kaspersky

Kaspersky Endpoint Security for Mac

© 2026 AO Kaspersky Lab

目录

Kaspersky Endpoint Security 概述
此版本中的新功能
Kaspersky Endpoint Security 功能比较（取决于 Kaspersky Security Center 管理工具）
安装和卸载应用程序
- 分发包
- 硬件和软件要求
- 准备安装
- 安装 Kaspersky Endpoint Security
- 准备使用应用程序
- 卸载 Kaspersky Endpoint Security

首次启动应用程序
Kaspersky Endpoint Security 应用程序界面
- 主应用程序窗口
- Kaspersky Endpoint Security 图标
- 应用程序设置窗口

关于通知
Kaspersky Endpoint Security 应用程序授权许可
- 关于最终用户授权许可协议
- 关于授权许可
- 关于订阅
- 关于授权许可证书
- 关于密钥
- 关于激活码
- 关于密钥文件
- 关于数据提供
- 激活 Kaspersky Endpoint Security
- 查看授权许可信息
- 管理授权许可和订阅
- 根据工作站授权许可类型比较应用程序功能

执行常规任务
- 打开和退出应用程序
- 查看计算机保护的状态
- 查看已安装组件的运行状态
- 禁用和恢复计算机保护
- 使用保护中心
- 执行扫描任务
- 配置自动启动计划扫描任务
- 更新应用程序数据库
- 文件访问被阻止时如何应对
- 恢复已被应用程序删除或清除的文件
- 查看应用程序运行报告
- 出现通知窗口时如何应对

应用程序高级配置
- 计算机保护范围
- 文件威胁防护
- Web 威胁防护
- 邮件威胁防护
- 反网络攻击
- 防火墙
- 行为检测
- 扫描
- 更新任务
- 本地任务
  - 外部磁盘扫描任务
- 备份
- 报告
- Managed Detection and Response
- Endpoint Detection and Response Expert (on-premise)
- Endpoint Detection and Response Optimum
  - 与 Endpoint Detection and Response Optimum 整合
  - 扫描入侵指标
  - 将文件移至隔离区
  - 获取文件
  - 删除文件
  - 启动进程
  - 终止进程
  - 执行防护
  - 计算机网络隔离
  - Cloud Sandbox
- 文件保险箱磁盘加密
- 密码保护
- 漏洞利用防御
- 修复引擎
- Web 控制
- 设备控制

加入卡巴斯基安全网络
检查应用程序组件的完整性
通过 Kaspersky Security Center 管理控制台管理应用程序
- 在企业网络上部署 Kaspersky Endpoint Security
- 将 Kaspersky Endpoint Security 版本 11.1 或更高版本更新到版本 12.2.1
- 准备远程安装 Kaspersky Endpoint Security
  - 安装 Kaspersky Endpoint Security 管理插件
  - 本地安装网络代理
  - 使用 Apple 远程桌面安装网络代理
  - 使用 Kaspersky Security Center 安装网络代理
  - 使用 SSH 协议安装网络代理
  - 本地卸载网络代理

从命令行管理网络代理
在远程计算机上启动/停止网络代理
手动检查客户端计算机与管理服务器之间的连接。Klnagchk 实用程序
将远程计算机手动连接到管理服务器。Klmover 实用程序
卸载网络代理
安装和卸载 Kaspersky Endpoint Security
使用 SSH 协议安装应用程序
使用 Kaspersky Security Center 安装应用程序
创建安装包
使用 Kaspersky Security Center 卸载应用程序
通过 Kaspersky Security Center 启动和停止应用程序
创建和管理任务
创建任务
手动启动和停止任务
导入和导出任务
查看任务
管理任务特定设置
创建和管理策略
创建策略
查看策略列表
配置策略设置
更改策略状态
将策略导出到 KLP 文件
从 KLP 文件导入策略
创建和管理策略配置文件
生成检测到的对象报告
获取加密驱动器的恢复密钥
通过 Kaspersky Security Center Web Console 和云控制台远程管理应用程序
安装 Kaspersky Endpoint Security Web 插件
创建策略
主机威胁防护
配置文件威胁防护组件
配置可移动驱动器扫描
配置行为检测
配置反加密勒索
配置漏洞利用防御组件
配置修复引擎组件
通信和 Web 保护
配置邮件威胁防护
配置 Web 威胁防护组件
配置网络威胁防护
配置防火墙组件
安全控制
配置设备控制组件
配置 Web 控件组件
数据加密

- 常规设置
  - 检测设置
  - 卡巴斯基安全网络
  - 用户交互
  - 自我保护
  - 性能
  - 报告和存储
  - 网络设置
  - 遥测设置
  - 事件设置
  - 更新设置
- 内置代理
  - 配置 Managed Detection and Response
  - 配置 Endpoint Detection and Response
  - 配置 Endpoint Detection and Response Expert (on-premise)
- 创建任务
  - 配置“扫描”任务设置
  - 配置“添加密钥”任务设置
  - 配置“更新”任务
- 获取加密驱动器的恢复密钥

从命令行管理应用程序

- 查看命令行帮助
- 运行恶意软件扫描
- 更新应用程序
- 回滚到上次更新
- 启动/停止组件或任务
- 查看组件或任务的状态和统计信息
- 导出保护设置
- 激活应用程序
- 安装系统功能扩展
- 配置网络连接
- 删除授权许可密钥
- 命令行返回代码
- 退出应用程序
- 卸载应用程序
- Detection and Response 管理命令
  - 管理执行防护
  - 管理网络隔离

联系技术支持

- 如何获得技术支持
- 通过 Kaspersky CompanyAccount 获取技术支持
- 为技术支持部门获取信息
- 使用追踪文件
- 创建追踪文件

有关应用程序的信息来源

附录
已知问题和限制
已修复的问题
按扩展名扫描的对象列表
文件和文件夹路径中的掩码
IOC 文件要求
支持的用于执行防护的脚本解释器
如何将 Kaspersky Endpoint Security 证书添加到 Mozilla Firefox 证书存储
与外部服务交互的网络设置
有关第三方代码的信息
商标声明

Kaspersky Endpoint Security 概述

Kaspersky Endpoint Security 应用程序可保护运行 macOS 的计算机免遭恶意软件和其他计算机安全威胁的侵害。

文件威胁防护

文件威胁防护通过拦截和分析任何文件访问尝试来实时保护计算机的文件系统。了解更多。

Web 威胁防护

Web 威胁防护可以保护计算机使用 Safari、Google Chrome™ 和 Firefox™ 通过 HTTP 和 HTTPS 协议发送和接收的信息。了解更多。

邮件威胁防护

“邮件威胁防护”会扫描传入和传出电子邮件的附件是否有恶意软件和其他威胁。该组件借助反恶意软件数据库、卡巴斯基安全网络云服务和启发式分析来提供计算机保护。了解更多。

反网络攻击

网络威胁防护可防止入侵操作系统。此组件可防范网络攻击者（使用端口扫描和暴力破解的攻击者）和网络攻击者安装的恶意软件（包括试图向犯罪分子发送个人数据的恶意软件）。了解更多。

防火墙

防火墙在互联网或本地网络上工作时阻止对计算机的未经授权的连接。这使您可以保护企业局域网免受身份盗窃和其他攻击。该组件借助反恶意软件数据库、卡巴斯基安全网络云服务和预定义网络规则来提供计算机保护。了解更多。

行为检测

行为检测组件接收有关计算机上应用程序操作的信息，并将其提供给其他保护组件以提高其性能。它还会执行所选的操作来响应恶意软件活动。了解更多。

漏洞利用防御

漏洞利用防御组件会检测利用计算机漏洞来获取管理员权限或执行恶意活动的程序代码。了解更多。

修复引擎

修复引擎让 Kaspersky Endpoint Security 回滚操作系统中恶意软件执行的操作。了解更多。

扫描

Kaspersky Endpoint Security 应用程序可以按需检测并清除指定扫描范围内的恶意软件和其他计算机安全威胁。Kaspersky Endpoint Security 可以对计算机进行全盘扫描，对关键区域进行快速扫描，以及对指定范围进行扫描。了解更多。

更新

Kaspersky Endpoint Security 可以从卡巴斯基更新服务器、分发点或您的系统管理员指定的其他来源更新应用程序数据库和模块，并创建所有更新文件的备份副本以允许回滚上一次更新。了解更多。

备份

在尝试清除或删除受感染文件之前，Kaspersky Endpoint Security 会创建受感染文件的备份副本，以便您能够恢复这些文件。了解更多。

报告

Kaspersky Endpoint Security 可以生成与应用程序组件相关的事件和操作的报告。了解更多。

通知

Kaspersky Endpoint Security 使用通知来告知您有关 Kaspersky Endpoint Security 运行中发生的某些事件。通知可以伴随声音。了解更多。

保护中心

Kaspersky Endpoint Security 会在保护中心中显示保护状态信息。保护中心将显示有关计算机保护状态以及如何消除计算机安全问题和威胁的信息。了解更多。

通过 Kaspersky Security Center 远程管理应用程序

您可以远程管理对已安装 Kaspersky Endpoint Security 的计算机的保护：接收有关当前计算机保护状态的信息，远程修复问题，响应计算机安全威胁，启用或禁用保护组件（文件威胁防护、Web 威胁防护、网络威胁防护、行为检测），启用或禁用 Web 控制、Managed Detection and Response、 Endpoint Detection and Response 和 Endpoint Detection and Response Expert (on-premise)，运行扫描任务，更新应用程序数据库，运行启动盘加密，以及管理 Kaspersky Endpoint Security 授权许可和订阅。您可以使用以下工具来管理 Kaspersky Endpoint Security：

- Kaspersky Security Center 管理控制台。了解更多。
- Kaspersky Security Center Web Console 和云控制台。了解更多。

注意： Kaspersky Endpoint Security 支持的功能取决于所使用的管理工具。

文件保险箱磁盘加密

Kaspersky Endpoint Security 允许远程管理文件保险箱加密功能。加密技术可防止未经授权的用户访问用户计算机的启动盘上存储的敏感数据。

Web 控制

您可以远程管理用户对网站的访问。您可以允许或阻止访问特定网址或网址组。您也可以基于网站内容允许或阻止访问特定类别的网站。了解更多。

设备控制

设备控制管理用户对安装在计算机上或连接到计算机的设备的访问。这样，当连接此类设备时，您就可以保护计算机免受感染，并防止数据丢失或泄漏。了解更多。

Managed Detection and Response

Managed Detection and Response 组件提供了与 Kaspersky Managed Detection and Response 服务的交互，该服务持续检测并消除针对您组织的安全威胁。了解更多。

Detection and Response

Endpoint Detection and Response 组件有助于与 Kaspersky Endpoint Detection and Response 解决方案进行交互。该解决方案的功能结合了自动检测威胁和对这些威胁做出反应的能力，以抵御包括新漏洞利用、勒索软件、无文件攻击以及使用合法系统工具的方法在内的高级攻击。了解更多。

Endpoint Detection and Response Expert (on-premise)

Endpoint Detection and Response Expert (on-premise) 组件有助于与 Kaspersky Anti Targeted Attack Platform 解决方案进行交互。该解决方案可及时检测高级威胁，例如定向攻击、高级持续威胁、零日攻击等。了解更多。

此版本中的新功能

该帮助应用到 Kaspersky Endpoint Security for Mac 版本 12.2.1。

Kaspersky Endpoint Security 提供以下新功能和改进：

- 现已支持新的 macOS 27 Golden Gate。
- Web Console 中的策略管理界面已更新。策略部分的结构已更改，以确保与 Kaspersky Endpoint Security for Windows 和 Linux 插件保持一致。
- 现在您可以查看在特定时期内对策略进行的修改，并将有关这些修改的信息保存到文件中。
- 我们添加了新的邮件威胁防护、设备控制、防火墙、修复引擎和漏洞利用防御组件。
- 现在，您可以从 Kaspersky Endpoint Security 应用程序激活 Managed Detection and Response 组件。
- 提高了警报详细信息响应操作的可见性。
- 现在，您可以在 Web Console 中管理行为检测组件。
- 我们添加了警报摘要。
- 现在，在执行任何响应操作之前，您将收到一个对象是关键系统对象的通知。
- 现在，在创建或编辑 IOC 扫描任务设置时，您可以直接在 Web Console 中编辑 IOC 文件。
- 现在，您可以将检测到的对象从警报详细信息中移动到隔离区。
- 我们为网络隔离任务添加了受限制操作的警告。
- 常规问题修复和改进。

Kaspersky Endpoint Security 功能比较（取决于 Kaspersky Security Center 管理工具）

Kaspersky Endpoint Security 支持的功能取决于所使用的管理工具（参见下表）。

您可以使用以下工具来管理 Kaspersky Endpoint Security：

- Kaspersky Security Center 管理控制台。Kaspersky Security Center 管理员工作站上安装的 Microsoft 管理控制台 (MMC) 管理单元。
- Kaspersky Security Center Web Console。管理服务器上安装的 Kaspersky Security Center 组件。您可以在可访问管理服务器的任何计算机上通过浏览器使用 Web Console。
- Kaspersky Security Center 云控制台。Kaspersky Security Center 的云版本。

Kaspersky Endpoint Security 功能比较

功能	Kaspersky Security Center		
	管理控制台	Web Console	云控制台
高级威胁防护			
卡巴斯基安全网络	✓	✓	✓
行为检测	✓	✓	
漏洞利用防御	✓	✓	
修复引擎	✓	✓	
基本威胁防护			
文件威胁防护	✓	✓	✓
Web 威胁防护	✓	✓	✓
反网络攻击	✓	✓	✓
邮件威胁防护	✓	✓	
防火墙	✓	✓	
安全控制			
Web 控制	✓	✓	✓
设备控制	✓	✓	
数据加密			
文件保险箱磁盘加密	✓	✓	✓
恢复密钥	✓	✓	✓
Detection and Response			
Managed Detection and Response	✓	✓	✓
Detection and Response		✓	
Endpoint Detection and Response Expert (on-premise)	✓	✓	✓
任务			
添加密钥	✓	✓	✓
更新	✓	✓	✓
快速扫描	✓	✓	

功能	Kaspersky Security Center		
	管理控制台	Web Console	云控制台
回滚	✓	✓	✓
扫描	✓	✓	✓

安装和卸载应用程序

分发包

分发包包含 Kaspersky Endpoint Security 安装包，其中包含以下文件：

- 通过任何可用方式安装应用程序所需的文件。
- 附带有最终用户授权许可协议的 license_<loc>.txt 文件。
  最终用户授权许可协议指定应用程序的使用条款。

解压压缩的安装包可访问其中的文件。

硬件和软件要求

Kaspersky Endpoint Security 对硬件和软件有以下要求：

- 处理器类型：Intel、 Apple silicon
- 4 GB 内存 (RAM)
- 5 GB 可用磁盘空间
- macOS 14，15，26，27
- 互联网连接

支持的浏览器：

- Safari
- Chrome
- Firefox

Kaspersky Endpoint Security 与以下虚拟化工具兼容：

- Parallels Desktop 16 for Mac Business Edition 或后续版本
- VMware Fusion™ 11.5 Professional
- VMware Fusion 12 Professional
- VMware Fusion 13 Pro

MDM 配置文件可以与 Jamf 和 Apple 服务器一起部署。如果使用其他服务器，请参阅技术支持网站（知识库）上的文章。

您可以通过 Kaspersky Security Center 远程管理 Kaspersky Endpoint Security。要使用 Kaspersky Security Center 管理控制台管理插件和 Kaspersky Security Center Web Console Web 插件管理 Kaspersky Endpoint Security，需要安装 Kaspersky Security Center 14.2 或后续版本。

注意：要通过 Kaspersky Security Center 管理 Kaspersky Endpoint Security for Mac 12.2.1，必须在远程计算机上安装网络代理版本 15。

准备安装

在计算机上安装应用程序之前，建议您执行以下操作：

- 确保您的计算机满足硬件和软件要求。
- 删除卡巴斯基安全软件 for Mac 版或任何其他反恶意软件应用程序以避免系统冲突，并最大限度地提高系统性能。

注意：在远程安装 Kaspersky Endpoint Security 之前，建议您从卡巴斯基技术支持网站下载 KES_for_macOS11_and_later.zip 压缩包，并使用 Apple 远程管理工具在客户端计算机上应用 KES_for_macOS11_and_later_profile.mobileconfig 配置文件。这将允许 Kaspersky Endpoint Security 获取以下权限：内核功能扩展和系统功能扩展安装权限、完全磁盘访问权限和网络连接配置权限。要了解有关配置文件和其他选项的更多信息，请访问技术支持网站。

安装 Kaspersky Endpoint Security

重要：卡巴斯基专家建议您仅按照本帮助中所述的步骤安装 Kaspersky Endpoint Security。

您可以采用以下方式之一安装 Kaspersky Endpoint Security：

- 使用从卡巴斯基网站下载的分发包本地安装。
- 使用 Apple 远程桌面远程安装
- 通过 Kaspersky Security Center 管理控制台远程安装。
- 通过 Kaspersky Security Center Web Console 或 Kaspersky Security Center 云控制台远程安装。

  有关使用 Kaspersky Security Center Web Console 部署卡巴斯基应用程序的详细信息，请参阅 Kaspersky Security Center 帮助。有关使用 Kaspersky Security Center 云控制台部署卡巴斯基应用程序的详细信息，请参阅 Kaspersky Security Center 云控制台帮助。

执行 Kaspersky Endpoint Security 标准安装

1. 解压缩分发包中的 ZIP 压缩包。
2. 打开解压缩的压缩包内容中的 .dmg 文件。

3. 在打开的窗口中，双击**安装 Kaspersky Endpoint Security**。
   将打开 Kaspersky Endpoint Security 安装助手。
4. 单击**安装**。
5. 按照安装助手的步骤完成安装。

安装完成后，将自动启动 Kaspersky Endpoint Security。无需重启计算机。

注意：如果使用此安装方法，则不会安装 Endpoint Detection and Response Expert (on-premise)、Endpoint Detection and Response (Optimum) 和 Cloud Sandbox 组件。

执行 Kaspersky Endpoint Security 自定义安装

1. 解压缩分发包中的 ZIP 压缩包。
2. 打开解压缩的压缩包内容中的 .dmg 文件。
3. 在打开的窗口中，双击**安装 Kaspersky Endpoint Security**。
   将打开 Kaspersky Endpoint Security 安装助手。
4. 单击“**定制**”，选中或取消选中您不想安装的组件旁边的复选框并单击“**继续**”。
5. 按照安装助手的步骤完成安装。

安装完成后，将自动启动 Kaspersky Endpoint Security。无需重启计算机。

使用 Apple 远程桌面远程安装 Kaspersky Endpoint Security

1. 在您的 Mac 上，选择 **Apple 菜单** > **系统设置** > **常规** > **共享**。
2. 选中**远程管理**复选框。
3. 在要用作服务器的另一台 Mac 上，安装 Apple 远程桌面。有关 Apple 远程桌面的更多信息，请参阅 Apple 支持。
4. 打开 Apple 远程桌面。
5. 在**远程桌面**窗口中，单击左侧的**扫描仪**，并选择要在其上安装 Kaspersky Endpoint Security 的设备。
6. 单击**安装**。
7. 当系统提示您输入管理员凭据时，输入管理员名称和密码并单击**添加**。
8. 单击 + 并选择包含 Kaspersky Endpoint Security 安装包的 .dmg 文件。
9. 单击**安装**。

将在所选设备上开始安装 Kaspersky Endpoint Security。

准备使用应用程序

安装 Kaspersky Endpoint Security 后，可执行以下操作：

- 激活 Kaspersky Endpoint Security。激活 Kaspersky Endpoint Security 后，该应用程序将开始保护您的计算机，您可以定期更新应用程序数据库和模块，执行恶意软件扫描任务，以及向技术支持发送请求。

  > Managed Detection and Response 组件在 Kaspersky Security Center 管理控制台或 Web Console 中被单独激活。

  如果您当前的授权许可不支持 Endpoint Detection and Response 组件，您需要单独激活 Kaspersky Endpoint Detection and Response。

- 评估计算机保护状态。
- 更新 Kaspersky Endpoint Security。
- 扫描您的计算机以查找恶意软件。

卸载 Kaspersky Endpoint Security

1. 打开应用程序分发包的 DMG 文件。
2. 在包含分发包内容的窗口中，双击**卸载 Kaspersky Endpoint Security**。
   将启动 Kaspersky Endpoint Security 卸载程序。
3. 在卸载程序窗口中，单击**卸载**。
4. 当系统提示您输入管理员凭据时，输入管理员名称和密码并确认您要卸载 Kaspersky Endpoint Security。
   将开始卸载 Kaspersky Endpoint Security。
5. 阅读有关卸载完成的信息并单击**退出**以退出卸载程序。

现在已从您的计算机中卸载 Kaspersky Endpoint Security。卸载应用程序后不必重启计算机。

首次启动应用程序

在计算机上安装 Kaspersky Endpoint Security 后，将立即启动该应用程序。为了立即保护您的 Mac，应用程序会提示您执行基本设置：

- 向 Kaspersky Endpoint Security 授予必要的权限，以保护您的 Mac 免遭恶意软件、网络攻击和互联网威胁的侵害。

  有关所授予权限的更多信息，请单击 ?。

- 激活 Kaspersky Endpoint Security。

注意： Kaspersky Endpoint Security 基本设置需要互联网连接。

首次启动 Kaspersky Endpoint Security

1. 在**基本保护**窗口中，执行以下操作以确保文件威胁防护和 Web 威胁防护工作正常：

   - 如果希望 Kaspersky Endpoint Security 应用程序正常工作，请允许应用程序扫描您的 Mac 上的每一个文件。为此，请单击**完全磁盘访问权限**项旁边的**允许**，并按照屏幕上的说明操作。
   - 如果您希望 Kaspersky Endpoint Security 在 URL 和网络数据包可能损害您的 Mac 之前对其进行检查，请安装系统扩展。为此，请单击**系统扩展程序**项旁边的**安装**，并按照屏幕上的说明操作。
   - 如果您希望系统扩展正常工作，请允许网络内容过滤。为此，请单击**网络内容过滤**项旁边的**允许**，并按照屏幕上的说明操作。
   - 如果您希望 Kaspersky Endpoint Security 搜索加密 HTTPS 流量中的恶意软件和互联网威胁，请安装受信任证书。为此，请单击**受信任证书**项旁边的**安装**，并按照屏幕上的说明操作。

   重要： 如果不授予这些权限，Kaspersky Endpoint Security 应用程序将无法正常工作。您必须在**基本保护**窗口中授予所有权限。

2. 单击**继续**。

将打开主应用程序窗口。

Kaspersky Endpoint Security 应用程序界面

主应用程序窗口

打开主应用程序窗口

在菜单栏上，单击应用程序图标并选择 **Kaspersky Endpoint Security**。

Kaspersky Endpoint Security 的主应用程序窗口包含可访问应用程序主要功能的界面元素。

主应用程序窗口分为两部分：

- 左侧部分包含侧边栏，可让您导航应用程序并快速访问其主要功能。
- 中央部分显示侧栏中所选部分的内容，并允许您管理数据。

侧边栏

主应用程序窗口的侧边栏具有以下选项：

监控	单击可打开**监控**页面，该页面提供有关 Kaspersky Endpoint Security 为保护您的计算机而采取的措施的信息。
保护中心	单击可查看您的计算机保护状态。了解更多。
安全性	单击可查看已安装组件的运行状态。了解更多。
扫描	单击可管理扫描任务。了解更多。
更新	单击可管理更新任务。了解更多。
授权许可	单击以激活应用程序或查看有关您的授权许可的信息。了解更多。

“**监控**”页面的控件

监控页面显示保护状态指示器，提供有关 Kaspersky Endpoint Security 为保护您的计算机所做的操作的信息，并包含以下控件。

保护中心	通知您有关计算机的保护问题。了解更多。
报告	允许您查看应用程序、各个组件和任务运行期间发生的事件。了解更多。
备份	允许您查看应用程序已删除的受感染文件的已保存副本列表。了解更多。了解更多。
威胁检测	允许您查看有关 Kaspersky Endpoint Security 应用的威胁检测技术以及这些技术检测到的威胁数量的信息。
卡巴斯基安全网络	显示 Kaspersky Endpoint Security 和卡巴斯基安全网络之间的连接状态，以及全球卡巴斯基安全网络统计信息。

Kaspersky Endpoint Security 图标

安装 Kaspersky Endpoint Security 之后，Kaspersky Endpoint Security 图标会随即出现在菜单栏中。激活应用程序后，应用程序图标将显示应用程序的状态。如果应用程序图标处于活动状态( )，表示所有或部分保护组件已启用。如果应用程序图标处于非活动状态( )，表示所有保护组件已禁用。

打开应用程序图标菜单

在菜单栏中，单击应用程序图标。

默认情况下，应用程序图标始终显示在菜单栏中。您可以从菜单栏中删除应用程序图标。

从菜单栏中删除应用程序图标

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**界面**选项卡的**应用程序图标**区域中，取消选中**在菜单栏中显示**复选框。

打开应用程序窗口，应用程序图标也会出现在 **Dock** 区。

从应用程序图标菜单中，您可以访问应用程序主窗口并执行以下操作：

- 禁用计算机保护。
- 恢复计算机保护。
- 打开保护中心。
- 开始快速扫描。
- 运行更新。
- 打开应用程序设置窗口。
- 退出 Kaspersky Endpoint Security。

应用程序设置窗口

打开应用程序设置窗口

执行下列操作之一：

- 在菜单栏，单击应用程序图标并选择**设置**。
- 在菜单栏中，单击 **Kaspersky Endpoint Security** > **设置**。
- 如果 Kaspersky Endpoint Security 正在运行，单击 **Dock** 中的应用程序图标并选择**设置**。

使用设置窗口上部的以下选项卡可快速访问应用程序设置：

- **基本**。在此选项卡上，可启用或禁用计算机保护，并配置文件威胁防护、Web 威胁防护和网络威胁防护设置。
- **扫描**。在此选项卡上，可配置扫描任务设置和扫描任务启动计划。
- **威胁**。在此选项卡上，可选择要检测的对象类别，创建受信任区域，以及配置备份设置。
- **高级**。在此选项卡上，可加入或选择退出卡巴斯基安全网络。
- **更新**。在此选项卡上，可配置应用程序更新设置，或回滚到应用程序数据库的先前版本。
- **界面**。在此选项卡上，可配置 Kaspersky Endpoint Security 图标、通知和报告的设置，以及启用或禁用在追踪文件中记录调试信息。

使用  按钮，可阻止不具有管理员权限的用户编辑 Kaspersky Endpoint Security 设置。此按钮位于应用程序设置窗口的下部。要编辑设置，您必须输入管理员的凭据。

单击 ? 按钮可打开 Kaspersky Endpoint Security 帮助，其中描述了当前应用程序窗口中的所有设置。您也可通过在**帮助**菜单中选择**打开此窗口的帮助**来打开活动应用程序窗口的帮助主题。

关于通知

Kaspersky Endpoint Security 可显示通知来告知您相关应用程序事件。通知将显示在操作系统的通知中心中，具体取决于计算机上安装的操作系统版本。通知的外观取决于操作系统通知设置中设置的选项。

根据事件的重要性，Kaspersky Endpoint Security 事件分为三种类型：

- *关键* – 会对计算机安全造成严重威胁的事件（检测到恶意对象、漏洞、Kaspersky Endpoint Security 问题）。关键事件需要您立即关注。我们建议您不要禁用关键事件通知。
- *重要* – 无需您立即关注，但将来可能会对计算机安全造成威胁的事件。
- *信息* – 报告给您以供参考的事件。

禁用通知

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**界面**选项卡的**通知**区域中，取消选中**启用通知**复选框。

启用记录非关键事件

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**界面**选项卡的**报告**区域中，选中**记录非关键事件**复选框以接收有关 Kaspersky Endpoint Security 信息事件的通知。

无论是否启用通知，应用程序报告均包含 Kaspersky Endpoint Security 运行期间发生的事件的相关信息。

通知可以伴随声音（例如，检测到恶意软件时的通知）。您可以禁用声音提醒。

记录非关键事件显著增加报告文件总大小。说明：该设置仅应用到文件威胁防护。

禁用通知伴随的声音提醒

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**界面**选项卡的**通知**区域中，取消选中**检测到恶意软件时打开警报音**复选框。

如果需要选择事件响应操作，Kaspersky Endpoint Security 将会显示通知窗口。例如，当应用程序检测到恶意对象时，它会提示您删除或清除该对象。只有在选择了其中一项操作后，通知窗口才会从屏幕上消失。

Kaspersky Endpoint Security 应用程序授权许可

关于最终用户授权许可协议

最终用户授权许可协议（以下简称"授权许可协议"）是您和 AO Kaspersky Lab 之间签订的具有约束力的协议，规定了与使用该应用程序相关的条款。

重要：在开始使用应用程序之前，请认真阅读授权许可协议。

您可以通过以下方式查看《最终用户授权许可协议》的条款：

- 在安装 Kaspersky Endpoint Security 过程中
- 阅读应用程序安装文件夹中的 license.txt 文档

一旦安装 Kaspersky Endpoint Security，即表示您确认您已了解并接受最终用户授权许可协议的条款。如果您不接受最终用户授权许可协议的条款，请取消安装 Kaspersky Endpoint Security 且不得使用该应用程序。

关于授权许可

*授权许可*是根据最终用户授权许可协议的条款授予的在有限时间内使用 Kaspersky Endpoint Security 的权利。

服务范围和有效期取决于应用程序所使用的授权许可。

提供以下授权许可类型：

- *试用*。用于试用该应用程序的免费授权许可。

  试用授权许可通常具有较短的有效期。当试用授权许可到期时，所有 Kaspersky Endpoint Security 功能都将被禁用。要继续使用该应用程序，您必须购买商业授权许可。

  您只能在试用授权许可下使用该应用程序一个试用期。

- *商业*。付费授权许可。

  当商业授权许可到期时，应用程序的关键功能将被禁用。要继续使用 Kaspersky Endpoint Security，您必须续费您的商业授权许可。商业授权许可到期后，您无法继续使用该应用程序，必须将其从设备中删除。

  建议您在授权许可到期之前续费授权许可，以确保不间断地防范所有安全威胁。

关于订阅

*Kaspersky Endpoint Security 订阅*是具有特定参数（到期日期、受保护的设备数量）的应用程序购买订单。您可以从服务提供商（例如您的 ISP）处订购 Kaspersky Endpoint Security 订阅。您可以通过服务提供商网站上的会员专区来管理订阅。例如，您可以续费或取消您的订阅，缩短订阅期限，或更改您的订阅下受保护的设备数量。

订阅可以是有限期的（例如，一年），也可以是无限期的（没有到期日期）。当有限订阅过期后，要继续使用 Kaspersky Endpoint Security，必须手动续费订阅。只要您已经提前向服务提供商付款，就会自动续费无限订阅。

如果依据有限订阅使用应用程序，当订阅到期时，将会向您提供一个订阅续费宽限期。在宽限期内，应用程序功能保持不变。

在您的更新订阅到期且订阅续费宽限期已过后，Kaspersky Endpoint Security 将继续提供保护，但将停止更新应用程序数据库。

在您的更新和保护订阅到期且订阅续费宽限期已过后，Kaspersky Endpoint Security 停止保护您的计算机。

要依据订阅使用 Kaspersky Endpoint Security，必须添加服务提供商提供的激活码。在依据订阅使用应用程序时，无法使用其他激活码续费订阅。只有当订阅到期或取消订阅时，才可以使用不同的激活码。要取消订阅，请联系向您销售 Kaspersky Endpoint Security 的服务提供商。

注意：仅当激活密钥已删除时，才能使用其他订阅激活码。订阅没有密钥文件。无法添加订阅作为备用密钥。在使用订阅时，无法添加备用密钥。

如果您已在依据有效授权许可使用 Kaspersky Endpoint Security，但希望改为依据订阅使用应用程序，请删除当前激活密钥，以便使用订阅密钥激活此应用程序。可将之前在此计算机上激活应用程序所使用的激活码用于其他计算机。

注意：服务提供商不同，可用的订阅选项可能也不同。某些服务提供商也可选择不提供用于续费订阅的宽限期。

关于授权许可证书

*授权许可证书*是一份随密钥文件或激活码一起发送给您的文档。

授权许可证书包含有关所提供的授权许可的以下信息：

- 授权许可密钥或订单号
- 已获得授权许可授权的用户的相关信息
- 依据所提供的授权许可可激活的应用程序的相关信息
- 授权许可单元的数量限制（例如，依据所提供的授权许可可在其上使用该应用程序的设备数量）
- 授权许可有效期开始日期
- 授权许可到期日期或授权许可期限
- 授权许可类型

关于密钥

*密钥*由一系列数位组成，您可以依据最终用户授权许可协议的条款使用它们激活并使用应用程序。密钥由卡巴斯基专家生成。

您可以采用以下方式之一为应用程序添加密钥：通过应用*密钥文件*，或者通过输入*激活码*。为应用程序添加密钥后，将在应用程序界面中显示该密钥的唯一字母数字序列。

如果违反授权许可协议的条款，卡巴斯基可能会阻止您的密钥。如果密钥已被阻止，您需要添加其他密钥才能继续使用应用程序。

密钥可以为激活密钥或备用密钥。

*激活密钥*是指应用程序当前正在使用的密钥。可以为试用授权许可、商业授权许可或订阅添加激活密钥。应用程序不能包含多个激活密钥。

*备用密钥*是指授予用户使用应用程序的资格但当前未使用的密钥。如果与当前激活密钥相关联的授权许可到期，备用密钥将自动成为激活密钥。仅当已添加激活密钥后，才可以添加备用密钥。

试用授权许可密钥可添加为激活密钥。试用授权许可密钥不能添加为备用密钥。当激活密钥为试用授权许可密钥时，无法添加备用密钥。

关于激活码

*激活码*是由 20 个字母和数字组成的唯一序列。要添加授权许可密钥以激活 Kaspersky Endpoint Security，您必须输入激活码。在购买 Kaspersky Endpoint Security 或请求 Kaspersky Endpoint Security 试用版本后，您会在您提供的电子邮件地址收到激活码。

要使用激活码激活应用程序，您需要互联网访问以便连接卡巴斯基激活服务器。

如果您在安装应用程序后丢失了激活码，请联系您购买授权许可的卡巴斯基合作伙伴。

关于密钥文件

*密钥文件*是卡巴斯基向您提供的具有 .key 扩展名的文件。密钥文件旨在通过添加授权许可密钥来激活应用程序。

在购买 Kaspersky Endpoint Security 或订购 Kaspersky Endpoint Security 试用版本后，您会在您提供的电子邮件地址收到密钥文件。

使用密钥文件无需连接至卡巴斯基激活服务器以激活应用程序。

如果密钥文件被意外删除，则您可以恢复它。例如，您可能需要密钥文件以注册 Kaspersky CompanyAccount。

要恢复密钥文件，请执行以下任一操作：

- 联系授权许可销售商。
- 通过使用可用的激活码从 卡巴斯基网站 获取密钥文件。

关于数据提供

最终用户授权许可协议

在使用激活码激活 Kaspersky Endpoint Security 时，为了验证应用程序使用的合法性并提供有关卡巴斯基产品的分发和使用统计信息，您同意在使用 Kaspersky Endpoint Security 的过程中自动提供以下信息：

- 已安装软件的类型、版本和本地化。
- 已安装的更新版本。
- 计算机的标识符和计算机上软件安装的标识符。
- 当前授权许可的激活码和唯一激活标识符。
- 操作系统的类型、版本和字长。
- 虚拟环境的名称（当软件安装在虚拟环境中时）。
- 提供信息时处于活动状态的软件组件的标识符。
- 支持的数据源。
- 超时。
- 用户计算机上的日期和时间。
- 协议版本。
- 协议内容类型。
- 协议内容长度。
- 所使用的数据压缩类型。
- 激活票证上的签名类型。
- 区域激活中心标识符。
- 使用 SHA1 算法计算的激活码哈希。
- 使用 SHA1 算法计算的票证正文哈希。
- 授权许可票证的创建日期和时间。
- 授权许可激活标识符。

- 当前授权许可票证标识符。
- 授权许可票证序列标识符。
- 授权许可激活日期和时间。
- 授权许可到期日期和时间。
- 授权许可状态。
- 授权许可版本。
- 用户计算机的唯一标识符。
- 授权许可票证标头版本。
- 应用程序名称。
- 传输的数据类型。
- 传输的数据架构版本。
- 操作系统的完整版本。
- 所使用的虚拟机的描述。
- 兼容应用程序的 ID 列表。

当使用 Kaspersky 更新服务器下载更新时，为了提高更新过程的效率，您同意提供以下信息，用于数据库和模块更新期间的应用程序识别目的：

- 软件 ID (AppID)。
- 活动授权许可 ID。
- 唯一的软件安装 ID (InstallationID)。
- 唯一的更新任务启动 ID (SessionID)。
- 应用程序版本 (BuildInfo)。

卡巴斯基安全网络 (KSN) 声明

使用 KSN 可以加快软件对信息和网络安全威胁的反应速度。通过以下方式实现所宣称的目的：

- 决定扫描对象的声誉。
- 识别新的和具有挑战性的信息安全威胁来检测，及其源。
- 立即采取措施提高对于最终用户使用计算机存储和处理的数据的保护力度。
- 降低误报的可能性。
- 提高应用程序组件的效率。
- 用户计算机感染调查。

- 改进卡巴斯基产品的性能。
- 接收有关已知声誉的对象数的参考信息。
- 及时识别并纠正与产品安装、删除和更新相关的错误。

在使用 KSN 期间，卡巴斯基将自动接收并处理数据。用户传输的数据取决于所安装的授权许可类型以及指定的卡巴斯基安全网络使用设置。

如果使用的是适用于 1-4 个节点的授权许可，在使用卡巴斯基安全网络期间，Kaspersky 将自动接收并处理以下数据：

- 有关使用的授权许可的信息： 授权许可的类型和有效期、授权许可到期前的天数、向其购买授权许可的合作伙伴的标识符、区域激活中心标识符、激活码的校验码、使用 SHA1 算法计算出的票证正文哈希值、授权许可票证的创建日期和时间、授权许可信息标识符、授权许可票证标识符、授权许可票证序列标识符、用户计算机的唯一标识符、授权许可票证的有效期开始日期、授权许可票证的有效期截止日期、授权许可票证当前状态、票证标头版本、授权许可版本、票证标头签名证书标识符、密钥文件的校验码、票证标头签名者序列号、身份验证令牌。
- 已安装软件的完整版本； 已安装软件的类型； 软件更新 ID； 信誉服务 ID； 协议类型 ID； 区域激活中心 ID； 已撤销的软件服务决定列表的版本； 软件反病毒数据库中触发记录的 ID； 软件反病毒数据库中触发记录的时间戳； 触发的软件反病毒数据库记录的类型； 计算机上的应用程序安装实例的独一 ID； 授权许可激活日期； 授权许可到期日期； 授权许可 ID； 软件使用的授权许可的状态； 正在处理的对象的校验和类型； 检测到的可用于破坏用户设备或数据的恶意软件或合法软件的名称； 正在处理的对象的校验和； 软件激活码校验和； 软件的完整版本； 独一设备 ID； 软件 ID； 软件密钥文件的校验和； 用于提供软件授权许可的信息模型的 ID； 用于签署软件授权许可 ticket 标头的证书的标识符； 软件授权许可 ticket 创建日期和时间； 软件授权许可 ticket 校验和； 软件授权许可 ticket 版本； 软件激活码版本； 向权利持有人基础结构的请求的数据格式； 当前授权许可 ticket ID； 软件组件 ID； 软件操作的结果； 错误代码； Web 服务的访问地址 (URL、IP)； 端口号； Web 服务请求源的 Web 地址 (Referrer)； 证书的公钥； 所扫描对象和哈希算法的数字证书指纹。

如果使用的是适用于 5 个或更多节点的授权许可，在使用卡巴斯基安全网络期间，Kaspersky 将自动接收并处理以下数据：

- 相关信息，包括已安装在计算机上的操作系统 (OS) 和服务包的版本、操作系统内核文件的版本与校验码（MD5、SHA2-256、SHA1）、操作系统运行模式的参数； 操作系统版本、操作系统内部版本号、操作系统更新编号、操作系统版本、有关操作系统版本的扩展信息； 操作系统 Service Pack 版本； 操作系统的启动日期和时间； 行为分析子系统中有关操作系统操作的事件的处理延迟时间； 当前类型的延迟操作系统操作事件的数量； 主动防御子系统中有关操作系统操作的事件的处理延迟时间； 已处理的操作系统操作事件的数量； 已处理的同步操作系统操作事件的数量； 当前类型的所有操作系统操作事件的总延迟； 持久事件存储子系统中有关操作系统操作的事件的处理延迟时间； 所有操作系统操作事件的总延迟； 等待同步操作系统操作事件的数量； 接收到的操作系统操作事件的日期和时间。
- 有关上次操作系统重启失败的信息： 重启失败次数。

- 有关权利持有人安装的应用程序和反病毒保护状态的信息： 软件安装 ID (PCID)； 软件数据库记录版本； 计算机上安装的应用程序实例的唯一标识符、应用程序类型、应用程序类型的 ID、已安装应用程序的完整版本、应用程序设置版本的标识符、计算机类型的标识符、安装应用程序的计算机的唯一标识符、权利持有人服务中的唯一用户标识符、区域设置语言和运行状态、已安装的软件组件的版本及其运行状态、连接权利持有人服务所使用的协议版本； 已安装软件的完整版本； 已安装软件的类型； 软件更新 ID； 信誉服务 ID； 协议类型 ID； 区域激活中心 ID； 已撤销的软件服务决定列表的版本； 软件反病毒数据库中触发记录的 ID； 软件反病毒数据库中触发记录的时间戳； 触发的软件反病毒数据库记录的类型； 计算机上的应用程序安装实例的独一 ID； 授权许可激活日期； 授权许可到期日期； 授权许可 ID； 软件使用的授权许可的状态； 正在处理的对象的校验和类型； 检测到的可用于破坏用户设备或数据的恶意软件或合法软件的名称； 正在处理的对象的校验和； 软件激活码校验和； 软件的完整版本； 软件 ID； 软件密钥文件的校验和； 用于提供软件授权许可的信息模型的 ID； 用于签署软件授权许可 ticket 标头的证书的标识符； 软件授权许可 ticket 创建日期和时间； 软件授权许可 ticket 校验和； 软件授权许可 ticket 版本； 软件激活码版本； 向权利持有人基础结构的请求的数据格式； 当前授权许可 ticket ID； 软件组件 ID； 软件操作的结果； 错误代码； Web 服务的访问地址 (URL、IP)； 端口号； Web 服务请求源的 Web 地址 (Referrer)； 反病毒数据库的更新应用周期数； 反病毒数据上次更新和应用的日期和时间； 软件数据库的发布日期和时间； 软件组件的版本； 软件更新 ID； 已安装软件的类型； 系统监控的启动日期和时间； 软件的安装日期和时间； 系统监控发送统计数据的概率； 系统监控进行处理所花费的时间长于标准时间的事件的代码； 系统监控进行处理所花费的时间长于标准时间的事件的数据库处理时间； 系统监控处理一个事件的最长允许时间； 系统监控进行处理所花费的时间长于标准时间的事件的处理时间； 系统监控进行处理所花费的时间长于标准时间的事件的总数。

- 有关所有已处理对象和操作的信息： 软件对正在处理的对象的裁定； 目录代码； 所处理对象的大小； 所处理对象的校验和 (SHA256)； 系统监控上下文中所检测软件的编号； 系统监控检测软件的日期和时间； 删除特征； 软件反病毒数据库中触发记录的 ID； 系统监控检测软件的原因； 所处理对象的校验和 (MD5)； 模块完整性检查的结果； 所处理对象的名称； 触发的软件反病毒数据库记录的类型； 所处理对象的路径； 已扫描对象的名称； 扫面的日期和时间； 下载它的 URL 和 Referrer 地址； 已扫描文件的大小及其路径； 存档标志； 文件创建的日期和时间； 打包程序的名称、大小和校验和（MD5、SHA2-256）（如果文件被打包）； 文件的熵； 文件的类型； 文件类型代码； 可执行文件的标志、ID 和格式； 对象的校验和（MD5、SHA2-256）； 对象的补充校验和的类型和值； 有关对象的数字签名（证书）的数据： 证书发布者的数据、上次统计交付后对象的启动次数、应用程序的扫描任务 ID、接收对象信誉信息的方式、目标过滤器的值、适用检测技术的技术参数； 所处理对象的路径； 目录代码。

- 对于可执行文件： 文件部分的熵、信誉验证标记或文件签名标记、名称、类型、ID 类型、校验码 (MD5)，以及正在接受验证的对象加载的应用程序的大小、应用程序路径和模板路径、表明在自动运行列表中存在的属性、输入日期、属性列表、打包程序名称、应用程序数字签名的相关信息： 发行商证书、以 MIME 格式上传的文件的名称、文件构建日期和时间。

- 有关已启动的应用程序及其模块的信息： 运行文件的校验码（MD5、SHA2-256）、大小、属性、创建日期、打包程序的名称（如果文件被打包）、文件的名称、系统上运行的进程的信息（进程 ID (PID)）、进程名称、启动进程的账户信息、启动进程的应用程序和命令、进程文件的完整路径、启动命令行、进程所属应用程序的描述（应用程序的名称和开发商信息，以及使用的数字证书和用于验证其真实性的信息或缺乏文件数字签名的信息），和进程中加载的模块信息： 它们的名称、大小、类型、创建日期、属性、校验码（MD5、SHA2-256、SHA1）、路径、PE 文件头信息、打包程序名称（如果文件被打包）、这些统计数据的可用性和有效性的相关信息、生成被发送的统计数据的模式的标识符。

- 如果检测到威胁或漏洞，除了提供检测到的对象的相关信息外，还应提供该记录在反病毒数据库中的标识符、版本和类型，该威胁在卡巴斯基分类中的名称，上一次更新反病毒数据库的日期和时间，可执行文件名称，向检测到威胁的网址发出请求的应用程序文件的校验码 (MD5)，检测到的威胁的 IP 地址（IPv4 或 IPv6），漏洞标识符及其威胁等级，检测到漏洞的网页的网址和 Referrer。

- 如果检测到潜在的恶意对象，则提供有关进程内存中的数据的信息。

- 网络攻击信息： 攻击计算机的 IP 地址和用户计算机上成为网络攻击目标的端口号，攻击协议的 ID，攻击的名称和类型。

- 关于网络连接的信息： 来自使打开端口的进程启动的文件的版本和校验和 (MD5、SHA2-256、SHA1)，进程文件的路径及其数字签名，本地和远程 IP 地址，本地和远程连接端口的数量，连接的状态，端口开放的时间戳。

- 检测到有害或可疑内容的网页的网址和 IP 地址，向该网址发出请求的文件名称、大小及校验码、实现裁定结果所用规则的标识符、权重和程度、攻击的目标。

- 有关已安装应用程序和反病毒数据库更新的信息： 更新任务的完成状态、更新过程中可能发生的错误的类型、未成功更新的数量、执行更新的应用程序组件的标识符。

- 有关使用卡巴斯基安全网络 (KSN) 的信息： KSN 标识符、应用程序标识符、应用程序完整版本、用户设备的匿名 IP 地址、KSN 请求履行质量指标、KSN 数据包处理质量指标、KSN 请求数量指标和 KSN 请求类型信息、统计数据开始发送的日期和时间、统计数据完成发送的日期和时间、KSN 配置更新的相关信息： 活动配置的标识符、接收的配置标识符、配置更新的错误代码。

- 有关系统日志事件的信息： 事件时间、检测到事件的日志的名称、事件的类型和类别、事件源的名称和事件描述。

- 用于确定文件和 URL 地址信誉的信息： 请求信誉的 URL 地址和 Referrer、连接的协议类型、应用程序类型的内部标识符、正在使用的端口号、用户标识符、扫描文件的校验码 (MD5)、检测到的威胁类型、用于检测威胁的记录的信息（反病毒数据库的记录标识符、记录时间戳和类型）； 证书的公钥； 所扫描对象和哈希算法的数字证书指纹。

- 应用程序地域分布数据： 应用程序安装和激活日期、为应用程序激活提供授权许可的合作伙伴 ID、应用程序 ID、应用程序语言本地化 ID、应用程序激活的授权许可序列号、KSN 参与标志。

- 有关使用的授权许可的信息： 授权许可的类型和有效期、授权许可到期前的天数、向其购买授权许可的合作伙伴的标识符、区域激活中心标识符、激活码的校验码、使用 SHA1 算法计算出的票证正文哈希值、授权许可票证的创建日期和时间、授权许可信息标识符、授权许可票证标识符、授权许可票证序列标识符、用户计算机的唯一标识符、授权许可票证的有效期开始日期、授权许可票证的有效期截止日期、授权许可票证当前状态、票证标头版本、授权许可版本、票证标头签名证书标识符、密钥文件的校验码、票证标头签名者序列号、身份验证令牌。

- 有关计算机上已安装硬件的信息： 类型、名称、型号名称、固件版本、内置设备和连接设备的参数。

- 设备信息： 设备 ID。

- 有关 Web 控制组件的操作的信息： 组件版本、分类原因、有关分类原因的其他信息、分类的 URL、被锁定或分类的对象的主机 IP 地址。

此外，为了实现提高应用程序提供的保护效果的声明的目的，Kaspersky 可能会收到被入侵者利用损害计算机并创建信息安全威胁的对象。此类对象包含：

- 可执行或非可执行文件或其部分

- 计算机的 RAM 区域

- OS 启动过程中涉及的分区

- 网络流量数据包

- 包含可疑对象或恶意对象的网页和电子邮件

- WMI 存储的类和类实例的说明

- 应用程序活动报告

应用程序活动报告包含有关文件和进程的以下信息：

- 要发送的文件的名称、大小和版本、说明和校验和 (MD5、SHA2-256、SHA1)、格式 ID、其制造商名称、文件所属应用程序的名称、计算机上文件的完全限定路径和路径模板代码、文件创建和更新的日期与时间。

- 如果发送的文件具有数字签名、证书签名的日期和时间，则有证书有效期开始日期、结束日期和时间，证书颁发者的姓名，证书持有人的信息，证书的印记和公钥及用于计算它们的算法，证书序列号。
- 运行进程的账户的名称。
- 用于运行进程的计算机名称的校验码 (MD5、SHA2-256、SHA1)。
- 进程的窗口标题。
- 反病毒数据库的 ID，根据卡巴斯基分类确定的威胁的名称。
- 用于应用程序、授权许可 ID、授权许可类型和到期日期的信息。
- 在提供信息的时的计算机的本地时间。
- 进程访问的文件的名称和路径。
- 进程访问的网址和 IP 地址。
- 从中下载运行文件的网址和 IP 地址。

此外，为了实现所宣称的有关防止误报的目的，权利持有人可接收值得信赖的可执行和不可执行文件或其部分。

阅读卡巴斯基安全网络声明

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**高级**选项卡上，单击**显示 KSN 声明**。

Kaspersky Endpoint Security 将以下信息保存在追踪文件中：

- 有关设备和操作系统的信息（唯一的设备 ID、设备类型、网络设备的 MAC 地址、操作系统类型、操作系统版本）。
- 有关应用程序及其模块的操作的信息。
- 有关订阅（订阅类型、区域）的信息。
- 有关语言区域设置、应用程序 ID、应用程序自定义、应用程序版本、唯一的应用程序安装 ID、唯一计算机 ID 的信息。
- 有关计算机反恶意软件保护状态，以及所有已处理和已检测到的对象的信息（包含已检测到的对象名称、检测的日期和时间、对象的下载网址、已感染文件的名称和大小及其路径、攻击计算机的 IP 地址和网络攻击的目标计算机端口号、恶意软件活动列表和不需要的网址），以及应用程序和用户所做相关操作和决定的信息。
- 有关用户下载的应用程序的信息（网址、属性、文件大小、下载文件的进程的相关信息）。
- 有关启动的应用程序及应用程序模块的信息（大小、属性、创建日期、PE 标头详细信息、区域、名称、位置、打包应用程序）。
- 有关界面错误和已安装卡巴斯基的应用程序界面用法的信息。
- 有关网络连接的信息：远程计算机和用户计算机的 IP 地址、用于建立连接的端口号和连接的网络协议。

- 有关计算机通过 IT 与电信网络接收和发送的网络包的信息。
- 有关发送和接收的电子邮件和即时消息的信息。
- 有关访问的网址的信息：使用开放式协议建立连接的时间、有关网站登录登录名和密码的数据和 Cookie 内容。
- 服务器的公共证书。

追踪文件只包含修复应用程序中的缺陷所需的信息。卡巴斯基使用追踪文件调查与 Kaspersky Endpoint Security 应用程序运行中的错误相关联的事件。

默认情况下，禁用追踪文件的创建。您可以在应用程序设置中启用追踪文件的生成。

追踪文件只能手动发送到卡巴斯基。应用程序不会自动向卡巴斯基发送追踪文件。

您可以选择如何将追踪文件发送到卡巴斯基。

在向卡巴斯基发送追踪文件之前，请查看它们包含的数据。

重要：追踪文件可能包含个人信息或敏感信息。通过向卡巴斯基发送追踪文件，您同意向卡巴斯基提供您发送的追踪文件中包含的所有数据，并且您同意用于发送它们的方法。

此外，可能会被入侵者用于危害计算机或数据的文件或其某些部分也可发送到卡巴斯基进行检查。

卡巴斯基保护根据法律和适用的卡巴斯基规则收到的任何信息。数据通过安全通道传输。

您可以自行决定是否加入卡巴斯基安全网络。安装应用程序时，会提示您选择是否加入卡巴斯基安全网络。您之后可随时更改决定。

激活 Kaspersky Endpoint Security

重要：激活 Kaspersky Endpoint Security 之前，请确保您计算机上设置的日期和时间与实际日期和时间相符。

在激活应用程序过程中，将会向应用程序中添加密钥。

注意：激活应用程序需要互联网连接。

激活试用版本

1. 打开主应用程序窗口。
2. 在主应用程序窗口的侧边栏上，单击“**授权许可**”。
   这将打开“**授权许可**”窗口。
3. 在“**授权许可**”窗口中，单击“**激活**”。

Kaspersky Endpoint Security 将连接到卡巴斯基激活服务器并发送数据进行验证。如果验证成功，应用程序将接收并添加免费试用版本的密钥。

重要：只有在之前未曾在计算机上激活 Kaspersky Endpoint Security 的前提下，才可以激活该应用程序的试用版本。

使用激活码激活应用程序

1. 打开主应用程序窗口。
2. 在主应用程序窗口的侧边栏上，单击“**授权许可**”。
   这将打开“**授权许可**”窗口。
3. 在“**授权许可**”窗口中，输入您在购买 Kaspersky Endpoint Security 时收到的激活码。
4. 单击**激活**。

注意：激活码是一个由 20 个拉丁字母和数字组成的唯一组合，采用 xxxxx-xxxxx-xxxxx-xxxxx 形式。

应用程序将连接到卡巴斯基激活服务器并发送激活码以验证真伪。如果已成功验证激活码，应用程序将自动接收并添加授权许可密钥。

注意：您可能需要填写注册表，具体取决于收到的激活码。

如果激活码验证失败，则会显示相应的通知。此时，请联系向您提供此激活码的软件供应商。

使用激活码激活应用程序后，您可在“**授权许可**”窗口中查看以下信息：

- 授权许可或订阅状态
- 活动密钥
- 备用密钥（如果有）
- 授权许可类型，以及可在当前授权许可或订阅下使用该应用程序的计算机数量
- 当前授权许可或订阅下可用的应用程序功能
- 授权许可到期日期和时间
- 授权许可到期之前的剩余天数

查看授权许可信息

查看授权许可信息

1. 打开主应用程序窗口。
2. 在主应用程序窗口的侧边栏上，单击“**授权许可**”。

这将打开“**授权许可**”窗口。

“**授权许可**”窗口可能包含以下信息：

- 授权许可或订阅状态
- 活动密钥
- 备用密钥（如果有）
- 授权许可类型，以及可在当前授权许可或订阅下使用该应用程序的计算机数量
- 当前授权许可或订阅下可用的应用程序功能
- 授权许可到期日期和时间
- 授权许可到期之前的剩余天数

管理授权许可和订阅

如果与激活密钥关联的授权许可已到期，并且未添加任何备用密钥，则必须续费授权许可。当授权许可到期时，应用程序将以受限功能模式继续运行（更新、卡巴斯基安全网络、Web 控制和文件保险箱磁盘加密将无法通过 Kaspersky Security Center 进行使用）。您仍然可以使用所有应用程序组件和运行恶意软件扫描，但只能使用授权许可到期之前安装的反恶意软件数据库。

重要：如果反恶意软件数据库已过期，您的计算机将面临更高的感染风险。

续费授权许可

1. 在主应用程序窗口的侧边栏上，单击**保护中心** 。

   保护中心窗口打开。

2. 在“**保护中心**”窗口中，单击“**续订**”。

   将会打开一个网页，显示如何通过卡巴斯基在线商店或卡巴斯基合作伙伴续费授权许可的相关信息。如果通过在线商店续费授权许可，在完成付款后，Kaspersky Endpoint Security 的激活码将发送到订单中指定的电子邮件地址。

当您在订阅下使用程序时，Kaspersky Endpoint Security 将按照指定间隔自动联系激活服务器，直至您的订阅过期。

如果您在无限订阅下使用该应用程序，Kaspersky Endpoint Security 将续费您的订阅，而不需要您执行任何操作。

如果您在有限订阅下使用该应用程序且订阅续费宽限期已结束，Kaspersky Endpoint Security 将向您发送相关通知，且不再尝试自动续费订阅和更新应用程序数据库。

您可以与向您销售 Kaspersky Endpoint Security 的供应商联系，手动续费订阅。

续费订阅

1. 打开主应用程序窗口。
2. 在主应用程序窗口的侧边栏上，单击“**授权许可**”。
   这将打开“**授权许可**”窗口。
3. 在“**授权许可**”窗口中，单击“**访问服务提供商网站**”。

   将会打开服务提供商的网站。

您的订阅状态可能变成已到期。此时，您需要手动更新订阅状态。如果您当前没有订阅，Kaspersky Endpoint Security 将停止更新应用程序数据库（如果您购买的是更新订阅），或者停止保护您的计算机（如果您购买的是更新和保护订阅）。

更新订阅状态

1. 打开主应用程序窗口。
2. 在主应用程序窗口的侧边栏上，单击“**授权许可**”。
   这将打开“**授权许可**”窗口。
3. 在“**授权许可**”窗口中，单击 按钮。

根据工作站授权许可类型比较应用程序功能

工作站上可用的 Kaspersky Endpoint Security 功能集取决于授权许可类型（见下表）。

Kaspersky Endpoint Security 功能比较

功能	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert
高级威胁防护						
卡巴斯基安全网络	✓	✓	✓	✓	✓	✓
行为检测	✓	✓	✓	✓	✓	✓
漏洞利用防御	✓	✓	✓	✓	✓	✓
修复引擎	✓	✓	✓	✓	✓	✓
基本威胁防护						
文件威胁防护	✓	✓	✓	✓	✓	✓
Web 威胁防护	✓	✓	✓	✓	✓	✓
邮件威胁防护	✓	✓	✓	✓	✓	✓
防火墙	✓	✓	✓	✓	✓	✓
反网络攻击	✓	✓	✓	✓	✓	✓
安全控制						
设备控制	✓	✓	✓	✓	✓	✓
Web 控制	✓	✓	✓	✓	✓	✓
数据加密						

功能	Kaspersky Endpoint Security for Business Select	Kaspersky Endpoint Security for Business Advanced	Kaspersky Total Security	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert
文件保险箱磁盘加密	–	✓	✓	✓	✓	✓
Detection and Response						
Endpoint Detection and Response Optimum	–	–	–	✓	✓	–
Endpoint Detection and Response Expert	–	–	–	–	–	✓
Kaspersky Sandbox *（Kaspersky Sandbox 授权许可必须单独购买）*	✓	✓	✓	✓	✓	✓

执行常规任务

打开和退出应用程序

安装完毕后，将自动启动该应用程序，并在菜单栏中显示应用程序图标。

打开应用程序

在菜单栏上，单击应用程序图标并选择 **Kaspersky Endpoint Security**。

退出应用程序

在菜单栏上，单击应用程序图标并选择**退出**。

退出应用程序后，应用程序进程将从计算机内存中删除。

重要：退出 Kaspersky Endpoint Security 应用程序后，计算机将不再受保护，并可能感染病毒，从而使您的数据面临丢失的危险。

查看计算机保护的状态

保护状态指示器会告知您计算机保护方面的问题。这个指示器形状像盾牌，位于主应用程序窗口。指示器的颜色可随计算机保护状态而改变。如果 Kaspersky Endpoint Security 检测到任何安全威胁，主应用程序窗口中会显示一条有关威胁的消息，并且指示器的颜色会发生变化。

指示器颜色可以通过以下方式改变：

- **绿色**。您的计算机受到适当的保护。

  绿色指示器表示反恶意软件数据库为最新版本，所有应用程序组件已按照卡巴斯基建议进行配置。未检测到恶意对象，或已清除检测到的任何恶意对象。

- **黄色**。计算机的保护水平下降。

  黄色指示器表示 Kaspersky Endpoint Security 发现问题。此类问题包括与推荐的保护设置有轻微差异或应用程序数据库刚刚过期。

- **红色**。计算机面临感染危险。

  红色指示器表示存在严重问题，可能导致计算机受到感染或数据丢失。例如，此反恶意软件应用程序数据库严重过期、此应用程序未激活或检测到恶意对象。

  我们建议您尽快修复任何问题并处理安全威胁。

查看已安装组件的运行状态

Kaspersky Endpoint Security 允许您在**安全性**窗口中检查已安装应用程序组件的状态。每个组件名称旁边的指示器反映了其状态。

查看组件状态

1. 打开主应用程序窗口。
2. 在主应用程序窗口的侧边栏上，单击**安全性** 。
   将会打开"**安全性**"窗口。

可能会显示以下状态指示器：

	该组件正在运行。
	该组件由安全策略运行和管理。
	该组件发生故障。
	该组件发生故障并由安全策略管理。
	该组件已关闭。
	该组件被关闭并由安全策略管理。
	该组件已暂停。
	当前授权许可不支持该组件。

注意：对于某些组件，您还可以使用组件名称旁边的三点菜单来打开报告或配置组件设置。

禁用和恢复计算机保护

默认情况下，Kaspersky Endpoint Security 会在操作系统启动后启动，并在关闭计算机之前始终保护您的计算机。所有保护组件（文件威胁防护、Web 威胁防护和网络威胁防护）均已启用并正在运行。

您可以完全禁用保护或禁用特定的保护组件。

重要：Kaspersky 强烈建议不要禁用保护或保护组件，因为禁用这些组件可能导致计算机感染病毒和丢失数据。

当计算机保护被禁用时：

- 菜单栏中的应用程序图标为非活动状态。
- 主应用程序窗口中的保护状态指示器为红色。

当一个或多个保护组件被禁用时，保护状态指示器为红色或黄色。

注意：禁用或暂停保护组件不会影响扫描任务或更新任务。

您可以通过采用以下方法之一禁用/恢复计算机保护：

- 从应用程序图标
- 从应用程序设置窗口
- 从**保护**菜单

从应用程序图标禁用/恢复计算机保护

1. 在菜单栏中，单击应用程序图标并选择**关闭保护/打开保护**。
   当您关闭保护时，将出现管理员凭据的提示。
2. 当系统提示您输入管理员凭据时，输入管理员名称和密码并确认您要关闭保护。

从应用程序设置窗口禁用/恢复计算机保护

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**基本**选项卡的**常规**区域中，取消选中/选中**启用保护**复选框。

从菜单栏禁用/恢复计算机保护

在菜单栏中，单击**保护** > **关闭保护/打开保护**。

重要：如果禁用计算机保护，在 Kaspersky Endpoint Security 重新启动时不会自动重新启用计算机保护。您必须手动重启保护组件。

禁用保护组件

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**基本**选项卡的 **<组件名称>** 区域中，取消选中**启用 <组件名称>** 复选框。

重要：如果禁用保护组件，在 Kaspersky Endpoint Security 重新启动时不会自动重新启用保护组件。您必须手动重启保护组件。

启用保护组件

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**基本**选项卡的 **<组件名称>** 区域中，选中**启用 <组件名称>** 复选框。

要启用计算机保护或保护组件，您还可以使用保护中心。禁用计算机保护或禁用保护组件会使您的计算机面临更高的感染风险。这就是在计算机保护功能禁用时保护中心会进行通知的原因。

使用保护中心

保护中心 是 Kaspersky Endpoint Security 的一项功能，可帮助您分析并修复问题和计算机安全威胁。

打开保护中心

在主应用程序窗口的侧边栏上，单击**保护中心** 。

在保护中心中，您可以找到有关活动威胁的信息，查看应用程序数据库的状态，并了解是否禁用了任何组件保护。

注意： 如果贵组织的系统管理员启用 Web 控制以阻止访问危险网络资源，则 Kaspersky Endpoint Security 会在保护中心中显示 **Web 控制已启用。** 通知。

对于每个问题或威胁，Kaspersky Endpoint Security 会提供操作建议，您可以执行这些操作以解决该问题或威胁。例如，如果 Kaspersky Endpoint Security 在计算机上检测到受感染文件，您可以单击**清除**。如果反恶意软件数据库已过期，您可以单击**更新**。您可立即修复问题或清除威胁，也可以稍后执行操作。

立即修复问题或清除威胁

单击具有推荐操作名称的按钮，以修复问题或清除威胁。

应用程序即会执行所选操作。

如果不清除危险威胁就关闭保护中心，主应用程序窗口中的保护状态指示器将保持为红色，提醒您存在这些威胁。

执行扫描任务

Kaspersky Endpoint Security 中包含默认的全盘扫描任务。在运行此任务时，该应用程序将扫描计算机的内存、启动对象和所有内部驱动器以确定是否存在病毒和其他恶意软件。

执行计算机全盘扫描

1. 在主应用程序窗口的侧边栏上，单击**扫描** 。
   将会打开**扫描**窗口。
2. 单击 **全盘扫描**按钮。

计算机的全盘扫描将开启。

Kaspersky Endpoint Security 中包含默认的快速扫描任务。在运行此任务时，该应用程序将扫描计算机的关键区域（内存、启动对象和系统文件夹）以确定是否存在病毒和其他恶意软件。

执行计算机快速扫描

1. 在主应用程序窗口的侧边栏上，单击**扫描** 。
   将会打开**扫描**窗口。
2. 单击 **快速扫描**按钮。

计算机的快速扫描将开启。

如果希望对个别对象（如内部磁盘、文件夹、文件或可移动磁盘）执行病毒和其他恶意软件扫描，可运行“自定义扫描”任务。

扫描所选项目

执行下列操作之一：

- 右键单击所选项目并选择**扫描恶意软件**。
- 将所选项目拖到 Dock 中的应用程序图标。
- 拖动选中的项到**扫描**窗口。

可以在**报告**窗口中查看已完成的扫描任务的结果。

注意： Kaspersky Endpoint Security 不会扫描位于 OneDrive 或 iCloud 存储或者其他云存储中的文件。请将这些文件排除在扫描范围之外。否则，扫描任务可能会以“*受感染文件未删除*”错误结束。

配置自动启动计划扫描任务

您可以创建快速扫描和全盘扫描任务启动计划。Kaspersky Endpoint Security 可依据配置的计划自动扫描整个计算机或计算机的指定区域。

从扫描窗口计划扫描任务

1. 在主应用程序窗口的侧边栏上，单击**扫描** 。
   将会打开**扫描**窗口。
2. 单击**计划扫描**。
   将会打开一个对话框，您可以在其中设置计划。
3. 选中**全盘扫描**或**快速扫描**复选框。
4. 指定扫描频率和扫描开始时间。
5. 单击**确定**。

从设置窗口计划扫描任务

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。

2. 在**扫描**选项卡上，单击**计划**。

3. 在打开的窗口中，选择您要按计划扫描的任务名称旁边的复选框。

4. 配置扫描任务频率和时间。

5. 单击**确定**保存更改。

可在**报告**窗口中查看扫描任务结果。

更新应用程序数据库

专用的卡巴斯基更新服务器是 Kaspersky Endpoint Security 的主更新源。Kaspersky Endpoint Security 也可以使用分发点、本地文件夹或其他 Web 服务器作为*更新源*。

注意：从更新服务器下载更新需要连接到互联网。

默认情况下，Kaspersky Endpoint Security 定期检查卡巴斯基更新服务器上的更新。如果服务器上存在新的更新，Kaspersky Endpoint Security 将在后台下载这些更新，并将其安装到您的计算机。

