。

## 保护

要修改 ESET Endpoint Antivirus for macOS 的**保护**高级设置，请通过使用 `cmd+` 来打开**应用程序偏好设置**，或单击 macOS 菜单栏中的 ESET Endpoint Antivirus for macOS 并选择**首选项**（设置）。

## 引擎灵敏度

引擎灵敏度使您能够为所有防护模块配置以下类别的报告和防护级别。

- **恶意软件** – 几段恶意代码，是计算机上现有文件的一部分。
- **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。但这些应用程序可能安装其他不受欢迎的软件、更改数字设备的行为，或者执行未批准的或意料之外的活动。有关这些应用程序的更多信息，请参阅[术语表](#)。
- **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，可将多种恶意软件合并到单个包中。常见的加壳程序包括 UPX、PE\_Compact、PKLite 和 ASPack。当同一个恶意软件使用不同的加壳程序进行压缩时，该恶意软件检测到的方式可能会有所不同。加壳程序还可以使其“签名”随着时间的推移而发生变异，从而更难以检测到和删除恶意软件。
- **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。该分类包括远程访问工具等程序。此选项默认情况下处于禁用状态。

## 文件系统防护

使用 ESET LiveGrid© 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。

可以将以下媒体从 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** - USB 磁盘、蓝牙设备等
- **网络媒体** - 所有映射的驱动器

默认情况下，所有文件都会在**文件打开**和**文件创建**过程中进行扫描。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。

还可以将特定进程排除扫描。

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。



# Web 访问防护

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。

可以通过定义 HTTP 通信的端口号和 URL 地址来实现 Web 过滤。

## Web 协议

在 Web 协议部分中，可以启用或禁用 HTTP 协议检查，并定义用于 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 地址管理

此部分使您能够指定要阻止、允许或排除检查的 HTTP 地址。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。

要激活允许、阻止或排除的地址列表，请选择一个列表，然后启用**列表活动**选项。如果您希望在输入来自当前列表的地址时收到通知，请选择**应用时发送通知**。

在任何列表中都可以使用特殊符号 \* (星号) 和 ? (问号)。星号可以替代任意字符串的字符，而问号可以替代任意符号。指定排除的地址时应特别小心，因为该列表应仅包含受信任的安全地址。同样地，必须确保在正确使用符号 \* 和 ?。

# 电子邮件客户端防护

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。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 协议通信扫描与使用何种电子邮件客户端无关。可用设置包括：

## 电子邮件协议

可以在此处启用/禁用对通过 POP3 和 IMAP 协议接收的电子邮件通信的检查。

### 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。无论使用哪种电子邮件客户端 ESET Endpoint Antivirus for macOS 都会为此协议提供保护。

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。确保该模块已启用，才能使协议过滤正常工作。POP3 协议检查是自动执行的，无需重新配置您的电子邮件客户端。默认情况下，将扫描端口 110 上的所有通信，但可以根据需要添加其他通信端口。端口号必须以逗号分隔。

如果启用 **POP3 协议检查** 选项，将监视所有 POP3 通信以查找是否存在恶意软件。

### IMAP 协议检查

Internet 消息访问协议 (IMAP) 是另一种用于电子邮件检索的 Internet 协议，并且比 POP3 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。无论使用哪种电子邮件客户端 ESET Endpoint Antivirus for macOS 为此协议提供保护。

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。确保 IMAP 协议检查已启用，

以便使该模块正常工作IMAP 协议控制是自动执行的，无需重新配置您的电子邮件客户端。默认情况下，将扫描端口 143 上的所有通信，但可以根据需要添加其他通信端口。端口号必须用逗号分隔。

如果已启用 **IMAP 协议检查**，将监视通过 IMAP 的所有通信，以查找是否存在恶意软件。

## 电子邮件标记

通过使用电子邮件标记，可以将标记消息附加到电子邮件脚注。扫描某个电子邮件后，可能会附加包含扫描结果的通知。标记邮件是一个有用的工具，不应该用来判定邮件安全性，因为它们可能会在有问题的 HTML 邮件中被忽略，并且可能由某些威胁伪造。有以下选项可供使用：

- o**检测发生时附加到已接收并阅读的电子邮件** - 仅将包含恶意软件的电子邮件标记为已检查。
- o**扫描时附加到所有电子邮件** - 所有已扫描的电子邮件都会附加有标记消息。
- o**从不** - 不会对任何电子邮件添加标记消息

