kaspersky

Kaspersky Endpoint Security 14.1 for Windows

© 2026 AO Kaspersky Lab

目录

Kaspersky Endpoint Security for Windows 帮助
- 新功能
- 已修复问题
- 常见问题回答

Kaspersky Endpoint Security for Windows
- 应用程序模式：标准、EDR Agent、Light Agent
- 分发包
- 硬件和软件要求
- 取决于操作系统类型的可用应用程序功能比较
- 根据管理工具比较应用程序功能
- 与其他应用程序的兼容性

安装和删除程序
- 通过 Kaspersky Security Center 部署
  - 应用程序的标准安装
  - 创建安装包
  - 更新安装包中的数据库
  - 创建远程安装任务
- 使用向导在本地安装应用程序
- 使用系统中心配置管理器远程安装应用程序
- setup.ini 文件安装设置说明
- 更改应用程序组件
- 从以前版本的应用程序升级
  - 无需重新启动即可升级应用程序
  - 应用程序的 SMU 更新
- 卸载应用程序

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
- 关于授权许可证书
- 关于订阅
- 关于授权许可密钥
- 关于激活码
- 关于密钥文件
- 根据工作站的授权许可类型比较应用程序功能
- 根据服务器的授权许可类型比较应用程序功能
- 激活应用程序
- 移除授权许可密钥
- 查看授权许可信息
- 购买授权许可
- 续费订阅

入门
- 关于 Kaspersky Endpoint Security for Windows 管理插件
- 使用不同版本的管理插件时的特别考虑

为与外部服务的交互使用加密协议时的特殊考虑
程序界面
任务栏通知区域中的程序图标
简化应用程序界面
配置应用程序界面的显示
准备应用程序以供使用
管理策略
创建策略
策略的导出和导入
安全级别指示器
任务管理
配置本地应用程序设置
启动和停止 Kaspersky Endpoint Security
暂停和恢复计算机保护和控制
创建和使用配置文件
恢复应用程序默认设置
Kaspersky Endpoint Security 的性能以及与其他应用程序的兼容性
启用或禁用节能模式
启用或禁用允许其他应用程序使用资源
优化 Kaspersky Endpoint Security 性能的最佳实践
恶意软件扫描
扫描计算机
扫描连接到计算机的可移动驱动器
后台扫描
从上下文菜单扫描
应用程序完整性检查
编辑扫描范围
运行计划扫描
以其他用户身份运行扫描
扫描优化
更新数据库和程序软件模块
数据库和应用程序模块更新方案
从服务器存储库更新
从共享文件夹更新
使用 Kaspersky 更新实用程序更新
在移动模式下更新
开始和停止更新任务
在不同用户帐户权限下开始更新任务
选择更新任务运行模式
添加更新源
更新应用程序模块
使用代理服务器进行更新
上次更新回滚
高级清除技术
清除工作站上的活动威胁
清除服务器上的活动威胁
消除未处理的威胁

计算机保护
文件威胁防护
启用和禁用文件威胁防护
自动暂停文件威胁防护
更改“文件威胁防护”组件对受感染文件执行的操作
构成“文件威胁防护”组件的保护范围
使用扫描方法
在“文件威胁防护”组件的运行中使用扫描技术
优化文件扫描
扫描复合文件
更改扫描模式
容器扫描
主机入侵防御
启用和禁用主机入侵防御
管理应用程序信任组
更改应用程序的信任组
配置信任组权限
选择在 Kaspersky Endpoint Security 启动之前启动的应用程序受信任组
为未知应用程序选择信任组
为数字签名的应用程序选择信任组
管理应用程序权限
保护操作系统资源和个人数据
删除有关未使用的应用程序的信息
监控主机入侵防御
保护对音频和视频的访问
BadUSB 攻击防护
启用和禁用 BadUSB 攻击防护
使用屏幕键盘授权 USB 设备
条形码扫描器授权
AMSI 保护
启用和禁用 AMSI 保护
通过 AMSI 保护优化文件扫描
Web 威胁防护
启用和禁用 Web 威胁防护
配置恶意网址检测方法
反钓鱼
创建受信任网址列表
导出和导入受信任网址列表
邮件威胁防护
启用和禁用邮件威胁防护
更改对受感染电子邮件采取的操作
构成“邮件威胁防护”组件的保护范围
扫描附加于电子邮件中的复合文件
邮件消息附件过滤器
导出和导入附件过滤的扩展名
扫描 Microsoft Office Outlook 中的电子邮件
在 Thunderbird、MyOffice 和 R7-Office 中扫描电子邮件

网络威胁防护
启用和禁用网络威胁防护
阻止攻击计算机
配置排除在阻止外的地址
导出和导入扩展名排除列表
按类型配置网络威胁防护
防火墙
启用或禁用防火墙
更改网络连接类型
管理网络数据包规则
创建网络数据包规则
启用或禁用网络数据包规则
更改网络数据包规则的防火墙操作
更改网络数据包规则的优先级
导出和导入网络包规则
用 XML 定义网络数据包规则
管理应用程序网络规则
创建应用程序网络规则
启用和禁用应用程序网络规则
更改应用程序网络规则的防火墙操作
更改应用程序网络规则的优先级
网络监控器
漏洞利用防御
启用和禁用漏洞利用防御
系统进程内存保护
行为检测
反加密
启用和禁用共享文件夹对外部加密的防护
配置不受信任的计算机的阻止期限
编辑保护范围
添加受信任的计算机以进行外部数据加密
从共享文件夹对外部加密的防护中导出和导入排除项列表
修复引擎
卡巴斯基安全网络
启用和禁用卡巴斯基安全网络
卡巴斯基私有安全网络的限制
为保护组件启用和禁用云模式
KSN 代理设置
在卡巴斯基安全网络中检查文件信誉
加密连接扫描
启用加密连接扫描
安装受信任根证书
扫描带有不受信任证书的加密连接
将卡巴斯基证书添加到自己的证书存储
从扫描中排除加密连接
擦除数据

计算机控制
Web 控制
添加 Web 资源访问规则
按 Web 资源地址过滤
按 Web 资源内容过滤
测试网页资源访问规则
导出和导入 Web 控制规则
导出和导入 Web 控件规则的 Web 资源地址
监控用户 Internet 活动
编辑 Web 控制消息模板
编辑网页资源地址的掩码
虚拟机的 Web 控制
Web 控制消息模板中的变量
设备控制
关于访问规则
按类型管理设备访问
通过连接总线管理对设备的访问
区分用户对设备的访问权限
管理对移动设备的访问
管理对蓝牙设备的访问
打印控制
Wi-Fi 连接控制
监控可移动驱动器的使用
更改缓存持续时间
对受信任设备的操作
在应用程序界面中向受信任列表添加设备
在 Kaspersky Security Center 中向受信任列表添加设备
导出和导入受信任设备的列表
获取访问被阻止设备的权限
授予访问权限的在线模式
授予访问权限的离线模式
编辑设备控制消息模板
反桥接
启用反桥接
更改连接规则的状态
更改连接规则的优先级
自适应异常控制
训练“自适应异常控制”
启用和禁用自适应异常控制规则
在自适应异常控制规则触发时更改执行的操作
为自适应异常控制规则创建排除项
为自适应异常控制规则导出和导入排除项
更新自适应异常控制规则
编辑自适应异常控制消息模板
监控自适应异常控制操作

应用程序控制
应用程序控制功能限制
接收有关安装在用户计算机上的应用程序的信息
如何启用阻止的应用程序模式
基于基线计算机的应用程序控制
管理应用程序控制规则
为应用程序控制规则添加触发条件
将“可执行文件”文件夹中的可执行文件添加到应用程序类别
将事件相关的可执行文件添加到应用程序类别
添加应用程序控制规则
通过 Kaspersky Security Center 更改应用程序控制规则的状态
导出和导入应用程序控制规则
查看“应用程序控制”组件的运行所产生的事件
查看有关阻止的应用程序的报告
测试应用程序控制规则
启用和禁用应用程序控制规则测试
查看有关测试模式下阻止的应用程序的报告
查看“应用程序控制”组件的测试运行所产生的事件
应用程序活动监控
为文件或文件夹创建名称掩码的规则
编辑应用程序控制消息模板
应用程序控制消息模板中的变量
允许的应用程序列表的最佳实践
为应用程序配置允许列表模式
而是允许列表模式
支持允许列表模式
网络端口监控
启用对所有网络端口的监控
创建受监控网络端口的列表
创建所有网络端口受监控的应用程序的列表
导入和导入受监控端口列表
日志审查
配置预定义规则
添加自定义规则
系统完整性监控
关于系统完整性监控规则
实时系统完整性监控
按需系统完整性检查
导出和导入系统完整性监控规则
查看系统完整性监控报告
系统完整性状态重置
云发现
信任区域
创建扫描排除项
按检测到的对象类型创建排除项
编辑受信任应用程序列表
创建本地受信任区域

- 导出和导入受信任域
- 使用受信任数字签名处理应用程序
- 附录。预定义的扫描排除项和受信任的应用程序
  - SQL 服务器
  - Microsoft Exchange 服务器
  - System Center Configuration Manager
  - Citrix
  - VMware
- 管理备份
  - 配置备份区中的文件的最长存储期
  - 配置备份区的最大大小
  - 从备份区中还原文件
  - 从备份区中删除文件备份副本
- 通知服务
  - 配置事件日志设置
  - 配置通知的显示和传送
  - 配置应用程序状态警告在通知区域的显示
  - 用户和管理员之间的消息传递
- 管理报告
  - 查看报告
  - 配置最大报告存储时间
  - 配置报告文件的最大大小
  - 将报告保存到文件
  - 清理报告
- Kaspersky Endpoint Security 自我保护
  - 启用和禁用自我防御
  - 启用和禁用 AM-PPL 支持
  - 针对外部管理对应用程序服务的保护
  - 支持远程管理应用程序
  - 密码保护
    - 启用密码保护
    - 为单个用户或组授予权限
    - 使用临时密码授予权限
    - 撤销临时密码
    - 密码保护权限的特殊方面
    - 重置 KLAdmin 密码
  - 管理服务器连接保护
- 数据加密
  - 加密功能限制
  - 更改加密密钥的长度 (AES56 / AES256)
  - 卡巴斯基磁盘加密
    - SSD 驱动器加密的特殊功能
    - 启动卡巴斯基磁盘加密
    - 创建硬盘驱动器加密排除列表
    - 导出或导入从加密范围中排除的硬盘驱动器列表
    - 启用单点登录 (SSO) 技术
    - 管理身份验证代理帐户

- 配合身份验证代理使用令牌和智能卡
- 硬盘驱动器解密
- 还原对受卡巴斯基磁盘加密技术保护的驱动器的访问权限
- 使用身份验证代理服务账户登录
- 更新操作系统
- 消除加密功能更新的错误
- 跟踪身份验证代理
- 编辑身份验证代理帮助文本
- 测试身份验证代理的操作后，删除剩余的对象和数据
- BitLocker 管理
  - 启动 BitLocker 驱动器加密
  - 解密受 BitLocker 保护的硬盘驱动器
  - 恢复对 BitLocker 保护的驱动器的访问权限
  - 暂停 BitLocker 保护以更新软件
- 本地计算机驱动器上的文件级加密
  - 加密本地计算机磁盘驱动器上的文件
  - 为应用程序创建加密文件访问规则
  - 加密特定应用程序创建或修改的文件
  - 生成解密规则
  - 在本地计算机磁盘驱动器上解密文件
  - 创建加密数据包
  - 还原对加密文件的访问权限
  - 操作系统故障后恢复对加密数据的访问
  - 编辑加密文件访问消息模板
- 可移动驱动器加密
  - 启动可移动驱动器加密
  - 为可移动驱动器添加加密规则
  - 为可移动驱动器导出和导入加密规则列表
  - 用于访问可移动驱动器上的加密文件的便携模式
  - 可移动驱动器解密
- 查看数据加密详细信息
  - 查看加密状态
  - 在 Kaspersky Security Center 信息显示板上查看加密统计信息
  - 查看本地计算机驱动器上文件加密错误
  - 查看数据加密报告
- 无法访问加密设备时的设备使用
  - 使用 FDERT 恢复实用程序恢复数据
  - 创建操作系统紧急修复磁盘
- Detection and Response 解决方案
  - MDR 和 EDR Optimum 授权许可
  - 与第三方 EDR 解决方案的兼容性
  - Kaspersky Endpoint Agent
    - 迁移 [KES+KEA] 配置到 [KES+内置代理] 配置
    - Kaspersky Endpoint Agent 的策略和任务迁移
  - Endpoint Detection and Response Agent (EDR Agent)
    - 安装 EDR Agent
    - 将 EDR Agent 与 MDR 集成

- 将 EDR Agent 与 EDR（KATA）集成
- 将 EDR Agent 与 NDR（KATA）集成
- 将 EDR Agent 与 EDR Expert (on-premises) 集成
- 与第三方 EPP 应用程序的兼容性

Managed Detection and Response
- 内置代理与 MDR 的集成
- MDR 的 KEA 到 KES 迁移指南

Endpoint Detection and Response
- 内置代理与 EDR Optimum / EDR Expert 的集成
- 妥协的指标扫描（标准任务）
- IOC 扫描的扩展遥测
- 移动文件到隔离区
- 获取文件
- 删除文件
- 进程启动
- 终止进程
- 执行防护
- 计算机网络隔离
- Cloud Sandbox
- EDR Optimum 的 KEA 到 KES 迁移指南

Kaspersky Sandbox
- 内置代理与 Kaspersky Sandbox 的集成
- 妥协的指标扫描（独立任务）
- Kaspersky Sandbox 的 KEA 到 KES 迁移指南

Kaspersky Anti Targeted Attack Platform
- 内置代理与 EDR / NDR（KATA）的集成
- 配置 EDR (KATA)遥测
- EDR (KATA) 遥测排除项
  - 例 1。排除的进程
  - 例 2。排除的网络通信
  - 例 3。排除的文件操作
  - 例 4。排除的注册表修改
- KATA Sandbox
  - 内置代理与 KATA Sandbox 的集成
  - 配置威胁响应操作
- EDR (KATA) 的 KEA 到 KES 迁移指南

Endpoint Detection and Response Expert（本地部署）
- 内置代理与 EDR Expert (on-premises) 的集成
- 配置 EDR Expert (on-premises) 遥测设置
- EDR Expert (on-premises) 遥测排除项
- 导出和导入 EDR Expert (on-premises) 事件过滤器
- 使用策略配置文件配置与 EDR Expert（(on-premises)和 EDR (KATA) 集成时的特殊注意事项

Endpoint Detection and Response Expert (cloud)
- 内置代理与 EDR Expert (cloud) 的集成
- 配置 EDR Expert (cloud) 遥测设置
- EDR Expert (cloud) 遥测排除项
- 导出和导入 EDR Expert (cloud) 事件过滤器

管理隔离
配置最大隔离区大小
发送有关隔离文件的数据到 Kaspersky Security Center
从隔离区中恢复文件
监控 EDR 操作
Kaspersky Unified Monitoring and Analysis Platform (KUMA)
Kaspersky Endpoint Security 与 KUMA 的集成
过滤要发送到 KUMA 的事件
导出和导入 KUMA 事件过滤器
KSWS 到 KES 的迁移指南
KSWS 和 KES 组件的对应关系
KSWS 和 KES 设置的对应关系
迁移 KSWS 组件
迁移 KSWS 任务和策略
迁移 KSWS 受信任区域
迁移 KSWS 应用程序启动控制规则
安装 KSWS 而不是 KES
迁移 [KSWS+KEA] 配置到 [KES+内置代理] 配置
确保已成功卸载 Kaspersky Security for Windows Server
使用 KSWS 密钥激活 KES
迁移高负载服务器的特殊注意事项
在 Server Core 模式下管理服务器上的应用程序
迁移 [KSWS+KEA] 到 [KES+内置代理]
用于保护虚拟机的 Light Agent 模式
Light Agent 模式的特殊注意事项
虚拟机的初步配置
与 Citrix App Layering 技术的兼容性
与 Citrix Provisioning（Citrix Provisioning Services）技术的兼容性
与 Omnissa App Volumes 技术的兼容性
安装 Light Agent
将 Light Agent 连接至 SVM
SVM 发现
为 Light Agent 配置 SVM 选择算法
将 Light Agent 的连接分发到 SVM（标签）
保护 Light Agent 和 SVM 之间的连接
激活 Light Agent
KSVLA Light Agent 至 KES Light Agent 迁移指南
安装 KES Light Agent 而不是 KSVLA Light Agent
KSVLA Light Agent 与 KES Light Agent 组件对应关系
迁移 KSVLA Light Agent 任务和策略
迁移 [KSVLA Light Agent+KEA] 配置到 [KES Light Agent+内置代理] 配置
从命令行管理应用程序
Setup。安装应用程序
Setup /x。卸载应用程序
msiexec /i。恢复应用程序

AVP 命令
- SCAN。恶意软件扫描
- UPDATE。更新数据库和程序软件模块
- ROLLBACK。上次更新回滚
- TRACES。跟踪
- START。启动配置文件
- STOP。停止配置文件
- STATUS。配置文件状态
- STATISTICS。配置文件操作统计
- RESTORE。从备份区中还原文件
- EXPORT。导出应用程序设置
- IMPORT。导入应用程序设置
- ADDKEY。应用密钥文件
- LICENSE。授权许可
- RENEW。购买授权许可
- PBATESTRESET。在加密磁盘之前重置磁盘检查结果
- EXIT。退出应用程序
- EXITPOLICY。禁用策略
- STARTPOLICY。启用策略
- DISABLE。禁用保护
- SPYWARE。间谍软件检测
- KSN。在 KSN / KPSN 之间切换
- SERVERBINDINGDISABLE。禁用服务器连接保护

KESCLI 命令
- SCAN。恶意软件扫描
- GetScanState。扫描完成状态
- GetLastScanTime。决定扫描完成时间
- GetThreats。获取检测到的威胁的数据
- UpdateDefinitions。更新数据库和程序软件模块
- GetDefinitionState。确定数据库上次更新的日期和时间
- EnableRTP。启用保护
- GetRealTimeProtectionState。“文件威胁防护”状态
- GetEncryptionState。磁盘加密状态
- Version。识别应用程序版本

Detection and Response 管理命令
- SANDBOX。管理 Sandbox
- PREVENTION。管理执行防护
- ISOLATION。管理网络隔离
- RESTORE。从隔离区中恢复文件
- IOCSCAN。妥协的指标 (IOC) 扫描
- MDRLICENSE。MDR 激活
- EDRKATA。与 EDR（KATA）集成
- KUMA。与 KUMA 的整合
- YARA。运行 YARA 扫描
- TELEMETRYFILTERS。过滤要发送到 KUMA 的事件

Light Agent 管理命令
KSVLAINFO。确定 Light Agent 模式
VIISINFO。Light Agent 与 Integration Server 的连接状态
SVMINFO。Light Agent 与 Protection Server 的连接状态
错误代码
附录。应用程序配置文件
通过 REST API 管理应用程序
使用 REST API 安装应用程序
使用 API
关于应用程序的信息源
联系技术支持
跟踪文件的内容和存储
应用程序操作跟踪
应用程序性能跟踪
转储写入
保护转储文件和跟踪文件
获取操作系统数据（Kaspersky Get System Info）
限制和警告
术语表
Integration Server
IOC
IOC 文件
Kerberos 身份验证
Light Agent
OLE 对象
OpenIOC
SVM
云发现
任务
便携式文件管理器
保护范围
反病毒数据库
受信任平台模块
受感染的文件
可疑网址的数据库
存档
已感染文件
扫描范围
授权许可证书
掩码
活动密钥
清除
管理组
网络代理
网页资源地址的规范化格式
证书发布者
误报

身份验证代理
钓鱼网页地址数据库
附录
附录 1.应用程序设置
文件威胁防护
Web 威胁防护
邮件威胁防护
网络威胁防护
防火墙
BadUSB 攻击防护
AMSI 保护
漏洞利用防御
行为检测
主机入侵防御
修复引擎
卡巴斯基安全网络
日志审查
反加密
Web 控制
设备控制
应用程序控制
自适应异常控制
系统完整性监控
Endpoint Sensor
Sandbox
Managed Detection and Response
Endpoint Detection and Response
Endpoint Detection and Response Expert（本地部署）
Network Detection and Response（KATA）
与 KUMA 的整合
完整磁盘加密
文件级加密
可移动驱动器加密
模板（数据加密）
排除
应用程序设置
报告和存储
网络设置
界面
管理设置
更新数据库和程序软件模块
附录 2.应用程序信任组
附录 3.快速可移动驱动器扫描的文件扩展名
附录 4.邮件威胁防护附件过滤的文件类型
附录 5.与外部服务交互的网络设置

附录 6.应用程序事件
严重
功能失败
警告
信息性消息
附录 7.执行防护支持的文件扩展名
附录 8.执行防护预防的脚本解释器
附录 9.注册表中的 IOC 扫描范围 (RegistryItem)
附录 10.IOC 文件需求
附录 11.EDR 威胁响应 API
附录 12.应用程序组件规则中的用户账户
法律信息
数据提供
在最终用户授权许可协议下的数据提供
使用卡巴斯基安全网络时的数据提供
使用 Detection and Response 解决方案时的数据提供
Kaspersky Endpoint Detection and Response
Kaspersky Sandbox
Kaspersky Endpoint Detection and Response Expert（本地部署）
Kaspersky Network Detection and Response (KATA)
与 Kaspersky Unified Monitoring and Analysis Platform (KUMA) 集成
与欧盟立法兼容(GDPR)
商标通知
有关第三方代码的信息

Kaspersky Endpoint Security for Windows 帮助

新功能

更新 14.1

Kaspersky Endpoint Security 14.1 for Windows 引入了以下功能和改进：

1. 已添加对 Windows Server 2025 操作系统的支持。

2. Endpoint Detection and Response Expert (on-premises) 和 Kaspersky Endpoint Detection and Response Expert (cloud) 的遥测事件过滤规则数量限制已增加。Kaspersky Endpoint Security 现在总共支持多达 10,000 条包含和排除过滤规则。

3. 现在您可以将任务配置为仅在一周的特定日期运行，并按指定的周间隔运行。计划功能在 Kaspersky Security Center 16.1 或更高版本中提供。

4. 对于“*恶意软件扫描*”任务，您现在可以指定任务暂停的时间间隔，例如，为了在负载增加期间最大限度地减少对计算机性能的影响。

5. 通过减少 I/O 操作次数，优化了受保护计算机上硬盘子系统的性能。

6. 在开发此版本的 Kaspersky Endpoint Security 时，我们纳入了以下私人补丁中包含的更改：PF14061、PF14062、PF14064、PF14065、PF14069、PF14070、PF14071、PF15054、PF15056、PF15058、PF15062、PF15063、PF15064、PF16052、PF16053、PF16055、PF16056、PF16057、PF16060、PF16061、PF16062、PF17027、PF17029、PF17039、PF17041、PF17043、PF17048、PF17050、PF17051、PF17053、PF17054、PF17060、PF18010、PF18011、PF18014、PF18015、PF18020、PF18021、PF18022、PF18023、PF18024、PF18028、PF18031、PF18032、PF18043、PF18050、PF18051、PF18053、PF18057、PF19003、PF19016、PF19018、PF19017、PF19032、PF19034、PF19036、PF19037、PF19041、PF19043、PF19049、PF19051、PF19055、PF19056、PF19065、PF20011、PF20016、PF20017、PF20020、PF20021、PF20033、PF20036、PF20038、PF20039、PF20049、PF20052、PF20055、PF20060、PF20065、PF20078、PF20080、PF20081、PF21007、PF21010、PF21019、PF21021、PF21024、PF21026、PF21040、PF21058、PF21062、PF21063、PF22004、PF22008、PF22014、PF22027、PF22036、PF22049、PF22053、PF22056、PF22059、PF23022、PF23026、PF23029、PF23031、PF23039、PF23049、PF23063、PF24005、PF24011、PF24013、PF24014、PF24017、PF24019、PF25013、PF25016、PF25019。

更新 14.0

Kaspersky Endpoint Security 14.0 for Windows 引入了以下功能和改进：

1. 现在支持基于 Arm 架构的计算机。您可以以标准模式或 EDR Agent 模式安装该应用程序。但是，该应用程序存在一些局限性（例如，在数据加密技术中，仅支持 BitLocker）。

2. Kaspersky Security Center Web Console 15.0 或更高版本支持扩展策略审核。现在您可以查看策略修订和将它们保存到文件中。一个*修订*是用户保存的一组修改后的参数。修订允许您比较和恢复策略参数的更改。

3. Kaspersky Endpoint Detection and Response 用户现在可以获取新的遥测事件。这些新事件增强了 Kaspersky EDR 解决方案的威胁检测能力。

4. 在开发此版本的 Kaspersky Endpoint Security for Windows 时，我们纳入了以下私人补丁中包含的更改：PF13115、PF13118、PF13119、PF13120、PF13123、PF13124、PF14061、PF14062、PF14064、PF14065、PF14069、PF14070、PF15054、PF15056、PF15058、PF15062、PF15063、PF15064、PF16052、PF16053、PF16055、PF16056、PF16057、PF16060、PF16061、PF16062、PF17027、PF17029、PF17039、PF17041、PF17043、PF17048、PF17050、PF17051、PF17053、PF17054、PF17060、PF18010、PF18011、PF18014、PF18015、PF18020、PF18021、PF18022、PF18023、PF18024、PF18028、PF18031、PF18032、PF18043、PF18050、PF18051、PF18053、PF19003、PF19016、PF19018、PF19017、PF19032、PF19034、PF19036、PF19037、PF19041、PF19043、PF19049、PF19051、PF19055、PF19056、PF19065、PF20011、PF20016、PF20017、PF20020、PF20021、PF20033、PF20036、PF20038、PF20039、PF20049、PF20052、PF20055、PF20060、PF20065、PF20078、PF20080、PF21007、PF21010、PF21019、PF21021、PF21024、PF21026、PF21040、PF21058、PF22004、PF22008、PF22014、PF22027、PF22036、PF22049、PF22053、PF22056、PF23022、PF23026、PF23029、PF23031、PF23039、PF23049、PF24005、PF24011。

更新 12.12

Kaspersky Endpoint Security 12.12 for Windows 引入了以下功能和改进：

1. 以前作为行为检测组件一部分的共享文件夹对外部加密的保护功能，现在已成为一个独立的组件，反加密。

2. 已添加对 Kerberos 协议的支持，以便通过用于互联网访问的代理服务器对应用程序进行身份验证。

3. 现在您可以为受信任应用程序，而不仅仅是完整路径指定文件哈希值了。

4. Endpoint Detection and Response (EDR) 解决方案的用户可以使用更多的 *IOC 扫描*任务功能。回顾性 IOC 扫描功能现已可用。*回顾性 IOC 扫描*是 *IOC 扫描* 任务的一种模式，在该模式下，Kaspersky Endpoint Security 使用特定时间段的数据扫描入侵指标。此模式旨在检测计算机网络活动数据中的入侵指标。Kaspersky Endpoint Security 分析计算机上的操作系统日志和浏览器日志中的数据。

5. Kaspersky Endpoint Detection and Response (EDR) 的用户可以移除隔离区大小限制。这对于 YARA 扫描来说可能是必要的，因为该应用程序可能会保存一个大的内存转储文件。现在您可以将所有可用磁盘空间用于隔离。

6. 现在支持 HTTPS 压缩，以优化将事件导出到 Kaspersky Unified Monitoring and Analysis Platform (KUMA)。这有助于减少传出流量。