启动 Kaspersky Endpoint Security 更新

1. 在主应用程序窗口的侧边栏上，单击**更新** 。
   将会打开**更新**窗口。

2. 单击**更新**。

   应用程序将检查更新。如果更新可用，应用程序将下载并安装到您的计算机上。

您也可以用以下方法之一启动更新任务：

- 单击应用程序图标并选择**更新**。
- 在菜单栏中，选择**保护** > **更新**。

您可以更改 Kaspersky Endpoint Security 更新应用程序数据库的方式。默认情况下，应用程序会自动更新数据库。

启用/禁用自动下载 Kaspersky Endpoint Security 数据库更新

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。

2. 在**更新**选项卡的**数据库**区域中，选中/取消选中**自动下载更新**复选框。

可以在**报告**窗口中查看已完成的更新任务的结果。

注意：在美国境内，本软件中将不再提供更新功能（包括提供反恶意软件签名更新和代码库更新）以及 KSN 功能。

文件访问被阻止时如何应对

Kaspersky Endpoint Security 应用程序可阻止访问受感染的文件和应用程序。如果某个文件受到感染，必须先对其进行清除才能访问该文件。

清除检测到的对象

1. 在菜单栏中，选择**保护** > **已检测到的对象**。

   将打开**已检测到的对象**窗口。

2. 在**已检测到的对象**区域中，单击所需文件旁边的 •••，然后选择**清除**。

   应用程序开始清除选择的对象。在进行清除时，应用程序会显示一个对话框，可以选择将向对象执行的操作。

清除所有检测到的对象

1. 在菜单栏中，选择**保护** > **已检测到的对象**。

   将打开**已检测到的对象**窗口。

2. 在**已检测到的对象**区域中，单击**清除全部**。

   应用程序开始清除已检测到的对象。在进行清除时，应用程序会显示一个对话框，可以选择将向对象执行的操作。在选择了操作之后，如果在通知窗口中选中**应用到全部**复选框，则应用程序会将此操作应用到所有此类型的文件。

如果您确信被文件威胁防护阻止的文件是安全的，可以将其纳入受信任区域中。

恢复已被应用程序删除或清除的文件

我们有时无法在清除过程中完整保存文件。如果已清除的文件包含重要信息，且这些信息在清除之后部分或完全无法访问，您可以尝试从备份副本恢复原始文件。

恢复在清除过程中已被应用程序删除或修改的文件

1. 在菜单栏中，选择**保护** > **已检测到的对象**。

   将打开**已检测到的对象**窗口。

2. 在**备份**区域中，单击要恢复的文件旁边的 •••。

   将打开弹出菜单。

3. 选择**恢复文件**。

   将打开一个窗口，用于指定文件名、标签和要将文件恢复到的文件夹。默认已指定原始文件名和位置。

4. 指定文件名和要将文件恢复到的文件夹。

5. 单击**保存**。

   应用程序将使用指定名称将该文件恢复到指定位置。

在恢复文件后，您需要立即对其进行恶意软件扫描。或许使用更新后的数据库可清除该对象而不会破坏其完整性。

重要：建议您不要恢复文件的备份副本，除非还原它们是绝对必要的，因为这样做可能会导致计算机感染。

查看应用程序运行报告

您可以查看 Kaspersky Endpoint Security 报告，所有检测到的对象均列出在**已处理的对象**选项卡上。系统事件显示在**系统事件**选项卡上。此外，还将为以下各个应用程序组件创建单独的详细报告：文件威胁防护、Web 威胁防护、网络威胁防护、行为检测、扫描以及更新任务。

打开报告窗口

在菜单栏中，选择**保护** > **报告**。

出现通知窗口时如何应对

以通知窗口形式显示的应用程序通知用于通知您需要引起注意的应用程序事件。

如果屏幕上出现通知，请选择建议的选项之一。最佳选项是卡巴斯基专家建议的默认选项。

应用程序高级配置

计算机保护范围

Kaspersky Endpoint Security 检测的对象按不同属性划分为多种类别。应用程序始终会搜索病毒、蠕虫、木马和恶意工具。这些应用程序可能会对计算机造成严重危害。为确保对您的计算机提供更可靠的保护，您可以通过允许应用程序检查可以被入侵者利用来危害您的计算机或个人数据的合法软件，来扩展可检测对象的列表。

Kaspersky Endpoint Security 可防御的对象按以下类别分组：

- **病毒、蠕虫、木马、恶意工具、广告软件和自动拨号软件**。
  此类别包括：
  - 所有类型的恶意软件。
  - 通过在您的计算机上显示广告（例如，广告栏）或将浏览器中的搜索结果替换为广告网站，而给您造成不便的软件。
  - 通过计算机的调制解调器秘密建立电话连接的应用程序。

  防御所有类型的恶意软件是必须达到的最低安全级别。按照卡巴斯基专家的建议，Kaspersky Endpoint Security 将始终监控属于此类别的对象。
- **可以被入侵者利用以损坏您的计算机或个人数据的合法软件**。此类别包括可以被入侵者利用来危害您的计算机或个人数据的合法软件，例如远程管理应用程序。

选择要检测的对象类别

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**威胁**选项卡的**要检测的对象**区域中，选中要检测的对象类别旁边的复选框。

> **注意：** Kaspersky Endpoint Security 会始终保护您的计算机免受病毒、蠕虫、木马程序、恶意工具、广告软件和自动拨号程序的侵害。因此，无法取消选中此类别的复选框。

根据所选择的要检测的对象类别，Kaspersky Endpoint Security 会在运行文件威胁防护、Web 威胁防护和扫描任务时使用部分或全部反恶意软件数据库。

> **注意：** 如果 Kaspersky Endpoint Security 将某个应用程序归类为恶意软件，但您认为该应用程序是安全的，则可以将其添加到受信任区域中。

受信任区域 是 Kaspersky Endpoint Security 不会扫描或监控的对象的列表。例如，如果 Kaspersky Endpoint Security 阻止访问某个文件、应用程序或网站，但您确信此对象、应用程序或网址是绝对安全的，则可能需要将该对象添加到受信任区域中。

将某个应用程序添加到受信任区域后，将不再监控其文件和网络活动（包括可疑活动）。但是，Kaspersky Endpoint Security 会继续扫描受信任应用程序的可执行文件和进程。

注意：当管理员将策略配置为禁止编辑受信任区域时，用户无法转到"受信任区域"设置。

向受信任文件和文件夹列表添加/删除文件或文件夹

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**威胁**选项卡的**排除项**区域中，单击**受信任区域**。
   将会打开受信任区域设置窗口。
3. 在**文件和文件夹**选项卡上，编辑受信任文件和文件夹列表：
   - 向列表中添加文件或文件夹：
     a. 单击 +。
        将会打开一个可在其中选择文件或文件夹的对话框。
     b. 选择要添加的文件或文件夹。
     c. 单击**打开**。
   - 从列表中删除文件或文件夹：
     a. 选择要从受信任文件和文件夹列表中删除的文件或文件夹。
     b. 单击 –。
4. 单击**确定**。

向受信任网址列表添加/删除受信任网址

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**威胁**选项卡的**排除项**区域中，单击**受信任区域**。
   将会打开受信任区域设置窗口。
   您也可以通过单击**基本**选项卡的**常规**部分中的**受信任区域**按钮来打开此窗口。
3. 在**网址**选项卡上，编辑受信任网址列表：
   - 向列表中添加网址：
     a. 单击 +。
     b. 输入您想添加到列表中的网址。
     c. 单击**确定**。

- 从列表中删除网址：

  a. 选择要删除的网址。

  b. 单击 – 。

4. 单击**确定**。

默认情况下，受信任网址列表为空。

向受信任应用程序列表添加/删除受信任应用程序

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**威胁**选项卡的**排除项**区域中，单击**受信任区域**。
   将会打开受信任区域设置窗口。
   您也可以通过单击**基本**选项卡的**常规**部分中的**受信任区域**按钮来打开此窗口。
3. 在**受信任的应用程序**选项卡上，编辑受信任的应用程序列表：

   - 要将应用程序添加到列表：

     a. 单击 + 。
     这将打开一个窗口，您可以在其中指定所需应用程序的参数。

     b. 指定要添加的应用程序的以下参数：

     - **路径**
     - **代码签名要求**

     > **注意：**您可以手动输入这两个参数的值，也可以单击“**选择**”按钮并在打开的窗口中选择要添加的应用程序。在这种情况下，这些参数的值将被自动插入。

     c. 在“**选项**”部分中，选择至少一种您不想被 Kaspersky Endpoint Security 应用程序监控的活动类型：

     - **不监控文件活动**
     - **不监控网络活动**

     d. 单击**确定**。

   - 要从列表中删除应用程序：

     a. 选择您想要删除的应用程序。

     b. 单击 – 。

默认情况下，受信任应用程序列表为空。

编辑受信任应用程序

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**威胁**选项卡的**排除项**区域中，单击**受信任区域**。
   将会打开受信任区域设置窗口。
   您也可以通过单击**基本**选项卡的**常规**部分中的**受信任区域**按钮来打开此窗口。
3. 在"**受信任应用程序**"选项卡上，选择要编辑的应用程序。
4. 单击"**编辑**"。
5. 在打开的窗口中，编辑应用程序的参数。
6. 单击**确定**。

启用对受信任网址的监控

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**威胁**选项卡的**排除项**区域中，单击**受信任区域**。
   将会打开受信任区域设置窗口。
3. 在**网址**选项卡上，取消选中希望 Kaspersky Endpoint Security 应用程序监控的网址旁边的复选框。
4. 单击**确定**。

文件威胁防护

文件威胁防护可防止计算机的文件系统受到感染。该组件随操作系统一起启动，保留在计算机的内存中，会针对在您的计算机和所有连接的磁盘上打开、保存或运行的所有文件进行恶意软件扫描。如果禁用文件威胁防护，则在启动操作系统时将不会启动该组件。您必须手动重新启用文件威胁防护。

启用/禁用文件威胁防护

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**基本**选项卡的**文件威胁防护**区域中，选中/取消选中**启用文件威胁防护**复选框。
   您还可以在保护中心中启用文件威胁防护。禁用计算机保护或禁用保护组件会使您的计算机面临更高的感染风险。这就是在计算机保护功能禁用时保护中心会进行通知的原因。

您可以创建文件威胁防护的保护范围。

向保护范围中添加/从中删除文件或文件夹

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。

2. 在**基本**选项卡的**文件威胁防护**区域中，单击**保护范围**。

   将会打开一个窗口，其中列出文件威胁防护将扫描的对象列表。默认情况下，文件威胁防护将扫描连接到您的计算机的内部磁盘、可移动磁盘和网络磁盘中的所有对象。

   注意：您可以跳过对只读系统卷的扫描以显著降低扫描时间。默认情况下，文件威胁防护不扫描只读系统卷。

3. 在**保护范围**区域，添加/删除对象：

   - 向保护范围中添加文件或文件夹：

     a. 单击 +。

     将会打开一个弹出菜单，可在其中选择要添加到保护范围中的对象。

     b. 在弹出菜单中，选择**文件和文件夹**项。

     将会打开一个可在其中选择文件或文件夹的对话框。

     c. 选择您想添加到保护范围中的文件或文件夹。

     d. 单击**打开**。

   - 从保护范围中删除文件或文件夹：

     a. 选择保护范围对象列表中的对象。

     b. 将所选对象从窗口中拖出或单击 –。

4. 如果您要扫描只读系统卷，在**优化**区域，取消选择**跳过扫描只读系统卷**复选框。

   重要：优化可能由于安全原因而禁用。

5. 单击**保存**。

在保护范围中添加/删除默认对象列表中的对象

1. 在菜单栏，单击应用程序图标并选择**设置**。

   此时会打开应用程序设置窗口。

2. 在**基本**选项卡的**文件威胁防护**区域中，单击**保护范围**。

   将会打开一个窗口，其中列出文件威胁防护将扫描的对象列表。默认情况下，文件威胁防护将扫描连接到您的计算机的内部磁盘、可移动磁盘和网络磁盘中的所有对象。

   注意：您可以跳过对只读系统卷的扫描以显著降低扫描时间。默认情况下，文件威胁防护不扫描只读系统卷。

3. 在**保护范围**区域，添加/删除默认对象列表中的对象：

   - 将默认对象列表中的对象添加到保护范围：

     a. 单击 +。
     将会打开一个弹出菜单，可在其中选择要添加到保护范围中的对象。

     b. 在弹出菜单中，选择您想要添加到保护范围中的对象（例如**所有内部磁盘**）。

   - 在保护范围中删除默认对象列表中的对象：

     a. 选择保护范围对象列表中的对象。

     b. 将所选对象从窗口中拖出或单击 –。

4. 如果您要扫描只读系统卷，在**优化**区域，取消选择**跳过扫描只读系统卷**复选框。

   重要：优化可能由于安全原因而禁用。

5. 单击**保存**。

禁用保护范围中的对象保护

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。

2. 在**基本**选项卡的**文件威胁防护**区域中，单击**保护范围**。
   将会打开一个窗口，其中列出文件威胁防护将扫描的对象列表。默认情况下，文件威胁防护将扫描连接到您的计算机的内部磁盘、可移动磁盘和网络磁盘中的所有对象。

   注意：您可以跳过对只读系统卷的扫描以显著降低扫描时间。默认情况下，文件威胁防护不扫描只读系统卷。

3. 取消选中保护范围对象列表中对象旁边的复选框。

4. 单击**保存**。

启用对只读系统卷的扫描

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。

2. 在**基本**选项卡的**文件威胁防护**区域中，单击**保护范围**。
   将会打开一个窗口，其中列出文件威胁防护将扫描的对象列表。默认情况下，文件威胁防护将扫描连接到您的计算机的内部磁盘、可移动磁盘和网络磁盘中的所有对象。

   注意：您可以跳过对只读系统卷的扫描以显著降低扫描时间。默认情况下，文件威胁防护不扫描只读系统卷。

3. 在**优化**区域，取消选择**跳过扫描只读系统卷**复选框。

重要：优化可能由于安全原因而禁用。

4. 单击**保存**。

当您或某个应用程序尝试访问保护范围内的某个文件时，文件威胁防护会检查 iSwift 数据库是否包含有关该文件的信息，并使用此信息确定是否需要扫描该文件。

由于使用*特征码分析*（一种基于应用程序反恶意软件数据库中的威胁描述来搜索威胁的方法），因此可识别恶意对象。除特征码分析外，文件威胁防护还使用启发式分析和其他扫描技术。

如果在文件中检测到威胁，Kaspersky Endpoint Security 会识别检测到的恶意软件的类型（例如，*病毒*或*木马*）。随后，应用程序会显示一条有关检测到的对象的通知，并基于文件威胁防护设置对该对象执行操作。

选择文件威胁防护在检测到受感染文件后执行的操作

1. 在菜单栏，单击应用程序图标并选择**设置**。

   此时会打开应用程序设置窗口。

2. 在**基本**选项卡的**文件威胁防护**区域中，选择文件威胁防护在检测到受感染文件后执行的操作。

尝试清除或删除受感染文件之前，Kaspersky Endpoint Security 会保存文件的备份副本，以供在以后恢复或清除该文件。

有关文件威胁防护和检测到的所有对象的信息会记录在报告中。

注意：如果文件威胁防护停止运行并显示错误，可查看报告并尝试重启该组件。如果问题未解决，请联系卡巴斯基技术支持。

查看文件威胁防护报告

1. 在菜单栏中，选择**保护** > **报告**。

   将会打开**报告**窗口。

2. 打开**文件威胁防护**选项卡。

Web 威胁防护

使用互联网时，您的计算机会暴露于受恶意软件和其他计算机安全威胁感染的风险之中。在您下载免费应用程序或访问已被黑客攻击的网站时，计算机安全威胁可能会渗透到您的计算机中。此外，网络蠕虫甚至可以在您打开网址或下载文件之前，在您的计算机连接到互联网时立即攻击您的计算机。

Kaspersky Endpoint Security 可保护您的计算机使用 Safari、Chrome 或 Firefox 通过 HTTP 和 HTTPS 协议发送和接收的信息。

注意：Kaspersky Endpoint Security 可监控 HTTP 和 HTTPS 数据传输最常用的端口上的 Web 流量。仅当在**常规**区域中选中**检查安全连接 (HTTPS)** 复选框时，Kaspersky Endpoint Security 才会扫描加密连接 (HTTPS)。

启用/禁用 Web 威胁防护

1. 在菜单栏，单击应用程序图标并选择**设置**。

   此时会打开应用程序设置窗口。

2. 在**基本**选项卡的 **Web 威胁防护**区域中，选中/取消选中**启用 Web 威胁防护**复选框。

您还可以通过保护中心启用 Web 威胁防护。禁用计算机保护或禁用保护组件会使您的计算机面临更高的感染风险。这就是在计算机保护功能禁用时保护中心会进行通知的原因。

重要：如果禁用 Web 威胁防护，在重新启动 Kaspersky Endpoint Security 或重启操作系统时不会自动重新启用该组件。您必须手动重新启用 Web 威胁防护。

Web 威胁防护根据卡巴斯基建议的设置来扫描 Web 流量。通过使用特征码分析、启发式分析和来自卡巴斯基安全网络的数据识别恶意对象。

通过检查网站上的链接是否为钓鱼威胁和恶意网址，可以避免受到*钓鱼攻击*。*钓鱼攻击*通常以入侵者的电子邮件形式或入侵者假装成金融机构（例如银行），并发送欺诈网站的链接。在这些电子邮件中，入侵者试图诱骗用户访问钓鱼网站和输入机密信息（例如，银行卡号或您的网上银行账户的名称和密码）。例如，钓鱼攻击可以伪装成来自您银行的、包含其官网链接的消息，但实际上链接会将您带到由骗子创建的以假乱真的假冒银行官网。

Web 威胁防护可监控 Web 流量对钓鱼网站的访问尝试，并阻止访问此类网站。Kaspersky Endpoint Security 使用应用程序数据库、启发式分析和来自卡巴斯基安全网络的数据来检查网站上的链接是否存在钓鱼威胁和恶意网址。

Web 流量扫描算法

Web 威胁防护会拦截您或应用程序通过 HTTP 和 HTTPS 协议访问的每个网站或文件，并对其进行恶意代码扫描：

- 如果网站或文件包含恶意代码，则 Kaspersky Endpoint Security 将会阻止该网站会文件并显示通知，指出请求的文件或网站已被感染。
- 如果文件或网页不包含恶意代码，您可立即访问。

选择 Web 威胁防护在检测到危险 Web 流量对象后执行的操作

1. 在菜单栏，单击应用程序图标并选择**设置**。

   此时会打开应用程序设置窗口。

2. 在**基本**选项卡的 **Web 威胁防护**区域中，选择 Web 威胁防护在检测到危险 Web 流量对象后执行的操作。

有关 Web 威胁防护和检测到的所有危险 Web 流量对象的信息记录会在报告中。

注意：如果 Web 威胁防护停止运行并显示错误，可查看 Web 威胁防护报告并尝试重启该组件。如果问题未解决，请联系卡巴斯基技术支持。

查看 Web 威胁防护报告

1. 在菜单栏中，选择**保护** > **报告**。
   将会打开**报告**窗口。
2. 打开 **Web 威胁防护**选项卡。

邮件威胁防护

“邮件威胁防护”组件会扫描传入和传出电子邮件的附件是否有恶意软件和其他威胁。该组件借助反恶意软件数据库、卡巴斯基安全网络云服务和启发式分析来提供计算机保护。

应用程序支持以下邮件客户端：Apple Mail、Microsoft Outlook、Mozilla Thunderbird、Canary Mail、Spark、Mimestream、Airmail、Post Box、Boxy Suite 2、Twobird、Shift、Clean Email、eM Client、Superhuman、Polymail、HEY、Mail+ for Gmail、Spike mail。

默认启用邮件威胁防护。如有必要，您可以禁用“邮件威胁防护”。

根据所选的操作模式，邮件威胁防护将执行以下操作：

- **自动删除恶意对象**。如果选中此选项，当 Kaspersky Endpoint Security 在电子邮件中检测到受感染的对象时，它会删除受感染的对象，并用文本“The requested file infected with<病毒名称>has been deleted”替换对象的内容。
- **自动阻止恶意对象**。如果选中此选项，当 Kaspersky Endpoint Security 在电子邮件中检测到受感染的对象时，它会将电子邮件主题替换为“Message is infected:<原始主题>”，其中 <原始主题> 为原始主题。仅为 POP3 协议替换电子邮件消息主题。

使用 Web Console 启用/禁用“邮件威胁防护”

1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**通信和 Web 保护 → 邮件威胁防护**”。
5. 使用“**邮件威胁防护**”拨动开关启用或禁用组件。
6. 如果启用“邮件威胁防护”，请选择检测到恶意软件时应用程序要执行的操作：
   - **删除**
   - **阻止**
7. 如有必要，在“**高级设置**”部分中配置压缩文件的检查时间限制或待扫描压缩文件的最大大小。
8. 保存您的更改。

使用管理控制台启用/禁用“邮件威胁防护”

1. 启动管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 在控制台树中，单击**受管理设备**。
4. 在工作区中，选择**策略**选项卡。
5. 右键单击要配置的策略并选择**属性**。
6. 在“**属性**”窗口中，选择“**关键威胁防护**”>“**邮件威胁防护**”。
7. 选中或取消选中“**启用邮件威胁防护**”复选框。
8. 在“**威胁检测操作**”部分中，选择当 Kaspersky Endpoint Security 检测到威胁时要执行的操作。
9. 如有必要，在“**邮件威胁防护: 设置**”部分中配置压缩文件的检查时间限制或待扫描压缩文件的最大大小。
10. 单击**确定**保存您的更改。
11. 执行以下操作之一以应用策略更改：
    - 单击“**应用**”，保存更改后，仍留在“**属性: <策略名称>**”窗口中。
    - 单击“**确定**”，保存更改后，将关闭“**属性: <策略名称>**”窗口。

使用 Kaspersky Endpoint Security 应用程序启用/禁用“邮件威胁防护”

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在“**基本**”选项卡的“**邮件威胁防护**”区域中，选中或取消选中“**启用邮件威胁防护**”复选框。
3. 如果选中“**启用邮件威胁防护**”复选框，请选择当 Kaspersky Endpoint Security 检测到威胁时要执行的操作。
4. 如有必要，配置压缩文件的检查时间限制或待扫描压缩文件的最大大小。

查看邮件威胁防护报告

1. 在菜单栏中，选择**保护** > **报告**。
   将会打开**报告**窗口。
2. 打开“**邮件威胁防护**”选项卡。

反网络攻击

Kaspersky Endpoint Security 保护您的计算机免受网络攻击。

*网络攻击*是为了入侵远程计算机的操作系统。入侵者进行网络攻击是为了建立对操作系统的控制，导致操作系统拒绝服务或访问敏感信息。为了实现这些目标，入侵者可以发动直接攻击，例如端口扫描和暴力破解攻击，也可以使用安装在受攻击计算机上的恶意软件。

网络攻击可以分为以下类型：

- *端口扫描*。此类网络攻击通常是为进行更加危险的网络攻击做准备。入侵者扫描在目标计算机上使用网络服务的 UDP/TCP 端口，并确定目标计算机受到其他更危险类型的网络攻击的漏洞。通过端口扫描，入侵者还可以确定目标计算机上的操作系统，选择适用于此类操作系统的网络攻击。

- *DoS 攻击*，即导致拒绝服务的网络攻击。此类网络攻击使目标操作系统变得不稳定或完全无法运行。

  存在以下主要的 DoS 攻击类型：

  - 传输经过专门设计但并非目标计算机所需要的网络包，导致目标操作系统运行出错或崩溃。

  - 短时间内向远程计算机发送大量网络包。目标计算机的所有资源都用于处理入侵者发送的网络包。这样，计算机停止执行其功能。

- *网络入侵攻击*。此类网络攻击用于"劫持"目标计算机的操作系统。这是最危险的一类网络攻击，因为如果成功，入侵者可以完全控制操作系统。

  当入侵者需要从远程计算机获取机密数据（例如，银行卡号和密码），或将远程计算机秘密用于入侵目的（例如，通过该计算机对其他计算机发起攻击）时，会使用此类网络攻击。

启用/禁用网络威胁防护

1. 在菜单栏，单击应用程序图标并选择**设置**。

   此时会打开应用程序设置窗口。

2. 在**基本**选项卡的**网络威胁防护**区域中，选中/取消选中**启用网络威胁防护**复选框。

您还可以在保护中心中启用网络威胁防护。禁用计算机保护或禁用保护组件会使您的计算机面临更高的感染风险。这就是在计算机保护功能禁用时保护中心会进行通知的原因。

重要：如果禁用网络威胁防护，在重新启动 Kaspersky Endpoint Security 或重启操作系统后不会自动重新启用该组件。您必须手动重新启用网络威胁防护。

当应用程序检测到危险网络活动时，Kaspersky Endpoint Security 会自动将发动攻击的计算机 IP 地址添加到阻止的计算机列表，除非发动攻击的计算机位于受信任计算机列表。

编辑被阻止的计算机列表

1. 在菜单栏，单击应用程序图标并选择**设置**。

   此时会打开应用程序设置窗口。

2. 在**基本**选项卡的**网络威胁防护**区域中，选中**启用网络威胁防护**复选框。

3. 单击**设置**。

   打开一个包含受信任计算机列表和被阻止计算机列表的窗口。

4. 打开**阻止的计算机**选项卡。

5. 如果您确定被阻止的计算机不是威胁，则在列表中选择该计算机的 IP 地址，然后单击**解除阻止**。

   将打开确认对话框。

6. 在确认窗口中，执行以下操作之一：

- 要解除对计算机的阻止，请单击**解除阻止**。
  Kaspersky Endpoint Security 会解除对 IP 地址的阻止。
- 如果您希望 Kaspersky Endpoint Security 始终不阻止选定的 IP 地址，请单击**解除阻止和排除**。
  Kaspersky Endpoint Security 会解除对 IP 地址的阻止，并将其添加到受信任计算机列表。

7. 单击**保存**。

您可以创建和编辑受信任计算机列表。Kaspersky Endpoint Security 应用程序不会阻止这些计算机 IP 地址，甚至在这些计算机上检测到危险网络活动时也是如此。

编辑受信任计算机列表

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**基本**选项卡的**网络威胁防护**区域中，选中**启用网络威胁防护**复选框。
3. 单击**设置**。
   打开一个包含受信任计算机列表和被阻止计算机列表的窗口。
4. 打开**受信任计算机**选项卡。
5. 编辑受信任计算机列表：

- 将 IP 地址添加到受信任计算机列表中：
  a. 单击 +。
  b. 在出现的字段中，输入您认为是安全的计算机 IP 地址。
- 从受信任计算机列表中删除 IP 地址：
  a. 选择列表中的 IP 地址。
  b. 单击 –。
- 编辑受信任计算机列表中的 IP 地址：
  a. 选择列表中的 IP 地址。
  b. 单击**编辑**。
  c. 更改 IP 地址。

6. 单击**保存**。

检测到网络攻击时，Kaspersky Endpoint Security 会在报告中记录有关该攻击的信息。

注意：如果网络威胁防护组件停止运行并显示错误，可查看报告并尝试重启该组件。如果问题未解决，请联系卡巴斯基技术支持。

查看网络威胁防护报告

1. 在菜单栏中，选择**保护** > **报告**。
   将会打开**报告**窗口。
2. 打开**网络威胁防护**选项卡。

防火墙

防火墙在互联网或本地网络上工作时阻止对计算机的未经授权的连接。这使您可以保护企业局域网免受身份盗窃和其他攻击。该组件借助反恶意软件数据库、卡巴斯基安全网络云服务和预定义网络规则来提供计算机保护。

网络规则属性

每条规则都有一个优先级。规则在列表中的位置越高，其优先级就越高。如果将网络活动添加到多条规则中，防火墙将根据优先级最高的规则来规范网络活动。

网络连接类型

防火墙允许您根据网络连接类型控制网络活动。您可以在 Kaspersky Endpoint Security 设置中更改网络连接的类型。

有以下网络连接类型可用：

- **公共网络**。网络不受反恶意软件应用程序、防火墙或过滤器的保护（例如咖啡馆中的 Wi-Fi）。当用户操作连接到此类网络的计算机时，防火墙会阻止对该计算机的文件和打印机的访问。外部用户也无法通过共享文件夹和远程访问此计算机的桌面来访问数据。防火墙默认将公共网络类型分配给互联网。您无法更改互联网的类型。
- **本地网络**。为对此计算机上的文件和打印机具有受限访问权限的用户提供的网络（例如企业 LAN 或家庭网络）。
- **受信任网络**。安全的网络，其中的计算机不会受到攻击或未经授权的数据访问尝试。防火墙允许具有此状态的网络内的任何网络活动。

在管理控制台中管理防火墙组件

1. 启动管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 在控制台树中，单击**受管理设备**。
4. 在工作区中，选择**策略**选项卡。
5. 右键单击要配置的策略并选择**属性**。

6. 在“**属性**”窗口中，选择“**关键威胁防护**”>“**防火墙**”。
7. 选中或取消选中“**启用防火墙**”复选框。
8. 在“**防火墙设置**”部分，点击“**设置**”按钮并添加、编辑、删除或更改规则的优先级。
9. 在“**可用网络**”部分，点击“**设置**”按钮并添加、编辑、删除或更改网络的类型。
10. 单击**确定**保存您的更改。
11. 执行以下操作之一以应用策略更改：
    - 单击“**应用**”，保存更改后，仍留在“**属性: <策略名称>**”窗口中。
    - 单击“**确定**”，保存更改后，将关闭“**属性: <策略名称>**”窗口。

在 Web Console 中管理防火墙组件

1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**通信和 Web 保护 → 防火墙**”。
5. 使用“**防火墙**”拨动开关启用或禁用组件。
6. 在“**防火墙设置**”部分，点击“**网络数据包规则**”按钮并添加、编辑、删除或更改规则的优先级。
7. 在“**可用网络**”部分，点击“**网络设置**”按钮并添加、编辑或更改网络的类型。
8. 保存您的更改。

管理 Kaspersky Endpoint Security 应用程序中的防火墙组件

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在“**基本**”选项卡上的“**防火墙**”区域中，选中或取消选中“**启用防火墙**”复选框。
3. 如果需要，请单击“**设置**”按钮并配置防火墙设置：
   - 在“**网络数据包规则**”选项卡上，您可以添加、编辑、删除或更改规则的优先级。
   - 在“**可用网络**”选项卡上，您可以添加、编辑或更改网络的类型。

因此，如果启用了防火墙，Kaspersky Endpoint Security 会控制网络活动并阻止对您计算机的未经授权的网络连接。

查看防火墙报告

1. 在菜单栏中，选择**保护** > **报告**。
   将会打开**报告**窗口。
2. 打开“**防火墙**”选项卡。

行为检测

行为检测组件接收有关计算机上应用程序操作的数据，并将此信息提供给其他保护组件以提高其性能。行为检测组件使用应用程序的行为流签名 (BSS)。如果应用程序的活动与行为流签名匹配，Kaspersky Endpoint Security 将执行所选的响应操作。基于行为流签名的 Kaspersky Endpoint Security 功能为计算机提供了主动防御。

默认情况下，行为检测处于启用状态并以卡巴斯基专家推荐的模式运行。如有必要，您可以禁用行为检测。

使用 Web Console 启用/禁用行为检测

1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**主机威胁防护 → 行为分析 → 行为检测**”部分。
5. 使用“**行为检测**”拨动开关启用或禁用组件。
6. 如果启用了行为检测，请选择在检测到恶意软件活动时执行的以下任一操作：
   - **阻止**

     如果选择此选项，Kaspersky Endpoint Security 应用程序会在检测到恶意活动时终止应用程序。
   - **删除**

     如果选择此选项，当检测到恶意活动时，Kaspersky Endpoint Security 应用程序会删除恶意应用程序的可执行文件并在备份区中创建该文件的备份副本。
   - **提示操作**

     如果选择此选项，当检测到恶意活动时，Kaspersky Endpoint Security 应用程序将显示一个通知窗口，其中包含有关恶意对象的信息，并提示用户选择 Kaspersky Endpoint Security 应用程序要采取的操作。可用的操作可能因对象的状态而异。
7. 如果启用了行为检测和共享文件夹外部加密防护，请选择在检测到外部加密时要执行的以下操作之一：
   - **通知**

     如果选择此选项，在检测到尝试修改共享文件夹中的文件时，Kaspersky Endpoint Security 应用程序会将有关此尝试的信息添加到活动威胁列表中，在本地应用程序报告中添加条目，并将有关检测到的恶意活动的信息发送到 Kaspersky Security Center。

- **阻止攻击设备**

  如果选择此选项，当 Kaspersky Endpoint Security 应用程序检测到尝试修改共享文件夹中的文件时，会阻止启动恶意活动的会话访问文件修改（只读），并创建修改文件的备份副本。

8. 保存您的更改。

使用管理控制台启用/禁用行为检测

1. 启动管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 在控制台树中，单击**受管理设备**。
4. 在工作区中，选择**策略**选项卡。
5. 右键单击要配置的策略并选择**属性**。
6. 在**"属性"**窗口中，选择**高级威胁防护** > **行为检测**
7. 选中或取消选中"**启用行为检测**"复选框。
8. 如有必要，在**检测到恶意软件活动时的操作**部分中，选择检测到恶意软件活动时要执行的操作。
9. 单击**确定**保存您的更改。
10. 执行以下操作之一以应用策略更改：

    - 单击"**应用**"，保存更改后，仍留在"**属性: <策略名称>**"窗口中。
    - 单击"**确定**"，保存更改后，将关闭"**属性: <策略名称>**"窗口。

使用 Kaspersky Endpoint Security 应用程序启用/禁用行为检测

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在"**高级**"选项卡的"**行为检测**"部分中，选中或取消选中"**启用行为检测**"复选框。
3. 如果选中**启用行为检测**复选框，请选择在检测到恶意软件活动时要执行的以下操作之一：

   - **阻止**

     如果选择此选项，Kaspersky Endpoint Security 应用程序会在检测到恶意活动时终止应用程序。

   - **删除**

     如果选择此选项，当检测到恶意活动时，Kaspersky Endpoint Security 应用程序会删除恶意应用程序的可执行文件并在备份区中创建该文件的备份副本。

   - **提示操作**

     如果选择此选项，当检测到恶意活动时，Kaspersky Endpoint Security 应用程序将显示一个通知窗口，其中包含有关恶意对象的信息，并提示用户选择 Kaspersky Endpoint Security 应用程序要采取的操作。可用的操作可能因对象的状态而异。

因此，如果启用行为检测，Kaspersky Endpoint Security 将使用行为流签名来分析操作系统中应用程序的活动。

重要提示：除非绝对必要，否则我们不建议禁用行为检测，因为这样做会降低保护组件的有效性。为了检测威胁，保护组件可能会请求行为检测组件收集的数据。

扫描

文件威胁防护和 Web 威胁防护提供实时计算机保护。我们也建议您定期扫描计算机，以检查是否存在恶意软件和其他计算机安全威胁。执行计算机扫描对于防止未被保护组件检测到的恶意软件的传播十分必要。

Kaspersky Endpoint Security 包含以下内置扫描任务：

- **全盘扫描**。
  计算机内存、启动对象和所有内部磁盘的恶意软件扫描。
- **快速扫描**。
  仅对计算机的关键区域执行恶意软件扫描：内存、启动对象和系统文件夹。
- **自定义扫描**。
  对指定对象（文件、文件夹、内部磁盘或可移动磁盘）执行恶意软件扫描。
- **外部磁盘扫描**
  当计算机连接到外部磁盘时，将执行外部磁盘恶意软件扫描。

当应用程序执行病毒扫描时，将通过特征码分析识别恶意对象。除特征码分析外，Kaspersky Endpoint Security 还使用启发式分析和其他扫描技术。

“**扫描**”窗口显示有关每个正在运行的扫描任务的进度（完成百分比和剩余时间）以及扫描历史记录（100 个最近的扫描任务）的信息。

开始全盘扫描和快速扫描任务

1. 在主应用程序窗口的侧边栏上，单击**扫描** 。
   将会打开**扫描**窗口。
2. 在“**扫描**”窗口中，单击“**全盘扫描**”或“**快速扫描**”按钮。

扫描任务开始。

启动自定义扫描任务

1. 在主应用程序窗口的侧边栏上，单击**扫描** 。
   将会打开**扫描**窗口。
2. 要启动**自定义扫描**任务，请执行以下操作之一：
   - 将文件或文件夹拖到该窗口中。
   - 单击**选择**按钮并打开文件或文件夹。

扫描任务开始。

停止扫描任务

1. 在主应用程序窗口的侧边栏上，单击**扫描** 。
   将会打开**扫描**窗口。
2. 在“**扫描**”窗口中，单击您想要停止的扫描任务旁边的停止按钮（ ）。
   将打开确认对话框。
3. 在确认对话框中，单击**停止**。

扫描任务将停止。

您可以安排全盘扫描或快速扫描任务。

从扫描窗口计划扫描任务

1. 在主应用程序窗口的侧边栏上，单击**扫描** 。
   将会打开**扫描**窗口。
2. 单击**计划扫描**。
   将会打开一个对话框，您可以在其中设置计划。
3. 选中**全盘扫描**或**快速扫描**复选框。
4. 指定扫描频率和扫描开始时间。
5. 单击**确定**。

从设置窗口计划扫描任务

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**扫描**选项卡上，单击**计划**。
3. 在打开的窗口中，选择您要按计划扫描的任务名称旁边的复选框。
4. 配置扫描任务频率和时间。
5. 单击**确定**保存更改。

当计算机连接到外部磁盘时，Kaspersky Endpoint Security 应用程序将会自动开始扫描磁盘、提示扫描或不执行任何操作。您可以在外部磁盘扫描任务的设置中选择一个选项。

选择当计算机连接到外部磁盘时，Kaspersky Endpoint Security 应用程序执行的操作

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在“**扫描**”选项卡左侧的列表中，选择“**外部磁盘扫描**”。
3. 在“**连接了外部磁盘时**”部分中，选择连接外部磁盘时 Kaspersky Endpoint Security 执行的操作。

全盘扫描和快速扫描任务已包含扫描范围。在执行全盘扫描任务时，Kaspersky Endpoint Security 应用程序将扫描计算机的内存、启动对象和所有内部磁盘。在执行快速扫描任务时，应用程序将扫描计算机内存、启动对象和系统文件夹。您可以更改快速扫描任务的扫描范围。

注意：您可以跳过对只读系统卷的扫描以显著降低扫描时间。默认下，Kaspersky Endpoint Security 在执行快速扫描任务时不扫描只读系统卷，但在执行全盘扫描任务时扫描只读系统卷。

注意：Kaspersky Endpoint Security 不会扫描位于 OneDrive 或 iCloud 存储或者其他云存储中的文件。请将这些文件排除在扫描范围之外。否则，扫描任务可能会以“*受感染文件未删除*”错误结束。

启用/禁用对只读系统卷的扫描

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**扫描**选项卡左侧的列表中，选择**全盘扫描**或**快速扫描**任务。
3. 在**优化**区域中，取消选中/选中**跳过扫描只读系统卷**复选框。

重要：优化可能由于安全原因而禁用。

在快速扫描任务的扫描范围中添加/删除文件或文件夹

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**扫描**选项卡左侧的列表中，选择**快速扫描**任务。
3. 在**扫描范围**区域中，单击**编辑**。
   将会打开一个窗口，其中的对象列表位于快速扫描任务的扫描范围。
4. 编辑扫描范围对象的列表：
   - 向快速扫描任务的扫描范围添加文件或文件夹：
     a. 单击 +。
        将会出现一个弹出菜单，可在其中选择要添加到扫描范围中的对象。
     b. 选择**文件和文件夹**项。
        将会打开一个可在其中选择文件或文件夹的对话框。
     c. 选择您想要添加到快速扫描任务的扫描范围中的文件或文件夹。
     d. 单击**打开**。

- 从快速扫描任务的扫描范围中删除文件或文件夹：

  a. 选择您想要删除的对象。

  b. 将所选对象从窗口中拖出或单击 –。

5. 单击**保存**。

将默认快速扫描列表上的对象添加到快速扫描任务的扫描范围

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**扫描**选项卡左侧的列表中，选择**快速扫描**任务。
3. 在**扫描范围**区域中，单击**编辑**。
   将会打开一个窗口，其中包含扫描范围对象的列表。
4. 单击 +。
   将会出现一个弹出菜单，可在其中选择要添加到扫描范围中的对象。
5. 在弹出菜单中，选择要添加到扫描范围中的对象（例如，**内存**）。
6. 单击**确定**。

禁用快速扫描任务扫描范围中的对象的保护

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**扫描**选项卡左侧的列表中，选择**快速扫描**任务。
3. 在**扫描范围**区域中，单击**编辑**。
   将会打开一个窗口，其中包含扫描范围对象的列表。
4. 在扫描范围对象列表中，取消选中对象旁边的复选框。
5. 单击**确定**。

如果在文件中检测到威胁，应用程序将显示一个通知并对此对象执行指定的操作。您可以修改检测到对象时要执行的操作。

选择 Kaspersky Endpoint Security 在检测到受感染文件后执行的操作

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**扫描**选项卡上，选择任务列表中的一项任务。
3. 在**操作**区域中，选择应用程序在检测到受感染文件后执行的操作。

在清除或删除受感染文件之前，Kaspersky Endpoint Security 会在备份中保存该文件的副本，以便您在必要时恢复原始文件。

有关扫描任务的结果和所有已检测到的对象的信息记录在报告中。

注意：如果运行恶意软件扫描任务时遇到任何错误，请重启该任务。如果重新尝试运行扫描仍然导致错误，请与卡巴斯基技术支持联系。

查看扫描任务报告

1. 在菜单栏中，选择**保护** > **报告**。
   将会打开**报告**窗口。
2. 打开**扫描**选项卡。

更新任务

及时更新应用程序数据库可确保您的计算机始终处于受保护状态。文件威胁防护、Web 威胁防护和扫描任务使用应用程序数据库来检测并清除您的计算机上的恶意软件。应用程序数据库会定期更新并加入不同类型的威胁和清除威胁的方法，因此定时更新数据库非常重要。

Kaspersky Endpoint Security 将从卡巴斯基更新服务器下载应用程序数据库和新的应用程序模块，并将它们安装到您的计算机。Kaspersky Endpoint Security 也可以使用分发点、本地文件夹或其他 Web 服务器。

注意：连接到更新服务器和下载更新需要访问互联网。如果通过代理服务器连接到互联网，则您可能需要配置网络设置。

可以采用以下方法之一下载应用程序数据库更新：

- **自动**。Kaspersky Endpoint Security 会定期检查卡巴斯基更新服务器上的更新。如果更新服务器上存在新的更新，Kaspersky Endpoint Security 将在后台下载此更新，并将其安装到您的计算机。默认启用此选项。
- **手动**。您可以随时手动检查 Kaspersky Endpoint Security 更新。

启用/禁用自动下载 Kaspersky Endpoint Security 数据库更新

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**更新**选项卡的**数据库**区域中，选中/取消选中**自动下载更新**复选框。

检查 Kaspersky Endpoint Security 数据库更新

1. 在主应用程序窗口的侧边栏上，单击**更新** 。
   将会打开**更新**窗口。
2. 单击**更新**。

应用程序开始更新数据库。

您也可以用以下方法之一启动更新任务：

- 单击应用程序图标并选择**更新**。
- 在菜单栏中，选择**保护** > **更新**。

更新过程中，应用程序数据库和模块将与更新服务器上当前可用的应用程序数据库和模块进行对比。如果计算机上已经安装了最新版本的数据库，则**更新**窗口将显示一条消息，告知您应用程序数据库为最新版本。如果应用程序版本和应用程序数据库与更新服务器上当前可用的应用程序版本和数据库不一致，将仅在计算机上下载和安装缺少的更新组件。应用程序数据库的增量更新所用时间更短，所需的 Web 流量也更少。

如果通过代理服务器连接到互联网，则您可以配置代理服务器连接设置。Kaspersky Endpoint Security 将使用这些设置更新应用程序数据库并下载应用程序模块更新。

配置与代理服务器的连接

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 选择**更新**选项卡。
3. 在**代理**区域中，选中**使用代理服务器**复选框并单击**设置**。
   将打开一个窗口，您可以在其中配置代理服务器连接设置。
4. 配置与代理服务器的连接。
5. 单击**保存**以保存对代理服务器连接设置所做的更改。

在更新应用程序数据库之前，Kaspersky Endpoint Security 会创建这些应用程序数据库的副本，以便必要时可执行回滚。如果新版本的应用程序数据库包含错误的特征码，导致 Kaspersky Endpoint Security 阻止安全应用程序，则回滚功能将很有用。

注意：如果 Kaspersky Endpoint Security 数据库损坏，我们建议您启动更新以下载并安装最新版本的应用程序数据库。

回滚到上次更新

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 选择**更新**选项卡。
3. 在**回滚**区域中，单击**回滚更新**。

Kaspersky Endpoint Security 将在**报告**窗口提供有关更新任务结果的详细报告。

查看更新任务报告

1. 在菜单栏中，选择**保护** > **报告**。
2. 将会打开**报告**窗口。
3. 选择**数据库更新**选项卡。

注意：在美国境内，本软件中将不再提供更新功能（包括提供反恶意软件签名更新和代码库更新）以及 KSN 功能。

本地任务

外部磁盘扫描任务

Kaspersky Endpoint Security 可以扫描您运行或复制的所有文件，即使该文件位于外部磁盘上。为了防止恶意软件的传播，您可以配置外部磁盘连接到设备时的自动扫描。

可以配置以下外部磁盘扫描设置：

- **当连接外部磁盘时 Kaspersky Endpoint Security 执行的操作。**

  扫描

  如果选择此选项，Kaspersky Endpoint Security 将启动对所连接的外部磁盘的恶意软件扫描任务。

  默认选择此选项。

  什么都不做

  如果选择此选项，Kaspersky Endpoint Security 将不会扫描连接的外部磁盘。

- **Kaspersky Endpoint Security 在检测到恶意对象时执行的操作。**

  清除，无法清除则删除

  如果选择此选项，Kaspersky Endpoint Security 阻止访问受感染的对象，并尝试在未请求用户确认的情况下对其进行清除。

  如果对象被清除，Kaspersky Endpoint Security 将其以原始文件名保存在原始位置。如果清除失败，Kaspersky Endpoint Security 将删除无法清除的受感染对象。

  默认选择此选项。

  提示操作

  如果选择此选项，Kaspersky Endpoint Security 将显示一个通知窗口，其中包含有关恶意对象的信息，并提示用户选择 Kaspersky Endpoint Security 要采取的操作。可用的操作可能因对象的状态而异。

您可以在管理控制台、Web Console 或 Kaspersky Endpoint Security 应用程序中配置外部磁盘扫描。

如何在管理控制台 (MMC) 中配置外部磁盘扫描

1. 启动 Kaspersky Security Center 管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 在控制台树中，单击**受管理设备**。
4. 在工作区中，选择**策略**选项卡。
5. 右键单击要配置的策略并选择**属性**。
6. 在“**属性**”窗口中，选择“**本地任务**” > “**外部磁盘扫描**”。
7. 配置任务设置。
8. 单击**确定**保存您的更改。

如何在 Web Console 和云控制台中配置运行外部磁盘扫描

1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**主机威胁防护 → 可移动驱动器扫描**”。
5. 使用“**可移动驱动器扫描**”拨动开关启用或禁用组件。
6. 保存您的更改。

如何在应用程序界面中配置运行外部磁盘扫描

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在“**扫描**”选项卡左侧的列表中，选择“**外部磁盘扫描**”。
3. 在“**连接了外部磁盘时**”部分中，选择连接外部磁盘时 Kaspersky Endpoint Security 执行的操作。

备份

在清除过程中，有时无法保持受感染文件的完整性。如果已清除的文件包含重要信息，且这些信息在清除之后部分或完全无法访问，您可以从备份中恢复原始文件。

备份副本 是在清除或删除文件时创建的危险文件的副本。它存储在备份中。

备份 是一个特殊存储区，包含清除过程中被删除或修改的文件的备份副本。备份的主要功能是允许用户随时恢复原始文件。备份中的文件以特殊格式保存，对计算机不具有危险性。

查看备份内容

1. 在菜单栏中，选择**保护** > **已检测到的对象**。
   将打开**已检测到的对象**窗口。
2. 在**备份**区域中，查看备份文件列表。

您可以从备份中恢复或删除文件的备份副本。

从备份中恢复文件的备份副本

1. 在菜单栏中，选择**保护** > **已检测到的对象**。
   将打开**已检测到的对象**窗口。
2. 在**备份**区域中，单击要恢复的文件旁边的 ⋯。
   将打开弹出菜单。
3. 选择**恢复文件**。
   将打开一个窗口，用于指定文件名、标签和要将文件恢复到的文件夹。默认已指定原始文件名和位置。
4. 指定文件名和要将文件恢复到的文件夹。
5. 单击**保存**。

   应用程序将使用指定名称将该文件恢复到指定位置。

在恢复文件后，您需要立即对其进行恶意软件扫描。或许使用更新后的数据库可清除该对象而不会破坏其完整性。

重要：建议您不要恢复文件的备份副本，除非还原它们是绝对必要的，因为这样做可能会导致计算机感染。

从备份中删除文件的备份副本

1. 在菜单栏中，选择**保护** > **已检测到的对象**。
   将打开**已检测到的对象**窗口。
2. 在**备份**区域中，执行以下操作：
   - 要删除文件的所有备份副本，请单击**删除全部**。
   - 要删除所选备份副本，请单击该备份副本旁边的 ⋯，然后选择**删除备份副本**。

默认情况下，文件在备份中的存储期限为 30 天。当此期限到期时，将删除这些文件。您可以更改文件在备份中的最长存储期限或删除存储期限限制。

配置文件在备份中的存储期限

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**威胁**选项卡的**备份**区域中，选中**在此天数后删除备份对象 <数字> 天**复选框，并指定文件在备份中的存储期限，超过此期限后，将自动删除该文件。

报告

您可以查看 Kaspersky Endpoint Security 报告，所有检测到的对象均列出在**已处理的对象**选项卡上。系统事件显示在**系统事件**选项卡上。此外，还将为以下各个应用程序组件创建单独的详细报告：文件威胁防护、Web 威胁防护、网络威胁防护、行为检测、扫描以及更新任务。

打开报告窗口

在菜单栏中，选择**保护** > **报告**。

Kaspersky Endpoint Security 可以保存文本格式的报告。如果应用程序组件或任务出现您无法自行修复的错误，并且需要卡巴斯基技术支持的帮助，则此功能可能会发挥作用。在这种情况下，可将文本格式的报告发送给卡巴斯基技术支持，以便我们的专家能够研究该问题并尽快修复。

将 Kaspersky Endpoint Security 组件报告或任务报告导出到文本文件

1. 在菜单栏中，选择**保护** > **报告**。
   将会打开**报告**窗口。
2. 在左侧窗格中，选择包含所需报告的选项卡。
3. 在右上角，单击 。
4. 在打开的窗口中，指定报告的文件名、标签和目标文件夹。
5. 单击**保存**。

默认情况下，Kaspersky Endpoint Security 不在报告中记录信息事件。您可以允许记录信息事件。

允许在报告中记录信息事件

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**界面**选项卡的**报告**区域中，选中**记录非关键事件**复选框以接收有关 Kaspersky Endpoint Security 信息事件的通知。

Managed Detection and Response

Managed Detection and Response 组件在 Kaspersky Endpoint Security 版本 11.2 中添加。该组件与 Kaspersky Managed Detection and Response 解决方案交互。*Kaspersky Managed Detection and Response (MDR)* 持续搜索、检测和消除针对您组织的威胁。对于该解决方案如何工作的详情，请参考 *Kaspersky Managed Detection and Response 帮助*。

当与 Kaspersky Managed Detection and Response 交互时，应用程序允许您执行以下功能：

- 使用 BLOB 配置文件激活 Managed Detection and Response。
- 从 Kaspersky Managed Detection and Response 执行命令。
- 发送遥测数据到 Kaspersky Managed Detection and Response 以检测威胁。

Managed Detection and Response 组件具有以下附加需求：

- macOS 14 或更高版本
- 基于 Intel 的 Mac、Apple silicon
- 激活的 Kaspersky Endpoint Security 授权许可

您必须启用以下组件以便 Managed Detection and Response 正常工作：

- 文件威胁防护
- Web 威胁防护
- 邮件威胁防护

启用这些组件是强制性的。否则，Kaspersky Managed Detection and Response 将无法正常工作，因为它无法接收所需的遥测数据。

此外，Kaspersky Managed Detection and Response 还使用从其他应用程序组件接收的数据。启用这些组件是可选的。提供额外数据的组件包括：

- 行为检测

与 Kaspersky Managed Detection and Response 整合

与 Kaspersky Managed Detection and Response 整合包含以下步骤：

1. **配置卡巴斯基安全网络代理服务器**

   卡巴斯基安全网络代理服务器通过管理服务器（而不是直接交换）促进计算机和卡巴斯基安全网络云服务基础架构之间的数据交换。

   在管理服务器属性中加载卡巴斯基安全网络配置文件。卡巴斯基安全网络配置文件位于 MDR 配置文件的 ZIP 压缩包。您可以在 Kaspersky Managed Detection and Response 控制台获取 ZIP 压缩包。关于配置卡巴斯基安全网络代理服务器的详情，请参考 *Kaspersky Security Center 帮助*。

   这样，Kaspersky Endpoint Security 将使用私有 KSN 决定文件、应用程序和网站的信誉。“*基础设施：卡巴斯基私人安全网络*”操作状态将在“卡巴斯基安全网络”区域的策略设置中指示。

   将私有 KSN 与 Kaspersky Managed Detection and Response 配合使用可以确保遥测数据被发送到 GDPR (General Data Protection Regulation) 反馈服务器。如果未使用私有 KSN，遥测数据可以被发送到全球 KSN。这可能违反您的国家法律。

   重要：您必须启用扩展 KSN 模式以便 Managed Detection and Response 正常工作。

2. **激活 Kaspersky Managed Detection and Response**

您可以使用以下方法在端点设备上激活 Managed Detection and Response 组件：

- **使用 Kaspersky Endpoint Security 应用程序中的激活码进行激活。**

  1. 打开主应用程序窗口。
  2. 在主应用程序窗口的侧边栏上，单击“**授权许可**”。

     这将打开“**授权许可**”窗口。
  3. 在“**授权许可**”窗口中，输入您在购买时收到的激活码。

     注意：激活码是一个由 20 个拉丁字母和数字组成的唯一组合，采用 xxxxx-xxxxx-xxxxx-xxxxx 形式。
  4. 单击**激活**。

     应用程序将连接到卡巴斯基激活服务器并发送激活码以验证真伪。如果已成功验证激活码，应用程序将自动接收并添加授权许可密钥。

     注意：您可能需要填写注册表，具体取决于收到的激活码。

  如果激活码验证失败，则会显示相应的通知。此时，请联系向您提供此激活码的软件供应商。

- **使用 BLOB 文件激活。**

  在 Kaspersky Endpoint Security 策略中加载 BLOB 配置文件（参见以下说明）。BLOB 文件包含客户端 ID 和 Kaspersky Managed Detection and Response 授权许可信息。BLOB 文件位于 MDR 配置文件的 ZIP 压缩包。您可以在 Kaspersky Managed Detection and Response 控制台获取 ZIP 压缩包。对于 BLOB 文件的详情，请参考 *Kaspersky Managed Detection and Response 帮助*。

  在管理控制台（MMC）激活 Kaspersky Managed Detection and Response

  1. 启动 Kaspersky Security Center 管理控制台。
  2. 最大化**管理服务器 <服务器名称>** 节点。
  3. 在控制台树中，单击**受管理设备**。
  4. 在工作区中，选择**策略**选项卡。
  5. 右键单击要配置的策略并选择**属性**。
  6. 在**属性**窗口，选择 **Detection and Response** > **Managed Detection and Response**。
  7. 选择**启用 Managed Detection and Response** 复选框。
  8. 在**MDR 配置文件**区域，单击**导入**并选择在 Kaspersky Managed Detection and Response 控制台接收的 BLOB 文件。该文件具有 .P7 扩展名。
  9. 单击**确定**保存您的更改。

在 Web Console 和云控制台激活 Kaspersky Managed Detection and Response

1. 在 Web Console 的主窗口，选择**设备** > **策略和配置文件**。
2. 单击 Kaspersky Endpoint Security for Mac 策略名称。
3. 策略属性窗口打开。
4. 选择**应用程序设置**选项卡。
5. 选择 **Detection and Response** > **Managed Detection and Response**。
6. 开启 **Managed Detection and Response** 切换开关。
7. 单击**导入**并选择在 Kaspersky Managed Detection and Response 控制台中获取的 BLOB 文件。该文件具有 .P7 扩展名。
8. 保存您的更改。

结果，Kaspersky Endpoint Security 将检查 BLOB 文件。BLOB 文件验证包括检查数字签名和授权许可条款。如果 BLOB 文件验证成功，Kaspersky Endpoint Security 将加载该文件并在下一次与 Kaspersky Security Center 同步时将其发送到计算机。

- **使用"添加密钥"任务激活**。

  - **在管理控制台（MMC）激活 Kaspersky Managed Detection and Response**

    1. 在"**选择任务类型**"窗口中，最大化 **Kaspersky Endpoint Security for Mac 12.2.1** 节点。
    2. 要创建用于添加密钥的任务，请选择**添加密钥**。
    3. 在**应用程序激活**窗口中，执行以下操作：

       a. 从 Kaspersky Security Center 存储中选择激活码或密钥，或者添加您的计算机上存储的密钥文件。

       b. 要将指定的密钥添加为备用密钥，请选中**添加为备用密钥**复选框。
       在当前激活密钥到期时，备用密钥将成为激活密钥。

       所指定密钥的相关信息（密钥、密钥类型和到期日期）显示在**应用程序激活**窗口中。

    4. 在选择要对其分配任务的设备窗口中，选择用于指定客户端计算机的方式：

       - 要从管理服务器检测到的网络计算机中进行选择，请选择**选择管理服务器检测到的网络设备**选项。
       - 要手动指定计算机的 IP 地址或从文件导入计算机的 IP 地址，请选择**手动指定设备地址或从列表中导入地址**选项。
       - 要为基于预设条件的设备分类创建任务，请选择**将任务分配给设备分类**选项。
       - 要从特定管理组中选择计算机，请选择**将任务分配给管理组**选项。

5. 在打开的窗口（**选择设备**、**设备分类**或**选择管理组**，具体取决于在上一步骤中选择的选项）中，选择客户端计算机，指定计算机 IP 地址，指定计算机分类，或选择要将任务应用到的管理组。

   注意：对于本地任务或组任务，可忽略此步骤。

6. 在**配置任务计划**窗口的**计划开始**下拉列表中，选择启动模式。

7. 如有必要，配置计划任务以自动启动任务（通过指定任务开始日期和时间）。

8. 如果希望运行应用程序未能按计划启动的任务（例如，由于计算机在计划时间已关机），请选中**运行错过的任务**复选框。

   当阻止任务启动的障碍消除后，Kaspersky Endpoint Security 将启动该任务。

9. 如果希望 Kaspersky Security Center 自动确定不同计算机上的任务启动间隔，请选中**自动随机设置任务启动延迟时间**复选框。

   这有助于降低 Kaspersky Security Center 管理服务器的负荷。

10. 要手动设置不同计算机上的任务启动间隔，请选中**在以下时间间隔内随机设置任务启动延迟时间（分钟）**复选框。

    这有助于降低 Kaspersky Security Center 管理服务器的负荷。

11. 在**定义任务名称**窗口的**名称**字段中，为正在创建的任务输入名称。

1. 在**完成任务创建**窗口中，执行以下操作：

   a. 如何希望在向导完成后立即启动该任务，请选中**向导完成时运行任务**复选框。

   b. 单击**完成**以关闭向导。

- **在 Web Console 和云控制台激活 Kaspersky Managed Detection and Response**

1. 在 Web Console 的主窗口，选择“**资产（设备）**”>“**任务**”。

   任务列表打开。

2. 单击“**添加**”。

   将启动**新任务向导**。

3. 配置任务设置：

   a. 在“**应用程序**”下拉列表中，选择 Kaspersky Endpoint Security for Mac (12.2.1)。

   b. 在“**任务类型**”下拉列表中，选择“**添加文件**”。

   c. 在“**任务名称**”字段中，输入简短描述。

   d. 选择以下选项之一：

   - **将任务分配给管理组**

     该任务被分配给管理组中包含的设备。您可以指定一个现有组，也可以创建一个新组。

     例如，如果消息特定于特定管理组中的设备，您可能希望使用此选项来运行向用户发送消息的任务。

如果将任务分配给管理组，则**"安全"**选项卡不会显示在任务属性窗口中，因为组任务受其适用的组的安全设置约束。

- **手动指定设备地址或从列表中导入地址**

  您可以指定要分配任务的设备的 NetBIOS 名称、DNS 名称、IP 地址和 IP 子网。

  您可能希望使用此选项为特定子网执行任务。例如，您可能想要在会计的设备上安装某个应用程序，或者扫描子网中可能被感染的设备。

- **将任务分配给设备分类**

  该任务被分配给设备分类中包含的设备。您可以指定其中一个现有分类。

  例如，您可能希望使用此选项在具有特定操作系统版本的设备上运行任务。

4. 根据选定的任务范围选项选择设备。
5. 从列表中选择授权许可密钥。如果列表中没有合适的授权许可，您可以将新的授权许可密钥添加到管理服务器存储库中。
6. 输入您想要使用其权限来运行该任务的用户的账户凭据。单击**下一步**。

   注意：默认情况下，Kaspersky Endpoint Security 以系统用户账户 (root) 启动任务。

7. 在"**完成任务创建**"步骤，单击"**完成**"按钮创建任务并关闭向导。

   如果您启用了"**创建完成时打开任务详细信息**"选项，则会打开任务设置窗口。在此窗口中，您可以检查任务参数、修改任务参数或配置任务启动计划（如果需要）。

8. 单击新任务。

   任务属性窗口打开。

9. 选择"**计划**"选项卡。
10. 配置任务计划。

    注意：确保计算机已打开以运行该任务。

11. 单击**保存**。
12. 要立即运行任务而不考虑配置的计划，请执行以下操作：

    a. 选中任务旁边的复选框。

    b. 单击"**运行**"按钮。

Endpoint Detection and Response Expert (on-premise)

Kaspersky Endpoint Security 支持与 Kaspersky Endpoint Detection and Response 组件整合，作为 Kaspersky Anti Targeted Attack Platform 解决方案的一部分。该解决方案旨在及时检测高级威胁，例如定向攻击、高级持续威胁、零日攻击等。对于该解决方案如何工作的详情，请参考 *Kaspersky Anti Targeted Attack Platform 帮助*。

配置与 Endpoint Detection and Response (KATA) 的整合后，KATA 服务器会接收有关 Kaspersky Endpoint Security 操作中发生的事件的信息、应用程序发现的威胁以及有关处理这些威胁的信息。为了对检测到的威胁做出反应， Kaspersky Endpoint Security 可能会执行在 Kaspersky Anti Targeted Attack Platform Web 界面中启动的任务。

Endpoint Detection and Response Expert (on-premise) 组件具有以下附加需求：

- Kaspersky Anti Targeted Attack Platform 6.0 或更高版本。
- Kaspersky Security Center 14.2 或更高版本。
- 可以在 Kaspersky Security Center 管理控制台 (MMC)、Web Console 或云控制台中配置与 Endpoint Detection and Response Expert (版本 7.1 或更早版本) 的整合。
- 可以在 Kaspersky Security Center 管理控制台 (MMC)、Web Console 或云控制台中配置与 Endpoint Detection and Response Expert (版本 8.0 或后续版本) 的整合。

与 Kaspersky Endpoint Detection and Response (KATA) 整合

与 Kaspersky Endpoint Detection and Response (KATA) 整合包含以下步骤：

1. **安装 Endpoint Detection and Response 组件**

   您可以在安装 Kaspersky Endpoint Security 期间选择 Endpoint Detection and Response 组件。

2. **激活 Endpoint Detection and Response**

   如果您当前的授权许可不支持 Endpoint Detection and Response 组件，您需要单独激活 Kaspersky Endpoint Detection and Response。

   您可以在“**授权许可**”窗口中检查当前授权许可是否支持 Endpoint Detection and Response 功能。

3. **连接到 KATA 服务器**

   Kaspersky Anti Targeted Attack Platform 需要在 Kaspersky Endpoint Security 和 KATA 服务器之间建立受信任连接。要配置受信任连接，您需要使用 TLS 证书。您可以在 Kaspersky Anti Targeted Attack Platform Web 界面中下载 TLS 证书。有关下载证书的详细信息，请参阅 *Kaspersky Anti Targeted Attack Platform 帮助*。

   默认情况下， Kaspersky Endpoint Security 仅检查 KATA 服务器的 TLS 证书。为了使连接更加安全，您可以启用双向验证。要启用双向验证，您需要使用受密码保护的加密容器。有关下载加密容器的详细信息，请参阅 *Kaspersky Anti Targeted Attack Platform 帮助*。

   使用管理控制台将装有 Kaspersky Endpoint Security 的计算机连接到 KATA 服务器

   1. 启动管理控制台。
   2. 最大化**管理服务器 <服务器名称>** 节点。
   3. 在控制台树中，单击**受管理设备**。
   4. 在工作区中，选择**策略**选项卡。

5. 右键单击要配置的策略并选择**属性**。

6. 在"**属性**"窗口，选择 **Detection and Response** > **Endpoint Detection and Response Expert (on-premise)**。

7. 选择"**启用 Endpoint Detection and Response Expert (版本 7.1 或更早版本)**"复选框。

8. 单击"**服务器连接设置**"。

9. 在打开的"**服务器连接设置**"窗口中，配置以下设置：

   - 单击**上传 TLS 证书**以选择将用于与 KATA 服务器建立受信任连接的 TLS 证书。
   - 如果要更改 KATA 服务器响应超时，请在**超时(秒)**字段中指定超时。超时后，Kaspersky Endpoint Security 会尝试连接到其他 KATA 服务器。
   - 如果要使用双向验证，请选中"**使用双向身份验证**"复选框。单击"**加载加密容器**"以选择加密容器文件，并在"**加密容器密码**"字段中输入密码。

10. 单击**保存**。

11. 要添加 KATA 服务器，请单击**添加** 。

12. 在打开的"**KATA 服务器**"窗口中，指定服务器地址和端口，然后单击**保存** 。

13. 单击**确定**保存您的更改。

使用 Web Console 将装有 Kaspersky Endpoint Security 的计算机连接到 KATA 服务器

1. 在 Web Console 的主窗口，选择**设备** > **策略和配置文件**。

2. 单击 Kaspersky Endpoint Security for Mac 策略名称。
   策略属性窗口打开。

3. 选择**应用程序设置**选项卡。

4. 选择 Detection and Response > **Endpoint Detection and Response Expert (on-premise)**。

5. 开启 **Endpoint Detection and Response Expert (on-premise)** 切换开关。

6. 单击"**连接设置**"。

7. 在打开的"**服务器连接设置**"窗口中，配置以下设置：

   - 单击**添加 TLS 证书**以选择将用于与 KATA 服务器建立受信任连接的 TLS 证书。
   - 如果要更改 KATA 服务器响应超时，请在**超时(秒)**字段中指定超时。超时后，Kaspersky Endpoint Security 会尝试连接到其他 KATA 服务器。
   - 如果要使用双向验证，请选中"**使用双向认证**"复选框。单击"**加载加密容器**"以选择加密容器文件，并在"**加密容器密码**"字段中输入密码。

8. 单击**确定**。

9. 要添加 KATA 服务器，请单击**"添加"** 。

10. 在打开的对话框中，指定服务器地址和端口，然后单击**"确定"**。

11. 保存您的更改。

这样，计算机将出现在 Kaspersky Anti Targeted Attack Platform Web 界面中。

Endpoint Detection and Response Optimum

从 12.1 版本开始，Kaspersky Endpoint Security for Mac 包含一个用于 Kaspersky Endpoint Detection and Response Optimum（以下也称为"EDR Optimum"）的内置代理。该解决方案旨在保护企业 IT 基础设施免受高级网络威胁。该解决方案的功能结合了自动检测威胁和对这些威胁做出反应的能力，以抵御包括新漏洞利用、勒索软件、无文件攻击以及使用合法系统工具的方法在内的高级攻击。有关此解决方案的详细信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助。