**更新已接收电子邮件的主题** - 如果想要电子邮件防护在被感染的电子邮件中包含威胁警告，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。

**添加到检测到的电子邮件的主题** - 编辑此模板以修改被感染电子邮件的主题前缀格式。

## ThreatSense 参数

高级扫描程序设置使您能够配置清除级别、扫描选项和排除扫描的文件扩展名。

## 网络钓鱼防护

网络钓鱼防护是另一层防护，可增强对试图获取密码和其他敏感信息的非法网站的防御。默认情况下，网络钓鱼防护处于启用状态，我们建议您将其保持启用状态。

## 更新

本部分指定更新源信息，包括使用的更新服务器和这些服务器的身份验证数据。要修改 ESET Endpoint Antivirus for macOS 的**更新**高级设置，请通过使用 `cmd+` 来打开**应用程序首选项**，或单击 macOS 菜单栏中的 ESET Endpoint Antivirus for macOS 并选择**首选项**（设置）。

## 模块和产品更新

### 模块更新

#### 更新类型

- **定期更新**。这是默认的更新类型，可确保检测病毒库和产品模块通过 ESET 更新服务器自动更新。
- **预发布更新**包括即将向公众提供的最新错误修复和检测方法。但是，它们可能并不总是稳定的；因此，不建议在生产环境中使用它们。
- **延迟更新**允许延迟至少 x 小时从提供新版本病毒库的特定更新服务器进行更新（即，在真实环境中

经过测试并视为稳定的数据库）。

## 模块回滚

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。

## 创建模块快照

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

**i** 当达到最大一数（例如，三个）时，最旧的快照将每 48 小时替换为新的快照。适用于 macOS 的 ESET Endpoint Antivirus for macOS 会将检测引擎和程序模块更新版本回滚至最旧的快照。

## 产品更新

产品更新确保您始终使用最新的产品版本。启用**自动更新**开关，以便在下次重新启动时自动安装产品更新，并保持对最新功能和保护的持续访问。

## 主服务器和辅助服务器

默认情况下，自动选择主更新服务器和辅助更新服务器的选项处于启用状态。禁用自动选择切换开关时，可以指定这两个服务器。

## 工具

要修改 ESET Endpoint Antivirus for macOS **工具**高级设置，请通过使用 **cmd+,** 来打开**应用程序首选项**，或单击 macOS 菜单栏中的 ESET Endpoint Antivirus for macOS 并选择**首选项**（设置）。

## 计划任务

**计划任务**可以用来设置在指定时间自动执行的手动扫描任务。要创建新的计划任务或删除现有计划任务，请选择 **+** 或 **-**。您还可以定义应重复任务的某一天或某几天。

## 日志文件

### 日志详细级别

日志记录详细程度定义日志文件包含的详细信息级别。

- **严重警告** - 仅包含严重错误（例如：**无法启动病毒防护保护**）
- **错误** - 记录错误，例如**下载文件时出错**以及严重警告
- **警告** - 记录严重错误和警告消息。
- **信息记录** - 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。
- **诊断记录** - 包括微调程序所需的信息和以上所有记录。

## 日志文件清理

自动删除几天前的记录 - 将自动删除超过指定天数的日志条目。

## 日志文件优化

自动优化日志文件 - 启用后，如果碎片百分比高于**如果未使用的记录数超过(%)** 字段中指定的值，将自动对日志文件进行碎片整理。将删除所有空白日志条目，以改善性能并提高日志处理速度。当日志包含大量条目时，您可以看到此改进。

## 代理服务器设置

可以在此处指定代理服务器设置。定义的参数将由所有需要互联网连接的模块使用。

要配置代理服务器，请执行以下操作：

1. 启用**使用代理服务器**，然后在**代理服务器**字段中输入代理服务器的地址和代理服务器的端口号。
2. 如果代理不可用，请启用**使用直接连接**来绕过代理并与 ESET 服务器直接通信。
3. 如果与代理服务器通信需要身份验证，请启用**代理服务器需要身份验证**，然后在相应字段中输入有效的用户名和密码。