7. 在开发此版本的 Kaspersky Endpoint Security for Windows 时，我们纳入了以下私人补丁中包含的更改：PF13115、PF13118、PF13119、PF13120、PF13123、PF13124、PF14061、PF14062、PF14064、PF14065、PF14069、PF14070、PF15054、PF15056、PF15058、PF15062、PF15063、PF15064、PF16052、PF16053、PF16055、PF16056、PF16057、PF16060、PF16061、PF16062、PF17027、PF17029、PF17039、PF17041、PF17043、PF17048、PF17050、PF17051、PF17053、PF17054、PF17060、PF18010、PF18011、PF18014、PF18015、PF18020、PF18021、PF18022、PF18023、PF18024、PF18028、PF18031、PF18032、PF18043、PF18050、PF18051、PF18053、PF19003、PF19016、PF19018、PF19017、PF19032、PF19034、PF19036、PF19037、PF19041、PF19043、PF19049、PF19051、PF19055、PF19056、PF19065、PF20011、PF20016、PF20017、PF20020、PF20021、PF20033、PF20036、PF20038、PF20039、PF20049、PF20052、PF20055、PF20060、PF20065、PF20078、PF20080、PF21007、PF21010、PF21019、PF21021、PF21024、PF21026、PF21040、PF21058、PF22004、PF22008、PF22014、PF22027、PF22036、PF22049、PF22053、PF22056、PF23022、PF23026、PF23029、PF23031、PF23039、PF23049、PF24005、PF24011。

更新 12.11

Kaspersky Endpoint Security 12.11 for Windows 提供了以下功能和改进：

1. 应用程序在保存设置之前会检查控制组件的配置。增加了对应用程序控制、设备控制、系统完整性监控组件的检查。如果控制组件的当前设置可能会增加计算机负载或导致系统故障，应用程序会显示警告。例如，在应用程序控制的情况下，如果您选择了阻止除允许的应用程序之外的所有应用程序的模式，并且您没有添加任何允许规则，则应用程序会显示警告，因为这样的配置可能会导致系统故障。

2. 增加了自动将文件提交至 KATA Sandbox 进行审核的支持。*KATA Sandbox* 是 Kaspersky Anti Targeted Attack Platform 的一个组件，在操作系统的虚拟映像上运行文件。Sandbox 分析对象行为，以检测恶意活动和针对组织 IT 基础设施的攻击的活动特征。Sandbox 使用部署的 Microsoft Windows 操作系统虚拟映像（Sandbox 服务器）分析和扫描特殊服务器上的对象。为了使 KATA Sandbox 以自动模式运行，必须部署 Kaspersky Anti Targeted Attack Platform 8.0 或更高版本。

3. 优化了 EDR 遥测发送。现在您可以指定最大数据包长度。

4. 改进了卡巴斯基安全网络连接诊断。扩展了卡巴斯基安全网络的连接错误详细信息以解决潜在问题。

5. 增加了对配置要发送到 Kaspersky Unified Monitoring and Analysis Platform (KUMA) 的事件列表的支持。现在，除了 KUMA 中的预定义事件列表之外，您还可以手动将事件添加到遥测中，或者通过 Windows 事件日志中的 ID 排除事件。

6. 更新了 Web Console 中的策略界面。策略部分的布局已经改变，以便更快地访问基本功能。

7. 支持 Windows 11 25H2。

8. 在开发此版本的 Kaspersky Endpoint Security for Windows 时，我们纳入了以下私人补丁中包含的更改：PF13115、PF13118、PF13119、PF13120、PF13123、PF13124、PF14061、PF14062、PF14064、PF14065、PF14069、PF14070、PF15054、PF15056、PF15058、PF15062、PF15063、PF15064、PF16052、PF16053、PF16055、PF16056、PF16057、PF16060、PF16061、PF16062、PF17027、PF17029、PF17039、PF17041、PF17043、PF17048、PF17050、PF17051、PF17053、PF17054、PF18010、PF18011、PF18014、PF18015、PF18020、PF18021、PF18022、PF18023、PF18024、PF18028、PF18031、PF18032、PF18043、PF18050、PF18051、PF18053、PF19003、PF19016、PF19018、PF19017、PF19032、PF19034、PF19036、PF19037、PF19041、PF19043、PF19049、PF19051、PF19055、PF19056、PF20011、PF20016、PF20017、PF20020、PF20021、PF20033、PF20036、PF20038、PF20039、PF20049、PF20052、PF20055、PF20060、PF20065、PF21007、PF21010、PF21019、PF21021、PF21024、PF21026、PF22004、PF22008、PF22014。

更新 12.10

Kaspersky Endpoint Security 12.10 for Windows 提供了以下功能和改进：

1. 对于 BadUSB 攻击防护组件，已添加通过从屏幕上读取条形码来授权条形码扫描器的选项。现在您无需使用屏幕键盘输入代码来授权条形码扫描器。

2. 卡巴斯基的 Endpoint Detection and Response (EDR) 解决方案的用户可以使用以下功能和改进：

   - 现在您可以在警报详细信息中管理计算机的网络隔离。此外，您可以在警报详细信息中指定计算机网络隔离时间段并添加排除项。

   - 使用新数据填写警报详细信息。现在警报详细信息包含有关威胁的更多信息，包括应用程序在响应 EDR 威胁时的行为方式。

   - IOC 文件处理已得到改进。现在您可以在 Kaspersky Security Center Web Console 界面中查看和编辑 IOC 文件的内容。加载 IOC 文件后，应用程序将显示有关 IOC 术语应用程序的报告。

   - 改进了对检测到的 IOC 的响应。现在，您可以在任务属性中的 IOC 检测结果中直接隔离 *IOC 扫描*任务检测到的文件。您还可以在任务属性中将计算机与网络隔离。

   - 现在，您可以直接在 *IOC 扫描*任务的属性中根据 TXT 文件中生成的文件哈希、IP 地址或 DNS 名称列表创建 IOC 文件。

   - 扩大 *IOC 扫描*任务的扫描范围。现在您可以为注册表的 IOC 扫描定义一个范围（**Windows 注册表 – RegistryItem**）。在应用程序的早期版本中，您只能使用注册表中预定义的 IOC 扫描范围。

3. 添加了新的密码保护权限，*导出设置*。默认情况下，只有 KLAdmin 用户可以在应用程序界面中创建带有 Kaspersky Endpoint Security 设置的配置文件。要授予其他用户访问权限，您需要授予他们相应的权限。

4. 在开发此版本的 Kaspersky Endpoint Security for Windows 时，我们纳入了以下私人补丁中包含的更改：PF12120、PF12121、PF12122、PF13115、PF13118、PF13119、PF13120、PF13123、PF14061、PF14062、PF14064、PF14065、PF15054、PF15056、PF15058、PF15062、PF16052、PF16053、PF16055、PF16056、PF16057、PF17027、PF17029、PF17039、PF17041、PF17043、PF17048、PF17050、PF18010、PF18011、PF18014、PF18015、PF18020、PF18021、PF18022、PF18023、PF18024、PF18028、PF18031、PF18032、PF18043、PF19003、PF19016、PF19018、PF19017、PF19032、PF19034、PF19036、PF19037、PF19041、PF19043、PF19049、PF20011、PF20016、PF20017、PF20020、PF20021、PF20033、PF20036、PF20038、PF20039、PF20049、PF21007。

更新 12.9

Kaspersky Endpoint Security 12.9 for Windows 提供了以下功能和改进：

1. *管理临时密码*的新功能已添加。临时密码允许您为单独的启用了密码保护的计算机提供对 Kaspersky Endpoint Security 的访问权限。临时密码管理允许保存密码历史记录（最多 30 天）、监控临时密码状态（*活动*、*已过期*、*已撤销*）和撤销临时密码。

2. 添加了应用策略后立即终止与 Web 控制规则禁止的 Web 资源的连接的选项。在应用程序的先前版本中，Web 控制仅限制与禁止的 Web 资源的新连接。

3. 对于 Kaspersky Anti Targeted Attack Platform 用户，已添加在计算机上本地运行 YARA 检查的选项。为此，您需要下载一个包含 YARA 规则的文件并在 CMD 中执行命令。

4. 修复了在驱动器已使用第三方工具由 BitLocker 进行保护的计算机上启用 BitLocker 时应用程序的行为。Kaspersky Endpoint Security 启动恢复程序，将恢复密钥发送至 Kaspersky Security Center。因此，BitLocker 管理被转移到 Kaspersky Security Center 控制台。

5. 一个新的部分，**响应历史**，可供卡巴斯基 Detection and Response 解决方案的用户使用。本节包含有关在计算机上执行的威胁响应操作的信息。这些操作包括，例如，运行"*终止进程*"任务或者将计算机与网络隔离。响应历史记录仅适用于以下卡巴斯基解决方案的用户：MDR、EDR、KATA。

6. 对于 Kaspersky Unified Monitoring and Analysis Platform 用户，现已推出支持 EDR 威胁响应操作。在应对威胁时，KUMA 会运行创建相应 EDR 任务的脚本。要执行 EDR 任务，您需要在 KUMA 控制台中为自定义脚本创建响应规则并选择事件。

7. 在开发此版本的 Kaspersky Endpoint Security for Windows 时，我们纳入了以下私人补丁中包含的更改：PF10360、PF10362、PF10363、PF12120、PF12121、PF12122、PF13115、PF13118、PF13119、PF14061、PF14062、PF14064、PF14065、PF15054、PF15056、PF15058、PF16052、PF16053、PF16055、PF16056、PF17027、PF17029、PF17039、PF17041、PF17043、PF18010、PF18011、PF18014、PF18015、PF18020、PF18021、PF18022、PF18023、PF18024、PF18028、PF19003、PF19016、PF19018、PF19017、PF19032、PF19034、PF19036、PF19037、PF19041、PF20011、PF20016、PF20017、PF20020、PF20021。

更新 12.8

Kaspersky Endpoint Security 12.8 for Windows 提供了以下功能和改进：

1. 应用程序现在支持用于保护虚拟环境的 Light Agent 模式。现在，您可以将应用程序部署为 Light Agent，作为 Kaspersky Security for Virtualization Light Agent 6.2 解决方案的一部分。

2. 现已支持拦截服务器上 Docker 容器中的文件操作。*容器*是一个隔离的环境，应用程序可以在其中运行而无需与操作系统直接交互。Kaspersky Endpoint Security 扫描用户可以访问的容器内的文件。当检测到威胁时，应用程序会阻止此恶意活动并尝试对容器内的文件进行清除。如果无法清除该文件，应用程序将停止该容器。

3. 现在您可以定义一个保护范围，以保护共享文件夹免受外部加密（行为检测组件）。现在您可以指定应用程序必须监控文件活动的共享文件夹。您还可以将文件排除在保护范围之外。在应用程序的先前版本中，行为检测组件监控所有共享文件夹中的文件活动。

4. 现在您可以在安装包中为不同类型的操作系统配置不同的组件集。也就是说，您可以使用相同的安装包部署应用程序到工作站和服务器。特定操作系统类型不可用的组件将被自动从安装包属性中排除。

5. 添加了选择预定义扫描排除项和受信任的应用程序的选项。预定义的扫描排除项和受信任的应用程序允许在虚拟环境（Citrix、VMware）中快速为应用程序配置受信任区域。此类排除项包括 VHD 和 VHDX 虚拟机文件。可以在创建应用程序安装包、创建策略或安装 Kaspersky Endpoint Security 时添加排除项。

6. EDR 遥测数据现在包括与通过 USB 连接的设备相关的操作事件。您还可以将这些事件添加到 EDR 遥测数据的排除项中。

7. 添加了阻止通过过时的 TLS 1.0 协议建立网络连接的选项。TLS 1.0 的安全级别较低，因此推荐禁用该协议并使用较新的 TLS 1.2 或 TLS 1.3 版本。默认情况下，Kaspersky Endpoint Security 会阻止 TLS 1.0 连接。更新应用程序版本后，使用 TLS 1.0 协议的第三方服务运行可能会失败。为了避免第三方服务运行出现问题，您可以在更新应用程序版本之前在组策略中允许使用 TLS 1.0 协议。

8. 在开发此版本的 Kaspersky Endpoint Security for Windows 时，我们纳入了以下私人补丁中包含的更改：PF10053、PF10054、PF10360、PF10362、PF10363、PF12120、PF12121、PF12122、PF13115、PF13118、PF13119、PF14061、PF14062、PF14064、PF14065、PF15054、PF15056、PF15058、PF16052、PF16053、PF16055、PF16056、PF17027、PF17029、PF17039、PF17041、PF17043、PF18010、PF18011、PF18014、PF18015、PF18020、PF18021、PF18022、PF18023、PF18024、PF18028、PF19003、PF19016、PF19018。

更新 12.7

Kaspersky Endpoint Security 12.7 for Windows 提供了以下功能和改进：

1. 现在您可以限制用于*恶意软件扫描*任务的 CPU 资源使用量。为此，在应用程序设置中，指定扫描计算机时可利用的所有内核的最大 CPU 负载百分比。

2. 现在您可以手动发送文件以在 KATA Sandbox 中扫描。*KATA Sandbox* 是 Kaspersky Anti Targeted Attack Platform 的一个组件，在操作系统的虚拟映像上运行文件。Sandbox 分析对象行为，以检测恶意活动和针对组织 IT 基础设施的攻击的活动特征。Sandbox 使用部署的 Microsoft Windows 操作系统虚拟映像（Sandbox 服务器）分析和扫描特殊服务器上的对象。要将文件发送到 KATA Sandbox 进行扫描，请在文件的上下文菜单中选择相关命令。

3. 现在，您可以设置与保护企业局域网的解决方案的集成， *Kaspersky Network Detection and Response*。Kaspersky Network Detection and Response (NDR) 是 Kaspersky Anti Targeted Attack Platform 的一部分。您可以在标准模式以及 EDR Agent 模式下配置与 NDR 的交互。

4. 邮件威胁防护扩展程序中已添加对 Microsoft Office Outlook 电子邮件客户端版本 2021 的支持。该扩展程序允许在邮件客户端级别而不是协议级别扫描邮件。除了消息之外，该扩展程序还允许您扫描通过 MAPI 接口从 Microsoft Exchange 存储库接收的对象（例如，日历中的对象）。此扫描在邮件客户端中进行。

5. 在开发此版本的 Kaspersky Endpoint Security for Windows 时，我们纳入了以下私人补丁中包含的更改：PF10049、PF10355、PF12114、PF13109、PF14056、PF15038、PF15045、PF16037、PF16042、PF16047、PF17014、PF17018、PF17021、PF17024、PF18006、PF18007。

更新 12.6

Kaspersky Endpoint Security 12.6 for Windows 提供了以下功能和改进：

1. 与卡巴斯基 SIEM 解决方案集成的功能 （*Kaspersky Unified Monitoring and Analysis Platform*；*KUMA*）已添加。现在可以将事件从 Windows 事件日志发送到 KUMA 收集器。这使得 KUMA 可以从安装了 Kaspersky Endpoint Security 的所有计算机接收 Windows 事件（支持一组有限的 EventID），而无需在这些计算机上安装 KUMA 代理。

2. 添加了新的*系统完整性监控*组件来取代文件完整性监控组件。系统完整性监控组件包括文件完整性监控的所有功能，另外还允许监控注册表更改和外部设备的连接。系统完整性监控组件监控操作系统中可能预示计算机安全漏洞的变化。当检测到此类变化时，Kaspersky Endpoint Security 会生成相应的事件并向管理员发出警报。文件完整性监控不再是该应用程序的一部分。当您更新应用程序时，文件完整性监控设置会自动迁移到系统完整性监控。为了确保系统完整性监控正常运行，Kaspersky Endpoint Security 应用程序和管理插件都应更新至 12.6 版本。

3. 已安装的内置 EDR Agent (KATA) 的状态已添加到 Kaspersky Security Center 控制台中的计算机属性中。现在，如果您安装了内置 EDR Agent (KATA)，"**Endpoint Sensor 状态**"列显示组件的当前状态（例如，*正在运行*、*已停止*、*不受授权许可支持*）。

4. 添加了选择预定义扫描排除项和受信任的应用程序的选项。预定义扫描排除项和受信任的应用程序有助于在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上使用应用程序时快速配置受信任区域。此类排除项包括 MDF 和 LDF 数据库文件。可以在创建新策略、修改现有策略或安装 Kaspersky Endpoint Security 时添加排除项。

5. Kaspersky Endpoint Detection and Response Optimum 的警报详细信息显示已从 Kaspersky Endpoint Security 管理插件移至单独的 Kaspersky Endpoint Detection and Response 管理插件。EDR 管理插件是一个用于与 Windows、Mac 和 Linux 操作系统上的代理协同工作的单一插件。现在，当使用 EDR Optimum 时，您将需要 Kaspersky Endpoint Security 管理插件来创建威胁响应任务，以及 EDR 管理插件来查看警报详细信息。

6. 支持 Windows 11 24H2。

7. 在开发此版本的 Kaspersky Endpoint Security for Windows 时，我们纳入了以下专用补丁中包含的更改：pf10048、pf10353、pf12106、pf12107、pf12108、pf13090、pf13100、pf15031、pf15034、pf15036、pf16021、pf16023、pf16029、pf17002。

更新 12.5

Kaspersky Endpoint Security 12.5 for Windows 提供了以下功能和改进：

1. 添加了配置遥测排除项的选项。*遥测*是受保护计算机上发生的事件的列表。Kaspersky Anti Targeted Attack Platform (EDR) 使用遥测数据来监控和保护组织的 IT 基础设施。配置遥测排除项帮助提高计算机性能并优化到遥测采集服务器的数据传输。

2. 应用程序信任区域的界面已得到改进。如果管理员禁止用户添加自己的（本地）扫描排除项和受信任应用程序，Kaspersky Endpoint Security 现在会对用户隐藏受信任区域对象。这可以防止入侵者对受信任区域进行未经授权的访问，从而提高计算机安全级别。

3. 添加了扫描 MyOffice Mail 和 R7-Office Organizer 邮件客户端流量的选项。邮件威胁防护组件现在不仅在下载时扫描邮件附件，还扫描发送和接收的邮件。

4. Web 资源的新类别"*生成型 AI 工具*"已添加。您可以使用 Web 控制配置对新类别网站的访问。

5. 现在您可以在防火墙列表中选择网络数据包规则的位置。网络数据包规则在列表中的位置决定其优先级。在应用程序的早期版本中，新规则只能添加到列表末尾，之后您必须手动在列表中移动规则以确定其优先级。现在，添加规则时，您可以选择是否将该规则放置在列表的开头、末尾或所选规则的旁边。

6. 在 Kaspersky Endpoint Security 组件的规则中，您现在不仅可以从 Active Directory 中选择用户，还可以从 Kaspersky Security Center 的用户列表中选择用户。您还可以手动输入本地用户账户数据。已为以下组件的规则添加了这种可能性：应用程序控制、设备控制、Web 控制、自适应异常控制和日志检查。

7. 网络攻击检测报告现在包含一个列，其中包含攻击计算机的 MAC 地址（网络威胁防护组件）。现在，除了 IP 地址之外，您还可以在报告中看到攻击计算机的 MAC 地址。这对于事件调查很有帮助。包含攻击计算机 MAC 地址的报告也将在 Kaspersky Security Center Linux 控制台版本 15.1 及更高版本中提供。

8. 提高了对计算机保护的要求。高保护级别现在需要启用应用程序服务免受外部管理的保护。在策略窗口的上部检查安全级别指示器。如果您的安全级别为中低，您可以在安全级别指标器建议窗口中启用应用程序服务免受外部管理的保护。

9. 增加了对应用程序在 Endpoint Detection and Response Agent (EDR Agent) 配置中运行时的对象检测新事件的支持。[KES+内置代理]配置中已支持这些事件。

10. 在开发此版本的 Kaspersky Endpoint Security for Windows 时，我们纳入了以下专用补丁中包含的更改：pf9640、pf9830、pf9831、pf10047、pf10351、pf12102、pf12105、pf13084、pf13089、pf14040、pf14047、pf15026、pf15028、pf16013。

更新 12.4

Kaspersky Endpoint Security 12.4 for Windows 提供了以下功能和改进：

1. 添加了新的功能来保护计算机与 Kaspersky Security Center 的连接。新的"*管理服务器连接保护*"任务允许设置连接到受信任服务器的密码。这意味着，如果没有此密码，就无法重新连接计算机并从另一台服务器运行命令。

2. 对于密码保护组件，添加了手动选择用户而不仅仅是从 Active Directory 中选择用户的功能。也就是说，您可以手动指定用户名和密码，并为此账户分配 Kaspersky Endpoint Security 的访问权限。这样，您就不需要与其他用户共享您的 KLAdmin 密码，也不需要创建新的 Active Directory 账户来控制对应用程序的访问。

3. 支持 Windows 11 23H2。

更新 12.3

Kaspersky Endpoint Security 12.3 for Windows 提供了以下功能和改进：

1. 现在您可以在 Endpoint Detection and Response Agent 配置下安装应用程序。此配置允许安装带有卡巴斯基的 Detection and Response 解决方案所需的一组组件的应用程序：Kaspersky Managed Detection and Response 和 Kaspersky Anti Targeted Attack Platform（EDR）.您可以在此配置中与第三方解决方案（例如 Dr.Web、Dallas Lock、ESET）一起安装应用程序。这使您可以将第三方基础设施安全工具与卡巴斯基的 Detection and Response 一起使用。

2. 改进了 Kaspersky Endpoint Security 对蓝牙设备的操作。现在，您可以配置排除项并限制对除输入设备（无线键盘、鼠标等）之外的所有蓝牙设备的访问。

3. 优化了应用程序控制组件对可执行文件数据库的操作。如果从计算机中删除某个文件，Kaspersky Endpoint Security 现在自动从数据库中删除文件信息。这可以使数据库保持最新并节省 Kaspersky Security Center 资源。

4. 提高了对计算机保护的要求。高防护级别现在需要启用密码保护。在策略窗口的上部检查安全级别指示器。如果您的保护级别为中或低，您可以在安全级别指示器建议窗口中启用密码保护。

5. 添加了 HTTPS 协议支持，使应用程序能够与卡巴斯基安全网络配合使用。在管理服务器属性的"KSN 代理服务器设置"中启用对 HTTPS 的使用。

更新 12.2

Kaspersky Endpoint Security 12.2 for Windows 提供了以下功能和改进：

1. 添加了 WPA3 协议支持以控制与 Wi-Fi 网络的连接（设备控制）。现在您可以在受信任的 Wi-Fi 网络设置中选择 WPA3 协议，并拒绝使用不太安全的协议连接到网络。

2. 现在您可以为网络威胁防护排除项选择协议和端口。现在除了指定受信任设备的 IP 地址外，您还可以选择端口和协议。这使您可以排除单个数据流并防止来自受信任 IP 地址的网络攻击。

3. 本地*"数据库和应用程序模块更新"任务*的更新源的不同顺序（如果策略应用于计算机）。Kaspersky Security Center 服务器现在默认用作第一个更新源，而不是卡巴斯基服务器。这有助于在用户运行本地"*数据库和应用程序模块更新*"任务时节省流量。

更新 12.1

Kaspersky Endpoint Security 12.1 for Windows 提供了以下功能和改进：

1. 添加了 Kaspersky Anti Targeted Attack Platform 解决方案的内置代理。您不再需要 Kaspersky Endpoint Agent 以使用 EDR（KATA）。Kaspersky Endpoint Agent 的所有功能将由 Kaspersky Endpoint Security 执行。要迁移 Kaspersky Endpoint Agent 策略，请使用迁移向导。更新应用程序后，Kaspersky Endpoint Security 切换到使用内置代理并卸载 Kaspersky Endpoint Agent。Kaspersky Endpoint Agent 已添加到不兼容软件列表中。Kaspersky Endpoint Security 具有适用于所有 Detection and Response 解决方案的内置代理，因此不再需要安装 Kaspersky Endpoint Agent 来与这些解决方案集成。

2. 现在支持 Azure WVD 兼容模式。此功能可确保在 Kaspersky Anti Targeted Attack Platform 控制台中正确显示 Azure 虚拟机状态。Azure WVD 兼容模式允许为这些虚拟机分配永久唯一的 Sensor ID。

3. 现在，您可以在 iTunes 或类似应用程序中配置用户对移动设备的访问。也就是说，例如，您可以允许移动设备仅在 iTunes 中使用，并阻止将移动设备用作可移动驱动器。该应用程序还支持 Android 调试桥 (ADB) 应用程序的这些规则。

4. 不再支持 Kaspersky Security Center 版本 11。将 Kaspersky Security Center 升级至最新版本。

已修复问题

下表列出了在 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。

版本 14.1 中修复的问题列表

问题 ID	问题描述
10140523	在 Windows 11 中启用原生 NVMe 可能会导致应用程序行为不稳定。
9340076	在安装了应用程序并启用了文件加密组件的设备上，当网络文件夹的内容从其他设备修改后，Windows 资源管理器不会自动刷新该文件夹的内容。
9722863	设备控制报告不包含 USB 令牌断开连接事件。
10006481	应用拒绝入站流量的规则后，由于超时计算不正确，与外部服务的活动 TCP 连接可能会过早终止。
10140912	应用程序无法检测到 BHT1100B PDA 设备。
10157563	Folder Redirection 在 VDI 工作站上重新启动后可能无法工作。
10158494	设备控制会记录可移动设备的多个连接和断开连接事件，而该设备并未进行物理重新连接。

常见问题回答

常规

Kaspersky Endpoint Security 可以在哪些计算机上运行？

自上个版本以来有哪些更改？

Kaspersky Endpoint Security 可以与其他哪些 Kaspersky 应用程序一起运行？

如何在 Kaspersky Endpoint Security 运行期间节省计算机资源？

部署

如何将 Kaspersky Endpoint Security 安装到组织的所有计算机上？

哪些安装设置可以在命令行中配置？

如何远程卸载 Kaspersky Endpoint Security？

更新

有哪些方法可以更新数据库？

如果更新后出现问题应该怎么办？

如何更新公司网络外部的数据库？

是否能使用代理服务器进行更新？

安全

Kaspersky Endpoint Security 如何扫描电子邮件？

如何从扫描中排除受信任的文件？

如何保护计算机免受闪存驱动器中的病毒的侵害？

如何运行对用户隐藏的恶意软件扫描？

如何临时暂停 Kaspersky Endpoint Security 的保护？

如何还原 Kaspersky Endpoint Security 错误删除的文件？

如何保护 Kaspersky Endpoint Security 不被用户卸载？

互联网

Kaspersky Endpoint Security 是否扫描加密连接 (HTTPS)？

如何允许用户只连接到受信任的 Wi-Fi 网络？

如何阻止社交网络？

应用程序

如何找出用户计算机上安装了哪些应用程序（资产）？

如何防止运行计算机游戏？

如何验证“应用程序控制”是否已正确配置？

如何将应用程序添加到受信任列表？

设备

如何阻止使用闪存驱动器？

如何将设备添加到受信任列表？

是否能获取对阻止的设备的访问权限？

加密

在哪些条件下无法进行加密？

如何使用密码限制对压缩文件的访问？

是否能使用加密的智能卡和令牌？

如果未与 Kaspersky Security Center 连接，是否能访问加密数据？

如果计算机操作系统出现故障但数据仍然加密，应该怎么办？

支持

报告文件存储在何处？

如何创建跟踪文件？

如何启用转储写入？

Kaspersky Endpoint Security for Windows

Kaspersky Endpoint Security for Windows（以下简称 Kaspersky Endpoint Security）为计算机提供全面保护，阻止各种类型的威胁、网络攻击和钓鱼攻击。

该应用程序不适用于涉及自动化控制系统的技术流程。为了保护此类系统中的设备，建议使用 Kaspersky Industrial CyberSecurity for Nodes 应用程序。

威胁检测技术

机器学习

Kaspersky Endpoint Security 使用基于机器学习的模型。该模型由 Kaspersky 专家开发。随后，该模型不断地输入来自 KSN（模型训练）的威胁数据。