Kaspersky Endpoint Detection and Response 审查并分析威胁发展，并向*安全人员*或*管理员*提供及时响应所需的潜在攻击信息。Kaspersky Endpoint Detection and Response 在单独的窗口中显示警报详细信息。*警报详细信息*是一种用于查看有关检测到的威胁的全部收集信息的工具。例如，警报详细信息包括计算机上出现的文件的历史记录。有关管理警报详细信息的详细信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助。

注意：您可以在 Web Console 中配置 EDR Optimum 组件。

Endpoint Detection and Response 设置

参数	描述
网络隔离	为响应检测到的威胁，自动将计算机与网络隔离。 当网络隔离打开时，应用程序会切断所有活动连接并阻止计算机上所有新的 TCP/IP 连接。应用程序仅使以下连接保持活动状态： • 网络隔离排除项中列出的连接。 • 由 Kaspersky Endpoint Security 服务启动的连接。 • 由 Kaspersky Security Center 网络代理发起的连接。
自动解锁隔离的计算机于N小时	网络隔离可以在指定时间后自动关闭，也可以手动关闭。默认情况下，Kaspersky Endpoint Security 会在隔离开始 8 小时后关闭网络隔离。
网络隔离排除项	网络隔离排除规则列表。开启网络隔离后，符合规则的网络连接不会被计算机阻止。 要配置网络隔离排除项，您可以使用标准网络配置文件列表。默认情况下，排除项包括包含确保具有 DNS/DHCP 服务器和 DNS/DHCP 客户端角色的设备不间断运行的规则的网络配置文件。您还可以修改标准网络配置文件的设置或手动定义排除项。 **重要提示：**仅当网络隔离响应检测到的威胁而自动打开时，才会应用策略属性中指定的排除项。仅当在 Kaspersky Security Center 控制台或警报详细信息中的计算机属性中手动打开网络隔离时，才会应用计算机属性中指定的排除项。
执行防护	执行防护允许管理可执行文件和脚本的运行，以及打开 office 格式的文件。例如，通过这种方式，您可以阻止执行您认为不安全的应用程序。这样，威胁的蔓延可以被停止。执行防护支持一组脚本解释器。 要使用执行防护组件，您需要添加执行防护规则。执行防护规则是应用程序在对对象执行做出反应时考虑的一组标准，例如在阻止对象执行时。应用程序通过使用 MD5 和 SHA256 哈希算法计算的路径或校验和来识别文件。

参数	描述
执行或打开禁止的对象时的操作	**阻止并写入报告**。在这种模式下，应用程序会阻止执行符合防护规则条件的对象或打开符合防护规则标准的文档。应用程序还会将有关尝试执行对象或打开文档的事件发布到 Kaspersky Security Center 事件日志和统一日志记录系统。 **仅记录事件**。在此模式下，Kaspersky Endpoint Security 会将有关尝试运行符合防护规则条件的可执行对象或打开符合防护规则条件的文档的事件发布到 Kaspersky Security Center 事件日志和统一日志记录系统，但不会阻止运行或打开对象或文档的尝试。默认选择此模式。
Cloud Sandbox	Cloud Sandbox 是一种可以让您检测计算机上的高级威胁的技术。Kaspersky Endpoint Security 自动将检测到的文件转发到 Cloud Sandbox 进行分析。Cloud Sandbox 在隔离的环境中运行这些文件以识别恶意活动并确定其信誉。然后，这些文件的数据被发送到卡巴斯基安全网络。因此，如果 Cloud Sandbox 检测到恶意文件，Kaspersky Endpoint Security 将在检测到此文件的所有计算机上执行适当的操作以消除此威胁。 **注意：** Cloud Sandbox 技术是永久启用的，并且可供所有卡巴斯基安全网络用户使用，无论他们使用何种授权许可类型。

与 Endpoint Detection and Response Optimum 整合

要与 Kaspersky Endpoint Detection and Response 集成，您必须添加 Endpoint Detection and Response Optimum (EDR Optimum) 组件并配置 Kaspersky Endpoint Security。

注意： EDR Optimum 和 Endpoint Detection and Response (KATA) 组件彼此不兼容。

为了使 Endpoint Detection and Response 正常工作，必须满足以下条件：

- Kaspersky Security Center 13.2 或更高版本。在 Kaspersky Security Center 的早期版本中，无法激活 Endpoint Detection and Response 功能。
- Kaspersky Endpoint Detection and Response 管理插件已安装。这是一个用于在 Windows、Mac 和 Linux 操作系统上使用代理的单一插件。使用 Endpoint Detection and Response Optimum 时，您将需要 Kaspersky Endpoint Security 管理插件来创建威胁响应任务，以及需要 EDR 管理插件来查看警报详细信息。
- 作为 Kaspersky Endpoint Security 一部分的 EDR Optimum 组件支持与 Kaspersky Endpoint Detection and Response Optimum 3.0 解决方案的交互。不支持与 Kaspersky Endpoint Detection and Response Optimum 的早期版本进行交互。
- EDR Optimum 可以在 Web Console 中进行管理。
- 应用程序已激活并且其功能受授权许可的保护。
- Endpoint Detection and Response 组件已启用。

与 Kaspersky Endpoint Detection and Response Optimum 整合

与 Kaspersky Endpoint Detection and Response Optimum 整合包含以下步骤：

1. **安装 Endpoint Detection and Response Optimum 组件**

   您可以在安装 Kaspersky Endpoint Security 期间选择 Endpoint Detection and Response 组件。

2. **激活 Endpoint Detection and Response**

   如果您当前的授权许可不支持 Endpoint Detection and Response 组件，您需要单独激活 Kaspersky Endpoint Detection and Response。

   您可以在“**授权许可**”窗口中检查当前授权许可是否支持 Endpoint Detection and Response 功能。

3. **启用 Endpoint Detection and Response 组件**

   您可以在 Kaspersky Endpoint Security for Mac 策略设置中启用或禁用该组件。

   如何在 Web Console 中启用或禁用 Endpoint Detection and Response 组件

   1. 在 Web Console 的主窗口，选择“**资产管理** → **策略**”。
   2. 单击 Kaspersky Endpoint Security 策略的名称。
      策略属性窗口打开。
   3. 选择**应用程序设置**选项卡。
   4. 选择“**Detection and Response**” > “**Endpoint Detection and Response**”。
   5. 开启 **Endpoint Detection and Response Expert (on-premise)** 切换开关。
   6. 保存您的更改。

扫描入侵指标

入侵指标 (IOC)是有关对象或活动的一组数据，表明对计算机进行了未经授权的访问（数据泄漏）。例如，多次尝试登录系统但均未成功，则可能构成入侵指标。“**IOC 扫描**”任务允许查找计算机上的入侵指标并采取威胁响应措施。

Kaspersky Endpoint Security 使用 IOC 文件搜索妥协的指标。IOC 文件是包含应用程序尝试匹配以计算检测结果的指标集的文件。IOC 文件必须符合 IOC 文件的要求。

IOC 扫描任务运行模式

Kaspersky Endpoint Detection and Response 允许您创建标准 IOC 扫描任务来检测泄漏的数据。标准 IOC 扫描任务是在 Web Console 中手动创建和配置的组或本地任务。使用用户准备的 IOC 文件运行任务。如果您想手动添加入侵指标，请阅读 IOC 文件的要求。

创建 IOC 扫描任务

您可以手动创建 IOC 扫描任务：

- 在警报详细信息中（仅适用于 EDR Optimum）。

  *警报详细信息*是一种用于查看有关检测到的威胁的全部收集信息的工具。例如，警报详细信息包括计算机上出现的文件的历史记录。有关管理警报详细信息的详细信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助。

- 使用任务向导。

要创建 IOC 扫描任务：

1. 在 Web Console 的主窗口，选择“**资产（设备）**”>“**任务**”。

   任务列表打开。

2. 单击“**添加**”。

   将启动**新任务向导**。

3. 配置任务设置：

   a. 在“**应用程序**”下拉列表中，选择 Kaspersky Endpoint Security for Mac (12.2.1)。

   b. 在“**任务类型**”下拉列表中，选择“**IOC 扫描**”。

   c. 在“**任务名称**”字段中，输入简短描述。

   d. 在“**选择将分配任务的设备**”块中，选择任务范围。

4. 根据选定的任务范围选项选择设备。

5. 在“**IOC 扫描设置**”部分，加载 IOC 文件以搜索入侵指标。您可以添加 IOC 文件或者根据包含文件哈希或 IP 地址的文件生成 IOC 文件。

   加载 IOC 文件后，您可以查看和编辑 IOC 文件中的指标列表。

   > **注意：**运行任务后不建议添加或删除 IOC 文件。这可能会导致 IOC 扫描结果在任务的先前运行中显示不正确。为了通过新的 IOC 文件搜索入侵指标，建议添加新任务。

6. 配置 IOC 检测的操作：

   - **从网络隔离计算机**。如果选择此选项，Kaspersky Endpoint Security 将计算机与网络隔离，以防止威胁扩散。您可以在“Endpoint Detection and Response 组件设置”中配置隔离的持续时间。

   - **将副本移动到隔离区并删除对象**。如果选择此选项，Kaspersky Endpoint Security 删除在计算机上发现的恶意对象。删除对象之前，Kaspersky Endpoint Security 创建备份副本，以便日后对其进行恢复。Kaspersky Endpoint Security 移动备份副本到隔离区。

   - **运行关键区域扫描**。如果选择此选项，Kaspersky Endpoint Security 将运行快速扫描任务。默认情况下，Kaspersky Endpoint Security 会扫描内存、启动对象和系统文件夹。

7. 转到“**高级**”区域。

8. 选择必须作为任务的一部分进行分析的数据类型（IOC 文档）。

   注意：Kaspersky Endpoint Security 根据加载的 IOC 文件的内容自动为 IOC 扫描任务选择数据类型（IOC 文档）。不建议取消选择数据类型。

   您还可以为以下数据类型配置扫描范围：

   - **进程** - ProcessItem
   - **文件** – FileItem
   - **网络端口** – PortItem
   - **用户账户** – UserItem
   - ARP **表格** – ArpEntryItem
   - **主机** – SystemInfoItem
   - URL – UrlHistoryItem
   - **路由** – RouteEntryItem

9. 单击**确定**。

10. 输入您想要使用其权限来运行该任务的用户的账户凭据。单击**下一步**。

    注意：默认情况下，Kaspersky Endpoint Security 以系统用户账户 (root) 启动任务。

11. 在“**完成任务创建**”步骤，单击“**完成**”按钮创建任务并关闭向导。

    如果您启用了“**创建完成时打开任务详细信息**”选项，则会打开任务设置窗口。在此窗口中，您可以检查任务参数、修改任务参数或配置任务启动计划（如果需要）。

12. 单击新任务。

    任务属性窗口打开。

13. 选择“**计划**”选项卡。

14. 配置任务计划。

    注意：确保计算机已打开以运行该任务。

15. 单击**保存**。

16. 要立即运行任务而不考虑配置的计划，请执行以下操作：

    a. 选中任务旁边的复选框。

    b. 单击“**运行**”按钮。

17. 结果，Kaspersky Endpoint Security 运行搜索以在计算机上查找妥协的指标。您可以在任务属性的“**结果**”部分中查看任务的结果。您可以在任务属性中查看有关检测到的入侵指标的信息：“**应用程序设置**” > “**IOC 扫描结果**”。

注意： IOC 扫描结果保留 30 天。在此时间之后，Kaspersky Endpoint Security 将自动删除最早条目。

将文件移至隔离区

在应对威胁时，Kaspersky Endpoint Detection and Response 可以创建“*将文件移动到隔离区*”任务。这对于尽量减少威胁的后果是必要的。“*隔离区*”是计算机上的一个特殊的本地存储。用户可以隔离其认为对计算机有危险的文件。隔离的文件以加密状态存储，不会威胁设备的安全。Kaspersky Endpoint Security 使用备份区作为文件存储。有关将隔离区作为解决方案的一部分进行管理的详细信息，请参阅“Kaspersky Endpoint Detection and Response Optimum 帮助”。

您可以通过以下方式创建“*将文件移至隔离区*”任务：

- 在警报详细信息中（仅适用于 EDR Optimum）。

  *警报详细信息*是一种用于查看有关检测到的威胁的全部收集信息的工具。例如，警报详细信息包括计算机上出现的文件的历史记录。有关管理警报详细信息的详细信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助。

- 使用任务向导。

  您必须输入文件路径或哈希值（SHA256 或 MD5），或者文件路径和文件哈希值都输入。

“*将文件移至隔离区*”任务具有以下限制：

- 文件大小不得超过 100 MB。
- 您可以在 Web Console 中为 EDR Optimum 配置任务。
- 备份区容量受可用磁盘空间的限制。

要创建“将文件移至隔离区”任务：

1. 在 Web Console 的主窗口，选择“**资产（设备）**”>“**任务**”。

   任务列表打开。

2. 单击“**添加**”。

   将启动**新任务向导**。

3. 配置任务设置：

   a. 在“**应用程序**”下拉列表中，选择 Kaspersky Endpoint Security for Mac (12.2.1)。

   b. 在“**任务类型**”下拉列表中，选择“**将文件移至隔离区**”。

   c. 在“**任务名称**”字段中，输入简短描述。

d. 选择以下选项之一：

- **将任务分配给管理组**

  该任务被分配给管理组中包含的设备。您可以指定一个现有组，也可以创建一个新组。

  例如，如果消息特定于特定管理组中的设备，您可能希望使用此选项来运行向用户发送消息的任务。

  如果将任务分配给管理组，则**"安全"**选项卡不会显示在任务属性窗口中，因为组任务受其适用的组的安全设置约束。

- **手动指定设备地址或从列表中导入地址**

  您可以指定要分配任务的设备的 NetBIOS 名称、DNS 名称、IP 地址和 IP 子网。

  您可能希望使用此选项为特定子网执行任务。例如，您可能想要在会计的设备上安装某个应用程序，或者扫描子网中可能被感染的设备。

- **将任务分配给设备分类**

  该任务被分配给设备分类中包含的设备。您可以指定其中一个现有分类。

  例如，您可能希望使用此选项在具有特定操作系统版本的设备上运行任务。

4. 根据选定的任务范围选项选择设备。

5. 在"**任务范围**"步骤中，指定管理组、具有特定地址的设备或设备分类。
   可用的设置取决于上一步选择的选项。

6. 在文件列表中，单击"**添加**"。
   文件添加向导启动。

7. 在"**请指定要移至隔离区的文件**"下拉列表中，选择其中一个选项并填写必填字段。要添加文件，您必须输入文件的完整路径，或者文件哈希和路径都输入。

8. 如果您希望任务适用于关键系统对象，请选中"**应用于关键系统对象**"复选框。

9. 输入您想要使用其权限来运行该任务的用户的账户凭据。单击**下一步**。

   注意：默认情况下，Kaspersky Endpoint Security 以系统用户账户 (root) 启动任务。

10. 在"**完成任务创建**"步骤，单击"**完成**"按钮创建任务并关闭向导。
    如果您启用了"**创建完成时打开任务详细信息**"选项，则会打开任务设置窗口。在此窗口中，您可以检查任务参数、修改任务参数或配置任务启动计划（如果需要）。

11. 单击新任务。
    任务属性窗口打开。

12. 选择"**计划**"选项卡。

13. 配置任务计划。

> **注意：**确保计算机已打开以运行该任务。

14. 单击**保存**。

15. 要立即运行任务而不考虑配置的计划，请执行以下操作：

    a. 选中任务旁边的复选框。

    b. 单击“**运行**”按钮。

结果，Kaspersky Endpoint Security 将文件移动到隔离区。

如果您尝试隔离当前正在运行的可执行文件，“*将文件移至隔离区*”任务可能会以“*访问被拒绝*”错误结束。为该文件创建一个终止进程任务并重试。

如果您尝试隔离的文件过大，则“*将文件移至隔离区*”任务可能会以“*隔离区存储空间不足*”错误结束。请释放磁盘空间并重试。

获取文件

您可以从用户计算机获取文件。例如，您可以配置获取由第三方应用程序创建的事件日志文件。要获取该文件，您必须创建一个专门的任务。任务执行的结果是，文件被保存在备份区中。您可以使用 Web Console 将此文件从备份区下载到您的计算机。在用户的计算机上，该文件仍保留在其原始文件夹中。

> **重要提示：**文件大小不得超过 100 MB。备份区容量受可用磁盘空间的限制。

要创建“获取文件”任务：

1. 在 Web Console 的主窗口，选择“**资产（设备）**”>“**任务**”。
   任务列表打开。

2. 单击“**添加**”。
   将启动**新任务向导**。

3. 配置任务设置：

   a. 在“**应用程序**”下拉列表中，选择 Kaspersky Endpoint Security for Mac (12.2.1)。

   b. 在“**任务类型**”下拉列表中，选择“**获取文件**”。

   c. 在“**任务名称**”字段中，输入简短描述。

   d. 选择以下选项之一：

   - **将任务分配给管理组**

     该任务被分配给管理组中包含的设备。您可以指定一个现有组，也可以创建一个新组。

例如，如果消息特定于特定管理组中的设备，您可能希望使用此选项来运行向用户发送消息的任务。

如果将任务分配给管理组，则**"安全"**选项卡不会显示在任务属性窗口中，因为组任务受其适用的组的安全设置约束。

- **手动指定设备地址或从列表中导入地址**

  您可以指定要分配任务的设备的 NetBIOS 名称、DNS 名称、IP 地址和 IP 子网。

  您可能希望使用此选项为特定子网执行任务。例如，您可能想要在会计的设备上安装某个应用程序，或者扫描子网中可能被感染的设备。

- **将任务分配给设备分类**

  该任务被分配给设备分类中包含的设备。您可以指定其中一个现有分类。

  例如，您可能希望使用此选项在具有特定操作系统版本的设备上运行任务。

4. 根据选定的任务范围选项选择设备。在"**获取文件**"窗口中，单击"**添加**"。

   "**获取文件**"对话框打开。

5. 在"**指定需要获取的文件**"下拉列表中，选择其中一个选项并填写必填字段。

   要添加文件，您必须输入文件的完整路径，或者文件哈希和路径都输入。

6. 单击**确定**。

   待添加文件的设置将显示在文件列表中。

7. 单击**下一步**。

8. 输入您想要使用其权限来运行该任务的用户的账户凭据。单击**下一步**。

   注意：默认情况下，Kaspersky Endpoint Security 以系统用户账户 (root) 启动任务。

9. 在"**完成任务创建**"步骤，单击"**完成**"按钮创建任务并关闭向导。

   如果您启用了"**创建完成时打开任务详细信息**"选项，则会打开任务设置窗口。在此窗口中，您可以检查任务参数、修改任务参数或配置任务启动计划（如果需要）。

10. 单击新任务。

    任务属性窗口打开。

11. 选择"**计划**"选项卡。

12. 配置任务计划。

    注意：确保计算机已打开以运行该任务。

13. 单击**保存**。

14. 要立即运行任务而不考虑配置的计划，请执行以下操作：

    a. 选中任务旁边的复选框。

    b. 单击“**运行**”按钮。

结果，Kaspersky Endpoint Security 会创建文件的副本并将该副本移至备份区。您可以在 Web Console 中从备份区下载该文件。

删除文件

您可以使用“*删除文件*”任务远程删除文件。例如，您可以在应对威胁时远程删除文件。

要创建“删除文件”任务：

1. 在 Web Console 的主窗口，选择“**资产（设备）**”>“**任务**”。
   任务列表打开。

2. 单击“**添加**”。
   将启动**新任务向导**。

3. 配置任务设置：

    a. 在“**应用程序**”下拉列表中，选择 Kaspersky Endpoint Security for Mac (12.2.1)。

    b. 在“**任务类型**”下拉列表中，选择“**删除文件**”。

    c. 在“**任务名称**”字段中，输入简短描述。

    d. 选择以下选项之一：

    - **将任务分配给管理组**

      该任务被分配给管理组中包含的设备。您可以指定一个现有组，也可以创建一个新组。

      例如，如果消息特定于特定管理组中的设备，您可能希望使用此选项来运行向用户发送消息的任务。

      如果将任务分配给管理组，则**“安全”**选项卡不会显示在任务属性窗口中，因为组任务受其适用的组的安全设置约束。

    - **手动指定设备地址或从列表中导入地址**

      您可以指定要分配任务的设备的 NetBIOS 名称、DNS 名称、IP 地址和 IP 子网。

      您可能希望使用此选项为特定子网执行任务。例如，您可能想要在会计的设备上安装某个应用程序，或者扫描子网中可能被感染的设备。

    - **将任务分配给设备分类**

      该任务被分配给设备分类中包含的设备。您可以指定其中一个现有分类。

      例如，您可能希望使用此选项在具有特定操作系统版本的设备上运行任务。

4. 根据选定的任务范围选项选择设备。

5. 在“**指定需要删除的文件**”下拉列表中，选择其中一个选项并填写必填字段。要添加文件，您必须输入文件的完整路径，或者文件哈希和路径都输入。

6. 如果您希望任务适用于关键系统对象，请选中“**应用于关键系统对象**”复选框。

7. 输入您想要使用其权限来运行该任务的用户的账户凭据。单击**下一步**。

   注意：默认情况下，Kaspersky Endpoint Security 以系统用户账户 (root) 启动任务。

8. 在“**完成任务创建**”步骤，单击“**完成**”按钮创建任务并关闭向导。

   如果您启用了“**创建完成时打开任务详细信息**”选项，则会打开任务设置窗口。在此窗口中，您可以检查任务参数、修改任务参数或配置任务启动计划（如果需要）。

9. 单击新任务。

   任务属性窗口打开。

10. 选择“**计划**”选项卡。

11. 配置任务计划。

    注意：确保计算机已打开以运行该任务。

12. 单击**保存**。

13. 要立即运行任务而不考虑配置的计划，请执行以下操作：

    a. 选中任务旁边的复选框。

    b. 单击“**运行**”按钮。

结果，Kaspersky Endpoint Security 将从计算机删除文件。如果文件被其他进程锁定，则任务显示为“*已完成*”，但只有在计算机重新启动后才会删除文件本身。重启计算机后，确认文件已被删除。

如果您尝试删除当前正在运行的可执行文件，则“*删除文件*”任务可能会以“*访问被拒绝*”错误结束。为该文件创建一个终止进程任务并重试。

启动进程

您可以使用“*启动进程*”任务远程运行文件。

重要提示：您可以在 Web Console 中配置 EDR Optimum 的任务。

要创建“启动进程”任务：

1. 在 Web Console 的主窗口，选择“**资产（设备）**”>“**任务**”。

   任务列表打开。

2. 单击“**添加**”。
将启动**新任务向导**。

3. 配置任务设置：

a. 在“**应用程序**”下拉列表中，选择 Kaspersky Endpoint Security for Mac (12.2.1)。

b. 在“**任务类型**”下拉列表中，选择“**启动进程**”。

c. 在“**任务名称**”字段中，输入简短描述。

d. 选择以下选项之一：

- **将任务分配给管理组**

  该任务被分配给管理组中包含的设备。您可以指定一个现有组，也可以创建一个新组。

  例如，如果消息特定于特定管理组中的设备，您可能希望使用此选项来运行向用户发送消息的任务。

  如果将任务分配给管理组，则**“安全”**选项卡不会显示在任务属性窗口中，因为组任务受其适用的组的安全设置约束。

- **手动指定设备地址或从列表中导入地址**

  您可以指定要分配任务的设备的 NetBIOS 名称、DNS 名称、IP 地址和 IP 子网。

  您可能希望使用此选项为特定子网执行任务。例如，您可能想要在会计的设备上安装某个应用程序，或者扫描子网中可能被感染的设备。

- **将任务分配给设备分类**

  该任务被分配给设备分类中包含的设备。您可以指定其中一个现有分类。

  例如，您可能希望使用此选项在具有特定操作系统版本的设备上运行任务。

4. 根据选定的任务范围选项选择设备。

5. 在“**任务范围**”步骤中，指定管理组、具有特定地址的设备或设备分类。
可用的设置取决于上一步选择的选项。

6. 配置任务设置：

a. 在“**可执行命令**”字段中，指定要在本地设备上执行的命令。

b. 如果需要，请在“**命令行参数(可选)**”字段中指定命令行参数。

c. 如有必要，请在“**工作文件夹路径(可选)**”字段中指定可执行文件的路径。

7. 在“**完成任务创建**”步骤，单击“**完成**”按钮创建任务并关闭向导。
如果您启用了“**创建完成时打开任务详细信息**”选项，则会打开任务设置窗口。在此窗口中，您可以检查任务参数、修改任务参数或配置任务启动计划（如果需要）。

8. 单击新任务。
任务属性窗口打开。

9. 选择“**计划**”选项卡。

10. 配置任务计划。

> **注意：**确保计算机已打开以运行该任务。

11. 单击**保存**。

12. 要立即运行任务而不考虑配置的计划，请执行以下操作：

    a. 选中任务旁边的复选框。

    b. 单击“**运行**”按钮。

结果，Kaspersky Endpoint Security 在静默模式下运行命令并启动进程。您可以在任务属性的“**执行结果**”部分中查看任务的结果。

终止进程

您可以使用“*终止进程*”任务远程终止进程。例如，您可以远程终止使用“启动进程”任务启动的互联网速度测试实用工具。

如果您想禁止运行某个文件，可以配置“执行防护组件”。您可以禁止可执行文件、脚本、office 格式文件的执行。

“*终止进程*”任务具有以下限制：

- 在 Web Console 中只能为 EDR Optimum 配置任务。

要创建“终止进程”任务：

1. 在 Web Console 的主窗口，选择“**资产（设备）**”>“**任务**”。
   任务列表打开。

2. 单击“**添加**”。
   将启动**新任务向导**。

3. 配置任务设置：

    a. 在“**应用程序**”下拉列表中，选择 Kaspersky Endpoint Security for Mac (12.2.1)。

    b. 在“**任务类型**”下拉列表中，选择“**终止进程**”。

    c. 在“**任务名称**”字段中，输入简短描述。

    d. 选择以下选项之一：

    - **将任务分配给管理组**

      该任务被分配给管理组中包含的设备。您可以指定一个现有组，也可以创建一个新组。

      例如，如果消息特定于特定管理组中的设备，您可能希望使用此选项来运行向用户发送消息的任务。

如果将任务分配给管理组，则**"安全"**选项卡不会显示在任务属性窗口中，因为组任务受其适用的组的安全设置约束。

- **手动指定设备地址或从列表中导入地址**

  您可以指定要分配任务的设备的 NetBIOS 名称、DNS 名称、IP 地址和 IP 子网。

  您可能希望使用此选项为特定子网执行任务。例如，您可能想要在会计的设备上安装某个应用程序，或者扫描子网中可能被感染的设备。

- **将任务分配给设备分类**

  该任务被分配给设备分类中包含的设备。您可以指定其中一个现有分类。

  例如，您可能希望使用此选项在具有特定操作系统版本的设备上运行任务。

4. 根据选定的任务范围选项选择设备。
5. 在"**任务范围**"步骤中，指定管理组、具有特定地址的设备或设备分类。

   可用的设置取决于上一步选择的选项。
6. 在向导的此步骤中，在"**请指定应终止其进程的文件**"下拉列表中，选择其中一个选项并填写必填字段。要指定文件，您必须输入文件的完整路径，或者文件哈希和路径都输入。

   注意：如果您为本地设备创建此任务，则可以通过 PID 指定进程。
7. 如果您希望任务适用于关键系统对象，请选中"**应用于关键系统对象**"复选框。
8. 输入您想要使用其权限来运行该任务的用户的账户凭据。单击**下一步**。

   注意：默认情况下，Kaspersky Endpoint Security 以系统用户账户 (root) 启动任务。
9. 在"**完成任务创建**"步骤，单击"**完成**"按钮创建任务并关闭向导。

   如果您启用了"**创建完成时打开任务详细信息**"选项，则会打开任务设置窗口。在此窗口中，您可以检查任务参数、修改任务参数或配置任务启动计划（如果需要）。
10. 单击新任务。

    任务属性窗口打开。
11. 选择"**计划**"选项卡。
12. 配置任务计划。

    注意：确保计算机已打开以运行该任务。
13. 单击**保存**。

14. 要立即运行任务而不考虑配置的计划，请执行以下操作：

    a. 选中任务旁边的复选框。

    b. 单击“**运行**”按钮。

结果，Kaspersky Endpoint Security 将在计算机上终止该进程。例如，如果“*游戏*”应用程序正在运行并且您终止“*游戏*”进程，则该应用程序将关闭而不保存数据。您可以在任务属性的“**结果**”部分中查看任务的结果。

执行防护

执行防护允许管理可执行文件和脚本的运行，以及打开 office 格式的文件。例如，通过这种方式，您可以阻止执行您认为不安全的应用程序。这样，威胁的蔓延可以被停止。执行防护支持一组脚本解释器。

执行防护规则

执行防护使用执行防护规则管理用户对文件的访问。执行防护规则是应用程序在对对象执行做出反应时考虑的一组标准，例如在阻止对象执行时。应用程序通过使用 MD5 和 SHA256 哈希算法计算的路径或校验和来识别文件。

您可以创建执行防护规则：

- 在警报详细信息中（仅适用于 EDR Optimum）。

  *警报详细信息*是一种用于查看有关检测到的威胁的全部收集信息的工具。例如，警报详细信息包括计算机上出现的文件的历史记录。有关管理警报详细信息的详细信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助。

- 使用组策略或本地应用程序设置。您必须输入文件路径或哈希值（SHA256 或 MD5），或者文件路径和文件哈希值都输入。

您还可以使用命令行在本地管理执行防护。

注意： 无法阻止系统关键对象（SCO）的启动。SCO 是操作系统和 Kaspersky Endpoint Security for Mac 应用程序运行所需要的文件。

执行防护规则模式

执行防护组件可以以两种模式工作：

- **仅统计**

  在此模式下，Kaspersky Endpoint Security 会将有关尝试运行符合防护规则条件的可执行对象或打开符合防护规则条件的文档的事件发布到 Kaspersky Security Center 事件日志和统一日志记录系统，但不会阻止运行或打开对象或文档的尝试。默认选择此模式。

- **活动**

  在这种模式下，应用程序会阻止执行符合防护规则条件的对象或打开符合防护规则标准的文档。应用程序还会将有关尝试执行对象或打开文档的事件发布到 Kaspersky Security Center 事件日志和统一日志记录系统。

管理执行防护

重要提示：您只能在 Web Console 中配置组件设置。

为了防止执行：

1. 在 Web Console 的主窗口，选择**设备** > **策略和配置文件**。
2. 单击 Kaspersky Endpoint Security for Mac 策略名称。

   策略属性窗口打开。
3. 选择**应用程序设置**选项卡。
4. 选择“**Detection and Response**” > “**Endpoint Detection and Response**”。
5. 打开“**执行防护**”切换开关。
6. 在“**执行或打开禁止的对象时的操作**”块中，选择组件操作模式：

   - **阻止并写入报告**。在这种模式下，应用程序会阻止执行符合防护规则条件的对象或打开符合防护规则标准的文档。应用程序还会将有关尝试执行对象或打开文档的事件发布到 Kaspersky Security Center 事件日志和统一日志记录系统。
   - **仅记录事件**。在此模式下，Kaspersky Endpoint Security 会将有关尝试运行符合防护规则条件的可执行对象或打开符合防护规则条件的文档的事件发布到 Kaspersky Security Center 事件日志和统一日志记录系统，但不会阻止运行或打开对象或文档的尝试。默认选择此模式。
7. 创建执行防护规则列表：

   a. 单击“**添加**”。

   b. 在打开的对话框中，输入执行防护规则的名称（例如，应用程序 A）。

   c. 在“**类型**”下拉列表中，选择要阻止的对象：**应用程序**、**脚本**、**文档**。

   如果您选择了错误的对象类型，Kaspersky Endpoint Security 不阻止文件或脚本。

   d. 要添加文件，您必须输入文件的哈希值（SHA256 或 MD5）、文件的完整路径，或哈希值和路径都输入。

注意：如果文件位于网络驱动器上，请按以下方式输入文件路径：/Volumes/shared_folder_name/filename。如果文件路径包含网络驱动器盘符，Kaspersky Endpoint Security 不阻止文件或脚本。

a. 单击**确定**。

8. 保存您的更改。

因此，Kaspersky Endpoint Security 会阻止对象的执行：运行可执行文件和脚本，打开 Office 格式文件。但是，即使无法运行脚本，您也可以在文本编辑器中打开该脚本文件。阻止对象执行时，如果在应用程序设置中启用了通知，Kaspersky Endpoint Security 将显示标准通知。

计算机网络隔离

计算机网络隔离允许在检测到入侵指标 (IOC) 时自动将计算机与网络隔离 - 这是自动模式。您可以在调查检测到的威胁时手动打开网络隔离 - 这是手动模式。

启用网络隔离后，应用程序将切断所有活动连接并阻止计算机上除以下连接之外的所有新的 TCP/IP 网络连接：

- 网络隔离排除项中列出的连接。
- 由 Kaspersky Endpoint Security 服务启动的连接。
- 由 Kaspersky Security Center 网络代理发起的连接。

重要提示：您只能在 Web Console 中配置组件设置。

自动网络隔离模式

您可以配置网络隔离在响应 IOC 检测时自动打开。您可以使用组策略配置自动网络隔离模式。

如何配置网络隔离在响应 IOC 检测时自动开启

1. 在 Web Console 的主窗口，选择“**设备**” > “**任务**”。
2. 任务列表打开。
3. 单击 Kaspersky Endpoint Security 的“**IOC 扫描**”任务。
   任务属性窗口打开。
   如有必要，创建“IOC 扫描”任务。
4. 选择**应用程序设置**选项卡。
5. 在“**检测到 IOC 后的操作**”块中，选择“**在发现 IOC 后发出警报并采取响应操作**”选项，然后选择“**从网络隔离计算机 (8 小时)**”复选框。

6. 保存您的更改。

7. 这样，当检测到 IOC 时，应用程序会将计算机与网络隔离，以防止威胁蔓延。

您可以配置网络隔离，使其在指定时间过后自动关闭。默认情况下，应用程序会在打开网络隔离 8 小时后关闭网络隔离。您也可以手动关闭网络隔离（请参阅下面的说明）。关闭网络隔离后，计算机可以不受限制地使用网络。

如何配置在自动模式下关闭计算机网络隔离的延迟

1. 在 Web Console 的主窗口，选择**设备** > **策略和配置文件**。

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口打开。

3. 选择**应用程序设置**选项卡。

4. 选择“**Detection and Response**” > “**Endpoint Detection and Response**”。

5. 在“**网络隔离**”块中，单击“**配置计算机解锁设置**”。

6. 在打开的窗口中，选中“**自动解锁隔离的计算机于**”复选框，并输入自动关闭网络隔离的延迟。

7. 保存您的更改。

手动网络隔离模式

您可以手动打开或关闭网络隔离。您可以在 Kaspersky Security Center 控制台中使用计算机属性配置手动网络隔离模式。

您可以打开网络隔离：

- 在警报详细信息中（仅适用于 EDR Optimum）。

  *警报详细信息*是一种用于查看有关检测到的威胁的全部收集信息的工具。例如，警报详细信息包括计算机上出现的文件的历史记录。有关管理警报详细信息的详细信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助。

- 使用本地应用程序设置。

如何手动打开计算机的网络隔离

1. 在 Web Console 的主窗口，选择“**设备**” > “**受管理设备**”。

2. 选择要配置本地应用程序设置的计算机。

   这将打开计算机属性。

3. 选择“**应用程序**”选项卡。

4. 单击 **Kaspersky Endpoint Security for Mac**。

   这将打开本地应用程序设置。

5. 选择**应用程序设置**选项卡。

6. 选择“**Detection and Response**” > “**Endpoint Detection and Response**”。

7. 在“**网络隔离**”块中，单击“**从网络隔离计算机**”。

您可以配置网络隔离，使其在指定时间过后自动关闭。默认情况下，应用程序会在打开网络隔离 8 小时后关闭网络隔离。关闭网络隔离后，计算机可以不受限制地使用网络。

如何配置手动模式下关闭计算机网络隔离的延迟

1. 在 Web Console 的主窗口，选择“**设备**” > “**受管理设备**”。

2. 选择要配置本地应用程序设置的计算机。
   这将打开计算机属性。

3. 选择“**任务**”选项卡。
   这将显示计算机上可用的任务列表。

4. 选择“**网络隔离**”任务。

5. 选择**应用程序设置**选项卡。

6. 在打开的窗口中，选择关闭网络隔离的延迟。

7. 保存您的更改。

如何手动关闭计算机的网络隔离

1. 在 Web Console 的主窗口，选择“**设备**” > “**受管理设备**”。

2. 选择要配置本地应用程序设置的计算机。

3. 这将打开计算机属性。

4. 选择“**应用程序**”选项卡。

5. 单击 Kaspersky Endpoint Security for Mac。

6. 这将打开本地应用程序设置。

7. 选择**应用程序设置**选项卡。

8. 选择“**Detection and Response**” > “**Endpoint Detection and Response**”。

9. 在“**网络隔离**”块中，单击“**解除阻止从网络隔离的计算机**”。

您也可以使用命令行在本地禁用网络隔离。

网络隔离排除项

您可以配置网络隔离排除项。开启网络隔离后，符合规则的网络连接不会被计算机阻止。

要配置网络隔离排除项，您可以使用标准网络配置文件列表。默认情况下，排除项包括包含确保具有 DNS/DHCP 服务器和 DNS/DHCP 客户端角色的设备不间断运行的规则的网络配置文件。您还可以修改标准网络配置文件的设置或手动定义排除项（请参阅下面的说明）。

重要提示：仅当网络隔离响应检测到的威胁而自动打开时，才会应用策略属性中指定的排除项。仅当在 Kaspersky Security Center 控制台的计算机属性中手动打开网络隔离时，才会应用计算机属性中指定的排除项。

注意：活动策略不会阻止应用计算机属性中配置的网络隔离排除项，因为这些参数具有不同的使用场景。

如何在自动模式下添加网络隔离排除项

1. 在 Web Console 的主窗口，选择**设备** > **策略和配置文件**。
2. 单击 Kaspersky Endpoint Security 策略的名称。
3. 策略属性窗口打开。
4. 选择**应用程序设置**选项卡。
5. 选择“**Detection and Response**” > “**Endpoint Detection and Response**”。
6. 在“**网络隔离排除项**”块中，单击“**排除项**”。
7. 在下一个窗口中，单击“**从配置文件中添加**”并选择用于配置排除项的标准网络配置文件。
8. 配置文件中的网络隔离排除项被添加到网络隔离排除项列表中。您可以查看网络连接的属性。如有必要，您可以修改网络连接设置。
9. 如有必要，请手动添加网络隔离排除项。为此，在包含排除项列表的窗口中，单击“**添加**”并手动编辑网络连接设置。
10. 保存您的更改。

如何在手动模式下添加网络隔离排除项

1. 在 Web Console 的主窗口，选择“**设备**” > “**受管理设备**”。
2. 选择要配置本地应用程序设置的计算机。
3. 这将打开计算机属性。
4. 选择“**任务**”选项卡。
5. 这将显示计算机上可用的任务列表。
6. 选择“**网络隔离**”任务。
7. 选择**应用程序设置**选项卡。
8. 在打开的窗口中，单击“**排除项**”。
9. 在下一个窗口中，单击“**从配置文件中添加**”并选择用于配置排除项的标准网络配置文件。

10. 配置文件中的网络隔离排除项被添加到网络隔离排除项列表中。您可以查看网络连接的属性。如有必要，您可以修改网络连接设置。

11. 如有必要，请手动添加网络隔离排除项。为此，在包含排除项列表的窗口中，单击“**添加**”并手动编辑网络连接设置。

12. 保存您的更改。

您还可以使用命令行在本地查看网络隔离排除项列表。在这种情况下，必须隔离计算机。

Cloud Sandbox

Cloud Sandbox 是一种可以让您检测计算机上的高级威胁的技术。Kaspersky Endpoint Security 自动将检测到的文件转发到 Cloud Sandbox 进行分析。Cloud Sandbox 在隔离的环境中运行这些文件以识别恶意活动并确定其信誉。然后，这些文件的数据被发送到卡巴斯基安全网络。因此，如果 Cloud Sandbox 检测到恶意文件，Kaspersky Endpoint Security 将执行适当的操作，以在检测到该文件的所有计算机上消除此威胁。

重要提示：为了使 Cloud Sandbox 正常运行，您必须启用卡巴斯基安全网络。

注意：如果您使用卡巴斯基私人安全网络，Cloud Sandbox 技术不可用。

要启用 Cloud Sandbox：

1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。

2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口打开。

3. 选择**应用程序设置**选项卡。

4. 转到“**内置代理配置 → Endpoint Detection and Response**”部分。

5. 选择“**Cloud Sandbox**”选项卡。

6. 打开“**Cloud Sandbox**”切换开关。

7. 保存您的更改。

每当出现威胁时，Kaspersky Endpoint Security 就会在主应用程序窗口的“**威胁检测**”部分激活使用 Cloud Sandbox 检测到的威胁计数器。Kaspersky Endpoint Security 还将在 Kaspersky Security Center 控制台的威胁报告中指明 Cloud Sandbox 威胁检测技术。

文件保险箱磁盘加密

Kaspersky Endpoint Security 允许远程管理文件保险箱加密功能。加密技术可防止未经授权的用户访问用户计算机的启动盘上存储的敏感数据。

当管理员通过 Kaspersky Security Center 在计算机上启动文件保险箱加密功能时，Kaspersky Endpoint Security 会提示此计算机的用户输入其凭据。仅当用户提供凭据、计算机重新启动并且计算机上收到策略设置 30 分钟后，磁盘加密才会启动。提示输入凭证之间的最短间隔也是 30 分钟。

为了防止用户在启用 FileVault 加密时解密 Mac 的启动磁盘，管理员需要使用 JAMF 部署禁止磁盘解密的 MDM 配置文件。要使用禁止磁盘解密的 MDM 配置文件解密 Mac 的启动磁盘，管理员首先需要删除该配置文件。

注意： 如果未在 Kaspersky Security Center 中启用文件保险箱加密管理功能，具有管理员权限的用户可以通过系统设置加密和解密其 Mac 启动盘。有关文件保险箱的更多信息，请参阅 Apple 文档。

如果计算机拥有多个计算机账户，则除已输入其凭据的用户外，文件保险箱加密功能将禁止所有其他用户访问磁盘。

允许其他用户解锁磁盘

1. 选择“Apple **菜单** > **系统设置** > **隐私与安全性**”。
2. 单击“**文件保险箱**”。
   将会打开“**文件保险箱**”窗口。
3. 单击**启用用户**。
4. 在打开的窗口中，选择授权解锁计算机的用户。
5. 输入用户计算机账户的密码，然后单击**“确定”** 。
6. 单击“**继续**”。

   该用户将能够访问加密磁盘。

注意： 允许其他用户解锁磁盘需要具有管理员权限。

如果管理员通过 Kaspersky Security Center 管理控制台、Web Console 或云控制台管理 Kaspersky Endpoint Security，且此计算机的用户忘记或丢失其凭据，导致无法访问加密磁盘，则管理员可以获取恢复密钥。

如何使用 Kaspersky Security Center 管理控制台获取恢复密钥

如何使用 Kaspersky Security Center Web Console 和云控制台获取恢复密钥

密码保护

Kaspersky Endpoint Security 允许通过设置管理员密码来限制用户设备上不需要的操作。

如果启用了密码保护，Kaspersky Endpoint Security 在尝试执行以下任一操作时都需要密码：

- 配置应用程序设置
- 退出应用程序
- 删除授权许可密钥

- 删除应用程序

> **注意：**仅当通过卸载程序执行时，密码保护才会限制 Kaspersky Endpoint Security 的删除。

- 从备份区中恢复被隔离的文件
- 查看报告。

禁用密码保护不会禁用策略设置。如果策略中禁止编辑设置，则即使禁用密码保护也无法编辑该设置。

使用管理控制台启用密码保护

1. 启动管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 在控制台树中，单击**受管理设备**。
4. 在工作区中，选择**策略**选项卡。
5. 右键单击要配置的策略并选择**属性**。
6. 在**"属性"**窗口中，选择**附加设置 > 用户交互**。
7. 在"**密码保护**"部分，选中"**启用密码保护**"复选框。
8. 在打开的"**密码保护设置**"窗口中，配置以下设置：
   - 在"**密码**"字段中输入密码，然后在"**确认密码**"字段中再次输入密码。
   - 在**需要密码以**部分中，选中所需的复选框以保护用户设备上的相应操作。
9. 单击**确定**保存您的更改。
10. 执行以下操作之一以应用策略更改：
    - 单击"**应用**"，保存更改后，仍留在"**属性: <策略名称>**"窗口中。
    - 单击"**确定**"，保存更改后，将关闭"**属性: <策略名称>**"窗口。

使用管理控制台编辑密码保护设置

1. 启动管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 在控制台树中，单击**受管理设备**。
4. 在工作区中，选择**策略**选项卡。
5. 右键单击要配置的策略并选择**属性**。
6. 在**"属性"**窗口中，选择**附加设置 > 用户交互**。

7. 在“**密码保护**”部分，单击“**设置**”按钮。

8. 在打开的“**密码保护设置**”窗口中，编辑您想要更改的设置。

9. 单击**确定**保存您的更改。

使用 Web Console 启用密码保护

1. 在 Web Console 的主窗口，选择**设备** > **策略和配置文件**。

2. 单击 Kaspersky Endpoint Security for Mac 策略名称。

3. 策略属性窗口打开。

4. 选择**应用程序设置**选项卡。

5. 选择“**附加设置**” > “**用户交互**”。

6. 打开“**密码保护**”切换开关。

7. 在打开的“**密码保护设置**”窗口中，配置以下设置：

   - 在“**密码**”字段中输入密码，然后在“**确认密码**”字段中再次输入密码。默认情况下，将出于安全原因隐藏密码字符。要查看密码，请单击“**显示**”。

   - 在**需要密码以**部分中，选中所需的复选框以保护用户设备上的相应操作。

8. 单击“**确定**”关闭“**密码保护设置**”对话框。

9. 单击“**确定**”关闭“**用户交互**”部分。

10. 单击**“保存”**以保存对策略的更改。

使用 Web Console 编辑密码保护

1. 在 Web Console 的主窗口，选择**设备** > **策略和配置文件**。

2. 单击 Kaspersky Endpoint Security for Mac 策略名称。

3. 策略属性窗口打开。

4. 选择**应用程序设置**选项卡。

5. 选择“**附加设置**” > “**用户交互**”。

6. 在“**密码保护**”部分，单击“**设置**”按钮。

7. 在打开的“**密码保护设置**”对话框中，编辑您想要更改的设置。

8. 单击“**确定**”关闭“**密码保护设置**”对话框。

9. 单击“**确定**”关闭“**用户交互**”部分。

10. 单击**“保存”**以保存对策略的更改。

使用 Kaspersky Endpoint Security 应用程序启用密码保护

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在“**界面**”选项卡的“**密码保护**”部分中，选中“**启用密码保护**”复选框。
3. 在打开的窗口中，配置以下设置：
   - 在“**密码**”字段中输入密码，然后在“**确认密码**”字段中再次输入密码。
   - 在**需要密码以**部分中，选中所需的复选框以保护用户设备上的相应操作。
4. 单击**确定**。

> **注意：**如果选择“**更改应用程序设置**”作为密码保护操作，则需要输入两次密码才能更改密码保护设置。

使用 Kaspersky Endpoint Security 应用程序编辑密码保护

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在“**界面**”选项卡的“**密码保护**”部分中，单击“**设置**”。
3. 在打开的窗口中，编辑您想要更改的设置。
4. 单击**确定**。

漏洞利用防御

漏洞利用防御组件会检测利用计算机漏洞来获取管理员权限或执行恶意活动的程序代码。例如，漏洞利用程序可以利用缓冲区溢出攻击。为此，漏洞利用程序会向易受攻击的应用程序发送大量数据。处理此数据时，易受攻击的应用程序会执行恶意代码。此攻击的结果是，漏洞利用程序可启动未经授权的恶意软件安装。当存在从易于感染的应用程序运行可执行文件的尝试，并且该尝试并非由用户执行时，Kaspersky Endpoint Security 将阻止该文件运行或通知用户。

默认启用漏洞利用防御。您可以根据需要禁用“漏洞利用防御”。

使用 Web Console 启用/禁用“漏洞利用防御”

1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**主机威胁防护 → 行为分析 → 漏洞利用防御**”部分。
5. 使用“**漏洞利用防御**”拨动开关启用或禁用组件。

6. 如果启用漏洞利用防御，请选择在检测到漏洞利用时要执行的操作：

   - **阻止**

     如果选择此项，在检测到漏洞利用时，Kaspersky Endpoint Security 会阻止此漏洞利用的操作，并生成一条包含此漏洞利用相关信息的日志条目。

   - **通知**

     如果选择此项，当 Kaspersky Endpoint Security 检测到漏洞利用时，它会记录一条包含此漏洞利用相关信息的条目，并将此漏洞利用的相关信息添加到活动威胁列表中。

7. 保存您的更改。

使用管理控制台启用/禁用“漏洞利用防御”

1. 启动管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 在控制台树中，单击**受管理设备**。
4. 在工作区中，选择**策略**选项卡。
5. 右键单击要配置的策略并选择**属性**。
6. 在“**属性**”窗口中，选择“**高级威胁防护**”>“**漏洞利用防御**”。
7. 选中或取消选中“**启用漏洞利用防御**”复选框。
8. 如有必要，在“**检测到漏洞时**”部分中，选择当 Kaspersky Endpoint Security 检测到漏洞利用时要执行的操作。
9. 单击**确定**保存您的更改。
10. 执行以下操作之一以应用策略更改：

    - 单击“**应用**”，保存更改后，仍留在“**属性: <策略名称>**”窗口中。
    - 单击“**确定**”，保存更改后，将关闭“**属性: <策略名称>**”窗口。

使用 Kaspersky Endpoint Security 应用程序启用/禁用“漏洞利用防御”

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在“**高级**”选项卡的“**启用漏洞利用防御**”部分中，选中或取消选中“启用漏洞利用防御”复选框。
3. 如果选中**“启用行为检测”**复选框，请选择在检测到恶意软件活动时要执行的以下操作之一：

   - **自动阻止危险的恶意软件活动**

     如果选择此项，在检测到漏洞利用时，Kaspersky Endpoint Security 会阻止此漏洞利用的操作，并生成一条包含此漏洞利用相关信息的日志条目。

- **通知**

  如果选择此项，当 Kaspersky Endpoint Security 检测到漏洞利用时，它会记录一条包含此漏洞利用相关信息的条目，并将此漏洞利用的相关信息添加到活动威胁列表中。

查看漏洞利用防御报告

1. 在菜单栏中，选择**保护** > **报告**。
   将会打开**报告**窗口。
2. 打开"**漏洞利用防御**"选项卡。

修复引擎

修复引擎让 Kaspersky Endpoint Security 回滚操作系统中恶意软件执行的操作。

在回滚操作系统中的恶意软件活动时，Kaspersky Endpoint Security 会处理以下类型的恶意软件活动：

- **文件活动**
  Kaspersky Endpoint Security 执行以下操作：
  - 删除恶意软件创建的可执行文件（在网络驱动器以外的所有媒体上）。
  - 删除已被恶意软件渗透的程序创建的可执行文件。
  - 恢复已被恶意软件修改或删除的文件。
- **系统活动**
  Kaspersky Endpoint Security 执行以下操作：
  - 终止由恶意软件启动的进程。
  - 终止恶意的应用程序渗透的进程。
  - 不恢复已被恶意软件停止的进程。
- **网络活动**
  Kaspersky Endpoint Security 执行以下操作：
  - 阻止恶意软件的网络活动。

恶意软件操作的回滚可以由文件威胁防护或行为检测组件启动，也可以在恶意软件扫描期间启动。

回滚恶意软件操作会影响严格定义的数据集。回滚不会对操作系统或计算机数据的完整性产生不利影响。

在管理控制台中启用/禁用"修复引擎"

1. 启动管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 在控制台树中，单击**受管理设备**。

4. 在工作区中，选择**策略**选项卡。
5. 右键单击要配置的策略并选择**属性**。
6. 在“**属性**”窗口中，选择“**高级威胁防护**”>“**修复引擎**”。
7. 选中或取消选中“**启用修复引擎**”复选框。
8. 单击**确定**保存您的更改。
9. 执行以下操作之一以应用策略更改：
   - 单击“**应用**”，保存更改后，仍留在“**属性: <策略名称>**”窗口中。
   - 单击“**确定**”，保存更改后，将关闭“**属性: <策略名称>**”窗口。

在 Web Console 中启用/禁用“修复引擎”

1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**主机威胁防护 → 行为分析 → 修复引擎**”部分。
5. 使用“**修复引擎**”拨动开关启用或禁用组件。
6. 保存您的更改。

在应用程序界面中启用/禁用修复引擎

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在“**高级**”选项卡的“修复引擎”部分中，选中或取消选中“**启用修复引擎**”复选框。

因此，如果启用了修复引擎，Kaspersky Endpoint Security 将回滚操作系统中恶意的应用程序采取的操作。

Web 控制

Web 控制管理用户对 Web 资源的访问。这有助于减少流量和工作时间的不当使用。当用户尝试打开受 Web 控制限制的网站时，Kaspersky Endpoint Security 将阻止访问或显示警告。

您可以阻止访问特定网站或选定类别的网站。

备注： Kaspersky Endpoint Security 应用程序只能阻止访问使用 HTTPS 连接的网站。仅当在“**基本**”区域中的“**常规**”选项卡上选中了“**检查安全连接 (HTTPS)**”复选框时，应用程序才会扫描加密连接 (HTTPS)。

在管理控制台中添加新规则

1. 启动管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 在控制台树中，单击**受管理设备**。
4. 在工作区中，选择**策略**选项卡。
5. 右键单击要配置的策略并选择**属性**。
6. 在“**属性**”窗口，选择“**安全控制** > **Web 控制**”。
7. 选择“**启用 Web 控制**”复选框。
8. 单击**添加**。
9. 在打开的窗口中，输入规则名称。
10. 如果您希望规则处于活动状态，请选择“**活动规则**”复选框。
11. 执行下列操作之一：
    - 如果您希望规则应用于特定网址，请选择“**网址或按掩码列出的一组网址**”选项。
    - 如果您希望规则应用于特定网站类别，请选择“**网站类别**”选项。
12. 点击“**指定**”。
13. 在打开的窗口中，指定规则范围。
14. 执行下列操作之一：
    - 如果您希望 Kaspersky Endpoint Security 阻止访问，请选择“**阻止**”选项。
    - 如果您希望 Kaspersky Endpoint Security 允许访问，请选择“**允许**”选项。
    - 如果您希望 Kaspersky Endpoint Security 显示警告，请选择“**显示警告**”选项。
15. 单击**确定**保存您的更改。
16. 执行以下操作之一以应用策略更改：
    - 单击“**应用**”，保存更改后，仍留在“**属性: <策略名称>**”窗口中。
    - 单击“**确定**”，保存更改后，将关闭“**属性: <策略名称>**”窗口。

在 Web Console 中添加新规则

1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口打开。

3. 选择**应用程序设置**选项卡。
4. 转到“**安全控制 → Web 控制**”。
5. 打开“**Web 控制**”开关。
6. 单击“**添加**”。
7. 在打开的窗口中，输入规则名称。
8. 执行下列操作之一：
   - 如果您希望规则处于活动状态，请选择“**活动**”选项。
   - 如果您希望规则处于非活动状态，请选择“**不活动**”选项。
9. 执行下列操作之一：
   - 如果您希望 Kaspersky Endpoint Security 允许访问，请选择“**允许**”选项。
   - 如果您希望 Kaspersky Endpoint Security 阻止访问，请选择“**阻止**”选项。
   - 如果您希望 Kaspersky Endpoint Security 显示警告，请选择“**显示警告**”选项。
10. 执行下列操作之一：
    - 如果您希望规则应用于特定网站类别，请选择“**类别**”选项并点击“**选择类别**”以选择类别。
    - 如果您希望规则应用于特定网址，请选择“**输入网址**”选项并将它们添加到下表中。
11. 保存您的更改。

备注：无法在 Kaspersky Endpoint Security 应用程序中管理 Web 控制设置。

设备控制

设备控制管理用户对安装在计算机上或连接到计算机的设备的访问。这样，当连接此类设备时，您就可以保护计算机免受感染，并防止数据丢失或泄漏。

设备访问级别

设备控制在以下级别控制访问：

- **设备类型**。您可以控制对硬盘、可移动磁盘、软盘、CD/DVD 驱动器和 Wi-Fi 网络的访问。

您可以按如下方式配置设备访问：

- 允许。
- 阻止。
- 阻止但带有例外（仅限 Wi-Fi）。

- **受信任设备。**受信任设备是受信任设备设置中指定的用户始终具有完全访问权限的设备。
  您可以根据以下数据添加受信任设备：
  - **设备 ID。**每个设备都有一个唯一的 ID（硬件 ID、HWID）。您可以使用操作系统工具在设备属性中查看该 ID。设备 ID 示例：SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000。如果您想添加多个特定设备，通过 ID 添加设备会很方便。
  - **设备型号。**每个设备都有一个供应商 ID (VID) 和一个产品 ID (PID)。您可以使用操作系统工具查看设备属性中的 ID。输入 VID 和 PID 的模板：VID_1234&PID_5678。如果您在组织中使用某种型号的设备，则按型号添加设备会很方便。这样，就可以添加该型号的所有设备了。
  - **设备 ID 掩码。**如果您使用具有相似 ID 的多个设备，则可以使用掩码将设备添加到受信任列表中。`*` 字符替换任意字符集。输入掩码时，Kaspersky Endpoint Security 不支持 `?` 字符。例如，`WDC_C*`。
  - **设备型号掩码。**如果您使用具有相似 VID 或 PID 的多个设备（例如，来自同一制造商的设备），则可以使用掩码将设备添加到受信任列表中。`*` 字符替换任意字符集。输入掩码时，Kaspersky Endpoint Security 不支持 `?` 字符。例如，`VID_05AC&PID_*`。

在管理控制台中管理设备控制组件

1. 启动管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 在控制台树中，单击**受管理设备**。
4. 在工作区中，选择**策略**选项卡。
5. 右键单击要配置的策略并选择**属性**。
6. 在“**属性**”窗口，选择“**安全控制** > **设备控制**”。
7. 选择“**启用设备控制**”复选框。
8. 在“**设备类型**”选项卡上，配置设备类型和 Wi-Fi 网络的访问规则。
9. 在“**受信任设备**”选项卡上，配置单个设备或设备组的访问规则。
10. 单击**确定**保存您的更改。
11. 执行以下操作之一以应用策略更改：
    - 单击“**应用**”，保存更改后，仍留在“**属性: <策略名称>**”窗口中。
    - 单击“**确定**”，保存更改后，将关闭“**属性: <策略名称>**”窗口。

在 Web Console 中管理设备控制组件

1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口打开。
3. 选择**应用程序设置**选项卡。
4. 转到“**安全控制 > 设备控制**”。
5. 打开“**设备控制**”开关。
6. 在“**设备控制设置**”部分，配置设备、设备类型和 Wi-Fi 网络的访问规则。
7. 保存您的更改。

> **备注：**无法在 Kaspersky Endpoint Security 应用程序中管理设备控制设置。

因此，如果启用了设备控制，应用程序会将有关已连接设备的信息传递到 Kaspersky Security Center。您可以在 Kaspersky Security Center 中查看已连接设备的列表，在“**高级 → 存储库 → 硬件文件夹**”。

查看“设备控制”报告

1. 在菜单栏中，选择**保护 > 报告**。
   将会打开**报告**窗口。
2. 打开“**设备控制**”选项卡。

加入卡巴斯基安全网络

加入卡巴斯基安全网络后，Kaspersky Endpoint Security 应用程序统计信息将自动发送到卡巴斯基，以加强对您的 Mac 的保护。

注意：卡巴斯基不会在没有您明确同意的情况下收集、处理或存储任何个人数据。

您可以自行决定是否加入卡巴斯基安全网络。安装应用程序时，会提示您选择是否加入卡巴斯基安全网络。您之后可随时更改决定。

启用卡巴斯基安全网络

1. 在菜单栏，单击应用程序图标并选择**设置**。

   此时会打开应用程序设置窗口。

2. 在**高级**选项卡的 KSN 区域中，单击**显示 KSN 声明**以查看卡巴斯基安全网络声明。

3. 如果希望 Kaspersky Endpoint Security 使用从卡巴斯基安全网络接收的有关文件、网络资源和应用程序信誉的信息，并且您接受本声明的所有条款，请选中**加入卡巴斯基安全网络**复选框。

4. 在打开的窗口中，单击**确认**。

   将选中**加入卡巴斯基安全网络**和**启用扩展 KSN 模式**复选框。

注意：默认情况下，Kaspersky Endpoint Security 使用扩展 KSN 模式。*扩展 KSN 模式*是 Kaspersky Endpoint Security 用来向卡巴斯基发送附加数据的一种模式。如果不希望向卡巴斯基提供这些数据，请取消选中**启用扩展 KSN 模式**复选框。

使用卡巴斯基安全网络时向卡巴斯基提供的数据

如果选中**加入卡巴斯基安全网络**复选框，但未选中**启用扩展 KSN 模式**复选框，则 Kaspersky Endpoint Security 将向卡巴斯基提供以下数据：

- 有关使用的授权许可的信息： 授权许可的类型和有效期、授权许可到期前的天数、向其购买授权许可的合作伙伴的标识符、区域激活中心标识符、激活码的校验码、使用 SHA1 算法计算出的票证正文哈希值、授权许可票证的创建日期和时间、授权许可信息标识符、授权许可票证标识符、授权许可票证序列标识符、用户计算机的唯一标识符、授权许可票证的有效期开始日期、授权许可票证的有效期截止日期、授权许可票证当前状态、票证标头版本、授权许可版本、票证标头签名证书标识符、密钥文件的校验码、票证标头签名者序列号、身份验证令牌。

- 已安装软件的完整版本；
  已安装软件的类型；
  软件更新 ID； 信誉服务 ID； 协议类型 ID； 区域激活中心 ID； 已撤销的软件服务决定列表的版本； 软件反病毒数据库中触发记录的 ID； 软件反病毒数据库中触发记录的时间戳； 触发的软件反病毒数据库记录的类型；计算机上的应用程序安装实例的独一 ID； 授权许可激活日期； 授权许可到期日期； 授权许可 ID； 软件使用的授权许可的状态； 正在处理的对象的校验和类型； 检测到的可用于破坏用户设备或数据的恶意软件或合法软件的名称； 正在处理的对象的校验和； 软件激活码校验和； 软件的完整版本； 独一设备 ID； 软件 ID； 软件密钥文件的校验和； 用于提供软件授权许可的信息模型的 ID； 用于签署软件授权许可 ticket 标头的证书的标识符； 软件授权许可 ticket 创建日期和时间； 软件授权许可 ticket 校验和； 软件授权许可 ticket 版本； 软件激活码版本； 向权利持有人基础结构的请求的数据格式； 当前授权许可 ticket ID； 软件组件 ID； 软件操作

的结果； 错误代码； Web 服务的访问地址 (URL、IP)； 端口号； Web 服务请求源的 Web 地址 (Referrer)； 证书的公钥； 所扫描对象和哈希算法的数字证书指纹。

如果选中**加入卡巴斯基安全网络**和**启用扩展 KSN 模式**复选框，则 Kaspersky Endpoint Security 将向卡巴斯基提供以下数据：

- 相关信息，包括已安装在计算机上的操作系统 (OS) 和服务包的版本、操作系统内核文件的版本与校验码（MD5、SHA2-256、SHA1）、操作系统运行模式的参数； 操作系统版本、操作系统内部版本号、操作系统更新编号、操作系统版本、有关操作系统版本的扩展信息； 操作系统 Service Pack 版本； 操作系统的启动日期和时间； 行为分析子系统中有关操作系统操作的事件的处理延迟时间； 当前类型的延迟操作系统操作事件的数量； 主动防御子系统中有关操作系统操作的事件的处理延迟时间； 已处理的操作系统操作事件的数量； 已处理的同步操作系统操作事件的数量； 当前类型的所有操作系统操作事件的总延迟； 持久事件存储子系统中有关操作系统操作的事件的处理延迟时间； 所有操作系统操作事件的总延迟； 等待同步操作系统操作事件的数量； 接收到的操作系统操作事件的日期和时间。

- 有关上次操作系统重启失败的信息： 重启失败次数。

- 有关权利持有人安装的应用程序和反病毒保护状态的信息： 软件安装 ID (PCID)； 软件数据库记录版本； 计算机上安装的应用程序实例的唯一标识符、应用程序类型、应用程序类型的 ID、已安装应用程序的完整版本、应用程序设置版本的标识符、计算机类型的标识符、安装应用程序的计算机的唯一标识符、权利持有人服务中的唯一用户标识符、区域设置语言和运行状态、已安装的软件组件的版本及其运行状态、连接权利持有人服务所使用的协议版本； 已安装软件的完整版本； 已安装软件的类型； 软件更新 ID； 信誉服务 ID； 协议类型 ID； 区域激活中心 ID； 已撤销的软件服务决定列表的版本； 软件反病毒数据库中触发记录的 ID； 软件反病毒数据库中触发记录的时间戳； 触发的软件反病毒数据库记录的类型； 计算机上的应用程序安装实例的独一 ID； 授权许可激活日期； 授权许可到期日期； 授权许可 ID； 软件使用的授权许可的状态； 正在处理的对象的校验和类型； 检测到的可用于破坏用户设备或数据的恶意软件或合法软件的名称； 正在处理的对象的校验和； 软件激活码校验和； 软件的完整版本； 软件 ID； 软件密钥文件的校验和； 用于提供软件授权许可的信息模型的 ID； 用于签署软件授权许可 ticket 标头的证书的标识符； 软件授权许可 ticket 创建日期和时间； 软件授权许可 ticket 校验和； 软件授权许可 ticket 版本； 软件激活码版本； 向权利持有人基础结构的请求的数据格式； 当前授权许可 ticket ID； 软件组件 ID； 软件操作的结果； 错误代码； Web 服务的访问地址 (URL、IP)； 端口号； Web 服务请求源的 Web 地址 (Referrer)； 反病毒数据库的更新应用周期数； 反病毒数据上次更新和应用的日期和时间； 软件数据库的发布日期和时间； 软件组件的版本； 软件更新 ID； 已安装软件的类型； 系统监控的启动日期和时间； 软件的安装日期和时间； 系统监控发送统计数据的概率； 系统监控进行处理所花费的时间长于标准时间的事件的代码； 系统监控进行处理所花费的时间长于标准时间的事件的数据库处理时间； 系统监控处理一个事件的最长允许时间； 系统监控进行处理所花费的时间长于标准时间的事件的处理时间； 系统监控进行处理所花费的时间长于标准时间的事件的总数。

- 有关所有已处理对象和操作的信息： 软件对正在处理的对象的裁定； 目录代码； 所处理对象的大小； 所处理对象的校验和 (SHA256)； 系统监控上下文中所检测软件的编号； 系统监控检测软件的日期和时间； 删除特征； 软件反病毒数据库中触发记录的 ID； 系统监控检测软件的原因； 所处理对象的校验和 (MD5)； 模块完整性检查的结果； 所处理对象的名称； 触发的软件反病毒数据库记录的类型； 所处理对象的路径； 已扫描对象的名称； 扫面的日期和时间； 下载它的 URL 和 Referrer 地址； 已扫描文件的大小及其路径； 存档标志； 文件创建的日期和时间； 打包程序的名称、大小和校验和（MD5、SHA2-256）（如果文件被打包）； 文件的熵； 文件的类型； 文件类型代码； 可执行文件的标志、ID 和格式； 对象的校验和（MD5、SHA2-256）； 对象的补充校验和的类型和值； 有关对象的数字签名（证书）的数据： 证书发布者的数据、上次统计交付后对象的启动次数、应用程序的扫描任务 ID、接收对象信誉信息的方式、目标过滤器的值、适用检测技术的技术参数； 所处理对象的路径； 目录代码。

- 对于可执行文件： 文件部分的熵、信誉验证标记或文件签名标记、名称、类型、ID 类型、校验码 (MD5)，以及正在接受验证的对象加载的应用程序的大小、应用程序路径和模板路径、表明在自动运行列表中存在的属性、输入日期、属性列表、打包程序名称、应用程序数字签名的相关信息： 发行商证书、以 MIME 格式上传的文件的名称、文件构建日期和时间。