## 用户界面

要修改 ESET Endpoint Antivirus for macOS 的用户界面高级设置，请通过使用 **cmd+,** 来打开**应用程序首选项**，或单击 macOS 菜单栏中的 ESET Endpoint Antivirus for macOS 并选择**首选项**（设置）。

## 系统集成

### 用户界面元素

**允许用户打开图形用户界面** - 禁用此设置可阻止用户访问 GUI。这在托管环境或需要保留系统资源的地方可能很有用。

**在菜单栏扩展中显示图标** - 禁用此设置可从 macOS 菜单栏的菜单栏扩展（位于屏幕顶部）中删除 ESET Endpoint Antivirus for macOS 图标。

### 通知

**在桌面上显示通知** - 桌面通知（例如，成功更新、病毒扫描任务完成或发现新威胁消息）由 macOS 菜单栏旁边的警报窗口表示。如果已启用，则 ESET Endpoint Antivirus for macOS 会在发生新事件时通知您。

## 应用程序状态

在这里，您可以选择在 ESET Endpoint Antivirus for macOS 产品和 Web 控制台中显示的应用程序状态。当**显示状态**开关处于禁用状态并报告问题时，ESET Endpoint Antivirus for macOS 应用程序会保持绿色的**您已受到保护**状态。

# 卸载

## 本地卸载

无法通过将 ESET Endpoint Antivirus for macOS 图标从“应用程序”文件夹拖到垃圾桶来完全卸载 ESET Endpoint Antivirus for macOS。系统扩展将继续安装在计算机上，并且 Uninstaller.app 以后将无法删除它们。

为了阻止用户卸载 ESET Endpoint Antivirus for macOS，建议您向 ESET Endpoint Antivirus for macOS 添加一个禁止修改标记。要添加禁止修改标记，请在目标计算机上运行以下命令：



```
sudo chflags -Rf schg /Applications/ESET\ Endpoint\ Antivirus\.app
```

在卸载 ESET Endpoint Antivirus for macOS 之前，您需要先删除禁止修改标记。要删除禁止修改标记，请在目标计算机上运行以下命令：

```
sudo chflags -Rf noschg /Applications/ESET\ Endpoint\ Antivirus\.app
```

要卸载 ESET Endpoint Antivirus for macOS，请执行以下操作：



如果使用 ESET PROTECT On-Prem 或 ESET PROTECT CLOUD 管理 ESET Endpoint Antivirus for macOS，可以创建并运行一个客户端任务来远程卸载 ESET Endpoint Antivirus for macOS。

- 在 [ESET PROTECT On-Prem 中创建并运行软件安装任务](#)
- 在 [ESET PROTECT CLOUD 中创建并运行软件安装任务](#)

1. 启动 ESET Endpoint Antivirus for macOS 卸载程序。有多种方法可用于启动 ESET Endpoint Antivirus for macOS 卸载程序：

- 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 Applications 文件夹，按住 Control 键并单击（或右键单击）ESET Endpoint Antivirus for macOS 图标 > 从快捷菜单中选择显示包内容。打开 Contents > Helpers 文件夹，然后双击 Uninstaller 图标。

2. 单击**卸载**以开始卸载过程。系统会提示您键入管理员密码。



如果在删除系统扩展时出现问题，系统可能会在卸载过程中提示您键入管理员密码。

3. 如果要卸载 macOS 12 Monterey 上的 ESET Endpoint Antivirus for macOS，系统会提示您允许 Uninstaller.app 以管理由 ESET Endpoint Antivirus for macOS 创建的用户。将显示以下对话框：“Uninstaller.app”想要管理您的电脑。管理可能包括修改密码、联网设置和系统设置。单击确定。如果单击不允许，ESET Endpoint Antivirus for macOS 将不会完全卸载。

4. 单击关闭以退出卸载程序。

5. 重新启动计算机。

## 通过命令行卸载

可以通过从终端运行卸载脚本来卸载 ESET Endpoint Antivirus for macOS。如果已安装 ESET Endpoint Antivirus for macOS 到默认位置，请运行以下命令：

```
sudo /Applications/ESET\ Endpoint\
```

## 技术支持

### 联系技术支持

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。

### 获取技术支持信息

为了确保能够快速成功地解决您的问题，建议您在创建支持票据时执行以下操作：

- 包括许可证详细信息、产品名称、产品版本和操作系统等信息。
- 详细描述您的问题。
- 附加您问题的屏幕截图或视频。
- 附加 ESET LogCollector 中的日志。