云分析

Kaspersky Endpoint Security 从卡巴斯基安全网络接收威胁数据。*卡巴斯基安全网络 (KSN)* 是一个云服务的基础架构。它可以访问在线卡巴斯基知识库。该知识库中包含了文件信誉、网页资源和软件的相关信息。

专家分析

Kaspersky Endpoint Security 使用由 Kaspersky 病毒分析师添加的威胁数据。如果对象的信誉不能被自动判定，则病毒分析师手动检查该对象。

行为分析

Kaspersky Endpoint Security 实时分析对象的活动。

自动分析

Kaspersky Endpoint Security 从对象自动分析系统接收数据。系统处理发送给 Kaspersky 的所有对象。然后，系统确定对象的信誉，并将数据添加到反病毒数据库中。如果系统无法确定对象的信誉，系统将询问 Kaspersky 病毒分析师。

Sandbox

Kaspersky Endpoint Security 在虚拟机上处理对象。Kaspersky Sandbox 分析对象的行为并判定其信誉。该技术仅在您使用 Kaspersky Sandbox 解决方案时可用。

Cloud Sandbox

Kaspersky Endpoint Security 在卡巴斯基提供的隔离环境中扫描对象。Cloud Sandbox 技术是永久启用的，可供所有卡巴斯基安全网络用户使用，无论他们使用的授权许可类型如何。如果您已经部署了 Endpoint Detection and Response 解决方案，您可以为 Cloud Sandbox 检测到的威胁启用单独的计数器。

选择树

每种类型的威胁均由专门的组件应对。各个组件均可独立启用或禁用，并可以配置其设置。

区域	组件
基本威胁防护	**文件威胁防护** 文件威胁防护组件可防止计算机文件系统受到感染。默认情况下，文件威胁防护组件永久驻留在计算机的 RAM 中，并实时扫描所有打开、保存和启动的文件。该组件扫描所有计算机驱动器（包括连接的驱动器）上的文件。该组件借助反病毒数据库、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。 **Web 威胁防护** "Web 威胁防护"组件可防止从 Internet 下载恶意文件，同时阻止恶意网站和钓鱼网站。该组件借助反病毒数据库、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。 **邮件威胁防护** "邮件威胁防护"组件扫描传入和传出电子邮件的附件是否有病毒和其他威胁。该组件借助反病毒数据库、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。 邮件威胁防护可以扫描传入和传出的邮件。该应用程序在以下邮件客户端中支持 POP3、SMTP、IMAP 和 NNTP： • Microsoft Office Outlook • Mozilla Thunderbird • Windows Mail • MyOffice Mail • R7-Office Organizer 要扫描 Mozilla Thunderbird、MyOffice Mail 和 R7-Office Organizer 邮件客户端中的流量，您需要将卡巴斯基证书添加到证书存储并选择自己的证书存储。 邮件威胁防护不支持其他协议和邮件客户端。 邮件威胁防护可能并不总是能够获得邮件的*协议级*访问权限（例如，使用 Microsoft Exchange 解决方案时）。为此，邮件威胁防护包括 Microsoft Office Outlook 扩展程序。该扩展程序允许在*邮件客户端级别*扫描邮件。邮件威胁防护扩展程序支持 Outlook 2010、2013、2016、2019、2021、2024 和 365 的 32 位和 64 位版本。在基于 Arm 的计算机上，邮件威胁防护扩展程序支持 32 位和 64 位版本的 Outlook 2016、Outlook 2021、Outlook 2024 和 Outlook 365 for Arm64。 **网络威胁防护** *网络威胁防护组件*组件（也称Intrusion Detection System，IDS）监控入站网络流量以查找网络攻击的活动特征。当应用程序在用户计算机上检测到网络攻击企图时，它将阻止与攻击计算机的网络连接。应用程序数据库提供了当前已知类型的网络攻击以及应对方法的描述。"网络威胁防护"组件检测到的网络攻击列表在数据库和应用程序模块更新期间更新。 **防火墙** 在互联网或局域网上工作时，防火墙组件会阻止未经授权的计算机连接。防火墙还控制计算机上应用程序的网络活动。这允许您保护公司局域网免受身份盗窃和其他攻击。该组件借助反病毒数据库、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。 **BadUSB 攻击防护** BadUSB 攻击防护组件可以防止受感染的模拟键盘 USB 设备连接至计算机。 **AMSI 保护** AMSI 保护组件旨在支持 Microsoft 的反恶意软件扫描接口。*反恶意软件扫描接口 (AMSI)* 允许具有 AMSI 支持的第三方应用程序将对象（例如，PowerShell 脚本）发送到 Kaspersky Endpoint Security 进行附加扫描，然后接收这些对象的扫描结果。

区域	组件
高级威胁防护	**卡巴斯基安全网络** *卡巴斯基安全网络 (KSN)* 是一个云服务的基础架构。它可以访问在线卡巴斯基知识库。该知识库中包含了文件信誉、网页资源和软件的相关信息。使用卡巴斯基安全网络的数据可确保 Kaspersky Endpoint Security 能够更快地对新威胁作出响应，提高一些保护组件的性能，并减少误报风险。如果您正在参与卡巴斯基安全网络，KSN 服务为 Kaspersky Endpoint Security 提供有关已扫描网址的信誉的信息，以及有关已扫描文件的类别和信誉 的信息。 **行为检测** “行为检测”组件接收您计算机上的应用程序操作的信息，并将此信息提供给其他保护组件以提高性能。“行为检测”组件将行为流签名 (BSS) 用于应用程序。如果应用程序操作匹配行为流签名，Kaspersky Endpoint Security 将执行选定的响应操作。Kaspersky Endpoint Security 功能基于行为流签名，并为计算机提供主动防御。 行为检测组件还会监控可能威胁计算机安全的应用程序进程的网络端口。应用程序通过反病毒数据库获取有关此类进程的信息。 **反加密** 反加密组件分析共享文件夹中的活动。如果该活动与外部加密的典型行为流签名匹配，Kaspersky Endpoint Security 将执行选定操作。 **漏洞利用防御** “漏洞利用防御”组件可检测利用计算机漏洞来利用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。 漏洞利用防御组件还会监控可能威胁计算机安全的应用程序进程的网络端口。应用程序通过反病毒数据库获取有关此类进程的信息。 **主机入侵防御** “主机入侵防御”组件可避免应用程序执行可能给操作系统带来危险的操作，并确保控制对操作系统资源和个人数据的访问。该组件借助反病毒数据库和卡巴斯基安全网络云服务来提供计算机保护。 **修复引擎** 修复引擎组件允许 Kaspersky Endpoint Security 回滚恶意软件在操作系统中执行的操作。
安全控制	**应用程序控制** “应用程序控制”管理用户计算机上的应用程序启动。这允许您在使用应用程序时实施公司安全策略。“应用程序控制”还通过限制对应用程序的访问来降低计算机感染的风险。 **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（例如，硬盘驱动器、相机或 Wi-Fi 模块）的访问。这样可以在连接此类设备时保护计算机免受感染，并防止数据丢失或数据泄漏。 **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 阻止访问或显示警告。 **自适应异常控制** 自适应异常控制组件会监视并阻止不是公司网络内计算机典型操作的相关操作。自适应异常控制使用一组规则来跟踪非典型行为（例如，*从 office 应用程序启动 Microsoft PowerShell* 规则）。规则由 Kaspersky 专家根据恶意活动的典型情景创建。您可以配置“自适应异常控制”处理每条规则的方式，例如，允许执行使某些工作流任务自动化的 PowerShell 脚本。Kaspersky Endpoint Security 会同时更新规则集和应用程序数据库。 **日志审查** 日志检查根据 Windows 事件日志分析监控受保护环境的完整性。当应用程序在系统中检测到非典型行为的迹象时，它会通知管理员，因为该行为可能表示试图进行网络攻击。 **系统完整性监控** 系统完整性监控组件监控操作系统中可能预示计算机安全漏洞的变化。当检测到此类变化时，Kaspersky Endpoint Security 会生成相应的事件并向管理员发出警报。
任务	**恶意软件扫描** Kaspersky Endpoint Security 扫描计算机以查找病毒和其他威胁。恶意软件扫描有助于排除传播未被保护组件检测到（例如，由于安全级别低）的恶意软件的可能性。 **数据库和应用程序模块更新** Kaspersky Endpoint Security 下载经过更新的应用程序数据库和模块。更新可以确保计算机防护最新的病毒和其他威胁。在默认设置下，程序将自动更新，但是如有需要，您可以手动更新数据库和程序模块。 **上次更新回滚** Kaspersky Endpoint Security将回滚最新更新的数据库和模块。这允许您在必要时将数据库和应用程序模块回滚到以前的版本，例如，当新数据库版本包含无效签名而导致 Kaspersky Endpoint Security 阻止了安全的应用程序时。 **应用程序完整性检查** Kaspersky Endpoint Security 将检查应用程序安装文件夹内的应用程序模块以检查任何损坏或修改。如果应用程序模块拥有错误的数字签名，则该模块被认定为损坏。

区域	组件
数据加密	**文件级加密** 该组件允许创建文件加密规则。您可以选择要加密的预定义文件夹、手动选择文件夹或按扩展名选择单个文件。 **完整磁盘加密** 该组件允许使用卡巴斯基磁盘加密或 BitLocker 驱动器加密来加密硬盘。 **可移动驱动器加密** 该组件允许保护可移动驱动器上的数据。您可以使用完整磁盘加密 (FDE) 或文件及加密 (FLE)。
Detection and Response	**Endpoint Detection and Response Optimum** Kaspersky Endpoint Detection and Response Optimum 解决方案（也叫 "EDR Optimum"）的内置代理。*Kaspersky Endpoint Detection and Response* 是一种保护企业 IT 基础架构免受高级网络威胁的解决方案。该解决方案的功能将自动检测威胁与应对这些威胁的能力结合起来，以抵御高级攻击，包括新的漏洞利用、勒索软件、无文件攻击以及使用合法系统工具的方法。有关该解决方案的更多信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助。 **Endpoint Detection and Response Expert** Kaspersky Endpoint Detection and Response Expert 解决方案（也叫 "EDR Expert"）的内置代理。EDR Expert 比 EDR Optimum 提供更多的威胁监控和响应功能。有关该解决方案的更多信息，请参阅 Kaspersky Endpoint Detection and Response Expert 帮助。 **Endpoint Detection and Response Expert (on-premises)** 和 **Network Detection and Response (KATA)** 用于管理 Endpoint Detection and Response 和 Network Detection and Response 组件的内置代理，这些组件是 Kaspersky Anti Targeted Attack Platform 解决方案的一部分。*Kaspersky Anti Targeted Attack Platform* 是旨在及时检测复杂威胁（如针对性攻击、高级持久性威胁 (APT)、零日攻击等）的解决方案。Kaspersky Anti Targeted Attack Platform 包括三个功能单元： • Kaspersky Anti Targeted Attack Platform（*KATA*） • Kaspersky Endpoint Detection and Response（*EDR（KATA）*） • Network Detection and Response（*NDR（KATA）*） 您可以购买所有功能单元，也可以单独购买单个功能单元。有关解决方案的详细信息，请参阅 Kaspersky Anti Targeted Attack Platform 帮助。 **Sandbox** Sandbox 内置代理。*Sandbox* 组件检测并自动阻止计算机上的高级威胁。Sandbox 分析对象行为，以检测恶意活动和针对组织 IT 基础设施的攻击的活动特征。Sandbox 使用部署的 Microsoft Windows 操作系统虚拟映像（Sandbox 服务器）分析和扫描特殊服务器上的对象。有关解决方案的详细信息，请参阅 Kaspersky Sandbox 帮助 和 Kaspersky Anti Targeted Attack Platform 帮助。 **Managed Detection and Response** 支持 Kaspersky Managed Detection and Response 解决方案操作的内置代理。*Kaspersky Managed Detection and Response (MDR)* 解决方案自动检测和分析您基础架构中的安全事故。为此，MDR 使用从端点和机器学习接收的遥测数据。MDR 发送事故数据到 Kaspersky 专家。然后专家便可以处理事故，例如，添加新条目到反病毒数据库。或者，专家可以发布处理事件的建议，例如，建议将计算机从网络隔离。对于该解决方案如何工作的详情，请参考 Kaspersky Managed Detection and Response 帮助。

应用程序模式：标准、EDR Agent、Light Agent

Kaspersky Endpoint Security for Windows 是众多卡巴斯基解决方案的一部分。根据解决方案，您需要为应用程序选择一种模式。

标准模式

这是应用程序的主要和默认模式。您可以在此模式下安装该应用程序作为 Kaspersky EPP 解决方案（Endpoint Protection Platform）的一部分。例如，标准模式下的 Kaspersky Endpoint Security 是 Kaspersky Endpoint Security for Business 的一部分。Kaspersky Endpoint Security 为工作站和服务器提供全面保护，防止各种威胁、网络攻击和诈骗。在标准模式下，内置代理也可与 Kaspersky Detection and Response 解决方案（包括 EDR、MDR、KUMA 等）集成。

EDR Agent

此模式允许将 Kaspersky Detection and Response 解决方案与第三方 EPP 解决方案一起部署。Detection and Response 解决方案包括 Kaspersky Managed Detection and Response (MDR) 和 Kaspersky Anti Targeted Attack Platform (KATA)。EDR Agent 还支持 Kaspersky SIEM 解决方案、Kaspersky Unified Monitoring and Analysis Platform (KUMA)。

在此模式下，文件威胁防护或 Web 威胁防护等标准防护组件不可用。计算机的标准保护由第三方 EPP 解决方案提供。EDR Agent 持续监控这些计算机上运行的进程、打开的网络连接以及正在修改的文件。，并与 Detection and Response 解决方案进行交互。

Light Agent

此模式用于保护虚拟环境。Light Agent 模式下的 Kaspersky Endpoint Security 是 Kaspersky Hybrid Cloud Security 解决方案的一部分。Light Agent 保护工作站和服务器中使用访客操作系统的虚拟机。此模式中提供的保护和控制组件与标准模式中相同。不同之处在于，通过安装在单独虚拟机上的特殊解决方案组件 SVM（Secure Virtual Machine）扫描对象以查找病毒和其他恶意软件。因此，Light Agent 使用 SVM 的资源而不是虚拟机的资源来确保基础设施的安全。

分发包

分发套装包括以下分发包：

- **AES256**

  此分发包适用于安装在具有 x86/x64 架构的计算机上。此分发包包含用于实施有效密钥长度为 256 位的 AES（高级加密标准）加密算法的加密工具。

- **AES56**

  此分发包适用于安装在具有 x86/x64 架构的计算机上。此分发包包含用于实施有效密钥长度为 56 位的 AES 加密算法的加密工具。

- **Arm64**

  此分发包旨在安装在基于 Arm 的计算机上。此分发包不适用于安装在服务器上。

安装前，请确保分发包与您的处理器架构相匹配。如果分发包与处理器架构不匹配，安装程序将终止安装并报错。

分发包为 EXE 格式的自解压存档。要查看分发包的内容，您需要将压缩包解压到单独的文件夹中。每个分发包都包含以下文件：

kes_win.msi	Kaspersky Endpoint Security 安装包。
setup_kes.exe	通过任一可用方法安装应用程序所需的文件。
kes_win.kud	用于创建 Kaspersky Endpoint Security 安装包的文件。
klcfginst.msi	Kaspersky Security Center 管理控制台中应用程序管理插件的安装包。
bases.cab	安装过程中使用的更新包文件。
cleaner_v2.cab cleanerapi_v2.cab	用于删除不兼容软件的文件。
incompatible.txt	包含可能导致与 Kaspersky Endpoint Security 出现兼容性问题的软件列表的文件。卡巴斯基不保证 Kaspersky Endpoint Security 与列表中的软件的兼容性。
ksn_<language ID>.txt	包含参与卡巴斯基安全网络的条款的文件。
license.txt	包含最终用户授权许可协议和隐私策略的文件。
installer.ini	包含分发套装内部设置的文件。
kes.cab	应用程序图形界面的文件。
aes256.cab / aes56.cab	AES 加密算法的文件（未包含在 Arm64 分发包中）。
package.kcat	带有应用程序分发包签名的文件。数字签名保证了应用程序分发包的真实性和完整性。

不建议更改这些设置的值。如果您希望更改安装选项，请使用 setup.ini 文件。

硬件和软件要求

本文列出了应用程序已经过测试并保证能够正常运行的软件版本。应用程序也可能适用于其他软件版本，但这些配置尚未经过完整测试周期，因此未包含在保证支持的版本列表中。

为确保 Kaspersky Endpoint Security 的良好运行，您的计算机必须满足以下要求：

要安装该应用程序，您需要拥有计算机的管理员权限。

最低一般要求

最低要求	工作站（x86/x64）	服务器（x86/x64）	Arm
存储	2 GB	2 GB	2 GB
CPU	1 GHz，支持 SSE2 指令集	1.4 Ghz，支持 SSE2 指令集	1 GHz，Armv8.1 架构
RAM	工作站(x86)：1 GB 工作站(x64)：2 GB	2 GB 注意：服务器需要 8 GB 内存才能安装具有内置代理的应用程序，以便与 Kaspersky Anti Targeted Attack Platform 集成。	4 GB
Microsoft .NET Framework	4 或更新	4 或更新	4.8 或更新

工作站

支持的工作站操作系统：

- Windows 7 Home / Professional / Ultimate / Enterprise Service Pack 1
- Windows 8 Professional / Enterprise；
- Windows 8.1 Professional / Enterprise；
- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multi-session
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise
- Windows 11 for Arm64 Home / Pro / Pro for Workstations / Education / Enterprise

Windows 操作系统从版本 11 24H2 开始支持 UDP Receive Segment Coalescing Offload （URO）技术。如果计算机上安装了兼容的网卡和驱动程序，则默认启用该技术。在用户的计算机上禁用 URO 会显著降低应用程序的性能。

为确保 Kaspersky Endpoint Security 正常运行，Windows Security Center (wscsvc) 服务必须在用户的计算机上运行

Kaspersky Endpoint Security 无法安装在未安装以下操作系统更新的 Microsoft Windows 7 上：KB4490628（2019 年 3 月 12 日）和 KB4474419（2019 年 9 月 23 日）。有关详细信息，请参阅技术支持知识库。

有关对 Microsoft Windows 10 操作系统的支持的详细信息，请参阅技术支持知识库。

有关对 Microsoft Windows 11 操作系统的支持的详细信息，请参阅技术支持知识库。

服务器

Kaspersky Endpoint Security 对运行 Windows 服务器操作系统的计算机上的应用程序核心组件进行支持。您可以在组织的服务器和集群上（Cluster Mode）使用 Kaspersky Endpoint Security for Windows，而不是 Kaspersky Security for Windows Server。应用程序还支持Server Core Mode（请参阅已知问题）。

支持的服务器操作系统：

- Windows Small Business Server 2011 Essentials / Standard (64-bit);

  Microsoft Small Business Server 2011 Standard (64-bit) 仅在 Service Pack 1 for Microsoft Windows Server 2008 R2 被安装时被支持。

- Windows MultiPoint Server 2011 (64-bit);
- Windows Server 2008 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 1
- Windows Web Server 2008 R2 Service Pack 1
- Windows Server 2012 Foundation / Essentials / Standard / Datacenter (包括 Server Core 模式)；
- Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter (包括 Server Core 模式)；
- Windows Server 2016 Essentials / Standard / Datacenter (包括 Server Core 模式)；
- Windows Server 2019 Essentials / Standard / Datacenter (包括 Server Core 模式)；
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (包括 Server Core 模式)
- Windows Server 2025 Standard / Datacenter

Kaspersky Endpoint Security 无法安装在未安装以下操作系统更新的 Microsoft Windows Server 2008 R2 上：KB4490628（2019 年 3 月 12 日）和 KB4474419（2019 年 9 月 23 日）。

有关对 Microsoft Windows Server 2016 和 Microsoft Windows Server 2019 操作系统的支持的详细信息，请参阅技术支持知识库。

有关对 Microsoft Windows Server 2022 操作系统的支持的详细信息，请参阅技术支持知识库。

不支持的服务器操作系统：

- Windows Server 2003 Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2003 R2 Foundation / Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2008 Standard / Enterprise / Datacenter Service Pack 2
- Windows Server 2008 Core Standard / Enterprise / Datacenter Service Pack 2
- Microsoft Small Business Server 2008 Standard / Premium Service Pack 2

虚拟平台

标准模式下应用程序运行所支持的虚拟平台：

- VMware Workstation Pro 26H1；
- VMware ESXi 8.0 Update 3i
- Windows Server 2025；
- Citrix Virtual Apps and Desktops 7 2507 LTSR
- Citrix Provisioning 2507 LTSR
- XenServer 8.4。

该应用程序支持使用 Hyper-V 创建的运行 Windows 11 Pro Arm64 的虚拟机。

用于安装 Light Agent 的虚拟机

不支持在基于 Arm 的虚拟机上以 Light Agent 模式安装 Kaspersky Endpoint Security。

虚拟机上的 BIOS 必须支持 SMBIOS 规范版本 2.1 或更高版本。

虚拟机上必须安装以下软件包和实用程序：

- 使用 Microsoft Hyper-V 时 – Integration Services 软件包。
- 使用 VMware vSphere 时 – VMware Tools 软件包。
- 使用 XenServer 时 – XenTools 软件包。
- 使用华为 FusionSphere 时 – 华为工具软件包。
- 使用基于 KVM 的虚拟机监控程序时 – QEMU Guest Agent。

在 Kaspersky Security for Virtualization Light Agent 帮助 中查看在 Light Agent 模式下运行应用程序的虚拟基础架构要求。

为了使应用程序正常工作，请使用带宽至少为 100 Mbit/s 的虚拟化网络接口。

终端服务器

支持的终端服务器类型：

- Microsoft Remote Desktop Services 基于 Windows Server 2008 R2 SP1
- Microsoft Remote Desktop Services 基于 Windows Server 2012
- Microsoft Remote Desktop Services 基于 Windows Server 2012 R2
- Microsoft Remote Desktop Services 基于 Windows Server 2016
- Microsoft Remote Desktop Services 基于 Windows Server 2019
- Microsoft Remote Desktop Services 基于 Windows Server 2022
- Microsoft Remote Desktop Services 基于 Windows Server 2025
- Citrix Virtual Apps and Desktops 7 2507 LTSR 中的 Citrix RDSH

Kaspersky Security Center 支持

Kaspersky Endpoint Security 支持以下版本 Kaspersky Security Center 的操作：

- Kaspersky Security Center 14.2。
- Kaspersky Security Center Linux 14.2。
- Kaspersky Security Center Linux 15。
- Kaspersky Security Center Windows 15.1。
- Kaspersky Security Center Linux 15.1。
- Kaspersky Security Center Linux 15.2。
- Kaspersky Security Center Linux 15.3。
- Kaspersky Security Center Linux 15.4。
- Kaspersky Security Center Linux 16。
- Kaspersky Security Center Linux 16.1。
- Kaspersky Security Center Linux 16.2。

取决于操作系统类型的可用应用程序功能比较

可用的 Kaspersky Endpoint Security 功能集取决于操作系统的类型：工作站或服务器（请参见下表）。

从 Kaspersky Endpoint Security 12.8 for Windows 开始，您可以在安装包中为不同的操作系统类型配置不同的组件集。也就是说，您可以使用相同的安装包部署应用程序到工作站和服务器。

不支持在基于 Arm 的虚拟机上以 Light Agent 模式安装 Kaspersky Endpoint Security。

Kaspersky Endpoint Security 功能比较

功能	工作站	基于 Arm 的工作站	服务器	Server Core 模式
高级威胁防护				
卡巴斯基安全网络	✓	✓	✓	✓
行为检测	✓	✓	✓	✓
反加密程序	✓	✓	✓	✓
漏洞利用防御	✓	✓	✓	✓
主机入侵防御	✓	✓	–	–
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	✓	✓	✓	✓
网络威胁防护	✓	✓	✓	✓
BadUSB 攻击防护	✓	✓	✓	–
AMSI 保护	✓	✓	✓	✓
安全控制				
日志审查	–	–	✓	–
应用程序控制	✓	✓	✓	✓
设备控制	✓	✓	✓	✓
Web 控制	✓	✓	✓	–
自适应异常控制	✓	✓	–	–
系统完整性监控	–	–	✓	–
Cloud Discovery	✓	✓	–	–
数据加密				
卡巴斯基磁盘加密	✓	–	–	–
BitLocker 驱动器加密	✓	✓	✓	✓
文件级加密	✓	–	–	–
可移动驱动器加密	✓	–	–	–
Detection and Response				

功能	工作站	基于 Arm 的工作站	服务器	Server Core 模式
Endpoint Detection and Response Optimum	✓	✓	✓	✓
Endpoint Detection and Response Expert (cloud)	✓	–	✓	✓
Endpoint Detection and Response (KATA)	✓	✓	✓	✓
Network Detection and Response (KATA)	✓	✓	✓	✓
Sandbox	✓	✓	✓	✓
Managed Detection and Response (MDR)	✓	✓	✓	✓
KUMA 整合	✓	✓	✓	✓

根据管理工具比较应用程序功能

Kaspersky Endpoint Security 中提供的功能集取决于管理工具（请参见下表）。

您可以使用 Kaspersky Security Center 的以下控制台管理应用程序：

- 管理控制台。管理员工作站上安装的 Microsoft 管理控制台 (MMC) 管理单元。
- Web 控制台。管理服务器上安装的 Kaspersky Security Center 组件。您可以在任何可访问管理服务器的计算机上通过浏览器在 Web Console 中工作。

您也可以使用 Kaspersky Security Center 云控制台管理应用程序。*Kaspersky Security Center 云控制台*是 Kaspersky Security Center 的云版本。这意味着 Kaspersky Security Center 的管理服务器和其他组件安装在卡巴斯基云基础架构中。有关使用 Kaspersky Security Center 云控制台管理应用程序的详细信息，请参阅 Kaspersky Security Center 云控制台帮助。

Kaspersky Endpoint Security 是 Kaspersky Next Pro View 解决方案的一部分。有关该应用程序作为此解决方案的一部分运行时可用的功能的更多信息，请参阅 Kaspersky Next 帮助。

Kaspersky Endpoint Security 功能比较

功能	Kaspersky Security Center		Kaspersky Security Center
	管理控制台	Web 控制台	云控制台
高级威胁防护			
卡巴斯基安全网络	✓	✓	✓
卡巴斯基私有安全网络	✓	✓	–
行为检测	✓	✓	✓
反加密程序			
漏洞利用防御	✓	✓	✓
主机入侵防御	✓	✓	✓
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	✓	✓	✓
网络威胁防护	✓	✓	✓

功能	Kaspersky Security Center		Kaspersky Security Center
	管理控制台	Web 控制台	云控制台
BadUSB 攻击防护	✓	✓	✓
AMSI 保护	✓	✓	✓
安全控制			
日志审查	✓	✓	✓
应用程序控制	✓	✓	✓
设备控制	✓	✓	✓
Web 控制	✓	✓	✓
自适应异常控制	✓	✓	✓
系统完整性监控	✓	✓	✓
Cloud Discovery	–	–	✓
数据加密			
卡巴斯基磁盘加密	✓	✓	–
BitLocker 驱动器加密	✓	✓	✓
文件级加密	✓	✓	–
可移动驱动器加密	✓	✓	–
Detection and Response			
Endpoint Detection and Response Optimum	–	✓	✓
Endpoint Detection and Response Expert (cloud)	–	–	✓
Endpoint Detection and Response (KATA)	✓	✓	–
Network Detection and Response (KATA)	✓	✓	–
Sandbox	–	✓	–
Managed Detection and Response (MDR)	✓	✓	✓
KUMA 整合	✓	✓	✓
任务			
添加密钥	✓	✓	✓
更改应用程序组件	✓	✓	✓
清查	✓	✓	✓
更新	✓	✓	✓
更新回滚	✓	✓	✓
恶意软件扫描	✓	✓	✓
应用程序完整性检查	✓	✓	–
擦除数据	✓	✓	✓
管理身份验证代理账户（卡巴斯基磁盘加密）	✓	✓	–
IOC 扫描 (EDR)	–	✓	✓
移动文件到隔离区 (EDR)	–	✓	✓
获取文件 (EDR)	–	✓	✓
删除文件 (EDR)	–	✓	✓
启动进程 (EDR)	–	✓	✓
终止进程 (EDR)	–	✓	✓