- 有关已启动的应用程序及其模块的信息： 运行文件的校验码（MD5、SHA2-256）、大小、属性、创建日期、打包程序的名称（如果文件被打包）、文件的名称、系统上运行的进程的信息（进程 ID (PID)）、进程名称、启动进程的账户信息、启动进程的应用程序和命令、进程文件的完整路径、启动命令行、进程所属应用程序的描述（应用程序的名称和开发商信息，以及使用的数字证书和用于验证其真实性的信息或缺乏文件数字签名的信息），和进程中加载的模块信息： 它们的名称、大小、类型、创建日期、属性、校验码（MD5、SHA2-256、SHA1）、路径、PE 文件头信息、打包程序名称（如果文件被打包）、这些统计数据的可用性和有效性的相关信息、生成被发送的统计数据的模式的标识符。

- 如果检测到威胁或漏洞，除了提供检测到的对象的相关信息外，还应提供该记录在反病毒数据库中的标识符、版本和类型，该威胁在卡巴斯基分类中的名称，上一次更新反病毒数据库的日期和时间，可执行文件名称，向检测到威胁的网址发出请求的应用程序文件的校验码 (MD5)，检测到的威胁的 IP 地址（IPv4 或 IPv6），漏洞标识符及其威胁等级，检测到漏洞的网页的网址和 Referrer。

- 如果检测到潜在的恶意对象，则提供有关进程内存中的数据的信息。

- 网络攻击信息： 攻击计算机的 IP 地址和用户计算机上成为网络攻击目标的端口号，攻击协议的 ID，攻击的名称和类型。

- 关于网络连接的信息： 来自使打开端口的进程启动的文件的版本和校验和 (MD5、SHA2-256、SHA1)，进程文件的路径及其数字签名，本地和远程 IP 地址，本地和远程连接端口的数量，连接的状态，端口开放的时间戳。

- 检测到有害或可疑内容的网页的网址和 IP 地址，向该网址发出请求的文件名称、大小及校验码、实现裁定结果所用规则的标识符、权重和程度、攻击的目标。

- 有关已安装应用程序和反病毒数据库更新的信息： 更新任务的完成状态、更新过程中可能发生的错误的类型、未成功更新的数量、执行更新的应用程序组件的标识符。

- 有关使用卡巴斯基安全网络 (KSN) 的信息： KSN 标识符、应用程序标识符、应用程序完整版本、用户设备的匿名 IP 地址、KSN 请求履行质量指标、KSN 数据包处理质量指标、KSN 请求数量指标和 KSN 请求类型信息、统计数据开始发送的日期和时间、统计数据完成发送的日期和时间、KSN 配置更新的相关信息： 活动配置的标识符、接收的配置标识符、配置更新的错误代码。

- 有关系统日志事件的信息： 事件时间、检测到事件的日志的名称、事件的类型和类别、事件源的名称和事件描述。

- 用于确定文件和 URL 地址信誉的信息： 请求信誉的 URL 地址和 Referrer、连接的协议类型、应用程序类型的内部标识符、正在使用的端口号、用户标识符、扫描文件的校验码 (MD5)、检测到的威胁类型、用于检测威胁的记录的信息（反病毒数据库的记录标识符、记录时间戳和类型）； 证书的公钥； 所扫描对象和哈希算法的数字证书指纹。

- 应用程序地域分布数据： 应用程序安装和激活日期、为应用程序激活提供授权许可的合作伙伴 ID、应用程序 ID、应用程序语言本地化 ID、应用程序激活的授权许可序列号、KSN 参与标志。

- 有关使用的授权许可的信息： 授权许可的类型和有效期、授权许可到期前的天数、向其购买授权许可的合作伙伴的标识符、区域激活中心标识符、激活码的校验码、使用 SHA1 算法计算出的票证正文哈希值、授权许可票证的创建日期和时间、授权许可信息标识符、授权许可票证标识符、授权许可票证序列标识符、用户计算机的唯一标识符、授权许可票证的有效期开始日期、授权许可票证的有效期截止日期、授权许可票证当前状态、票证标头版本、授权许可版本、票证标头签名证书标识符、密钥文件的校验码、票证标头签名者序列号、身份验证令牌。

- 有关计算机上已安装硬件的信息： 类型、名称、型号名称、固件版本、内置设备和连接设备的参数。

- 设备信息： 设备 ID。

- 有关 Web 控制组件的操作的信息：
  组件版本、分类原因、有关分类原因的其他信息、分类的 URL、被锁定或分类的对象的主机 IP 地址。

注意：您可以加入卡巴斯基私人安全网络，而不是加入卡巴斯基安全网络，具体取决于 Kaspersky Security Center 设置。当 Kaspersky Endpoint Security 从卡巴斯基私人安全网络切换到卡巴斯基安全网络时，该应用程序会向您发送通知，并提示您接受卡巴斯基安全网络声明的条款。有关加入卡巴斯基私人安全网络的详细信息，请参阅 Kaspersky Security Center 帮助。

卡巴斯基安全网络基础架构

Kaspersky Endpoint Security 支持以下卡巴斯基安全网络基础架构解决方案：

- *全球 KSN* 是被大多数卡巴斯基应用程序使用的解决方案。KSN 参与者从卡巴斯基安全网络接收信息，并发送给 Kaspersky 有关在用户计算机上检测到的对象的信息，由卡巴斯基分析师进行额外分析，并包含在卡巴斯基安全网络的信誉和统计数据库中。
- *私有 KSN* 是这样一种解决方案，它使运行 Kaspersky Endpoint Security 或其他卡巴斯基应用程序的计算机的用户能够访问卡巴斯基安全网络信誉数据库和其他统计信息，而无需从自己的计算机向卡巴斯基安全网络发送数据。私有 KSN 专为因以下任何原因无法加入卡巴斯基安全网络的公司客户设计：
  - 本地工作站未连接到互联网。
  - 法律禁止或公司安全策略限制将任何数据传输到国家/地区外部或公司 LAN 外部。

默认下，Kaspersky Security Center 使用全球 KSN。您可以在 Kaspersky Security Center 管理控制台 (MMC) 和 Kaspersky Security Center Web Console 中配置私有 KSN 的使用。无法在 Kaspersky Security Center 云控制台配置私有 KSN 的使用。

KSN 代理

由 Kaspersky Security Center 管理服务器管理的计算机可以通过 KSN 代理服务与卡巴斯基安全网络交互。

KSN 代理服务提供以下功能：

- 用户的计算机可以查询 KSN 并将信息提交给 KSN，甚至不需要直接访问互联网。
- KSN 代理服务缓存处理过的数据，从而减少外部网络通信信道上的负载，并加速接收用户计算机请求的信息。

对于更多 KSN 代理服务的详情，请参考 Kaspersky Security Center 帮助。

注意：在美国境内，本软件中将不再提供更新功能（包括提供反恶意软件签名更新和代码库更新）以及 KSN 功能。

检查应用程序组件的完整性

Kaspersky Endpoint Security 包含各种动态链接库、可执行文件、配置文件和接口文件形式的二进制模块。入侵者可能会用包含恶意代码的其他文件替换一个或多个应用程序可执行模块或文件。为了防止这种情况，Kaspersky Endpoint Security 可以检查应用程序组件的完整性。应用程序检查模块和文件是否有未经授权的更改或损坏。如果应用程序模块或文件的校验和不正确，则认为其已损坏。应用程序检查模块和文件是否有未经授权的更改或损坏。如果应用程序模块或文件的校验和不正确，则认为其已损坏。

应用程序组件的完整性使用位于 /Library/Application Support/Kaspersky Lab/KAV/Binaries 目录中的 integrity_checker 实用程序进行检查。此实用工具检查包含应用程序文件列表的清单文件的完整性，该列表的完整性对于应用程序组件的正确操作至关重要。

Integrity_check.xml 清单文件受卡巴斯基加密签名保护，与 integrity_checker 实用工具位于同一目录中（/Library/Application Support/Kaspersky Lab/KAV/Binaries）。

注意：运行 integrity_checker 实用工具需要根用户账户权限。

可以使用与应用程序一起安装的实用工具或使用经认证的 CD 上的实用工具执行完整性检查。

要检查应用程序组件的完整性，请运行以下命令：

```
sudo "/Library/Application Support/Kaspersky Lab/KAV/Binaries/integrity_checker"
```

默认情况下，该实用工具使用位于 /Library/Application Support/Kaspersky Lab/KAV/Binaries 目录中的 integrity_check.xml 文件。

要显示实用工具设置的帮助，请运行以下命令：

```
--help
```

检查每个清单文件的结果显示在清单文件名称旁边，格式如下：

- `SUCCEEDED`—已确认文件的完整性（返回代码 `0`）
- `FAILED`—未确认文件的完整性（返回代码不是 `0`）

通过 Kaspersky Security Center 管理控制台管理应用程序

Kaspersky Security Center 专为集中管理企业网络安全而设计。有关 Kaspersky Security Center 的详细信息，请参阅 Kaspersky Security Center 帮助。

您还可以通过应用程序的图形用户界面、Kaspersky Security Center Web Console 和云控制台及命令行来管理 Kaspersky Endpoint Security。

在企业网络上部署 Kaspersky Endpoint Security

1. 在网络上部署*管理服务器*。

   管理服务器是 Kaspersky Security Center 用于集中存储企业网络内安装的所有卡巴斯基应用程序的相关信息以及管理这些应用程序的组件。

2. 在 Kaspersky Security Center 管理员工作站上安装*管理控制台*。

   管理控制台是 Kaspersky Security Center 用于为管理服务器和*网络代理*的管理服务提供用户界面的组件。网络代理可协调管理服务器与企业网络内的计算机上安装的 Kaspersky Endpoint Security 之间的交互。

3. 在 Kaspersky Security Center 管理员工作站上安装 Kaspersky Endpoint Security 管理插件。

   *管理插件*是一个专用组件，可提供相关界面以便通过管理控制台来管理卡巴斯基 应用程序。每个应用程序都有自己的管理插件。该管理插件适用于可从 Kaspersky Security Center 管理的所有卡巴斯基应用程序。

4. 通过以下方式之一在远程 Mac 计算机上安装网络代理：

   - 本地安装
   - 使用 Apple 远程桌面远程安装
   - 通过 Kaspersky Security Center 远程安装
   - 使用 SSH 协议远程安装

   注意：要通过 Kaspersky Security Center 管理 Kaspersky Endpoint Security for Mac 12.2.1，必须在远程计算机上安装网络代理版本 15。

5. 通过以下方式之一在远程 Mac 计算机上安装 Kaspersky Endpoint Security：

   - 本地安装
   - 使用 Apple 远程桌面远程安装
   - 使用 SSH 协议远程安装
   - 通过 Kaspersky Security Center 远程安装

重要：如果远程计算机上安装有卡巴斯基安全软件 for Mac 版或第三方反恶意软件应用程序，请在安装 Kaspersky Endpoint Security 之前卸载这些应用程序。

有关如何部署管理服务器和安装管理控制台的详细信息，请参阅 Kaspersky Security Center 帮助。

将 Kaspersky Endpoint Security 版本 11.1 或更高版本更新到版本 12.2.1

注意：要通过 Kaspersky Security Center 管理 Kaspersky Endpoint Security for Mac 12.2.1，必须在远程计算机上安装网络代理版本 15。

您可以采用以下方式之一，将由 Kaspersky Security Center 管理的 Kaspersky Endpoint Security 从版本 11.1 或更高版本更新到版本 12.2.1：

- 同时将远程计算机上的 Kaspersky Endpoint Security 更新到版本 12.2.1 以及将网络代理更新到版本 15。
- 首先将网络代理更新到版本 15，然后再将 Kaspersky Endpoint Security 更新到版本 12.2.1。

将应用程序更新到较新版本时，请考虑以下事项：

- 要将 Kaspersky Endpoint Security 更新到版本 12.2.1，需要 macOS 14 或更高版本。
- 您需要从技术支持网站下载 KES_11.3_profile.zip 压缩包以应用新的配置文件。
- 将 Kaspersky Endpoint Security 更新到版本 12.2.1 后，网络设置中可能会出现两个卡巴斯基过滤器和两个卡巴斯基监视器项目。
- 若您有 Kaspersky Endpoint Security 版本 11.0.1 或更早版本，要将应用程序更新到版本 12.2.1，您需要卸载应用程序并将 macOS 更新到版本 14 或更高版本。然后您可以安装 Kaspersky Endpoint Security 版本 12.2.1。

注意：在美国境内，本软件中将不再提供更新功能（包括提供反恶意软件签名更新和代码库更新）以及 KSN 功能。

准备远程安装 Kaspersky Endpoint Security

本节包含有关在 Kaspersky Security Center 管理员工作站上安装 Kaspersky Endpoint Security 管理插件以及在远程计算机上安装网络代理的信息。

在通过 Kaspersky Security Center 安装 Kaspersky Endpoint Security 之前，必须首先安装 Kaspersky Endpoint Security 管理插件和网络代理。

安装 Kaspersky Endpoint Security 管理插件

Kaspersky Endpoint Security 管理插件可提供相关界面，以便通过管理控制台来管理 Kaspersky Endpoint Security。

安装 Kaspersky Endpoint Security 管理插件

1. 在 Kaspersky Security Center 管理员工作站上，解压缩包含 Kaspersky Endpoint Security 安装包文件的压缩包。
2. 打开包含 Kaspersky Endpoint Security 安装包文件的文件夹。
3. 双击 klcfginst.exe。

将开始安装 Kaspersky Endpoint Security 管理插件。

重要：在安装 Kaspersky Endpoint Security 管理插件之前，请在 Kaspersky Security Center 管理员工作站上关闭管理控制台。

本地安装网络代理

网络代理可协调管理服务器与企业网络内的计算机上安装的 Kaspersky Endpoint Security 之间的交互。

本地安装网络代理

1. 在远程计算机上，打开包含网络代理分发包的文件夹。
2. 打开网络代理分发包（DMG 文件）。
   将会打开一个窗口，其中包含分发包的内容。
3. 在包含分发包内容的窗口中，双击 **卡巴斯基网络代理**。
4. 单击**继续**，确认要安装网络代理。
5. 在**介绍**窗口中，单击**继续**。
6. 在**授权许可**窗口中，阅读您与 AO Kaspersky Lab 之间的网络代理最终用户授权许可协议的文本。执行以下操作：
   - 要接受该协议的所有条款并继续安装，请单击**继续**。
   - 要打印协议文本，请单击**打印**。
   - 要将该协议另存为文本文件，请单击**保存**。

7. 在确认窗口中，执行以下操作之一：
   - 要继续安装网络代理，请单击**同意**。
   - 要返回到最终用户授权许可协议的文本，请单击**阅读授权许可**。
   - 要取消安装，请单击**不同意**。
8. 在**设置**窗口中，执行以下操作：
   a. 在**服务器**字段中，指定安装有 Kaspersky Security Center 的服务器的 IP 地址或 DNS 名称。
   b. 在**端口**字段中，指定与服务器的未加密连接的端口号。
   c. 在 **SSL 端口**字段中，指定与服务器的 SSL 连接的端口号。
   d. 如果希望在安装后立即启动网络代理，请选中**安装后运行**复选框。

   如果不希望使用 SSL 连接到服务器，请取消选中**使用 SSL** 复选框。要继续安装，请单击**继续**。
9. 在**安装类型**窗口中，阅读将在其上安装网络代理的磁盘的相关信息。
   要使用推荐的设置安装网络代理，请单击**安装**并输入管理员密码以确认您所做的选择。
   等待网络代理安装程序完成应用程序组件的安装。
10. 单击**关闭**以退出安装程序。

使用 Apple 远程桌面安装网络代理

1. 在远程计算机上，选择 **Apple 菜单** > **系统设置** > **常规** > **共享**。
2. 选中**远程管理**复选框。
3. 在要用作服务器的另一台 Mac 上，安装 Apple 远程桌面。有关 Apple 远程桌面的更多信息，请参阅 Apple 支持。
4. 打开 Apple 远程桌面。
5. 在**远程桌面**窗口中，单击左侧的**扫描仪**，并选择要在其上安装网络代理的设备。
6. 单击**拷贝**。
7. 单击 + 并选择网络代理安装文件：DMG 文件、KUD 文件和 SH 文件。
8. 在**将项目放入**弹出菜单中，选择**磁盘的顶层文件夹**。
9. 单击**拷贝**。
10. 成功拷贝文件后，单击 **Unix**。
11. 输入以下命令：

```
cd /;
./install.sh --accept_eula -r <管理服务器地址>
```

其中 <管理服务器地址> 为 Kaspersky Security Center 管理服务器的 DNS 名称或 IP 地址。

> **注意：**一旦输入此命令，即表示您接受最终用户授权许可协议。

12. 选择以 **User** 的身份运行此命令，并向字段中键入“root”。
13. 单击**发送**。

将在所选设备上开始安装网络代理。

使用 Kaspersky Security Center 安装网络代理

Kaspersky Security Center 使用 SSH 连接在客户端计算机上安装网络代理。

在客户端计算机上安装网络代理之前，请确保满足以下条件：

- 企业网络上已部署 Kaspersky Security Center 管理服务器。
- Kaspersky Security Center 管理员工作站上已安装管理控制台。
- 远程计算机上已启用远程登录功能。
- 远程计算机上已创建将用来运行远程安装任务的专用管理员账户。您可以使用域账户执行安装。
- 已为专用账户禁用 sudo 密码。

创建网络代理安装包

1. 启动 Kaspersky Security Center 管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 在控制台树中，依次选择**高级**文件夹、**远程安装**子文件夹和**安装包**子文件夹。
4. 在工作区中，单击**创建安装包**。
5. 在**选择安装包类型**窗口中，单击**创建卡巴斯基应用程序安装包**。
6. 在**定义安装包名称**窗口的**名称**字段中，键入新安装包的名称，然后单击**下一步**。
7. 在**为安装选择分发包**窗口中，单击**浏览**。
   将打开一个窗口，用于选择创建安装包所需的文件。
8. 打开包含网络代理安装包内容的文件夹，并选择 klnagent.kud 文件。
   为安装选择分发包窗口将显示要使用所添加的文件远程安装的应用程序的名称和版本。
9. 单击**下一步**。
   已使用指定设置完成 Kaspersky Endpoint Security 安装包的创建。
10. 在向导的最后一个窗口中，单击**完成**以退出新安装包向导。

创建用于在客户端计算机上远程安装网络代理的任务

1. 启动 Kaspersky Security Center 管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 选择**任务**文件夹。
4. 在工作区中，通过单击**新任务**启动新任务向导。
5. 按照新任务向导中的步骤（如下所述）操作，创建用于在客户端计算机上远程安装 Kaspersky Endpoint Security 的任务。

要继续执行向导的下一步骤，请单击**下一步**。要返回到向导的上一步骤，请单击 ←。要在任意步骤退出向导，请单击**取消**。

> **注意：** 按钮外观可能因 Windows 版本而异。

步骤 1.选择任务类型

1. 在“**选择任务类型**”窗口中，最大化“**Kaspersky Security Center 管理服务器**”节点。
2. 选择**远程安装应用程序**任务。

步骤 2.选择安装包

在**选择安装包**窗口中，执行以下操作之一：

- 如果之前已创建包含所需设置的网络代理安装包，请在**选择安装包**窗口上部的安装包列表中选择该安装包。
- 如果尚未创建所需安装包，请单击**新建**以启动新安装包向导。

步骤 3.配置安装设置

在**设置**窗口中，执行以下操作：

1. 选中**通过管理服务器使用操作系统资源**复选框。
2. 取消选中所有其他复选框。

步骤 4.选择在安装后要将计算机添加到的管理组

如有必要，在**移动到受管理设备列表**窗口中，选择在安装后要将计算机移动到的组。

步骤 5.定义如何选择要为其创建任务的客户端计算机

在**选择要对其分配任务的设备**窗口中，选择用于指定客户端计算机的方式：

- 要从管理服务器检测到的网络计算机中进行选择，请选择**选择管理服务器检测到的网络设备**选项。
- 要手动指定计算机的 IP 地址或从文件导入计算机的 IP 地址，请选择**手动指定设备地址或从列表中导入地址**选项。

- 要为基于预设条件的设备分类创建任务，请选择**将任务分配给设备分类**选项。
- 要从特定管理组中选择计算机，请选择**将任务分配给管理组**选项。

步骤 6.选择客户端计算机

在打开的窗口（**选择设备**、**设备分类**或**选择管理组**，具体取决于在上一步骤中选择的选项）中，选择客户端计算机，指定计算机 IP 地址，指定计算机分类，或选择要将任务应用到的管理组。

步骤 7.选择运行任务的账户

1. 在**选择运行任务的账户**窗口中，选中**需要账户（不使用网络代理）**复选框。
2. 单击**添加** > **账户**。
   将打开**账户**窗口。
3. 输入远程计算机的专用管理员账户的登录名和密码。
4. 单击**确定**。

步骤 8.配置任务计划

1. 在**配置任务计划**窗口的**计划开始**下拉列表中，选择启动模式。
2. 如有必要，配置计划任务以自动启动任务（通过指定任务开始日期和时间）。
3. 如果希望运行应用程序未能按计划启动的任务（例如，由于计算机在计划时间已关机），请选中**运行错过的任务**复选框。
   当阻止任务启动的障碍消除后，Kaspersky Endpoint Security 将启动该任务。

步骤 9.指定任务名称

在**定义任务名称**窗口的**名称**字段中，为正在创建的任务输入名称。

步骤 10.完成任务创建

在**完成任务创建**窗口中，执行以下操作：

1. 如何希望在向导完成后立即启动该任务，请选中**向导完成时运行任务**复选框。
2. 单击**完成**以关闭向导。

使用 SSH 协议安装网络代理

在远程计算机上安装网络代理的方式之一是使用 SSH 协议。

确保满足以下要求：

- 企业网络上已部署 Kaspersky Security Center 管理服务器。
- Kaspersky Security Center 管理员工作站上已安装管理控制台。
- 已创建网络代理安装包并将其存储在管理服务器的共享文件夹中。

- 远程计算机上已启用远程登录功能。
- 用于安装网络代理的计算机账户已包含在 sudoer 中。

有关安装包的详细信息，请参阅 Kaspersky Security Center 帮助。

使用 SSH 协议安装网络代理

1. 在管理员工作站上启动 SSH 客户端。
2. 连接到远程计算机。
3. 连接管理服务器的共享文件夹并将其作为远程计算机上的网络驱动器。为此，请在 SSH 客户端中输入以下命令：

   ```
   mkdir /Volumes/KLSHARE
   mount_smbfs //<管理员账户>:<密码>@<管理服务器 IP 地址>/KLSHARE /Volumes/KLSHARE
   ```

   参数描述：

   - <管理员账户> – 管理服务器上的管理员账户名称。
   - <密码> – 管理服务器上的管理员密码。
   - <管理服务器 IP 地址> – 承载 Kaspersky Security Center 的服务器的 IP 地址。

4. 运行安装脚本。为此，请在 SSH 客户端中输入以下命令：

   ```
   cd /Volumes/KLSHARE/<klnagent 包文件夹>
   ```

   其中，<klnagent 包文件夹> 为网络代理安装包所在的文件夹。

   ```
   sudo ./install.sh --accept_eula [-r <服务器>] [-p <端口号>] [-s use_ssl 0|1] [-l
   <SSL 端口号>] [-x use_proxy 0|1] [-a <代理>] [-n <代理登录名>] [-w <代理密码>]
   ```

   参数描述：

   - <服务器> – 安装有 Kaspersky Security Center 的服务器的 IP 地址或 DNS 名称。
   - <端口号> – 与管理服务器建立未加密连接时要使用的端口号。默认情况下使用 14000 端口。
   - use_ssl 0|1 – 定义在网络代理与管理服务器之间建立连接时是否要使用加密的参数。如果该值为“0”，则使用未加密连接。如果该值为“1”，则通过 SSL 协议建立连接（默认值）。
   - <SSL 端口号> – 使用 SSL 协议与管理服务器建立加密连接时要使用的端口号。默认情况下使用 13000 端口。
   - use_proxy 0|1 – 定义连接到互联网时是否使用代理服务器的参数。如果该值为“0”，则不使用代理服务器。如果该值为“1”，则通过代理服务器建立连接（默认值）。
   - <代理> – 代理服务器的 IP 或 DNS 名称。
   - <代理登录名> – 连接到代理服务器所使用的用户账户。
   - <代理密码> – 连接到代理服务器所使用的密码。

   重要： 运行此命令需要具有管理员权限。

5. 断开远程计算机上的网络驱动器连接。为此，请在 SSH 客户端中输入以下命令：
```
umount /Volumes/KLSHARE
```

6. 检查网络代理在远程计算机上是否工作正常。为此，请在 SSH 客户端中输入以下命令：
```
cd /Library/Application\ Support/Kaspersky\ Lab/klnagent/Binaries/
sudo ./klnagchk
```
如果检查成功，则表示网络代理工作正常。

本地卸载网络代理

1. 在远程计算机上，打开包含网络代理分发包的文件夹。
2. 打开网络代理分发包（DMG 文件）。
将会打开一个窗口，其中包含分发包的内容。
3. 在包含分发包内容的窗口中，双击**网络代理卸载程序**。
4. 在**介绍**窗口中，单击**继续**。
5. 在**信息**窗口中，单击**卸载**。
6. 当系统提示您输入管理员凭据时，输入管理员名称和密码并确认您要卸载网络代理。
将开始卸载网络代理。
7. 阅读有关卸载的信息并单击**完成**以退出卸载程序。

现在已从远程计算机中删除网络代理。

从命令行管理网络代理

本节包含有关如何在客户端计算机上使用命令行管理网络代理的信息。

您可以在客户端计算机上使用命令行停止并重新启动网络代理。

您也可以使用 klmover 实用程序将远程计算机手动连接到管理服务器，并使用 klnagchk 实用程序检查远程计算机与管理服务器之间的连接。

您可以卸载网络代理。

在远程计算机上启动/停止网络代理

您可以在客户端计算机上使用命令行停止并重新启动网络代理。

停止网络代理

在远程计算机上，从命令行启动 launchctl 实用程序并执行 unload 命令。

命令语法：

```
sudo launchctl unload /Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

启动网络代理

在远程计算机上，从命令行启动 launchctl 实用程序并执行 load 命令。

命令语法：

```
sudo launchctl load /Library/LaunchDaemons/com.kaspersky.klnagent.plist
```

重要：停止和启动网络代理需要具有管理员权限。

手动检查客户端计算机与管理服务器之间的连接。Klnagchk 实用程序

检查远程计算机与管理服务器之间的连接

在远程计算机上，从命令行运行 klnagchk 实用程序。

klnagchk 实用程序包含在网络代理分发包中。

在安装网络代理后，klnagchk 实用程序位于 /Library/Application Support/Kaspersky Lab/klnagent/Binaries 文件夹中。

根据指定的参数，klnagchk 实用程序在从命令行运行时可执行以下操作：

- 显示为远程计算机上安装的网络代理与管理服务器之间的连接指定的设置，或者将这些设置保存到文件中。
- 将网络代理统计信息（自上次启动网络代理以来）和实用程序执行结果保存到文件中，或在屏幕上显示此信息。
- 尝试在网络代理与管理服务器之间建立连接。
- 如果该实用程序无法建立连接，则会发送 ICMP 数据包以检查安装管理服务器的计算机的状态。

在运行该实用程序之前，在命令行中转到 /Library/Application Support/Kaspersky Lab/klnagent/Binaries。

命令语法：

```
sudo ./klnagchk [-logfile <文件名称>] [-sp] [-savecert <证书文件路径>] [-restart]
```

重要：运行该实用程序需要具有管理员权限。

参数描述

`-logfile <文件名称>` – 将网络代理与管理服务器之间的连接设置和实用程序执行结果保存到文件中。如果未指定此参数，则将在屏幕上显示服务器连接设置、执行结果和错误消息。

`-sp` – 在屏幕上显示代理服务器身份验证的密码或将该密码保存到文件中。如果网络代理通过代理服务器连接到管理服务器，则需使用此参数。默认情况下，不使用此参数。

`-savecert <文件名称>` – 将管理服务器的身份验证证书保存到指定的文件中。

`-restart` – 实用程序运行完成后重启网络代理。

例如：
sudo ./klnagchk -logfile klnagchk.log -sp

将远程计算机手动连接到管理服务器。Klmover 实用程序

将远程计算机连接到管理服务器

在远程计算机上，从命令行运行 klmover 实用程序。

Klmover 实用程序包含在网络代理安装包中。

在安装网络代理后，klmover 实用程序位于 /Library/Application Support/Kaspersky Lab/klnagent/Binaries 文件夹中。

根据指定的参数，klmover 实用程序在从命令行运行时可执行以下操作：

- 使用指定的参数将网络代理连接到管理服务器。
- 将实用程序执行结果保存到文件中或显示在屏幕上。

在运行该实用程序之前，在命令行中转到 /Library/Application Support/Kaspersky Lab/klnagent/Binaries。

命令行语法：

```
sudo ./klmover [-logfile <文件名称>] [-address <服务器地址>] [-pn <端口号>] [-ps <SSL 端口号>] [-nossl] [-cert <证书文件路径>] [-silent] [-dupfix]
```

重要：运行该实用程序需要具有管理员权限。

参数描述

`-logfile <文件名称>` – 将执行结果保存到文件中。如果未指定此参数，则将在屏幕上显示执行结果和错误消息。

`-address <服务器地址>` – 网络代理连接管理服务器时所使用的地址。可以指定服务器的 IP 地址，也可以指定服务器的 DNS 地址。

注意： 通过指定此参数，您还可以使用该命令来更改远程计算机要连接到的管理服务器地址。

`-pn <端口号>` – 与管理服务器建立未加密连接时要使用的端口号。默认情况下使用 14000 端口。

`-ps <SSL 端口号>` – 通过 SSL 协议与管理服务器建立加密连接时要使用的端口号。默认情况下使用 13000 端口。

`-nossl` – 与管理服务器使用未加密连接。如果未指定此参数，网络代理将通过加密 SSL 协议与管理服务器建立安全连接。

`-cert <证书文件路径>` – 在新管理服务器上，使用指定的证书进行身份验证。如果未指定此参数，在首次连接到管理服务器时，网络代理将会收到一份证书。

`-silent` – 以静默模式运行该实用程序。

`-dupfix` – 如果网络代理的安装方式与本帮助中描述的方法不同，例如，从已安装网络代理的磁盘镜像中恢复安装，则需使用此参数。如果网络代理的自动自我识别功能导致原始计算机的图标与管理控制台中的其他计算机的图标重复，请尝试重新连接重复的计算机。

注意： 在运行 klmover 实用程序时，建议指定所有参数的值。

例如：
sudo ./klmover -logfile klmover.log -address 192.0.2.12 -ps 13001

通过网络代理连接到管理服务器的远程计算机称为*客户端计算机*。

卸载网络代理

命令语法：