### ESET LogCollector

ESET LogCollector 会创建包含重要信息的日志，可帮助支持人员和开发人员识别您使用 ESET Endpoint Antivirus for macOS 时遇到的问题。

可以在 [ESET 知识库文章](#) 中查找有关 ESET LogCollector 的更详细信息。该文章可能不会提供所有语言版本。

要使用 ESET LogCollector 创建日志，请执行以下操作：

1. 下载 [ESET LogCollector](#)
2. 打开 **eset\_logcollector.dmg** 文件，然后运行 LogCollector 应用程序。
3. 按照屏幕上的说明操作以创建日志。

#### 使用 ESET LogCollector 的提示

- ! 要为 ESET 支持创建更多详细日志，请在**复制**部分中，单击齿轮图标以打开高级选项。
- 在准备好重新创建问题以及引导您遇到它的步骤之前，请勿启动复制。

在创建日志文件后，可以在桌面上找到名为 **customer\_info.zip** 的日志文件。将此文件附加到您的支持请求中。

## 最终用户许可协议

自 2021 年 10 月 19 日起生效。

**重要说明:**在下载、安装、复制或使用前，请仔细阅读产品应用程序的以下条款。**下载、安装、复制或使**  
**用本软件即表示您同意这些条款和条件并承认隐私政策** [隐私政策](#)

最终用户许可协议



本最终用户使用许可协议(“协议”)由 ESET, spol. s r. o. (“ESET”或“提供商”)与作为自然人或法人的您(“您”或“最终用户”)签订。ESET 位于 Einsteinova 24, 85101 Bratislava, Slovak Republic。注册地为布拉迪斯拉发第一地区法院商业注册处, 企业性质为股份有限公司, 注册号 3586/B。BIN 31333532。协议授权您使用此处第 1 条中定义的软件。此处条款 1 中定义的软件可能存储在数据承载工具上、通过电子邮件发送、从 Internet 下载、从提供商的服务器下载或者按照以下指定的条款从其他来源获得。

这不是购买合同, 而是关于最终用户权利的协议。无论是此软件的副本, 还是经过商业包装的包含此软件的物理介质, 亦或根据本协议最终用户有权使用的任何其他副本, 所有权均归提供商所有。

在安装、下载、复制或使用软件过程中单击“我接受”或“我接受...”, 即表示您同意本协议的条款和条件并确认隐私政策。如果您不同意本协议的任意条款及条件和/或隐私政策, 请立刻单击取消选项、取消安装或下载、销毁或退还本软件、安装介质、随附文档和购买发票给提供商或您从中获取软件的渠道。

您同意使用软件表示您已经阅读本协议, 您理解并同意遵守本协议的条款。

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

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

**3. 许可。**如果您同意本条件, 同意本协议条款并且遵守此处规定的所有条款, 提供商将授予您以下权利(“许可”):

**a) 安装和使用。**您将具有在计算机硬盘或其他永久介质中安装软件以进行数据存储, 在计算机系统内存中安装和存储软件, 实施、存储和显示软件的非独占、不可转让的权利。

**b) 许可数量规定。**软件的使用权利受最终用户数量约束。一位最终用户指: (i) 在一个计算机系统上安装软件; 或 (ii) 如果许可约束范围为邮箱数量, 则单个用户指的是通过邮件用户代理“MUA”接收电子邮件的计算机用户。如果 MUA 接受电子邮件, 然后将其自动分发到多个用户, 则最终用户数量应根据收到电子邮件的实际用户数量确定。如果邮件服务器执行邮件网关的功能, 则最终用户数量应等于上述网关所服务的邮件服务器用户数量。如果未指定数量的电子邮件地址(例如通过别名)指向一个用户, 用户接受这些地址, 并且客户端不自动将邮件分发给大量用户, 则需要一台计算机的许可证。您不得同时在多台计算机上使用同一许可。仅当最终用户根据限制(因提供商授予的许可证数量而引起)而有权使用本软件时, 最终用户才有权输入本软件的许可证密钥。许可证密钥被视为保密信息, 除非本协议或提供商允许, 否则您不得与第三方共享许可证或允许第三方使用许可证密钥。如果您的许可证密钥被盗用, 请立即通知提供商。