与其他应用程序的兼容性

Kaspersky Endpoint Security 与某些卡巴斯基应用程序以及某些第三方应用程序不兼容。因此，在安装之前，更新应用程序版本，并更改应用程序组件，Kaspersky Endpoint Security 会扫描计算机，查看是否存在此类应用程序。

与第三方应用程序的兼容性

Kaspersky Endpoint Security 与第三方端点保护系统 (Endpoint Protection Platform, EPP) 中的应用程序不兼容。Kaspersky Endpoint Security 也可能遇到与其他应用程序的兼容性问题。为了确定兼容性，Kaspersky Endpoint Security 参考了卡巴斯基准备的软件列表。此列表包含在 incompatible.txt 文件中。此文件包含在分发包中。

卡巴斯基不保证 Kaspersky Endpoint Security 与列表中的软件的兼容性。如果发现列表中的应用程序，安装程序将停止部署 Kaspersky Endpoint Security。安装程序可能会自动从列表中删除一些应用程序。如果您愿意忽略风险并希望在同一台计算机上安装 Kaspersky Endpoint Security 和列表中的软件，则可以跳过计算机检查（请参阅下面的说明）。

下载 INCOMPATIBLE.TXT 文件

与卡巴斯基应用程序的兼容性

Kaspersky Endpoint Security 与以下 Kaspersky 应用程序不兼容：

- 卡巴斯基标准版 | Plus | 优选版。
- Kaspersky Small Office Security。
- 卡巴斯基安全软件。
- 卡巴斯基反病毒软件。
- 卡巴斯基全方位安全软件。
- Kaspersky Safe Kids。
- Kaspersky 免费版。
- Kaspersky Anti-Ransomware Tool。
- Endpoint Sensor 作为 Kaspersky Anti Targeted Attack Platform 和 Kaspersky Endpoint Detection and Response 解决方案的一部分。

- Kaspersky Endpoint Agent 作为卡巴斯基的 Detection and Response 解决方案的一部分。

  卡巴斯基正在将所有 Detection and Response 切换为使用 Kaspersky Endpoint Security 内置代理，而不是 Kaspersky Endpoint Agent。从版本 12.1 开始，该应用程序支持所有 Detection and Response 解决方案。

- Kaspersky Security for Virtualization Light Agent。
- Kaspersky Fraud Prevention for Endpoint。
- Kaspersky Security for Windows Server

  从 Kaspersky Endpoint Security 12.0 开始，您可以从 Kaspersky Security for Windows Server 迁移到 Kaspersky Endpoint Security for Windows，并使用单一解决方案来保护工作站和服务器。

- Kaspersky Embedded Systems Security。

如果计算机安装了该列表中的 Kaspersky 应用程序，Kaspersky Endpoint Security 会删除这些应用程序。请等待此过程结束，然后再继续安装 Kaspersky Endpoint Security。

跳过可能导致兼容性问题的软件检查

如果 Kaspersky Endpoint Security 检测到来自 incompatible.txt 列表的软件，应用程序的安装将被终止。要继续安装，您必须删除该应用程序。然而，如果第三方软件供应商在其文档中指出其软件与Endpoint Protection Platform（EPP）兼容，则可以将 Kaspersky Endpoint Security 安装到包含该供应商的应用程序的计算机上。例如，Endpoint Detection and Response（EDR）解决方案提供商可以声明其与第三方 EPP 系统的兼容性。如果是这种情况，则需要在不运行已安装软件检查的情况下开始安装 Kaspersky Endpoint Security。为此，请将以下参数传递给安装程序：

- `SKIPPRODUCTCHECK=1` 禁用已安装软件检查。可能导致兼容性问题的软件列表位于分发包中的 incompatible.txt 文件中。如果没有为该参数设置值并且检测到来自列表的软件，则将终止 Kaspersky Endpoint Security 的安装。
- `SKIPPRODUCTUNINSTALL=1` 禁用从 incompatible.txt 列表中自动删除检测到的软件。如果没有为此参数设置任何值，则 Kaspersky Endpoint Security 将尝试删除可能导致兼容性问题的软件。
- `CLEANERSIGNCHECK=0` 禁用检查发现的应用程序的数字签名验证。如果未设置此参数，则在通过 Kaspersky Security Center 部署应用程序时，将禁用数字签名验证。在本地安装应用程序时，默认情况下启用数字签名验证。

在本地安装应用程序时，您可以在命令行中传递参数。

如果在安装过程中您跳过了可能导致兼容性问题的软件扫描，Kaspersky Endpoint Security 可以在应用程序组件更改时再次执行此检查。要跳过已安装软件的扫描，您需要配置*更改应用程序组件*任务。

例如：
```
C:\KES\setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0 /s
```

要远程安装 Kaspersky Endpoint Security，您需要在 `[Setup]` 中向名为 `kes_win.kud` 的安装包生成文件添加适当的参数（见下文）。`kes_win.kud` 文件包含在分发工具中。

kes_win.kud

```
[Setup]
UseWrapper=1
ExecutableRelPath=EXEC
Params=/s /pAKINSTALL=1 /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=0 /pSKIPPRODUCTCHECK=1 /pSKIPPRODUCTUNINSTALL=1
/pCLEANERSIGNCHECK=0
Executable=setup_kes.exe
RebootDelegated = 1
RebootAllowed=1
ConfigFile=installer.ini
RelPathsToExclude=klcfginst.msi
```

安装和删除程序

可以通过以下方式在计算机上安装 Kaspersky Endpoint Security：

- 本地使用安装向导。
- 本地使用命令行。
- 使用 Kaspersky Security Center 远程。
- 远程通过 Microsoft Windows 组策略管理编辑器（有关详细信息，请参阅 Microsoft 技术支持网站）。
- 远程使用系统中心配置管理器。

您可以通过多种方式配置应用程序安装设置。如果同时使用多种方法配置设置，Kaspersky Endpoint Security 将应用具有最高优先级的设置。Kaspersky Endpoint Security 使用以下优先级顺序：

1. 从 setup.ini 文件收到的设置。
2. 从 installer.ini 文件收到的设置。
3. 从命令行收到的设置。
4. 从配置文件 (install.cfg) 收到的设置。

我们建议您在启动 Kaspersky Endpoint Security 安装（包括远程安装）之前关闭所有活动的应用程序。

安装 Kaspersky Endpoint Security 时，操作系统可能会显示自己的消息。安装应用程序时网络和互联网连接也可能会中断。

安装、更新或卸载 Kaspersky Endpoint Security 时，可能会出现错误。有关解决这些错误的更多信息，请参阅技术支持知识库。

通过 Kaspersky Security Center 部署

Kaspersky Endpoint Security 可以通过多种方式部署在企业网络内的计算机上。您可以为您的组织选择最合适的部署方案，或同时组合多个部署方案。在安装应用程序之前，您必须确保计算机上安装了 Kaspersky Security Center 网络代理。*网络代理*可促进管理服务器与客户端计算机之间的交互。

Kaspersky Security Center 支持以下主要部署方法：

- 使用保护部署向导安装应用程序。

  如果您满意 Kaspersky Endpoint Security for Windows 的默认设置，并且的您组织的基础架构很简单，不需要特殊配置，则标准安装方法很方便。

- 使用远程安装任务安装应用程序。

通用安装方法允许您配置 Kaspersky Endpoint Security 设置并灵活管理远程安装任务。Kaspersky Endpoint Security 的安装包括以下步骤：

1. 创建安装包。
2. 创建远程安装任务。

Kaspersky Security Center 还支持使用其他方法来安装 Kaspersky Endpoint Security，例如在操作系统映像内部署。有关其他部署方法的详细信息，请参阅 Kaspersky Security Center 帮助。

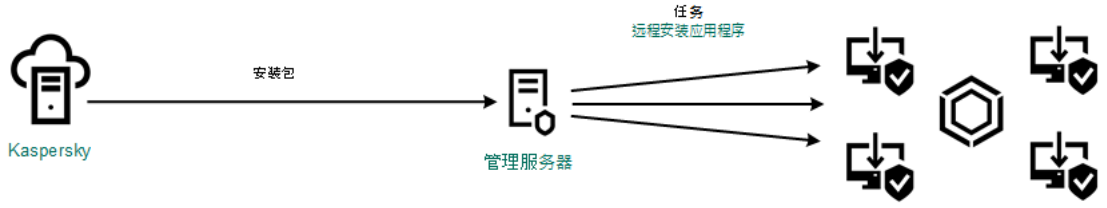
应用程序的标准安装

Kaspersky Security Center 提供了保护部署向导，以便在企业计算机上安装应用程序。保护部署向导包括以下主要操作：

1. 选择 Kaspersky Endpoint Security 安装包。

   *安装包*是为通过 Kaspersky Security Center 远程安装 Kaspersky 应用程序而创建的一组文件。安装包中包含安装应用程序以及安装后立即运行应用程序所需的一系列设置。安装包通过应用程序分发包中包括的扩展名为 .kpd 和 .kud 的文件创建。Kaspersky Endpoint Security 安装包通用于所有受支持的 Windows 版本和处理器架构类型。

2. 创建 Kaspersky Security Center 管理服务器的"*远程安装应用程序*"任务。



Kaspersky Endpoint Security 部署

如何在管理控制台 (MMC) 中运行保护部署向导

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择"**高级**" → "**远程安装**"。
3. 单击**在受管理设备上部署安装包(工作站)**链接。

   这将启动保护部署向导。按照向导的说明进行操作。

客户端计算机上的 TCP 端口 139 和 445 以及 UDP 端口 137 和 138 必须开放。

步骤 1. 选择安装包

从列表中选择 Kaspersky Endpoint Security 安装包。如果列表不包含 Kaspersky Endpoint Security 安装包，可以在向导中创建安装包。

您可以在 Kaspersky Security Center 中配置安装包设置。例如，您可以选择将安装到计算机的应用程序组件。

网络代理也将与 Kaspersky Endpoint Security 一起安装。*网络代理*可促进管理服务器与客户端计算机之间的交互。如果计算机上已安装网络代理，则不会再次安装。

步骤 2.

选择“**部署 Kaspersky Security Center 包**”源。

步骤 3. 选择要进行安装的设备

选择要安装 Kaspersky Endpoint Security 的计算机。下列选项可用：

- 将任务分配给管理组。在这种情况下，任务分配给先前创建的管理组中包括的计算机。
- 选择管理服务器在网络中检测到的计算机：*未分配设备*。网络代理不会安装在未分配设备上。在这种情况下，任务将分配给特定设备。特定设备可包括管理组中的设备以及未分配设备。
- 手动指定设备地址或从列表中导入地址。您可以指定您要将任务分配给的设备的 NetBIOS 名称、IP 地址和 IP 子网。

步骤 4. 定义远程安装任务设置

配置以下其他应用程序设置：

- “**强制下载安装包**”。选择应用程序安装方法：
  - “**使用网络代理**”。网络代理负责将 Kaspersky Endpoint Security 安装包分发到客户端计算机。如果未安装网络代理，则任务将以错误结束。在这种情况下，请将网络代理安装包添加到“*远程安装应用程序*”任务并通过操作系统资源实现文件传输。然后，网络代理将使用操作系统资源进行安装。然后通过网络代理的工具安装 Kaspersky Endpoint Security。
  - “**通过分发点使用操作系统资源**”。通过分发点使用操作系统资源将安装包传输到客户端计算机。如果网络中有至少一个分发点，则可以选择此选项。有关分发点的详细信息，请参阅 Kaspersky Security Center 帮助。
  - “**通过管理服务器使用操作系统资源**”。文件将通过管理服务器使用操作系统资源传送到客户端计算机。如果客户端计算机上未安装网络代理，但客户端计算机与管理服务器在同一网络中，可以选择此选项。
- **通过其他管理服务器管理的设备的行为**。选择 Kaspersky Endpoint Security 安装方法。如果网络中安装了多个管理服务器，这些管理服务器可能看到相同的客户端计算机。例如，这可能导致通过不同的管理服务器在同一客户端计算机上多次远程安装同一应用程序，或产生其他冲突。
- “**如果已经安装应用程序则不再重新安装**”。例如，如果要安装较早版本的应用程序，则清除此复选框。
- **在活动目录组策略中指定网络代理的安装**。使用 Active Directory 资源手动安装网络代理。要安装网络代理，必须以域管理员权限运行远程安装任务。

步骤 5. 选择授权许可密钥

向安装包添加用于激活应用程序的密钥。该步骤为可选项。如果管理服务器包含带自动分发功能的授权许可密钥，则该密钥稍后将自动添加。您也可以在以后使用“*添加密钥*”任务来激活应用程序。

步骤 6. 选择操作系统重启设置

选择当需要重新启动计算机时所执行的操作。安装 Kaspersky Endpoint Security 时，不需要重新启动。仅当在安装前必须删除不兼容的应用程序时，才需要重新启动。更新应用程序版本时也可能需要重新启动。

步骤 7. 在安装应用程序前删除不兼容的应用程序

请仔细阅读不兼容应用程序列表并允许删除这些应用程序。如果计算机上安装了不兼容的应用程序，安装 Kaspersky Endpoint Security 将以出错结束。

步骤 8. 选择用于访问设备的账户

选择用于使用操作系统工具安装网络代理的账户。在这种情况下，访问计算机需要管理员权限。您可以添加多个账户。如果某个账户没有足够权限，安装向导将使用下一个账户。如果使用网络代理工具安装 Kaspersky Endpoint Security，则无需选择账户。

步骤 9. 开始安装

退出向导。如有必要，选中“**向导完成时运行任务**”复选框。您可以在任务属性中监控任务进度。

如何在 Web Console 和云控制台中启动保护部署向导

在 Web Console 的主窗口中，选择“**发现和部署**” → “**部署和分配**” → “**保护部署向导**”。

这将启动保护部署向导。按照向导的说明进行操作。

> 客户端计算机上的 TCP 端口 139 和 445 以及 UDP 端口 137 和 138 必须开放。

步骤 1. 选择安装包

从列表中选择 Kaspersky Endpoint Security 安装包。如果列表不包含 Kaspersky Endpoint Security 安装包，可以在向导中创建安装包。要创建安装包，您无需搜索分发包并将其保存到计算机内存中。在 Kaspersky Security Center 中，可以查看位于 Kaspersky 服务器中的分发包列表，安装包会自动创建。Kaspersky 在发布新版本的应用程序后会更新该列表。

您可以在 Kaspersky Security Center 中配置安装包设置。例如，您可以选择将安装到计算机的应用程序组件。

步骤 2. 选择授权许可密钥

向安装包添加用于激活应用程序的密钥。该步骤为可选项。如果管理服务器包含带自动分发功能的授权许可密钥，则该密钥稍后将自动添加。您也可以在以后使用"*添加密钥*"任务来激活应用程序。

步骤 3. 选择网络代理

选择将与 Kaspersky Endpoint Security 一起安装的网络代理的版本。*网络代理*可促进管理服务器与客户端计算机之间的交互。如果计算机上已安装网络代理，则不会再次安装。

步骤 4. 选择要进行安装的设备

选择要安装 Kaspersky Endpoint Security 的计算机。下列选项可用：

- 将任务分配给管理组。在这种情况下，任务分配给先前创建的管理组中包括的计算机。
- 选择管理服务器在网络中检测到的计算机：*未分配设备*。网络代理不会安装在未分配设备上。在这种情况下，任务将分配给特定设备。特定设备可包括管理组中的设备以及未分配设备。
- 手动指定设备地址或从列表中导入地址。您可以指定您要将任务分配给的设备的 NetBIOS 名称、IP 地址和 IP 子网。

步骤 5. 配置高级设置

配置以下其他应用程序设置：

- **强制下载安装包**。选择应用程序安装方法：
  - "**使用网络代理**"。网络代理负责将 Kaspersky Endpoint Security 安装包分发到客户端计算机。如果未安装网络代理，则任务将以错误结束。在这种情况下，请将网络代理安装包添加到"*远程安装应用程序*"任务并通过操作系统资源实现文件传输。然后，网络代理将使用操作系统资源进行安装。然后通过网络代理的工具安装 Kaspersky Endpoint Security。
  - "**通过分发点使用操作系统资源**"。通过分发点使用操作系统资源将安装包传输到客户端计算机。如果网络中有至少一个分发点，则可以选择此选项。有关分发点的详细信息，请参阅 Kaspersky Security Center 帮助。
  - "**通过管理服务器使用操作系统资源**"。文件将通过管理服务器使用操作系统资源传送到客户端计算机。如果客户端计算机上未安装网络代理，但客户端计算机与管理服务器在同一网络中，可以选择此选项。
- **如果已经安装应用程序则不再重新安装**。例如，如果要安装较早版本的应用程序，则清除此复选框。
- "**在 Active Directory 组策略中指定安装包的安装**"。Kaspersky Endpoint Security 通过网络代理安装或通过 Active Directory 手动安装。要安装网络代理，必须以域管理员权限运行远程安装任务。

步骤 6. 选择操作系统重启设置

选择当需要重新启动计算机时所执行的操作。安装 Kaspersky Endpoint Security 时，不需要重新启动。仅当在安装前必须删除不兼容的应用程序时，才需要重新启动。更新应用程序版本时也可能需要重新启动。

步骤 7. 在安装应用程序前删除不兼容的应用程序

请仔细阅读不兼容应用程序列表并允许删除这些应用程序。如果计算机上安装了不兼容的应用程序，安装 Kaspersky Endpoint Security 将以出错结束。

步骤 8. 分配到管理组

选择安装网络代理后计算机将被移动到的管理组。需要将计算机移至管理组，以便应用策略和组任务。如果计算机已在任意管理组中，则该计算机不会被移动。如果不选择管理组，计算机将被添加到"**未分配的设备**"组。

步骤 9. 选择用于访问设备的账户

选择用于使用操作系统工具安装网络代理的账户。在这种情况下，访问计算机需要管理员权限。您可以添加多个账户。如果某个账户没有足够权限，安装向导将使用下一个账户。如果使用网络代理工具安装 Kaspersky Endpoint Security，则无需选择账户。

步骤 10.开始安装

退出向导。如有必要，选中“**向导完成时运行任务**”复选框。您可以在任务属性中监控任务进度。

创建安装包

*安装包*是为通过 Kaspersky Security Center 远程安装 Kaspersky 应用程序而创建的一组文件。安装包中包含安装应用程序以及安装后立即运行应用程序所需的一系列设置。安装包通过应用程序分发包中包括的扩展名为 .kpd 和 .kud 的文件创建。Kaspersky Endpoint Security 安装包通用于所有受支持的 Windows 版本和处理器架构类型。

如何在管理控制台 (MMC) 中创建安装包

1. 在管理控制台中，转到文件夹“**管理服务器**”→“**高级**”→“**远程安装**”→“**安装包**”。

   这将打开已下载到 Kaspersky Security Center 的安装包列表。

2. 单击“**创建安装包**”。

新安装包向导启动。按照向导的说明进行操作。

步骤 1. 选择安装包类型

请选择**为卡巴斯基应用程序创建安装包**选项。

步骤 2. 定义安装包名称

输入安装包的名称，例如，*Kaspersky Endpoint Security for Windows 14.1*。

步骤3. 选择用于安装的分发包

单击“**浏览**”按钮，然后选择分发包中包含的 `kes_win.kud` 文件。

如果需要，请使用“**从存储库中复制更新到安装包**”复选框更新安装包中的反病毒数据库。

步骤4. 最终用户授权许可协议和隐私策略

阅读并接受最终用户授权许可协议和隐私策略的条款。

安装包将被创建并添加到 Kaspersky Security Center 中。使用安装包，您可以在企业网络计算机上安装 Kaspersky Endpoint Security 或更新应用程序版本。

在安装包设置中，您可以针对不同的操作系统类型选择应用程序组件。也就是说，安装包包含两套组件：用于工作站的和用于服务器的。在部署安装包之前，安装程序会检测操作系统的类型，并仅安装您为该操作系统类型选择的应用程序组件。这样，您就可以对工作站和服务器使用相同的安装包。

安装包包含来自管理服务器存储库的反病毒数据库。您可以更新安装包中的数据库，以减少在安装 Kaspersky Endpoint Security 之后更新数据库时的流量消耗。

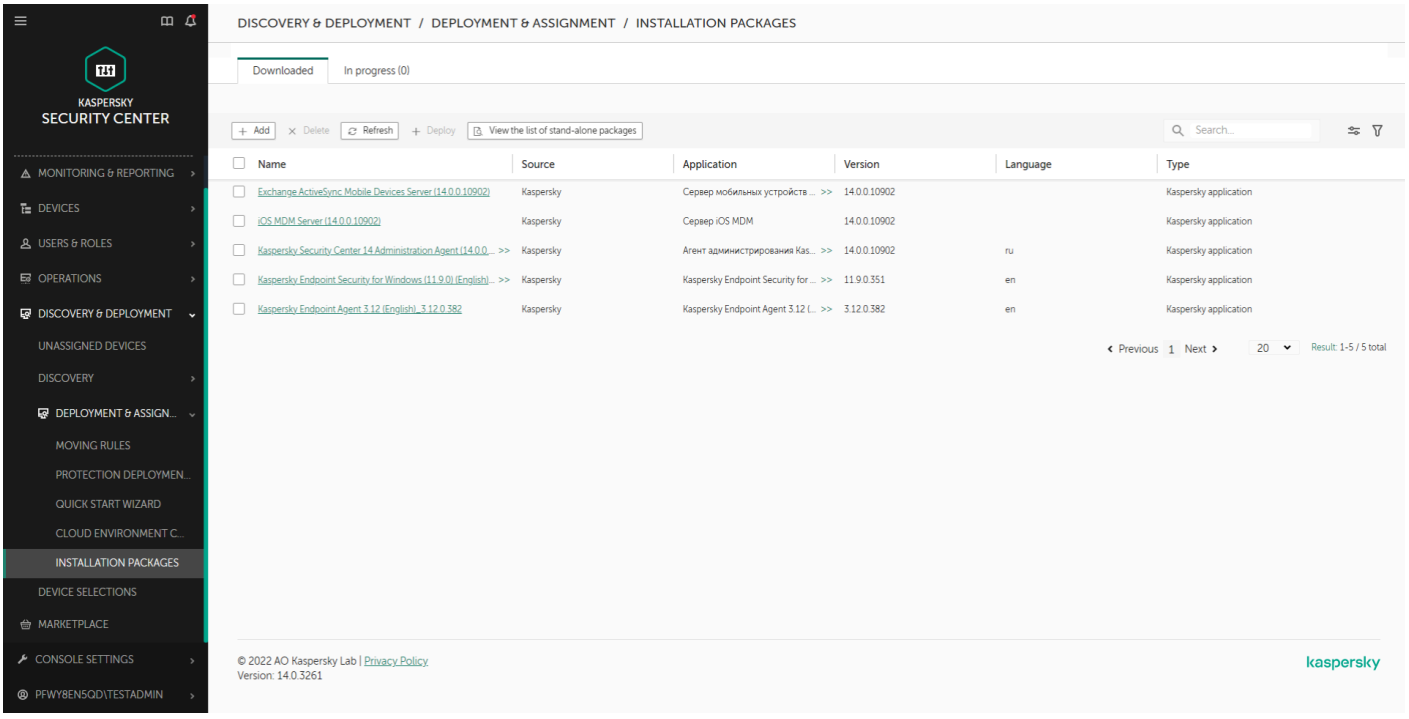
如何在 Web Console 和云控制台中创建安装包

1. 在 Web Console 的主窗口中，选择“**发现和部署**” → “**部署和分配**” → “**安装包**”。

   这将打开已下载到 Kaspersky Security Center 的安装包列表。

2. 单击“**添加**”。

   新安装包向导启动。按照向导的说明进行操作。



安装包列表

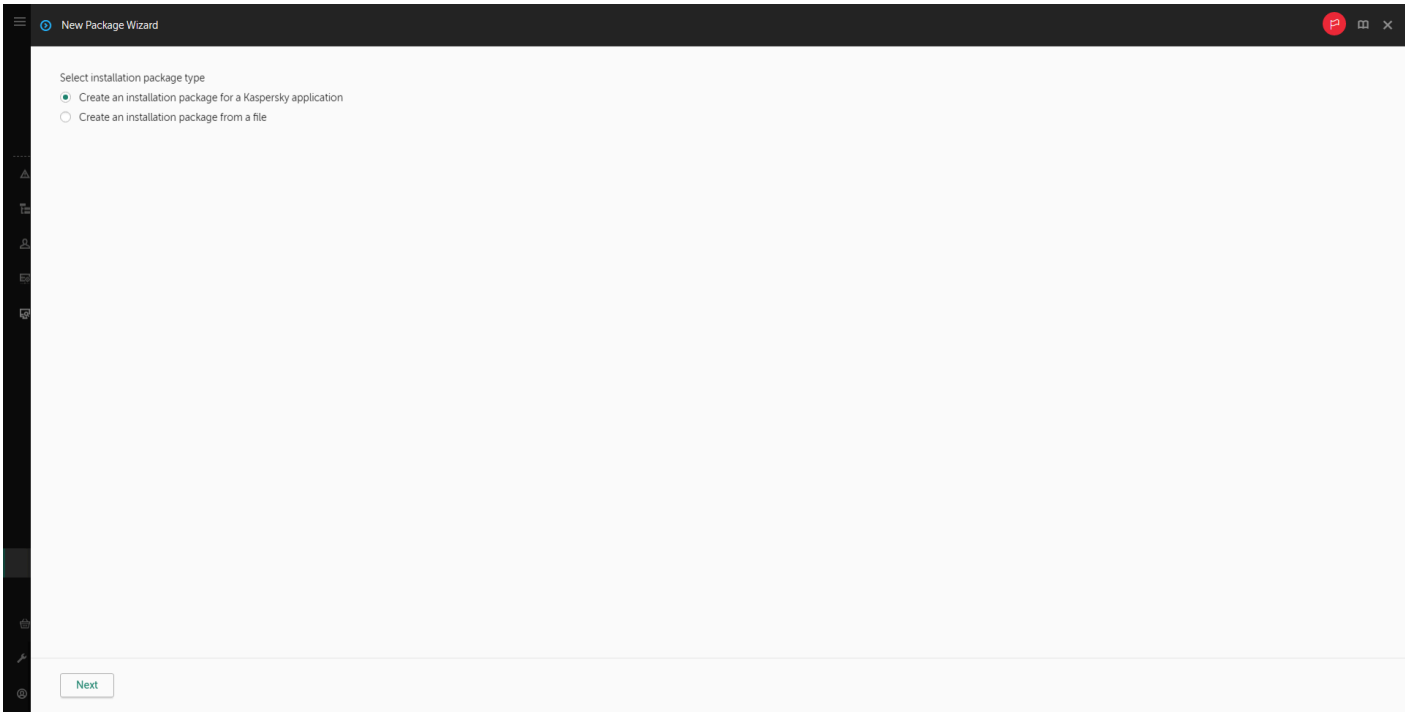
步骤 1. 选择安装包类型

请选择**为卡巴斯基应用程序创建安装包**选项。

向导将根据 Kaspersky 服务器上的分发包创建安装包。该列表在新版本的应用程序发布时会自动更新。建议选择此选项来 安装 Kaspersky Endpoint Security。