```
sudo '/Library/Application Support/Kaspersky Lab/klnagent/Binaries/UninstallScript'
```

安装和卸载 Kaspersky Endpoint Security

本节描述如何在客户端计算机上远程安装和卸载 Kaspersky Endpoint Security。

您还可以本地安装或卸载 Kaspersky Endpoint Security，或者通过 Kaspersky Security Center Web Console 或 Kaspersky Security Center 云控制台进行安装或卸载。

使用 SSH 协议安装应用程序

在远程计算机上安装 Kaspersky Endpoint Security 之前，请确保满足以下条件：

- 企业网络上已部署 Kaspersky Security Center 管理服务器。
- Kaspersky Security Center 管理员工作站上已安装管理控制台。
- 已创建 Kaspersky Endpoint Security 安装包且该安装包位于管理服务器上的共享文件夹中。
- Kaspersky Endpoint Security 密钥文件已存储在管理服务器上的共享文件夹中（可选）。
- 远程计算机上已启用远程登录功能。
- 用于安装应用程序的计算机账户已包含在 sudoer 中。

使用 SSH 协议在客户端计算机上安装 Kaspersky Endpoint Security

1. 在 Kaspersky Security Center 管理员工作站上启动 SSH 客户端。
2. 连接到远程计算机。
3. 连接管理服务器的共享文件夹并将其作为远程计算机上的网络驱动器。为此，请在 SSH 客户端中输入以下命令：
   ```
   mkdir /Volumes/KLSHARE
   mount_smbfs //<管理员账户>:<密码>@<管理服务器 IP 地址>/KLSHARE /Volumes/KLSHARE
   ```
   参数描述：
   - <管理员账户> – 管理服务器上的管理员账户名称。
   - <密码> – 管理服务器上的管理员密码。
   - <管理服务器 IP 地址> – 承载 Kaspersky Security Center 的服务器的 IP 地址。
4. 运行安装脚本。为此，请在 SSH 客户端中输入以下命令：
   ```
   cd /Volumes/KLSHARE/<KES 包文件夹>
   ./install.sh --accept_eula
   ```
   其中，<KES 包文件夹> 为 Kaspersky Endpoint Security 安装包所在的文件夹。

   重要：运行此命令需要具有管理员权限。
5. 断开远程计算机上的网络驱动器连接。为此，请在 SSH 客户端中输入以下命令：
   ```
   umount /Volumes/KLSHARE
   ```

使用 Kaspersky Security Center 安装应用程序

在客户端计算机上安装 Kaspersky Endpoint Security 之前，请确保满足以下条件：

- 企业网络上已部署 Kaspersky Security Center 管理服务器。
- Kaspersky Security Center 管理员工作站上已安装管理控制台。
- 客户端计算机上已安装网络代理。
- 已创建 Kaspersky Endpoint Security 安装包并将其存储在管理服务器上的共享文件夹中。
- Kaspersky Endpoint Security 密钥文件已存储在管理服务器上的共享文件夹中（可选）。
- 已将客户端计算机添加到管理服务器上的**受管理设备**管理组中。

有关管理服务器上的管理组的详细信息，请参阅 Kaspersky Security Center 帮助。

要使用 Kaspersky Security Center 在客户端计算机上安装 Kaspersky Endpoint Security，必须创建并启动**远程安装应用程序**任务。

创建用于在客户端计算机上远程安装 Kaspersky Endpoint Security 的任务

1. 启动 Kaspersky Security Center 管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 选择**任务**文件夹。
4. 在工作区中，通过单击**新任务**启动新任务向导。
5. 按照新任务向导中的步骤（如下所述）操作，创建用于在客户端计算机上远程安装 Kaspersky Endpoint Security 的任务。

要继续执行向导的下一步骤，请单击**下一步**。要返回到向导的上一步骤，请单击 ←。要在任意步骤退出向导，请单击**取消**。

> **注意：** 按钮外观可能因 Windows 版本而异。

步骤 1.选择任务类型

1. 在“**选择任务类型**”窗口中，最大化“**Kaspersky Security Center 管理服务器**”节点。
2. 选择**远程安装应用程序**任务。

步骤 2.选择安装包

在**选择安装包**窗口中，执行以下操作之一：

- 如果之前已创建包含所需设置的 Kaspersky Endpoint Security 安装包，请在**选择安装包**窗口上部的安装包列表中选择该安装包。
- 如果尚未创建所需安装包，请单击**新建**以启动新安装包向导。

步骤 3.安装附加应用程序

如果还希望在客户端计算机上安装网络代理，请在**高级**窗口中选中**网络代理和该程序一起安装**及 **<网络代理安装包名称>** 复选框。

注意：必须预先创建好网络代理安装包。如果尚未创建该安装包，请单击**创建**以启动新安装包向导。

步骤 4.配置安装设置

在**设置**窗口中，配置应用程序远程安装设置。

步骤 5.选择在安装后要将计算机添加到的管理组

如有必要，在**移动到受管理设备列表**窗口中，选择在安装后要将计算机移动到的组。

注意：如果在步骤 3 中选择安装网络代理，则会显示**移动到受管理设备列表**窗口。

步骤 6.定义如何选择要为其创建任务的客户端计算机

在**选择要对其分配任务的设备**窗口中，选择用于指定客户端计算机的方式：

- 要从管理服务器检测到的网络计算机中进行选择，请选择**选择管理服务器检测到的网络设备**选项。
- 要手动指定计算机的 IP 地址或从文件导入计算机的 IP 地址，请选择**手动指定设备地址或从列表中导入地址**选项。
- 要为基于预设条件的设备分类创建任务，请选择**将任务分配给设备分类**选项。
- 要从特定管理组中选择计算机，请选择**将任务分配给管理组**选项。

步骤 7.选择客户端计算机

在打开的窗口（**选择设备**、**设备分类**或**选择管理组**，具体取决于在上一步骤中选择的选项）中，选择客户端计算机，指定计算机 IP 地址，指定计算机分类，或选择要将任务应用到的管理组。

步骤 8.选择运行任务的账户

在**选择运行任务的账户**窗口中，选中**不需要账户（网络代理已安装）**复选框。

该选项假定您在启动此向导之前已安装网络代理。

步骤 9.配置任务计划

1. 在**配置任务计划**窗口的**计划开始**下拉列表中，选择启动模式。
2. 如有必要，配置计划任务以自动启动任务（通过指定任务开始日期和时间）。
3. 如果希望运行应用程序未能按计划启动的任务（例如，由于计算机在计划时间已关机），请选中**运行错过的任务**复选框。

   当阻止任务启动的障碍消除后，Kaspersky Endpoint Security 将启动该任务。

步骤 10.指定任务名称

在**定义任务名称**窗口的**名称**字段中，为正在创建的任务输入名称。

步骤 11.完成任务创建

在**完成任务创建**窗口中，执行以下操作：

1. 如何希望在向导完成后立即启动该任务，请选中**向导完成时运行任务**复选框。
2. 单击**完成**以关闭向导。

所创建的任务将显示在**任务**文件夹的工作区中。

创建安装包

在创建**远程安装应用程序**任务时，您可以使用现有的安装包，也可以创建新的安装包。要查看已创建的安装包列表，请单击**高级** > **远程安装** > **安装包**。

在 Kaspersky Security Center 中创建安装包

1. 启动 Kaspersky Security Center 管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 在控制台树中，依次选择**高级**文件夹、**远程安装**子文件夹和**安装包**子文件夹。
4. 在工作区中，单击**创建安装包**。
5. 在**选择安装包类型**窗口中，单击**创建卡巴斯基应用程序安装包**。
6. 在**定义安装包名称**窗口的**名称**字段中，键入新安装包的名称，然后单击**下一步**。
7. 在**为安装选择分发包**窗口中，单击**浏览**。
   将打开一个窗口，用于选择创建安装包所需的文件。
8. 打开包含 Kaspersky Endpoint Security 安装包内容的文件夹，并选择 kesmac.kud 文件。
   为安装选择分发包窗口将显示要使用所添加的文件远程安装的应用程序的名称和版本。
9. 如有必要，选中**将更新从存储库复制到安装包**复选框，以将应用程序更新从 Kaspersky Security Center 存储库复制到安装包，然后单击**下一步**。
   安装包开始上传到管理服务器。上传完成后，将打开**安装类型**窗口。
10. 在“**安装类型**”窗口的“**要安装的包**”区域中，取消选中希望在客户端计算机上执行安装的过程中跳过的组件名称旁边的复选框，然后单击“**下一步**”。
    已使用指定设置完成 Kaspersky Endpoint Security 安装包的创建。
11. 在向导的最后一个窗口中，单击**完成**以完成新安装包向导。

使用 Kaspersky Security Center 卸载应用程序

在通过 Kaspersky Security Center 从客户端计算机中删除 Kaspersky Endpoint Security 之前，请确保满足以下条件：

- 企业网络上已部署 Kaspersky Security Center 管理服务器。
- Kaspersky Security Center 管理员工作站上已安装管理控制台。
- 客户端计算机上已安装网络代理。

要通过 Kaspersky Security Center 从客户端计算机中卸载 Kaspersky Endpoint Security，必须创建并启动**远程卸载应用程序**任务。

重要：从客户端计算机中删除 Kaspersky Endpoint Security 可能导致感染风险。

创建用于从客户端计算机中远程卸载 Kaspersky Endpoint Security 的任务

1. 启动 Kaspersky Security Center 管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 选择**任务**文件夹。
4. 在工作区中，通过单击**新任务**启动新任务向导。
5. 按照新任务向导中的步骤（如下所述）操作，创建用于从客户端计算机中远程卸载 Kaspersky Endpoint Security 的任务。

要继续执行向导的下一步骤，请单击**下一步**。要返回到向导的上一步骤，请单击 ←。要在任意步骤退出向导，请单击**取消**。

注意：按钮外观可能因 Windows 版本而异。

步骤 1.选择任务类型

1. 在“**选择任务类型**”窗口中，最大化“**Kaspersky Security Center 管理服务器**”节点。
2. 展开**高级**子节点。
3. 选择**远程卸载应用程序**任务。

步骤 2.选择要卸载的应用程序

在“**选择要卸载的应用程序**”窗口中，选择“**卸载 Kaspersky Security Center 支持的应用程序**”。

步骤 3.配置卸载设置

在**设置**窗口中，执行以下操作：

1. 在“**要卸载的应用程序**”下拉列表中，选择 **Kaspersky Endpoint Security for Mac 12.2.1**。
2. 单击**下一步**。
3. 配置应用程序远程卸载设置。

步骤 4.选择操作系统重启选项

在**选择操作系统重启选项**窗口中，选择**不重启设备**选项。

步骤 5.定义如何选择要为其创建任务的客户端计算机

在**选择要对其分配任务的设备**窗口中，选择用于指定客户端计算机的方式：

- 要从管理服务器检测到的网络计算机中进行选择，请选择**选择管理服务器检测到的网络设备**选项。
- 要手动指定计算机的 IP 地址或从文件导入计算机的 IP 地址，请选择**手动指定设备地址或从列表中导入地址**选项。
- 要为基于预设条件的设备分类创建任务，请选择**将任务分配给设备分类**选项。
- 要从特定管理组中选择计算机，请选择**将任务分配给管理组**选项。

步骤 6.选择客户端计算机

在打开的窗口（**选择设备**、**设备分类**或**选择管理组**，具体取决于在上一步骤中选择的选项）中，选择客户端计算机，指定计算机 IP 地址，指定计算机分类，或选择要将任务应用到的管理组。

步骤 7.选择运行任务的账户

在**选择运行任务的账户**窗口中，选中**不需要账户（网络代理已安装）**复选框。

该选项假定您在启动此向导之前已安装网络代理。

步骤 8.配置任务计划

1. 在**配置任务计划**窗口的**计划开始**下拉列表中，选择启动模式。
2. 如有必要，配置计划任务以自动启动任务（通过指定任务开始日期和时间）。
3. 如果希望运行应用程序未能按计划启动的任务（例如，由于计算机在计划时间已关机），请选中**运行错过的任务**复选框。

   当阻止任务启动的障碍消除后，Kaspersky Endpoint Security 将启动该任务。

步骤 9.指定任务名称

在**定义任务名称**窗口的**名称**字段中，为正在创建的任务输入名称。

步骤 10.完成任务创建

在**完成任务创建**窗口中，执行以下操作：

1. 如何希望在向导完成后立即启动该任务，请选中**向导完成时运行任务**复选框。
2. 单击**完成**以关闭向导。

所创建的任务将显示在**任务**文件夹的工作区中。

通过 Kaspersky Security Center 启动和停止应用程序

您可以通过 Kaspersky Security Center 在受管理设备列表中的选定计算机上启动或停止 Kaspersky Endpoint Security。

通过 Kaspersky Security Center 启动或停止 Kaspersky Endpoint Security

1. 启动 Kaspersky Security Center 管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 在控制台树中，单击**受管理设备**。
4. 选择包含所需客户端计算机的管理组。
5. 选择**设备**选项卡。
6. 从客户端计算机列表中选择计算机。
7. 采用以下方式之一打开**属性: <计算机名称>** 窗口：
   - 双击客户端计算机的名称。
   - 右键单击客户端计算机并从上下文菜单中选择**属性**。
8. 选择**应用程序**区域。
9. 在"**设备上安装的卡巴斯基应用程序**"列表中，右键单击以打开 **Kaspersky Endpoint Security for Mac 12.2.1** 项的上下文菜单，并执行以下操作之一：
   - 要启动应用程序，请选择**开始**项。
   - 要停止应用程序，请选择**停止**项。

重要： 停止 Kaspersky Endpoint Security 后，客户端计算机将在未受保护模式下继续运行，这可能导致感染风险。

创建和管理任务

本节描述如何使用 Kaspersky Security Center 创建和配置供 Kaspersky Endpoint Security 在一台客户端计算机或一组计算机上执行的任务。

任务 是供 Kaspersky Endpoint Security 在客户端计算机上执行的一组可配置的操作。

在 Kaspersky Security Center 中，您可以创建以下任务：

- 添加密钥
- 快速扫描
- 回滚
- 扫描
- 更新

您可以对任务执行以下操作：

- 启动和停止任务。
- 配置任务设置。
- 跟踪任务进度。
- 将任务从一个组复制和移动到另一个组。
- 删除任务。
- 导入和导出任务。

有关任务的更多信息，请参阅 Kaspersky Security Center 帮助。

创建任务

通过 Kaspersky Security Center 管理 Kaspersky Endpoint Security 时，可创建以下类型的任务：

- 本地任务。*本地任务* 是指在单独的客户端计算机上运行的任务。
- 组任务。*组任务* 是指在管理组内的计算机上运行的任务。
- 适用于任意计算机组的任务。您可以创建要在任意计算机上运行的任务，无论这些计算机是否属于某个管理组或计算机分类。

为单独的客户端计算机创建本地任务

1. 启动 Kaspersky Security Center 管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 在控制台树中，单击**受管理设备**。
4. 选择包含所需客户端计算机的管理组。
5. 在工作区中，选择**设备**选项卡。
6. 从客户端计算机列表中选择计算机。

7. 采用以下方式之一打开**属性: <计算机名称>** 窗口：
   - 双击客户端计算机的名称。
   - 右键单击客户端计算机并从上下文菜单中选择**属性**。
8. 在**属性: <计算机名称>** 窗口中，选择**任务**区域。
   将在右侧的工作区中显示所选客户端计算机的系统任务和自定义任务列表。
9. 单击工作区下部的**添加**。
   将启动新任务向导。
10. 按照新任务向导的步骤操作，为单独的客户端计算机创建本地任务。

为管理组中的客户端计算机创建任务

1. 启动 Kaspersky Security Center 管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 在控制台树中，单击**受管理设备**。
4. 选择包含所需客户端计算机的管理组。
5. 在工作区中，选择**任务**选项卡。
6. 在工作区中，通过单击**新任务**启动新任务向导。
7. 按照新任务向导的步骤操作，为管理组中包含的客户端计算机创建任务。

有关如何创建组任务的详细信息，请参阅 Kaspersky Security Center 帮助。

为任意计算机组创建任务

1. 启动 Kaspersky Security Center 管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 在控制台树中，单击**任务**。
4. 在工作区中，通过单击**新任务**启动新任务向导。
5. 按照新任务向导的步骤操作，为任意计算机组创建任务。

要继续执行向导的下一步骤，请单击**下一步**。要返回到向导的上一步骤，请单击 ←。要在任意步骤退出向导，请单击**取消**。

注意： 按钮外观可能因 Windows 版本而异。

步骤 1.选择应用程序并定义任务类型

1. 在“**选择任务类型**”窗口中，最大化 **Kaspersky Endpoint Security for Mac 12.2.1** 节点。
2. 选择要创建的任务的类型：
   - 要创建用于添加密钥的任务，请选择**添加密钥**。
   - 要创建关键区域扫描任务，请选择**快速扫描**。
   - 要创建用于回滚上一次更新的任务，请选择**回滚**。
   - 要创建恶意软件扫描任务，请选择**扫描**。
   - 要创建更新任务，请选择**更新**。

步骤 2.配置所选任务类型的设置

取决于上一步骤所选择的任务类型，设置窗口中的内容可能会有所不同。“回滚”任务不显示此窗口。

应用程序激活

在**应用程序激活**窗口中，执行以下操作：

1. 从 Kaspersky Security Center 存储中选择激活码或密钥，或者添加您的计算机上存储的密钥文件。
2. 要将指定的密钥添加为备用密钥，请选中**添加为备用密钥**复选框。
   在当前激活密钥到期时，备用密钥将成为激活密钥。

所指定密钥的相关信息（密钥、密钥类型和到期日期）显示在**应用程序激活**窗口中。

更新

专用的卡巴斯基更新服务器是 Kaspersky Endpoint Security 的主更新源。Kaspersky Endpoint Security 也可以使用分发点、本地文件夹或其他 Web 服务器作为*更新源*。

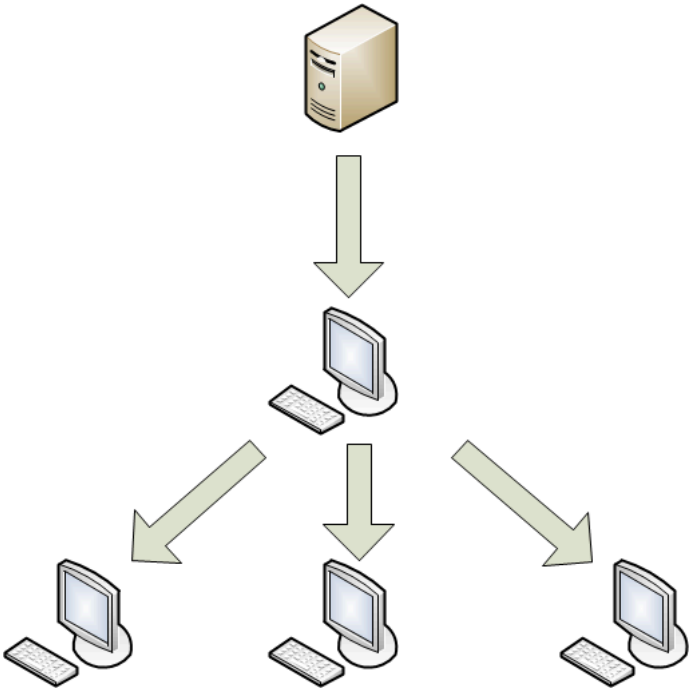
您可以将更新下载到本地文件夹以更新企业网络中其他计算机上的应用程序数据库和 Kaspersky Endpoint Security 模块，以便减少网络流量。

可按如下方式设置更新分发：

1. 网络上的一台计算机从卡巴斯基更新服务器或其他更新源接收 Kaspersky Endpoint Security 更新包。将检索到的更新放置到共享的本地文件夹中。

   注意：必须提前创建共享的本地文件夹。

2. 网络上的其他计算机使用共享的本地文件夹作为更新源。



通过本地计算机分发更新

如有必要，在**更新**窗口中编辑更新任务设置：

1. 要禁用应用程序模块更新，请取消选中**更新应用程序模块**复选框。
2. 更改更新源：
   a. 单击**设置**。
   将打开**设置: 更新**窗口。
   b. 选中要使用的更新源旁边的复选框。
3. 要指定其他更新源，请单击**添加**。
   将打开**更新源**窗口。
   a. 指定更新源的网址或者作为更新源的本地或网络文件夹的路径，然后单击**确定**。
   b. 单击**确定**以保存更改并关闭**设置: 更新**窗口。

扫描和快速扫描

默认情况下，Kaspersky Endpoint Security 使用**建议**安全级别，在执行扫描后，当检测到受感染对象时提示用户执行操作，该安全级别将扫描以下对象：

- 所有可移动驱动器
- 所有内部驱动器

- 所有网络驱动器
- 内存

注意：Kaspersky Endpoint Security 不会扫描位于 OneDrive 或 iCloud 存储或者其他云存储中的文件。请将这些文件排除在扫描范围之外。否则，扫描任务可能会以“*受感染文件未删除*”错误结束。

如有必要，在**扫描**窗口中编辑扫描设置：

1. 选择预设的安全级别之一，或自定义安全设置。
2. 选择 Kaspersky Endpoint Security 在检测到受感染对象时执行的操作。
3. 定义扫描范围。

步骤 3.定义如何选择要为其创建任务的客户端计算机

注意：对于本地任务或组任务，可忽略此步骤。

在**选择要对其分配任务的设备**窗口中，选择用于指定客户端计算机的方式：

- 要从管理服务器检测到的网络计算机中进行选择，请选择**选择管理服务器检测到的网络设备**选项。
- 要手动指定计算机的 IP 地址或从文件导入计算机的 IP 地址，请选择**手动指定设备地址或从列表中导入地址**选项。
- 要为基于预设条件的设备分类创建任务，请选择**将任务分配给设备分类**选项。
- 要从特定管理组中选择计算机，请选择**将任务分配给管理组**选项。

步骤 4.选择客户端计算机

注意：对于本地任务或组任务，可忽略此步骤。

在打开的窗口（**选择设备**、**设备分类**或**选择管理组**，具体取决于在上一步骤中选择的选项）中，选择客户端计算机，指定计算机 IP 地址，指定计算机分类，或选择要将任务应用到的管理组。

步骤 5.配置任务计划

1. 在**配置任务计划**窗口的**计划开始**下拉列表中，选择启动模式。
2. 如有必要，配置计划任务以自动启动任务（通过指定任务开始日期和时间）。
3. 如果希望运行应用程序未能按计划启动的任务（例如，由于计算机在计划时间已关机），请选中**运行错过的任务**复选框。

   当阻止任务启动的障碍消除后，Kaspersky Endpoint Security 将启动该任务。
4. 如果希望 Kaspersky Security Center 自动确定不同计算机上的任务启动间隔，请选中**自动随机设置任务启动延迟时间**复选框。

   这有助于降低 Kaspersky Security Center 管理服务器的负荷。

5. 要手动设置不同计算机上的任务启动间隔，请选中**在以下时间间隔内随机设置任务启动延迟时间（分钟）**复选框。

   这有助于降低 Kaspersky Security Center 管理服务器的负荷。

步骤 6.指定任务名称

在**定义任务名称**窗口的**名称**字段中，为正在创建的任务输入名称。

步骤 7.完成任务创建

在**完成任务创建**窗口中，执行以下操作：

1. 如何希望在向导完成后立即启动该任务，请选中**向导完成时运行任务**复选框。
2. 单击**完成**以关闭向导。

手动启动和停止任务

计划任务会按照计划自动启动。不过，您也可以随时手动启动任务。

注意：仅当网络代理正在运行时，才可在客户端计算机上启动任务。如果网络代理停止运行，则所有活动任务都将被中断。

手动启动和停止任务

1. 打开包含要启动或停止的任务的任务列表。
2. 选择要启动或停止的任务。
3. 采用以下方式之一启动或停止任务：
   - 右键单击任务以显示其上下文菜单，然后选择**启动**或**停止**。
   - 在工作区中，单击**启动**或**停止**。
   - 右键单击任务以显示其上下文菜单，然后选择**属性**。在打开的窗口中，单击**启动**或**停止**。

导入和导出任务

您可以将组任务和适用于任意计算机组的任务导出到文件。

导出任务

1. 选择要从中导出任务的任务列表：
   - 选择管理组并打开**任务**选项卡。
   - 在控制台树中，单击**任务**。

2. 右键单击要导出的任务，然后在任务的快捷菜单中，选择**所有任务** > **导出**。

3. 在**另存为**窗口中，指定文件名和要将导出的任务保存到的位置。

4. 单击**保存**。

导入任务

1. 选择要将任务导入到的任务列表：

   - 选择管理组并打开**任务**选项卡。
   - 在控制台树中，单击**任务**。

2. 采用以下任一方式导入任务：

   - 在任务列表的快捷菜单中，选择**所有任务** > **导入**。
   - 单击**从文件导入任务**。

3. 在**打开**窗口中，指定要导入的任务文件的路径。

4. 单击**打开**。

   该任务将显示在任务列表中。

查看任务

您可以查看为特定计算机或特定管理组中的计算机创建的任务列表，或查看所有非本地任务列表。

查看特定管理组的任务

1. 启动 Kaspersky Security Center 管理控制台。

2. 最大化**管理服务器 <服务器名称>** 节点。

3. 在控制台树中，单击**受管理设备**。

4. 选择包含所需客户端计算机的管理组。

5. 在工作区中，选择**任务**选项卡。

   将显示所选管理组中的计算机的任务列表。

查看本地任务

1. 启动 Kaspersky Security Center 管理控制台。

2. 最大化**管理服务器 <服务器名称>** 节点。

3. 在控制台树中，单击**受管理设备**。

4. 选择包含所需客户端计算机的管理组。

5. 在工作区中，选择**设备**选项卡。

6. 从客户端计算机列表中选择计算机。

7. 采用以下方式之一打开**属性: <计算机名称>** 窗口：

   - 双击客户端计算机的名称。
   - 右键单击客户端计算机并从上下文菜单中选择**属性**。

8. 在**属性: <计算机名称>** 窗口中，选择**任务**区域。

将在右侧的工作区中显示所选客户端计算机的系统任务和自定义任务列表。

查看非本地任务

1. 启动 Kaspersky Security Center 管理控制台。

2. 最大化**管理服务器 <服务器名称>** 节点。

3. 在控制台树中，单击**任务**。

将显示为计算机（无论是否属于管理组）创建的非本地任务列表。

管理任务特定设置

查看本地任务设置

1. 打开本地任务列表。

2. 选择列表中的任务，并采用以下方式之一打开任务设置：

   - 双击任务名称。
   - 右键单击任务以显示其快捷菜单，然后选择**属性**。

查看组任务设置

1. 打开管理组的组任务列表。

2. 选择列表中的任务，并采用以下方式之一打开任务设置：

   - 双击任务名称。
   - 右键单击任务以显示其快捷菜单，然后选择**属性**。
   - 单击工作区中的**配置任务**链接。

查看非本地任务设置

1. 打开非本地任务列表。
2. 选择列表中的任务，并采用以下方式之一打开任务设置：
   - 双击任务名称。
   - 右键单击任务以显示其快捷菜单，然后选择**属性**。
   - 单击工作区中的**配置任务**链接。

有关任务的更多信息，请参阅 Kaspersky Security Center 帮助。

对于本地任务、组任务或适用于任意计算机组的任务

配置“添加密钥”任务设置

1. 打开包含**添加密钥**任务设置的窗口。
2. 选择**应用程序激活**区域。
3. 如有必要，采用以下方式之一添加其他密钥：
   - 从添加到 Kaspersky Security Center 存储的激活码中选择密钥或激活码：
     a. 选择**密钥或激活码**选项。
     b. 单击**浏览**。
     将打开 **Kaspersky Security Center 存储中的密钥和激活码**窗口。
     c. 选择密钥或激活码。
     d. 单击**确定**。
   - 添加密钥文件：
     a. 选择**密钥文件**选项。
     b. 单击**添加**。
     将打开文件选择窗口。
     c. 选择密钥文件。
     d. 单击**打开**。

> **注意：**添加其他密钥时，将会删除当前密钥。

4. 要将指定的密钥添加为备用密钥，请选中**添加为备用密钥**复选框。
   在当前密钥到期时，备用密钥将成为激活密钥。

注意：备用密钥到期日期必须晚于当前密钥到期日期。

5. 通过以下方式之一保存更改：

- 单击**应用**，保存更改后，仍留在**属性: <任务名称>** 窗口中。
- 单击**确定**，保存更改后，将关闭**属性: <任务名称>** 窗口。

管理"快速扫描"任务设置

1. 打开包含**快速扫描**任务设置的窗口。
2. 选择**快速扫描**区域。
3. 要更改 Kaspersky Endpoint Security 运行快速扫描任务的安全级别，请在**安全级别**区域中执行以下操作之一：

- 通过沿刻度向上或向下移动滑块，选择预设的安全级别。
  您可以选择以下安全级别之一：
  - **最大保护**。Kaspersky Endpoint Security 对打开、保存或执行的文件执行最大范围的监控。
  - **建议**。Kaspersky Endpoint Security 采用卡巴斯基推荐设置对文件进行监控。
    这是默认的安全级别。
  - **最大速度**。Kaspersky Endpoint Security 对最小范围的文件进行监控。如果您想使用其他需要大量内存资源的应用程序，可以选择此安全级别。
- 手动配置安全设置：
  a. 单击**设置**。
  将打开**设置: 扫描**窗口。
  b. 在**常规**选项卡的**文件类型**区域中，选择 Kaspersky Endpoint Security 在运行快速扫描任务时应扫描的文件类型。
  c. 在**常规**选项卡的**优化**区域中，配置扫描性能设置。
  d. 在**常规**选项卡的**复合文件**区域中，选择希望 Kaspersky Endpoint Security 对其执行可检测对象分析的复合文件。
  e. 在**高级**选项卡的**高级设置**区域中，配置使用 iSwift 技术，并在应用程序统计信息中保存检测到的对象的相关信息。
  f. 在**高级**选项卡的**启发式分析器**区域中，配置使用启发式分析器，并选择恶意软件扫描过程中启发式分析器要应用的保护级别。
  g. 单击**确定**以保存更改并关闭**设置: 扫描**窗口。
  安全级别将更改为**自定义**。
- 要恢复默认设置，请单击**默认**。
  安全级别将更改为**建议**。

4. 如有必要，在**操作**区域中，选择 Kaspersky Endpoint Security 在检测到受感染对象时要执行的操作。

5. 要指定扫描范围，请在**扫描范围**区域中，单击**设置**，然后在打开的**扫描范围**窗口中执行以下操作：

   a. 如果希望 Kaspersky Endpoint Security 扫描计算机内存，请选中**内存**复选框。

   b. 如果希望 Kaspersky Endpoint Security 扫描启动对象，请选中**登录项**复选框。

   c. 如果希望 Kaspersky Endpoint Security 扫描其他文件或文件夹，请选择**添加**，并指定文件或文件夹，或者指定文件或文件夹名称的掩码。

   d. 单击**确定**以保存更改并关闭**扫描范围**窗口。

6. 通过以下方式之一保存更改：

   - 单击**应用**，保存更改后，仍留在**属性: <任务名称>** 窗口中。
   - 单击**确定**，保存更改后，将关闭**属性: <任务名称>** 窗口。

配置"扫描"任务设置

1. 打开包含**扫描**任务设置的窗口。
2. 选择**扫描**区域。
3. 要更改 Kaspersky Endpoint Security 运行扫描任务的安全级别，请在**安全级别**区域中执行以下操作之一：

   - 通过沿刻度向上或向下移动滑块，选择预设的安全级别。

     您可以选择以下安全级别之一：

     - **最大保护**。Kaspersky Endpoint Security 对打开、保存或执行的文件执行最大范围的监控。
     - **建议**。Kaspersky Endpoint Security 采用卡巴斯基推荐设置对文件进行监控。

       这是默认的安全级别。
     - **最大速度**。Kaspersky Endpoint Security 对最小范围的文件进行监控。如果您想使用其他需要大量内存资源的应用程序，可以选择此安全级别。

   - 手动配置安全设置：

     a. 单击**设置**。

     将打开**设置: 扫描**窗口。

     b. 在**常规**选项卡的**文件类型**区域中，选择 Kaspersky Endpoint Security 在运行扫描任务时应扫描的文件类型。

     c. 在**常规**选项卡的**优化**区域中，配置扫描性能设置。

     d. 在**常规**选项卡的**复合文件**区域中，选择希望 Kaspersky Endpoint Security 对其执行可检测对象分析的复合文件。

     e. 在**高级**选项卡的**高级设置**区域中，配置使用 iSwift 技术，并在应用程序统计信息中保存检测到的对象的相关信息。

     f. 在**高级**选项卡的**启发式分析器**区域中，配置使用启发式分析器，并选择恶意软件扫描过程中启发式分析器要应用的保护级别。

g. 单击**确定**以保存更改并关闭**设置: 扫描**窗口。
安全级别将更改为**自定义**。

- 要恢复默认设置，请单击**默认**。
安全级别将更改为**建议**。

4. 如有必要，在**操作**区域中，选择 Kaspersky Endpoint Security 在检测到受感染对象时要执行的操作。

5. 要指定扫描范围，请在**扫描范围**区域中，单击**设置**，然后在打开的**扫描范围**窗口中执行以下操作：

a. 如果希望 Kaspersky Endpoint Security 扫描所有可移动驱动器，请选中**所有可移动磁盘**复选框。

b. 如果希望 Kaspersky Endpoint Security 扫描所有内部驱动器，请选中**所有内部磁盘**复选框。

c. 如果希望 Kaspersky Endpoint Security 扫描所有网络驱动器，请选中**所有网络磁盘**复选框。

d. 如果希望 Kaspersky Endpoint Security 扫描计算机内存，请选中**内存**复选框。

e. 如果希望 Kaspersky Endpoint Security 扫描启动对象，请选中**登录项**复选框。

f. 如果希望 Kaspersky Endpoint Security 扫描其他文件或文件夹，请选择**添加**，并指定文件或文件夹，或者指定文件或文件夹名称的掩码。

g. 单击**确定**以保存更改并关闭**扫描范围**窗口。

6. 通过以下方式之一保存更改：

- 单击**应用**，保存更改后，仍留在**属性: <任务名称>** 窗口中。

- 单击**确定**，保存更改后，将关闭**属性: <任务名称>** 窗口。

管理“更新”任务设置

1. 打开包含**更新**任务设置的窗口。

2. 选择**更新**区域。

3. 如果希望 Kaspersky Endpoint Security 同时更新应用程序模块和应用程序数据库，请选中**更新应用程序模块**复选框。

4. 选择更新源：

a. 单击**设置**。
将打开**设置: 更新**窗口。

b. 通过以下方式之一指定更新源：

- 如果希望应用程序从管理服务器下载更新，请选中 **Kaspersky Security Center** 复选框。

- 如果希望应用程序从卡巴斯基更新服务器下载更新，请选中 **Kaspersky 更新服务器**复选框。

- 要添加其他更新源，请单击**添加**，然后在打开的窗口中，输入更新源的路径。
  默认情况下，Kaspersky Endpoint Security 从卡巴斯基更新服务器下载更新。

c. 单击**确定**以保存更改并关闭**设置: 更新**窗口。

5. 通过以下方式之一保存更改：

- 单击**应用**，保存更改后，仍留在**属性: <任务名称>** 窗口中。
- 单击**确定**，保存更改后，将关闭**属性: <任务名称>** 窗口。

仅对于本地任务

管理“文件威胁防护”任务设置

1. 打开客户端计算机的本地任务列表。
2. 在本地任务列表中，选择“文件威胁防护”任务，并采用以下方式之一打开其属性：
   - 双击任务名称。
   - 右键单击任务以显示其快捷菜单，然后选择**属性**。
   - 单击**属性**。
3. 选择**文件威胁防护**区域。
4. 如有必要，配置以下设置：
   - 在客户端计算机上启用或禁用文件威胁防护。
   - 要选择预设的安全级别之一，请使用**安全级别**区域中的滑块。
   - 要手动配置安全级别，请单击**设置**，然后在打开的**设置: 文件威胁防护**窗口中，执行以下操作：
     a. 在**常规**选项卡的**文件类型**区域中，选择在打开、执行或保存文件时，Kaspersky Endpoint Security 应扫描的文件类型。
     b. 在**常规**选项卡的**优化**区域中，配置扫描性能设置，并选择扫描技术，以及选择在客户端计算机上，Kaspersky Endpoint Security 是否将跳过扫描只读系统卷。
     c. 在**常规**选项卡的**复合文件**区域中，选择应对其执行可检测对象扫描的复合文件，并对大型对象设置扫描限制。
     d. 在**保护范围**选项卡上，指定文件威胁防护应扫描的文件或文件夹。
     默认情况下，将扫描位于连接到客户端计算机的可移动驱动器、内部驱动器和网络驱动器上的所有对象。您可以向保护范围中添加对象，修改列表中的对象，暂时禁用对列表中某个对象的扫描，或者从列表中删除对象。
     e. 在**高级**选项卡的**扫描模式**区域中，选择“文件威胁防护”模式。

f. 在**高级**选项卡的**暂停任务**区域中，启用或禁用文件威胁防护的暂停计划，并配置按照计划自动暂停任务。

g. 在**高级**选项卡的**启发式分析器**区域中，配置文件威胁防护使用启发式分析器。

h. 单击**确定**以保存更改并关闭**设置: 文件威胁防护**窗口。

- 在**若检测到恶意对象**区域中，选择在检测到受感染对象时，文件威胁防护要执行的操作。

5. 通过以下方式之一保存更改：

- 单击**应用**，保存更改后，仍留在**属性: 文件威胁防护**窗口中。
- 单击**确定**，保存更改后，将关闭**属性: 文件威胁防护**窗口。

管理“Web 威胁防护”任务设置

1. 打开客户端计算机的本地任务列表。
2. 在本地任务列表中，选择“Web 威胁防护”任务，并采用以下方式之一打开其属性：

- 双击任务名称。
- 右键单击任务以显示其快捷菜单，然后选择**属性**。
- 单击**属性**。

3. 选择 **Web 威胁防护**区域。
4. 如有必要，配置以下设置：

- 在客户端计算机上启用或禁用 Web 威胁防护。
- 要选择预设的安全级别之一，请使用**安全级别**区域中的滑块。
- 要手动配置安全级别，请单击**设置**，然后在打开的**设置: Web 威胁防护**窗口中，执行以下操作：

a. 在**常规**选项卡的**扫描模式**区域中，启用或禁用对照恶意网址数据库检查网址。

b. 在**常规**选项卡的**反钓鱼设置**区域中，启用或禁用对照钓鱼网址数据库检查网址。

c. 在**常规**选项卡的**反钓鱼设置**区域中，启用或禁用使用启发式分析器检测钓鱼链接。

d. 在**信受任网址**选项卡上，启用或禁用扫描受信任网址的 Web 流量，以及创建或编辑受信任网址列表。

e. 单击**确定**以保存更改并关闭**设置: Web 威胁防护**窗口。

5. 在**若检测到恶意对象**区域中，选择当在 Web 流量中检测到危险对象时，Web 威胁防护要执行的操作。
6. 通过以下方式之一保存更改：

- 单击**应用**，保存更改后，仍留在**属性: Web 威胁防护**窗口中。
- 单击**确定**，保存更改后，将关闭**属性: Web 威胁防护**窗口。

管理“快速扫描”任务设置

1. 打开客户端计算机的本地任务列表。
2. 在本地任务列表中，选择“快速扫描”任务，并采用以下方式之一打开其属性：
   - 双击任务名称。
   - 右键单击任务以显示其快捷菜单，然后选择**属性**。
   - 单击**属性**。
3. 选择**扫描**区域。
4. 如有必要，配置以下设置：
   - 要选择预设的安全级别之一，请使用**安全级别**区域中的滑块。
   - 要手动配置安全级别，请单击**设置**，然后在打开的**设置: 扫描**窗口中，执行以下操作：
     a. 在**常规**选项卡的**文件类型**区域中，选择 Kaspersky Endpoint Security 应扫描的文件类型。
     b. 在**常规**选项卡的**优化**区域中，配置扫描性能设置。
     c. 在**常规**选项卡的**复合文件**区域中，选择希望 Kaspersky Endpoint Security 扫描的复合文件。
     d. 在**高级**选项卡的**高级设置**区域中，配置使用 iSwift 技术，并在应用程序统计信息中保存检测到的对象的相关信息。
     e. 在**高级**选项卡的**启发式分析器**区域中，配置使用启发式分析器，并选择启发式分析器要应用的保护级别。
     f. 单击**确定**以保存更改并关闭**设置: 扫描**窗口。
   - 在**操作**区域中，选择 Kaspersky Endpoint Security 在检测到受感染对象时要执行的操作。
   - 要指定扫描范围，请在**扫描范围**区域中，单击**设置**，然后在打开的**扫描范围**窗口中执行以下操作：
     - 如果希望 Kaspersky Endpoint Security 扫描默认列表中的对象，请选中相关对象旁边的复选框。
     - 如果希望 Kaspersky Endpoint Security 扫描其他文件或文件夹，请选择**添加**，并指定文件或文件夹，或者指定文件或文件夹名称的掩码。
     - 单击**确定**以保存更改并关闭**扫描范围**窗口。
5. 通过以下方式之一保存更改：
   - 单击**应用**，保存更改后，仍留在**属性: 快速扫描**窗口中。
   - 单击**确定**，保存更改后，将关闭**属性: 快速扫描**窗口。

管理“全盘扫描”任务设置

1. 打开客户端计算机的本地任务列表。
2. 在本地任务列表中，选择“全盘扫描”任务，并采用以下方式之一打开其属性：
   - 双击任务名称。
   - 右键单击任务以显示其快捷菜单，然后选择**属性**。
   - 单击**属性**。
3. 选择**扫描**区域。
4. 如有必要，配置以下设置：
   - 要选择预设的安全级别之一，请使用**安全级别**区域中的滑块。
   - 要手动配置安全级别，请单击**设置**，然后在打开的**设置: 扫描**窗口中，执行以下操作：
     a. 在**常规**选项卡的**文件类型**区域中，选择 Kaspersky Endpoint Security 应扫描的文件类型。
     b. 在**常规**选项卡的**优化**区域中，配置扫描性能设置。
     c. 在**常规**选项卡的**复合文件**区域中，选择希望 Kaspersky Endpoint Security 扫描的复合文件。
     d. 在**高级**选项卡的**高级设置**区域中，配置使用 iSwift 技术，并在应用程序统计信息中保存检测到的对象的相关信息。
     e. 在**高级**选项卡的**启发式分析器**区域中，配置使用启发式分析器，并选择启发式分析器要应用的保护级别。
     f. 单击**确定**以保存更改并关闭**设置: 扫描**窗口。
   - 在**操作**区域中，选择 Kaspersky Endpoint Security 在检测到受感染对象时要执行的操作。
   - 要指定扫描范围，请在**扫描范围**区域中，单击**设置**，然后在打开的**扫描范围**窗口中执行以下操作：
     - 如果希望 Kaspersky Endpoint Security 扫描默认列表中的对象，请选中相关对象旁边的复选框。
     - 如果希望 Kaspersky Endpoint Security 扫描其他文件或文件夹，请选择**添加**，并指定文件或文件夹，或者指定文件或文件夹名称的掩码。
     - 单击**确定**以保存更改并关闭**扫描范围**窗口。
5. 通过以下方式之一保存更改：
   - 单击**应用**，保存更改后，仍留在**属性: 全盘扫描**窗口中。
   - 单击**确定**，保存更改后，将关闭**属性: 全盘扫描**窗口。

管理“自定义扫描”任务设置

1. 打开客户端计算机的本地任务列表。
2. 在本地任务列表中，选择“自定义扫描”任务，并采用以下方式之一打开其属性：
   - 双击任务名称。
   - 右键单击任务以显示其快捷菜单，然后选择**属性**。
   - 单击**属性**。
3. 选择**扫描**区域。
4. 如有必要，配置以下设置：
   - 要选择预设的安全级别之一，请使用**安全级别**区域中的滑块。
   - 要手动配置安全级别，请单击**设置**，然后在打开的**设置: 扫描**窗口中，执行以下操作：
     a. 在**常规**选项卡的**文件类型**区域中，选择 Kaspersky Endpoint Security 应扫描的文件类型。
     b. 在**常规**选项卡的**优化**区域中，配置扫描性能设置。
     c. 在**常规**选项卡的**复合文件**区域中，选择希望 Kaspersky Endpoint Security 扫描的复合文件。
     d. 在**高级**选项卡的**高级设置**区域中，配置使用 iSwift 技术，并在应用程序统计信息中保存检测到的对象的相关信息。
     e. 在**高级**选项卡的**启发式分析器**区域中，配置使用启发式分析器，并选择启发式分析器要应用的保护级别。
     f. 单击**确定**以保存更改并关闭**设置: 扫描**窗口。
   - 在**操作**区域中，选择 Kaspersky Endpoint Security 在检测到受感染对象时要执行的操作。
   - 要指定扫描范围，请在**扫描范围**区域中，单击**设置**，然后在打开的**扫描范围**窗口中执行以下操作：
     - 单击**添加**，并指定文件或文件夹，或者指定文件或文件夹名称的掩码。
     - 单击**确定**以保存更改并关闭**扫描范围**窗口。
5. 通过以下方式之一保存更改：
   - 单击**应用**，保存更改后，仍留在**属性: 自定义扫描**窗口中。
   - 单击**确定**，保存更改后，将关闭**属性: 自定义扫描**窗口。

管理“网络威胁防护”任务设置

1. 打开客户端计算机的本地任务列表。
2. 在本地任务列表中，选择“网络威胁防护”任务，并采用以下方式之一打开其属性：
   - 双击任务名称。
   - 右键单击任务以显示其快捷菜单，然后选择**属性**。
   - 单击**属性**。
3. 选择**网络威胁防护**区域。
4. 如有必要，配置以下设置：
   - 在客户端计算机上启用或禁用网络威胁防护。
   - 在**网络威胁防护设置**区域中，选中或取消选中**阻止攻击计算机的时间 <值> 分钟**复选框，并指定时间值。
   - 您还可以指定将不会阻止其网络活动的计算机的 IP 地址。为此，请执行以下步骤：
     a. 单击**排除项**。
     将打开**排除项**窗口。
     b. 单击**添加**。
     将打开 **IP 地址**窗口。
     c. 指定将不会阻止其网络活动的计算机的 IP 地址，然后单击**确定**。
     d. 单击**确定**以保存更改并关闭**排除项**窗口。
5. 通过以下方式之一保存更改：
   - 单击**应用**，保存更改后，仍留在**属性: 网络威胁防护**窗口中。
   - 单击**确定**，保存更改后，将关闭**属性: 网络威胁防护**窗口。

创建和管理策略

本节包含有关如何为 Kaspersky Endpoint Security 创建和配置策略的信息。

策略可决定应用程序设置，并管理针对管理组内的设备配置该应用程序的能力。必须为每一个应用程序创建单独的策略。可以为每个管理组内的设备上安装的应用程序创建各种策略且数量不限，但对于管理组内的每一个应用程序，一次只能应用一个策略。

注意： 在创建和配置策略时，您可以使用 和 按钮允许或禁止对策略内的任何设置组进行更改。

您可以对自定义策略执行以下操作：

- 创建策略。
- 配置策略。
- 将策略从一个组复制或移动到另一个组。
- 删除策略。
- 更改策略状态。
- 将策略导出到文件。
- 从文件导入策略。

有关 Kaspersky Security Center 策略的详细信息，请参阅 Kaspersky Security Center 帮助。

创建策略

本节包含有关如何启动新策略向导以创建策略的说明。

从管理组的文件夹创建策略

1. 启动 Kaspersky Security Center 管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 在控制台树中，单击**受管理设备**。
4. 选择包含所需客户端计算机的管理组。
5. 在工作区中，选择**策略**选项卡并单击**新策略**。
   将打开新策略向导。
6. 按照新策略向导的步骤操作以创建策略。

从“策略”文件夹创建策略

1. 启动 Kaspersky Security Center 管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 在控制台树中，单击**策略**。
4. 在工作区中，单击**新策略**。
   将打开新策略向导。
5. 按照新策略向导的步骤操作以创建策略。

要继续执行向导的下一步骤，请单击**下一步**。要返回到向导的上一步骤，请单击 ←。要在任意步骤退出向导，请单击**取消**。

注意：按钮外观可能因 Windows 版本而异。

步骤 1.选择应用程序

在“**选择您要为其创建组策略的应用程序**”窗口的应用程序列表中，选择 **Kaspersky Endpoint Security for Mac (12.2.1)**。

步骤 2.指定策略名称

1. 在**输入组策略名称**窗口的**名称**字段中，为正在创建的策略指定名称。名称不得包含以下符号：“ * < : > ? \ |。
2. 如果希望将现有 Kaspersky Endpoint Security 策略中的设置导入新策略，请选中**使用早期版本的应用程序的策略设置**复选框。

步骤 3.指定保护设置

如有必要，在**保护**窗口中配置以下设置：

- 配置客户端计算机上操作系统的保护设置。
- 配置受信任区域。
  您可以创建 Kaspersky Endpoint Security 不会对其进行扫描或监控的对象列表。
- 配置受信任应用程序。
  您可以创建 Kaspersky Endpoint Security 将不会监控其网络和文件活动的应用程序列表。
- 选择要检测的对象类型。
- 禁用或启用当计算机使用电池电源运行时启动计划扫描任务。
- 限制扫描任务对 CPU 的使用。

步骤 4.配置文件威胁防护设置

如有必要，在**文件威胁防护**窗口中执行以下操作：

- 开启/关闭文件威胁防护。
  默认开启文件威胁防护。
- 选择安全级别。
  默认选择 Kaspersky 推荐的安全级别。
- 配置文件威胁防护设置。
- 选择当检测到恶意对象时要执行的操作。

步骤 5.配置 Web 威胁防护设置

如有必要，在 **Web 威胁防护**窗口中执行以下操作：

- 开启/关闭 Web 威胁防护。
  默认开启 Web 威胁防护。
- 选择安全级别。
  默认选择 Kaspersky 推荐的安全级别。
- 配置 Web 威胁防护设置。
- 选择当在网络流量中检测到恶意对象时要执行的操作。

步骤 6.配置网络威胁防护设置

如有必要，在**网络威胁防护**窗口中执行以下操作：

- 开启/关闭网络威胁防护。
  默认启用网络威胁防护。
- 配置网络威胁防护设置。
- 创建或编辑 Kaspersky Endpoint Security 永远不会阻止其网络活动的远程计算机的 IP 地址列表。

步骤 7.配置更新设置

如有必要，在**更新**窗口中执行以下操作：

- 开启/关闭应用程序模块更新。
- 指定更新源。

步骤 8.配置 KSN 设置

如有必要，在**卡巴斯基安全网络**窗口中执行以下操作：

- 单击 **KSN 声明**，阅读卡巴斯基安全网络声明全文。
- 查看 Kaspersky Security Center 提供的 KSN 基础设施的相关信息。
- 开启/关闭使用卡巴斯基安全网络。
- 启用或禁用扩展 KSN 模式。
- 启用或禁用使用 KSN 代理。
- 启用或禁用当 KSN 代理不可用时使用卡巴斯基服务器。

注意：仅当使用 Kaspersky Security Center 管理服务器作为代理服务器时，才可在远程计算机上使用卡巴斯基安全网络和 KSN 代理。有关管理服务器属性的详细信息，请参阅 Kaspersky Security Center 帮助。

如果 Kaspersky Security Center 使用全球 KSN 基础设施，并且您在策略设置中选择加入卡巴斯基安全网络，则会将应用该策略的客户端计算机中的 Kaspersky Endpoint Security 统计信息自动发送到卡巴斯基，以增强对这些计算机的保护。

注意：卡巴斯基不会在没有您明确同意的情况下收集、处理或存储任何个人数据。

在全球 KSN 基础设施中使用卡巴斯基安全网络时向卡巴斯基提供的数据

如果选中**我同意使用卡巴斯基安全网络**复选框，但未选中**启用扩展 KSN 模式**复选框，则 Kaspersky Endpoint Security 将向卡巴斯基提供以下数据：

- 有关使用的授权许可的信息： 授权许可的类型和有效期、授权许可到期前的天数、向其购买授权许可的合作伙伴的标识符、区域激活中心标识符、激活码的校验码、使用 SHA1 算法计算出的票证正文哈希值、授权许可票证的创建日期和时间、授权许可信息标识符、授权许可票证标识符、授权许可票证序列标识符、用户计算机的唯一标识符、授权许可票证的有效期开始日期、授权许可票证的有效期截止日期、授权许可票证当前状态、票证标头版本、授权许可版本、票证标头签名证书标识符、密钥文件的校验码、票证标头签名者序列号、身份验证令牌。

- 已安装软件的完整版本；
  已安装软件的类型；
  软件更新 ID； 信誉服务 ID； 协议类型 ID； 区域激活中心 ID； 已撤销的软件服务决定列表的版本； 软件反病毒数据库中触发记录的 ID； 软件反病毒数据库中触发记录的时间戳； 触发的软件反病毒数据库记录的类型；计算机上的应用程序安装实例的独一 ID； 授权许可激活日期； 授权许可到期日期； 授权许可 ID； 软件使用的授权许可的状态； 正在处理的对象的校验和类型； 检测到的可用于破坏用户设备或数据的恶意软件或合法软件的名称； 正在处理的对象的校验和； 软件激活码校验和； 软件的完整版本； 独一设备 ID； 软件 ID； 软件密钥文件的校验和； 用于提供软件授权许可的信息模型的 ID； 用于签署软件授权许可 ticket 标头的证书的标识符； 软件授权许可 ticket 创建日期和时间； 软件授权许可 ticket 校验和； 软件授权许可 ticket 版本； 软件激活码版本； 向权利持有人基础结构的请求的数据格式； 当前授权许可 ticket ID； 软件组件 ID； 软件操作的结果； 错误代码； Web 服务的访问地址 (URL、IP)； 端口号； Web 服务请求源的 Web 地址 (Referrer)； 证书的公钥； 所扫描对象和哈希算法的数字证书指纹。

如果选中**我同意使用卡巴斯基安全网络**和**启用扩展 KSN 模式**复选框，则 Kaspersky Endpoint Security 将向卡巴斯基提供以下数据：

- 相关信息，包括已安装在计算机上的操作系统 (OS) 和服务包的版本、操作系统内核文件的版本与校验码（MD5、SHA2-256、SHA1）、操作系统运行模式的参数； 操作系统版本、操作系统内部版本号、操作系统更新编号、操作系统版本、有关操作系统版本的扩展信息； 操作系统 Service Pack 版本； 操作系统的启动日期和时间； 行为分析子系统中有关操作系统操作的事件的处理延迟时间； 当前类型的延迟操作系统操作事件的数量； 主动防御子系统中有关操作系统操作的事件的处理延迟时间； 已处理的操作系统操作事件的数量；已处理的同步操作系统操作事件的数量； 当前类型的所有操作系统操作事件的总延迟； 持久事件存储子系统中有关操作系统操作的事件的处理延迟时间； 所有操作系统操作事件的总延迟； 等待同步操作系统操作事件的数量； 接收到的操作系统操作事件的日期和时间。

- 有关上次操作系统重启失败的信息： 重启失败次数。

- 有关权利持有人安装的应用程序和反病毒保护状态的信息： 软件安装 ID (PCID)； 软件数据库记录版本； 计算机上安装的应用程序实例的唯一标识符、应用程序类型、应用程序类型的 ID、已安装应用程序的完整版本、应用程序设置版本的标识符、计算机类型的标识符、安装应用程序的计算机的唯一标识符、权利持有人服务中的唯一用户标识符、区域设置语言和运行状态、已安装的软件组件的版本及其运行状态、连接权利持有人服务所使用的协议版本； 已安装软件的完整版本； 已安装软件的类型； 软件更新 ID； 信誉服务 ID； 协议类型 ID； 区域激活中心 ID； 已撤销的软件服务决定列表的版本； 软件反病毒数据库中触发记录的 ID； 软件反病毒数据库中触发记录的时间戳； 触发的软件反病毒数据库记录的类型； 计算机上的应用程序安装实例的独一 ID； 授权许可激活日期； 授权许可到期日期； 授权许可 ID； 软件使用的授权许可的状态； 正在处理的对象的校验和类型； 检测到的可用于破坏用户设备或数据的恶意软件或合法软件的名称； 正在处理的对象的校验和； 软件激活码校验和； 软件的完整版本； 软件 ID； 软件密钥文件的校验和； 用于提供软件授权许可的信息模型的 ID； 用于签署软件授权许可 ticket 标头的证书的标识符； 软件授权许可 ticket 创建日期和时间； 软件授权许可 ticket 校验和； 软件授权许可 ticket 版本； 软件激活码版本； 向权利持有人基础结构的请求的数据格式； 当前授权许可 ticket ID； 软件组件 ID； 软件操作的结果； 错误代码； Web 服务的访问地址 (URL、IP)； 端口号； Web 服务请求源的 Web 地址 (Referrer)； 反病毒数据库的更新应用周期数； 反病毒数据上次更新和应用的日期和时间； 软件数据库的发布日期和时间； 软件组件的版本； 软件更新 ID； 已安装软件的类型； 系统监控的启动日期和时间； 软件的安装日期和时间； 系统监控发送统计数据的概率； 系统监控进行处理所花费的时间长于标准时间的事件的代码； 系统监控进行处理所花费的时间长于标准时间的事件的数据库处理时间； 系统监控处理一个事件的最长允许时间； 系统监控进行处理所花费的时间长于标准时间的事件的处理时间； 系统监控进行处理所花费的时间长于标准时间的事件的总数。

- 有关所有已处理对象和操作的信息： 软件对正在处理的对象的裁定； 目录代码； 所处理对象的大小； 所处理对象的校验和 (SHA256)； 系统监控上下文中所检测软件的编号； 系统监控检测软件的日期和时间； 删除特征； 软件反病毒数据库中触发记录的 ID； 系统监控检测软件的原因； 所处理对象的校验和 (MD5)； 模块完整性检查的结果； 所处理对象的名称； 触发的软件反病毒数据库记录的类型； 所处理对象的路径； 已扫描对象的名称； 扫面的日期和时间； 下载它的 URL 和 Referrer 地址； 已扫描文件的大小及其路径； 存档标志； 文件创建的日期和时间； 打包程序的名称、大小和校验和（MD5、SHA2-256）（如果文件被打包）； 文件的熵； 文件的类型； 文件类型代码； 可执行文件的标志、ID 和格式； 对象的校验和（MD5、SHA2-256）； 对象的补充校验和的类型和值； 有关对象的数字签名（证书）的数据： 证书发布者的数据、上次统计交付后对象的启动次数、应用程序的扫描任务 ID、接收对象信誉信息的方式、目标过滤器的值、适用检测技术的技术参数； 所处理对象的路径； 目录代码。

- 对于可执行文件： 文件部分的熵、信誉验证标记或文件签名标记、名称、类型、ID 类型、校验码 (MD5)，以及正在接受验证的对象加载的应用程序的大小、应用程序路径和模板路径、表明在自动运行列表中存在的属性、输入日期、属性列表、打包程序名称、应用程序数字签名的相关信息： 发行商证书、以 MIME 格式上传的文件的名称、文件构建日期和时间。

- 有关已启动的应用程序及其模块的信息： 运行文件的校验码（MD5、SHA2-256）、大小、属性、创建日期、打包程序的名称（如果文件被打包）、文件的名称、系统上运行的进程的信息（进程 ID (PID)）、进程名称、启动进程的账户信息、启动进程的应用程序和命令、进程文件的完整路径、启动命令行、进程所属应用程序的描述（应用程序的名称和开发商信息，以及使用的数字证书和用于验证其真实性的信息或缺乏文件数字签名的信息），和进程中加载的模块信息： 它们的名称、大小、类型、创建日期、属性、校验码（MD5、SHA2-256、SHA1）、路径、PE 文件头信息、打包程序名称（如果文件被打包）、这些统计数据的可用性和有效性的相关信息、生成被发送的统计数据的模式的标识符。

- 如果检测到威胁或漏洞，除了提供检测到的对象的相关信息外，还应提供该记录在反病毒数据库中的标识符、版本和类型，该威胁在卡巴斯基分类中的名称，上一次更新反病毒数据库的日期和时间，可执行文件名称，向检测到威胁的网址发出请求的应用程序文件的校验码 (MD5)，检测到的威胁的 IP 地址（IPv4 或 IPv6），漏洞标识符及其威胁等级，检测到漏洞的网页的网址和 Referrer。

- 如果检测到潜在的恶意对象，则提供有关进程内存中的数据的信息。

- 网络攻击信息： 攻击计算机的 IP 地址和用户计算机上成为网络攻击目标的端口号，攻击协议的 ID，攻击的名称和类型。

- 关于网络连接的信息： 来自使打开端口的进程启动的文件的版本和校验和 (MD5、SHA2-256、SHA1)，进程文件的路径及其数字签名，本地和远程 IP 地址，本地和远程连接端口的数量，连接的状态，端口开放的时间戳。

- 检测到有害或可疑内容的网页的网址和 IP 地址，向该网址发出请求的文件名称、大小及校验码、实现裁定结果所用规则的标识符、权重和程度、攻击的目标。

- 有关已安装应用程序和反病毒数据库更新的信息： 更新任务的完成状态、更新过程中可能发生的错误的类型、未成功更新的数量、执行更新的应用程序组件的标识符。

- 有关使用卡巴斯基安全网络 (KSN) 的信息： KSN 标识符、应用程序标识符、应用程序完整版本、用户设备的匿名 IP 地址、KSN 请求履行质量指标、KSN 数据包处理质量指标、KSN 请求数量指标和 KSN 请求类型信息、统计数据开始发送的日期和时间、统计数据完成发送的日期和时间、KSN 配置更新的相关信息： 活动配置的标识符、接收的配置标识符、配置更新的错误代码。

- 有关系统日志事件的信息： 事件时间、检测到事件的日志的名称、事件的类型和类别、事件源的名称和事件描述。

- 用于确定文件和 URL 地址信誉的信息： 请求信誉的 URL 地址和 Referrer、连接的协议类型、应用程序类型的内部标识符、正在使用的端口号、用户标识符、扫描文件的校验码 (MD5)、检测到的威胁类型、用于检测威胁的记录的信息（反病毒数据库的记录标识符、记录时间戳和类型）； 证书的公钥； 所扫描对象和哈希算法的数字证书指纹。

- 应用程序地域分布数据： 应用程序安装和激活日期、为应用程序激活提供授权许可的合作伙伴 ID、应用程序 ID、应用程序语言本地化 ID、应用程序激活的授权许可序列号、KSN 参与标志。

- 有关使用的授权许可的信息： 授权许可的类型和有效期、授权许可到期前的天数、向其购买授权许可的合作伙伴的标识符、区域激活中心标识符、激活码的校验码、使用 SHA1 算法计算出的票证正文哈希值、授权许可票证的创建日期和时间、授权许可信息标识符、授权许可票证标识符、授权许可票证序列标识符、用户计算机的唯一标识符、授权许可票证的有效期开始日期、授权许可票证的有效期截止日期、授权许可票证当前状态、票证标头版本、授权许可版本、票证标头签名证书标识符、密钥文件的校验码、票证标头签名者序列号、身份验证令牌。

- 有关计算机上已安装硬件的信息： 类型、名称、型号名称、固件版本、内置设备和连接设备的参数。

- 设备信息： 设备 ID。

- 有关 Web 控制组件的操作的信息： 组件版本、分类原因、有关分类原因的其他信息、分类的 URL、被锁定或分类的对象的主机 IP 地址。

如果 Kaspersky Security Center 使用私有 KSN 基础设施，并且您在策略设置中选择加入卡巴斯基安全网络，则应用该策略的客户端计算机中的 Kaspersky Endpoint Security 不会将统计信息发送到卡巴斯基。

在删除策略或将其设置为不活动策略后，客户端计算机上的 KSN 设置将恢复到初始状态。

步骤 9.配置用户交互设置

如有必要，在**用户交互**窗口中，配置 Kaspersky Endpoint Security 与客户端计算机用户之间的交互设置。

步骤 10.配置网络连接设置

如有必要，在**网络**窗口中执行以下操作：

- 配置与代理服务器的连接。

- 启用或禁用扫描入站和出站 HTTPS 流量。

- 选择用于检查 Mozilla Firefox 浏览器中加密 HTTPS 流量的证书存储。

- 管理受信任的根证书列表。

- 配置受监控的端口。

  您可以创建受 Kaspersky Endpoint Security 监控的端口列表。

步骤 11.配置报告和备份设置

如有必要，在**报告和备份**窗口中执行以下操作：

- 配置报告的生成和存储设置。
- 配置对象在备份中的存储设置。

步骤 12.配置文件保险箱磁盘加密

如有必要，在**文件保险箱磁盘加密**窗口中执行以下操作：

- 为用户的启动盘启用或禁用文件保险箱磁盘加密管理。

  默认禁用文件保险箱磁盘加密管理。

- 在对客户端计算机应用策略时，如果希望对用户的启动盘进行加密，请选择**加密磁盘**选项。

如果取消选中**启用文件保险箱磁盘加密管理**复选框，则具有管理员权限的用户可以在系统设置中加密和解密 Mac 启动盘。

如果选中**启用文件保险箱磁盘加密管理**复选框并选择**加密磁盘**选项，则具有管理员权限的用户无法在系统设置中解密其 Mac 启动盘。

如果选中**启用文件保险箱磁盘加密管理**复选框并选择**解密磁盘**选项，则具有管理员权限的用户无法在系统设置中加密其 Mac 启动盘。

步骤 13.配置 Web 控制

如有必要，在 **Web 控制**窗口中执行以下操作：

- 开启/关闭 Web 控制。

> **注意：**如果启用 Web 控制以阻止访问危险的网络资源，Kaspersky Endpoint Security 会在远程计算机上的保护中心中显示 **Web 控制已启用。**通知。
> 如果在新策略向导的**网络**窗口中选中**检查安全连接 (HTTPS)** 复选框，当用户在远程计算机上访问被 Web 控制阻止的网络资源时，Kaspersky Endpoint Security 将会显示通知。

- 通过单击**添加**以添加新的 Web 控制规则。

  您可以输入规则名称，选择规则是否处于活动状态，通过创建特定的网址列表或选择网站类别来指定规则区域，以及选择当用户访问此规则中包含的网站时 Kaspersky Endpoint Security 要执行的操作。

- 编辑、删除或组织列表中已创建的规则。

规则的排序顺序决定了 Kaspersky Endpoint Security 管理的应用程序的优先级。

步骤 14.配置 Managed Detection and Response

如有必要，在 **Managed Detection and Response** 窗口中执行以下操作：

- 启用或禁用 Managed Detection and Response 组件。

默认下，Managed Detection and Response 被禁用。

- 导入或删除用于在受管理设备上激活 Managed Detection and Response 组件的配置文件。

如果**启用 Managed Detection and Response** 复选框被选中且 MDR 配置文件被导入，Managed Detection and Response 组件被激活并与 Kaspersky Managed Detection and Response 服务交互。该服务持续检测和消除针对您组织的安全威胁。

步骤 15.配置 Endpoint Detection and Response Expert (on-premise)

如有必要，在 **Endpoint Detection and Response Expert (on-premise)** 窗口中执行以下操作：

- 启用或禁用 Endpoint Detection and Response Expert (on-premise) 组件。
  默认情况下，Endpoint Detection and Response Expert (on-premise) 组件处于禁用状态。
- 配置服务器连接设置并添加 TLS 证书。
- 添加服务器。

如果选中“**启用 Endpoint Detection and Response Expert (版本 7.1 或更早版本)**”复选框并添加 TLS 证书和服务器，Endpoint Detection and Response Expert (on-premise) 组件将处于活动状态并与 Kaspersky Anti Targeted Attack Platform 解决方案进行交互。该解决方案可及时检测高级威胁，例如定向攻击、高级持续威胁、零日攻击等。

步骤 16.配置外部磁盘扫描

在“**外部磁盘扫描**”窗口中，配置以下设置：

- 当连接外部磁盘时 Kaspersky Endpoint Security 执行的操作。
- Kaspersky Endpoint Security 在检测到恶意对象时执行的操作。

步骤 17.配置行为检测

“**行为检测**”窗口中，在必要时做以下操作：

- 启用或禁用“行为检测”。
  默认情况下，“行为检测”处于启用状态。
- 选择检测到恶意软件活动时要执行的操作。
- 启用或禁用共享文件夹的外部加密防护。
  - 选择检测到恶意软件活动时要执行的操作。

步骤 18.配置邮件威胁防护

如有必要，在**邮件威胁防护**窗口中执行以下操作：

- 启用或禁用邮件威胁防护。
  默认启用网络威胁防护。
- 选择当检测到恶意对象时要执行的操作。
- 配置邮件威胁防护设置。

步骤 19.配置漏洞利用防御

如有必要，在**漏洞利用防御**窗口中执行以下操作：

- 启用或禁用漏洞利用防御。
  默认启用漏洞利用防御。
- 选择检测到漏洞利用时要执行的操作。

步骤 20.配置修复引擎

如有必要，在**修复引擎**窗口中执行以下操作：

- 启用或禁用修复引擎。
  默认启用修复引擎。

步骤 21.配置设备控制

如有必要，在**设备控制**窗口中执行以下操作：

- 启用或禁用设备控制。
  默认启用设备控制。
- 配置设备控制设置。

步骤 22.配置防火墙

如有必要，在**防火墙**窗口中执行以下操作：

- 启用或禁用防火墙。
  默认启用防火墙。
- 配置防火墙设置。

步骤 23.定义要将策略应用到的管理组

在**目标组**窗口中，单击**浏览**以选择要将策略应用到的管理组。

步骤 24.选择策略状态并完成策略创建

在**为应用程序创建组策略**窗口中，执行以下操作：

1. 选择要为该策略分配的状态：
   - *活动策略*：将该策略应用到所选管理组。
   - *不活动策略*：不应用该策略。
   - *漫游策略*：当计算机与企业网络断开连接时，将该策略应用到所选管理组。

   > **注意：**您可以为管理组中的应用程序创建多个策略，但只能有一个策略处于活动状态。

   有关策略状态的详细信息，请参阅 Kaspersky Security Center 帮助。

2. 如果希望在创建策略后查看策略设置，请选中**创建策略后立即打开策略属性**复选框。

3. 单击**完成**以关闭新策略向导。

   所创建的策略将显示在相关管理组工作区中的**策略**选项卡上。在客户端计算机首次与管理服务器同步后，该策略将应用到这些计算机。

您可以编辑所创建的策略的设置。您还可以使用与各个设置组相应的 和 按钮来禁止或允许在客户端计算机上更改该设置组。设置组旁边的 按钮表示不允许客户端计算机的用户在用户计算机上编辑这些设置。设置组旁边的 按钮表示允许客户端计算机的用户在用户计算机上编辑这些设置。

查看策略列表

可以为每个管理组内的计算机上安装的应用程序创建各种策略且数量不限，但对于管理组内的每一个应用程序，一次只能应用一个策略。

查看管理组的策略列表

1. 启动 Kaspersky Security Center 管理控制台。

2. 最大化**管理服务器 <服务器名称>** 节点。

3. 在控制台树中，单击**受管理设备**。

4. 选择包含所需客户端计算机的管理组。

5. 在工作区中，选择**策略**选项卡。

   将显示策略列表。

配置策略设置

您可以对自己在 Kaspersky Security Center 中创建的策略进行更改，并阻止在子组的策略及任务设置中对其设置进行任何更改。

Kaspersky Endpoint Security 策略设置包括应用程序设置和任务设置。

配置策略设置

1. 启动 Kaspersky Security Center 管理控制台。

2. 最大化**管理服务器 <服务器名称>** 节点。

3. 在控制台树中，单击**受管理设备**。

4. 在工作区中，选择**策略**选项卡。

5. 右键单击要配置的策略并选择**属性**。

6. 在**属性: <策略名称>** 窗口中，配置策略设置：

   - 在**关键威胁防护**区域中

配置以下文件威胁防护设置

- 开启/关闭文件威胁防护。
- 选择预设的安全级别之一，或手动配置安全设置。
- 选择当检测到恶意对象时要执行的操作。

配置以下 Web 威胁防护设置

- 开启/关闭 Web 威胁防护。
- 选择预设的安全级别之一，或手动配置安全设置。
- 启用或禁用对照恶意网址数据库检查网址。
- 配置反钓鱼设置。
- 添加 Web 威胁防护将不会对其流量进行扫描的受信任地址。
- 选择当在网络流量中检测到恶意对象时要执行的操作。

配置以下邮件威胁防护设置

- 启用或禁用邮件威胁防护。
- 选择当检测到恶意对象时要执行的操作。
- 配置邮件威胁防护设置。

配置以下网络威胁防护设置

- 开启/关闭网络威胁防护。
- 配置网络威胁防护设置。
- 指定将不会阻止其网络活动的计算机的 IP 地址。

配置以下防火墙设置

- 启用或禁用防火墙。
- 配置防火墙设置。

- 在**高级威胁防护**区域中

  配置以下 KSN 设置

  - 单击 **KSN 声明**，阅读卡巴斯基安全网络声明全文。
  - 开启/关闭使用卡巴斯基安全网络。
  - 启用或禁用扩展 KSN 模式。
  - 开启/关闭云模式。

- 启用或禁用使用 KSN 代理。
- 启用或禁用当 KSN 代理不可用时使用卡巴斯基服务器。

> **注意：**仅当使用 Kaspersky Security Center 管理服务器作为代理服务器时，才可在远程计算机上使用卡巴斯基安全网络和 KSN 代理。有关管理服务器属性的详细信息，请参阅 Kaspersky Security Center 帮助。

配置以下“行为检测”设置

- 启用或禁用“行为检测”。
  默认情况下，“行为检测”处于启用状态。
- 选择检测到恶意软件活动时要执行的操作。

配置以下漏洞利用防御设置

- 启用或禁用漏洞利用防御。
- 选择检测到漏洞利用时要执行的操作。

配置以下修复引擎设置

启用或禁用修复引擎。

- 在**安全控制**区域中
  配置以下设备控制设置
  - 启用或禁用设备控制。
  - 配置设备控制设置。

  配置以下 Web 控制设置
  - 开启/关闭 Web 控制。
  - 通过单击**添加**以添加新的 Web 控制规则。
  - 编辑、删除或组织列表中已创建的规则。
- 在**数据加密**区域中
  配置以下文件保险箱磁盘加密设置
  - 为客户端计算机启用或禁用文件保险箱磁盘加密管理。
  - 加密或解密客户端计算机上的启动盘。
    如果取消选中**启用文件保险箱磁盘加密管理**复选框，则具有管理员权限的用户可以在系统设置中加密和解密 Mac 启动盘。
    如果选中**启用文件保险箱磁盘加密管理**复选框并选择**加密磁盘**选项，则具有管理员权限的用户无法在系统设置中解密其 Mac 启动盘。
    如果选中**启用文件保险箱磁盘加密管理**复选框并选择**解密磁盘**选项，则具有管理员权限的用户无法在系统设置中加密其 Mac 启动盘。
- 在 **Detection and Response** 区域

配置以下 Managed Detection and Response 设置

- 启用或禁用 Managed Detection and Response 组件。
- 导入或删除用于在受管理设备上激活 Managed Detection and Response 组件的配置文件。

配置以下 Endpoint Detection and Response 设置

- 启用或禁用 Endpoint Detection and Response 组件。
- 配置服务器连接设置并添加 TLS 证书。
- 添加 KATA 服务器。

- 在“**本地任务**”部分
  配置以下外部磁盘扫描设置
  - 当连接外部磁盘时 Kaspersky Endpoint Security 执行的操作。
  - Kaspersky Endpoint Security 在检测到恶意对象时执行的操作。
- 在**更新**区域中
  配置以下更新设置
  - 开启/关闭应用程序模块更新。
  - 指定更新源。
- 在**附加设置**区域中
  配置以下保护设置
  - 启用或禁用实时保护客户端计算机。
  - 启用或禁用客户端计算机启动时启动 Kaspersky Endpoint Security。
  - 配置受信任区域。
  - 配置受信任应用程序。
  - 选择要检测的对象类型。
  - 禁用或启用当计算机使用电池电源运行时启动计划扫描任务。

  配置以下网络设置
  - 启用或禁用使用代理服务器。
  - 指定代理服务器地址。
  - 启用或禁用为本地地址使用代理服务器。
  - 指定代理服务器身份验证的用户名和密码。
  - 启用或禁用扫描入站和出站 HTTPS 流量。

- 选择用于检查 Mozilla Firefox 浏览器中加密 HTTPS 流量的证书存储。
- 配置受监控的端口。

配置以下报告和备份设置

- 启用或禁用在报告中保存非关键事件。
- 启用或禁用仅保存最近事件。
- 启用或禁用在指定期限后删除事件。
- 指定事件存储期限。
- 启用或禁用在指定期限后从备份中删除对象。
- 指定对象在备份中的存储期限。

配置以下用户交互设置

- 启用或禁用事件通知。
- 选择 Kaspersky Endpoint Security 向用户发送事件通知的方式。
- 启用或禁用在菜单栏中显示 Kaspersky Endpoint Security 图标。
- 配置用户是否可以在客户端计算机上打开 Kaspersky Endpoint Security 主窗口并使用应用程序界面。
- 启用或禁用客户端计算机上 Kaspersky Endpoint Security 图标的上下文菜单中**退出**菜单项的可用性。
- 选择用于显示 Kaspersky Security Center 事件的语言。
- 配置可供客户端计算机用户使用的 Kaspersky Endpoint Security 设置。
- 配置密码保护以限制用户设备上不需要的操作。

7. 单击**确定**以保存更改并关闭策略属性窗口。

更改策略状态

策略状态定义策略的运行情况。策略可以处于活动、漫游或不活动状态。您可以在策略设置中更改策略状态。

更改策略状态

1. 启动 Kaspersky Security Center 管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 在控制台树中，单击**受管理设备**。
4. 选择包含所需客户端计算机的管理组。
5. 在工作区中，选择**策略**选项卡。

6. 右键单击要更改其状态的策略，并从上下文菜单中选择**属性**。
7. 在**属性: <策略名称>** 窗口中，选择**常规**区域。
8. 在**策略状态**区域中，选择以下策略状态之一：
   - **活动策略**。该策略始终应用于所选管理组。
   - **漫游策略**。当客户端计算机与企业网络断开连接时，将该策略应用到所选管理组。
   - **不活动策略**。该策略未应用于所选管理组。
9. 单击**确定**以保存更改并关闭**属性: <策略名称>** 窗口。

将策略导出到 KLP 文件

您可以将自定义策略导出到文件，以便在另一台管理服务器上使用该策略。

将策略导出到 KLP 文件

1. 启动 Kaspersky Security Center 管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 在控制台树中，单击**受管理设备**。
4. 选择包含所需客户端计算机的管理组。
5. 在工作区中，选择**策略**选项卡。
6. 右键单击策略以显示其上下文菜单，然后选择**导出**。
   将打开**另存为**窗口。
7. 选择要在其中保存该策略的 KLP 文件的文件夹。
8. 指定文件名。
9. 单击**保存**以在所选文件夹中保存该文件。

从 KLP 文件导入策略

您可以从文件中导入具有预定义设置的现有策略。

从 KLP 文件导入策略

1. 启动 Kaspersky Security Center 管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 在控制台树中，单击**受管理设备**。

4. 选择包含所需客户端计算机的管理组。

5. 在工作区中，选择**策略**选项卡。

6. 采用以下方式之一打开文件选择窗口：

   - 通过单击**从文件导入策略**按钮。
   - 通过右键单击工作区中的空白区域以打开上下文菜单，并选择**导入**菜单项。

7. 选择包含策略的 KLP 文件，然后单击**打开**。

导入的策略将添加到工作区的策略列表中。

创建和管理策略配置文件

策略配置文件 是策略的可变设置的命名集，当满足特定条件时，将会在客户端计算机激活策略配置文件。激活配置文件会修改当激活策略配置文件时设备上有效的策略设置。

创建策略配置文件

1. 在控制台树中，选择要为其创建策略配置文件的管理组。

2. 在工作区中，选择**策略**选项卡。

3. 执行以下操作之一，以打开要为其创建配置文件的策略的属性：

   - 双击策略名称。
   - 右键单击策略名称以显示上下文菜单，然后选择**属性**。
   - 单击**配置策略**链接。

4. 在**属性: <策略名称>** 窗口中，选择**策略配置文件**区域。

5. 在工作区中，单击**添加**。

6. 在**分配策略配置文件**窗口中，阅读策略的相关信息，然后单击**下一步**。
   如果不希望在创建新策略配置文件时显示此窗口，请选中**不再显示此窗口**复选框，然后再单击**下一步**。

7. 在**策略配置文件名称**窗口中，执行以下操作以配置策略配置文件：

   - 输入新策略配置文件的名称。

     > **注意：** 配置文件名称的长度不得超过 100 个字符。

   - 在**策略配置文件状态**区域中，选择是启用还是禁用策略配置文件。

- 在**策略配置文件状态**区域内的下拉列表中，选择是否可编辑策略配置文件。
- 如果希望配置策略配置文件的激活规则，请选中**关闭新策略配置文件向导后，继续配置策略配置文件激活规则**复选框。

8. 单击**完成**。
9. 如果已选中**关闭新策略配置文件向导后，继续配置策略配置文件激活规则**复选框，继续完成新策略配置文件激活规则向导的步骤。

所创建的策略配置文件将显示在**属性: <策略名称>** 窗口的**策略配置文件**区域中。

创建策略配置文件激活规则

1. 在控制台树中，选择要在其中创建策略配置文件激活规则的管理组。
2. 在工作区中，选择**策略**选项卡。
3. 执行以下操作之一以打开策略属性：
   - 双击策略名称。
   - 右键单击策略名称以显示上下文菜单，然后选择**属性**。
   - 单击**配置策略**链接。
4. 在**属性: <策略名称>** 窗口中，选择**策略配置文件**区域。
5. 在工作区中，选择要为其创建激活规则的策略配置文件，然后单击**属性**。
   将打开**属性: <策略配置文件名称>**窗口。
6. 选择**激活规则**区域。
7. 在工作区中，单击**添加**。
   将启动新策略配置文件激活规则向导。

按照新策略配置文件激活规则向导的步骤操作。

修改策略配置文件

1. 在控制台树中，选择要为其修改策略配置文件的管理组。
2. 在工作区中，选择**策略**选项卡。
3. 执行以下操作之一，以打开要为其修改配置文件的策略的属性：
   - 双击策略名称。
   - 右键单击策略名称以显示上下文菜单，然后选择**属性**。
   - 单击**配置策略**链接。
4. 在**属性: <策略名称>** 窗口中，选择**策略配置文件**区域。

5. 在工作区中，选择要修改的策略配置文件，然后单击**属性**。

   将打开**属性: <策略配置文件名称>**窗口。

6. 如有必要，对配置文件进行配置：

   - 在**常规**区域中，重命名配置文件，或通过选中/取消选中**启用配置文件**复选框来启用/禁用配置文件。
   - 在**激活规则**区域中，创建、编辑或删除激活规则。
   - 在**设备**区域中，选择要将策略配置文件应用到的设备。
   - 编辑相关区域中的策略设置。

7. 单击**确定**。

如果策略配置文件处于活动状态，将在客户端计算机与管理服务器同步后应用修改的设置。如果策略配置文件处于不活动状态，将在触发激活规则后应用修改的设置。

更改策略配置文件的优先级

1. 在控制台树中，选择要为其更改策略配置文件优先级的管理组。
2. 在工作区中，选择**策略**选项卡。
3. 执行以下操作之一，以打开要为其更改策略配置文件优先级的策略的属性：

   - 双击策略名称。
   - 右键单击策略名称以显示上下文菜单，然后选择**属性**。
   - 单击**配置策略**链接。

4. 在**属性: <策略名称>** 窗口中，选择**策略配置文件**区域。
5. 在工作区中，选择要更改其优先级的策略配置文件。
6. 通过单击  /  按钮提高/降低所选配置文件的优先级。

删除策略配置文件

1. 在控制台树中，选择要为其删除策略配置文件的管理组。
2. 在工作区中，选择**策略**选项卡。
3. 执行以下操作之一，以打开要为其删除配置文件的策略的属性：

   - 双击策略名称。
   - 右键单击策略名称以显示上下文菜单，然后选择**属性**。
   - 单击**配置策略**链接。

4. 在**属性: <策略名称>** 窗口中，选择**策略配置文件**区域。
5. 在工作区中，选择要删除的配置文件，然后单击**删除**。

有关策略配置文件的详细信息，请参阅 Kaspersky Security Center 帮助。

生成检测到的对象报告

生成检测到的对象报告

1. 启动 Kaspersky Security Center 管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 在控制台树中，单击**受管理设备**。
4. 选择包含所需客户端计算机的管理组。
5. 选择**设备**选项卡。
6. 从客户端计算机列表中选择计算机。
7. 右键单击所选计算机以打开上下文菜单，然后选择**所有任务** > **查看威胁报告**。

将在浏览器窗口中显示生成的报告。

您可以在 Kaspersky Security Center 帮助中找到有关生成应用程序在客户端计算机上检测到的对象报告的其他方式的信息。

获取加密驱动器的恢复密钥

如果客户端计算机的用户忘记或丢失其凭据，导致无法访问加密驱动器，则您可以获取恢复密钥。

获取恢复密钥

1. 启动 Kaspersky Security Center 管理控制台。
2. 最大化**管理服务器 <服务器名称>** 节点。
3. 在控制台树中，依次选择**高级**文件夹、**数据加密和保护**子文件夹和**加密驱动器**子文件夹。
4. 在工作区中，右键单击具有加密磁盘的设备以显示快捷菜单，然后选择**获取 macOS 的恢复密钥**。
   将打开一个窗口，其中包含恢复密钥。
5. 采用任何方便的方式保存恢复密钥。

您可以在客户端计算机上使用此恢复密钥来访问加密驱动器。

通过 Kaspersky Security Center Web Console 和云控制台远程管理应用程序

Kaspersky Security Center Web Console (Web Console) 是专门为集中执行与管理和维护组织的网络活动相关的主要任务而提供的 Web 应用程序。Web Console 是 Kaspersky Security Center 的一个组件，它在浏览器窗口中提供了一个用于管理 Kaspersky Endpoint Security 的界面。有关 Kaspersky Security Center Web Console 的详细信息，请参阅 Kaspersky Security Center 帮助。

Kaspersky Security Center 云控制台（云控制台）是用于保护和管理组织网络的基于云的解决方案。有关 Kaspersky Security Center 云控制台的详细信息，请参阅 Kaspersky Security Center 云控制台帮助。

您还可以通过应用程序的图形用户界面、Kaspersky Security Center 管理控制台及命令行来管理 Kaspersky Endpoint Security。

安装 Kaspersky Endpoint Security Web 插件

Kaspersky Endpoint Security Web 插件实现了 Kaspersky Endpoint Security 与 Kaspersky Security Center 之间的交互。必须在已安装 Kaspersky Security Center Web Console 的设备上安装该 Web 插件。所有可以通过浏览器访问 Kaspersky Security Center Web Console 的管理员都可以使用该 Web 插件的功能。

您可以按照如下方式安装 Web 插件：

- 使用 Kaspersky Security Center Web Console 的快速启动向导。

  首次将 Web Console 连接到管理服务器时，Web Console 会自动提示您运行快速启动向导。您也可以在 Web Console 界面中运行快速启动向导（“**发现和部署**”→“**部署和分配**”→“**快速启动向导**”）。快速启动向导还可以检查已安装的 Web 插件是否是最新的并下载必要的更新。有关 Kaspersky Security Center Web Console 快速启动向导的更多详细信息，请参阅 Kaspersky Security Center 帮助。

- 手动，使用来自外部源的 Web Console 分发包。

  要安装 Web 插件，请在 Web Console 界面中添加 Kaspersky Endpoint Security Web 插件分发包的 ZIP 存档：**设置** → **Web 插件**。该 Web 插件的分发包可以在卡巴斯基网站上下载。

要手动安装 Kaspersky Endpoint Security Web 插件：

1. 在 Kaspersky Security Center Web Console 主窗口中，选择“**设置** → **Web 插件**”。

   将打开已安装的 Web 插件列表。

2. 通过以下方式之一开始安装 Kaspersky Endpoint Security Web 插件：

   - 从卡巴斯基 Web 插件列表中安装：

     a. 单击**添加**。

        将打开所有可用的卡巴斯基 Web 插件列表。当 Web 插件有新版本发布后，该列表会自动更新。

     b. 在列表中找到 Kaspersky Endpoint Security for Mac 12.2.1 Web 插件并单击其名称。

     c. 在带有 Web 插件描述的窗口中，单击“**安装插件**”按钮。

     d. 等待安装完成，然后在信息窗口中单击“**确定**”。

- 从外部源安装 Web 插件（安装 Web 插件所需的存档包含在分发包中）：

  a. 单击“**从文件添加**”按钮。

  b. 在打开的窗口中，指定包含 Web 插件分发包的 ZIP 存档的路径以及 TXT 格式的签名文件的路径。该文件位于 Web 插件的存档中。

  c. 单击“**添加**”。

  d. 等待安装完成，然后在信息窗口中单击**“确定”**。

新的插件显示在已安装的 Web 插件列表中（**设置** → **Web 插件**）。

注意：如果您在 Kaspersky Security Center 管理服务器的属性中选择了 Kaspersky Endpoint Security 分发包中未包含的语言，则授权许可协议和整个 Kaspersky Security Center Web Console 界面将以英文显示。

创建策略

本节包含有关如何使用 Kaspersky Security Center Web Console 和云控制台为 Kaspersky Endpoint Security 创建和配置策略的信息。

策略可决定应用程序设置，并管理针对管理组内的设备配置该应用程序的能力。必须为每一个应用程序创建单独的策略。可以为每个管理组内的设备上安装的应用程序创建各种策略且数量不限，但对于管理组内的每一个应用程序，一次只能应用一个策略。

注意：在创建和配置策略时，您可以使用**强制**切换开关允许或禁止对策略内的任何设置组进行更改。

创建策略

1. 在左侧的**设备**区域中，选择**策略和配置文件**区域。
2. 单击“**添加**”。
3. 选择要为其创建策略的应用程序，然后单击**下一步**。
   将打开**新策略**窗口。
4. 在**常规**选项卡上，指定策略名称并配置策略状态和策略设置继承选项。
5. 在**应用程序设置**选项卡上，配置当强制执行策略时将对客户端计算机上的 Kaspersky Endpoint Security 应用的应用程序设置。
6. 单击**保存**。

您可以对自定义策略执行以下操作：

- 创建策略。
- 配置策略。
- 将策略从一个组复制或移动到另一个组。

- 删除策略。
- 更改策略状态。

有关 Kaspersky Security Center Web Console 策略的详细信息，请参阅 Kaspersky Security Center 帮助。

有关 Kaspersky Security Center 云控制台策略的详细信息，请参阅 Kaspersky Security Center 云控制台帮助。

注意： 在使用 Kaspersky Security Center Web Console 和云控制台为 Kaspersky Endpoint Security 策略创建策略配置文件后，您需要检查客户端计算机上是否已正确应用这些设置。

主机威胁防护

配置文件威胁防护组件

您可以通过以下方式之一配置文件威胁防护组件：

- **使用统一保护和管理插件**
  1. 在 Web Console 的主窗口，选择“**资产管理** → **策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**主机威胁防护**”>“**文件威胁防护**”。
  5. 使用“**文件威胁防护**”拨动开关启用或禁用组件。
  6. 配置文件威胁防护组件。
  7. 保存您的更改。
- **使用 Kaspersky Endpoint Security 插件**
  1. 在 Web Console 的主窗口，选择“**资产管理** → **策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**关键威胁防护**”>“**文件威胁防护**”。
  5. 使用“**文件威胁防护**”拨动开关启用或禁用组件。

6. 配置文件威胁防护组件。

7. 保存您的更改。

文件威胁防护设置

设置	描述
扫描排除项	"*扫描排除项*"是一组条件，必须满足这些条件，Kaspersky Endpoint Security 才不会扫描特定对象是否存在病毒和其他威胁。扫描排除项可确保用户安全地使用入侵者用以损害计算机或用户数据的合法软件。尽管此类应用程序并不具备任何恶意功能，但它们可被入侵者利用。有关入侵者可以用来危害计算机或用户数据的合法应用程序的详细信息，请访问 Kaspersky IT 百科全书网站。
检测到威胁后的操作	**清除；如果清除失败则删除** 如果选择该选项，应用程序将自动尝试对已检测到的受感染文件执行清除操作。如果清除失败，应用程序将删除文件。 **提示操作**。Kaspersky Endpoint Security 显示一个通知窗口，其中包含有关已感染该文件的恶意对象的信息，并提示您选择 Kaspersky Endpoint Security 要执行的操作。可用的操作可能因对象的状态而异。
保护范围	包含"文件威胁防护"组件扫描的对象。扫描对象可能是硬盘驱动器、可移动驱动器、网络驱动器、文件夹、文件或由掩码定义的多个文件。 默认情况下，"文件威胁防护"组件将扫描任何硬盘驱动器、网络驱动器或可移动驱动器中启动的文件。无法更改或删除这些对象的保护范围。您仅可以从扫描中排除对象（例如可移动驱动器）。
扫描优化	在"**扫描优化**"下，您可以配置 Kaspersky Endpoint Security，以便在扫描文件时获得更高的性能。 • **仅扫描新建和已修改的文件**。仅扫描新文件以及自从上次扫描以来被修改的文件。这有助于缩短扫描的持续时间。此模式适用于简单文件和复合文件。 • **跳过扫描只读系统卷**。如果选中此复选框，应用程序将不会扫描只读系统卷。这大大缩短了扫描时间。
扫描复合文件	隐藏病毒和其他恶意软件的一种常用方法就是将其植入复合文件中，例如存档或数据库中。为了检测以这种方式隐藏的病毒和其它恶意软件，必须将复合文件解压缩，但是这可能会降低扫描速度。您可以限制要扫描的复合文件类型，从而加快扫描速度。 • **扫描压缩包**。扫描 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR、ICE 和其他压缩包。应用程序不仅按扩展名扫描压缩包，还按格式扫描压缩包。当检查存档时，应用程序执行递归解包。这允许检测多级存档（存档中的存档）中的威胁。 • **扫描分发包和自解压存档文件**。扫描第三方应用程序的安装包和自解压存档。自解压存档包含一个可执行的解压模块。要扫描自解压存档，必须选中"**扫描压缩包**"复选框。 • **扫描 Microsoft Office 格式的文件和嵌入的 OLE 对象**。Microsoft Office 文件（例如 DOC、DOCX、XLS、PPT）和嵌入文件中的 OLE 对象（例如 Excel 表格、宏、电子邮件附件）。
允许在后台解压大于此值的存档文件 (MB)	如果选中该复选框，应用程序会提供对大于指定值的复合文件的访问权限，然后再扫描这些文件。在这种情况下，Kaspersky Endpoint Security 在后台解压并扫描复合文件。 对于小于该值的复合文件，只有在解压和扫描这些文件后，应用程序才会提供对这些文件的访问权限。 如果未选中该复选框，则只有在解压和扫描任何大小的复合文件后，应用程序才会提供对这些文件的访问权限。
不扫描大小大于该值(MB)的压缩包	如果选中该复选框，应用程序不会扫描其大小超过指定值的复合文件。 如果清除该复选框，应用程序将扫描所有大小的复合文件。 应用程序扫描从存档中提取的大文件，无论是否选择该复选框。

配置可移动驱动器扫描

您可以通过以下方式之一配置可移动驱动器扫描组件：

- **使用统一保护和管理插件**

1. 在 Web Console 的主窗口，选择"**资产管理 → 策略**"。

2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口打开。

3. 选择**应用程序设置**选项卡。

4. 转到"**主机威胁防护 → 可移动驱动器扫描**"。

5. 使用"**可移动驱动器扫描**"拨动开关启用或禁用组件。

6. 配置可移动驱动器扫描组件。
7. 保存您的更改。

- **使用 Kaspersky Endpoint Security 插件**
  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**本地任务 → 外部磁盘扫描**”。
  5. 配置可移动驱动器扫描组件。
  6. 保存您的更改。

配置行为检测

您可以通过以下方式之一配置行为检测组件：

- **使用统一保护和管理插件**
  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**主机威胁防护 → 行为分析 → 行为检测**”部分。
  5. 使用“**行为检测**”拨动开关启用或禁用组件。
  6. 配置行为检测组件。
  7. 保存您的更改。
- **使用 Kaspersky Endpoint Security 插件**
  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**高级威胁防护**”→“**行为检测**”。
  5. 使用“**行为检测**”拨动开关启用或禁用组件。

6. 配置行为检测组件。

7. 保存您的更改。

行为检测设置

设置	描述
受信任应用程序	*受信任应用程序列表*是一个应用程序列表，其中所包含应用程序的文件和网络活动（包含恶意活动）以及对系统注册表的访问不受 Kaspersky Endpoint Security 的监控。默认情况下，Kaspersky Endpoint Security 将监控任何应用程序进程打开、执行或保存的对象，并控制所有应用程序的活动及其产生的网络流量。将应用程序添加到受信任应用程序列表后，Kaspersky Endpoint Security 将停止监控该应用程序的活动。
扫描排除项	"*扫描排除项*"是一组条件，必须满足这些条件，Kaspersky Endpoint Security 才不会扫描特定对象是否存在病毒和其他威胁。扫描排除项可确保用户安全地使用入侵者用以损害计算机或用户数据的合法软件。尽管此类应用程序并不具备任何恶意功能，但它们可被入侵者利用。有关入侵者可以用来危害计算机或用户数据的合法应用程序的详细信息，请访问 Kaspersky IT 百科全书网站。
检测到威胁后的操作	**请求操作**。如果检测到恶意的活动，Kaspersky Endpoint Security 会提示用户选择检测到恶意活动时要执行的操作。可用的操作可能因对象的状态而异。 **阻止**。如果检测到恶意活动，Kaspersky Endpoint Security 会阻止执行恶意活动的应用程序，并记录有关检测到的恶意活动的信息。 **删除**。如果选择此选项，当检测到恶意活动时，Kaspersky Endpoint Security 会删除恶意应用程序的可执行文件并在备份中创建该文件的备份副本。

配置反加密勒索

您可以通过以下方式之一配置反加密勒索组件：

- **使用统一保护和管理插件**

  1. 在 Web Console 的主窗口，选择"**资产管理 → 策略**"。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到"**主机威胁防护 → 行为分析 → 反加密**"部分。
  5. 使用"**反加密勒索**"拨动开关启用或禁用组件。
  6. 配置反加密勒索组件。
  7. 保存您的更改。

- **使用 Kaspersky Endpoint Security 插件**

  1. 在 Web Console 的主窗口，选择"**资产管理 → 策略**"。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到"**高级威胁防护**"→"**行为检测**"。
  5. 使用"**保护共享文件夹免受外部加密**"拨动开关启用或禁用组件。

6. 配置反加密勒索组件。
7. 保存您的更改。

反加密设置

参数	描述
检测到威胁后的操作	**通知**如果选择此选项，在检测到修改共享文件夹中的文件的尝试时，Kaspersky Endpoint Security 会将有关此尝试的信息添加到活动威胁列表中，并将条目添加到报告中。 **阻止连接(分钟)**。当检测到试图修改共享文件夹中的文件时，Kaspersky Endpoint Security 会阻止来自执行恶意活动的设备的网络流量。应用程序将创建一个*检测到加密*事件，其中包含有关受感染设备的信息。

配置漏洞利用防御组件

您可以通过以下方式之一配置漏洞利用防御组件：

- **使用统一保护和管理插件**
  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**主机威胁防护 → 行为分析 → 漏洞利用防御**”部分。
  5. 使用“**漏洞利用防御**”拨动开关启用或禁用组件。
  6. 配置漏洞利用防御组件。
  7. 保存您的更改。
- **使用 Kaspersky Endpoint Security 插件**
  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**高级威胁防护**”→“**漏洞利用防御**”
  5. 使用“**漏洞利用防御**”拨动开关启用或禁用组件。
  6. 配置漏洞利用防御组件。
  7. 保存您的更改。

设置	描述
检测到威胁后的操作	**通知**。如果选择此项目，Kaspersky Endpoint Security 将在检测到漏洞时记录包含漏洞相关信息的条目，并将此漏洞的相关信息添加至活动威胁列表。 **阻止**。如果选择此项，在检测到漏洞利用时，Kaspersky Endpoint Security 会阻止此漏洞利用的操作，并生成一条包含此漏洞利用相关信息的日志条目。

配置修复引擎组件

您可以通过以下方式之一配置修复引擎组件：

- **使用统一保护和管理插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**主机威胁防护 → 行为分析 → 修复引擎**”部分。
  5. 使用“**修复引擎**”拨动开关启用或禁用组件。
  6. 配置修复引擎组件。
  7. 保存您的更改。

- **使用 Kaspersky Endpoint Security 插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**高级威胁防护**”→“**修复引擎**”。
  5. 使用“**修复引擎**”拨动开关启用或禁用组件。
  6. 配置修复引擎组件。
  7. 保存您的更改。

通信和 Web 保护

配置邮件威胁防护

您可以通过以下方式之一配置邮件威胁防护组件：

- **使用统一保护和管理插件**

  1. 在 Web Console 的主窗口，选择“**资产管理** → **策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**通信和 Web 保护** → **邮件威胁防护**”。
  5. 使用“**邮件威胁防护**”拨动开关启用或禁用组件。
  6. 配置邮件威胁防护组件。
  7. 保存您的更改。

- **使用 Kaspersky Endpoint Security 插件**

  1. 在 Web Console 的主窗口，选择“**资产管理** → **策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**关键威胁防护**”>“**Web 威胁防护**”。
  5. 使用“**邮件威胁防护**”拨动开关启用或禁用组件。
  6. 配置邮件威胁防护组件。
  7. 保存您的更改。

邮件威胁防护设置

设置	描述
检测到威胁后的操作	**清除；如果清除失败则删除** 在入站或出站邮件中检测到受感染对象时，应用程序会尝试对检测到的对象进行清除。用户将能够访问带安全附件的邮件。如果无法清除对象，应用程序将删除受感染的对象。应用程序会将有关已执行操作的信息添加到邮件主题，例如，*[邮件已被处理]<邮件主题>*。 **阻止**。如果在入站邮件中检测到受感染的对象，应用程序会将警告添加到邮件主题。用户将能够访问带原始附件的邮件。如果在出站邮件中检测到受感染的对象，应用程序会阻止邮件的传输，邮件客户端会显示错误。
不扫描大小大于该值(MB)的压缩包	如果选择此选框，“邮件威胁防护”组件将在扫描中排除大小超过指定值的电子邮件附件。如果清空该选框，则“邮件威胁防护”组件可以扫描任意尺寸的电子邮件附件。
跳过扫描时间超过以下值的文件(秒)	如果选择该选框，则分配的用于扫描电子邮件压缩文件附件的时间将被限制为指定的长度。

配置 Web 威胁防护组件

您可以通过以下方式之一配置网络威胁防护组件：

- **使用统一保护和管理插件**

  1. 在 Web Console 的主窗口，选择“**资产管理** → **策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**通信和 Web 保护** → **Web 威胁防护**”部分。
  5. 使用“**Web 威胁防护**”拨动开关启用或禁用组件。
  6. 配置 Web 威胁防护组件。
  7. 保存您的更改。

- **使用 Kaspersky Endpoint Security 插件**

  1. 在 Web Console 的主窗口，选择“**资产管理** → **策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**关键威胁防护**”>“**Web 威胁防护**”。
  5. 使用“**Web 威胁防护**”拨动开关启用或禁用组件。
  6. 配置 Web 威胁防护组件。
  7. 保存您的更改。

Web 威胁防护设置

设置	描述
受信任网址	Web 威胁防护认为可信的网址列表。该组件不会扫描来自这些地址的传入和传出流量以检测威胁。在一些情况下可以使用受信任地址列表，例如，当“Web 威胁防护”组件干扰您从一个已知网站上下载文件时。
扫描排除项	“*扫描排除项*”是一组条件，必须满足这些条件，Kaspersky Endpoint Security 才不会扫描特定对象是否存在病毒和其他威胁。扫描排除项可确保用户安全地使用入侵者用以损害计算机或用户数据的合法软件。尽管此类应用程序并不具备任何恶意功能，但它们可被入侵者利用。有关入侵者可以用来危害计算机或用户数据的合法应用程序的详细信息，请访问 Kaspersky IT 百科全书网站。
检测到威胁后的操作	**阻止**。如果选择此选项并且在 Web 流量中检测到受感染对象，“Web 威胁防护”组件将阻止访问对象并在浏览器中显示一条消息。 **提示操作**。Kaspersky Endpoint Security 显示一个通知，其中包含有关已感染 Web 流量对象的恶意软件类型的信息，并提示您选择 Kaspersky Endpoint Security 对此对象采取的操作。可用的操作可能因对象的状态而异。

配置网络威胁防护

您可以通过以下方式之一配置网络威胁防护组件：

- **使用统一保护和管理插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**通信和 Web 保护 → 网络威胁防护**”部分。
  5. 使用“**网络威胁防护**”拨动开关启用或禁用组件。
  6. 配置网络威胁防护组件。
  7. 保存您的更改。

- **使用 Kaspersky Endpoint Security 插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**关键威胁防护 → 网络威胁防护**”。
  5. 使用“**网络威胁防护**”拨动开关启用或禁用组件。
  6. 配置网络威胁防护组件。
  7. 保存您的更改。

网络威胁防护设置

设置	描述
受信任 IP 地址	受信任设备的 IP 地址列表。网络威胁防护组件不会阻止来自这些地址的网络活动。
检测到威胁后的操作	**阻止**。当检测到威胁时，网络威胁防护会阻止该攻击。 **阻止攻击和攻击设备(分钟)**。如果启用此选项，“网络威胁防护”组件将把攻击计算机添加至阻止列表。这意味着，“网络威胁防护”组件将会在攻击计算机的首次网络攻击尝试后的指定时间段内，阻止与该计算机的网络连接。此阻止动作将会自动保护计算机免受以后来自同一地址的更多攻击。攻击计算机必须保持在阻止列表中的最短时间为一分钟。最长时间为 999 分钟。

配置防火墙组件

您可以通过以下方式之一配置防火墙组件：

- **使用统一保护和管理插件**

  1. 在 Web Console 的主窗口，选择“**资产管理** → **策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**通信和 Web 保护** → **防火墙**”。
  5. 使用“**防火墙**”拨动开关启用或禁用组件。
  6. 配置防火墙组件。
  7. 保存您的更改。

- **使用 Kaspersky Endpoint Security 插件**

  1. 在 Web Console 的主窗口，选择“**资产管理** → **策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**关键威胁防护** → **防火墙**”部分。
  5. 使用“**防火墙**”拨动开关启用或禁用组件。
  6. 配置防火墙组件。
  7. 保存您的更改。

防火墙设置

设置	描述
网络数据包规则	包含网络数据包规则清单的表。网络数据包规则将对网络数据包进行限制，与应用程序无关。此类规则将限制通过特定端口的选定数据协议发送和接收的网络流量。 该表格列出了由卡巴斯基推荐的预配置网络数据包规则，它们能最好地为运行 macOS 操作系统的计算机提供网络流量保护。 防火墙将为每条网络数据包规则设置执行优先级。防火墙将按照包规则列表上的顺序从上到下处理网络数据包规则。防火墙将找到最适合网络连接的网络数据包规则，并应用该规则来允许或阻止网络活动。然后，防火墙会对特定网络连接忽略所有后续网络数据包规则。 网络数据包规则的优先级比应用程序网络规则高。

设置	描述
可用网络	该表格包含防火墙在计算机上检测到的网络连接的信息。 有以下网络连接类型可用： • 网络不受反恶意软件应用程序、防火墙或过滤器的保护（例如咖啡馆中的 Wi-Fi）。当用户操作连接到此类网络的计算机时，防火墙会阻止对该计算机的文件和打印机的访问。外部用户也无法通过共享文件夹和远程访问此计算机的桌面来访问数据。防火墙根据为每一个应用程序设置的网络规则，过滤应用程序的网络活动。 • 为对此计算机上的文件和打印机具有受限访问权限的用户提供的网络（例如企业 LAN 或家庭网络）。 • 安全的网络，其中的计算机不会受到攻击或未经授权的数据访问尝试。防火墙允许具有此状态的网络内的任何网络活动。

安全控制

配置设备控制组件

您可以通过以下方式之一配置设备控制组件：

- **使用统一保护和管理插件**

  1. 在 Web Console 的主窗口，选择“**资产管理** → **策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**安全控制** → **设备控制**”。
  5. 使用“**设备控制**”拨动开关启用或禁用组件。
  6. 配置设备控制。
  7. 保存您的更改。

- **使用 Kaspersky Endpoint Security 插件**

  1. 在 Web Console 的主窗口，选择“**资产管理** → **策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**安全控制** → **设备控制**”。
  5. 使用“**设备控制**”拨动开关启用或禁用组件。
  6. 配置设备控制。
  7. 保存您的更改。

设备控制设置

设置	描述
受信任设备	被授权访问这些设备的受信任设备和用户的列表。
设备和 Wi-Fi 网络	符合“设备控制”组件分类的所有可用设备类型的列表，包括其各自的访问状态。

配置 Web 控件组件

您可以通过以下方式之一配置 Web 控件组件：

- **使用统一保护和管理插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**安全控制 → Web 控制**”。
  5. 使用“**Web 控制**”拨动开关启用或禁用组件。
  6. 配置 Web 控制组件。
  7. 保存您的更改。

- **使用 Kaspersky Endpoint Security 插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**安全控制 → Web 控制**”。
  5. 使用“**Web 控制**”拨动开关启用或禁用组件。
  6. 配置 Web 控制组件。
  7. 保存您的更改。

Web 控制设置

设置	描述
规则列表	包含 Web 资源访问规则的列表。每条规则都有一个优先级。规则在列表中的位置越高，其优先级就越高。如果某个网站已添加到多条规则，“Web 控制”会基于优先级最高的规则来管理对该网站的访问。
默认操作	对不被任何其他规则覆盖的 Web 资源的访问规则。下列选项可用： • **允许除规则列表外的所有内容**。 • **阻止除规则列表外的所有内容**。

数据加密

您可以通过以下方式之一配置数据加密组件：

- **使用统一保护和管理插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**数据加密**”区域。
  5. 使用“**数据加密**”拨动开关启用或禁用组件。
  6. 配置数据加密组件。
  7. 保存您的更改。

- **使用 Kaspersky Endpoint Security 插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**数据加密**”区域。
  5. 使用“**文件保管库磁盘加密**”拨动开关启用或禁用组件。
  6. 配置数据加密组件。
  7. 保存您的更改。

“完整磁盘加密”设置

设置	描述
设备上的操作	**加密所有硬盘驱动器**。如果选定了该选项，应用策略后，应用程序将加密所有硬盘驱动器。 **解密所有硬盘驱动器**。如果选定了该选项，应用策略后，应用程序将解密所有先前加密的硬盘驱动器。

常规设置

检测设置

您可以通过以下方式之一配置检测设置：

- **使用统一保护和管理插件**

  1. 在 Web Console 的主窗口，选择“**资产管理** → **策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**常规设置** → **检测设置**”。
  5. 配置检测设置。
  6. 保存您的更改。

- **使用 Kaspersky Endpoint Security 插件**

  1. 在 Web Console 的主窗口，选择“**资产管理** → **策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**附加设置** → **保护**”。
  5. 配置检测设置。
  6. 保存您的更改。

检测设置

检测设置

设置	描述
检测其他类型的对象	不管应用程序设置的配置如何，Kaspersky Endpoint Security 始终会检测并阻止病毒、蠕虫、木马和恶意工具。它们可能会给计算机带来巨大的损害。 您还可以启用对以下类型对象的检测： • **可能会被入侵者利用以破坏您的计算机或个人数据的合法软件**。尽管此类应用程序并不具备任何恶意功能，但它们可被入侵者利用。有关入侵者可以用来危害计算机或用户数据的合法应用程序的详细信息，请访问 Kaspersky IT 百科全书网站。

卡巴斯基安全网络

您可以通过以下方式之一配置卡巴斯基安全网络设置：

- **使用统一保护和管理插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**常规设置 → 卡巴斯基安全网络**”。
  5. 使用“**卡巴斯基安全网络（KSN）**”切换开关以启用或禁用该组件。
  6. 配置卡巴斯基安全网络组件。
  7. 保存您的更改。

- **使用 Kaspersky Endpoint Security 插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**高级威胁防护 → 卡巴斯基安全网络**”。
  5. 使用“**卡巴斯基安全网络**”切换开关以启用或禁用该组件。
  6. 配置卡巴斯基安全网络组件。
  7. 保存您的更改。

检测设置

设置	描述
使用扩展 KSN 模式	*扩展 KSN 模式*是 Kaspersky Endpoint Security 向 Kaspersky 发送附加数据的一种模式。 Kaspersky Endpoint Security 使用 KSN 检测威胁，无论切换位置如何。
使用云模式	*云模式*是指 Kaspersky Endpoint Security 使用轻量级版本的反病毒数据库的应用程序运行模式。当使用轻量级反病毒数据库时，卡巴斯基安全网络支持应用程序运行。与通常的数据库相比，轻量级版本的反病毒数据库仅需要大约一半的计算机 RAM。如果您未参与卡巴斯基安全网络或已禁用云模式，Kaspersky Endpoint Security 会从 Kaspersky 服务器下载完整版本的反病毒数据库。 如果选中该复选框，Kaspersky Endpoint Security 将使用反病毒数据库的轻量级版本，这可以减少操作系统资源上的负载。 选中该复选框后，Kaspersky Endpoint Security 在下次更新期间下载反病毒数据库的轻量级版本。 如果清空该复选框，Kaspersky Endpoint Security 将使用反病毒数据库的完整版本。 清除该复选框后，Kaspersky Endpoint Security 在下次更新期间下载反病毒数据库的完全版本。
使用管理服务器作为 KSN 代理服务器	如果选中该复选框，Kaspersky Endpoint Security 将使用 KSN 代理服务。您可以在管理服务器属性中配置 KSN 代理服务设置。
如果 KSN 代理服务器不可用则使用卡巴斯基安全网络服务器	如果选中该复选框，当 KSN Proxy 服务不可用时，Kaspersky Endpoint Security 将使用 KSN 服务器。KSN 服务器可以位于卡巴斯基侧，也可以位于第三方一侧（使用卡巴斯基私有安全网络）。

用户交互

您可以通过以下方式之一配置应用程序界面设置以及应用程序与用户交互的设置：

- **使用统一保护和管理插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**常规设置 → 用户交互**”。
  5. 配置用户交互设置。
  6. 保存您的更改。

- **使用 Kaspersky Endpoint Security 插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。

4. 转到“**附加设置 → 用户交互**”。

5. 配置用户交互设置。

6. 保存您的更改。

用户交互设置

设置	描述
在计算机启动时启动 Kaspersky Endpoint Security (建议)	启用此功能后，Kaspersky Endpoint Security 将在操作系统加载后启动，从而在整个会话期间保护计算机。 禁用此功能后，Kaspersky Endpoint Security 不会在操作系统加载后启动，直到用户手动启动它。计算机保护已禁用，用户数据可能受到威胁。
显示应用程序图标	此复选框启用/禁用远程计算机菜单栏中应用程序图标的显示。 如果选中此复选框，应用程序图标将显示在菜单栏中。 如果清除此复选框，应用程序图标将从菜单栏中隐藏。 默认情况下已选定该选框。
在本地管理更新	如果选中此复选框，将启用远程计算机上 Kaspersky Endpoint Security 更新的本地管理。 如果清除此复选框，则只能使用 Kaspersky Security Center 中的 Kaspersky Endpoint Security 管理插件来管理远程计算机上的 Kaspersky Endpoint Security 更新。
在本地管理密钥	如果选中该复选框，将启用远程计算机上 Kaspersky Endpoint Security 密钥的本地管理。 如果清除此复选框，则只能使用 Kaspersky Security Center 中的 Kaspersky Endpoint Security 管理插件来管理远程计算机上的 Kaspersky Endpoint Security 密钥。
退出应用程序	如果选中此复选框，则“**退出**”命令在应用程序图标的上下文菜单中可用。远程计算机的用户可以退出远程计算机上的 Kaspersky Endpoint Security。 如果清除此复选框，则“**退出**”命令在应用程序图标的上下文菜单中不可用。远程计算机的用户无法退出远程计算机上的 Kaspersky Endpoint Security。

自我保护

您可以通过以下方式之一配置自我保护设置：

- **使用统一保护和管理插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。

  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。

  3. 选择**应用程序设置**选项卡。

  4. 转到“**常规设置 → 自我保护**”。

  5. 使用“**密码保护**”拨动开关启用或禁用组件。

  6. 配置自我保护。

  7. 保存您的更改。

- **使用 Kaspersky Endpoint Security 插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**附加设置 → 用户交互**”。
  5. 使用“**密码保护**”拨动开关启用或禁用组件。
  6. 配置密码保护。
  7. 保存您的更改。

自我保护设置

设置	描述
密码保护	如果启用了此拨动开关，当用户尝试执行密码保护范围内的操作时，Kaspersky Endpoint Security 将提示用户输入密码。密码保护范围包括禁止的操作（如禁用保护组件）和密码保护范围适用的用户账户。 启用密码保护后，Kaspersky Endpoint Security 会提示您设置 KLAdmin 账户的密码。

性能

您可以通过以下方式之一配置性能设置：

- **使用统一保护和管理插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**常规设置 → 性能**”。
  5. 配置性能设置。
  6. 保存您的更改。

- **使用 Kaspersky Endpoint Security 插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**附加设置 → 保护**”。

5. 配置性能设置。

6. 保存您的更改。

性能设置

设置	描述
使用电池供电时推迟或跳过计划任务	如果启用此功能，Kaspersky Endpoint Security 将切换到省电模式。 Kaspersky Endpoint Security *取消*计划任务。如果需要，您可以手动启动扫描和更新任务。
限制扫描任务的 CPU 使用率	为了优化 Kaspersky Endpoint Security 的性能，您可以通过恶意软件扫描任务限制 CPU 使用率。 如果启用此功能，则恶意软件扫描任务的所有 CPU 内核上的平均负载接近指定值。

报告和存储

您可以通过以下方式之一配置报告和存储设置：

- **使用统一保护和管理插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。

  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。

  3. 选择**应用程序设置**选项卡。

  4. 转到“**常规设置 → 报告和存储**”。

  5. 配置报告和存储设置。

  6. 保存您的更改。

- **使用 Kaspersky Endpoint Security 插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。

  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。

  3. 选择**应用程序设置**选项卡。

  4. 转到“**附加设置 → 报告和备份**”。

  5. 配置报告和存储设置。

  6. 保存您的更改。

"报告和存储"设置

设置	描述
在此时间段后删除报告(天)	如果选中该复选框，则最大报告存储期限制为定义的时间间隔。在此时间之后，Kaspersky Endpoint Security 将自动删除报告文件中的最早条目。
仅保留最近事件	如果选中此复选框，则每次启动任务时，Kaspersky Endpoint Security 都会删除自上次启动任务以来发生的非关键事件的信息，但会保留报告中的重要注释（例如，有关检测到的恶意对象的信息）。
记录非关键事件	如果选中此复选框，则 Kaspersky Endpoint Security 会在报告中记录非关键事件（例如，信息性事件）。非关键事件不会影响保护。
在此时间段后删除对象(天)	如果选中该复选框，则最大文件存储期限制为定义的时间间隔。最长存储期限到期后，Kaspersky Endpoint Security 将删除备份区中最旧的文件。

网络设置

您可以通过以下方式之一配置网络设置：

- **使用统一保护和管理插件**

  1. 在 Web Console 的主窗口，选择"**资产管理 → 策略**"。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到"**常规设置 → 网络设置**"。
  5. 配置网络设置。
  6. 保存您的更改。

- **使用 Kaspersky Endpoint Security 插件**

  1. 在 Web Console 的主窗口，选择"**资产管理 → 策略**"。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到"**附加设置 → 网络**"。
  5. 配置网络设置。
  6. 保存您的更改。

网络设置

设置	描述
受信任的根证书	受信任的根证书列表。Kaspersky Endpoint Security 允许您在用户计算机上安装受信任的根证书，例如，如果您需要部署新的证书中心。该应用程序允许您将证书添加到特殊的 Kaspersky Endpoint Security 证书存储中。在这种情况下，证书仅被认为是 Kaspersky Endpoint Security 应用程序的受信任证书。换句话说，用户可以通过浏览器中的新证书访问网站。如果另一个应用程序试图访问该网站，您可能会因为证书问题而出现连接错误。
代理服务器	用于客户端计算机用户访问 Internet 的代理服务器的设置。Kaspersky Endpoint Security 使用这些设置来配置某些保护组件，包括进行与更新数据库和程序模块有关的配置。

设置	描述
使用代理服务器身份验证	如果选中此复选框，则应用程序在连接到代理服务器时将使用用户名和密码进行身份验证。
对本地地址不使用代理服务器	如果选择该选框，则 Kaspersky Endpoint Security 从共享文件夹执行更新时不使用代理服务器。
加密连接扫描	此功能允许 Web 威胁防护、邮件威胁防护和 Web 控制组件监控和处理加密 (HTTPS) 连接。

遥测设置

您可以通过以下方式之一配置遥测设置：

- **使用统一保护和管理插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**常规设置 → 遥测设置**”。
  5. 配置遥测设置。
  6. 保存您的更改。

- **使用 Kaspersky Endpoint Security 插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**附加设置 → 受信任区域 → 遥测设置**”。
  5. 配置遥测设置。
  6. 保存您的更改。

遥测设置

设置	描述
EDR Expert (on-premise) 遥测	**导入**和**导出**。您可以将 EDR Expert (on-premise) 遥测设置导出到 JSON 文件。然后可以修改文件，例如，添加大量事件 ID。您还可以使用导出/导入功能备份已发送事件的设置，或将列表迁移到另一个策略。
常规排除项	为了优化传输的数据，您可以为某些事件类型配置排除规则。Kaspersky Endpoint Security 不会采集属于此类规则范围内的遥测数据。这样可以减少流量，并避免处理来自受信任对象和进程的事件。

事件设置

在应用程序运行时，可能会发生各种*事件*。它们可以是纯粹的信息或包含重要信息。例如，应用程序可以使用事件来通知数据库更新成功，或者指出需要修复的组件错误。

Kaspersky Endpoint Security 事件可分为以下几个严重级别：

- *关键事件* – 会对计算机安全造成严重威胁的事件（检测到恶意对象、漏洞、Kaspersky Endpoint Security 问题）。关键事件需要您立即关注。我们建议您不要禁用关键事件通知。
- *功能性故障*是 Kaspersky Endpoint Security 发生故障时发生的事件（处理错误、任务设置错误）。此类事件不会直接威胁计算机的安全，但需要您进行干预，以确保 Kaspersky Endpoint Security 正常工作并保护您的设备。
- *警告* – 无需您立即关注，但将来可能会对计算机安全造成威胁的事件。
- *信息性消息* – 报告给您以供参考的事件。

无论是否启用通知，Kaspersky Endpoint Security 都会将所有应用程序事件的信息记录在应用程序报告中。

更新设置

您可以通过以下方式之一配置更新设置：

- **使用统一保护和管理插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**常规设置 → 更新**”。
  5. 配置更新设置。
  6. 保存您的更改。

- **使用 Kaspersky Endpoint Security 插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**更新**”区域。

5. 配置更新设置。

6. 保存您的更改。

更新设置

设置	描述
更新源	*更新源*是包含 Kaspersky Endpoint Security 的数据库和程序模块更新的资源。 更新源包括 Kaspersky Security Center 服务器、卡巴斯基更新服务器以及网络或本地文件夹。 如果卡巴斯基的更新服务器不可用，Kaspersky Endpoint Security 可以使用备用域来接收数据库和应用程序模块更新。有关详细信息，请参阅技术支持知识库。 更新源的默认列表包括了 Kaspersky Security Center 和卡巴斯基更新服务器。您可以在列表中添加其他更新源。您可以指定 HTTP/FTP 服务器和共享文件夹作为更新源。 Kaspersky Endpoint Security 不支持来自 HTTPS 服务器的更新，除非它们是 Kaspersky 的服务器。 如果选择了多个源作为更新源，Kaspersky Endpoint Security 将尝试从列表顶端开始依次连接，使用从第一个可用源检索到的更新包执行更新任务。 默认情况下，Kaspersky Endpoint Security 使用 Kaspersky Security Center 服务器作为第一个更新源。这有助于在更新时节省流量。如果策略未应用到计算机，卡巴斯基服务器将被选为"更新"本地任务设置中的第一个更新源，因为应用程序可能无法访问 Kaspersky Security Center 服务器。

内置代理

配置 Managed Detection and Response

您可以通过以下方式之一配置 Managed Detection and Response 组件：

- **使用统一保护和管理插件**

  1. 在 Web Console 的主窗口，选择"**资产管理 → 策略**"。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到"**内置代理配置 → Managed Detection and Response**"部分。
  5. 使用"**Managed Detection and Response**"拨动开关启用或禁用组件。
  6. 配置 Managed Detection and Response 组件
  7. 保存您的更改。

- **使用 Kaspersky Endpoint Security 插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**Detection and Response → Managed Detection and Response**”。
  5. 使用“**Managed Detection and Response**”拨动开关启用或禁用组件。
  6. 配置 Managed Detection and Response 组件
  7. 保存您的更改。

Managed Detection and Response 组件设置

设置	描述
MDR 配置文件	BLOB 文件包含客户端 ID 和 Kaspersky Managed Detection and Response 授权许可信息。BLOB 文件位于 MDR 配置文件的 ZIP 压缩包。您可以在 Kaspersky Managed Detection and Response 控制台获取 ZIP 压缩包。对于 BLOB 文件的详情，请参考 Kaspersky Managed Detection and Response 帮助。

配置 Endpoint Detection and Response

您可以通过以下方式之一配置 Endpoint Detection and Response 组件：

- **使用统一保护和管理插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。
  4. 转到“**内置代理配置 → Endpoint Detection and Response**”部分。
  5. 使用“**Managed Detection and Response**”拨动开关启用或禁用组件。
  6. 配置 Endpoint Detection and Response 组件。
  7. 保存您的更改。

- **使用 Kaspersky Endpoint Security 插件**

  1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。
  2. 单击 Kaspersky Endpoint Security 策略的名称。
     策略属性窗口打开。
  3. 选择**应用程序设置**选项卡。

4. 选择“**Detection and Response**” > “**Endpoint Detection and Response**”。

5. 使用“**Endpoint Detection and Response**”拨动开关启用或禁用组件。

6. 配置 Endpoint Detection and Response 组件。

7. 保存您的更改。

Endpoint Detection and Response 设置

设置	描述
网络隔离	为响应检测到的威胁，自动将计算机与网络隔离。 当网络隔离打开时，应用程序会切断所有活动连接并阻止计算机上所有新的 TCP/IP 连接。应用程序仅使以下连接保持活动状态： • 网络隔离排除项中列出的连接。 • 由 Kaspersky Endpoint Security 服务启动的连接。 • 由 Kaspersky Security Center 网络代理发起的连接。
自动解锁被隔离设备的时间(小时)	网络隔离可以在指定时间后自动关闭，也可以手动关闭。
网络隔离排除项	网络隔离排除规则列表。开启网络隔离后，符合规则的网络连接不会被计算机阻止。 要配置网络隔离排除项，您可以使用*标准网络配置文件*列表。默认情况下，排除项包括包含确保具有 DNS/DHCP 服务器和 DNS/DHCP 客户端角色的设备不间断运行的规则的网络配置文件。您还可以修改标准网络配置文件的设置或手动定义排除项。 只有在网络隔离自动打开以响应检测到的威胁时，才会应用策略属性中指定的排除项。仅当在 Kaspersky Security Center 控制台或警报详细信息中的计算机属性中手动打开网络隔离时，才会应用计算机属性中指定的排除项。
执行防护	控制可执行文件和脚本的执行以及 Office 格式文件的打开。例如，您可以防止在所选计算机上执行被认为不安全的应用程序。执行防护支持一组 Office 文件扩展名和一组脚本解释器。 要使用执行防护组件，您需要添加执行防护规则。
执行或打开禁止的对象时的操作	**阻止并添加到事件日志**。在这种模式下，应用程序会阻止执行符合防护规则条件的对象或打开符合防护规则标准的文档。应用程序还将尝试执行对象或打开文档的事件发布到系统事件日志和 Kaspersky Security Center。 **添加到事件日志**。在此模式下，Kaspersky Endpoint Security 将发布关于尝试执行符合防护规则标准的可执行对象或打开这样的文档的事件到系统事件日志和 Kaspersky Security Center，但不会阻止尝试运行对象或打开文档。默认选择此模式。
执行防护规则	*执行防护规则*是应用程序在对对象执行做出反应时（例如，在阻止对象执行时）考虑的一组条件。应用程序通过使用 MD5 和 SHA256 哈希算法计算的路径或校验和来识别文件。
Cloud Sandbox	*Cloud Sandbox* 是一种可以让您检测计算机上的高级威胁的技术。Kaspersky Endpoint Security 自动将检测到的文件转发到 Cloud Sandbox 进行分析。Cloud Sandbox 在隔离的环境中运行这些文件以识别恶意活动并确定其信誉。然后，这些文件的数据被发送到卡巴斯基安全网络。因此，如果 Cloud Sandbox 检测到恶意文件，Kaspersky Endpoint Security 将在检测到此文件的所有计算机上执行适当的操作以消除此威胁。 要获取有关被分析对象的信息，需要建立 KSN 连接。

配置 Endpoint Detection and Response Expert (on-premise)

您可以通过以下方式之一配置 Endpoint Detection and Response Expert (on-premise) 组件：

- **使用统一保护和管理插件**

1. 在 Web Console 的主窗口，选择“**资产管理 → 策略**”。

2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口打开。

3. 选择**应用程序设置**选项卡。
4. 转到"**内置代理配置 → Endpoint Detection and Response Expert (on-premise)**"部分。
5. 使用"**Managed Detection and Response Expert (on-premise)**"拨动开关启用或禁用组件。
6. 配置 Managed Detection and Response Expert (on-premise) 组件
7. 保存您的更改。

- **使用 Kaspersky Endpoint Security 插件**

1. 在 Web Console 的主窗口，选择"**资产管理 → 策略**"。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口打开。
3. 选择**应用程序设置**选项卡。
4. 转到"**Detection and Response → Endpoint Detection and Response Expert (on-premise)**"。
5. 使用"**Managed Detection and Response Expert (on-premise)**"拨动开关启用或禁用组件。
6. 配置 Managed Detection and Response Expert (on-premise) 组件
7. 保存您的更改。

Endpoint Detection and Response Expert (on-premise) 组件设置

设置	描述
Endpoint Detection and Response Expert 解决方案	Kaspersky Endpoint Security 可与之集成的 Endpoint Detection and Response Expert 解决方案。 • **Endpoint Detection and Response Expert (版本 7.1 或更早版本)** • **Endpoint Detection and Response Expert (版本 8.0 或更高版本)**
连接设置	管理以下 KATA 或遥测采集服务器连接设置： • **服务器连接超时**。最大 Central Node 服务器响应超时。当超时用完时，Kaspersky Endpoint Security 会尝试连接到不同的 Central Node 服务器。 • **服务器证书**。用于与 Central Node 服务器建立可信连接的 TLS 证书。您可以在 Kaspersky Anti Targeted Attack Platform 控制台中获取 TLS 证书（请参阅 Kaspersky Anti Targeted Attack Platform 帮助中的说明）。 • **使用双向身份验证**。在 Kaspersky Endpoint Security 和 Central Node 之间建立安全连接时进行双向身份验证。要使用双向身份验证，您需要在 Central Node 服务器设置中启用双向身份验证，然后获取加密容器并设置密码以保护加密容器。加密容器是带有证书和私钥的 PFX 存档。您可以在 Kaspersky Anti Targeted Attack Platform 控制台中获得一个加密容器（请参阅 Kaspersky Anti Targeted Attack Platform 帮助中的说明）。配置 Central Node 设置后，您还需要在 Kaspersky Endpoint Security 设置中启用双向身份验证并加载受密码保护的加密容器。 加密容器必须受密码保护。无法添加密码为空的加密容器。
发送同步请求到服务器的间隔(分钟) *（仅适用于 Endpoint Detection and Response Expert 7.1 或更早版本）*	发送到服务器的同步请求的频率。在同步期间，Kaspersky Endpoint Security 发送有关修改的应用程序设置和任务的信息。
连接到 KATA 服务器/连接到遥测采集服务器	输入与 Kaspersky Anti Targeted Attack Platform 服务器或遥测采集服务器连接的 IP 地址和端口。 您可以添加 Central Node（对于 KATA）或遥测采集服务器的多个地址。Kaspersky Endpoint Security 尝试连接到第一个 IP 地址的服务器。如果连接失败，Kaspersky Endpoint Security 将尝试连接到列表中的第二个 IP 地址，依此类推。 EDR (KATA) 和 EDR Expert (on-premise) 解决方案具有不同的架构。对于遥测处理，EDR Expert (on-premise) 使用遥测采集服务器， EDR (KATA) 使用 Central Node 服务器。因此，如果您要将应用程序与 EDR Expert (on-premise) 集成，则需要添加遥测采集服务器。

设置	描述
发送遥测到 KATA/将遥测发送到遥测采集服务器	根据所选解决方案，此功能可完全阻止将遥测数据发送到 KATA 服务器或遥测采集服务器。例如，如果您将 Kaspersky Anti Targeted Attack Platform 与另一个也使用遥测的解决方案一起使用，您可以关闭 KATA (EDR) 的遥测发送。这使您可以优化这些解决方案的服务器负载。 如果您部署了 Managed Detection and Response 解决方案和 KATA (EDR)，则可以使用 MDR 遥测并在 KATA (EDR) 中创建威胁响应任务。
最大事件传输延迟 (秒)	应用程序在同步间隔到期后与服务器同步以发送事件。
启用请求限制	该功能有助于优化服务器上的负载。如果选中该复选框，应用程序将限制传输的事件。如果事件数量超过配置的限制，Kaspersky Endpoint Security 将停止发送事件。 **每小时最大事件数**。如果事件流超过配置的每小时事件数限制，应用程序会分析遥测数据流并限制事件的发送。Kaspersky Endpoint Security 在一小时后恢复发送事件。如果应用程序安装在服务器上，遥测数据流会更高。对于服务器，建议将该值增加到每小时 60,000 个事件。 **超出事件限制的百分比**。该应用程序按类型对事件进行排序（例如，"注册表中的更改"事件），如果相同类型的事件占事件总数的比率超过配置的百分比限制，则限制事件的传输。当其他事件与事件总数的比率再次变得足够大时，Kaspersky Endpoint Security 将恢复发送事件。
连接到响应服务器 *（仅适用于 Endpoint Detection and Response Expert 8.0 或后续版本）*	到响应服务器的连接设置。请输入响应服务器 IP 地址（IPv4 或 IPv6）和连接到服务器的端口。 您可以添加多个响应服务器地址。Kaspersky Endpoint Security 尝试连接到第一个 IP 地址的服务器。如果连接失败，Kaspersky Endpoint Security 将尝试连接到列表中的第二个 IP 地址，依此类推。
连接设置 *（仅适用于 Endpoint Detection and Response Expert 8.0 或后续版本）*	为响应服务器连接配置以下内容： • **服务器连接超时**。最大响应服务器响应超时。超时后，Kaspersky Endpoint Security 会尝试连接到其他响应服务器。 • **服务器证书**。用于与响应服务器建立受信任连接的 TLS 证书。 • **使用双向身份验证**。在 Kaspersky Endpoint Security 和响应服务器之间建立安全连接时进行双向身份验证。要使用双向身份验证，您需要在响应服务器设置中启用双向身份验证，然后获取加密容器并设置密码以保护加密容器。*加密容器*是带有证书和私钥的 PFX 存档。您可以在 Kaspersky Anti Targeted Attack Platform 控制台中获得一个加密容器（请参阅 Kaspersky Anti Targeted Attack Platform 帮助 中的说明）。配置响应服务器设置后，您还需要在 Kaspersky Endpoint Security 设置中启用双向身份验证并加载受密码保护的加密容器。 加密容器必须受密码保护。无法添加密码为空的加密容器。

创建任务

本节描述如何使用 Kaspersky Security Center Web Console 和云控制台创建和配置供 Kaspersky Endpoint Security 在受 Kaspersky Security Center 管理的一台客户端计算机或一组计算机上执行的任务。

任务 是供 Kaspersky Endpoint Security 在客户端计算机上执行的一组可配置的操作。

在 Kaspersky Security Center Web Console 和云控制台中，可创建以下任务：

- 扫描
- 更新
- 回滚
- 添加密钥

创建任务

1. 在左侧的**设备**区域中，选择**任务**区域。
2. 单击“**添加**”。
   将启动添加任务向导。
3. 在“**应用程序**”下拉列表中，选择 **Kaspersky Endpoint Security for Mac 12.2.1**。
4. 在**任务类型**下拉列表中，选择要创建的任务。
5. 如果需要，在**任务名称**字段中编辑任务名称。
6. 选择要将任务分配到的设备。
7. 配置所选任务类型的设置。
8. 通过单击**完成**以完成添加任务向导。

> **注意：**如果在**完成任务创建**窗口中选中**创建完成后打开任务详细信息**复选框，您可以继续修改默认任务设置。如果未选中此复选框，则将使用默认设置创建任务。您之后可随时修改默认任务设置。

您可以对任务执行以下操作：

- 启动和停止任务。
- 配置任务设置。
- 跟踪任务进度。
- 将任务从一个组复制和移动到另一个组。
- 删除任务。

有关 Kaspersky Security Center Web Console 任务的详细信息，请参阅 Kaspersky Security Center 帮助。

有关 Kaspersky Security Center 云控制台任务的详细信息，请参阅 Kaspersky Security Center 云控制台帮助。

配置“扫描”任务设置

在**应用程序设置**选项卡上，您可以为远程计算机上的 Kaspersky Endpoint Security 配置**扫描**任务设置。

打开“扫描”任务设置

1. 转到**设备** > **任务**。
2. 双击具有**扫描**任务类型的任务。
3. 选择**应用程序设置**选项卡。

如有必要，执行以下操作：

- 定义扫描范围。
- 选择 Kaspersky Endpoint Security 在检测到受感染对象时执行的操作。
- 选择 Kaspersky Endpoint Security 在运行“扫描”任务时要扫描的文件类型。
- 配置扫描性能设置。
- 选择 Kaspersky Endpoint Security 要分析的复合文件。

注意： Kaspersky Endpoint Security 不会扫描位于 OneDrive 或 iCloud 存储或者其他云存储中的文件。请将这些文件排除在扫描范围之外。否则，扫描任务可能会以“*受感染文件未删除*”错误结束。

配置“添加密钥”任务设置

在**应用程序设置**选项卡上，您可以为远程计算机上的 Kaspersky Endpoint Security 配置**添加密钥**任务设置。

打开“添加密钥”任务设置

1. 转到**设备** > **任务**。
2. 双击具有**添加密钥**任务类型的任务。
3. 选择**应用程序设置**选项卡。

如有必要，执行以下操作：

- 将当前授权许可密钥设置为备用密钥。
- 在用户计算机上选择其他密钥来激活 Kaspersky Endpoint Security。
- 向 Kaspersky Security Center 存储库中添加新的授权许可密钥。

配置“更新”任务

在**应用程序设置**选项卡上，您可以为远程计算机上的 Kaspersky Endpoint Security 配置**更新**任务设置。

打开“更新”任务设置

1. 转到**设备** > **任务**。
2. 双击具有**更新**任务类型的任务。
3. 选择**应用程序设置**选项卡。

专用的卡巴斯基更新服务器是 Kaspersky Endpoint Security 的主更新源。Kaspersky Endpoint Security 也可以使用分发点、本地文件夹或其他 Web 服务器作为*更新源*。

如果通过 Kaspersky Security Center Web Console 管理 Kaspersky Endpoint Security，则更新源列表默认包含卡巴斯基更新服务器和 Kaspersky Security Center 服务器。Kaspersky Endpoint Security 首先从 Kaspersky Security Center 服务器下载更新，其次才是从卡巴斯基更新服务器下载。

如果通过 Kaspersky Security Center 云控制台管理 Kaspersky Endpoint Security，则更新源列表默认包含卡巴斯基更新服务器和分发点。Kaspersky Endpoint Security 首先从分发点下载更新，其次才是从卡巴斯基更新服务器下载。有关分发点的详细信息，请参阅 Kaspersky Security Center 帮助。

如有必要，执行以下操作：

- 开启/关闭应用程序模块更新。
- 添加或删除将用于更新 Kaspersky Endpoint Security 的更新源。

获取加密驱动器的恢复密钥

如果客户端计算机的用户忘记或丢失其凭据，导致无法访问加密驱动器，则您可以获取恢复密钥。

获取恢复密钥

1. 在 Kaspersky Security Center Web Console 或云控制台的主窗口中，选择“**设置** → **界面选项**”。
2. 开启“显示数据加密和保护”切换开关以启用数据加密管理，然后单击“**保存**”。
3. 转到“**操作** → **数据加密和保护** → **加密驱动器**”。
   将打开加密设备列表。
4. 选中具有加密驱动器的设备旁边的复选框。
5. 单击**授予移动模式设备访问权限**。
6. 在**以离线模式授予设备访问权限**对话框中，选择 Kaspersky Endpoint Security Web 插件，然后单击**确定**。
7. 单击**获取恢复密钥**。
   将在当前对话框窗口中显示恢复密钥。
8. 采用任何方便的方式保存恢复密钥。

您可以在客户端计算机上使用此恢复密钥来访问加密驱动器。

从命令行管理应用程序

您可以从命令行管理 Kaspersky Endpoint Security 应用程序。

注意： 安装 Kaspersky Endpoint Security 模块更新后，命令行中的应用程序客户端版本可能不同于安装的应用程序版本。

命令行语法：