**c) 家庭版/商业版。**本软件的家庭版应仅在私人 and/或非商业环境中专供家庭和家人使用。必须获得本软件的商业版, 才能在商业环境中使用, 以及将本软件用于邮件服务器、邮件中继、邮件网关或 Internet 网关。

**d) 许可条款。**您使用软件的权利将受时间限制。

**e) OEM 软件。**分类为“OEM”的软件应限于在您获得该软件的计算机上使用。不得转移到其他计算机。



**f) NFR®试用软件。**分类为“非转售性”NFR 或试用的软件不得用于付费用途，只能用于演示或测试软件功能。

**g) 许可终止。**许可将在授予的期限结束时自动终止。如果不遵守本协议的任何条款，提供商有权撤销协议，不影响提供商在此类不测事件下的任何权利或合法补救措施。如果取消许可，您必须立刻删除、销毁本软件及所有备份副本，或自行承担费用将软件及所有备份副本返还至 ESET 或您购买软件的地方。在许可终止后，提供商有权取消最终用户使用本软件功能（这些功能需要连接到提供商的服务器或第三方服务器）的权利。

**4. 具有数据收集和 Internet 连接要求的功能。**要正确操作本软件，需要连接到 Internet®并且必须定期连接到提供商服务器或第三方服务器和遵循“隐私政策”的适用的数据收集。以下软件功能要求必须连接到 Internet 和适用的数据收集：

**a) 软件更新。**提供商有权时常发布本软件的更新或升级（即“更新”），但没有义务提供更新。此功能在软件标准设置下启用，因此自动安装更新，除非最终用户禁用自动安装更新。为了提供更新，需要进行许可证真实性验证，包括根据“隐私政策”获取其上安装本软件的计算机和/或平台的相关信息。

任何更新的提供可能都要遵循生命周期结束政策（即“EOL 政策”），可通过访问 [https://go.eset.com/eol\\_business](https://go.eset.com/eol_business) 了解该政策。在本软件或其任何功能达到 EOL 政策中定义的生命周期结束日期后，将不会提供任何更新。

**b) 将渗透和信息发送给提供商。**本软件包含多项功能，这些功能用于收集计算机病毒和其他恶意计算机程序与可疑对象、问题对象、潜在不受欢迎对象或潜在不安全对象（例如文件 URL IP 数据包和以太网帧）的样本（“渗透”）并将其发送给提供商，包括但不限于安装过程、安装本软件的计算机和/或平台的信息，本软件的操作和功能信息（“信息”）。这些信息和渗透可能包含已安装本软件的计算机上的最终用户或其他用户的数据（包括随机或意外获得的个人数据），以及受附带相关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(ii) 反映对本软件或 ESET 开展业务方式的更改(ii) 出于法律、法规或安全原因，或(iii) 防止滥用或损害。将通过电子邮件、应用内通知或其他电子方式通知您本协议的任何修订。如果您不同意对本协议的拟议变更，可以在收到变更通知后的 30 内，根据第 10 条终止履行本协议。除非您在该时限内终止履行本协议，否则拟议变更将视为被接受，并自您收到变更通知之日起开始对您生效。

您与提供商签署的本协议是关于本软件的唯一完整协议，它完全取代任何之前的关于软件的表述、讨论、承诺、沟通或广告。

EULAID: EULA-PRODUCT-LG-MAC; 3537.0

## 隐私策略

ESET, spol. s r. o.注册办公室位于斯洛伐克共和国 Einsteinova 24, 851 01 Bratislava在布拉迪斯拉发第一地区法院商业注册处注册，企业性质为股份有限公司，注册号为 3586/B业务识别号：31333532（简称为“ESET”或“我们”）ESET 希望在处理个人数据和客户隐私时保持透明。为了达到上述目的，我们发布了此隐私政策，唯一目的是告知我们的客户（“最终用户”或“您”）有关以下主题的信息：

- 个人数据处理、
- 数据机密性、
- 数据主体的权利。

## 个人数据处理

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

- 涵盖涉及安装过程和计算机信息的更新和其他统计数据，包括产品安装所在的平台以及我们产品的操作和功能信息，例如操作系统、硬件信息、安装 ID许可证 IDIP 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；
- 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；
- 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。

- 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。根据您的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 and 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露时，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