您还可以从文件创建安装包。

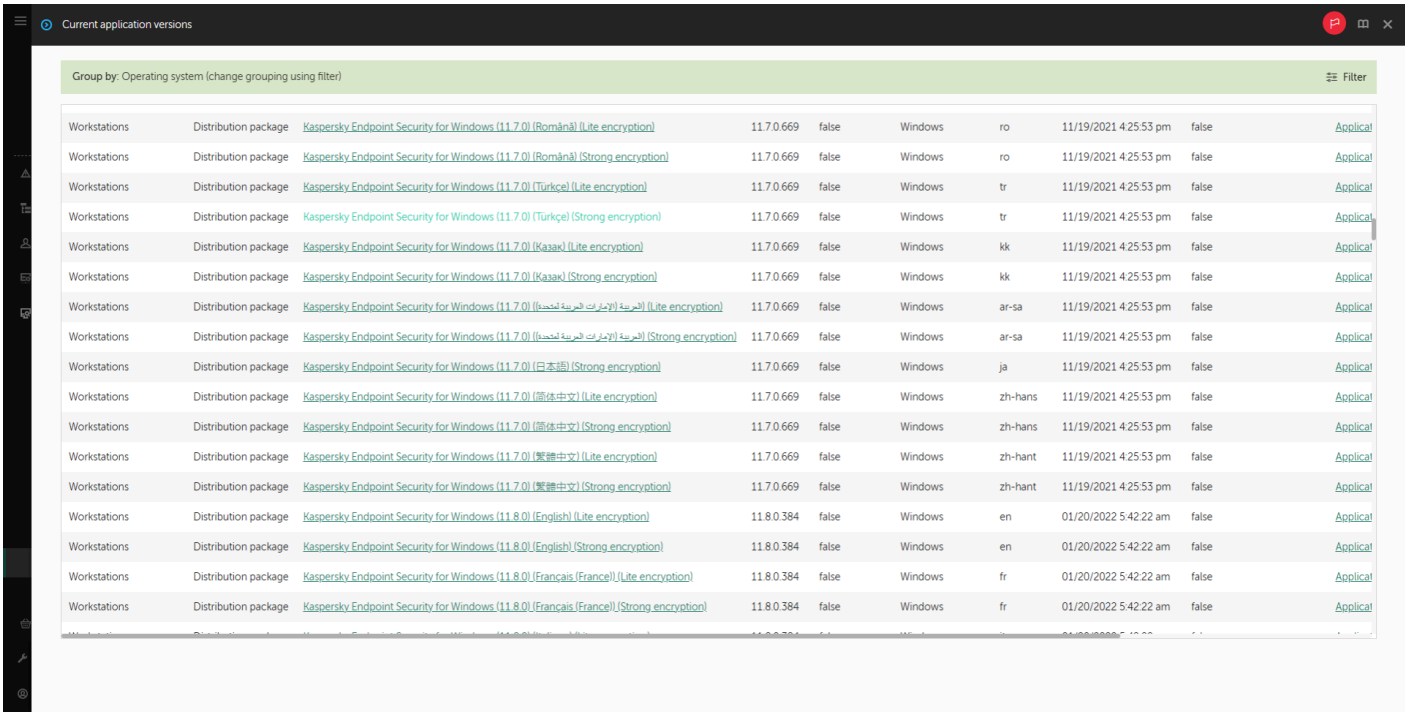
从文件创建 Kaspersky Endpoint Security 的安装包只能在 Kaspersky Security Center Web Console 中实现。



安装包类型

步骤 2. 安装包

选择 Kaspersky Endpoint Security for Windows 安装包。安装包创建过程启动。在安装包创建期间，您必须接受最终用户授权许可协议和隐私策略的条款。



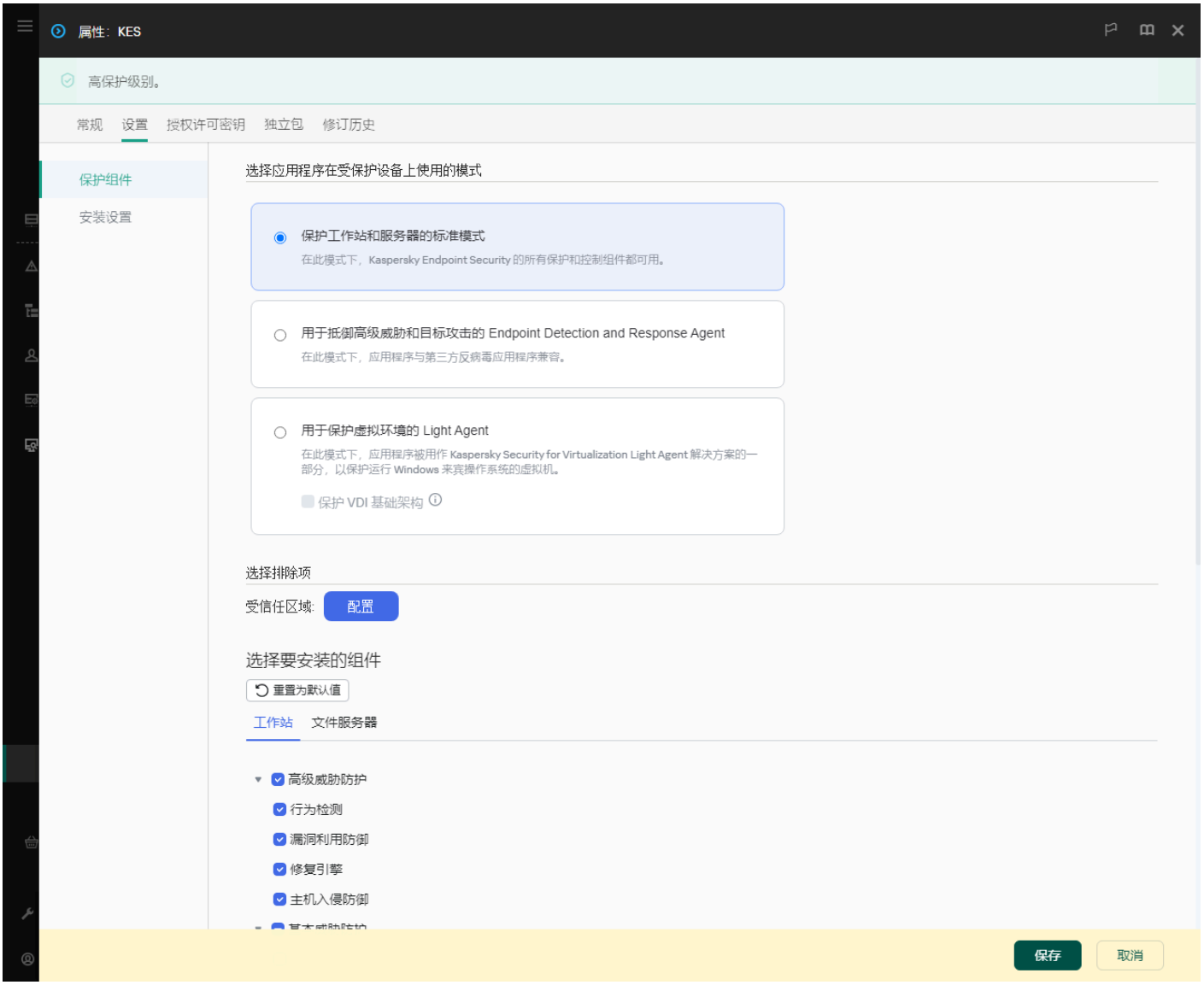
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Română) (Lite encryption)	11.7.0.669	false	Windows	ro	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Română) (Strong encryption)	11.7.0.669	false	Windows	ro	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Türkçe) (Lite encryption)	11.7.0.669	false	Windows	tr	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Türkçe) (Strong encryption)	11.7.0.669	false	Windows	tr	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Қазақ) (Lite encryption)	11.7.0.669	false	Windows	kk	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (Қазақ) (Strong encryption)	11.7.0.669	false	Windows	kk	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (العربية (الإمارات العربية المتحدة)) (Lite encryption)	11.7.0.669	false	Windows	ar-sa	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (العربية (الإمارات العربية المتحدة)) (Strong encryption)	11.7.0.669	false	Windows	ar-sa	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (日本語) (Strong encryption)	11.7.0.669	false	Windows	ja	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (简体中文) (Lite encryption)	11.7.0.669	false	Windows	zh-hans	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (简体中文) (Strong encryption)	11.7.0.669	false	Windows	zh-hans	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (繁體中文) (Lite encryption)	11.7.0.669	false	Windows	zh-hant	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.7.0) (繁體中文) (Strong encryption)	11.7.0.669	false	Windows	zh-hant	11/19/2021 4:25:53 pm	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.8.0) (English) (Lite encryption)	11.8.0.384	false	Windows	en	01/20/2022 5:42:22 am	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.8.0) (English) (Strong encryption)	11.8.0.384	false	Windows	en	01/20/2022 5:42:22 am	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.8.0) (Français (France)) (Lite encryption)	11.8.0.384	false	Windows	fr	01/20/2022 5:42:22 am	false	Applicat
Workstations	Distribution package	Kaspersky Endpoint Security for Windows (11.8.0) (Français (France)) (Strong encryption)	11.8.0.384	false	Windows	fr	01/20/2022 5:42:22 am	false	Applicat

卡巴斯基服务器安装包列表

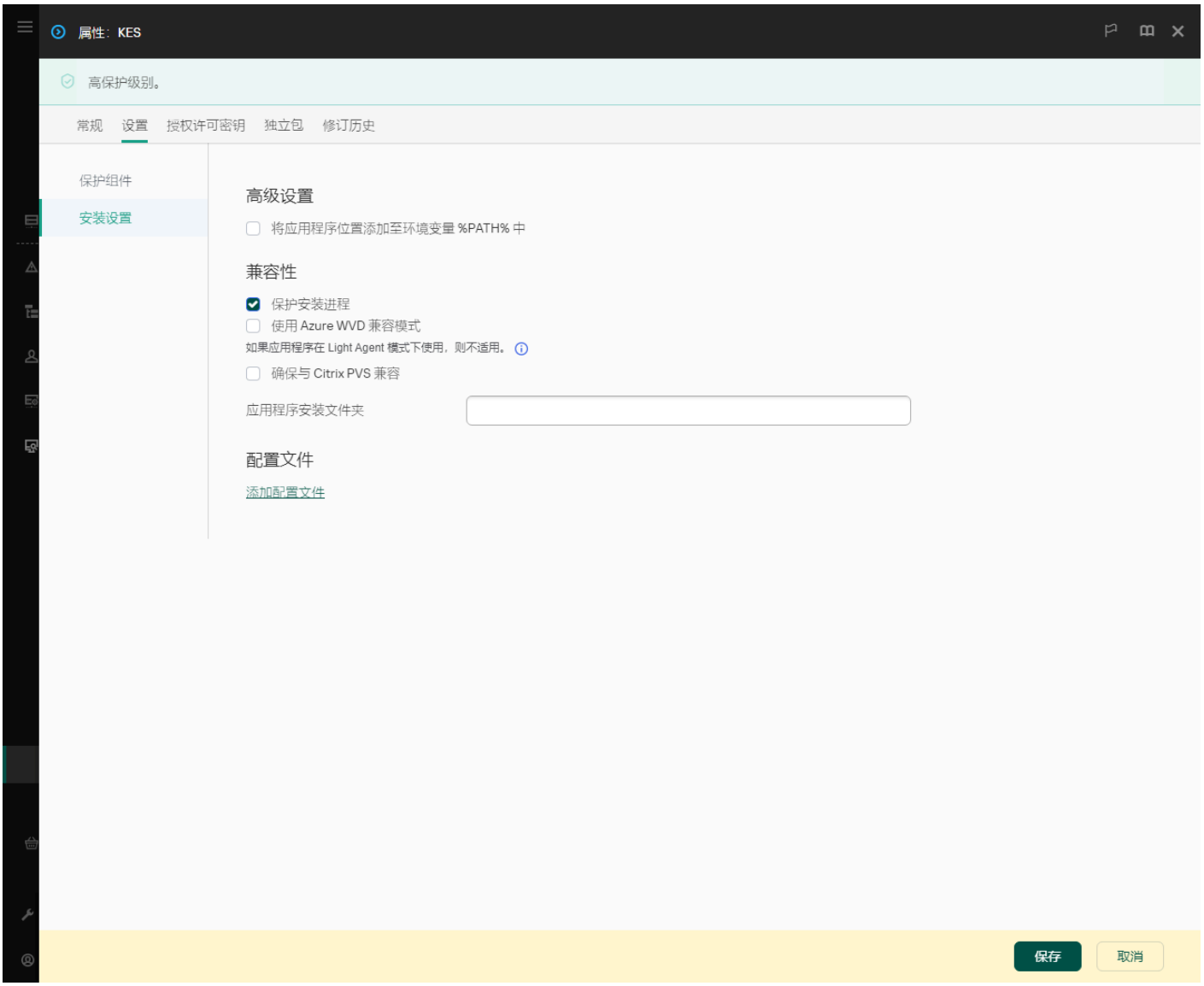
安装包将被创建并添加到 Kaspersky Security Center 中。使用安装包，您可以在企业网络计算机上安装 Kaspersky Endpoint Security 或更新应用程序版本。

在安装包设置中，您可以针对不同的操作系统类型选择应用程序组件。也就是说，安装包包含两套组件：用于工作站的和用于服务器的。在部署安装包之前，安装程序会检测操作系统的类型，并仅安装您为该操作系统类型选择的应用程序组件。这样，您就可以对工作站和服务器使用相同的安装包。

安装包包含来自管理服务器存储库的反病毒数据库。您可以更新安装包中的数据库，以减少在安装 Kaspersky Endpoint Security 之后更新数据库时的流量消耗。



安装包中包含的组件



安装包的安装设置

安装包设置

区域	描述
保护组件	"**标准模式**"。默认配置。此配置允许您使用应用程序的所有组件，包括为 Detection and Response 解决方案提供支持的组件。此配置用于全面保护计算机免受各种威胁、网络攻击和欺诈。 "**Endpoint Detection and Response Agent**"。在此配置下，您只能安装为 Detection and Response 解决方案提供支持的组件：MDR、EDR (KATA)、NDR (KATA)、EDR Expert (on-premises) 和 KUMA。如果您的组织中与 Kaspersky Detection and Response 解决方案一起部署了第三方Endpoint Protection Platform (EPP)，则需要此配置。这使得在 Endpoint Detection and Response Agent 配置下的 Kaspersky Endpoint Security 与第三方 EPP 应用程序兼容。 "**用于保护虚拟环境的 Light Agent**"。此配置适用于作为 Kaspersky Security for Virtualization Light Agent 解决方案的一部分使用的应用程序。Light Agent 必须安装在需要使用解决方案保护的每个虚拟机上。在此配置中，您不能使用数据加密组件或自适应异常控制。如果您正在虚拟机模板上安装 Light Agent，该模板将用于创建*非持久虚拟机*，选择"**保护 VDI 基础架构**"复选框（VDI 代表 Virtual Desktop Infrastructure）。VDI 保护模式能够在临时虚拟机上优化 Kaspersky Endpoint Security 的性能。在此模式下，Light Agent 会拒绝需要重新启动虚拟机的应用程序更新。当接收到需要重新启动的应用程序更新时，Light Agent 会生成需要更新受保护虚拟机模板的事件。
排除项	从 Kaspersky Endpoint Security 12.6 for Windows 开始，扫描排除项和受信任的应用程序被添加到信任区域。预定义的扫描排除项和受信任的应用程序有助于在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上快速配置 Kaspersky Endpoint Security。这意味着您不需要在服务器上为应用程序手动设置信任区域。 从 Kaspersky Endpoint Security 12.8 for Windows 开始，您可以在 Light Agent 模式下安装该应用程序来保护虚拟环境。预定义的扫描排除项和受信任的应用程序可以帮助您在 Citrix 和 VMware 虚拟环境中快速配置 Kaspersky Endpoint Security。 您还可以稍后在策略属性中配置受信任区域：扫描排除项和受信任的应用程序。

区域	描述
选择要安装的组件	在此区域中，可以选择将可用的应用程序组件。您可以在稍后使用"*更改应用程序组件*"任务更改应用程序组件集。 您可以为工作站和服务器创建单独的组件集。在部署安装包之前，安装程序会检测操作系统的类型，并仅安装您为该操作系统类型选择的应用程序组件。这样，您就可以对工作站和服务器使用相同的安装包。 可用组件集取决于应用程序的配置： **标准模式** 默认情况下不安装"BadUSB 攻击防护"组件、"Detection and Response"组件和数据加密组件。这些组件可以在安装包设置中添加。 **Endpoint Detection and Response Agent** 在此配置中，只有 Kaspersky Detection and Response 解决方案的内置代理可用。 **用于保护虚拟环境的 Light Agent** 在此配置中，您可以使用"**标准模式**"配置中几乎所有可用的应用程序组件，数据加密组件和自适应异常控制除外。
授权许可密钥	在本节中，您可以激活应用程序。要激活应用程序，您必须选择授权许可密钥。在执行此操作之前，您必须将密钥添加到管理服务器。有关将密钥添加到 Kaspersky Security Center 管理服务器的详细信息，请参阅 Kaspersky Security Center 帮助。
不兼容的应用程序	请仔细阅读不兼容应用程序列表并允许删除这些应用程序。如果计算机上安装了不兼容的应用程序，安装 Kaspersky Endpoint Security 将以出错结束。
安装设置	"**将 avp.com 文件路径添加至系统变量 %PATH%**"。您可以将安装路径添加到 %PATH% 变量中，以方便使用命令行界面。 "**保护安装进程**"。安装保护包括防止分发包被替换为恶意应用程序、阻止对 Kaspersky Endpoint Security 安装文件夹的访问，以及阻止对包含应用程序密钥的系统注册表部分的访问。但是，如果无法安装应用程序（例如，当使用Windows Remote Desktop执行远程安装时），我们建议您禁用安装过程的保护。 "**确保与 Citrix PVS 兼容**"。您可以启用 Citrix Provisioning Services 支持以将 Kaspersky Endpoint Security 安装到虚拟机。 "**使用 Azure WVD 兼容模式**"。此功能可确保在 Kaspersky Anti Targeted Attack Platform 控制台中正确显示 Azure 虚拟机状态。为了监控计算机的性能，Kaspersky Endpoint Security 将遥测数据发送到 KATA 服务器。遥测包括计算机的 ID（Sensor ID）。Azure WVD 兼容模式允许为这些虚拟机分配永久唯一的 Sensor ID。如果关闭兼容模式，由于 Azure 虚拟机的工作方式，Sensor ID 可能会在计算机重新启动后发生变化。这可能会导致控制台上出现重复的虚拟机。 "**应用程序安装文件夹**"。您可以更改客户端计算机上的 Kaspersky Endpoint Security 安装路径。默认情况下，应用程序安装在文件夹 `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.1` 中。 "**配置文件**"。使用预定义设置安装应用程序。为此，您需要上传定义了 Kaspersky Endpoint Security 设置的文件。您可以在应用程序的本地界面中创建配置文件。

更新安装包中的数据库

安装包包含来自管理服务器存储库的反病毒数据库，这些数据库在创建安装包时是最新的。创建安装包后，可以更新安装包中的反病毒数据库。这样可以减少在安装 Kaspersky Endpoint Security 后更新反病毒数据库时的流量消耗。

要更新管理服务器存储库中的反病毒数据库，请使用管理服务器的"*将更新下载至管理服务器存储库*"任务。有关更新管理服务器存储库中的反病毒数据库的详细信息，请参阅 Kaspersky Security Center 帮助。

> 您只能在管理控制台和 Kaspersky Security Center Web Console 中更新安装包中的数据库。无法在 Kaspersky Security Center 云控制台中更新安装包中的数据库。

如何通过管理控制台 (MMC) 更新安装包中的反病毒数据库

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择"**高级**" → "**远程安装**" → "**安装包**"文件夹。
   这将打开已下载到 Kaspersky Security Center 的安装包列表。
3. 打开安装包的属性。
4. 在"**常规**"区域中单击"**更新数据库**"。

结果，将从管理服务器存储库更新安装包中的反病毒数据库。分发包中包含的 `bases.cab` 文件将被 `bases` 文件夹替换。更新包文件将位于该文件夹中。

如何通过 Web Console 更新安装包中的反病毒数据库

1. 在 Web Console 的主窗口中，选择“**发现和部署**” → “**部署和分配**” → “**安装包**”。

   这将打开已下载到 Web Console 的安装包列表。

2. 单击要更新其中的反病毒数据库的 Kaspersky Endpoint Security 安装包的名称。

   安装包属性窗口将打开。

3. 在“**常规信息**”选项卡上，单击“**更新数据库**”链接。

结果，将从管理服务器存储库更新安装包中的反病毒数据库。分发包中包含的 `bases.cab` 文件将被 `bases` 文件夹替换。更新包文件将位于该文件夹中。

创建远程安装任务

“*远程安装应用程序*”任务旨在远程安装 Kaspersky Endpoint Security。“*远程安装应用程序*”任务允许您将应用程序的安装包部署到组织中的所有计算机。在部署安装软件包之前，您可以更新安装包内的反病毒数据库，并在安装包的属性中选择可用的应用程序组件。

如何在管理控制台 (MMC) 中创建远程安装任务

1. 打开 Kaspersky Security Center Administration Console。

2. 在控制台树中，选择“**任务**”。

   任务列表打开。

3. 单击“**新任务**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 选择任务类型

选择“**Kaspersky Security Center 管理服务器**” → “**远程安装应用程序**”。

步骤 2. 选择安装包

从列表中选择 Kaspersky Endpoint Security 安装包。如果列表不包含 Kaspersky Endpoint Security 安装包，可以在向导中创建安装包。

您可以在 Kaspersky Security Center 中配置安装包设置。例如，您可以选择将安装到计算机的应用程序组件。

网络代理也将与 Kaspersky Endpoint Security 一起安装。*网络代理*可促进管理服务器与客户端计算机之间的交互。如果计算机上已安装网络代理，则不会再次安装。

步骤 3. 其他

选择网络代理安装包。所选版本的网络代理将与 Kaspersky Endpoint Security 一起安装。

步骤 4. 设置

配置以下其他应用程序设置：

- "**强制下载安装包**"。选择应用程序安装方法：
  - "**使用网络代理**"。网络代理负责将 Kaspersky Endpoint Security 安装包分发到客户端计算机。如果未安装网络代理，则任务将以错误结束。在这种情况下，请将网络代理安装包添加到"*远程安装应用程序*"任务并通过操作系统资源实现文件传输。然后，网络代理将使用操作系统资源进行安装。然后通过网络代理的工具安装 Kaspersky Endpoint Security。
  - "**通过分发点使用操作系统资源**"。通过分发点使用操作系统资源将安装包传输到客户端计算机。如果网络中有至少一个分发点，则可以选择此选项。有关分发点的详细信息，请参阅 Kaspersky Security Center 帮助。
  - "**通过管理服务器使用操作系统资源**"。文件将通过管理服务器使用操作系统资源传送到客户端计算机。如果客户端计算机上未安装网络代理，但客户端计算机与管理服务器在同一网络中，可以选择此选项。
- "**通过其他管理服务器管理的设备的行为**"。选择 Kaspersky Endpoint Security 安装方法。如果网络中安装了多个管理服务器，这些管理服务器可能看到相同的客户端计算机。例如，这可能导致通过不同的管理服务器在同一客户端计算机上多次远程安装同一应用程序，或产生其他冲突。
- "**如果已经安装应用程序则不再重新安装**"。例如，如果要安装较早版本的应用程序，则清除此复选框。

步骤 5. 选择操作系统重启设置

选择当需要重新启动计算机时所执行的操作。安装 Kaspersky Endpoint Security 时，不需要重新启动。仅当在安装前必须删除不兼容的应用程序时，才需要重新启动。更新应用程序版本时也可能需要重新启动。

步骤 6. 选择任务将分配到的设备

选择要安装 Kaspersky Endpoint Security 的计算机。下列选项可用：

- 将任务分配给管理组。在这种情况下，任务分配给先前创建的管理组中包括的计算机。
- 选择管理服务器在网络中检测到的计算机：*未分配设备*。网络代理不会安装在未分配设备上。在这种情况下，任务将分配给特定设备。特定设备可包括管理组中的设备以及未分配设备。
- 手动指定设备地址或从列表中导入地址。您可以指定您要将任务分配给的设备的 NetBIOS 名称、IP 地址和 IP 子网。

步骤 7. 选择要运行任务的账户

选择用于使用操作系统工具安装网络代理的账户。在这种情况下，访问计算机需要管理员权限。您可以添加多个账户。如果某个账户没有足够权限，安装向导将使用下一个账户。如果使用网络代理工具安装 Kaspersky Endpoint Security，则无需选择账户。

步骤 8. 配置任务启动计划

配置启动任务的计划，例如，手动或在计算机空闲时。

步骤 9. 定义任务名称

输入任务的名称，例如“*安装 Kaspersky Endpoint Security for Windows 14.1*”。

步骤 10.完成任务创建

退出向导。如有必要，选中“**向导完成时运行任务**”复选框。您可以在任务属性中监控任务进度。应用程序将以静默模式安装。安装后，图标将添加到用户计算机的通知区域。如果图标看起来像，请确保您已激活应用程序。

如何在 Web Console 和云控制台中创建远程安装任务

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**任务**”。
   任务列表打开。
2. 单击“**添加**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 配置常规任务设置

配置常规任务设置：

1. 在“**应用程序**”下拉列表中，选择“**Kaspersky Security Center**”。
2. 在“**任务类型**”下拉列表中，选择“**远程安装应用程序**”。
3. 在“**任务名称**”字段中，输入简要说明，例如，“*为经理安装 Kaspersky Endpoint Security*”。
4. 在“**要对其分配任务的设备**”块，选择任务范围。

步骤 2. 选择要进行安装的计算机

在此步骤中，按照选定的任务范围选项，选择要安装 Kaspersky Endpoint Security 的计算机。

步骤 3. 配置安装包

在此步骤中，配置安装包：

1. 选择 Kaspersky Endpoint Security for Windows （14.1）安装包。

2. 选择网络代理安装包。

   所选版本的网络代理将与 Kaspersky Endpoint Security 一起安装。*网络代理*可促进管理服务器与客户端计算机之间的交互。如果计算机上已安装网络代理，则不会再次安装。

3. 在“**强制下载安装包**”块中，选择应用程序安装方法：

   - “**使用网络代理**”。网络代理负责将 Kaspersky Endpoint Security 安装包分发到客户端计算机。如果未安装网络代理，则任务将以错误结束。在这种情况下，请将网络代理安装包添加到“*远程安装应用程序*”任务并通过操作系统资源实现文件传输。然后，网络代理将使用操作系统资源进行安装。然后通过网络代理的工具安装 Kaspersky Endpoint Security。

   - “**通过分发点使用操作系统资源**”。通过分发点使用操作系统资源将安装包传输到客户端计算机。如果网络中有至少一个分发点，则可以选择此选项。有关分发点的详细信息，请参阅 Kaspersky Security Center 帮助。

   - “**通过管理服务器使用操作系统资源**”。文件将通过管理服务器使用操作系统资源传送到客户端计算机。如果客户端计算机上未安装网络代理，但客户端计算机与管理服务器在同一网络中，可以选择此选项。

4. 在“**同时下载的最大数量**”字段中，设置发送到管理服务器的安装包下载请求数量限制。限制请求数有助于防止网络过载。

5. 在“**安装尝试最大数量**”字段中，设置应用程序安装尝试次数限制。如果安装 Kaspersky Endpoint Security 以出错结束，任务将自动再次启动安装。