```
kav <命令> <参数>
```

每条命令都有各自的受支持参数范围。

查看命令行帮助

使用以下命令查看应用程序命令行语法的相关信息：

```
kav -? | help
```

运行恶意软件扫描

命令语法：

```
kav scan <扫描范围> <操作> <文件类型> <排除项> <报告参数> <高级参数>
```

注意： 要运行恶意软件扫描，您也可以通过从命令行启动任务来使用在应用程序中创建的任务。该任务将采用在 Kaspersky Endpoint Security 界面中指定的参数启动。

参数描述

<扫描范围> – 此参数指定要进行恶意代码扫描的对象列表。您可以包含多个参数（以空格分隔）。

注意： Kaspersky Endpoint Security 不会扫描位于 OneDrive 或 iCloud 存储或者其他云存储中的文件。请将这些文件排除在扫描范围之外。否则，扫描任务可能会以“*受感染文件未删除*”错误结束。

以下值可用：

- <文件> – 要扫描的文件和/或文件夹的路径列表。您可以指定文件的绝对或相对路径。列表中的项用空格分隔。

  注意：如果某个对象的名称或此对象的路径包含空格或特殊字符（例如 `$`、`&` 或 `@`），它应该用单引号 (`' '`) 引起来，或者在每个特殊字符前面添加反斜杠 (`\`) 对其进行转义。如果引用特定文件夹，将会扫描此文件夹内的所有文件和文件夹。

- `-all` – 对计算机进行全盘扫描。
- `-remdrives` – 所有可移动驱动器。
- `-fixdrives` – 所有内部驱动器。
- `-netdrives` – 所有网络驱动器。
- `-@:<filelist.lst>` – 文件路径和处于扫描范围内的对象和文件夹的列表。文件必须为文本格式，每个扫描对象必须单独列一行。仅可以输入文件的绝对路径。

<操作> – 此参数确定要对在扫描过程中检测到的恶意对象采取的操作。如果未定义此参数，默认操作是与值 `-i8` 对应的操作。

以下值可用：

- `-i0` – 不对对象采取任何操作，仅将对象信息保存在报告中。
- `-i1` – 清除受感染对象，如果无法清除，则跳过此类对象。
- `-i2` – 清除受感染对象，如果无法清除，则删除；除非容器具有可执行标头，否则不删除容器（SFX 压缩文件）。
- `-i3` – 清除受感染对象，如果无法清除，则删除此类对象；如果无法删除容器中受感染的文件，则完全删除容器。
- `-i4` – 删除受感染对象；如果无法删除容器中受感染的文件，则完全删除容器。
- `-i8` – 如果检测到受感染对象，提示用户执行操作（默认使用）。
- `-i9` – 扫描完成时提示用户执行操作。

<文件类型> – 此参数定义要进行恶意软件扫描的文件类型。默认情况下，如果未定义此参数，将仅扫描潜在感染文件（基于文件内容）。

以下值可用：

- `-fe` – 仅扫描潜在感染文件（基于文件扩展名）。
- `-fi` – 仅扫描潜在感染文件（基于文件内容）。默认使用此参数。
- `-fa` – 扫描所有文件。

<排除项> – 此参数定义排除在扫描范围外的对象。您可以包含多个参数（以空格分隔）。

以下值可用：

- `-e:a` – 不扫描压缩文件。
- `-e:b` – 不扫描电子邮件数据库。
- `-e:m` – 不扫描文本格式的电子邮件。
- `-e:` <掩码> – 不根据掩码扫描对象。
- `-e:` <秒> – 跳过扫描时间超过指定值（单位：秒）的对象。
- `-es:` <大小> – 跳过大小超过指定值（单位：MB）的对象。

<报告参数> – 这些参数定义扫描结果报告的格式。您可以指定报告文件的绝对或相对路径。如果未定义此参数，将显示回滚结果和所有事件。

以下值可用：

- `-r:` <报告文件> – 仅将重要事件记录到指定的报告文件中。
- `-ra:` <报告文件> – 将所有事件记录到指定的报告文件中。

<高级参数> – 此类参数定义恶意软件扫描技术和配置文件的使用：

- `-iSwift=<on|off>` – 启用/禁用 iSwift 技术。
- `-c:` <配置文件> – 定义配置文件的路径，此文件包含恶意软件扫描任务的应用程序设置。您可以指定文件的绝对或相对路径。如果未指定此参数，在应用程序界面中设置的值和命令行中指定的值将一起使用。

例如：
开始扫描文件夹 ~/Documents、/Applications 和名称为 my test.exe 的文件：

```
kav scan ~/Documents /Applications 'my test.exe'
```

扫描在文件 objects2scan.txt 中列出的对象。使用 scan_settings.txt 配置文件。扫描完成后，创建报告记录所有事件：

```
kav scan -@:objects2scan.txt -c:scan_settings.txt -ra:scan.log
```

配置文件示例：

```
-netdrives -@:objects2scan.txt -ra:scan.log
```

更新应用程序

命令语法：

`kav update` <更新源> <报告参数> <高级参数>

参数描述

<更新源> – 从中下载更新的 HTTP 服务器或者网络或本地文件夹。如果未选择路径，将选择应用程序更新设置中的更新源。

<报告参数> – 这些参数定义扫描结果报告的格式。您可以指定报告文件的绝对或相对路径。如果未定义此参数，将显示回滚结果和所有事件。

以下值可用：

- `-r:` <报告文件> – 仅将重要事件记录到指定的报告文件中。
- `-ra:` <报告文件> – 将所有事件记录到指定的报告文件中。

<高级参数> – 此参数定义配置文件的使用。

`-c:` <配置文件> – 定义配置文件的路径，此文件包含用于更新应用程序的应用程序设置。您可以指定文件的绝对或相对路径。如果未指定此参数，将使用在此应用程序界面中设置的值。

例如：
使用默认更新源更新应用程序数据库，并将所有事件记录在报告中：

```
kav update -ra:avbases_upd.txt
```

使用 updateapp.ini 配置文件的参数更新 Kaspersky Endpoint Security 模块：

```
kav update -app=on -c:updateapp.ini
```

回滚到上次更新

命令语法：

`kav rollback` <报告参数>

重要： 运行此命令需要具有管理员权限。

参数描述

<报告参数> – 此参数定义包含更新回滚结果的报告的格式。您可以指定报告文件的绝对或相对路径。如果未定义此参数，将显示回滚结果和所有事件。

以下值可用：

- `-r:` <报告文件> – 仅将重要事件记录到指定的报告文件中。
- `-ra:` <报告文件> – 将所有事件记录到指定的报告文件中。

例如：

```
kav rollback -ra:rollback.txt
```

启动/停止组件或任务

启动命令语法：

`kav start <任务或组件名称> <报告参数>`
停止命令语法：

`kav stop <任务或组件名称>`

> **重要：**运行 stop 命令需要具有管理员权限。

参数描述

<任务或组件名称> – 指定以下值之一：

- `fm` 或 `file_monitoring` – 文件威胁防护
- `wm` 或 `web_monitoring` – Web 威胁防护
- `mail_monitoring` – 邮件威胁防护
- `ids` – 网络威胁防护
- `firewall` –防火墙
- `behaviordetection` – 行为检测
- `exploitprevention` –漏洞利用防御
- `remediationengine` –修复引擎
- `devicecontrol` – 设备控制
- `webcontrol` – Web 控制
- `full` 或 `scan_my_computer` – 全盘扫描任务
- `scan_objects` – 自定义扫描任务
- `quick` 或 `scan_critical_areas` – 快速扫描任务
- `externalstoragesscanner` – 可移动磁盘扫描任务
- `updater` – 更新任务
- `rollback` – 回滚任务
- `diskencryption` – 文件保险箱磁盘加密
- `edroptimum` – Endpoint Detection and Response Optimum
- `edrkata` – Endpoint Detection and Response Expert (on-premise)

- `cloudsandbox` – Cloud Sandbox
- `mdr` – Managed Detection and Response

<报告参数> – 这些参数定义组件或任务结果报告的格式。您可以指定报告文件的绝对或相对路径。如果不定义此参数，Kaspersky Endpoint Security 将根据图形用户界面中配置的参数显示结果。

注意： <报告参数> 仅可用于 `scan_objects`、`updater` 和 `rollback` 值。

以下值可用：

- `-r:` <报告文件> – 仅将重要事件记录到指定的报告文件中。
- `-ra:` <报告文件> – 将所有事件记录到指定的报告文件中。

注意： 通过命令提示符启动的组件和任务将使用在图形用户界面中配置的参数运行。

例如：
要启用文件威胁防护组件，请在命令行中输入以下命令：

```
kav start fm
```

要从命令行停止全盘扫描任务，请输入以下命令：

```
kav stop scan_my_computer
```

查看组件或任务的状态和统计信息

状态命令语法：

```
kav status <任务或组件名称>
```

统计信息命令语法：

```
kav statistics <任务或组件名称>
```

参数描述

<任务或组件名称> – 指定以下值之一：

- `fm` 或 `file_monitoring` – 文件威胁防护
- `wm` 或 `web_monitoring` – Web 威胁防护
- `mail_monitoring` – 邮件威胁防护
- `ids` – 网络威胁防护
- `firewall` –防火墙

- `behaviordetection` – 行为检测
- `exploitprevention` –漏洞利用防御
- `remediationengine` –修复引擎
- `devicecontrol` – 设备控制
- `webcontrol` – Web 控制
- `full` 或 `scan_my_computer` – 全盘扫描任务
- `scan_objects` – 自定义扫描任务
- `quick` 或 `scan_critical_areas` – 快速扫描任务
- `externalstoragesscanner` – 可移动磁盘扫描任务
- `updater` – 更新任务
- `rollback` – 回滚任务
- `diskencryption` – 文件保险箱磁盘加密
- `edroptimum` – Endpoint Detection and Response Optimum
- `edrkata` – Endpoint Detection and Response Expert (on-premise)
- `cloudsandbox` – Cloud Sandbox
- `mdr` – Managed Detection and Response

注意：如果在运行 status 命令时未指定 <任务或组件名称> 参数的值，将显示应用程序所有任务和组件的状态。对于 statistics 命令，必须为 <任务或组件名称> 参数指定值。

导出保护设置

命令语法：

```
kav export <任务或组件名称> <导出文件>
```

参数描述

<任务或组件名称> – 指定以下值之一：

- `fm` 或 `file_monitoring` – 文件威胁防护
- `wm` 或 `web_monitoring` – Web 威胁防护

- `mail_monitoring` – 邮件威胁防护
- `ids` – 网络威胁防护
- `firewall` –防火墙
- `behaviordetection` – 行为检测
- `exploitprevention` –漏洞利用防御
- `remediationengine` –修复引擎
- `devicecontrol` – 设备控制
- `webcontrol` – Web 控制
- `full` 或 `scan_my_computer` – 全盘扫描任务
- `scan_objects` – 自定义扫描任务
- `quick` 或 `scan_critical_areas` – 快速扫描任务
- `externalstoragesscanner` – 可移动磁盘扫描任务
- `updater` – 更新任务
- `rollback` – 回滚任务
- `diskencryption` – 文件保险箱磁盘加密
- `edroptimum` – Endpoint Detection and Response Optimum
- `edrkata` – Endpoint Detection and Response Expert (on-premise)
- `cloudsandbox` – Cloud Sandbox
- `mdr` – Managed Detection and Response

<导出文件> – 要将应用程序设置导出到的文件的路径。您可以指定文件的绝对或相对路径。

例如:
```
kav export fm fm_settings.txt
```

激活应用程序

您可以通过应用密钥文件来激活 Kaspersky Endpoint Security。

命令语法:

```
kav license /add <密钥文件或密钥激活码>
```

参数描述

<密钥文件> – 具有 .key 扩展名的应用程序密钥文件。

<密钥激活码> – XXXX-XXXX-XXXX-XXXX 格式的激活码。

例如：

```
kav license /add ./1AA111A1.key
kav license /add A11A1-11111-1A1AA-1A11A
```

安装系统功能扩展

命令语法：

```
kav activatesystemextension /sysext
```

注意：您需要在**隐私与安全性**设置中授予 Kaspersky Endpoint Security 权限以完成功能扩展的安装。

配置网络连接

您可以为 Web 威胁防护和网络威胁防护组件配置网络连接。

命令语法：

```
kav activatesystemextension /webav
```

注意：您需要为网络内容过滤授予 Kaspersky Endpoint Security 权限以完成配置。

删除授权许可密钥

您可以删除应用程序中当前添加的所有授权许可密钥。

命令语法：

```
kav license /del
```

重要：运行此命令需要具有管理员权限。

命令行返回代码

命令行中的任何命令都可能返回常规代码。返回代码包括常规代码和某些任务特定的代码。

用于接收返回代码的命令语法：

```
echo $?
```

常规返回代码：

- `0` – 操作成功完成
- `1` – 无效的参数值
- `2` – 未知错误
- `3` – 任务完成出错
- `4` – 任务已取消

恶意软件扫描任务返回代码：

- `101` – 已处理所有恶意对象
- `102` – 检测到恶意对象

退出应用程序

命令语法：

```
kav exit
```

重要： 运行此命令需要具有管理员权限。

卸载应用程序

使用以下命令序列从命令行卸载 Kaspersky Endpoint Security：

```
sudo /Library/Application\ Support/Kaspersky\ Lab/klnagent/Binaries/UninstallScript
sudo /Library/Application\ Support/Kaspersky\ Lab/KAV/Binaries/UninstallScript
```

```
sudo rm -rf /Library/Application\ Support/Kaspersky\ Lab/ /Applications/Kaspersky
```

重要：卸载应用程序需要管理员权限。

Detection and Response 管理命令

您可以使用命令行来管理 Detection and Response 解决方案的内置功能。如果无法使用 Kaspersky Security Center 控制台进行管理，您可以管理 Detection and Response 解决方案。

管理执行防护

您可以查看客户端计算机的执行防护设置，并禁用客户端计算机上的执行防护。

命令语法：

```
kav prevention </disable | /show>
```

命令描述

`/disable` - 关闭客户端计算机上的执行防护的命令。

`/show` - 显示当前执行防护设置的命令，包括模式和执行防护规则列表。

管理网络隔离

您可以查看主机的网络隔离设置，并在主机上禁用网络隔离。

命令语法：