6. 如有必要，清空“**如果已经安装应用程序则不再重新安装**”复选框。例如，这样可以安装应用程序的一个先前版本。

7. 如有必要，清空“**下载之前验证操作系统类型**”复选框。这样可避免在计算机的操作系统不符合软件要求时下载应用程序分发包。如果您确定计算机的操作系统符合软件要求，可以跳过此验证。

8. 如有必要，选中“**在 Active Directory 组策略中指定安装包的安装**”复选框。Kaspersky Endpoint Security 通过网络代理安装或通过 Active Directory 手动安装。要安装网络代理，必须以域管理员权限运行远程安装任务。

9. 如有必要，选中“**提示用户关闭运行中应用程序**”复选框。安装 Kaspersky Endpoint Security 会占用计算机资源。为方便用户，应用程序安装向导会在开始安装前提示您关闭正在运行的应用程序。这有助于防止其他应用程序运行中端，并防止可能的计算机故障。

10. 在“**通过其他管理服务器管理的设备的行为**”块中，选择 Kaspersky Endpoint Security 安装方法。如果网络中安装了多个管理服务器，这些管理服务器可能看到相同的客户端计算机。例如，这可能导致通过不同的管理服务器在同一客户端计算机上多次远程安装同一应用程序，或产生其他冲突。

步骤 4. 选择要运行任务的账户

选择用于使用操作系统工具安装网络代理的账户。在这种情况下，访问计算机需要管理员权限。您可以添加多个账户。如果某个账户没有足够权限，安装向导将使用下一个账户。如果使用网络代理工具安装 Kaspersky Endpoint Security，则无需选择账户。

步骤 5. 完成任务创建

单击“**完成**”按钮完成向导。在任务列表中将显示一个新任务。要运行任务，请选中与任务对应的复选框，然后单击“**开始**”按钮。应用程序将以静默模式安装。安装后，图标将添加到用户计算机的通知区域。如果图标看起来像，请确保您已激活应用程序。

使用向导在本地安装应用程序

应用程序安装向导的界面包含了对应于应用程序安装步骤的一系列窗口。确保运行安装向导的用户账户属于管理员组。

使用“安装向导”安装程序或从上一版本升级程序：

1. 复制分发包文件夹到用户计算机。
2. 运行 setup_kes.exe。

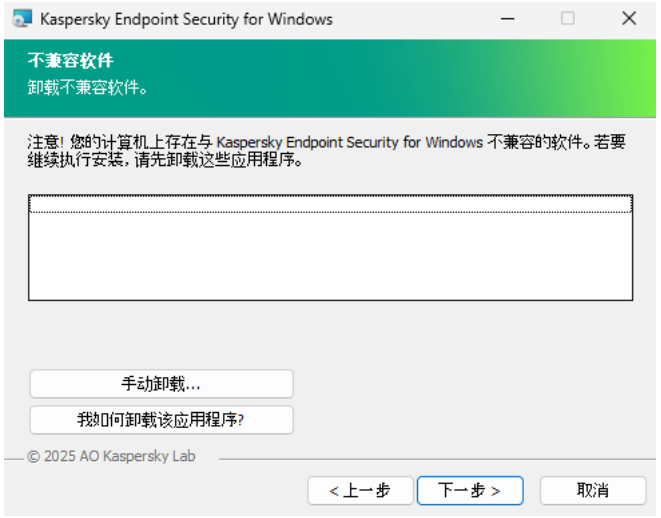
   “安装向导”将启动。

准备安装

在计算机上安装 Kaspersky Endpoint Security 或从先前版本升级之前，将检查以下条件：

- 是否安装了任何可能与 Kaspersky Endpoint Security 存在兼容性问题的软件（软件列表可在分发包中的 incompatible.txt 文件中找到）。
- 无论是否满足软硬件要求。
- 是否存在 Microsoft .NET Framework。
- 用户是否有权限安装软件产品。

如果不满足以上任何要求，系统将在计算机屏幕上显示相关通知。例如，关于不兼容软件的通知（参见下图）。



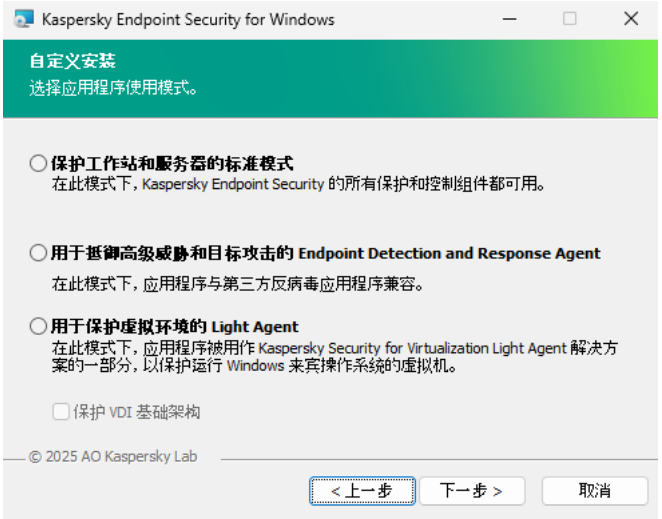
删除不兼容的软件

如果计算机满足列出的要求，“安装向导”将搜索应用程序安装期间可能导致冲突的卡巴斯基应用程序。如果找到这样的程序，系统将提示您手动删除它们。

如果检测到的应用包括以前版本的 Kaspersky Endpoint Security，所有可以被迁移的数据（如激活数据和应用程序设置）会在安装 Kaspersky Endpoint Security 14.1 for Windows 时被保留和使用，以前版本的应用程序将被自动删除。这适用于以下应用程序版本:

- Kaspersky Endpoint Security 12.1 for Windows（版本 12.1.0.506）
- Kaspersky Endpoint Security 12.2 for Windows（版本 12.2.0.462）
- Kaspersky Endpoint Security 12.3 for Windows（版本 12.3.0.493）
- Kaspersky Endpoint Security 12.4 for Windows（版本 12.4.0.467）
- Kaspersky Endpoint Security 12.5 for Windows（版本 12.5.0.539）
- Kaspersky Endpoint Security 12.6 for Windows（版本 12.6.0.438）
- Kaspersky Endpoint Security 12.7 for Windows（版本 12.7.0.533）
- Kaspersky Endpoint Security 12.8 for Windows（版本 12.8.0.505）
- Kaspersky Endpoint Security 12.9 for Windows（版本 12.9.0.384）
- Kaspersky Endpoint Security 12.10 for Windows（版本 12.10.0.466）
- Kaspersky Endpoint Security 12.11 for Windows（版本 12.11.0.637）
- Kaspersky Endpoint Security 12.12 for Windows（版本 12.12.0.522）
- Kaspersky Endpoint Security 14.0 for Windows（版本 14.0.0.504）

Kaspersky Endpoint Security 的配置



选择应用程序的配置

“**标准模式**”。默认配置。此配置允许您使用应用程序的所有组件，包括为 Detection and Response 解决方案提供支持的组件。此配置用于全面保护计算机免受各种威胁、网络攻击和欺诈。

“**Endpoint Detection and Response Agent**”。在此配置下，您只能安装为 Detection and Response 解决方案提供支持的组件： MDR、EDR (KATA)、NDR (KATA)、EDR Expert (on-premises) 和 KUMA。如果您的组织中与 Kaspersky Detection and Response 解决方案一起部署了第三方Endpoint Protection Platform (EPP)，则需要此配置。这使得在 Endpoint Detection and Response Agent 配置下的 Kaspersky Endpoint Security 与第三方 EPP 应用程序兼容。

“**用于保护虚拟环境的 Light Agent**”。此配置适用于作为 Kaspersky Security for Virtualization Light Agent 解决方案的一部分使用的应用程序。Light Agent 必须安装在需要使用解决方案保护的每个虚拟机上。在此配置中，您不能使用数据加密组件或自适应异常控制。如果您正在虚拟机模板上安装 Light Agent，该模板将用于创建*非持久虚拟机*，选择“**保护 VDI 基础架构**”复选框（VDI 代表 Virtual Desktop Infrastructure）。VDI 保护模式能够在临时虚拟机上优化 Kaspersky Endpoint Security 的性能。在此模式下，Light Agent 会拒绝需要重新启动虚拟机的应用程序更新。当接收到需要重新启动的应用程序更新时，Light Agent 会生成需要更新受保护虚拟机模板的事件。

Kaspersky Endpoint Security 组件

在安装过程中，您可以选择想要安装的 Kaspersky Endpoint Security 组件（参见下图）。“文件威胁防护”组件是必须安装的必备组件。您无法取消其安装。

选择要安装的应用程序组件

默认情况下，除了以下组件之外选定安装所有应用程序组件：

- BadUSB 攻击防护。
- 数据加密组件。
- Detection and Response 组件。

安装应用程序后，您可以更改可用的应用程序组件。为此，您需要再次运行安装向导，然后选择更改可用组件。

如果您需要安装 Detection and Response 组件，Kaspersky Endpoint Security 支持以下配置：

- 仅 Endpoint Detection and Response Optimum
- 仅 Endpoint Detection and Response Expert (cloud)
- 仅 Endpoint Detection and Response Expert (on-premises)
- 仅 Network Detection and Response (KATA)
- 仅 Sandbox
- Endpoint Detection and Response Optimum 和 Sandbox
- Endpoint Detection and Response Expert (cloud) 和 Sandbox
- Endpoint Detection and Response Expert (on-premises) 和 Sandbox
- Network Detection and Response (KATA) 和 Endpoint Detection and Response Expert (on-premises)
- Network Detection and Response (KATA) 和 Managed Detection and Response

Kaspersky Endpoint Security 在安装应用程序之前验证选择的组件。如果所选的 Detection and Response 组件配置不被支持，Kaspersky Endpoint Security 无法被安装。

选择安装应用程序的文件夹

您可以更改客户端计算机上的 Kaspersky Endpoint Security 安装路径。默认情况下，应用程序安装在文件夹 `%ProgramFiles(x86)%\Kaspersky Lab\KES.14.1` 中。

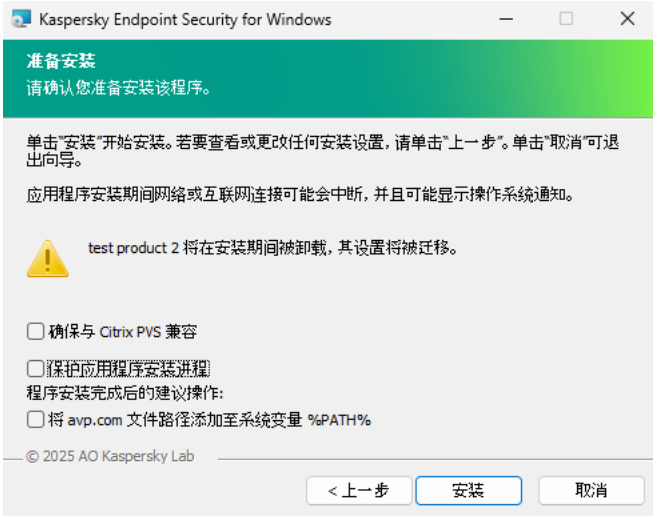
配置受信任区域

从 Kaspersky Endpoint Security 12.6 for Windows 开始，扫描排除项和受信任的应用程序被添加到信任区域。预定义的扫描排除项和受信任的应用程序有助于在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上快速配置 Kaspersky Endpoint Security。这意味着您不需要在服务器上为应用程序手动设置信任区域。

从 Kaspersky Endpoint Security 12.8 for Windows 开始，您可以在 Light Agent 模式下安装该应用程序来保护虚拟环境。预定义的扫描排除项和受信任的应用程序可以帮助您在 Citrix 和 VMware 虚拟环境中快速配置 Kaspersky Endpoint Security。

您还可以稍后在策略属性中配置受信任区域：扫描排除项和受信任的应用程序。

高级设置



高级应用程序安装设置

"**保护应用程序安装进程**"。安装保护包括防止分发包被替换为恶意应用程序、阻止对 Kaspersky Endpoint Security 安装文件夹的访问，以及阻止对包含应用程序密钥的系统注册表部分的访问。但是，如果无法安装应用程序（例如，当使用Windows Remote Desktop执行远程安装时），我们建议您禁用安装过程的保护。

"**确保与 Citrix PVS 兼容**"。您可以启用 Citrix Provisioning Services 支持以将 Kaspersky Endpoint Security 安装到虚拟机。

“**将 avp.com 文件路径添加至系统变量 %PATH%**”。您可以将安装路径添加到 %PATH% 变量中，以方便使用命令行界面。

使用系统中心配置管理器远程安装应用程序

这些指南适用于 System Center Configuration Manager 2012 R2。

若要使用系统中心配置管理器远程安装应用程序：

1. 打开配置管理器控制台。
2. 在控制台右侧，在“**应用管理**”块中选择“**软件包**”。
3. 在控制面板中控制台右上部分，单击“**创建安装包**”按钮。
   这会启动“*新建软件包和应用程序向导*”。
4. 在新建软件包和应用程序向导中：
   a. 在“**软件包**”区域中：
      - 在“**名称**”字段中输入安装包名称。
      - 在“**源文件夹**”字段中指定包含 Kaspersky Endpoint Security 分发包的文件夹的路径。
   b. 在“**应用程序类型**”区域中选择“**标准程序**”选项。
   c. 在“**标准程序**”区域中：
      - 在“**名称**”字段中，输入安装包的唯一名称（例如包含版本的应用程序名称）。
      - 在“**命令行**”字段中从命令行中指定 Kaspersky Endpoint Security 安装选项。
      - 单击“**浏览**”按钮指定应用程序可执行文件的路径。
      - 确保**运行模式**列表选择了**使用管理权限运行**项。
   d. 在“**要求**”区域中：
      - 如果您希望在安装 Kaspersky Endpoint Security 之前启用其他应用程序，则选择“**首先运行其他程序**”复选框。
        从“**应用程序**”下拉列表中选择该应用程序，或者单击“**浏览**”按钮指定该应用程序可执行文件的路径。
      - 如果您希望只在指定操作系统中安装该应用程序，则选择“**平台要求**”块中的“**此程序只能在指定的平台上运行**”选项。
        在该列表中选择要安装 Kaspersky Endpoint Security 的操作系统旁的复选框。

      该步骤为可选项。
   e. 在“**摘要**”区域中选中所有输入的设置值，单击“**下一步**”。

创建的安装包将显示在可用安装包列表的“**软件包**”区域中。

5. 在安装包的上下文菜单中，选择“**部署**”。
   这将启动“*部署指南*”。

6. 在部署向导中：

   a. 在“**常规**”区域中：

      - 在“**软件**”字段中输入安装包的唯一名称或者单击“**浏览**”按钮从列表中选择安装包。
      - 在“**集合**”字段中输入要安装应用程序的计算机集合的名称，或者单击“**浏览**”按钮选择集合。

   b. 在“**包括**”区域中，添加分发点（有关详情，请参阅系统中心配置管理器的帮助文档）。

   c. 如有必要，在部署向导中指定其他设置的值。这些设置是 Kaspersky Endpoint Security 远程安装的可选项。

   d. 在“**摘要**”区域中选中所有输入的设置值，单击“**下一步**”。

部署向导完成后将创建远程安装 Kaspersky Endpoint Security 的任务。

setup.ini 文件安装设置说明

从命令行安装应用程序或使用 Microsoft Windows 的组策略编辑器时需要使用 setup.ini 文件。要应用 setup.ini 文件中的设置，请将该文件放入包含 Kaspersky Endpoint Security 分发包的文件夹。

仅当在静默模式下安装应用程序时才使用 setup.ini 文件。

您无法将路径添加到 install.cfg setup.ini 文件中的配置文件。如果您将 install.cfg 配置文件放在 Kaspersky Endpoint Security 分发套件所在的文件夹中，则应用程序还将跳过此配置文件。要应用 install.cfg 配置文件中的设置，您需要在以下应用程序安装命令中指定文件路径：`CONFIGPATH=<path to the configuration file>`。

下载 SETUP.INI 文件

setup.ini 文件包含以下部分：

- `[Setup]` – 应用程序安装的常规设置。
- `[Components]` – 选择要在独立模式下安装的应用程序组件。如果未指定任何组件，则安装所有可在操作系统中使用的组件。“文件威胁防护”是强制性组件，无论该区域中表明的是哪种设置都会安装在计算机上。
- `[Tasks]` – 选择要包含在 Kaspersky Endpoint Security 任务列表中的任务。如果未指定任务，则将所有任务包括在 Kaspersky Endpoint Security 的任务列表中。

> `1` 值的替代值可为 `yes`, `on`, `enable`, `enabled` 和 `true`。`0` 值的替代值可为 `no`, `off`, `disable`, `disabled` 和 `false`。

setup.ini 文件的设置

区域	参数	描述
`[Setup]`	`InstallDir`	应用程序安装文件夹的路径。
	`ActivationCode`	Kaspersky Endpoint Security 激活码。
	`Eula`	接受最终用户授权许可协议的条款。许可协议的内容包括在 Kaspersky Endpoint Security 分发套装中。 必须接受最终用户授权许可协议的条款才能安装应用程序或升级应用程序版本。
	`PrivacyPolicy`	接受隐私策略。隐私策略的文本包含在 Kaspersky Endpoint Security 分发包中。 要安装应用程序或升级应用程序版本，您必须接受隐私策略。
	`KSN`	接受或拒绝参与卡巴斯基安全网络（KSN）。如果没有为此参数设置任何值，在首次启动 Kaspersky Endpoint Security 时，Kaspersky Endpoint Security 将提示您确认同意或拒绝加入 KSN。可用值： • `1` – 同意加入 KSN。 • `0` – 拒绝加入 KSN（默认值）。 Kaspersky Endpoint Security 分发包已针对与卡巴斯基安全网络（KSN）配合使用进行优化。如果您选择不加入卡巴斯基安全网络，则应该在安装完成后立即更新 Kaspersky Endpoint Security。
	`CLEANERSIGNCHECK`	验证 incompatible.txt 列表中检测到的软件文件的数字签名。要删除该软件，Kaspersky Endpoint Security 会运行软件安装程序文件。如果安装程序文件没有数字签名，Kaspersky Endpoint Security 会认为该文件不受信任，并停止软件卸载，以避免运行潜在的恶意代码。如果应用程序无法验证检测到的软件文件的数字签名，Kaspersky Endpoint Security 安装将停止并出现错误。 默认值因软件安装方法而异： • `0` 表示禁用了数字签名验证（如果通过 Kaspersky Security Center 部署，则为默认值）。 • `1` 表示启用了数字签名验证（如果应用程序正在本地安装，则为默认值）。
	`Login`	设置用于访问 Kaspersky Endpoint Security 功能和设置的用户名（“密码保护”组件）。该用户名与“`Password`”和“`PasswordArea`”设置一起进行设置。默认使用用户名 KLAdmin。
	`Password`	指定用于访问 Kaspersky Endpoint Security 功能和设置的密码（该密码与“`Login`”和“`PasswordArea`”参数一起指定）。 如果您指定了口令，但没有指定带有 `Login` 参数的用户名，将默认使用 KLAdmin 用户名。

区域	参数	描述
	PasswordArea	指定用于访问 Kaspersky Endpoint Security 的密码范围。当用户尝试执行包含在此范围中的操作时，Kaspersky Endpoint Security 将提示用户输入账户凭据（"Login"和"Password"参数）。使用";"字符以指定多个值。 可用值： • SET – 修改应用程序设置。 • EXIT – 退出应用程序。 • DISPROTECT – 禁用保护组件并停止扫描任务。 • DISPOLICY – 禁用 Kaspersky Security Center 策略。 • UNINST – 从计算机中删除应用程序。 • DISCTRL – 禁用控制组件。 • REMOVELIC – 删除密钥。 • REPORTS – 查看报告。 • EXPORT – 导出应用程序设置。 例如，PasswordArea=SET;PasswordArea=UNINST;PasswordArea=EXIT。
	SelfProtection	启用或禁用应用程序安装保护机制。可用值： • 1 – 启用程序安装保护机制（默认值）。 • 0 – 禁用程序安装保护机制。 安装保护包括防止分发包被替换为恶意应用程序、阻止对 Kaspersky Endpoint Security 安装文件夹的访问，以及阻止对包含应用程序密钥的系统注册表部分的访问。但是，如果无法安装应用程序（例如，当使用Windows Remote Desktop执行远程安装时），我们建议您禁用安装过程的保护。
	PROTECTOSSERVICES	保护操作系统服务功能。操作系统服务保护防止第三方应用程序干扰操作系统服务的操作。例如，这样的服务包括应用程序自动启动服务。 • 1 表示操作系统服务的保护已启用（默认值）。 • 0 表示操作系统服务的保护被禁用。
	EnableAzureSupport	启用或禁用 Azure WVD 兼容模式。可用值： • 1 – 启用 Azure WVD 兼容模式。 • 0 – 禁用 Azure WVD 兼容模式（默认值）。 此功能可确保在 Kaspersky Anti Targeted Attack Platform 控制台中正确显示 Azure 虚拟机状态。为了监控计算机的性能，Kaspersky Endpoint Security 将遥测数据发送到 KATA 服务器。遥测包括计算机的 ID（Sensor ID）。Azure WVD 兼容模式允许为这些虚拟机分配永久唯一的 Sensor ID。如果关闭兼容模式，由于 Azure 虚拟机的工作方式，Sensor ID 可能会在计算机重新启动后发生变化。这可能会导致控制台上出现重复的虚拟机。
	Reboot	自动重新启动计算机（如果安装或升级应用程序后需要重新启动）。如果未为此参数设置任何值，则阻止计算机自动重启。 安装 Kaspersky Endpoint Security 时，不需要重新启动。仅当在安装前必须删除不兼容的应用程序时，才需要重新启动。更新应用程序版本时也可能需要重新启动。
	AddEnvironment	在 %PATH% 系统变量中，添加位于 Kaspersky Endpoint Security 安装文件夹的可执行文件的路径。可用值： • 1 – 以位于 Kaspersky Endpoint Security 安装文件夹的可执行文件的路径补充 %PATH% 系统变量。 • 0 – 不以位于 Kaspersky Endpoint Security 安装文件夹的可执行文件的路径补充 %PATH% 系统变量。
	AMPPL	启用或禁用 Kaspersky Endpoint Security 进程使用 AM-PPL 技术（Antimalware Protected Process Light）提供的保护。有关 AM-PPL 技术的详细信息，请访问 Microsoft 网站。 AM-PPL 技术适用于 Windows 10 版本 1703 (RS2) 或更高版本以及 Windows Server 2019 操作系统。 可用值： • 1 – 启用 Kaspersky Endpoint Security 进程使用 AM-PPL 技术提供的保护。 • 0 – 禁用 Kaspersky Endpoint Security 进程使用 AM-PPL 技术提供的保护。

区域	参数	描述
	UPGRADEMODE	应用程序升级模式： • Seamless 意味着通过计算机重启升级应用程序（默认值）。 • Force 意味着在不重新启动的情况下升级应用程序。 从 11.10.0 版开始，无需重新启动即可升级应用程序。要升级应用程序的早期版本，必须重新启动计算机。从 11.11.0 版开始，您也可以无需重新启动即可安装补丁。 安装 Kaspersky Endpoint Security 时，不需要重新启动。因此，应用程序的升级模式将在应用程序设置中指定。您可以在应用程序设置或策略中更改此参数。 升级已安装的应用程序时，在 setup.ini 文件中指定的参数的优先级高于在应用程序设置或命令行中指定的参数的优先级。例如，如果在 setup.ini 文件中指定了"Force"升级模式，而在应用程序设置中指定了"Seamless"模式，升级将在不重新启动的情况下安装（Force）。如果您正在使用 setup.ini 文件，其中未指定 UPGRADEMODE 参数，安装程序将使用默认值（Seamless），并在计算机重新启动时安装升级。
	SetupReg	启用将 setup.reg 文件中的注册表项写入注册表。 SetupReg: setup.reg 参数值。
	EnableTraces	启用或禁用应用程序跟踪。Kaspersky Endpoint Security 在启动后将跟踪文件保存在文件夹 %ProgramData%\Kaspersky Lab\KES.14.1\Traces 中。可用值： • 1 – 启用跟踪。 • 0 – 禁用跟踪（默认值）。
	TracesLevel	跟踪详细级别。可用值： • 100（关键）。仅包含有关致命错误的消息。 • 200（高）。有关所有错误的消息，包括致命错误。 • 300（诊断）。有关所有错误的消息以及警告。 • 400（重要）。所有错误消息、警告和其他信息。 • 500（常规）。有关所有错误的消息和警告，以及有关正常模式下应用程序操作的详细信息（默认）。 • 600（低）。所有消息。
	RESTAPI	通过 REST API 管理应用程序。要通过 REST API 管理应用程序，必须指定用户名（RESTAPI_User 参数）。 可用值： • 1 –允许通过 REST API 进行管理。 • 0 –阻止通过 REST API 进行管理（默认值）。 要通过 REST API 管理应用程序，必须允许使用管理系统进行管理。要执行此操作，请设置 AdminKitConnector=1 参数。如果通过 REST API 管理应用程序，则无法使用 Kaspersky 的管理系统来管理应用程序。
	RESTAPI_User	用于通过 REST API 管理应用程序的 Windows 域账户的用户名。只有此用户可以通过 REST API 管理应用程序。输入格式为 <DOMAIN>\<UserName> 的用户名（例如，RESTAPI_User=COMPANY\Administrator）。您只能选择一个用户来使用 REST API。 添加用户名是通过 REST API 管理应用程序的先决条件。
	RESTAPI_Port	用于通过 REST API 管理应用程序的端口。默认情况下使用 6782 端口。确保端口空闲。
	RESTAPI_Certificate	识别请求的证书（例如，RESTAPI_Certificate=C:\cert.pem）。Kaspersky Endpoint Security 与 REST 客户端的安全交互需要配置请求标识。为此，您必须安装证书，然后对每个请求的有效负载进行签名。
	StandaloneMode	在 Endpoint Detection and Response Agent (EDR Agent) 模式下安装应用程序。*Endpoint Detection and Response Agent* 是安装在组织 IT 基础设施中的各个工作站和服务器上的应用程序，用于支持 Kaspersky Managed Detection and Response 和 Kaspersky Anti Targeted Attack Platform 解决方案。EDR Agent 与第三方 EPP 应用程序兼容。这使您可以将第三方基础设施安全工具与卡巴斯基的 Detection and Response 一起使用。 要安装 EDR Agent，请在"[Components]"部分，选择"StandaloneKATA"、"StandaloneNDR"或者"StandaloneMDR"组件。EDR Agent 不支持其他应用程序组件。 可用值： • 1 以 EDR Agent 模式安装应用程序。 • 0 以标准模式（默认）安装应用程序。
	KSVLAMode	以 Light Agent 模式安装应用程序。此配置适用于作为 Kaspersky Security for Virtualization Light Agent 解决方案的一部分使用的应用程序。Light Agent 必须安装在需要使用解决方案保护的每个虚拟机上。 可用值： • 1 以 Light Agent 模式安装应用程序。 • 0 以标准模式（默认）安装应用程序。

区域	参数	描述
	`InstallOnVDI`	在 Light Agent 模式下安装应用程序时启用 VDI 保护模式（`KSVLAMode=1`）。VDI 保护模式能够在临时虚拟机上优化 Kaspersky Endpoint Security 的性能。在此模式下，Light Agent 会拒绝需要重新启动虚拟机的应用程序更新。当接收到需要重新启动的应用程序更新时，Light Agent 会生成需要更新受保护虚拟机模板的事件。 可用值： • `1` 启用 VDI 保护模式。 • `0` 禁用 VDI 保护模式（默认）。
	`KESExclusions`	在服务器上安装应用程序时，添加预定义扫描排除项和受信任的应用程序。预定义的扫描排除项和受信任的应用程序有助于在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上快速配置 Kaspersky Endpoint Security。例如，SQL 服务器的预定义扫描排除项包括 MDF 和 LDF 数据库文件。这意味着您不需要在服务器上为应用程序手动设置信任区域。 可用值： • `1` 添加预定义的扫描排除项和受信任的应用程序。 • `0` 禁用预定义的扫描排除项和受信任的应用程序（默认）。
	`LAExclusions`	在虚拟机上安装应用程序时（Light Agent 模式）添加预定义的扫描排除项和受信任的应用程序。预定义的扫描排除项和受信任的应用程序可以帮助您在 Citrix 和 VMware 虚拟环境中快速配置 Kaspersky Endpoint Security。 可用值： • `1` 添加预定义的扫描排除项和受信任的应用程序。 • `0` 禁用预定义的扫描排除项和受信任的应用程序（默认）。
	`EnableUniqueSensorID`	在安装或更新应用程序期间创建唯一的计算机标识符 (Sensor ID)。Sensor ID 在 Kaspersky Anti Targeted Attack Platform 解决方案中用于识别向服务器发送遥测数据的计算机。在创建 Sensor ID 时，应用程序使用一种考虑到计算机配置（例如主板序列号）的算法。在某些情况下，例如在虚拟环境中使用应用程序时，Sensor ID 可能会重复。因此，Kaspersky Anti Targeted Attack Platform 无法识别发送遥测数据的计算机。要创建唯一的 Sensor ID，您需要设置参数 `EnableUniqueSensorID=1`。因此，应用程序将使用不同的算法来创建 Sensor ID，该算法会考虑有关计算机的其他数据。这确保了 Sensor ID 的唯一。 默认情况下，没有设置该参数。应用程序在以下情况下继承 Sensor ID： • 更新应用程序版本； • 迁移 [KES+KEA] 配置到 [KES+内置代理] 配置 作为应用程序修复的一部分，安装程序尝试继承 Sensor ID。如果 Sensor ID 无法恢复，应用程序会创建一个新的 Sensor ID。
	`CitrixCompatibility`	启用 Citrix Provisioning Services 支持以将 Kaspersky Endpoint Security 安装到虚拟机。
`[Components]`	`ALL`	安装所有组件。如果指定了参数值 `1`，所有组件都将安装，与单个组件的安装设置无关。 由于 Detection and Response 解决方案的支持方式，计算机上已安装 Endpoint Detection and Response Optimum 和 Sandbox 组件。Endpoint Detection and Response Expert (cloud) 组件与此配置不兼容。
	`MailThreatProtection`	邮件威胁防护。
	`WebThreatProtection`	Web 威胁防护。
	`AMSI`	AMSI 保护。
	`HostIntrusionPrevention`	主机入侵防御。
	`BehaviorDetection`	行为检测。
	`ExploitPrevention`	漏洞利用防御。
	`RemediationEngine`	修复引擎。
	`Firewall`	防火墙。
	`NetworkThreatProtection`	网络威胁防护。
	`WebControl`	Web 控制。
	`DeviceControl`	设备控制。
	`ApplicationControl`	应用程序控制。
	`AdaptiveAnomaliesControl`	自适应异常控制。

区域	参数	描述
	`CloudDiscovery`	Cloud Discovery。
	`LogInspector`	日志审查
	`AntiCryptor`	反加密
	`FileThreatProtection`	文件威胁防护。
	`SystemIntegrityMonitor`	系统完整性监控。
	`FileEncryption`	“文件级加密”库。
	`DiskEncryption`	“完整磁盘加密”库。
	`MSBitLocker`	BitLocker 加密管理库。
	`BadUSBAttackPrevention`	BadUSB 攻击防护。
	`EDR`	Endpoint Detection and Response Optimum 该组件与 Endpoint Detection and Response Expert (cloud) (`EDRCloud`) 和 Endpoint Detection and Response Expert (on-premises) (`AntiAPT`) 组件不兼容。
	`EDRCloud`	Endpoint Detection and Response Expert (cloud) 该组件与 Endpoint Detection and Response Optimum (`EDR`) 和 Endpoint Detection and Response Expert (on-premises) (`AntiAPT`) 组件不兼容。
	`AntiAPT`	Endpoint Detection and Response Expert (on-premises) 该组件与 Endpoint Detection and Response Expert (cloud) (`EDRCloud`) 和 Endpoint Detection and Response Optimum (`EDR`) 组件不兼容。
	`SB`	Kaspersky Sandbox 或 KATA Sandbox。 *Kaspersky Sandbox* 是卡巴斯基的独立 Detection and Response 解决方案。*KATA Sandbox* 是 Kaspersky Anti Targeted Attack Platform 解决方案的一个组件。
	`MDR`	Managed Detection and Response
	`NDR`	Network Detection and Response (KATA) 该组件与 Endpoint Detection and Response Expert (cloud) (`EDRCloud`) 和 Endpoint Detection and Response Optimum (`EDR`) 组件不兼容。
	`AdminKitConnector`	使用管理系统管理应用程序。例如，管理系统包括 Kaspersky Security Center。除了 Kaspersky 管理系统，您还可以使用第三方解决方案。Kaspersky Endpoint Security 为此提供了一个 API。 可用值： • `1` - 允许在管理系统的帮助下管理应用程序（默认值）。 • `0` - 仅允许通过本地界面管理应用程序。
	`KUMAIntegration`	与 KUMA 的整合。
	`StandaloneKATA`	在 Endpoint Detection and Response Agent (EDR Agent) 模式下安装应用程序，用于与 Kaspersky Anti Targeted Attack Platform (EDR) 整合。
	`StandaloneMDR`	在 Endpoint Detection and Response Agent (EDR Agent) 模式下安装应用程序，用于与 Kaspersky Managed Detection and Response 整合。
	`StandaloneNDR`	在 Endpoint Detection and Response Agent (EDR Agent) 模式下安装应用程序，用于与 Kaspersky Anti Targeted Attack Platform (NDR) 整合。

区域	参数	描述
	`StandaloneSiemTelemetry`	在 Endpoint Detection and Response Agent (EDR Agent) 模式下安装应用程序，用于与 KUMA 整合。
`[Tasks]`	`ScanMyComputer`	全盘扫描任务。可用值： • `1` – 该任务将包含在 Kaspersky Endpoint Security 任务列表中。 • `0` – 该任务不会包含在 Kaspersky Endpoint Security 任务列表中。
	`ScanCritical`	关键区域扫描任务。可用值： • `1` – 该任务将包含在 Kaspersky Endpoint Security 任务列表中。 • `0` – 该任务不会包含在 Kaspersky Endpoint Security 任务列表中。
	`Updater`	更新任务。可用值： • `1` – 该任务将包含在 Kaspersky Endpoint Security 任务列表中。 • `0` – 该任务不会包含在 Kaspersky Endpoint Security 任务列表中。

更改应用程序组件

在安装应用程序期间，您可以选择将可用的组件。您可以通过以下方式更改可用的应用程序组件：

- 本地使用安装向导。

  使用 Windows 操作系统的常规方法（通过“控制面板”）更改应用程序组件。运行应用程序安装向导，然后选择用于更改可用应用程序组件的选项。按照屏幕上的说明进行操作。

  > 如果应用程序是通过 Kaspersky Security Center 安装的，则此方法不可用。只有在以下情况下，您才能在控制面板中更改应用程序组件的选择：本地安装应用程序。

- 使用 Kaspersky Security Center 远程。

  “*更改应用程序组件*”任务允许您在安装应用程序后更改 Kaspersky Endpoint Security 组件。

更改应用程序组件时，请考虑以下特殊注意事项：

- 在运行 Windows Server 的计算机上，无法安装 Kaspersky Endpoint Security 的所有组件（例如，“自适应异常控制”组件不可用）。
- 如果计算机上的硬盘驱动器受“完整磁盘加密 (FDE)”保护，则无法删除“完整磁盘加密”组件。要删除“完整磁盘加密”组件，请解密计算机的所有硬盘驱动器。
- 如果计算机具有加密的文件 (FLE) 或用户使用加密的可移动驱动器（FDE 或 FLE），则在删除数据加密组件之后将无法访问文件和可移动驱动器。您可以通过重新安装数据加密组件来访问这些文件和可移动驱动器。
- 如果应用程序在 VDI 基础架构中以 Light Agent 模式安装，不支持更改设置的组件。

如何在管理控制台 (MMC) 中添加或删除应用程序组件

1. 在 Kaspersky Security Center 管理控制台树中，选择“**任务**”。

   任务列表打开。

2. 单击“**新任务**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 选择任务类型

选择“**Kaspersky Endpoint Security for Windows (14.1)**”→ “**选择要安装的组件**”。

步骤 2. 更改应用程序组件的任务设置

检查应用程序的配置：

- “**保护主机的标准模式**”。默认配置。此配置允许您使用应用程序的所有组件，包括为 Detection and Response 解决方案提供支持的组件。此配置用于全面保护计算机免受各种威胁、网络攻击和欺诈。
- “**用于抵御高级威胁和目标攻击的 Endpoint Detection and Response Agent**”。在此配置下，您只能安装为 Detection and Response 解决方案提供支持的组件： MDR、EDR (KATA)、NDR (KATA)、EDR Expert (on-premises) 和 KUMA。如果您的组织中与 Kaspersky Detection and Response 解决方案一起部署了第三方 Endpoint Protection Platform (EPP)，则需要此配置。这使得在 Endpoint Detection and Response Agent 配置下的 Kaspersky Endpoint Security 与第三方 EPP 应用程序兼容。

  当更改 EDR Agent 的应用程序配置以使其与 MDR 协同工作时，请确保已启用负责接收遥测数据的组件。

- “**用于保护虚拟环境的 Light Agent**”。此配置适用于作为 Kaspersky Security for Virtualization Light Agent 解决方案的一部分使用的应用程序。Light Agent 必须安装在需要使用解决方案保护的每个虚拟机上。在此配置中，您不能使用数据加密组件或自适应异常控制。如果您正在虚拟机模板上安装 Light Agent，该模板将用于创建*非持久虚拟机*，选择“**保护 VDI 基础架构**”复选框（VDI 代表 Virtual Desktop Infrastructure）。VDI 保护模式能够在临时虚拟机上优化 Kaspersky Endpoint Security 的性能。在此模式下，Light Agent 会拒绝需要重新启动虚拟机的应用程序更新。当接收到需要重新启动的应用程序更新时，Light Agent 会生成需要更新受保护虚拟机模板的事件。

选择将在用户计算机上可用的应用程序组件。

步骤 3. 高级设置

为任务（参加下表）配置高级设置。

步骤 4. 选择任务将分配到的设备

选择将要执行任务的计算机。下列选项可用：

- 将任务分配给管理组。在这种情况下，任务分配给先前创建的管理组中包括的计算机。
- 选择管理服务器在网络中检测到的计算机：*未分配设备*。特定设备可包括管理组中的设备以及未分配设备。
- 手动指定设备地址或从列表中导入地址。您可以指定您要将任务分配给的设备的 NetBIOS 名称、IP 地址和 IP 子网。

步骤 5. 配置任务启动计划

配置启动任务的计划，例如，手动或在计算机空闲时。

步骤 6. 定义任务名称

输入任务的名称，例如“*添加应用程序控制组件*”。

步骤 7. 完成任务创建

退出向导。如有必要，选中“**向导完成时运行任务**”复选框。您可以在任务属性中监控任务进度。

如何在 Web Console 和云控制台中添加或删除应用程序组件

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
2. 单击“**添加**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 配置常规任务设置

配置常规任务设置：

1. 在“**应用程序**”下拉列表中，选择“**Kaspersky Endpoint Security for Windows 14.2.0**”。
2. 在“**任务类型**”下拉列表中，选择“**更改应用程序组件**”。
3. 在“**任务名称**”字段中，输入简要说明，例如，“*添加应用程序控制组件*”。
4. 在“**要对其分配任务的设备**”块，选择任务范围。

步骤 2. 选择任务将分配到的设备

选择将要执行任务的计算机。例如，选择单独的管理组或构建一个选项。

步骤 3. 完成任务创建

选择“**创建完成时打开任务详情**”复选框并完成向导。

在任务属性中，选择“**应用程序设置**”选项卡。接下来，选择应用程序的配置：

- “**保护工作站和服务器的标准模式**”。默认配置。此配置允许您使用应用程序的所有组件，包括为 Detection and Response 解决方案提供支持的组件。此配置用于全面保护计算机免受各种威胁、网络攻击和欺诈。

- “**用于抵御高级威胁和目标攻击的 Endpoint Detection and Response Agent**”。在此配置下，您只能安装为 Detection and Response 解决方案提供支持的组件：MDR、EDR (KATA)、NDR (KATA)、EDR Expert (on-premises) 和 KUMA。如果您的组织中与 Kaspersky Detection and Response 解决方案一起部署了第三方 Endpoint Protection Platform (EPP)，则需要此配置。这使得在 Endpoint Detection and Response Agent 配置下的 Kaspersky Endpoint Security 与第三方 EPP 应用程序兼容。

  当更改 EDR Agent 的应用程序配置以使其与 MDR 协同工作时，请确保已启用负责接收遥测数据的组件。

- “**用于保护虚拟环境的 Light Agent**”。此配置适用于作为 Kaspersky Security for Virtualization Light Agent 解决方案的一部分使用的应用程序。Light Agent 必须安装在需要使用解决方案保护的每个虚拟机上。在此配置中，您不能使用数据加密组件或自适应异常控制。如果您正在虚拟机模板上安装 Light Agent，该模板将用于创建*非持久虚拟机*，选择“**保护 VDI 基础架构**”复选框（VDI 代表 Virtual Desktop Infrastructure）。VDI 保护模式能够在临时虚拟机上优化 Kaspersky Endpoint Security 的性能。在此模式下，Light Agent 会拒绝需要重新启动虚拟机的应用程序更新。当接收到需要重新启动的应用程序更新时，Light Agent 会生成需要更新受保护虚拟机模板的事件。

选择将在用户计算机上可用的应用程序组件。为任务（参加下表）配置高级设置。

结果，用户计算机上的 Kaspersky Endpoint Security 组件集将在静默模式下更改。可用组件的设置将显示在应用程序的本地界面中。应用程序中未包括的组件将被禁用，并且这些组件的设置不可用。

安装、更新或卸载 Kaspersky Endpoint Security 时，可能会出现错误。有关解决这些错误的更多信息，请参阅技术支持知识库。

任务高级设置

参数	描述
任务设置	“**检查不兼容的第三方应用程序**”。默认情况下，Kaspersky Endpoint Security 检查已安装应用程序的兼容性。可能导致兼容性问题的软件列表位于 incompatible.txt 文件中。文件包含在分发工具中。如果启用了已安装软件的扫描功能，当检测到列表中的应用程序时，Kaspersky Endpoint Security 会停止该任务。如果第三方软件的供应商文档声称与 Endpoint Protection Platform (EPP) 兼容，您可以禁用已安装软件的扫描。 “**卸载不兼容的第三方应用程序**”。在更改组件集之前，自动删除 incompatible.txt 文件中列出的应用程序。如果启用此功能，Kaspersky Endpoint Security 会尝试删除可能导致兼容性问题的应用程序，以便继续执行任务。 “**使用 Azure WVD 兼容模式**”。此功能可确保在 Kaspersky Anti Targeted Attack Platform 控制台中正确显示 Azure 虚拟机状态。为了监控计算机的性能，Kaspersky Endpoint Security 将遥测数据发送到 KATA 服务器。遥测包括计算机的 ID（Sensor ID）。Azure WVD 兼容模式允许为这些虚拟机分配永久唯一的 Sensor ID。如果关闭兼容模式，由于 Azure 虚拟机的工作方式，Sensor ID 可能会在计算机重新启动后发生变化。这可能会导致控制台上出现重复的虚拟机。
排除项	从 Kaspersky Endpoint Security 12.6 for Windows 开始，扫描排除项和受信任的应用程序被添加到信任区域。预定义的扫描排除项和受信任的应用程序有助于在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上快速配置 Kaspersky Endpoint Security。这意味着您不需要在服务器上为应用程序手动设置信任区域。 从 Kaspersky Endpoint Security 12.8 for Windows 开始，您可以在 Light Agent 模式下安装该应用程序来保护虚拟环境。预定义的扫描排除项和受信任的应用程序可以帮助您在 Citrix 和 VMware 虚拟环境中快速配置 Kaspersky Endpoint Security。 您还可以稍后在策略属性中配置受信任区域：扫描排除项和受信任的应用程序。

参数	描述
单独模式 / 组合模式	您可以为工作站和服务器创建单独的组件集 – **单独模式**。在部署安装包之前，安装程序会检测操作系统的类型，并仅安装您为该操作系统类型选择的应用程序组件。这样，您就可以对工作站和服务器使用相同的安装包。 "**组合模式**"提供工作站和服务器的常用组件列表。各个组件的可用性取决于操作系统的类型。在这种模式下，我们建议为工作站创建单独的安装包，为服务器创建单独的安装包。仅在标准模式下才可以配置安装包中的常用组件列表。
使用密码修改应用程序组件集	管理员通常启用密码保护以限制对 Kaspersky Endpoint Security 的访问。也就是说，要修改应用程序组件的选择，您必须输入具有**卸载/修改/恢复应用程序**权限的用户的凭据。例如，您可以使用 KLAdmin 账户。
使用密码卸载 Kaspersky Endpoint Agent 和 Kaspersky Security for Windows Server	管理员通常在这些任务的设置中启用密码保护，以限制对 Kaspersky Endpoint Agent (KEA) 和 Kaspersky Security for Windows Server (KSWS) 的访问。也就是说，如果您从 [KES+KEA] 配置迁移到 [KES+内置代理]，或者如果您从 KSWS 迁移到 KES，则必须输入密码才能删除这些应用程序。

从以前版本的应用程序升级

将以前版本的应用程序更新为较新版本时，请考虑以下事项：

- Kaspersky Endpoint Security 新版本的本地化必须与应用程序安装版本的本地化相匹配。如果应用程序的本地化不匹配，应用程序升级将完成，但带有错误。
- 建议在开始更新之前退出所有活动的应用程序。
- 在更新之前，Kaspersky Endpoint Security 会阻止完整磁盘加密功能。如果无法锁定完整磁盘加密，升级安装将不会启动。更新应用程序后，将恢复完整磁盘加密功能。

Kaspersky Endpoint Security 支持以下应用程序版本的更新：

- Kaspersky Endpoint Security 12.1 for Windows（版本 12.1.0.506）
- Kaspersky Endpoint Security 12.2 for Windows（版本 12.2.0.462）
- Kaspersky Endpoint Security 12.3 for Windows（版本 12.3.0.493）
- Kaspersky Endpoint Security 12.4 for Windows（版本 12.4.0.467）
- Kaspersky Endpoint Security 12.5 for Windows（版本 12.5.0.539）
- Kaspersky Endpoint Security 12.6 for Windows（版本 12.6.0.438）
- Kaspersky Endpoint Security 12.7 for Windows（版本 12.7.0.533）
- Kaspersky Endpoint Security 12.8 for Windows（版本 12.8.0.505）
- Kaspersky Endpoint Security 12.9 for Windows（版本 12.9.0.384）
- Kaspersky Endpoint Security 12.10 for Windows（版本 12.10.0.466）
- Kaspersky Endpoint Security 12.11 for Windows（版本 12.11.0.637）

- Kaspersky Endpoint Security 12.12 for Windows（版本 12.12.0.522）
- Kaspersky Endpoint Security 14.0 for Windows（版本 14.0.0.504）

安装、更新或卸载 Kaspersky Endpoint Security 时，可能会出现错误。有关解决这些错误的更多信息，请参阅技术支持知识库。

应用程序升级方法

可以通过以下方式在计算机上更新 Kaspersky Endpoint Security：

- 使用卡巴斯基更新服务（Seamless Update – SMU）。
- 本地使用安装向导。
- 本地使用命令行。
- 使用 Kaspersky Security Center 远程。
- 远程通过 Microsoft Windows 组策略管理编辑器（有关详细信息，请参阅 Microsoft 技术支持网站）。
- 远程使用系统中心配置管理器。

如果公司网络中部署的应用程序所包含的组件集与默认组件集不同，则通过管理控制台 (MMC) 更新应用程序与通过 Web Console 和云控制台更新应用程序也有所差异。在更新 Kaspersky Endpoint Security 时，应考虑以下事项：

- Kaspersky Security Center Web Console 或 Kaspersky Security Center 云控制台。

  如果使用默认组件集为新版本的应用程序创建安装包，则将不会更改用户计算机上的组件集。要为 Kaspersky Endpoint Security 使用默认组件集，您需要打开安装包属性，更改组件集，然后恢复为原始组件集并保存更改。

- Kaspersky Security Center 管理控制台。

  更新后的应用程序组件集将与安装包中的组件集相匹配。也就是说，例如，如果新版本的应用程序采用默认组件集，则将从计算机中删除 BadUSB 攻击防护组件，因为此组件已从默认组件集中排除。要继续为应用程序使用与更新之前相同的组件集，请在安装包设置中选择所需的组件。

无需重新启动即可升级应用程序

在应用程序版本更新时，无需重新启动即可升级应用程序可提供不间断的服务器操作。

在不重新启动的情况下升级应用程序有以下限制：

- 从 11.10.0 版开始，无需重新启动即可升级应用程序。要升级应用程序的早期版本，必须重新启动计算机。
- 从 11.11.0 版开始，您可以无需重新启动即可安装补丁。要安装应用程序早期版本的补丁，可能需要重新启动计算机。

- 在启用了数据加密（卡巴斯基加密（FDE）、BitLocker、文件级加密（FLE））的计算机上，无法在不重新启动的情况下升级应用程序。要在启用了数据加密的计算机上升级应用程序，必须重新启动计算机。
- 如果不重新启动，则无法在虚拟机上升级该应用程序。要升级虚拟机上的应用程序，必须重新启动虚拟机。

升级应用程序、安装补丁、更改应用程序组件集或恢复后， Kaspersky Endpoint Security 将重新启动以开始使用新版本。重新启动 Kaspersky Endpoint Security 可能需要一分钟。在该期间计算机保护级别降低。重新启动应用程序后，计算机的保护级别将恢复。

如何在管理控制台 (MMC) 中选择应用程序升级模式

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **用户交互**。
5. 在“**应用程序更新设置**”块，选择或清空“**安装应用程序更新而不重启计算机**”复选框以配置应用程序升级模式。
6. 保存更改。

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **应用程序设置**。
4. 在“**高级设置**”块，选择或清空“**安装应用程序更新而不重启计算机**”复选框以配置应用程序升级模式。
5. 保存更改。

如何在应用程序界面中选择应用程序升级模式

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**常规设置**” → “**应用程序设置**”。

Kaspersky Endpoint Security for Windows 设置

3. 在“**常规**”块，选择或清空“**安装更新而不重启计算机**”复选框以配置应用程序升级模式。

4. 保存更改。

在不重启的情况下完成应用程序升级程序后，新版本的 Kaspersky Endpoint Security 将安装在计算机上。应用程序的旧版本将自动删除。

> 在前一次升级完全完成之前，您无法启动应用程序升级。

您可以使用 Kaspersky Security Center 控制台中的卡巴斯基应用程序版本报告来检查 Kaspersky Endpoint Security 升级状态。

应用程序的 SMU 更新

要使用卡巴斯基更新服务更新应用程序（Seamless Update；SMU），与其他更新方法不同，您无需运行安装程序。Kaspersky Endpoint Security 获得了新版本的应用程序以及来自同一源的反病毒数据库。

SMU 更新允许将您组织的所有计算机上的应用程序更新到最新版本。在应用 SMU 更新之前，我们建议在几台计算机上测试应用程序的新版本。为此，您必须手动更新这些计算机上的应用程序（例如，在本地使用安装向导）。执行 SMU 更新时，您无法选择单个计算机。

应用程序的更新计划由卡巴斯基工作人员决定。为了确保新版本的应用程序顺利运行，卡巴斯基会逐步提供更新。这意味着您可能会在新版本发布后最多两个月内获得 SMU 更新。

您可以使用"*数据库和应用程序模块更新*"任务管理应用程序的 SMU 更新。要将应用程序的新版本包含在与反病毒数据库相同的软件包中，您必须在"*数据库和应用程序模块更新*"任务设置中允许更新*应用程序模块*。此外，在"*数据库和应用程序模块更新*"任务设置中，您可以允许更新应用程序而无需重启。

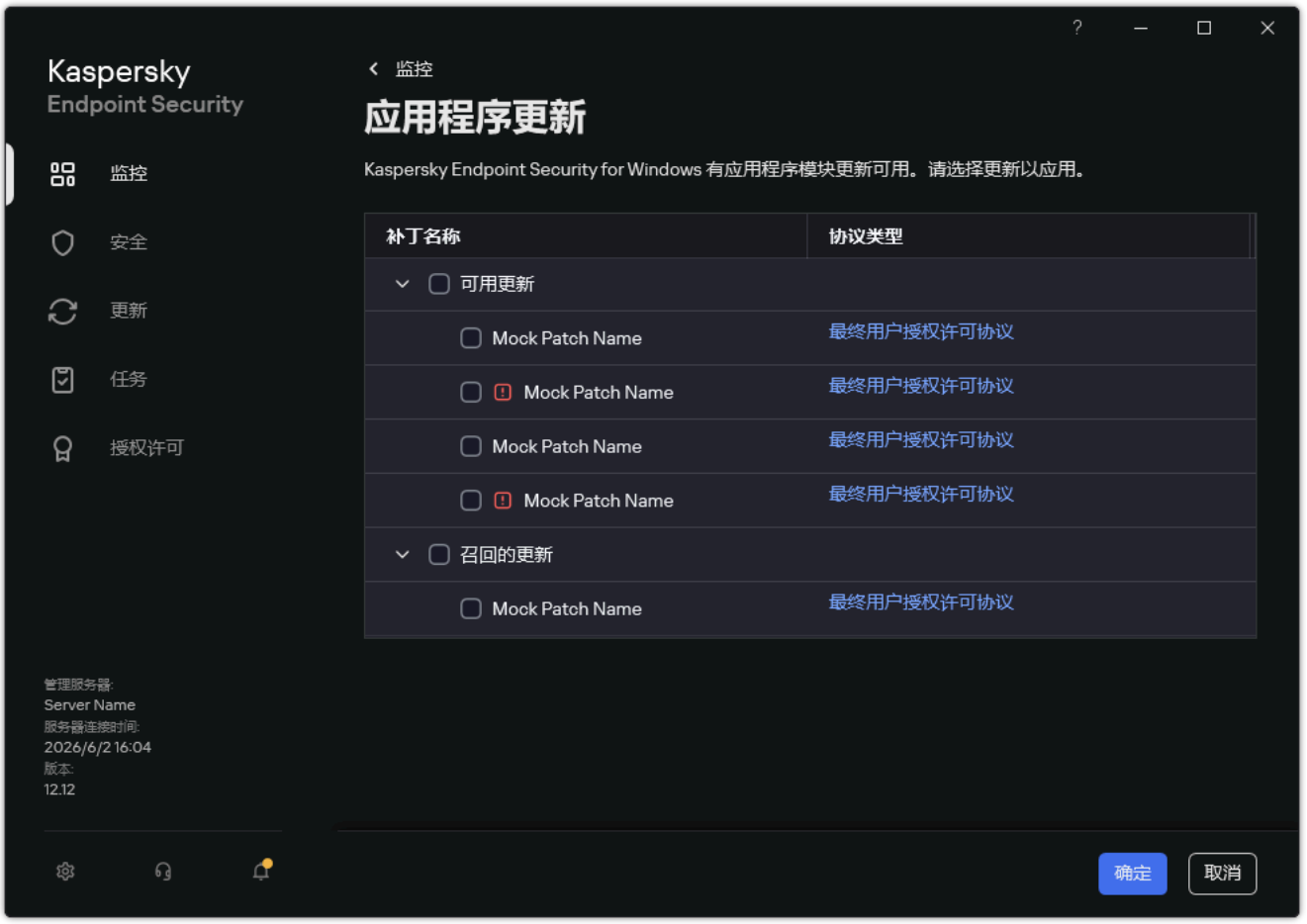
应用程序 SMU 更新的步骤

1. **在应用程序的新版本发布后，卡巴斯基会分发更新。**
2. **用户批准应用程序的更新。**

   如果计算机已连接到 Kaspersky Security Center，则可以在 Kaspersky Security Center 的"**卡巴斯基数据库和应用程序模块的更新**"部分获取更新。有关批准更新的详细信息，请参阅 Kaspersky Security Center 帮助。