```
kav isolation </off | /status>
```

命令描述

`/off` - 关闭网络隔离的命令。

重要：运行此命令需要具有管理员权限。

`/status` - 显示网络隔离状态和排除项的命令。

> **注意：**这些命令必须同时运行。

联系技术支持

本部分介绍如何获得技术支持以及提供技术支持的条款。

如何获得技术支持

如果在 Kaspersky Endpoint Security 文档或与 Kaspersky Endpoint Security 相关的信息源中未找到问题的解决方案，建议您联系卡巴斯基技术支持。技术支持专家将为您解答有关安装和使用 Kaspersky Endpoint Security 的所有问题。

注意： 卡巴斯基将在 Kaspersky Endpoint Security 的整个生命周期内为您提供支持（请参阅应用程序支持生命周期页面）。与技术支持部门联系之前，请阅读支持规则。

您可以采用以下方式之一联系技术支持：

- 通过访问技术支持网站
- 通过 Kaspersky CompanyAccount 门户向技术支持发送请求

通过 Kaspersky CompanyAccount 获取技术支持

Kaspersky CompanyAccount 是为使用卡巴斯基应用程序的公司提供的门户。Kaspersky CompanyAccount 门户旨在通过在线请求促进用户与卡巴斯基专家之间的交互。您可以使用 Kaspersky CompanyAccount 跟踪您的在线请求的状态并保存请求历史记录。

您可以在一个 Kaspersky CompanyAccount 帐户下注册您所有的公司员工。单个帐户让您集中管理注册员工向卡巴斯基发送的电子请求，同时通过 Kaspersky CompanyAccount 管理这些员工的权限。

Kaspersky CompanyAccount 门户网站拥有以下语言版本：

- 英语
- 西班牙语
- 意大利语
- 德语
- 波兰语
- 葡萄牙语
- 俄语

- 法语
- 日语

若要了解有关 Kaspersky CompanyAccount 的更多信息，请访问技术支持网站。

为技术支持部门获取信息

为了更有效地为您提供支持并排查应用程序问题，在诊断过程中，技术支持专家可能会出于调试目的要求您临时更改应用程序设置。可能会要求您执行以下操作：

- 激活用于提取扩展诊断信息的功能。
- 微调某些无法通过标准用户界面元素进行调整的单个应用程序组件的设置。
- 更改用于传输所提取的诊断信息的设置。

技术支持专家将向您提供执行上述操作所需的所有信息，并告知您出于调试目的要获取的数据范围。在提取扩展诊断信息后，该信息将保存在用户的计算机上。该数据不会自动发送到卡巴斯基。

使用追踪文件

向卡巴斯基技术支持专家报告问题后，他们可能要求您生成包含有关 Kaspersky Endpoint Security 运行情况的信息的报告，并将报告发送给卡巴斯基技术支持。卡巴斯基技术支持专家还可能要求您创建*追踪文件*。通过追踪文件，可以逐步检查应用程序命令的执行情况，并确定何时发生错误。

创建追踪文件

追踪是记录有关应用程序活动的详细信息的有效方式。技术支持专家使用追踪文件来排查问题。

创建追踪文件

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**界面**选项卡的**跟踪**区域中，选中**启用跟踪**复选框。

重要：建议仅在卡巴斯基技术支持专家的要求下启用追踪。

追踪文件可能需要大量的磁盘空间。当您不再需要追踪文件时，请禁用追踪。

禁用追踪

1. 在菜单栏，单击应用程序图标并选择**设置**。
   此时会打开应用程序设置窗口。
2. 在**界面**选项卡的**跟踪**区域中，取消选中**启用跟踪**复选框。

Kaspersky Endpoint Security 将以下信息保存在追踪文件中：

- 有关设备和操作系统的信息（唯一的设备 ID、设备类型、网络设备的 MAC 地址、操作系统类型、操作系统版本）。
- 有关应用程序及其模块的操作的信息。
- 有关订阅（订阅类型、区域）的信息。
- 有关语言区域设置、应用程序 ID、应用程序自定义、应用程序版本、唯一的应用程序安装 ID、唯一计算机 ID 的信息。
- 有关计算机反恶意软件保护状态，以及所有已处理和已检测到的对象的信息（包含已检测到的对象名称、检测的日期和时间、对象的下载网址、已感染文件的名称和大小及其路径、攻击计算机的 IP 地址和网络攻击的目标计算机端口号、恶意软件活动列表和不需要的网址），以及应用程序和用户所做相关操作和决定的信息。
- 有关用户下载的应用程序的信息（网址、属性、文件大小、下载文件的进程的相关信息）。
- 有关启动的应用程序及应用程序模块的信息（大小、属性、创建日期、PE 标头详细信息、区域、名称、位置、打包应用程序）。
- 有关界面错误和已安装卡巴斯基的应用程序界面用法的信息。
- 有关网络连接的信息：远程计算机和用户计算机的 IP 地址、用于建立连接的端口号和连接的网络协议。
- 有关计算机通过 IT 与电信网络接收和发送的网络包的信息。
- 有关发送和接收的电子邮件和即时消息的信息。
- 有关访问的网址的信息：使用开放式协议建立连接的时间、有关网站登录登录名和密码的数据和 Cookie 内容。
- 服务器的公共证书。

追踪文件只包含修复应用程序中的缺陷所需的信息。卡巴斯基使用追踪文件调查与 Kaspersky Endpoint Security 应用程序运行中的错误相关联的事件。

默认情况下，禁用追踪文件的创建。您可以在应用程序设置中启用追踪文件的生成。

追踪文件只能手动发送到卡巴斯基。应用程序不会自动向卡巴斯基发送追踪文件。

您可以选择如何将追踪文件发送到卡巴斯基。

在向卡巴斯基发送追踪文件之前，请查看它们包含的数据。

重要：追踪文件可能包含个人信息或敏感信息。通过向卡巴斯基发送追踪文件，您同意向卡巴斯基提供您发送的追踪文件中包含的所有数据，并且您同意用于发送它们的方法。

有关应用程序的信息来源

本节介绍有关应用程序的信息来源。

您可以根据手头问题的重要性和紧迫性选择最方便的信息来源。

卡巴斯基网站上的 Kaspersky Endpoint Security 页面

在 卡巴斯基网站上的 Kaspersky Endpoint Security 页面，您可以查看有关该应用程序的常规信息及应用程序功能和特性。

Kaspersky Endpoint Security 页面包含指向在线商店的链接。您可以在那里购买或续订该应用程序。

知识库中的 Kaspersky Endpoint Security 页面

*知识库*是卡巴斯基技术支持网站的一部分。

在知识库中的 Kaspersky Endpoint Security 页面上，您可以阅读相关文章，这些文章提供了有用的信息、建议以及有关如何购买、安装和使用应用程序的常见问题解答。

知识库中的文章可能会解答 Kaspersky Endpoint Security 以及卡巴斯基其他应用程序的相关问题。知识库中的文章可能还包含卡巴斯基技术支持新闻。

从“帮助”下拉菜单进入知识库

1. 选择**帮助** → **支持**。
2. 单击**技术支持**。

在我们的论坛上讨论卡巴斯基应用程序

如果您的问题无需立答复，您可以在我们的论坛上与卡巴斯基专家和其他用户一起进行讨论。

在此论坛上，您可以查看讨论主题、发表评论并创建新的讨论主题。

从“帮助”下拉菜单进入论坛

1. 选择**帮助** → **支持**。
2. 单击**社区**。

附录

本节提供对文档文本的补充信息。

已知问题和限制

Kaspersky Endpoint Security 具有以下已知问题和限制：

- 如果您计算机上安装的某个应用程序收集信息并将其发送以供处理，则 Kaspersky Endpoint Security 应用程序可能会将其归类为恶意软件。若要避免该信息，您可以按照文档所述通过配置 Kaspersky Endpoint Security 应用程序从扫描中排除该应用程序。
- 可通过编辑配置文件修改应用程序功能设置。
- 在 Kaspersky Security Center 中，本地任务可能会在受管理设备的属性中列出两次。
- 更改本地更新任务的更新源将禁用自动执行更新任务。
- 如果您通过管理控制台启动计算机重新启动任务，并向用户发送包含分号 (;) 的消息，则该任务将显示为已完成，但不会提示用户重新启动 Mac。
- 要从 Kaspersky Endpoint Security 扫描范围中排除 Safari 网络流量，您需要将以下路径添加到排除项列表中：
  - `/System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.N`
  - `/System/Library/Frameworks/WebKit.framework/Versions/A/XPCServices/com.apple.WebKit.N`
  - `/System/Library/PrivateFrameworks/SafariShared.framework/Versions/A/XPCServices/com.a`
  - `/System/Library/Frameworks/webkit2.framework/versions/a/xpcservices/com.apple.webkit`
- 要从 Kaspersky Endpoint Security 扫描范围中排除 Google Chrome 网络流量，您需要将以下路径添加到排除项列表中：
  - `/Applications/Google Chrome.app/Contents/Frameworks/Google Chrome Framework.framework/Versions/<版本号>/Helpers/Google Chrome Helper.app/Contents/MacOS/Google Chrome Helper`
- 在使用 Kaspersky Security Center Web Console 和云控制台为 Kaspersky Endpoint Security 策略创建策略配置文件后，您需要检查客户端计算机上是否已正确应用这些设置。
- 在策略设置中启用文件保险箱磁盘加密后，具有管理员权限的用户可通过系统设置（系统偏好设置）解密其 Mac 的启动盘。
- 在代理服务器选项中所做的更改将仅在重启 Kaspersky Endpoint Security 后应用。
- Safari 可能无法连接到具有不受信任证书的网站。您可以将此类网站添加到排除项中，或者使用其他浏览器。
- 在通过 Kaspersky Security Center 远程卸载 Kaspersky Endpoint Security 11.2 或更高版本之后，应用程序系统功能扩展之一可能保存在计算机内存。之后，在极少数情况下，在安装 Kaspersky Endpoint Security 时，可能会出现完整磁盘访问权限问题。在这种情况下，我们建议在本地卸载应用程序并重新安装。

- 如果 Kaspersky Endpoint Security 正在运行，需要 Rosetta 的应用程序可能无法安装。要解决此问题，请退出 Kaspersky Endpoint Security 并尝试重新安装应用程序。
- 在复合对象中检测到的威胁的警报详细信息仅包含有关检测到的对象本身的信息，而不包含威胁发展链图。
- 保存“密码保护”的密码时，可能会出现错误。在这种情况下，我们建议卸载并重新安装该应用程序。
- Kaspersky Endpoint Security 不会扫描位于 OneDrive 或 iCloud 存储或者其他云存储中的文件。请将这些文件排除在扫描范围之外。否则，扫描任务可能会以“*受感染文件未删除*”错误结束。
- 您无法扫描被“将文件移至隔离区”任务隔离的对象。
- 在 Kaspersky Security Center 中，仅当 NetBIOS 名称、计算机名称和主机名相同时，设备名称才会正确显示。

已修复的问题

下表列出了Kaspersky Endpoint Security先前版本中发现并已在当前版本中修复的所有问题。

12.2.1 版本中修复的问题列表

问题 ID	问题描述
10054891	在Web Console的Kaspersky Endpoint Security for Mac策略中，无法将应用程序添加到受信任区域。

按扩展名扫描的对象列表

在 Kaspersky Security Center 中创建扫描任务时，如果在扫描设置中选择**按扩展名扫描应用程序和文档**选项，则 Kaspersky Endpoint Security 将对无扩展名对象和具有以下扩展名的对象执行恶意软件扫描：

常规格式：

- txt
- csv
- htm
- html

多媒体（音频/视频）文件：

- flv
- f4v
- avi
- 3gp
- 3g2
- 3gp2
- 3p2
- divx
- mp4
- mkv
- mov
- qt
- asf
- wmv
- rm
- rmvb
- vob
- dat
- mpg
- mpeg
- bik
- fcs
- mp3
- mpeg3
- flac
- ape

- ogg
- aac
- m4a
- wma
- ac3
- wav
- mka
- rm
- ra
- ravb
- mid
- midi
- cda

图像文件：

- jpg
- jpe
- jpeg
- jff
- gif
- png
- bmp
- tif
- tiff
- emf
- wmf
- eps

- psd
- cdr
- swf

可执行文件和系统文件：

- exe
- dll
- scr
- ocx
- com
- sys
- class
- o
- so
- elf
- prx
- vb
- vbs
- js
- bat
- cmd
- msi
- deb
- rpm
- sh
- pl
- dylib

文档和模板：

- doc
- dot
- docx
- dotx
- docm
- dotm
- xsl
- xls
- xlsx
- xltx
- xlsm
- xltm
- xlam
- xlsb
- ppt
- pot
- pps
- pptx
- potx
- pptm
- potm
- ppsx
- ppsm
- rtf
- pdf
- msg

- eml
- vsd
- vss
- vst
- vdx
- vsx
- vtx
- xps
- oxps
- one
- onepkg
- xsn
- odt
- ods
- odp
- sxw
- pub
- mdb
- accdb
- accde
- accdr
- accdc
- chm
- mht

压缩包：

- zip
- 7z*
- 7-z
- rar
- iso
- cab
- jar
- bz
- bz2
- tbz
- tbz2
- gz
- tgz
- arj
- dmg
- smi
- img
- xar

注意：文件的实际格式可能与文件扩展名不相符。

文件和文件夹路径中的掩码

*文件名称掩码*或*文件夹名称掩码*表示文件的名称和扩展名，或使用常用符号表示文件夹的名称。

在指定保护范围、扫描范围和受信任区域时，可以使用这些符号：

- 波浪形符号 `~` 替换文件或文件夹路径中的 `/Users/<用户名>`。例如，路径 `~/Desktop` 意味着保护范围包括要保护的计算机上的所有用户的 `Desktop` 文件夹。
- 星号 `*` 代替文件或文件夹名称中的任何一组字符，但 `\` 和 `/` 字符除外（用于在文件和文件夹路径中分隔文件和文件夹的名称）。例如，掩码 `/*/*.db*` 将包括指向扩展名以 `db` 开头的文件的所有路径，这些文件位于内部磁盘上的文件夹中，但不在子文件夹中。
- 两个连续的星号 `**` 代替文件或文件夹名称中的任何一组字符（包括空组），包括 `\` 和 `/` 字符（用于在文件和文件夹路径中分隔文件和文件夹的名称）。例如，掩码 `/Folder/**/*.txt` 将包括名为 `Folder` 及其子文件夹中具有 `TXT` 扩展名的文件的所有路径。掩码必须至少包含一个嵌套级别。掩码 `/**/*.txt` 不是有效的掩码。
- 问号 `?` 代替文件或文件夹名称中的单个字符，但 `\` 和 `/` 字符除外（用于在文件和文件夹路径中分隔文件和文件夹的名称）。例如，掩码 `/Folder/???.txt` 将包括位于名为 `Folder` 的文件夹中的所有文件的路径，这些文件的扩展名为 `TXT`，名称由三个字符组成。

IOC 文件要求

创建 IOC 扫描任务时，请考虑以下 IOC 文件要求和限制：

- 应用程序支持采用开放标准 OpenIOC 版本 1.0 和 1.1 或 STIX 版本 2.0 和 2.1、用于描述入侵指标、扩展名为 IOC、XML 和 JSON 的 IOC 文件。
- 如果在命令行上创建 IOC 扫描任务时上传了某些不受支持的 IOC 文件，则运行该任务时，应用程序仅使用受支持的 IOC 文件。如果在命令行上创建 IOC 扫描任务时，您上传的所有 IOC 文件均不受支持，则该任务仍可运行，但不会检测到任何入侵指标。无法使用 Web Console 或云控制台上传不受支持的 IOC 文件。
- IOC 文件中的语义错误和不受支持的 IOC 术语和标签不会导致任务执行失败。在 IOC 文件的此类部分中，应用程序未检测到匹配项。
- 单个 IOC 扫描任务中使用的所有 IOC 文件的标识符必须是唯一的。如果有相同标识符的 IOC 文件，可能会影响任务执行结果。
- 单个 IOC 文件大小不得超过 2 MB。使用较大的文件将导致 IOC 扫描任务因错误而终止。添加到 IOC 集合的所有文件的总大小不应超过 10 MB。如果所有文件的总大小超过 10 MB，则需要拆分 IOC 集合并创建多个 IOC 扫描任务。
- 建议为每个威胁创建一个 IOC 文件。这使得分析 IOC 扫描任务的结果变得更加容易。

下表显示了应用程序对 IOC 文件的支持的特点和限制。

对 IOC 文件的支持的特点和限制。

支持的条件	OpenIOC 1.0： is isnot （作为集合的例外） contains containsnot （作为集合的例外） OpenIOC 1.1： is contains starts-with ends-with matches greater-than less-than STIX 2.0 和 2.1： = != > < => <= in like matches
支持的条件属性	OpenIOC 1.1： preserve-case negate
支持的运算符	AND OR
支持的数据类型	"date"：日期（适用条件：is、greater-than、less-than） "int"：整数（适用条件：is、greater-than、less-than） "string"：字符串（适用条件：is、contains、matches、starts-with、ends-with） "duration"：持续时间（以秒为单位）（适用条件：is、greater-than、less-than）
数据类型解释的特点	"boolean string"、"restricted string"、"md5"、"IP"、"sha256"、"base64Binary"数据类型被解释为字符串。 当以间隔形式设置时，应用程序支持对"int"和"date"数据类型的"Content"设置的解释： OpenIOC 1.0： 在"Content"字段中使用"TO"运算符： <Content type="int">49600 TO 50700</Content> <Content type="date">2009-04-28T10:00:00Z TO 2009-04-28T16:00:00Z</Content> <Content type="int">[154192 TO 154192]</Content> OpenIOC 1.1： 使用"greater-than"和"less-than"条件 在"Content"字段中使用"TO"运算符 如果指标设置为"ISO 8601"、"Zulu Time Zone"、"UTC format"，则应用程序支持对"date"和"duration"数据类型的解释。

支持的用于执行防护的脚本解释器

执行防护支持以下脚本解释器：

- PkgUtil
- PkgInstaller

- /usr/bin/osascript
- /usr/bin/osacompile
- /usr/local/bin/python
- /usr/local/bin/python3
- /usr/bin/perl
- /usr/bin/ruby
- /bin/bash
- /bin/zsh
- /bin/sh
- /bin/dash
- /bin/csh
- /bin/ksh
- /bin/tcsh

重要：如果执行防护规则中指定的脚本由已经启动的 PkgUtil 或 PkgInstaller 脚本解释器打开，则不会阻止该脚本的执行。

如何将 Kaspersky Endpoint Security 证书添加到 Mozilla Firefox 证书存储

如果浏览器使用 Mozilla Firefox 证书存储，您需要手动导出卡巴斯基证书并将其添加到该证书存储中。否则浏览器将无法打开 HTTPS 页面。

导出卡巴斯基证书

1. 在 Mac 上打开“**启动板**”>“**其他**”>“**钥匙串访问**”。
2. 在窗口的左侧窗格中，单击**“系统”**并打开**“证书”**选项卡。
3. 在证书列表中，找到 **Kaspersky Web Anti-Virus Certification Authority**。
4. 右键单击该证书并选择**导出“Kaspersky Web Anti-Virus Certification Authority”**。
5. 选择保存证书的位置，然后单击**“保存”**。

卡巴斯基证书被保存。

将卡巴斯基证书添加到 Mozilla Firefox 证书存储

1. 打开 Mozilla Firefox
2. 在右上角，单击菜单按钮并选择“**设置**”。
3. 在窗口的左侧窗格中，选择“**隐私和安全**”。
4. 向下滚动到“**证书**”部分。
5. 单击“**查看证书**”。
6. 在打开的窗口中，单击“**导入**”。
7. 选择卡巴斯基证书文件并单击**“打开”**。
8. 选中**“信任此 CA 来识别网站”**和**“信任此 CA 来识别电子邮件用户”**复选框。单击**确定**。
   卡巴斯基证书被导入到 Mozilla Firefox 证书存储中。它显示在**“证书管理器”**窗口的证书列表中。

重要提示：每次重新安装 Kaspersky Endpoint Security 应用程序时，都会生成新的卡巴斯基根证书。这意味着，您需要在每次重新安装 Kaspersky Endpoint Security 应用程序后完成此过程。

与外部服务交互的网络设置

Kaspersky Endpoint Security 使用以下网络设置与外部服务交互。

网络设置

地址	描述
`activation-v2.kaspersky.com/activationservice/activationservice.svc` 协议：`HTTPS` 端口：`443`	激活应用程序。

地址	描述

`s00.upd.kaspersky.com`
`s01.upd.kaspersky.com`
`s02.upd.kaspersky.com`
`s03.upd.kaspersky.com`
`s04.upd.kaspersky.com`
`s05.upd.kaspersky.com`
`s06.upd.kaspersky.com`
`s07.upd.kaspersky.com`
`s08.upd.kaspersky.com`
`s09.upd.kaspersky.com`
`s10.upd.kaspersky.com`
`s11.upd.kaspersky.com`
`s12.upd.kaspersky.com`
`s13.upd.kaspersky.com`
`s14.upd.kaspersky.com`
`s15.upd.kaspersky.com`
`s16.upd.kaspersky.com`
`s17.upd.kaspersky.com`
`s18.upd.kaspersky.com`
`s19.upd.kaspersky.com`
`cm.k.kaspersky-labs.com`
协议：`HTTPS`
端口：`443`
	更新数据库和用于程序软件模块。

`downloads.upd.kaspersky.com` 协议：`HTTPS` 端口：`443`	• 更新数据库和用于程序软件模块。 • 验证对卡巴斯基服务器的访问。如果无法使用系统 DNS 访问服务器，应用程序将使用公共 DNS。这对于确保更新反病毒数据库和维护计算机的安全级别是必要的。Kaspersky Endpoint Security 按以下顺序使用以下公共 DNS 服务器列表： 1. Google Public DNS (8.8.8.8)。 2. Cloudflare DNS (1.1.1.1)。 3. Alibaba Cloud DNS (223.6.6.6)。 4. Quad9 DNS (9.9.9.9)。 5. CleanBrowsing (185.228.168.168)。 **重要：**应用程序发出的请求可能包含域地址和用户的公共 IP 地址，因为应用程序与 DNS 服务器建立了 TCP/UDP 连接。例如，在使用 HTTPS 时，需要此信息来验证 Web 资源的证书。如果 Kaspersky Endpoint Security 使用的是公共 DNS 服务器，则数据处理受相关服务的隐私策略约束。 **如何防止 Kaspersky Endpoint Security 使用公共 DNS 服务器** 1. 退出用户设备上的 Kaspersky Endpoint Security 应用程序。 2. 在位于 `/Library/Application Support/Kaspersky Lab/KAV/Binaries/config.xml` 的 Kaspersky Endpoint Security 应用程序的配置文件中添加 `ForceUseSystemDNS` 变量，并将值设置为 `1`。 3. 启动 Kaspersky Endpoint Security 应用程序。 这样，Kaspersky Endpoint Security 应用程序将仅使用系统 DNS。
`touch.kaspersky.com` 协议：`HTTP`	• 接收用于检查证书有效期（TLS 连接）的受信任时间。 • 运行 Web 威胁防护时，拒绝访问浏览器中的 Web 资源的警告。

地址	描述
p00.upd.kaspersky.com p01.upd.kaspersky.com p02.upd.kaspersky.com p03.upd.kaspersky.com p04.upd.kaspersky.com p05.upd.kaspersky.com p06.upd.kaspersky.com p07.upd.kaspersky.com p08.upd.kaspersky.com p09.upd.kaspersky.com p10.upd.kaspersky.com p11.upd.kaspersky.com p12.upd.kaspersky.com p13.upd.kaspersky.com p14.upd.kaspersky.com p15.upd.kaspersky.com p16.upd.kaspersky.com p17.upd.kaspersky.com p18.upd.kaspersky.com p19.upd.kaspersky.com downloads.kaspersky-labs.com cm.k.kaspersky-labs.com 协议：`HTTP` 端口：`80`	更新数据库和用于程序软件模块。
ds.kaspersky.com dc1.ksn.kaspersky-labs.com dc1-file.ksn.kaspersky-labs.com dc1-pp.ksn.kaspersky-labs.com dc1-st.ksn.kaspersky-labs.com 协议：`HTTPS` 端口：`443`	使用卡巴斯基安全网络。
ksn-a-stat-geo.kaspersky-labs.com ksn-file-geo.kaspersky-labs.com ksn-verdict-geo.kaspersky-labs.com ksn-url-geo.kaspersky-labs.com ksn-a-p2p-geo.kaspersky-labs.com ksn-info-geo.kaspersky-labs.com ksn-cinfo-geo.kaspersky-labs.com 协议：`KSN` 端口：`443`、`1443`	使用卡巴斯基安全网络。
click.kaspersky.com redirect.kaspersky.com 协议：`HTTPS` 端口：`443`	遵从界面的链接。

用于加密的设置

地址	描述
crl.kaspersky.com ocsp.kaspersky.com 协议：`HTTP` 端口：`80`	公共密钥基础架构(PKI)。

有关第三方代码的信息

有关第三方代码的信息包含在应用程序安装文件夹的 legal_notices.txt 文件中。

商标声明

注册商标和服务标志均为其各自拥有者的财产。

ActiveSync、Active Directory、Excel、IIS、Microsoft、Outlook、Windows、Windows Installer 和 WMI 是 Microsoft Corporation 的商标。

Apple、Apple Remote Desktop、FileVault、iCloud、Keychain、Launchpad、Mac、macOS、Rosetta、Safari 和 Xcode 是 Apple Inc. 的商标。

Chrome、Gmail、Google 和 Google Chrome 是 Google LLC. 的商标。

Composer 和 JAMF 是 JAMF SOFTWARE，LLC 在美国和其他国家的注册商标或普通法商标。

Firefox、Mozilla 和 Thunderbird 是 Mozilla Foundation 在美国和其他国家的商标。

Intel 是英特尔公司或其子公司的商标。

JavaScript 是 Oracle 和/或其附属公司的注册商标。

Linux 是 Linus Torvalds 在美国和其他国家/地区的注册商标。

Parallels、Parallels 徽标和 Coherence 是 Parallels International GmbH 的商标或注册商标。

Vmware 和 VMware Fusion 是 VMware, Inc. 在美国和/或其他地区的注册商标和/或商标。

“用户支持”窗口

此窗口提供以下信息：

- Kaspersky Endpoint Security 的版本
- Kaspersky Endpoint Security 当前使用的数据库的发布日期
- 计算机上安装的操作系统版本

技术支持

单击此按钮可打开卡巴斯基技术支持知识库，您可以在其中找到 卡巴斯基专家发布的有关 Kaspersky Endpoint Security 的文章。

社区

单击此按钮可打开社区，您可以在其中与卡巴斯基专家和其他用户讨论 Kaspersky Endpoint Security 的相关问题。

关闭

单击此按钮关闭用户支持窗口。

“证书设置”窗口

在“**常规**”选项卡上，您可以选择用于在 Mozilla Firefox 浏览器中检查加密 HTTPS 流量的证书存储：

- **System Roots 证书链(推荐)**
- **Mozilla Firefox 浏览器设置中的证书存储**

  此种情况下，您需要手动将 Kaspersky Endpoint Security 证书添加到 Mozilla Firefox 浏览器的证书存储中。有关更多信息，请参阅“如何将 Kaspersky Endpoint Security 证书添加到 Mozilla Firefox 证书存储”。

在“**受信任证书**”选项卡，您可以在其中创建受信任的根证书列表，以连接到相应的服务器，而无需通知。

该列表默认为空。

+

单击此按钮将打开一个对话框，用于添加将被视为受信任的证书。

–

单击该按钮可以从受信任证书列表中删除选定的证书。

证书名称

该列显示受信任的根证书的名称。

取消

单击此按钮将关闭窗口而不保存更改。

保存

单击此按钮可保存受信任根证书的当前列表并关闭窗口。

“验证证书”窗口

显示证书

单击此按钮将打开一个包含证书信息的系统窗口。

取消

单击此按钮关闭窗口。

添加到受信任

单击此按钮将证书添加到受信任证书列表中。这样，您将能够连接到相应的服务器而无需通知。

连接

单击此按钮可将您连接到服务器。

> **注意：**可用按钮可能因证书类型而异。

“选择证书”窗口

可用证书列表

选中证书旁边的复选框，以便在连接到服务器时使用该证书。

显示证书

单击此按钮将打开一个包含证书信息的系统窗口。

取消

单击此按钮关闭窗口。

继续

单击此按钮将继续使用所选证书连接到服务器。

“检测到受密码保护的压缩包”窗口

在运行文件威胁防护或扫描任务时，如果 Kaspersky Endpoint Security 需要扫描受密码保护的压缩包，则会显示一个通知窗口。

压缩包

存档的路径。

密码

用于输入密码的字段。

如果输入密码，Kaspersky Endpoint Security 将对该压缩包执行恶意软件和其他计算机安全威胁扫描。

跳过受保护的压缩包

单击此按钮将跳过该对象以及相同类型的所有对象。

跳过

单击此按钮可跳过对象。

“检测到的对象”对话框

当 Kaspersky Endpoint Security 检测到病毒或其他计算机安全威胁时，将在屏幕上显示一个通知窗口。

检测到

根据 卡巴斯基病毒百科全书 分类的对象名称。

详细信息

单击该按钮打开 卡巴斯基病毒百科全书 中带有所检测对象信息的页面。

对象

包含检测到对象的文件夹路径或检测到该对象的网址。

应用到全部

在文件威胁防护、Web 威胁防护或恶意软件扫描任务的当前会话期间，此复选框可启用/禁用针对相同类型的所有对象执行所选操作。

默认取消选中此复选框。

文件威胁防护或 Web 威胁防护的当前会话是指从组件启动到其停止运行或此应用程序关闭或重启的持续时间段。恶意软件扫描任务的当前会话是指从恶意软件扫描任务开始到完成之间的时间。

带有对所检测对象可执行的操作的按钮根据所检测对象的类型而变化。

您可以选择以下操作之一：

- **清除**。清除该对象。在执行清除之前，Kaspersky Endpoint Security 会创建文件的备份副本，以便您以后可以恢复原始文件。
- **删除**。删除该对象。在执行删除之前，Kaspersky Endpoint Security 会创建文件的备份副本，以便您以后可以恢复原始文件。
- **不阻止**。允许访问被视为危险 Web 流量对象的网站。
- **阻止**。拒绝访问被视为危险 Web 流量对象的网站。
- **删除压缩包**。删除包含已检测到的对象的压缩文件。
- **跳过受保护的压缩包**。恶意软件扫描期间跳过受密码保护的压缩文件。
- **跳过**。阻止访问该对象，但不对其执行任何操作。

“扫描”窗口



单击此按钮可返回到上一个 Kaspersky Endpoint Security 窗口。



单击此按钮可前进到下一个 Kaspersky Endpoint Security 窗口。

单击此按钮可删除“**扫描**”窗口中所有恶意软件扫描任务的所有记录。

计划扫描

单击此按钮将会打开一个对话框，您可以在其中安排全盘扫描或快速扫描任务。

快速扫描

单击该部分中的开始按钮（）运行快速扫描任务。

全盘扫描

单击该部分中的开始按钮（）运行全盘扫描任务。

单击此按钮可停止所选恶意软件扫描任务。

如果恶意软件扫描任务正在运行，将显示此按钮。

设置

单击此按钮将打开“**扫描**”选项卡，您可以在其中配置扫描任务设置。

选择

单击此按钮将会打开一个对话框，您可以在其中选择要扫描的文件或文件夹。

在“**文件和文件夹**”部分的下半部分，您可以查看对所选文件或文件夹执行的所有恶意软件扫描任务的记录。

详细信息

单击此按钮可打开恶意软件扫描任务报告窗口。

将指针悬停在扫描任务上时，将显示此按钮。

清空扫描历史记录

单击此按钮将删除所有恶意软件扫描任务的所有记录。

显示全部

单击此按钮可打开**已检测到的对象**窗口，可在其中查看所有已检测到的对象。

注意： Kaspersky Endpoint Security 不会扫描位于 OneDrive 或 iCloud 存储或者其他云存储中的文件。请将这些文件排除在扫描范围之外。否则，扫描任务可能会以“*受感染文件未删除*”错误结束。

“已检测到的对象”窗口

已检测到的对象区域包含应用程序检测到的恶意对象。

清除全部

单击此按钮启动对已检测到的所有恶意对象的清除。

忽略全部

单击此按钮可从**已检测到的对象**区域的恶意对象列表中删除所有恶意对象。

•••

单击此按钮可打开一个弹出菜单，可从中选择对恶意对象执行以下操作之一：

- **清除**。清除该对象。在清除之前，Kaspersky Endpoint Security 应用程序会创建文件的备份副本，以便可以在以后恢复或清除此文件，而不会面临数据丢失的风险。
- **忽略**。从检测到的对象列表中删除对象。

其他对象区域包含检测到的非恶意但会被黑客利用损害您的计算机或数据的对象。

删除全部

单击此按钮可从计算机中删除所有已检测到的对象。

忽略全部

单击此按钮可从**其他对象**区域的检测到的对象列表中删除所有检测到的对象。

•••

单击此按钮可打开一个弹出菜单，可从中选择对检测到的对象执行以下操作之一：

- **删除**。从计算机中删除检测到的对象。
- **忽略**。从检测到的对象列表中删除对象。

备份区域包含检测到的对象的备份副本。

删除全部

单击此按钮可从计算机中删除检测到的对象的所有备份副本。

•••

单击此按钮可打开一个弹出菜单，可从中选择对备份对象执行以下操作之一：

- **删除备份副本**。从计算机中删除检测到的对象的备份副本。
- **恢复文件**。将列表中选定文件的备份副本恢复到其原始位置，并使用与清除或删除之前的原始文件相同的名称。如果原始位置存在同名对象（例如，在清除前 Kaspersky Endpoint Security 已创建原始文件副本或已清除原始文件），将会显示警告。您可以更改要将对象恢复到的位置或者重命名对象。

“授权许可”窗口



单击此按钮可返回到上一个 Kaspersky Endpoint Security 窗口。



单击此按钮可前进到下一个 Kaspersky Endpoint Security 窗口。

注意：该窗口根据 Kaspersky Endpoint Security 是否被激活以及所使用的授权许可或订阅类型而变化。

该窗口可能包含以下信息：

- 授权许可或订阅状态
- 活动密钥
- 备用密钥（如果有）
- 授权许可类型，以及可在当前授权许可或订阅下使用该应用程序的计算机数量
- 当前授权许可或订阅下可用的应用程序功能
- 授权许可到期日期和时间
- 授权许可到期之前的剩余天数

在该窗口中，您可以执行以下操作：

- 使用激活码激活应用程序。
- 转到关于如何在卡巴斯基在线商店购买授权许可的网站。
- 打开包含订阅续费信息的 Kaspersky Endpoint Security 供应商的网站。
- 更新您的订阅状态。

有关 Kaspersky Endpoint Security 授权许可的更多信息，请与贵组织的系统管理员联系。

“保护范围”窗口

在**保护范围**区域，您可以查看和编辑保护范围。

所有可移动磁盘

此复选框可启用/禁用所有可移动磁盘的实时保护。

默认情况下已选定该选框。

所有内部磁盘

此复选框可启用/禁用所有内部磁盘的实时保护。

默认情况下已选定该选框。

所有网络磁盘

此复选框可启用/禁用所有网络磁盘的实时保护。

默认情况下已选定该选框。

+

单击此按钮会打开一个列表，您可以在其中选择项目以创建保护范围：

- **文件和文件夹**。选择此项可打开一个用于向保护范围中添加文件或文件夹的对话框。
- **所有磁盘**。选择此项可将计算机的所有可移动磁盘、内部磁盘和网络磁盘添加到保护范围。
- **所有可移动磁盘**。选择此项可将计算机的所有可移动磁盘添加到保护范围。
- **所有内部磁盘**。选择此项可将计算机的所有内部磁盘添加到保护范围。
- **所有网络磁盘**。选择此项可将计算机的所有网络磁盘添加到保护范围。
- **内存**。选择此项可将计算机内存添加到保护范围。
- **启动对象**。选择此项可将在操作系统启动时启动的所有可执行文件添加到保护范围。扫描启动对象可以检测 Rootkit。

使用列表项旁边的复选框，可启用/禁用与此项关联的对象的实时保护。

–

单击此按钮可从保护范围列表中删除选定的项。

默认无法删除保护范围列表中包含的项。

在**优化**部分，您可以配置 Kaspersky Endpoint Security 是否扫描只读系统卷。

跳过扫描只读系统卷

此复选框禁用/启用由 Kaspersky Endpoint Security 扫描只读系统卷。

默认情况下已选定该选框。

重要：优化可能由于安全原因而禁用。

“扫描范围”窗口

在此窗口中，您可以查看和编辑快速扫描任务的扫描范围。

使用列表中的对象旁边的复选框可启用/禁用该对象的扫描。

+
单击此按钮可打开一个用于调整扫描范围的列表：

- **文件和文件夹**。选择此项将会打开一个对话框，用于向扫描范围添加文件或文件夹。
- **所有磁盘**。选择此项可将计算机的所有可移动磁盘、内部磁盘和网络磁盘添加到扫描范围。
- **所有外部磁盘**。选择此项可将计算机的所有可移动磁盘添加到扫描范围。
- **所有内部磁盘**。选择此项可将计算机的所有内部磁盘添加到扫描范围。
- **所有网络磁盘**。选择此项可将计算机的所有网络磁盘添加到扫描范围。
- **内存**。选择此项可将计算机内存添加到扫描范围。
- **启动对象**。选择此项可将在操作系统启动时启动的所有可执行文件添加到扫描范围。扫描启动对象可以检测 Rootkit。

–
单击此按钮可以从扫描范围列表中删除选定的项。
默认无法删除扫描范围列表中包含的项。
在**优化**区域中，您可以配置 Kaspersky Endpoint Security 在执行扫描任务时是否扫描只读系统卷。

跳过扫描只读系统卷

此复选框禁用/启用由 Kaspersky Endpoint Security 扫描只读系统卷。
如果选择此复选框，则 Kaspersky Endpoint Security 将不扫描只读系统卷。这大大缩短了扫描时间。
如果清除此复选框，则 Kaspersky Endpoint Security 将扫描只读系统卷。
默认情况下已选定该选框。

注意： Kaspersky Endpoint Security 不会扫描位于 OneDrive 或 iCloud 存储或者其他云存储中的文件。请将这些文件排除在扫描范围之外。否则，扫描任务可能会以“*受感染文件未删除*”错误结束。

“基本”选项卡

在**常规**区域中，您可以启用或禁用使计算机免受恶意软件和其他计算机安全威胁侵害的保护组件。

启用保护

此复选框可启用/禁用实时保护以抵御恶意软件和其他计算机安全威胁侵害。

默认情况下已选定该选框。

检查安全连接 (HTTPS)

此复选框可启用/禁用 Kaspersky Endpoint Security 对加密连接 (HTTPS) 进行扫描，并在“Web 控制”阻止用户访问危险网络资源时显示通知。

默认取消选中此复选框。

受信任区域

单击此按钮将打开一个窗口，您可以在其中通过创建您信任且不想扫描恶意软件的对象列表来编辑受信任区域。

设置

单击此按钮将打开一个窗口，您可以在其中管理受信任的根证书列表并选择证书存储以在 Mozilla Firefox 浏览器中检查加密的 HTTPS 流量。

在**文件威胁防护**区域中，可启用或禁用文件威胁防护，并选择 Kaspersky Endpoint Security 在检测到受感染文件时执行的操作。

启用文件威胁防护

此复选框启用/禁用文件威胁防护。

默认情况下已选定该选框。

保护范围

单击此按钮可打开一个窗口，您可在此窗口中创建保护范围。

自动清除或删除恶意对象

Kaspersky Endpoint Security 阻止对受感染文件的访问，并尝试在未请求用户确认的情况下对其进行清除。在执行清除前，Kaspersky Endpoint Security 将在备份中保存文件的备份副本。清除成功，Kaspersky Endpoint Security 将文件保存在原始文件名下的原始位置。如果清除失败，Kaspersky Endpoint Security 会将受感染的文件保持在其原始位置的阻止状态。有关删除受感染对象的信息记录在**已处理的对象**报告中。

提示操作

Kaspersky Endpoint Security 将显示一个通知窗口，其中包含可能使文件受到感染的恶意对象的相关信息，并提示您选择 Kaspersky Endpoint Security 要执行的操作。可用的操作可能因对象的状态而异。

默认选择此操作。

在 **Web 威胁防护**区域中，可启用或禁用 Web 威胁防护，并选择 Kaspersky Endpoint Security 在检测到危险 Web 流量对象时执行的操作。

启用 Web 威胁防护

此复选框启用/禁用 Web 威胁防护。

默认情况下已选定该选框。

自动阻止危险 Web 流量对象

Kaspersky Endpoint Security 将阻止访问从中检测到危险 Web 流量对象的网站，而不请求确认。

提示操作

Kaspersky Endpoint Security 将显示一个通知窗口，其中包含检测到的危险 Web 流量对象的相关信息，并提示您选择 Kaspersky Endpoint Security 要执行的操作。可用的操作可能因对象的状态而异。

默认选择此操作。

在“**邮件威胁防护**”区域中，您可以启用或禁用邮件威胁防护，并选择 Kaspersky Endpoint Security 在检测到恶意对象时执行的操作。

启用邮件威胁防护

此复选框启用/禁用邮件威胁防护。

默认情况下已选定该选框。

自动删除恶意对象

当 Kaspersky Endpoint Security 在电子邮件中检测到受感染的对象时，它会删除受感染的对象，并用文本“The requested file infected with <病毒名称> has been deleted”替换对象的内容。

自动阻止恶意对象

当 Kaspersky Endpoint Security 在电子邮件中检测到受感染的对象时，它会将电子邮件主题替换为“Message is infected: <原始主题>”，其中 <原始主题> 为原始主题。仅为 POP3 协议替换电子邮件消息主题。

在“**网络威胁防护**”区域中，可启用或禁用网络威胁防护。

启用网络威胁防护

此复选框启用/禁用网络威胁防护。

默认情况下已选定该选框。

设置

单击此按钮可打开一个窗口，您可在其中创建受信任计算机列表或查看和编辑阻止的计算机列表。



单击此按钮可防止不具有管理员权限的用户更改 Kaspersky Endpoint Security 应用程序的设置。



单击此按钮会提示您输入管理员凭证。输入管理员凭证后，应用程序设置将可编辑。

“受信任应用程序”选项卡

在“**受信任应用程序**”选项卡上，可以创建不希望 Kaspersky Endpoint Security 应用程序监控的应用程序列表。

默认情况下，受信任区域对象列表为空。

+

单击此按钮将打开一个窗口，您可以在其中输入应用程序的路径，指定其代码签名要求并选择 Kaspersky Endpoint Security 不会监控的活动类型。

–

单击该按钮可以从受信任区域中删除选定的应用程序。

编辑

单击此按钮可打开一个窗口，您可在此窗口编辑受信任应用程序的参数。

“添加受信任应用程序”窗口

路径

其网络或文件活动将不受 Kaspersky Endpoint Security 监控的应用程序的路径。

注意：不能使用符号链接来指定此字段中的路径。

选择

单击此按钮将打开一个窗口，您可以在其中选择其活动将不受 Kaspersky Endpoint Security 监控的应用程序。在这种情况下，“**路径**”和“**代码签名要求**”字段的值会自动插入。

代码签名要求

对其活动不受 Kaspersky Endpoint Security 监控的应用程序的代码签名的要求。

这是一个可选参数。

在“**选项**”部分，您可以选择不想被 Kaspersky Endpoint Security 应用程序监控的活动类型。

不监控文件活动

此复选框启用/禁用应用程序对客户端计算机上的文件的操作的监控。

如果选中此复选框，则 Kaspersky Endpoint Security 将不会监控应用程序的文件活动。

如果清除此复选框，则 Kaspersky Endpoint Security 将监控应用程序的文件活动。

默认情况下已选定该选框。

不监控网络活动

此复选框启用/禁用对客户端计算机上应用程序的入站和出站互联网流量的监控。

如果选中此复选框，则 Kaspersky Endpoint Security 将不会监控应用程序的网络活动。

如果清除此复选框，则 Kaspersky Endpoint Security 将监控应用程序的网络活动。

默认情况下已选定该选框。

取消

单击此按钮将关闭窗口而不保存更改。

确定

单击此按钮将保存受信任应用程序的参数并关闭窗口。

“受信任文件和文件夹”选项卡

在**文件和文件夹**选项卡上，可以创建不希望 Kaspersky Endpoint Security 应用程序监控的文件和文件夹列表。

默认情况下，受信任区域对象列表为空。

+

单击此按钮将打开一个用于选择文件或文件夹的对话框。

–

单击此按钮可以从受信任区域移除选中的对象。

“信受任网址”选项卡

在**网址**选项卡上，可以创建不希望 Kaspersky Endpoint Security 应用程序监控的网址列表。

默认情况下，受信任区域对象列表为空。

+

单击此按钮可添加一个用于输入网址的字段。

指定网站地址时，您可以使用以下符号：

- 星号 (`*`) 代替任意字符集，除了 `\` 和 `/` 字符。
- 两个连续的星号 (`**`) 代替任意字符集（包括空集），包括 `\` 和 `/` 字符。
- 问号 (`?`) 代替文件或文件夹名称中的任何单个字符，除了 `\` 和 `/` 字符。

–

单击该按钮可以从受信任区域中删除选定的网址。

“邮件威胁防护”设置窗口

跳过大于此大小的存档 <值> MB

如果选中此复选框，则当电子邮件消息中附加的存档大小超过指定值时，邮件威胁防护会将其排除在扫描范围之外。

如果清除此复选框，邮件威胁防护将扫描任意大小的电子邮件附件存档。

默认值为 8 MB。

默认情况下已选定该选框。

限制检查存档的时间到 <值> 秒

如果选中此复选框，则分配给扫描电子邮件附件存档的时间将限制为指定的时间段。

如果清除此复选框，则分配给扫描存档的时间不受限制。

默认值是 5 秒。

默认情况下已选定该选框。

“设置”窗口

在**受信任计算机**选项卡上，您可以创建受信任计算机的列表。Kaspersky Endpoint Security 应用程序不会阻止这些计算机 IP 地址，甚至在这些计算机上检测到危险网络活动时也是如此。

受信任计算机列表默认为空。

+

单击此按钮可添加一个字段，用于输入受信任计算机 IP 地址。

–

单击该按钮可以从受信任计算机列表中删除选定的 IP 地址。

编辑

单击此按钮将使所选 IP 地址可编辑。

在**阻止的计算机**选项卡上，您可以查看和编辑阻止的计算机列表。

检测到来自此计算机的危险网络活动后，Kaspersky Endpoint Security 应用程序会将此 IP 地址的计算机阻止一个小时。

IP 地址

此列显示被阻止的计算机 IP 地址。

事故时间

此列显示在计算机上检测到危险网络活动的日期和时间。

解除阻止

单击该按钮可以从被阻止的计算机列表中删除选定的 IP 地址。

“网络数据包规则”选项卡

规则名称

网络数据包规则名称。

在“**操作**”区域中，您可以选择 Kaspersky Endpoint Security 在检测到网络活动时要执行的操作。

在“**协议**”区域，您可以指定网络规则适用的协议。

在“**方向**”区域，您可以指定被监控的网络活动的方向。

在“**TTL**”区域，您可以指定被监控的网络数据包的生存期。

在“**网络适配器**”区域，您可以指定网络规则适用的网络适配器。

在“**远程地址**”区域，您可以指定可以发送和接收网络数据包的远程设备的网络地址。

在“**本地地址**”区域，您可以指定可以发送和接收网络数据包的设备的本地网络地址。

记录事件

使用此复选框可启用/禁用记录防火墙事件。

如果选中此复选框，则 Kaspersky Endpoint Security 会在报告中记录防火墙事件。

如果清除此复选框，则 Kaspersky Endpoint Security 不会在报告中记录防火墙事件。

默认取消选中此复选框。

“网络适配器”窗口

适配器名称

网络适配器名称。

接口类型

从此下拉列表中，您可以选择网络适配器的接口类型。

IP 地址

IP 地址列表。

MAC 地址

MAC 地址列表。

“网络适配器”窗口

名称

此列包含网络适配器名称。

接口类型

此列包含网络适配器的接口类型。

IP 地址

此列包含网络适配器的 IP 地址。

MAC 地址

此列显示网络适配器的 MAC 地址。

“本地地址”窗口

本地地址

此列包含本地地址。

“本地地址”窗口

类型

此下拉列表用于指定希望网络规则适用的本地 IP 条目的类型。

IP 地址

IP 地址输入字段。此字段仅当在**类型**下拉列表中选择 **IP 地址**时可用。

范围起始值

IP 地址范围起始值输入字段。此字段仅当在**类型**下拉列表中选择 **IP 地址范围**时可用。

范围结束值

IP 地址范围结束值输入字段。此字段仅当在**类型**下拉列表中选择 **IP 地址范围**时可用。

“远程地址”窗口

远程地址

此列包含远程地址。

“远程地址”窗口

类型

此下拉列表用于指定希望网络规则适用的远程地址条目的类型。

地址

IP 地址或 DNS 名称输入字段。此字段仅当在**类型**下拉列表中选择 **IP 地址或 DNS 名称**时可用。

范围起始值

IP 地址范围起始值输入字段。此字段仅当在**类型**下拉列表中选择 **IP 地址范围**时可用。

范围结束值

IP 地址范围结束值输入字段。此字段仅当在**类型**下拉列表中选择 **IP 地址范围**时可用。

“模板”窗口

网络规则模板

此列包含网络规则模板。

“网络数据包规则”选项卡

名称

网络规则的名称。

操作

防火墙在检测到网络活动类型时要执行的操作。

地址

应用网络规则的网络地址。

“可用网络”选项卡

名称

此列包含网络名称。

网络状态

此列包含网络状态。

IP 地址

此列包含网络 IP 地址。

“可用网络”窗口

网络名称

网络名称。

网络状态

网络状态下拉列表。

IP 地址

网络 IP 地址。

“MAC 地址”窗口

类型

此下拉列表用于指定希望网络规则适用的 MAC 地址条目的类型。

MAC 地址

MAC 地址输入字段。此字段仅当在**类型**下拉列表中选择 **MAC 地址**时可用。

掩码

MAC 地址掩码输入字段。此字段仅当在**类型**下拉列表中选择 **MAC 地址掩码**时可用。

范围起始值

MAC 地址范围起始值输入字段。此字段仅当在**类型**下拉列表中选择 **MAC 地址范围**时可用。

范围结束值

MAC 地址范围结束值输入字段。此字段仅当在**类型**下拉列表中选择 **MAC 地址范围**时可用。

“高级”选项卡

在“**KSN**”区域中，您可以阅读卡巴斯基安全网络声明的条款并选择是否加入卡巴斯基安全网络。

显示 KSN 声明

单击此按钮会打开一个窗口，其中显示卡巴斯基安全网络声明的文本。

Kaspersky Endpoint Security 可使用全球或私有 KSN 基础设施。如果加入卡巴斯基安全网络，则 Kaspersky Endpoint Security 将使用从卡巴斯基安全网络接收的有关文件、网络资源和应用程序信誉的信息，并向卡巴斯基安全网络提供检测服务运行所需的数据。

加入卡巴斯基安全网络

使用此复选框可启用/禁用加入卡巴斯基安全网络的选项。

参与卡巴斯基私人安全网络

使用此复选框可启用/禁用加入卡巴斯基私人安全网络。有关加入卡巴斯基私人安全网络的更多信息，请与贵组织的系统管理员联系。

启用扩展 KSN 模式

此复选框用于启用/禁用向卡巴斯基安全网络提供其他数据。这些数据用于提高您计算机的保护性能和 Kaspersky Endpoint Security 的易用性。您可以在卡巴斯基安全网络声明和 Kaspersky Endpoint Security 帮助中找到数据列表。

如果选中**加入卡巴斯基安全网络**复选框，则将自动选中此复选框，但您可以取消选中此复选框。

启用云模式

云模式是指 Kaspersky Endpoint Security 使用轻量版本反恶意软件数据库的应用程序操作模式。此模式仅在启用卡巴斯基安全网络的参与时可用。轻量版本的反恶意软件数据库所占用的计算机内存大概是通常数据库的一半。如果您不参与卡巴斯基安全网络或禁用云模式，Kaspersky Endpoint Security 将从卡巴斯基服务器下载完整版本的反恶意软件数据库。

如果打开了切换按钮，Kaspersky Endpoint Security 将使用轻量版本的反恶意软件数据库，这将减少操作系统资源的负载。

注意：选中该复选框后，Kaspersky Endpoint Security 在下次更新期间下载轻量版本的反恶意软件数据库。

如果切换按钮关闭，Kaspersky Endpoint Security 将使用完整版本的反恶意软件数据库。

注意：清空该复选框后，Kaspersky Endpoint Security 在下次更新期间下载完整版本的反恶意软件数据库。

在“**行为检测**”部分，您可以启用/禁用行为检测组件并选择在检测到恶意软件活动时执行的操作。

启用行为检测

此复选框启用/禁用行为检测组件，该组件接收有关计算机上应用程序操作的信息并将其提供给其他保护组件以提高其性能。

阻止恶意软件活动

如果选择此选项，Kaspersky Endpoint Security 会在检测到恶意活动时终止应用程序。

删除检测到的危险对象

如果选择此选项，Kaspersky Endpoint Security 会在检测到恶意活动时删除恶意应用程序的可执行文件并在备份中创建该文件的备份副本。

提示操作

如果选择此选项，当检测到恶意活动时，Kaspersky Endpoint Security 应用程序将显示一个通知窗口，其中包含有关恶意对象的信息，并提示用户选择 Kaspersky Endpoint Security 应用程序要采取的操作。可用的操作可能因对象的状态而异。



单击此按钮可防止不具有管理员权限的用户更改 Kaspersky Endpoint Security 应用程序的设置。



单击此按钮会提示您输入管理员凭证。输入管理员凭证后，应用程序设置将可编辑。

“扫描”选项卡

恶意软件扫描任务列表

包含预设恶意软件扫描任务：

- **全盘扫描**。计算机内存、启动对象和所有内部磁盘的恶意软件扫描。
- **快速扫描**。仅对计算机的关键区域执行恶意软件扫描：内存、启动对象和系统文件夹。
- **自定义扫描**。对指定对象（文件、文件夹、内部磁盘或可移动磁盘）执行恶意软件扫描。
- **外部磁盘扫描**。当计算机连接到外部磁盘时，将执行外部磁盘恶意软件扫描。

注意： Kaspersky Endpoint Security 不会扫描位于 OneDrive 或 iCloud 存储或者其他云存储中的文件。请将这些文件排除在扫描范围之外。否则，扫描任务可能会以“*受感染文件未删除*”错误结束。

在**扫描范围**区域中，可以查看和编辑快速扫描任务的扫描范围。

编辑

单击此按钮可打开一个窗口，您可在该窗口中查看和编辑扫描范围。

仅当在列表中选择了快速扫描任务时，此按钮才可用。

在**操作**区域中，可以选择 Kaspersky Endpoint Security 在检测到受感染文件时执行的操作，并安排任务计划。

自动清除或删除恶意对象

Kaspersky Endpoint Security 阻止对受感染文件的访问，并尝试在未请求用户确认的情况下对其进行清除。在执行清除前，Kaspersky Endpoint Security 将在备份中保存文件的备份副本。清除成功，Kaspersky Endpoint Security 将文件保存在原始文件名下的原始位置。如果清除失败，Kaspersky Endpoint Security 会将受感染的文件保持在其原始位置的阻止状态。有关删除受感染对象的信息记录在**已处理的对象**报告中。

扫描完成时提示操作

在扫描完成之前，Kaspersky Endpoint Security 将推迟处理检测到的受感染文件。扫描完成后，Kaspersky Endpoint Security 将显示通知窗口，通知您检测到每一个受感染对象，并提示您选择进一步操作。可用的操作可能因对象的状态而异。

默认选择此操作。

在“**外部磁盘扫描**”选项卡的“**连接了外部磁盘时**”部分，您可以选择连接外部磁盘时 Kaspersky Endpoint Security 执行的操作。

扫描

如果选择此选项，Kaspersky Endpoint Security 将启动对所连接的外部磁盘的恶意软件扫描任务。

默认选择此选项。

什么都不做

如果选择此选项，Kaspersky Endpoint Security 将不会扫描连接的外部磁盘。

在**优化**区域中，您可以配置 Kaspersky Endpoint Security 在执行快速扫描或全盘扫描时是否扫描只读系统卷。

跳过扫描只读系统卷

此复选框禁用/启用由 Kaspersky Endpoint Security 扫描只读系统卷。

该复选框对快速扫描任务默认选中，对全盘扫描任务默认不选。

重要：优化可能由于安全原因而禁用。

CPU 使用

单击此按钮将打开一个对话框，您可以在其中启用或禁用在执行扫描任务时限制应用程序对受保护设备的 CPU 的使用。如果选择**将扫描的 CPU 使用率限制为**选项，您可以在相应字段中指定允许的最大 CPU 使用率。

注意：这是所有 CPU 内核的累积限制。活动监控中显示的 CPU 利用率是每个 CPU 内核利用率的总和，因此可能会超过 100%。

启用此选项会对 Kaspersky Endpoint Security 的性能产生负面影响。

默认情况下，该选项已禁用。

计划

单击此按钮将会打开一个对话框，您可以在其中安排全盘扫描或快速扫描任务。



单击此按钮可防止不具有管理员权限的用户更改 Kaspersky Endpoint Security 应用程序的设置。



单击此按钮会提示您输入管理员凭证。输入管理员凭证后，应用程序设置将可编辑。

“威胁”选项卡

您可以在**要检测的对象**部分中配置要检测的对象列表。

病毒、蠕虫、木马、恶意工具、广告软件和自动拨号软件

此类别包括以下类型的程序：

- 所有类型的恶意软件。
- 在您的计算机上显示广告（例如，广告栏）或使用广告网站替换浏览器中的搜索结果的应用程序。
- 通过计算机的调制解调器秘密建立电话连接的应用程序。

Kaspersky Endpoint Security 始终监控此类程序。

始终选中此复选框，且无法取消选中。

可以被入侵者利用以损坏您的计算机或个人数据的合法软件

使用此复选框可启用/禁用对合法应用程序的管理，入侵者可能会利用这些应用程序对用户的计算机或数据造成危害（例如，远程管理应用程序）。

默认取消选中此复选框。

在**备份**区域中，您可以指定对象在备份中可存储多长时间。

在此天数后删除备份对象天

此复选框启用/禁用在指定时间段后从备份中删除对象。

如果选中此复选框，则在该复选框旁边的数字字段中指定的期限后，应用程序将从备份中删除对象。如果取消选中此复选框，对象将无限期地存储在备份中。

默认选中此复选框，对象将在备份中存储 30 天。

在“**排除项**”区域中，您可以创建您信任而无需进行恶意软件扫描的文件、文件夹、应用程序和网站的列表。

受信任区域

单击此按钮将打开一个窗口，您可以在其中通过创建您信任且不想扫描恶意软件的对象列表来编辑受信任区域。

注意：当管理员将策略配置为禁止编辑受信任区域时，用户无法转到“受信任区域”设置。



单击此按钮可防止不具有管理员权限的用户更改 Kaspersky Endpoint Security 应用程序的设置。



单击此按钮会提示您输入管理员凭证。输入管理员凭证后，应用程序设置将可编辑。

“更新”选项卡

在**数据库**区域中，可以配置 Kaspersky Endpoint Security 数据库的更新模式。

自动下载更新

此复选框可启用/禁用应用程序数据库的自动更新。

默认情况下已选定该选框。

在**代理**区域中，可配置使用代理服务器更新 Kaspersky Endpoint Security。

使用代理服务器

此复选框可启用/禁用在更新反恶意软件数据库和应用程序模块时使用代理服务器连接到互联网。

默认情况下已选定该选框。

设置

单击此按钮可打开一个窗口，您可以在其中配置代理服务器连接设置。

在**回滚**区域中，可回滚到上一版本的应用程序数据库。如果新版本的应用程序数据库包含错误的特征码，导致 Kaspersky Endpoint Security 阻止安全的应用程序，则您可能需要回滚更新。

回滚更新

单击此按钮可执行应用程序数据库回滚。



单击此按钮可防止不具有管理员权限的用户更改 Kaspersky Endpoint Security 应用程序的设置。



单击此按钮会提示您输入管理员凭证。输入管理员凭证后，应用程序设置将可编辑。

“代理服务器设置”窗口

使用系统代理服务器设置

Kaspersky Endpoint Security 使用 Mac 的系统设置中指定的代理服务器设置。

默认选择此操作。

使用指定的代理服务器设置

Kaspersky Endpoint Security 使用此窗口中指定的代理服务器设置。

地址

用于输入代理服务器的 IP 地址或域名的字段。

如果选择**使用指定的代理服务器设置**选项，则此字段可用。

端口

用于输入更新 Kaspersky Endpoint Security 所使用的代理服务器端口号的字段。

如果选择**使用指定的代理服务器设置**选项，则此字段可用。

默认值为 80。

使用身份验证

身份验证 是指在连接到代理服务器时验证用户名和密码的过程。

此复选框可启用/禁用在连接到代理服务器时进行身份验证。

默认取消选中此复选框。

用户名

用于输入在连接到代理服务器时进行身份验证所需的用户名的字段。

如果选中**使用身份验证**复选框，则此字段可用。

密码

用于输入在连接到代理服务器时进行身份验证所需的密码的字段。

如果选中**使用身份验证**复选框，则此字段可用。

如果未指定用户名和密码或指定的用户名和密码被代理服务器拒绝，则将会打开一个窗口，您必须在其中输入用户名和密码以进行代理服务器身份验证。如果身份验证成功且在请求窗口中选中了**记住密码**复选框，则所指定的用户名和密码将用于未来所有需要进行身份验证的场合。如果未在用户名和密码输入窗口中选中**记住密码**复选框，则在下次连接代理服务器时，将会提示您输入用户名和密码。

对本地地址不使用代理服务器

此复选框可启用/禁用在从本地或网络文件夹更新应用程序时使用代理服务器。

默认情况下已选定该选框。

“需要代理服务器身份验证”对话框

用户名

用于输入连接到代理服务器的用户名的字段。

密码

用于输入密码的字段。

记住密码

此复选框启用/禁用将来在代理服务器上使用指定的用户名和密码进行身份验证。

默认取消选中此复选框。

“界面”选项卡

在**通知**区域中，您可以设置 Kaspersky Endpoint Security 显示的通知，以通知您各类事件。

启用通知

此复选框可启用/禁用有关应用程序事件的通知。

默认情况下已选定该选框。

检测到恶意软件时打开警报音

此复选框可启用/禁用当 Kaspersky Endpoint Security 在检测到恶意对象时发出提示音。

默认情况下已选定该选框。

在**应用程序图标**区域中，可配置在菜单栏中显示应用程序图标。

在菜单栏中显示

此复选框可启用/禁用在菜单栏中显示应用程序图标。

在**报告**区域中，可启用/禁用在 Kaspersky Endpoint Security 报告中记录非关键事件。

记录非关键事件

使用此复选框可启用/禁用在报告中记录信息性事件。通常，这些事件对于计算机安全性而言并不重要。

在**跟踪**区域中，可启用或禁用跟踪。

追踪是一种记录有关应用程序活动详细信息的方式。卡巴斯基技术支持专家使用追踪文件来排查问题。您可以启用应用程序事件记录以创建追踪文件，并在需要时将其发送给技术支持。默认下，应用程序事件记录被禁用。

重要：只有在技术支持专家要求您开启跟踪时才这样做。

启用跟踪

使用此复选框允许/禁止创建追踪文件。

默认取消选中此复选框。

在“**密码保护**”部分，您可以启用密码保护以防止在您的计算机上执行不需要的操作。

启用密码保护

此复选框启用/禁用不需要的操作的密码保护。

默认取消选中此复选框。

选中此复选框将打开一个窗口，您可以在其中设置和配置管理员密码。

设置

单击此按钮将打开一个窗口，您可以在其中编辑管理员密码参数。



单击此按钮可防止不具有管理员权限的用户更改 Kaspersky Endpoint Security 应用程序的设置。



单击此按钮会提示您输入管理员凭证。输入管理员凭证后，应用程序设置将可编辑。

设置管理员密码窗口

密码

用于输入密码的字段，以限制用户设备上不需要的操作。

确认密码

用于再次输入密码以确认密码的字段。

选项

可以被密码保护的操作列表。选中所需的复选框来保护设备上的相应操作。您必须至少选中一个复选框。

取消

单击此按钮将关闭窗口而不保存更改。

确定

单击此按钮保存管理员密码设置并关闭窗口。保存更改后，当您尝试在设备上执行不需要的操作时，系统会提示您输入密码。

“系统事件”报告

窗口的右窗格包含有关 Kaspersky Endpoint Security 操作的报告。

时间

此列显示事件发生的日期和时间。

事件

此列显示事件的状态。

程序名称

此列显示发生事件的程序的名称。

用户

此列显示引发事件的用户的名称。

用户类型

此列显示引发事件的用户的类型。



单击此按钮可打开一个窗口，您可以在此窗口中将报告保存为 .txt 格式的文件。

“已处理的对象”报告

窗口的右侧窗格包含 Kaspersky Endpoint Security 应用程序检测到的所有受感染对象和危险 Web 流量对象的列表。

时间

此列显示检测到对象的时间。

对象

此列显示检测到对象的位置的路径或对象的网址。

状态

此列显示应用程序在检测到对象后执行的操作。

已检测到

此列根据卡巴斯基病毒百科全书中的分类显示已检测到的对象的类型。

名称

此列根据卡巴斯基病毒百科全书中的分类显示已检测到的对象的名称。



单击此按钮可打开一个窗口，您可以在此窗口中将报告保存为 .txt 格式的文件。

“数据库更新”报告

窗口的右侧窗格包含有关应用程序执行的更新任务的报告。

启动时间

此列显示每个更新任务的开始日期和时间。如果展开操作列表，此列还会列出更新应用程序时执行的操作以及执行这些操作的时间。

状态

此列显示更新任务的状态。

大小

此列显示所下载的更新文件的大小。

平均速度

此列显示更新文件的下载速度。

结束时间

此列显示更新任务的完成时间。

单击此按钮可展开更新任务中包含的操作的列表。

单击此按钮可折叠更新任务中包含的操作的列表。



单击此按钮可打开一个窗口，您可以在此窗口中将报告保存为 .txt 格式的文件。

“扫描”报告

窗口的右侧窗格包含有关 Kaspersky Endpoint Security 执行的扫描任务的报告。

任务

此列显示扫描任务的名称。

状态

此列显示扫描任务的状态或已扫描对象的状态。

日期

此列显示扫描任务的日期和时间。

发起者

此列显示发起扫描任务的用户、应用程序或进程。

>

单击此按钮将展开扫描对象列表。

⌄

单击此按钮将折叠扫描对象列表。



单击此按钮可打开一个窗口，您可以在此窗口中将报告保存为 .txt 格式的文件。

“文件威胁防护”报告

窗口的右窗格包含有关文件威胁防护操作的报告。

日期

此列显示应用程序访问已扫描对象的日期和时间。

路径

此列显示已扫描对象的原始位置的路径。

状态

此列显示扫描对象的状态。

程序名称

此列显示访问已扫描对象的应用程序。



单击此按钮可打开一个窗口，您可以在此窗口中将报告保存为 .txt 格式的文件。

“Web 威胁防护”报告

窗口的右窗格包含有关 Web 威胁防护操作的报告。

日期

此列显示检测到 Web 流量对象的日期和时间。

网址

此列显示 Web 威胁防护检测到的 Web 流量对象。对于检测到的每个 Web 流量对象，此列指定检测到此类对象的网址。

状态

此列显示检测到的 Web 流量对象的状态。

程序名称

此列显示访问检测到的 Web 流量对象的程序。



单击此按钮可打开一个窗口，您可以在此窗口中将报告保存为 .txt 格式的文件。

“邮件威胁防护”报告

窗口的右窗格包含有关邮件威胁防护操作的报告。

日期

此列显示在电子邮件中检测到受感染对象的日期和时间。

路径

此列显示有关检测到受感染对象的电子邮件的信息。

状态

此列显示在检测到受感染对象后 Kaspersky Endpoint Security 执行的操作。

程序名称

此列显示电子邮件客户端名称。



单击此按钮可打开一个窗口，您可以在此窗口中将报告保存为 .txt 格式的文件。

“网络威胁防护”报告

窗口的右窗格包含有关网络威胁防护操作的报告。

日期

此列显示在计算机上检测到危险网络活动的日期和时间。

IP 地址

此列显示 Kaspersky Endpoint Security 从中检测到危险网络活动的计算机的 IP 地址。

状态

此列显示在检测到危险网络活动后 Kaspersky Endpoint Security 执行的操作。

攻击类型

此列显示检测到的网络攻击类型。

本地端口

此列显示尝试通过其入侵的本地端口号。

协议

此列显示用于执行攻击的协议类型。



单击此按钮可打开一个窗口，您可以在此窗口中将报告保存为 .txt 格式的文件。

Endpoint Detection and Response 报告

窗口的右侧窗格包含有关 Endpoint Detection and Response 组件操作的报告。

日期

此列显示事件发生的日期和时间。

事件

此列显示事件的状态。



单击此按钮可打开一个窗口，您可以在此窗口中将报告保存为 .txt 格式的文件。

防火墙报告

窗口的右窗格包含有关防火墙操作的报告。

日期

此列显示事件发生的日期和时间。

事件

此列显示事件的状态。



单击此按钮可打开一个窗口，您可以在此窗口中将报告保存为 .txt 格式的文件。

“漏洞利用防御”报告

窗口的右窗格包含有关漏洞利用防御操作的报告。

日期

此列显示事件发生的日期和时间。

事件

此列显示事件的状态。



单击此按钮可打开一个窗口，您可以在此窗口中将报告保存为 .txt 格式的文件。

“设备控制”报告

窗口的右窗格包含有关设备控制操作的报告。

日期

此列显示事件发生的日期和时间。

事件

此列显示事件的状态。



单击此按钮可打开一个窗口，您可以在此窗口中将报告保存为 .txt 格式的文件。

“系统监控”报告

窗口的右侧窗格包含有关“系统监控”组件操作的报告。

日期

此列显示事件发生的日期和时间。

事件

此列显示事件的状态。



单击此按钮可打开一个窗口，您可以在此窗口中将报告保存为 .txt 格式的文件。

“安装类型”窗口

在**要安装的包**区域中，您可以选择要在客户端计算机上安装的应用程序组件。

扫描

此复选框将扫描组件添加到 Kaspersky Endpoint Security 安装包。

默认情况下，该复选框处于选中状态，无法清除。

文件威胁防护

此复选框启用/禁用将文件威胁防护组件添加到 Kaspersky Endpoint Security 安装包。

如果选中此复选框，则文件威胁防护组件将包含在 Kaspersky Endpoint Security 安装包中。

如果清除此复选框，则文件威胁防护组件不包括在 Kaspersky Endpoint Security 安装包中。

默认情况下已选定该选框。

Web 威胁防护

此复选框启用/禁用将 Web 威胁防护组件添加到 Kaspersky Endpoint Security 安装包。

如果选中此复选框，则 Web 威胁防护组件将包含在 Kaspersky Endpoint Security 安装包中。

如果清除此复选框，则 Web 威胁防护组件将不包含在 Kaspersky Endpoint Security 安装包中。

默认情况下已选定该选框。

网络威胁防护

此复选框启用/禁用将网络威胁防护组件添加到 Kaspersky Endpoint Security 安装包。

如果选中此复选框，则网络威胁防护组件将包含在 Kaspersky Endpoint Security 安装包中。

如果清除此复选框，则网络威胁防护组件不包括在 Kaspersky Endpoint Security 安装包中。

默认情况下已选定该选框。

网络代理连接器

此复选框将网络代理连接器组件添加到 Kaspersky Endpoint Security 安装包。

默认情况下，该复选框处于选中状态，无法清除。

“密码保护设置”窗口

密码

用于输入密码的字段，以限制用户设备上不需要的操作。
单击**“显示”**可查看输入的符号。

确认密码

用于再次输入密码以确认密码的字段。
单击**“显示”**可查看输入的符号。

需要密码以

可以被密码保护的操作列表。选中所需的复选框来保护用户设备上的相应操作。

“授予访问权限”对话框

获取恢复密钥

单击此按钮可生成在客户端计算机上访问加密磁盘所需的恢复密钥。

“高级威胁防护”区域

在 KSN **设置**区域中，可配置使用卡巴斯基安全网络。

卡巴斯基安全网络

卡巴斯基安全网络切换开关可启用/禁用加入卡巴斯基安全网络。

如果开启**卡巴斯基安全网络**切换开关，则应用该策略的客户端计算机将加入卡巴斯基安全网络。

如果关闭**卡巴斯基安全网络**切换开关，则应用该策略的客户端计算机将不加入卡巴斯基安全网络。

默认关闭此切换开关。

扩展 KSN 模式

扩展 KSN 模式切换开关可启用/禁用从远程计算机向卡巴斯基发送附加数据。这些数据用于提高客户端计算机的保护性能和 Kaspersky Endpoint Security 的易用性。

如果开启**扩展 KSN 模式**，则该策略下的客户端计算机将向卡巴斯基安全网络提供检测服务运行所需的数据和附加数据。

如果关闭**扩展 KSN 模式**，则该策略下的客户端计算机将仅提供检测服务运行所需的数据。不会向卡巴斯基安全网络提供任何额外数据。

默认关闭**扩展 KSN 模式**切换开关。

如果开启**卡巴斯基安全网络**切换开关，将会自动开启该切换开关，但您可以关闭该切换开关。

在全球 KSN 基础设施中使用卡巴斯基安全网络时向卡巴斯基提供的数据

如果启用**卡巴斯基安全网络**切换开关并禁用**扩展 KSN 模式**切换开关，则客户端计算机上运行的 Kaspersky Endpoint Security 将向卡巴斯基提供以下数据：

- 有关使用的授权许可的信息： 授权许可的类型和有效期、授权许可到期前的天数、向其购买授权许可的合作伙伴的标识符、区域激活中心标识符、激活码的校验码、使用 SHA1 算法计算出的票证正文哈希值、授权许可票证的创建日期和时间、授权许可信息标识符、授权许可票证标识符、授权许可票证序列标识符、用户计算机的唯一标识符、授权许可票证的有效期开始日期、授权许可票证的有效期截止日期、授权许可票证当前状态、票证标头版本、授权许可版本、票证标头签名证书标识符、密钥文件的校验码、票证标头签名者序列号、身份验证令牌。

- 已安装软件的完整版本；
  已安装软件的类型；
  软件更新 ID； 信誉服务 ID； 协议类型 ID； 区域激活中心 ID； 已撤销的软件服务决定列表的版本； 软件反病毒数据库中触发记录的 ID； 软件反病毒数据库中触发记录的时间戳； 触发的软件反病毒数据库记录的类型； 计算机上的应用程序安装实例的独一 ID； 授权许可激活日期； 授权许可到期日期； 授权许可 ID； 软件使用的授权许可的状态； 正在处理的对象的校验和类型； 检测到的可用于破坏用户设备或数据的恶意软件或合法软件的名称； 正在处理的对象的校验和； 软件激活码校验和； 软件的完整版本； 独一设备 ID； 软件 ID； 软件密钥文件的校验和； 用于提供软件授权许可的信息模型的 ID； 用于签署软件授权许可 ticket 标头的证书的标识符； 软件授权许可 ticket 创建日期和时间； 软件授权许可 ticket 校验和； 软件授权许可 ticket 版本； 软件激活码版本； 向权利持有人基础结构的请求的数据格式； 当前授权许可 ticket ID； 软件组件 ID； 软件操作的结果； 错误代码； Web 服务的访问地址 (URL、IP)； 端口号； Web 服务请求源的 Web 地址 (Referrer)； 证书的公钥； 所扫描对象和哈希算法的数字证书指纹。

如果启用**卡巴斯基安全网络**和**扩展 KSN 模式**切换开关，则客户端计算机上运行的 Kaspersky Endpoint Security 将向卡巴斯基提供以下数据：

- 相关信息，包括已安装在计算机上的操作系统 (OS) 和服务包的版本、操作系统内核文件的版本与校验码（MD5、SHA2-256、SHA1）、操作系统运行模式的参数； 操作系统版本、操作系统内部版本号、操作系统更新编号、操作系统版本、有关操作系统版本的扩展信息； 操作系统 Service Pack 版本； 操作系统的启动日期和时间； 行为分析子系统中有关操作系统操作的事件的处理延迟时间； 当前类型的延迟操作系统操作事件的数量； 主动防御子系统中有关操作系统操作的事件的处理延迟时间； 已处理的操作系统操作事件的数量； 已处理的同步操作系统操作事件的数量； 当前类型的所有操作系统操作事件的总延迟； 持久事件存储子系统中有关操作系统操作的事件的处理延迟时间； 所有操作系统操作事件的总延迟； 等待同步操作系统操作事件的数量； 接收到的操作系统操作事件的日期和时间。

- 有关上次操作系统重启失败的信息： 重启失败次数。

- 有关权利持有人安装的应用程序和反病毒保护状态的信息： 软件安装 ID (PCID)； 软件数据库记录版本； 计算机上安装的应用程序实例的唯一标识符、应用程序类型、应用程序类型的 ID、已安装应用程序的完整版本、应用程序设置版本的标识符、计算机类型的标识符、安装应用程序的计算机的唯一标识符、权利持有人服务中的唯一用户标识符、区域设置语言和运行状态、已安装的软件组件的版本及其运行状态、连接权利持有人服务所使用的协议版本； 已安装软件的完整版本； 已安装软件的类型； 软件更新 ID； 信誉服务 ID； 协议类型 ID； 区域激活中心 ID； 已撤销的软件服务决定列表的版本； 软件反病毒数据库中触发记录的 ID； 软件反病毒数据库中触发记录的时间戳； 触发的软件反病毒数据库记录的类型； 计算机上的应用程序安装实例的独一 ID； 授权许可激活日期； 授权许可到期日期； 授权许可 ID； 软件使用的授权许可的状态； 正在处理的对象的校验和类型； 检测到的可用于破坏用户设备或数据的恶意软件或合法软件的名称； 正在处理的对象的校验和； 软件激活码校验和； 软件的完整版本； 软件 ID； 软件密钥文件的校验和； 用于提供软件授权许可的信息模型的 ID； 用于签署软件授权许可 ticket 标头的证书的标识符； 软件授权许可 ticket 创建日期和时间； 软件授权许可 ticket 校验和； 软件授权许可 ticket 版本； 软件激活码版本； 向权利持有人基础结构的请求的数据格式； 当前授权许可 ticket ID； 软件组件 ID； 软件操作的结果； 错误代码； Web 服务的访问地址 (URL、IP)； 端口号； Web 服务请求源的 Web 地址 (Referrer)； 反病毒数据库的更新应用周期数； 反病毒数据上次更新和应用的日期和时间； 软件数据库的发布日期和时间； 软件组件的版本； 软件更新 ID； 已安装软件的类型； 系统监控的启动日期和时间； 软件的安装日期和时间； 系统监控发送统计数据的概率； 系统监控进行处理所花费的时间长于标准时间的事件的代码； 系统监控进行处理所花费的时间长于标准时间的事件的数据库处理时间； 系统监控处理一个事件的最长允许时间； 系统监控进行处理所花费的时间长于标准时间的事件的处理时间； 系统监控进行处理所花费的时间长于标准时间的事件的总数。

- 有关所有已处理对象和操作的信息： 软件对正在处理的对象的裁定； 目录代码； 所处理对象的大小； 所处理对象的校验和 (SHA256)； 系统监控上下文中所检测软件的编号； 系统监控检测软件的日期和时间； 删除特征； 软件反病毒数据库中触发记录的 ID； 系统监控检测软件的原因； 所处理对象的校验和 (MD5)； 模块完整性检查的结果； 所处理对象的名称； 触发的软件反病毒数据库记录的类型； 所处理对象的路径； 已扫描对象的名称； 扫面的日期和时间； 下载它的 URL 和 Referrer 地址； 已扫描文件的大小及其路径； 存档标志； 文件创建的日期和时间； 打包程序的名称、大小和校验和（MD5、SHA2-256）（如果文件被打包）； 文件的熵； 文件的类型； 文件类型代码； 可执行文件的标志、ID 和格式； 对象的校验和（MD5、SHA2-256）； 对象的补充校验和的类型和值； 有关对象的数字签名（证书）的数据： 证书发布者的数据、上次统计交付后对象的启动次数、应用程序的扫描任务 ID、接收对象信誉信息的方式、目标过滤器的值、适用检测技术的技术参数； 所处理对象的路径； 目录代码。

- 对于可执行文件： 文件部分的熵、信誉验证标记或文件签名标记、名称、类型、ID 类型、校验码 (MD5)，以及正在接受验证的对象加载的应用程序的大小、应用程序路径和模板路径、表明在自动运行列表中存在的属性、输入日期、属性列表、打包程序名称、应用程序数字签名的相关信息： 发行商证书、以 MIME 格式上传的文件的名称、文件构建日期和时间。

- 有关已启动的应用程序及其模块的信息： 运行文件的校验码（MD5、SHA2-256）、大小、属性、创建日期、打包程序的名称（如果文件被打包）、文件的名称、系统上运行的进程的信息（进程 ID (PID)）、进程名称、启动进程的账户信息、启动进程的应用程序和命令、进程文件的完整路径、启动命令行、进程所属应用程序的描述（应用程序的名称和开发商信息，以及使用的数字证书和用于验证其真实性的信息或缺乏文件数字签名的信息），和进程中加载的模块信息： 它们的名称、大小、类型、创建日期、属性、校验码（MD5、SHA2-256、SHA1）、路径、PE 文件头信息、打包程序名称（如果文件被打包）、这些统计数据的可用性和有效性的相关信息、生成被发送的统计数据的模式的标识符。

- 如果检测到威胁或漏洞，除了提供检测到的对象的相关信息外，还应提供该记录在反病毒数据库中的标识符、版本和类型，该威胁在卡巴斯基分类中的名称，上一次更新反病毒数据库的日期和时间，可执行文件名称，向检测到威胁的网址发出请求的应用程序文件的校验码 (MD5)，检测到的威胁的 IP 地址（IPv4 或 IPv6），漏洞标识符及其威胁等级，检测到漏洞的网页的网址和 Referrer。

- 如果检测到潜在的恶意对象，则提供有关进程内存中的数据的信息。

- 网络攻击信息： 攻击计算机的 IP 地址和用户计算机上成为网络攻击目标的端口号，攻击协议的 ID，攻击的名称和类型。

- 关于网络连接的信息： 来自使打开端口的进程启动的文件的版本和校验和 (MD5、SHA2-256、SHA1)，进程文件的路径及其数字签名，本地和远程 IP 地址，本地和远程连接端口的数量，连接的状态，端口开放的时间戳。

- 检测到有害或可疑内容的网页的网址和 IP 地址，向该网址发出请求的文件名称、大小及校验码、实现裁定结果所用规则的标识符、权重和程度、攻击的目标。

- 有关已安装应用程序和反病毒数据库更新的信息： 更新任务的完成状态、更新过程中可能发生的错误的类型、未成功更新的数量、执行更新的应用程序组件的标识符。

- 有关使用卡巴斯基安全网络 (KSN) 的信息： KSN 标识符、应用程序标识符、应用程序完整版本、用户设备的匿名 IP 地址、KSN 请求履行质量指标、KSN 数据包处理质量指标、KSN 请求数量指标和 KSN 请求类型信息、统计数据开始发送的日期和时间、统计数据完成发送的日期和时间、KSN 配置更新的相关信息： 活动配置的标识符、接收的配置标识符、配置更新的错误代码。

- 有关系统日志事件的信息： 事件时间、检测到事件的日志的名称、事件的类型和类别、事件源的名称和事件描述。

- 用于确定文件和 URL 地址信誉的信息： 请求信誉的 URL 地址和 Referrer、连接的协议类型、应用程序类型的内部标识符、正在使用的端口号、用户标识符、扫描文件的校验码 (MD5)、检测到的威胁类型、用于检测威胁的记录的信息（反病毒数据库的记录标识符、记录时间戳和类型）； 证书的公钥； 所扫描对象和哈希算法的数字证书指纹。

- 应用程序地域分布数据： 应用程序安装和激活日期、为应用程序激活提供授权许可的合作伙伴 ID、应用程序 ID、应用程序语言本地化 ID、应用程序激活的授权许可序列号、KSN 参与标志。

- 有关使用的授权许可的信息： 授权许可的类型和有效期、授权许可到期前的天数、向其购买授权许可的合作伙伴的标识符、区域激活中心标识符、激活码的校验码、使用 SHA1 算法计算出的票证正文哈希值、授权许可票证的创建日期和时间、授权许可信息标识符、授权许可票证标识符、授权许可票证序列标识符、用户计算机的唯一标识符、授权许可票证的有效期开始日期、授权许可票证的有效期截止日期、授权许可票证当前状态、票证标头版本、授权许可版本、票证标头签名证书标识符、密钥文件的校验码、票证标头签名者序列号、身份验证令牌。

- 有关计算机上已安装硬件的信息： 类型、名称、型号名称、固件版本、内置设备和连接设备的参数。

- 设备信息： 设备 ID。

- 有关 Web 控制组件的操作的信息：
  组件版本、分类原因、有关分类原因的其他信息、分类的 URL、被锁定或分类的对象的主机 IP 地址。

云模式

云模式开关启用或禁用 Kaspersky Endpoint Security 使用轻量版本反恶意软件数据库的应用程序操作模式。此模式仅在启用卡巴斯基安全网络的参与时可用。轻量版本的反恶意软件数据库所占用的计算机内存大概是通常数据库的一半。如果您不参与卡巴斯基安全网络或禁用云模式，Kaspersky Endpoint Security 将从卡巴斯基服务器下载完整版本的反恶意软件数据库。

如果打开了切换按钮，Kaspersky Endpoint Security 将使用轻量版本的反恶意软件数据库，这将减少操作系统资源的负载。

注意：选中该复选框后，Kaspersky Endpoint Security 在下次更新期间下载轻量版本的反恶意软件数据库。

如果切换按钮关闭，Kaspersky Endpoint Security 将使用完整版本的反恶意软件数据库。

注意：清空该复选框后，Kaspersky Endpoint Security 在下次更新期间下载完整版本的反恶意软件数据库。

KSN 声明

单击此链接可打开一个窗口，您可以在其中阅读卡巴斯基安全网络声明的文本并接受加入卡巴斯基安全网络的条款。

注意：如果通过 Kaspersky Security Center Web Console 管理 Kaspersky Endpoint Security，则您可以加入卡巴斯基私人安全网络，而不是加入卡巴斯基安全网络，具体取决于 Kaspersky Security Center 设置。如果通过 Kaspersky Security Center 云控制台管理 Kaspersky Endpoint Security，则加入卡巴斯基私人安全网络将不可用。有关加入卡巴斯基私人安全网络的详细信息，请参阅 Kaspersky Security Center 帮助。

在 **KSN 代理设置**区域中，您可以配置 KSN 代理设置。

使用 KSN 代理

此复选框启用/禁用在连接到卡巴斯基安全网络时使用代理服务器。

如果选中该复选框，Kaspersky Endpoint Security 将使用代理服务器连接到卡巴斯基安全网络。

如果清除该复选框，Kaspersky Endpoint Security 将直接连接到卡巴斯基安全网络。

默认清除此复选框。

当 KSN 代理不可用时使用卡巴斯基服务器

如果 KSN 代理不可用，此复选框启用/禁用卡巴斯基服务器的使用。

如果选中此复选框，当 KSN 代理不可用时，Kaspersky Endpoint Security 将使用卡巴斯基服务器。

如果清除此复选框，当 KSN 代理不可用时，Kaspersky Endpoint Security 不使用卡巴斯基服务器。

默认清除此复选框。

如果选中**使用 KSN 代理**复选框，则此复选框可用。

强制

开启**强制**切换开关后，Kaspersky Endpoint Security 将禁止在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

关闭**强制**切换开关后，Kaspersky Endpoint Security 将允许在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

“加入卡巴斯基安全网络/卡巴斯基私有安全网络”窗口

了解更多

单击此链接可打开一个新的浏览器窗口，您可以在其中阅读卡巴斯基安全网络声明或卡巴斯基私人安全网络声明的文本。

我接受加入卡巴斯基安全网络/卡巴斯基私人安全网络的条款

应用策略的计算机将加入卡巴斯基安全网络/卡巴斯基私人安全网络。

我不接受加入卡巴斯基安全网络/卡巴斯基私人安全网络的条款

应用策略的计算机将不会加入卡巴斯基安全网络/卡巴斯基私人安全网络。

注意：如果通过 Kaspersky Security Center 云控制台管理 Kaspersky Endpoint Security，则加入卡巴斯基私人安全网络将不可用。有关加入卡巴斯基私人安全网络的详细信息，请参阅 Kaspersky Security Center 帮助。

基本威胁防护区域

文件威胁防护

单击此链接可打开一个窗口，您可以在其中设置文件威胁防护设置。

Web 威胁防护

单击此链接可打开一个窗口，您可以在其中设置 Web 威胁防护设置。

网络威胁防护

单击此链接可打开一个窗口，您可以在其中设置网络威胁防护设置。

邮件威胁防护

单击此链接可打开一个窗口，您可以在其中设置邮件威胁防护设置。

防火墙

单击此链接可打开一个窗口，您可以在其中设置防火墙设置。

“文件威胁防护”窗口

文件威胁防护

文件威胁防护切换开关可启用/禁用文件威胁防护。

如果开启**文件威胁防护**切换开关，则 Kaspersky Endpoint Security 将对应用该策略的客户端计算机的文件系统执行实时监控。

如果关闭**文件威胁防护**切换开关，则 Kaspersky Endpoint Security 将不会对应用该策略的客户端计算机的文件系统进行保护。

默认开启此切换开关。

在**保护范围**区域中，通过选择预设项之一或添加所选择的文件或文件夹，可设置保护范围。

添加

单击此按钮将打开一个对话框，您可以在其中指定要添加到保护范围中包含的对象列表的文件、文件夹或掩码。

删除

单击此按钮将从保护范围中删除对象。

如果在受保护对象列表中选择了对象，则此按钮可用。

您无法删除保护范围中包含的默认对象。

保护范围

此列包含在启用文件威胁防护后 Kaspersky Endpoint Security 将扫描的对象。

默认情况下，Kaspersky Endpoint Security 扫描以下对象：

- **所有可移动磁盘**。Kaspersky Endpoint Security 将扫描所有可移动驱动器。
- **所有内部磁盘**。Kaspersky Endpoint Security 将扫描所有内部驱动器。
- **所有网络磁盘**。Kaspersky Endpoint Security 将扫描所有网络驱动器。

状态

如果开启此列中的切换开关，在启用文件威胁防护后，Kaspersky Endpoint Security 将扫描**保护范围**列中的相应对象。

如果关闭此列中的切换开关，在启用文件威胁防护后，Kaspersky Endpoint Security 将不会扫描**保护范围**列中的相应对象。

附加

此列指示 Kaspersky Endpoint Security 是否扫描相应对象的子文件夹。

在**若检测到恶意对象**区域中，您可以选择 Kaspersky Endpoint Security 在检测到恶意对象时要执行的操作。

提示操作

Kaspersky Endpoint Security 显示一个通知窗口，其中包含有关已感染该文件的恶意对象的信息，并提示您选择 Kaspersky Endpoint Security 要执行的操作。可用的操作可能因对象的状态而异。

默认选择此选项。

清除，无法清除则删除

Kaspersky Endpoint Security 阻止对受感染文件的访问，并尝试在未请求用户确认的情况下对其进行清除。

清除成功，Kaspersky Endpoint Security 将文件保存在原始文件名下的原始位置。如果清除失败，Kaspersky Endpoint Security 将删除受感染文件。

清除，无法清除则阻止

Kaspersky Endpoint Security 阻止对受感染文件的访问，并尝试在未请求用户确认的情况下对其进行清除。

清除成功，Kaspersky Endpoint Security 将文件保存在原始文件名下的原始位置。如果清除失败，Kaspersky Endpoint Security 会将受感染的文件保持在其原始位置的阻止状态。

在**优化**区域中，您可以配置扫描性能并选择扫描算法。

仅扫描新建和已修改的文件

此复选框启用/禁用仅扫描自上次扫描以来 Kaspersky Endpoint Security 识别为新建或已更改的文件。

如果选中此复选框，则 Kaspersky Endpoint Security 仅扫描自上次扫描以来识别为新建或已更改的文件。

如果清除此复选框，则 Kaspersky Endpoint Security 将扫描所有文件。

默认情况下已选定该选框。

跳过扫描只读系统卷

此复选框禁用/启用由 Kaspersky Endpoint Security 扫描只读系统卷。

如果选择此复选框，则 Kaspersky Endpoint Security 将不扫描只读系统卷。这大大缩短了扫描时间。

如果清除此复选框，则 Kaspersky Endpoint Security 将扫描只读系统卷。

默认情况下已选定该选框。

使用 iSwift

此复选框启用/禁用扫描期间使用 iSwift 技术。iSwift 允许 Kaspersky Endpoint Security 使用一种特殊的算法从扫描中排除某些对象，这有助于提高扫描速度。

如果选中此复选框，则 Kaspersky Endpoint Security 在扫描期间使用 iSwift。

如果清除此复选框，则 Kaspersky Endpoint Security 在扫描期间不使用 iSwift。

默认情况下已选定该选框。

在**文件类型**区域中，您可以选择在启用文件威胁防护后 Kaspersky Endpoint Security 将扫描哪些文件。

扫描所有文件

Kaspersky Endpoint Security 扫描所有执行、打开或保存的文件系统对象。

按内容扫描应用程序和文档

Kaspersky Endpoint Security 只扫描基于内容可能被感染的对象。

按扩展名扫描应用程序和文档

Kaspersky Endpoint Security 只扫描基于文件扩展名可能被感染的对象。

扩展列表由卡巴斯基定义，并包含在 Kaspersky Endpoint Security 数据库中。

Kaspersky Endpoint Security 总是扫描没有扩展名的文件。

在**复合文件**区域中，您可以选择在启用文件威胁防护后 Kaspersky Endpoint Security 将扫描的复合文件类型。

扫描压缩包

此复选框启用/禁用扫描压缩包。有关扩展名的列表，请参阅 Kaspersky Endpoint Security 帮助。

如果选中此复选框，则 Kaspersky Endpoint Security 将扫描压缩包。

如果清除此复选框，则 Kaspersky Endpoint Security 在扫描过程中将跳过压缩包。

扫描安装包

该选框用于启用或禁用对安装包的扫描。

如果选中此复选框，则 Kaspersky Endpoint Security 将扫描安装包。

如果清除该复选框，则 Kaspersky Endpoint Security 将在扫描时跳过安装包。

扫描嵌入的 OLE 对象

此复选框启用/禁用对文件中嵌入的对象（如 Excel 电子表格、宏或电子邮件附件）的扫描。

如果选中此复选框，则 Kaspersky Endpoint Security 将扫描嵌入的 OLE 对象。

如果清除此复选框，则 Kaspersky Endpoint Security 在扫描过程中将跳过嵌入的 OLE 对象。

不解压大于此值的压缩包 <值> MB

此复选框启用/禁用对要扫描的压缩包大小的限制。

如果选中此复选框，则 Kaspersky Endpoint Security 将在扫描期间跳过大于指定值的压缩包。

如果清除此复选框，则 Kaspersky Endpoint Security 将提取并扫描压缩包，而不考虑其大小。

如果选中**扫描压缩包**复选框，则此复选框可用。

推迟大于此值的压缩包的解压 <值> MB

限制要扫描的压缩包大小的选项。

如果选中此复选框，则 Kaspersky Endpoint Security 将扫描大小超过设置限制的所有压缩包，但在检测到此类压缩包两分钟后以较低的优先级进行扫描。

如果清除此复选框，则 Kaspersky Endpoint Security 将以同等优先级扫描所有压缩包。

如果选中**扫描压缩包**复选框，则此复选框可用。

强制

开启**强制**切换开关后，Kaspersky Endpoint Security 将禁止在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

关闭**强制**切换开关后，Kaspersky Endpoint Security 将允许在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

“添加保护范围”对话框

输入文件名、文件夹名或掩码输入字段

文件、文件夹或文件/文件夹掩码的路径。

对象是个文件夹

此复选框启用/禁用对象作为文件夹的扫描。

如果选中此复选框，则 Kaspersky Endpoint Security 会将您在**输入文件名称、文件夹名称或掩码**字段中指定的对象作为文件夹进行扫描。

如果清除此复选框，则 Kaspersky Endpoint Security 会将您在**输入文件名称、文件夹名称或掩码**字段中指定的对象作为文件进行扫描。

默认情况下已选定该选框。

包含子文件夹

此复选框可启用/禁用扫描在**输入文件名称、文件夹名称或掩码**字段中指定的文件夹中的子文件夹。

如果选中此复选框，则 Kaspersky Endpoint Security 在恶意软件扫描过程中将扫描子文件夹。

如果清除此复选框，则 Kaspersky Endpoint Security 在恶意软件扫描过程中将仅扫描直接位于在**输入文件名称、文件夹名称或掩码**字段中指定的文件夹中的文件。

默认情况下已选定该选框。

“Web 威胁防护”窗口

Web 威胁防护

Web 威胁防护切换开关可启用/禁用 Web 威胁防护。

如果开启 **Web 威胁防护**切换开关，则 Web 威胁防护将扫描您的计算机使用 Safari、Google Chrome 或 Firefox 通过 HTTP 和 HTTPS 协议发送和接收的数据扫描。

如果关闭 **Web 威胁防护**切换开关，则 Web 威胁防护将不会扫描您的计算机通过网页浏览器发送和接收的数据。

默认开启此切换开关。

在**若检测到恶意对象**区域中，您可以选择 Kaspersky Endpoint Security 在检测到恶意对象时要执行的操作。

提示操作

Kaspersky Endpoint Security 显示一个通知窗口，其中包含有关已感染 Web 流量对象的恶意软件类型的信息，并提示您选择 Kaspersky Endpoint Security 对此对象采取的操作。可用的操作可能因对象的状态而异。

默认选择此操作。

自动阻止

Kaspersky Endpoint Security 自动阻止访问危险的 Web 流量对象。

在**受信任网址**区域中，您可以创建或编辑受信任网址列表，并启用或禁用扫描来自此列表中的网址的流量。

不扫描来自受信任网址的 Web 流量

此复选框启用/禁用从受信任的网址扫描 Web 流量。

如果选中此复选框，则 Kaspersky Endpoint Security 不会从受信任的网址扫描 Web 流量。

如果清除此复选框，则 Kaspersky Endpoint Security 将从受信任的网址扫描 Web 流量。

默认清除此复选框。

网址列表

此列表包含受信任的网址。

您可以清除列表上的网址旁边的复选框。如果清除此复选框，Web 威胁防护将从网址扫描 Web 流量。

如果选中**不扫描来自受信任网址的 Web 流量**复选框，则此列表可用。

添加

单击此按钮可打开一个对话框，您可以在其中输入要添加到受信任网址列表中的网址或网址掩码。

删除

单击此按钮可从列表中删除选定的网址或网址掩码。

当在受信任的网址列表中选择网址或网址掩码时，此按钮可用。

网址

此列包含受信任网址。

状态

如果开启此列中的切换开关，在启用 Web 威胁防护且选中**不扫描来自受信任网址的 Web 流量**复选框后，Kaspersky Endpoint Security 将不扫描**网址**列中的相应对象。

如果关闭此列中的切换开关，在启用 Web 威胁防护且选中**不扫描来自受信任网址的 Web 流量**复选框后，Kaspersky Endpoint Security 将扫描**网址**列中的相应对象。

强制

开启**强制**切换开关后，Kaspersky Endpoint Security 将禁止在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

关闭**强制**切换开关后，Kaspersky Endpoint Security 将允许在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

“添加网址”对话框

网址输入字段

Web 威胁防护将不对其流量进行扫描的网址或网址掩码。

在**状态**区域中，您可以定义 Kaspersky Endpoint Security 是否扫描来自此网址或网址组的流量。

禁用

网址或网址掩码已添加到**受信任网址**列表中，但 Kaspersky Endpoint Security 将扫描其流量。

启用

网址或网址掩码已添加到**受信任网址**列表中，且 Kaspersky Endpoint Security 不扫描其流量。

“网络威胁防护”窗口

反网络攻击

网络威胁防护切换开关可启用/禁用网络威胁防护。

如果开启**网络威胁防护**切换开关，则 Kaspersky Endpoint Security 将保护远程计算机免受网络攻击。

如果关闭**网络威胁防护**切换开关，则 Kaspersky Endpoint Security 将无法为远程计算机提供网络攻击防护。

默认开启此切换开关。

在**网络威胁防护设置**区域中，您可以修改 Kaspersky Endpoint Security 阻止攻击计算机的期限。

阻止攻击计算机的时间 <值> 分钟

此复选框启用/禁用在指定时间段内将攻击计算机添加到被阻止计算机的列表中。

如果选中此复选框，则 Kaspersky Endpoint Security 会将攻击计算机添加到指定时间段内被阻止计算机的列表中。

如果清除此复选框，则 Kaspersky Endpoint Security 不会阻止攻击计算机。

默认情况下已选定该选框。

默认情况下，攻击计算机被阻止 60 分钟。

在**排除项**区域中，您可以创建或编辑 Kaspersky Endpoint Security 永远不会阻止其网络活动的远程计算机的 IP 地址列表。

IP 地址列表

此列表包含其网络活动从未被 Kaspersky Endpoint Security 阻止的远程计算机的 IP 地址。

添加

单击此按钮可打开一个对话框，您可以在其中输入远程计算机的 IP 地址。

删除

单击此按钮可从列表中删除选定的 IP 地址。

如果在IP地址列表中选择了远程计算机的 IP 地址，则此按钮可用。

强制

开启**强制**切换开关后，Kaspersky Endpoint Security 将禁止在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

关闭**强制**切换开关后，Kaspersky Endpoint Security 将允许在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

“添加排除项”对话框

IP 地址输入字段

远程计算机的 IP 地址。

“安全控制”区域

Web 控制

Web 控制切换开关可启用/禁用 Web 控制。

如果开启 **Web 控制**切换开关，则您可以创建规则，以管理用户在远程计算机上访问的网站。

如果关闭 **Web 控制**切换开关，则您将无法管理用户在远程计算机上访问的网站。

默认关闭此切换开关。

规则列表

此列表包含您为管理用户在远程计算机上访问的网站而创建的规则。

规则的排序顺序决定了 Kaspersky Endpoint Security 管理的应用程序的优先级。

添加

单击此按钮可打开一个窗口，您可以在其中创建新的 Web 控制规则。

删除

单击此按钮可从规则列表中删除所选规则。

如果选中规则旁边的复选框，则此按钮可用。

向上

单击此按钮将所选规则在规则列表中上移，并通过 Kaspersky Endpoint Security 提高其应用程序的优先级。

向下

单击此按钮将所选规则在规则列表中下移，并通过 Kaspersky Endpoint Security 降低其应用程序的优先级。

名称

规则名称。

状态

此列中的切换开关可定义规则是否处于活动状态。
您可以开启/关闭相应规则旁边的切换开关，以更改该规则的状态。

操作

当用户访问受规则影响的特定网址、网址组或网站类别时，Kaspersky Endpoint Security 要执行的操作。
通过在此列的相应快捷菜单中选择其他选项，可更改已分配的操作。

强制

开启**强制**切换开关后，Kaspersky Endpoint Security 将禁止在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。
关闭**强制**切换开关后，Kaspersky Endpoint Security 将允许在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

“编辑规则”窗口

规则名称输入字段

规则名称。

在**状态**区域中，可以将规则设置为活动或不活动状态。

活动

如果选择此选项，则将创建活动规则。强制执行策略后，它将立即应用于远程计算机。

不活动

如果选择此选项，则将创建不活动规则。当策略强制执行时，它将处于挂起状态。

在**操作**区域中，您可以选择当用户访问受规则影响的特定网址、网址组或网站类别时，Kaspersky Endpoint Security 要执行的操作。

允许

如果选择此选项，Kaspersky Endpoint Security 允许用户访问受规则影响的网址、网址组或网站类别。

注意：如果在新策略向导的**网络**窗口中开启**安全连接 (HTTPS) 检查**切换开关，Kaspersky Endpoint Security 将允许在远程计算机上访问网络资源。

默认选择此选项。

阻止

如果选中此选项，Kaspersky Endpoint Security 将阻止用户访问受规则影响的网址、网址组或网站类别。

注意：如果在新策略向导的**网络**窗口中开启**安全连接 (HTTPS) 检查**切换开关，当用户访问远程计算机上被 Web 控制阻止的网络资源时，Kaspersky Endpoint Security 将会显示通知。

显示警告

如果选择此选项，当用户尝试访问受规则影响的网址、网址组或网站类别时，Kaspersky Endpoint Security 将会显示警告。

在**规则区域**区域中，您可以选择为特定网址、网址组或网站类别创建规则。

类别

如果选择此选项，则为网站类别创建规则。

选择类别

单击此链接可打开一个对话框，您可以在其中选择受规则影响的网站类别。

输入网址

如果选择此选项，则为特定网址或一组网址创建规则。

默认选择此选项。

添加

单击此按钮可打开一个对话框，您可以在其中指定受规则影响的网址或网址掩码。

删除

单击此按钮可从受规则影响的网址列表中删除所选网址或网址掩码。
如果选中网址或网址掩码旁边的复选框，则此按钮可用。

地址

受规则影响的网址或网址掩码。

“添加网址”对话框

网址输入字段

将受规则影响的网址或网址掩码。

“内容类别”对话框

内容类别列表

此列表包含可添加到规则的网站类别列表。

网站类别名称旁边的复选框将属于此类别的网站添加到规则中或从规则中删除。

默认情况下清除所有复选框。

“检测与响应”区域

Managed Detection and Response

单击此链接将打开一个窗口，您可以在其中配置 Managed Detection and Response 设置。

Endpoint Detection and Response

单击此链接将打开一个窗口，您可以在其中配置 Endpoint Detection and Response 设置。

Endpoint Detection and Response Expert (on-premise)

单击此链接将打开一个窗口，您可以在其中配置 Endpoint Detection and Response Expert (on-premise) 设置。

“Managed Detection and Response”窗口

Managed Detection and Response

Managed Detection and Response 切换开关启用/禁用与 Kaspersky Managed Detection and Response 服务交互的 Managed Detection and Response 组件。该服务持续检测和消除针对您组织的安全威胁。

如果 **Managed Detection and Response** 切换开关被开启且 MDR 配置文件被导入，Managed Detection and Response 组件被启用。

如果 **Managed Detection and Response** 切换开关被关闭，Managed Detection and Response 组件被禁用。

默认关闭此切换开关。

导入

单击该按钮打开一个窗口，在该窗口中，您可以将 MDR 配置文件导入到 Kaspersky Endpoint Security 策略中。

删除配置文件

单击该按钮从 Kaspersky Endpoint Security 策略中删除 MDR 配置文件。

强制

开启**强制**切换开关后，Kaspersky Endpoint Security 将禁止在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

关闭**强制**切换开关后，Kaspersky Endpoint Security 将允许在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

Endpoint Detection and Response 窗口

Endpoint Detection and Response

Endpoint Detection and Response 切换开关启用/禁用与 Kaspersky Endpoint Detection and Response 解决方案交互的 Endpoint Detection and Response 组件。该解决方案可保护计算机免受复杂威胁的侵扰，包括新的漏洞利用、勒索软件和无文件攻击。

如果 **Endpoint Detection and Response** 切换开关被开启，Endpoint Detection and Response 组件被启用。

如果 **Endpoint Detection and Response** 切换开关被关闭，Endpoint Detection and Response 组件被禁用。

默认关闭此切换开关。

在“**网络隔离**”部分，您可以配置设置，以便在检测到入侵指标时将计算机与网络隔离。

配置计算机解锁设置

单击此链接将打开一个窗口，您可以在其中指定自动关闭网络隔离的延迟。

排除项

单击此链接将打开一个窗口，您可以在其中指定在自动启用网络隔离后计算机上不会被阻止的网络连接。

在“**执行防护**”部分，您可以配置可执行文件和脚本的运行以及 Office 格式文件的打开设置。

执行防护

“**执行防护**”切换开关可启用/禁用执行防护。

如果打开了“**执行防护**”切换开关，您可以创建和编辑执行防护规则列表，并选择在执行或打开禁止对象时要执行的操作。

如果关闭“**执行防护**”切换开关，您将无法管理用户在其设备上执行或打开的对象。

默认关闭此切换开关。

执行或打开禁止的对象时的操作

阻止并写入报告

如果选择此模式，应用程序将阻止执行或打开符合防护规则标准的对象或文档。应用程序还会将有关尝试执行对象或打开文档的事件发布到 Kaspersky Security Center 事件日志和统一日志记录系统。

仅记录事件

如果选择此模式，Kaspersky Endpoint Security 会将有关尝试运行符合防护规则标准的可执行对象或打开符合防护规则标准的文档的事件发布到 Kaspersky Security Center 事件日志和统一日志记录系统，但不会阻止运行或打开对象或文档的尝试。默认选择此模式。

添加

单击此按钮将打开一个对话框，您可以在其中创建新的执行防护规则。

编辑

单击此按钮将打开一个对话框，您可以在其中编辑现有的执行防护规则。

如果在规则列表中选择了规则，则此按钮可用。

删除

单击此按钮可从规则列表中删除执行防护规则。

如果在规则列表中选择了规则，则此按钮可用。

在“**Cloud Sandbox 设置**”部分，您可以启用或禁用 Cloud Sandbox 组件。

Cloud Sandbox

Cloud Sandbox 切换开关可启用/禁用 Cloud Sandbox 技术，该技术有助于检测计算机上的高级威胁。Kaspersky Endpoint Security 自动将检测到的文件转发到 Cloud Sandbox 进行分析。Cloud Sandbox 在隔离的环境中运行这些文件以识别恶意活动并确定其信誉。然后，这些文件的数据被发送到卡巴斯基安全网络。因此，如果 Cloud Sandbox 检测到恶意文件，Kaspersky Endpoint Security 将执行适当的操作，以在检测到该文件的所有计算机上消除此威胁。

如果打开 **Cloud Sandbox** 切换开关，则启用 Cloud Sandbox 技术。

如果关闭 **Cloud Sandbox** 切换开关，则禁用 Cloud Sandbox 技术。

默认关闭此切换开关。

强制

开启**强制**切换开关后，Kaspersky Endpoint Security 将禁止在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

关闭**强制**切换开关后，Kaspersky Endpoint Security 将允许在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

计算机解锁设置窗口

自动解锁隔离的计算机于

此复选框启用/禁用在指定时间后自动关闭网络隔离。

如果选中此复选框，您可以指定自动关闭计算机网络隔离的延迟。

如果清除此复选框，Kaspersky Endpoint Security 将在隔离开始 8 小时后关闭网络隔离。

默认情况下已选定该选框。

小时

网络隔离将自动关闭的时间间隔。

仅当选中“**自动解锁隔离的计算机于**”复选框时，此字段才可供编辑。

“网络隔离排除项”窗口

网络隔离排除项

此列表包含您作为网络隔离排除项添加的网络连接。

添加

单击此按钮将打开一个窗口，您可以在其中手动指定要添加为排除项的网络连接设置。

从配置文件添加

单击此按钮将打开一个窗口，您可以在其中选择用于配置排除项的标准网络配置文件。

删除

单击此按钮将从网络隔离排除列表中删除网络连接。

如果在网络隔离排除列表中选择了连接，则此按钮可用。

“规则属性”窗口

规则名称

网络隔离排除规则的名称。

这是一个可选参数。

方向

流量方向。

协议

协议类型。

号码

协议编号。

该值必须符合分配的互联网协议号码 IANA 列表。

如果选择了“**自定义**”协议类型，则此字段可用。

本地端口或范围

正在配置网络隔离排除项的计算机的本地端口或范围。

远程端口或范围

正在配置网络隔离排除项的计算机的远程端口或范围。

远程地址

正在配置网络隔离排除项的计算机的网址。

应用程序

此复选框可让您添加一个应用程序，该应用程序被允许建立添加到隔离计算机上的网络隔离排除项的网络连接。

如果选中此复选框，您可以添加这样的应用程序。

如果清除此复选框，则添加到网络隔离排除项的网络连接可由隔离计算机上的任何应用程序建立。

默认清除此复选框。

添加

单击此按钮将打开一个窗口，您可以在其中指定允许建立添加到网络隔离排除项的网络连接的应用程序的路径。

编辑

单击此按钮将打开一个窗口，您可以在其中编辑已添加应用程序的路径。

如果在列表中选择了应用程序，则此按钮可用。

删除

单击此按钮可删除已添加的应用程序。

如果在列表中选择了应用程序，则此按钮可用。

“防护规则”窗口

名称

规则名称。

类型

想要阻止的对象的类型。

在“**对象路径**”部分，您可以选择是否指定要禁止的对象的完整路径。如果选择指定路径，请在相应的字段中输入其值。

在“**对象校验和**”部分，您可以选择是否指定要禁止的对象的校验和。如果选择指定校验和，请选择其类型并在相应的字段中输入其值。

“Endpoint Detection and Response (KATA)”窗口

Endpoint Detection and Response Expert (on-premise)

“**Endpoint Detection and Response Expert (on-premise)**”切换开关启用/禁用与 Kaspersky Anti Targeted Attack Platform 解决方案交互的 Endpoint Detection and Response Expert (on-premise) 组件。该解决方案可及时检测高级威胁，例如定向攻击、高级持续威胁、零日攻击等。

如果 **Endpoint Detection and Response Expert (on-premise)** 切换开关被开启，Endpoint Detection and Response Expert (on-premise) 组件被启用。

如果 **Endpoint Detection and Response Expert (on-premise)** 切换开关被关闭，Endpoint Detection and Response Expert (on-premise) 组件被禁用。

默认关闭此切换开关。

Endpoint Detection and Response Expert (版本 7.1 或更早版本)

如果选择此选项，则 Endpoint Detection and Response Expert (on-premise) 组件将以与 Endpoint Detection and Response Expert（版本 7.1 或更早版本）兼容的模式运行。

Endpoint Detection and Response Expert (版本 8.0 或后续版本)

如果选择此选项，则 Endpoint Detection and Response Expert (on-premise) 组件将以与 Endpoint Detection and Response Expert（版本 8.0 或更高版本）兼容的模式运行。

从策略继承连接设置

如果选择此选项，则遥测采集服务器连接设置、遥测采集服务器、遥测采集服务器数据传输设置、发送到遥测采集服务器的事件数量限制、响应服务器连接设置和响应服务器将从父策略继承，并且无法编辑。

如果选中了“**Endpoint Detection and Response Expert (版本 8.0 或后续版本)**”模式，则该选项可用。

默认选择此选项。

使用自定义连接设置

如果选择此选项，则连接到遥测采集服务器的设置、遥测采集服务器、遥测采集服务器数据传输设置、发送到遥测采集服务器的事件数量限制、连接到响应服务器的设置以及响应服务器将不会从父策略继承，并且仍然可供编辑。

如果选中了“**Endpoint Detection and Response Expert (版本 8.0 或后续版本)**”模式，则该选项可用。

根据“**连接到 KATA 服务器**”或者“**连接到遥测采集服务器**”区域中的所选模式，您可以配置与服务器的连接设置。

连接设置

单击此链接将打开一个对话框，您可以在其中配置连接到服务器的设置。

发送同步请求到服务器的间隔(分钟)

发送到 KATA 服务器的同步请求之间的时间间隔。

默认值是 5 分钟。

如果选中了“**Endpoint Detection and Response Expert (版本 8.0 或后续版本)**”模式，则该选项可用。

添加

单击此按钮将打开一个窗口，您可以在其中配置与服务器的连接。

编辑

单击此按钮将打开一个窗口，您可以在其中编辑与服务器的现有连接。

如果在服务器列表中选择了服务器，则此按钮可用。

删除

单击此按钮可从列表中删除选定的服务器。

如果在列表中选择了服务器，则此按钮可用。

地址

服务器的 IP 地址。

端口

服务器的端口号。

在“**数据传输设置**”部分中，您可以配置将数据发送到服务器的设置。

发送遥测到 KATA

此复选框用于启用/禁用向 KATA 服务器发送事件。

如果选中此复选框，则会将事件发送到 KATA 服务器。

如果清除此复选框，则不会将事件发送到 KATA 服务器。

如果选择了“**Endpoint Detection and Response Expert (版本 7.1 或更早版本)**”模式，则此选项可用。

默认清除此复选框。

将遥测发送到遥测采集服务器

此复选框用于启用/禁用向遥测采集服务器发送事件。

如果选中此复选框，则会将事件发送到遥测采集服务器。

如果清除此复选框，则不会将事件发送到遥测采集服务器。

如果选中了“**Endpoint Detection and Response Expert (版本 8.0 或后续版本)**”模式，此复选框可用。

默认清除此复选框。

最大事件传输延迟(秒)

Kaspersky Endpoint Security 向服务器发送事件的时间间隔。

默认值是 30 秒。

在“**请求限制**”部分，您可以限制传输事件的数量。

启用请求限制

此复选框启用/禁用限制 Kaspersky Endpoint Security 发送到 KATA 服务器的事件数量。

如果选中此复选框，则应用程序发送的事件数将受到限制。

如果清空此复选框，则应用程序发送的事件数量不受限制。

默认情况下已选定该选框。

每小时最大事件数

Kaspersky Endpoint Security 每小时发送到 KATA 服务器的最大事件数。Kaspersky Endpoint Security 在一小时后恢复发送事件。

默认值为每小时 3000 个事件。

超出事件限制的百分比

相同类型事件的阈值（以百分比表示）。

如果特定类型的事件与事件总数的比率超过配置的阈值， Kaspersky Endpoint Security 将限制该类型事件的传输。

默认值是 15%。

在“**连接到响应服务器**”区域，您可以在此部分配置与响应服务器的连接设置。

连接设置

单击此链接将打开一个对话框，您可以在其中配置连接到服务器的设置。

发送同步请求到服务器的间隔(分钟)

发送到 KATA 服务器的同步请求之间的时间间隔。

默认值是 5 分钟。

如果选中了“**Endpoint Detection and Response Expert (版本 8.0 或后续版本)**”模式，则该选项可用。

添加

单击此按钮将打开一个窗口，您可以在其中配置与服务器的连接。

编辑

单击此按钮将打开一个窗口，您可以在其中编辑与服务器的现有连接。

如果在服务器列表中选择了服务器，则此按钮可用。

删除

单击此按钮可从列表中删除选定的服务器。

如果在列表中选择了服务器，则此按钮可用。

地址

服务器的 IP 地址。

端口

服务器的端口号。

强制

开启**强制**切换开关后，Kaspersky Endpoint Security 将禁止在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

关闭**强制**切换开关后，Kaspersky Endpoint Security 将允许在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

“KATA 服务器”窗口

地址

KATA 服务器的 IP 地址。

端口

KATA 服务器的端口号。

默认值为 443。

“服务器连接设置”窗口

超时(秒)

KATA 服务器响应超时。超时后，Kaspersky Endpoint Security 会尝试连接到其他 KATA 服务器。

默认值是 10 秒。

在“**服务器 TLS 证书**”部分中，您可以添加或删除 TLS 证书并查看有关所添加的证书的信息。

添加 TLS 证书

单击此按钮将打开一个窗口，您可以在其中选择将用于与 KATA 服务器建立受信任连接的 TLS 证书。

卸载

单击此按钮将删除当前的 TLS 证书。

如果已添加 TLS 证书，则此按钮可用。

在“**附加连接安全**”部分中，您可以为 Kaspersky Endpoint Security 和 KATA 服务器之间的连接配置增强保护。

使用双向认证

此复选框启用/禁用双向验证，使 Kaspersky Endpoint Security 和 KATA 服务器之间的连接更加安全。要使用双向验证，您需要加载加密容器。

如果选中此复选框，Kaspersky Endpoint Security 使用双向验证连接到 KATA 服务器。

如果清除此复选框， Kaspersky Endpoint Security 不使用双向验证连接到 KATA 服务器。

默认清除此复选框。

加载加密容器

单击此按钮将打开一个窗口，您可以在其中选择将用于双向验证的加密容器。加密容器文件的扩展名为 .PFX。

注意：加密容器必须受密码保护。无法添加密码为空的加密容器。

加密容器密码

用于双向验证的加密容器的密码。

“更新”部分

更新应用程序模块

此复选框启用/禁用应用程序模块的更新。始终更新应用程序数据库。

如果选中此复选框，则 Kaspersky Endpoint Security 将更新应用程序模块。

如果清除此复选框，则 Kaspersky Endpoint Security 不会更新应用程序模块。

默认情况下已选定该选框。

更新源

此列表包含 Kaspersky Endpoint Security 可从中下载并安装应用程序数据库和模块更新的资源的地址。您可以指定本地或网络文件夹，或 FTP 或 HTTP 服务器作为更新源。

默认情况下，更新源列表包含卡巴斯基更新服务器。

如果通过 Kaspersky Security Center Web Console 管理 Kaspersky Endpoint Security，则更新源列表默认还包含 Kaspersky Security Center 服务器。

如果通过 Kaspersky Security Center 云控制台管理 Kaspersky Endpoint Security，则更新源列表默认还包含分发点。有关分发点的详细信息，请参阅 Kaspersky Security Center 帮助。

无法从列表中删除默认更新源。

添加

单击此按钮可打开一个对话框，您可以在其中指定要添加到更新源列表中的本地或网络文件夹路径或网址。

删除

单击此按钮可从列表中删除选定的更新源。

如果选中更新源旁边的复选框，则此按钮可用。

更新源

此列包含 Kaspersky Endpoint Security 的更新源。

状态

如果开启此列中的切换开关，则 Kaspersky Endpoint Security 将使用**更新源**列中的相应更新源来接收更新。

如果关闭此列中的切换开关，则 Kaspersky Endpoint Security 将不使用**更新源**列中的相应更新源来接收更新。

强制

开启**强制**切换开关后，Kaspersky Endpoint Security 将禁止在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

关闭**强制**切换开关后，Kaspersky Endpoint Security 将允许在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

“添加更新源”对话框

“输入本地或网络文件夹路径，或者网址”输入字段

Kaspersky Endpoint Security 从中复制更新的资源的地址。

您可以指定本地或网络文件夹的路径，或将 FTP 或 HTTP 服务器的网址或 IP 地址指定为资源地址。

您可以按以下格式指定 FTP 服务器的网址：FTP://<用户名>：<密码>@<主机>：<端口>。

在**状态**区域中，您可以定义 Kaspersky Endpoint Security 是否使用指定的网址作为更新源。

已禁用

网址已添加到更新源列表中，但 Kaspersky Endpoint Security 并未使用此网址作为更新源。

已启用

网址已添加到更新源列表中，且 Kaspersky Endpoint Security 将使用此网址作为更新源。

“数据加密”区域

文件保险箱磁盘加密

文件保险箱磁盘加密切换开关可启用/禁用文件保险箱磁盘加密管理。

如果开启**文件保险箱磁盘加密**切换开关，则可从 Kaspersky Security Center 将文件保险箱磁盘加密应用到客户端计算机。

如果关闭**文件保险箱磁盘加密**切换开关，则无法从 Kaspersky Security Center 将文件保险箱磁盘加密应用到客户端计算机。

默认关闭此切换开关。

注意：如果关闭**文件保险箱磁盘加密**切换开关，则具有管理员权限的用户可以在系统设置中加密和解密 Mac 启动盘。有关文件保险箱的更多信息，请参阅 Apple 文档。

加密磁盘

Kaspersky Endpoint Security 在应用策略的客户端计算机上显示计算机账户凭据提示。当用户输入凭据时，Kaspersky Endpoint Security 开始加密用户的启动盘。

如果开启**文件保险箱磁盘加密**切换开关并选择**加密磁盘**选项，则具有管理员权限的用户无法在系统设置中解密其 Mac 启动盘。

解密磁盘

Kaspersky Endpoint Security 在应用策略的客户端计算机上显示计算机账户凭据提示。当用户输入凭据时，Kaspersky Endpoint Security 开始解密用户的启动盘。

如果开启**文件保险箱磁盘加密**切换开关并选择**解密磁盘**选项，则具有管理员权限的用户无法在系统设置中加密其 Mac 启动盘。

强制

开启**强制**切换开关后，Kaspersky Endpoint Security 将禁止在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

关闭**强制**切换开关后，Kaspersky Endpoint Security 将允许在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

“遥测设置”窗口

添加

单击此按钮可打开一个窗口，您可以在其中向受信任区域中添加规则。

编辑

单击此按钮可打开一个窗口，您可在该窗口中编辑所选规则。

删除

单击该按钮可以从受信任区域中删除选定的规则。

状态

此列中的切换开关用于禁用/启用添加到受信任区域的规则。

如果拨动开关已启用，则该规则处于活动状态。

如果切换开关被禁用，则该规则处于非活动状态。

规则名称

此列包含添加到受信任区域的规则名称。

描述

向受信任区域添加的规则的注释。

添加/编辑排除规则窗口

状态

此切换开关用于启用/禁用添加到受信任区域的规则。

如果拨动开关已启用，则该规则处于活动状态。

如果切换开关被禁用，则该规则处于非活动状态。

规则名称

添加到受信任区域的规则名称。

描述

向受信任区域添加的规则的注释。

攻击指标 (IOA)

用于输入攻击指标 GUID 的字段。

“附加设置”区域

保护

单击此链接可打开**保护**窗口，您可以在其中管理客户端计算机上安装的 Kaspersky Endpoint Security 的常规设置，并选择 Kaspersky Endpoint Security 将检测的对象类型。

报告和备份

单击此链接可打开**报告和备份**窗口，您可以在其中管理报告和备份设置。

用户交互

单击此链接可打开**用户交互**窗口，您可以在其中设置 Kaspersky Endpoint Security 显示的通知、Kaspersky Security Center 显示的事件的显示语言以及 Kaspersky Endpoint Security 的附加设置。

网络

单击此链接将打开**网络**窗口，您可以在其中管理代理服务器设置、启用或禁用加密连接 (HTTPS) 扫描、选择用于检查 Mozilla Firefox 浏览器中加密 HTTPS 流量的证书存储以及配置受监控端口。

受信任区域

单击此链接可打开**受信任区域**窗口，您可以在其中添加文件威胁防护或扫描任务的排除项，以及配置受信任应用程序。

“保护”窗口

在**常规**区域中，您可以对远程计算机启用或禁用文件保护，并配置在启动计算机或重启操作系统时自动启动该应用程序。

在计算机启动时启动应用程序

此复选框启用/禁用在远程计算机打开或操作系统重新启动后自动启动 Kaspersky Endpoint Security。

如果选中此复选框，则当远程计算机打开或其操作系统重新启动时，Kaspersky Endpoint Security 将自动启动。

如果清除该复选框，则当远程计算机打开或其操作系统重新启动时，Kaspersky Endpoint Security 不会自动启动。

默认情况下已选定该选框。

重要提示：如果您在 Kaspersky Endpoint Security 未运行时选中此复选框，则只有在于本地或使用 Kaspersky Security Center 启动应用程序后才会应用更改。

启用保护

此复选框启用/禁用对安装了 Kaspersky Endpoint Security 的远程计算机的保护。

如果选中此复选框，则启用对远程计算机的保护。

如果清除此复选框，则禁用对远程计算机的保护。

默认情况下已选定该选框。

在**要检测的对象类型**区域中，您可以选择 Kaspersky Endpoint Security 要检测的对象类型。

病毒、蠕虫、木马程序、恶意工具、广告软件和自动拨号软件

此复选框启用/禁用以下类型程序的检测：

- 所有类型的恶意软件。
- 在您的计算机上显示广告（例如，广告栏）或使用广告网站替换浏览器中的搜索结果的应用程序。
- 通过计算机的调制解调器秘密建立电话连接的应用程序。

默认情况下，该复选框处于选中状态，无法清除。

可以被入侵者利用以损坏用户计算机或个人数据的合法软件

此复选框启用/禁用对非恶意或危险的应用程序的检测，但在某些情况下，这些应用程序可能被用来危害用户的计算机。

如果选中此复选框，Kaspersky Endpoint Security 将检测入侵者可用于损坏用户计算机或个人数据的合法软件。

如果清除此复选框，Kaspersky Endpoint Security 将不会检测到入侵者可用于损坏用户计算机或个人数据的合法软件。

默认清除此复选框。

在**高级**区域中，您可以启用节能模式。

使用电池电源运行时跳过计划任务

此复选框启用/禁用在使用电池供电的计算机上启动计划的扫描任务。

如果选中此复选框，则 Kaspersky Endpoint Security 不会在使用电池供电的计算机上启动计划的扫描任务。

如果清除此复选框，Kaspersky Endpoint Security 将在使用电池供电的计算机上启动计划的扫描任务。

默认情况下已选定该选框。

限制扫描任务对 CPU 的使用

Kaspersky Endpoint Security 将其在按需扫描任务期间对受保护设备的 CPU 的使用限制为对应输入字段中指定的值。

启用此选项会对 Kaspersky Endpoint Security 的性能产生负面影响。

默认情况下，该选项已禁用。

上限(百分比)

Kaspersky Endpoint Security 对扫描任务允许的最大 CPU 使用率。

如果选择了“**限制扫描任务对 CPU 的使用**”选项，则该输入字段可用。

注意：这是所有 CPU 内核的累积限制。活动监控中显示的 CPU 利用率是每个 CPU 内核利用率的总和，因此可能会超过 100%。

强制

开启**强制**切换开关后，Kaspersky Endpoint Security 将禁止在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

关闭**强制**切换开关后，Kaspersky Endpoint Security 将允许在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

“报告和备份”窗口

在**报告**区域中，您可以为 Kaspersky Endpoint Security 运行期间发生的事件配置事件报告的生成和存储设置。

在此时间段后删除报告 <值> 天

此复选框启用/禁用在指定时间段后删除报告。

如果选中此复选框，则 Kaspersky Endpoint Security 会在指定时间段后删除报告。默认情况下，Kaspersky Endpoint Security 将报告存储 30 天。

如果清除此复选框，则 Kaspersky Endpoint Security 将无限期地存储报告。

默认情况下已选定该选框。

记录非关键事件

此复选框启用/禁用报告中非关键事件（如信息性事件）的日志记录。非关键事件不会影响安全性。

如果选中此复选框，则 Kaspersky Endpoint Security 会在报告中记录信息性事件。

如果清除此复选框，则 Kaspersky Endpoint Security 不会在报告中记录信息性事件。

默认清除此复选框。

仅保留最近事件

此复选框启用/禁用仅保留与任务上次运行中的重要事件有关的信息。

如果选中此复选框，则每次任务启动时，Kaspersky Endpoint Security 都会从任务的上一次运行中删除有关非关键事件的信息，但会在报告中保留重要信息（例如，关于检测到的恶意软件）。

如果清除此复选框，Kaspersky Endpoint Security 将保留任务上一次运行中的所有信息。

默认清除此复选框。

在**备份**区域中，您可以指定对象在备份中可存储多长时间。

在此时间段后删除对象 <值> 天

此复选框启用/禁用在指定时间段后从备份中删除对象。

如果选中此复选框，则 Kaspersky Endpoint Security 将在指定时间段后从备份中删除对象。默认存储期为 30 天。

如果清除此复选框，则 Kaspersky Endpoint Security 将对象无限期地存储在备份中。

默认情况下已选定该选框。

强制

开启**强制**切换开关后，Kaspersky Endpoint Security 将禁止在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

关闭**强制**切换开关后，Kaspersky Endpoint Security 将允许在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

“用户交互”窗口

在**应用程序界面**区域中，您可以配置是否在远程计算机上的菜单栏中显示应用程序图标，以及用户是否可打开应用程序主窗口并使用应用程序界面。

在菜单栏中显示应用程序图标

此复选框启用/禁用远程计算机菜单栏中应用程序图标的显示。

如果选中此复选框，应用程序图标将显示在菜单栏中。

如果清除此复选框，应用程序图标将从菜单栏中隐藏。

默认情况下已选定该选框。

允许用户打开应用程序

此复选框启用/禁用用户打开 Kaspersky Endpoint Security 主窗口和使用远程计算机上的应用程序界面的能力。

如果选中此复选框，则用户可以打开 Kaspersky Endpoint Security 主窗口并使用远程计算机上的应用程序界面。

如果清除此复选框，Kaspersky Endpoint Security 将阻止用户打开主应用程序窗口并隐藏远程计算机上的应用程序界面。

默认情况下已选定该选框。

在**通知**区域中，您可以启用有关 Kaspersky Endpoint Security 事件的通知并选择首选通知类型。

通知

通知切换开关可启用/禁用有关 Kaspersky Endpoint Security 事件的通知。

如果开启**通知**切换开关，则 Kaspersky Endpoint Security 将显示有关 Kaspersky Endpoint Security 组件运行期间发生的事件的通知。

如果关闭**通知**切换开关，则 Kaspersky Endpoint Security 将不会显示 Kaspersky Endpoint Security 组件运行期间发生的事件的相关通知。

默认开启此切换开关。

用户通知

单击此链接可打开一个窗口，您可以在其中选择要为所有事件类型使用的通知类型。

在“**允许用户退出应用程序**”部分，您可以配置远程计算机上的用户是否可以关闭 Kaspersky Endpoint Security。

在应用程序图标的上下文菜单中显示“退出”

此复选框可启用/禁用菜单栏中显示的应用程序图标的上下文菜单中的**退出**菜单项的可用性。

如果选中此复选框，则**退出**菜单项在应用程序图标的上下文菜单中可用。远程计算机的用户可以退出远程计算机上的 Kaspersky Endpoint Security。

如果清除此复选框，则**退出**菜单项在应用程序图标的上下文菜单中不可用。远程计算机的用户无法退出远程计算机上的 Kaspersky Endpoint Security。

默认情况下已选定该选框。

在**Kaspersky Security Center 中的事件**区域中，您可以选择 Kaspersky Endpoint Security 事件在 Kaspersky Security Center 中的显示语言。

显示语言

从该下拉列表中，您可以选择 Kaspersky Security Center 中 Kaspersky Endpoint Security 事件的显示语言。

在**限制**区域中，您可以允许在远程计算机上本地管理 Kaspersky Endpoint Security 密钥和更新。

允许用户在本地管理更新

此复选框启用/禁用远程计算机上 Kaspersky Endpoint Security 更新的本地管理。

如果选中此复选框，将启用远程计算机上 Kaspersky Endpoint Security 更新的本地管理。

如果清除此复选框，则只能使用 Kaspersky Security Center 中的 Kaspersky Endpoint Security 管理插件来管理远程计算机上的 Kaspersky Endpoint Security 更新。

默认情况下已选定该选框。

允许用户在本地管理密钥

此复选框启用/禁用远程计算机上 Kaspersky Endpoint Security 密钥的本地管理。

如果选中该复选框，将启用远程计算机上 Kaspersky Endpoint Security 密钥的本地管理。

如果清除此复选框，则只能使用 Kaspersky Security Center 中的 Kaspersky Endpoint Security 管理插件来管理远程计算机上的 Kaspersky Endpoint Security 密钥。

默认情况下已选定该选框。

在“**密码保护**”部分，您可以设置和配置密码以限制用户设备上的不必要的操作。

密码保护

“**密码保护**”切换开关可启用/禁用对用户设备上不需要的操作的密码保护。

如果打开了“**密码保护**”切换开关，您可以设置和配置密码来限制用户在其设备上的操作。

如果关闭“**密码保护**”切换开关，用户无需输入密码即可执行不需要的操作。

默认关闭此切换开关。

打开此切换开关将打开一个窗口，您可以在其中配置密码，以限制用户设备上不需要的操作。

设置

单击此按钮将打开一个窗口，您可以在其中配置密码，以限制用户设备上不需要的操作。

强制

开启**强制**切换开关后，Kaspersky Endpoint Security 将禁止在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

关闭**强制**切换开关后，Kaspersky Endpoint Security 将允许在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

“用户通知”窗口

事件

此列列出了 Kaspersky Endpoint Security 运行期间可能发生的事件：

- **关键事件**。对安全至关重要的事件。
- **功能失败**。导致系统故障的事件。
- **重要事件**。用户应该关注的事件。
- **信息事件**。本质上是信息性的事件。

通知

通知是一个弹出消息，用于通知用户某个事件。

通知列中的复选框可启用/禁用有关特定类别事件的弹出通知。

声音

与事件有关的声音通知。

声音列中的复选框可启用/禁用有关特定类别事件的声音通知。

“受信任区域”窗口：“文件和文件夹”区域

添加

单击此按钮可打开一个对话框，您可以在其中向受信任区域中添加文件或文件夹。

删除

单击此按钮可从排除项列表中删除选定的文件或文件夹。

如果选中文件或文件夹旁边的复选框，则此按钮可用。

文件或文件夹

此列包含已添加到受信任区域中的文件或文件夹。

状态

此列中的切换开关可禁用/启用扫描已添加到受信任区域中的文件或文件夹。

如果开启该切换开关，则 Kaspersky Endpoint Security 将不会扫描相应文件或文件夹。

如果关闭该切换开关，则 Kaspersky Endpoint Security 将扫描相应文件或文件夹。

评论

已添加到受信任区域中的文件或文件夹的相关信息。

强制

开启**强制**切换开关后，Kaspersky Endpoint Security 将禁止在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

关闭**强制**切换开关后，Kaspersky Endpoint Security 将允许在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

“添加排除项”对话框

输入文件名、文件夹名或掩码输入字段

要从保护范围中排除的文件路径、文件夹路径或文件/文件夹掩码。

包含子文件夹

此复选框可启用/禁用扫描在**输入文件名称、文件夹名称或掩码**字段中指定的文件夹中的子文件夹。

如果选中此复选框，则 Kaspersky Endpoint Security 在恶意软件扫描过程中将不会扫描指定文件夹的子文件夹。

如果清除此复选框，则 Kaspersky Endpoint Security 在恶意软件扫描过程中将仅排除直接位于在**输入文件名称、文件夹名称或掩码**字段中指定的文件夹中的文件。指定文件夹的子文件夹即将被扫描。

默认情况下已选定该选框。

在**组件**区域中，您可以选择将不会扫描指定文件或文件夹的组件。

任何

无论是“扫描”组件还是“文件威胁防护”组件，均不会扫描指定文件或文件夹。

从列表

此选项允许您选择组件。

文件威胁防护

如果选中此复选框，则“文件威胁防护”组件将不会扫描指定文件或文件夹。
如果选择**从列表**选项，则此复选框可用。

扫描

如果选中此复选框，则“扫描”组件将不会扫描指定文件或文件夹。
如果选择**从列表**选项，则此复选框可用。

“注释”输入字段

已添加到受信任区域中的文件或文件夹的相关信息。

在**状态**区域中，您可以选择排除项是否处于活动状态。

已禁用

Kaspersky Endpoint Security 将扫描相应文件或文件夹。

已启用

Kaspersky Endpoint Security 将不会扫描相应文件或文件夹。

“受信任区域”窗口：“受信任应用程序”区域

受信任应用程序列表

Kaspersky Endpoint Security 将不会监控其网络活动的受信任应用程序列表。

添加

单击此按钮可打开一个对话框，您可以在其中输入 Kaspersky Endpoint Security 将不会监控其网络活动的应用程序路径。

删除

单击此按钮可从列表中删除选定的受信任应用程序。

如果选中受信任应用程序旁边的复选框，则此按钮可用。

应用程序

此列包含应用程序名称或应用程序路径的最后一段。

状态

此列包含指示应用程序网络活动监控状态的切换开关。

如果状态为**已启用**，则 Kaspersky Endpoint Security 将不会监控相应应用程序的网络活动。

如果状态为**已禁用**，则 Kaspersky Endpoint Security 将监控相应应用程序的网络活动。

路径

此列包含您手动添加的应用程序在客户端计算机上的路径。

强制

开启**强制**切换开关后，Kaspersky Endpoint Security 将禁止在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

关闭**强制**切换开关后，Kaspersky Endpoint Security 将允许在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

“添加应用程序”对话框

路径输入字段

其网络活动或文件活动将不受 Kaspersky Endpoint Security 应用程序监控的应用程序的路径。

代码签名要求

对其活动不受 Kaspersky Endpoint Security 监控的应用程序的代码签名的要求。

这是一个可选参数。

选项

在本部分中，您可以选择您不希望被 Kaspersky Endpoint Security 应用程序监控的活动类型。

不监控文件活动

此复选框启用/禁用应用程序对客户端计算机上的文件的操作的监控。

如果选中此复选框，则 Kaspersky Endpoint Security 将不会监控应用程序的文件活动。

如果清除此复选框，则 Kaspersky Endpoint Security 将监控应用程序的文件活动。

默认情况下已选定该选框。

不监控网络活动

此复选框启用/禁用对客户端计算机上应用程序的入站和出站互联网流量的监控。

如果选中此复选框，则 Kaspersky Endpoint Security 将不会监控应用程序的网络活动。

如果清除此复选框，则 Kaspersky Endpoint Security 将监控应用程序的网络活动。

默认情况下已选定该选框。

“网络”窗口

在**代理服务器设置**区域中，您可以配置使用代理服务器及连接到代理服务器时要使用的设置。

不使用代理服务器

如果选中此选项，则 Kaspersky Endpoint Security 不会使用代理服务器连接到应用程序数据库和模块的更新源。

使用系统代理服务器设置

如果选择此选项，Kaspersky Endpoint Security 将使用操作系统中配置的代理服务器设置连接到应用程序数据库和模块的更新源。

默认选择此选项。

使用指定的代理服务器设置

如果选择此选项，Kaspersky Endpoint Security 将使用您指定的代理服务器设置连接到应用程序数据库和模块的更新源。

地址

l代理服务器的 IP 地址或符号名。

如果选择**使用指定的代理服务器设置**选项，则此字段可用。

端口

代理服务器端口号。

默认端口号是 8080。

如果选择**使用指定的代理服务器设置**选项，则此字段可用。

使用身份验证

此复选框启用/禁用连接到代理服务器时使用身份验证。

如果选中此复选框，Kaspersky Endpoint Security 要求用户的凭据才能连接到代理服务器。

如果清除此复选框，Kaspersky Endpoint Security 不要求用户的凭据连接到代理服务器。

默认情况下已选定该选框。

如果选择**使用指定的代理服务器设置**选项，则此复选框可用。

用户名称

用于连接到代理服务器的用户名。

如果选择**使用指定的代理服务器设置**选项并选中**使用身份验证**复选框，则此字段可用。

密码

指定用户名的密码。

如果选择**使用指定的代理服务器设置**选项并选中**使用身份验证**复选框，则此字段可用。

显示

单击此按钮可显示在**密码**字段中输入的密码字符。

本地地址不使用代理服务器

此复选框启用/禁用从本地或网络文件夹更新应用程序数据库和模块时使用代理服务器。

如果选中此复选框，则 Kaspersky Endpoint Security 在从本地或网络文件夹更新应用程序数据库和模块时不使用代理服务器。

如果清除此复选框，则 Kaspersky Endpoint Security 将在从本地或网络文件夹更新应用程序数据库和模块时使用代理服务器。

默认情况下已选定该选框。

如果选择**使用指定的代理服务器设置**选项，则此复选框可用。

在**检查安全连接**区域中，您可以定义 Kaspersky Endpoint Security 是否扫描安全连接 (HTTPS)。

安全连接 (HTTPS) 检查

安全连接 (HTTPS) 检查切换开关可启用/禁用扫描通过 HTTPS 协议建立的安全连接，以及当 Web 控制阻止用户访问危险网络资源时显示通知。

如果开启**安全连接 (HTTPS) 检查**切换开关，则 Kaspersky Endpoint Security 将执行以下操作：

- Web 威胁防护会扫描您的计算机通过 Safari、Google Chrome 或 Firefox 中的 HTTPS 协议发送和接收的数据。
- 当用户访问被远程计算机上的 Web 控制阻止的 Web 资源时，应用程序将显示通知。

如果关闭**安全连接 (HTTPS) 检查**切换开关，则 Kaspersky Endpoint Security 将执行以下操作：

- Web 威胁防护不会扫描计算机通过 HTTPS 协议发送和接收的数据。
- 当用户访问被远程计算机上的 Web 控制阻止的 Web 资源时，应用程序不显示通知。

默认开启此切换开关。

在“**选择 Firefox 要使用的证书存储**”部分中，您可以选择用于检查 Mozilla Firefox 浏览器中加密 HTTPS 流量的证书存储。

System Roots 证书链(推荐)

如果选择此选项，Kaspersky Endpoint Security 将使用来自 System Roots 钥匙串的根证书来检查 Mozilla Firefox 浏览器中的加密 HTTPS 流量。

默认选择此选项。

Mozilla Firefox 浏览器设置中的证书存储

如果选择此选项，Kaspersky Endpoint Security 将使用来自浏览器证书存储区的证书。

此种情况下，您需要手动将 Kaspersky Endpoint Security 证书添加到 Mozilla Firefox 浏览器的证书存储中。有关更多信息，请参阅“如何将卡巴斯基证书添加到 Mozilla Firefox 证书存储”。

在“**受信任的根证书**”部分，您可以管理受信任的根证书列表。

管理受信任的根证书

单击此链接将打开一个窗口，您可以在其中创建受信任的根证书列表，以连接到相应的服务器，而无需通知。

在**受监控端口**区域中，您可以配置受 Kaspersky Endpoint Security 监控的端口。

选择端口

单击此链接可打开一个窗口，您可以在其中配置受 Kaspersky Endpoint Security 监控的端口列表。

强制

开启**强制**切换开关后，Kaspersky Endpoint Security 将禁止在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

关闭**强制**切换开关后，Kaspersky Endpoint Security 将允许在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

“管理受信任的根证书”窗口

添加

单击此按钮将打开一个对话框，用于添加将被视为受信任的证书。

删除

单击此按钮可从列表中删除选定的证书。

受信任证书列表

显示受信任的根证书名称的列表。

该列表默认为空。

强制

开启**强制**切换开关后，Kaspersky Endpoint Security 将禁止在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

关闭**强制**切换开关后，Kaspersky Endpoint Security 将允许在本地计算机上更改任务设置、应用程序设置、子组的策略和从属管理服务器的值。

“受监控的端口”窗口

受监控的端口列表

一个端口列表，您可以为其配置对传输数据的监视。

默认情况下，端口列表包含最常见服务常用的端口。

添加

单击此按钮可打开一个对话框，您可以在其中添加希望 Kaspersky Endpoint Security 监控的端口。

删除

单击此按钮可从列表中删除选定的端口。

如果选中端口旁边的复选框，则此按钮可用。

端口

该列包含端口号。

状态

此列包含指示对通过端口传输的数据的监控状态的切换开关。
如果状态为**已监控**，则 Kaspersky Endpoint Security 将扫描通过相应端口传输的流量。
如果状态为**未监控**，则 Kaspersky Endpoint Security 将不会扫描通过相应端口传输的流量。

描述

此列包含端口的说明。

“添加端口”对话框

端口输入字段

您希望 Kaspersky Endpoint Security 扫描传输数据的端口号。

说明输入字段

有关端口的附加信息，例如，端口类型。

“授权许可信息”窗口

在**授权许可信息**窗口中，您可以查看授权许可的相关信息，包括授权许可到期日期、依据此授权许可可在其上使用 Kaspersky Endpoint Security 的计算机数量以及授权许可类型。

添加为备用密钥

此复选框启用/禁用将特定密钥文件或激活码添加为备用密钥。

如果选中此复选框，则 Kaspersky Endpoint Security 将指定的密钥文件或激活码添加为备用密钥。

如果清除此复选框，则 Kaspersky Endpoint Security 将指定的密钥文件或激活码添加为活动密钥。

默认清除此复选框。

“扫描”窗口

扫描范围

单击此链接可打开一个窗口，您可以在其中创建扫描范围。

在**若检测到恶意对象**区域中，您可以选择 Kaspersky Endpoint Security 在检测到受感染对象时要执行的操作。

扫描后提示用户采取操作

在扫描完成之前，Kaspersky Endpoint Security 不会处理对象。此时，Kaspersky Endpoint Security 将显示一个通知，其中包含每个受感染对象的信息，并提示用户选择要采取的操作。可用选项取决于对象的类型。

默认选择此选项。

立即提示用户采取操作

Kaspersky Endpoint Security 显示一个通知，其中包含应用程序检测到的每个受感染对象的信息，并提示用户选择进一步的操作。可用选项取决于对象的类型。

不提示操作

Kaspersky Endpoint Security 在报告中记录有关检测到的对象的信息，而不进行处理。

自动清除

此复选框启用/禁用 Kaspersky Endpoint Security 检测到的受感染对象的清除，而不提示用户进行确认。

如果选中此复选框，Kaspersky Endpoint Security 将自动清除受感染对象。

如果清除复选框，Kaspersky Endpoint Security 跳过受感染的对象。

如果选择**不提示操作**选项，则此复选框可用。

默认情况下已选定该选框。

清除，无法清除则删除

此复选框启用/禁用在尝试清除失败后删除受感染或可能受感染的对象。

如果选中此复选框，则 Kaspersky Endpoint Security 会自动删除无法清除的受感染对象。

如果清除此复选框，则 Kaspersky Endpoint Security 不会删除无法清除的受感染对象。

如果选择**不提示操作**选项并选中**自动清除**复选框，则会显示此复选框。

默认情况下已选定该选框。

在**文件类型**区域中，您可以选择 Kaspersky Endpoint Security 要扫描的文件格式。

扫描所有文件

Kaspersky Endpoint Security 扫描所有执行、打开或保存的文件系统对象。

按内容扫描应用程序和文档

Kaspersky Endpoint Security 只扫描基于格式可能被感染的对象。

文件格式列表由卡巴斯基定义，并包含在 Kaspersky Endpoint Security 数据库中。

按扩展名扫描应用程序和文档

Kaspersky Endpoint Security 只扫描基于文件扩展名可能被感染的对象。

文件扩展名列表由卡巴斯基定义，并包含在 Kaspersky Endpoint Security 数据库中。

Kaspersky Endpoint Security 总是扫描没有扩展名的文件。

在**优化**区域中，您可以配置扫描性能。

仅扫描新建和已修改的文件

此复选框启用/禁用仅扫描自上次扫描以来 Kaspersky Endpoint Security 识别为新建或已更改的文件。

如果选中此复选框，则 Kaspersky Endpoint Security 仅扫描自上次扫描以来识别为新建或已更改的文件。

如果清除此复选框，则 Kaspersky Endpoint Security 将扫描所有文件。

跳过扫描只读系统卷

此复选框禁用/启用由 Kaspersky Endpoint Security 扫描只读系统卷。

如果选择此复选框，则 Kaspersky Endpoint Security 将不扫描只读系统卷。这大大缩短了扫描时间。

如果清除此复选框，则 Kaspersky Endpoint Security 将扫描只读系统卷。

默认情况下已选定该选框。

跳过大于此大小的文件 <值> MB

此复选框启用/禁用从扫描中排除大于指定大小的文件。

如果选中此复选框，则 Kaspersky Endpoint Security 将跳过超过指定大小的文件。

如果清除此复选框，则 Kaspersky Endpoint Security 扫描文件，不管其大小。

默认清除此复选框。

默认情况下，大小被设置为 100 MB。

如果扫描大于此时间则跳过 <值> 秒

此复选框启用/禁用对文件扫描持续时间的限制。如果扫描文件超过指定的时间限制，Kaspersky Endpoint Security 将跳过该文件。

如果选中此复选框，则如果扫描文件超过指定的时间限制，Kaspersky Endpoint Security 将跳过该文件。

如果清除此复选框，则 Kaspersky Endpoint Security 将扫描文件，而不管扫描可能需要多长时间。

默认值是 30 秒。

在**复合文件**区域中，您可以选择 Kaspersky Endpoint Security 将扫描的复合文件类型。

扫描压缩包

此复选框启用/禁用扫描压缩包。

如果选中此复选框，则 Kaspersky Endpoint Security 将扫描压缩包。

如果清除此复选框，则 Kaspersky Endpoint Security 在扫描过程中将跳过压缩包。

所有

Kaspersky Endpoint Security 将扫描所有压缩包。

如果选中**扫描压缩包**复选框，则此选项可用。

仅新建

Kaspersky Endpoint Security 将仅扫描新压缩包。

如果选中**扫描压缩包**复选框，则此选项可用。

扫描受密码保护的压缩包

此复选框启用/禁用扫描密码保护的压缩包。

如果选中此复选框，则 Kaspersky Endpoint Security 将扫描密码保护的压缩包。

如果清除此复选框，则 Kaspersky Endpoint Security 将在扫描时跳过密码保护的压缩包。

扫描嵌入的 OLE 对象

此复选框启用/禁用对文件中嵌入的对象（如 Excel 电子表格、宏或电子邮件附件）的扫描。
如果选中此复选框，则 Kaspersky Endpoint Security 将扫描嵌入的 OLE 对象。
如果清除此复选框，则 Kaspersky Endpoint Security 在扫描过程中将跳过嵌入的 OLE 对象。

所有

Kaspersky Endpoint Security 将扫描所有 OLE 对象。
如果选中**扫描嵌入的 OLE 对象**复选框，则此选项可用。

仅新建

Kaspersky Endpoint Security 仅扫描新嵌入的 OLE 对象。
如果选中**扫描嵌入的 OLE 对象**复选框，则此选项可用。

扫描电子邮件格式文件

该选框用于启用/禁用对电子邮件格式文件和电子邮件数据库的扫描。
如果选中此复选框，则 Kaspersky Endpoint Security 将扫描电子邮件格式文件和电子邮件数据库。
如果清除此复选框，则 Kaspersky Endpoint Security 将在扫描期间跳过电子邮件格式文件和电子邮件数据库。

“扫描范围”窗口

添加

单击此按钮可打开一个对话框，您可以在其中指定要添加到扫描范围中的文件、文件夹或文件/文件夹掩码。

删除

单击按钮可从扫描范围中删除对象。
如果选中对象旁边的复选框，则此按钮可用。
您不能删除扫描范围中包含的默认对象。

扫描范围

此列包含恶意软件扫描期间扫描的对象。

状态

此列中的切换开关可启用/禁用扫描已添加到扫描范围中的对象。

如果开启该切换开关，则 Kaspersky Endpoint Security 将扫描相应对象。
如果关闭该切换开关，则 Kaspersky Endpoint Security 将不会扫描相应对象。

附加

此列指示 Kaspersky Endpoint Security 是否扫描相应对象的子文件夹。

注意： Kaspersky Endpoint Security 不会扫描位于 OneDrive 或 iCloud 存储或者其他云存储中的文件。请将这些文件排除在扫描范围之外。否则，扫描任务可能会以“*受感染文件未删除*”错误结束。

“添加扫描范围”对话框

输入文件名称、文件夹名称或掩码

文件、文件夹或文件/文件夹掩码的路径。

对象是个文件夹

此复选框启用/禁用对象作为文件夹的扫描。

如果选中此复选框，则 Kaspersky Endpoint Security 会将您在**输入文件名称、文件夹名称或掩码**字段中指定的对象作为文件夹进行扫描。

如果清除此复选框，则 Kaspersky Endpoint Security 会将您在**输入文件名称、文件夹名称或掩码**字段中指定的对象作为文件进行扫描。

默认情况下已选定该选框。

包含子文件夹

此复选框可启用/禁用扫描在**输入文件名称、文件夹名称或掩码**字段中指定的文件夹中的子文件夹。

如果选中此复选框，则 Kaspersky Endpoint Security 在恶意软件扫描过程中将扫描子文件夹。

如果清除此复选框，则 Kaspersky Endpoint Security 在恶意软件扫描过程中将仅扫描直接位于在**输入文件名称、文件夹名称或掩码**字段中指定的文件夹中的文件。

默认情况下已选定该选框。

注意： Kaspersky Endpoint Security 不会扫描位于 OneDrive 或 iCloud 存储或者其他云存储中的文件。请将这些文件排除在扫描范围之外。否则，扫描任务可能会以“*受感染文件未删除*”错误结束。

文件参数窗口

支持以下类型的文件哈希：

- **MD5**
  此类型的哈希必须长 32 个字符，且包含 0-9、a-f、A-F。
- **SHA256**
  此类型的哈希必须长 64 个字符，且包含 0-9、a-f、A-F。