   如果计算机未连接到 Kaspersky Security Center，则可以在应用程序界面的通知部分中获取更新：。要批准更新，请选择应用程序的版本并接受协议的条款和条件（见下图）。
3. **Kaspersky Endpoint Security 按照配置的计划运行"*数据库和应用程序模块更新*"任务。**

结果，Kaspersky Endpoint Security 将在“静默”模式下更新应用程序。



可用的应用程序更新

卸载应用程序

删除 Kaspersky Endpoint Security 将导致计算机和用户数据失去对威胁的防护。

安装、更新或卸载 Kaspersky Endpoint Security 时，可能会出现错误。有关解决这些错误的更多信息，请参阅技术支持知识库。

使用 Kaspersky Security Center 远程卸载应用程序

您可以使用“*远程卸载应用程序*”任务远程卸载应用程序。执行该任务时，Kaspersky Endpoint Security 会将应用程序卸载实用程序下载到用户的计算机。完成应用程序的卸载后，将自动删除该实用程序。

如何通过管理控制台 (MMC) 删除应用程序

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**任务**”。
   任务列表打开。
3. 单击“**新任务**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 选择任务类型

选择“**Kaspersky Security Center 管理服务器**” →“**高级**” →“**远程卸载应用程序**”。

步骤 2. 选择要删除的应用程序

选择“**卸载 Kaspersky Security Center 支持的应用程序**”。

步骤 3. 应用程序卸载的任务设置

选择“**Kaspersky Endpoint Security for Windows (14.1)**”。

步骤 4. 卸载实用程序设置

配置以下其他应用程序设置：

- “**强制下载卸载实用程序**”。选择实用程序传送方式：
  - “**使用网络代理**”。如果计算机上未安装网络代理，将首先使用操作系统的工具安装网络代理。然后通过网络代理的工具卸载 Kaspersky Endpoint Security。
  - “**通过管理服务器使用操作系统资源**”。实用程序将通过管理服务器使用操作系统资源传送到客户端计算机。如果客户端计算机上未安装网络代理，但客户端计算机与管理服务器在同一网络中，可以选择此选项。
  - “**通过分发点使用操作系统资源**”。通过分发点使用操作系统资源将实用程序传输到客户端计算机。如果网络中有至少一个分发点，则可以选择此选项。有关分发点的详细信息，请参阅 Kaspersky Security Center 帮助。
- “**下载之前验证操作系统类型**”。如有必要，清除此复选框。这样可避免在计算机的操作系统不符合软件要求时下载卸载实用程序。如果您确定计算机的操作系统符合软件要求，可以跳过此验证。

如果应用程序卸载操作受密码保护，请执行以下操作：

1. 选择**使用卸载密码**复选框。
2. 单击“**编辑**”按钮。
3. 输入 KLAdmin 账户密码。

步骤 5. 选择操作系统重启设置

卸载应用程序后，需要重新启动。选择将要执行的用于重新启动计算机的操作。

步骤 6. 选择任务将分配到的设备

选择将要执行任务的计算机。下列选项可用：

- 将任务分配给管理组。在这种情况下，任务分配给先前创建的管理组中包括的计算机。
- 选择管理服务器在网络中检测到的计算机：*未分配设备*。特定设备可包括管理组中的设备以及未分配设备。
- 手动指定设备地址或从列表中导入地址。您可以指定您要将任务分配给的设备的 NetBIOS 名称、IP 地址和 IP 子网。

步骤 7. 选择要运行任务的账户

选择用于使用操作系统工具安装网络代理的账户。在这种情况下，访问计算机需要管理员权限。您可以添加多个账户。如果某个账户没有足够权限，安装向导将使用下一个账户。如果使用网络代理工具卸载 Kaspersky Endpoint Security，则无需选择账户。

步骤 8. 配置任务启动计划

配置启动任务的计划，例如，手动或在计算机空闲时。

步骤 9. 定义任务名称

输入任务的名称，例如“*卸载 Kaspersky Endpoint Security 14.1*”。

步骤 10.完成任务创建

退出向导。如有必要，选中“**向导完成时运行任务**”复选框。您可以在任务属性中监控任务进度。

应用程序将以静默模式卸载。

如何通过 Web Console 和云控制台删除应用程序

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
2. 单击“**添加**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 配置常规任务设置

配置常规任务设置：

1. 在“**应用程序**”下拉列表中，选择“**Kaspersky Security Center**”。
2. 在“**任务类型**”下拉列表中，选择“**远程卸载应用程序**”。
3. 在“**任务名称**”字段中，输入简要说明，例如，“*卸载技术支持计算机中的 Kaspersky Endpoint Security*”。
4. 在“**要对其分配任务的设备**”块，选择任务范围。

步骤 2. 选择任务将分配到的设备

选择将要执行任务的计算机。例如，选择单独的管理组或构建一个选项。

步骤 3. 配置应用程序卸载设置

在此步骤中，配置应用程序卸载设置：

1. 选择“**卸载受管理应用程序**”类型。
2. 选择“**Kaspersky Endpoint Security for Windows**”。

3. “**强制下载卸载实用程序**”。选择实用程序传送方式：

   - “**使用网络代理**”。如果计算机上未安装网络代理，将首先使用操作系统的工具安装网络代理。然后通过网络代理的工具卸载 Kaspersky Endpoint Security。

   - “**通过管理服务器使用操作系统资源**”。实用程序将通过管理服务器使用操作系统资源传送到客户端计算机。如果客户端计算机上未安装网络代理，但客户端计算机与管理服务器在同一网络中，可以选择此选项。

   - “**通过分发点使用操作系统资源**”。通过分发点使用操作系统资源将实用程序传输到客户端计算机。如果网络中有至少一个分发点，则可以选择此选项。有关分发点的详细信息，请参阅 Kaspersky Security Center 帮助。

4. 在“**同时下载的最大数量**”字段中，设置发送到管理服务器的下载应用程序卸载实用程序请求数量限制。限制请求数有助于防止网络过载。

5. 在“**尝试卸载的最大次数**”字段中，设置应用程序卸载尝试次数限制。如果卸载 Kaspersky Endpoint Security 以出错结束，任务将自动再次启动卸载。

6. 如有必要，清空“**下载之前验证操作系统类型**”复选框。这样可避免在计算机的操作系统不符合软件要求时下载卸载实用程序。如果您确定计算机的操作系统符合软件要求，可以跳过此验证。

步骤 4. 选择要运行任务的账户

选择用于使用操作系统工具安装网络代理的账户。在这种情况下，访问计算机需要管理员权限。您可以添加多个账户。如果某个账户没有足够权限，安装向导将使用下一个账户。如果使用网络代理工具卸载 Kaspersky Endpoint Security，则无需选择账户。

步骤 5. 完成任务创建

单击“**完成**”按钮完成向导。在任务列表中将显示一个新任务。

要运行任务，请选中与任务对应的复选框，然后单击“**开始**”按钮。应用程序将以静默模式卸载。卸载完成后，Kaspersky Endpoint Security 会显示重新启动计算机的提示。

> 如果应用程序卸载操作受密码保护，请在“*远程卸载应用程序*”任务的属性中输入 KLAdmin 账户密码。如果没有密码，任务不会执行。

要在“远程卸载应用程序”任务中使用 KLAdmin 账户密码：

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

   任务列表打开。

2. 单击 Kaspersky Security Center 的“**远程卸载应用程序**”任务。

   任务属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择**使用卸载密码**复选框。

5. 输入 KLAdmin 账户密码。

6. 保存更改。

重新启动计算机以完成卸载。为此，网络代理将显示一个弹出窗口。

使用活动目录远程卸载应用程序

您可以使用 Microsoft Windows 组策略远程卸载应用程序。要卸载应用程序，您需要打开组策略管理控制台（gpmc.msc），并使用组策略编辑器创建应用程序卸载任务（有关详细信息，请访问 Microsoft 技术支持网站）。

如果应用程序卸载操作受密码保护，您需要执行以下操作：

1. 创建包含以下内容的 BAT 文件：

   ```
   msiexec.exe /x<GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
   ```

   `<GUID>` 是应用程序的唯一 ID。您可以在技术支持知识库或使用以下命令找到应用程序的 GUID：

   ```
   wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
   ```

   示例

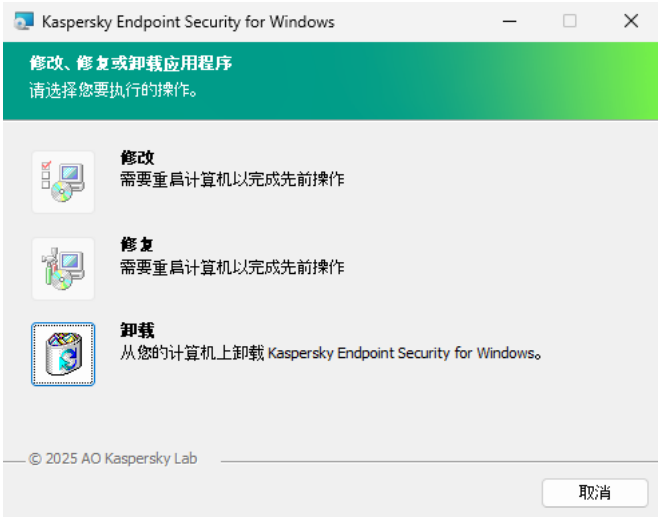
   ```
   msiexec.exe /x{6BB76C8F-365E-4345-83ED-6D7AD612AF76} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
   ```

2. 在组策略管理控制台（gpmc.msc）中为计算机创建新的 Microsoft Windows 策略。

3. 使用新策略在计算机上运行创建的 BAT 文件。

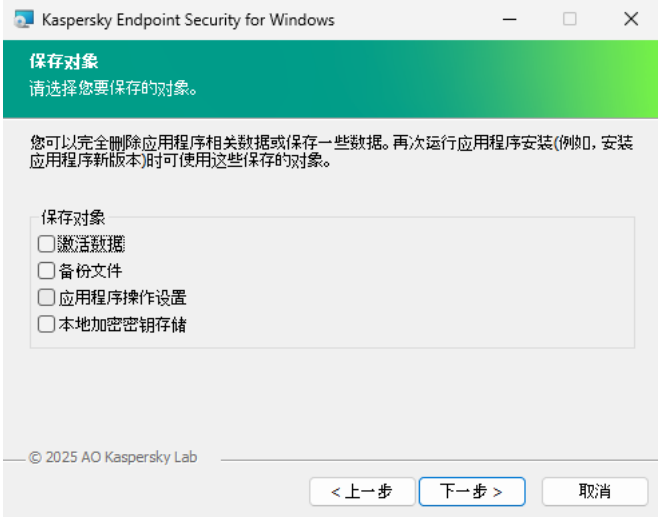
本地卸载应用程序

您也可以使用安装向导在本地卸载应用程序。使用 Windows 操作系统的常规方法（通过“控制面板”）卸载 Kaspersky Endpoint Security。“安装向导”将启动。按照屏幕上的说明进行操作。



选择应用程序卸载操作

您可以指定要保存应用程序使用的哪些数据，以供在下次安装应用程序（例如升级到较新版本的应用程序）时使用。如果不指定任何数据，应用程序将被完全卸载（参见下图）。



卸载后保存数据

您可以保存以下数据：

- **激活数据**，让您避免再次激活应用程序。如果授权许可期限在安装之前未到期，Kaspersky Endpoint Security 会自动添加授权许可密钥。
- **备份文件** – 程序要扫描的置于“备份区”中的对象。

> 在删除应用程序之后保存的备份文件只能在用于保存这些文件的同一版本应用程序中访问。

> 如果您计划在删除应用程序之后使用备份对象，必须在删除应用程序之前还原这些对象。但是，Kaspersky 专家不推荐从备份区中还原对象，因为这可能会损坏计算机。

- **应用程序操作设置** – 应用程序配置过程中选择的应用程序设置值。
- **本地加密密钥存储** – 该数据提供对在卸载程序之前加密的文件和驱动器的访问权限。为保证对加密文件和驱动器的访问权限，请确保在重新安装 Kaspersky Endpoint Security 时选择了数据加密功能。访问以前加密的文件和驱动器不需要进一步操作。

Kaspersky Endpoint Security 保存数据到 `C:\ProgramData\Kaspersky Lab\KES.14.1\QB` 文件夹。

您还可以使用命令行在本地卸载应用程序。

应用程序授权许可

本部分提供了 Kaspersky Endpoint Security 授权许可相关常规概念的信息。

关于最终用户授权许可协议

*最终用户授权许可协议*是您和 AO Kaspersky Lab 之间的绑定协议，其中规定了您使用该应用程序应遵守的条款。

建议您在使用应用程序前认真阅读《授权许可协议》条款。

您可通过下列方式查看该许可协议的条款：

- 以互动模式安装 Kaspersky Endpoint Security 时。
- 通过阅读 license.txt 文件。该文档包括在应用程序分发包中，还位于应用程序安装文件夹 `%ProgramFiles(x86)%\Kaspersky Lab\KES\Doc\<locale>\KES` 中。

安装程序时确认您同意最终用户授权许可协议即表示您同意最终用户授权许可协议中的条款。如果您不接受最终用户授权许可协议的条款，您必须终止安装。

关于授权许可

*授权许可*是根据最终用户授权许可协议授予的在有限时间内使用本应用程序的权限。

该授权许可授权您根据最终用户授权许可协议的条款使用该应用程序，并获得技术支持。可用功能列表和应用程序使用期限取决于用于激活该应用程序的授权许可的类型。

提供以下授权许可类型：

- *试用版* – 用于试用该应用程序的免费授权许可。

  试用版授权许可通常拥有较短的有效期。当试用版授权许可过期时，所有 Kaspersky Endpoint Security 功能都将被禁用。要继续使用程序，您必须购买商业版授权许可。

  您只能使用试用授权许可激活应用程序一次。应用程序通过商业授权许可激活后，无法在试用授权许可下激活。

- *商业版* – 当您购买 Kaspersky Endpoint Security 时获得的付费授权许可。

  商业授权许可中所能使用的应用程序功能取决于所选产品。所选的产品指定在 授权许可证书 中。可用产品的信息可以在Kaspersky 网站找到。

  当商业版授权许可到期时，应用程序的关键功能将不可用。要继续使用应用程序，您必须续费您的商业版授权许可。如果您不打算续费授权许可，则必须从计算机中卸载应用程序。

关于授权许可证书

*授权许可证书*是发送给用户的一个带有密钥文件或激活码的文档。

授权许可证书包含以下授权许可信息：

- 授权许可 ID 或订单号。
- 被授予授权许可的用户详情。
- 可以使用授权许可激活的应用程序详情。
- 授权单元的数量限制（例如，可以在该授权许可下使用应用程序的设备数量）。
- 授权许可期限开始日期。
- 授权许可到期日期或授权许可期限。
- 授权许可类型。

关于订阅

*Kaspersky Endpoint Security 订阅*是一项带有特定参数（如订阅过期日期和受保护设备数量）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。您可以手动或自动对订阅进行续费，也可以取消订阅。您可以在服务提供商的网站上管理您的订阅。

订阅可以是有限订阅（例如一年时间）或无限订阅（无过期时间）。有限订阅期到期后，要使 Kaspersky Endpoint Security 继续工作，您需要续费订阅。如果按时预支付供应商服务，则可以自动续费无限订阅。

有限订阅过期时，您可能得到订阅续费宽限期，在此期间应用程序继续运行。宽限期的可用性和期限由服务提供商决定。

要在订阅下使用 Kaspersky Endpoint Security，您需要应用从服务提供商处接收到的激活码。应用激活码之后，将添加活动密钥。活动密钥确定了在订阅下使用应用程序的授权许可。您无法使用密钥文件激活订阅下的应用程序。服务提供商只能提供激活码。无法在订阅下添加备用密钥。

> 在订阅下购买的激活码可能无法用于激活先前版本的 Kaspersky Endpoint Security。

关于授权许可密钥

*授权许可密钥*是一个位序列，可用于按照最终用户授权许可协议条款激活和使用应用程序。

> 对于订阅下添加的密钥，不提供授权许可证书。

您可以通过应用密钥文件或输入激活码来向应用程序添加授权许可密钥。

如果违反了最终用户授权许可协议的条款，则 Kaspersky 可以阻止该密钥。如果密钥被阻止，您需要添加其他密钥才能继续使用应用程序。

有两种类型的密钥：活动密钥和备用密钥。

*活动密钥*是程序当前正在使用的密钥。试用版授权许可或商业版授权许可密钥可以被添加为活动密钥。本应用程序不能拥有两个及以上活动密钥。

*备用密钥*是允许用户使用程序但是当前未使用的密钥。活动密钥过期后，备用密钥将自动生效。仅当活动密钥可用时才能添加备用密钥。

> 只能将试用版授权许可的密钥以活动密钥的形式进行添加。无法将其添加为备用密钥。试用版授权许可密钥无法替换商业版授权许可的活动密钥。

如果有密钥被添加到禁止的密钥列表，由激活应用程序的授权许可定义的应用程序功能维持八天可用。应用程序通知用户密钥已被添加到禁止的密钥列表。八天后，应用程序功能将限制为授权许可到期后可用的功能级别。您可以使用保护和控制组件并使用授权许可过期之前安装的应用程序数据库运行扫描。该应用程序也会继续加密在授权许可过期前经过修改或加密过的文件，但是不会加密新文件。卡巴斯基安全网络不可用。

关于激活码

*激活码*是由 20 个字母数字字符组成的唯一序列。输入激活码以添加用于激活 Kaspersky Endpoint Security 的授权许可密钥。在您购买 Kaspersky Endpoint Security 之后，您指定的电子邮件地址会收到激活码。

要用激活码激活应用程序，需要互联网接入连接到 Kaspersky 的激活服务器。

当应用程序使用激活码激活时，将添加活动密钥。备用密钥只能使用激活码添加，而不能使用密钥文件添加。

如果激活应用程序后丢失了激活码，则您可以恢复激活码。您可能会需要激活码，例如用于注册 Kaspersky CompanyAccount。如果激活码在应用程序激活后丢失，请联系您购买授权许可的 Kaspersky 合作伙伴。

关于密钥文件

*密钥文件*是您从 Kaspersky 接收到的 .key 扩展名的文件。密钥文件的目的是添加能够激活应用程序的授权许可密钥。

在购买 Kaspersky Endpoint Security 或订购 Kaspersky Endpoint Security 试用版后，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。您可能需要密钥文件注册诸如 Kaspersky CompanyAccount 之类的服务。

若要恢复密钥文件，请执行以下操作：

- 联系授权许可销售商。
- 基于您现有的激活码在Kaspersky 网站上获得密钥文件。
- 从另一个管理服务器获取密钥文件。

当使用密钥文件激活应用程序时，将添加活动密钥。备用密钥只能使用密钥文件添加，而不能使用激活码添加。

根据工作站的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）。

另请参见服务器应用程序功能的比较

根据“卡巴斯基新一代安全”授权许可类型比较应用程序功能，请参阅““卡巴斯基新一代安全”帮助”。

Kaspersky Endpoint Security 功能比较

功能	卡巴斯基网络安全解决方案标准版支持	卡巴斯基网络安全解决方案高级版	卡巴斯基全方位安全软件	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
高级威胁防护								
卡巴斯基安全网络	✓	✓	✓	✓	✓	✓	✓	✓
行为检测	✓	✓	✓	✓	✓	✓	✓	✓
反加密程序	✓	✓	✓	✓	✓	✓	✓	✓
漏洞利用防御	✓	✓	✓	✓	✓	✓	✓	✓
主机入侵防御	✓	✓	✓	✓	✓	✓	✓	✓
修复引擎	✓	✓	✓	✓	✓	✓	✓	✓
关键威胁防护								
文件威胁防护	✓	✓	✓	✓	✓	✓	✓	✓
Web 威胁防护	✓	✓	✓	✓	✓	✓	✓	✓
邮件威胁防护	✓	✓	✓	✓	✓	✓	✓	✓
防火墙	✓	✓	✓	✓	✓	✓	✓	✓
网络威胁防护	✓	✓	✓	✓	✓	✓	✓	✓
BadUSB 攻击防护	✓	✓	✓	✓	✓	✓	✓	✓
AMSI 保护	✓	✓	✓	✓	✓	✓	✓	✓
安全控制								
日志审查	–	–	–	–	–	–	–	–
应用程序控制	✓	✓	✓	✓	✓	✓	✓	✓
设备控制	✓	✓	✓	✓	✓	✓	✓	✓
Web 控制	✓	✓	✓	✓	✓	✓	✓	✓
自适应异常控制	–	✓	✓	✓	✓	✓	–	✓

功能	卡巴斯基网络安全解决方案标准版支持	卡巴斯基网络安全解决方案高级版	卡巴斯基全方位安全软件	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
系统完整性监控	–	–	–	–	–	–	–	–
数据加密								
卡巴斯基磁盘加密	–	✓	✓	✓	✓	✓	–	✓
BitLocker 驱动器加密	–	✓	✓	✓	✓	✓	–	✓
文件级加密	–	✓	✓	✓	✓	✓	–	✓
可移动驱动器加密	–	✓	✓	✓	✓	✓	–	✓
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)*	✓	✓	✓	✓	✓	✓	✓	✓
与 KUMA 的整合 *（KUMA 集成授权许可必须单独购买）*	✓	✓	✓	✓	✓	✓	✓	✓
Light Agent 模式 *（要激活应用程序，您必须将授权许可密钥添加到 Light Agent 所连接的 SVM）*	–	–	–	–	–	–	✓	✓

根据服务器的授权许可类型比较应用程序功能

服务器上可用的 Kaspersky Endpoint Security 功能集取决于授权许可类型（见下表）。

另请参见工作站应用程序功能的比较

根据“卡巴斯基新一代安全”授权许可类型比较应用程序功能，请参阅““卡巴斯基新一代安全”帮助”。

Kaspersky Endpoint Security 功能比较

功能	卡巴斯基网络安全解决方案标准版支持	卡巴斯基网络安全解决方案高级版	卡巴斯基全方位安全软件	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
高级威胁防护								
卡巴斯基安全网络	✓	✓	✓	✓	✓	✓	✓	✓

功能	卡巴斯基网络安全解决方案标准版支持	卡巴斯基网络安全解决方案高级版	卡巴斯基全方位安全软件	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
行为检测	✓	✓	✓	✓	✓	✓	✓	✓
反加密程序	✓	✓	✓	✓	✓	✓	✓	✓
漏洞利用防御	✓	✓	✓	✓	✓	✓	✓	✓
主机入侵防御	–	–	–	–	–	–	–	–
修复引擎	✓	✓	✓	✓	✓	✓	✓	✓
关键威胁防护								
文件威胁防护	✓	✓	✓	✓	✓	✓	✓	✓
Web 威胁防护	–	✓	✓	✓	✓	✓	✓	✓
邮件威胁防护	–	✓	✓	✓	✓	✓	✓	✓
防火墙	✓	✓	✓	✓	✓	✓	✓	✓
网络威胁防护	✓	✓	✓	✓	✓	✓	✓	✓
BadUSB 攻击防护	✓	✓	✓	✓	✓	✓	✓	✓
AMSI 保护	✓	✓	✓	✓	✓	✓	✓	✓
安全控制								
日志审查	–	–	–	–	–	–	–	✓
应用程序控制	–	✓	✓	✓	✓	✓	–	✓
设备控制	–	✓	✓	✓	✓	✓	✓	✓
Web 控制	–	✓	✓	✓	✓	✓	✓	✓
自适应异常控制	–	–	–	–	–	–	–	–
系统完整性监控	–	–	–	–	–	–	–	✓
数据加密								
卡巴斯基磁盘加密	–	–	–	–	–	–	–	–
BitLocker 驱动器加密	–	✓	✓	✓	✓	✓	–	✓
文件级加密	–	–	–	–	–	–	–	–
可移动驱动器加密	–	–	–	–	–	–	–	–
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)*	✓	✓	✓	✓	✓	✓	✓	✓

功能	卡巴斯基网络安全解决方案标准版支持	卡巴斯基网络安全解决方案高级版	卡巴斯基全方位安全软件	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Optimum Security	Kaspersky Endpoint Detection and Response Expert	Kaspersky Hybrid Cloud Security Standard	Kaspersky Hybrid Cloud Security Enterprise
与 KUMA 的整合 *（KUMA 集成授权许可必须单独购买）*	✓	✓	✓	✓	✓	✓	✓	✓
Light Agent 模式 *（要激活应用程序，您必须将授权许可密钥添加到 Light Agent 所连接的 SVM）*	–	–	–	–	–	–	✓	✓

激活应用程序

*激活*是一种激活授权许可的过程，允许您在授权许可过期之前使用该应用程序全部的功能。应用程序激活涉及添加授权许可密钥。

您可以采用以下方式之一激活应用程序：

- 使用激活向导从应用程序界面本地进行。您可以使用这种方式添加活动密钥和备用密钥。
- 远程使用 Kaspersky Security Center 软件套装。
  - 使用“*添加密钥*”任务。

    此方法允许您向特定计算机或属于管理组的计算机添加密钥。您可以使用这种方式添加活动密钥和备用密钥。
  - 通过将存储在 Kaspersky Security Center 管理服务器中的密钥分发到计算机。

    使用此方法可以自动将密钥添加到已连接到 Kaspersky Security Center 的计算机和新计算机。要使用此方法，需要先将密钥添加到 Kaspersky Security Center 管理服务器。有关将密钥添加到 Kaspersky Security Center 管理服务器的详细信息，请参阅 Kaspersky Security Center 帮助。

    在订阅下购买的激活码位于第一位。
  - 通过向 Kaspersky Endpoint Security 安装包添加密钥。

    此方法允许您在 Kaspersky Endpoint Security 部署期间添加安装包属性中的密钥。安装后，应用程序将自动激活。
- 使用命令行。

根据 Kaspersky 的激活服务器的负载分布情况，（在远程安装或非交互安装时）程序用激活码激活可能会花一定时间。如果您需要立即激活应用程序，您可以中断正在进行的激活过程，然后使用激活向导进行激活。

如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 来保护虚拟环境，则无需单独激活应用程序。

激活应用程序

如何在管理控制台 (MMC) 中激活应用程序

1. 在 Kaspersky Security Center 管理控制台树中，选择“**任务**”。
   任务列表打开。
2. 单击“**新任务**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 选择任务类型

选择“**Kaspersky Endpoint Security for Windows (14.1)**”→ “**添加密钥**”。

步骤 2. 添加密钥

输入激活码或选择密钥文件。

有关将密钥添加到 Kaspersky Security Center 存储库的详细信息，请参阅 Kaspersky Security Center 帮助。

步骤 3. 选择任务将分配到的设备

选择将要执行任务的计算机。下列选项可用：

- 将任务分配给管理组。在这种情况下，任务分配给先前创建的管理组中包括的计算机。
- 选择管理服务器在网络中检测到的计算机：*未分配设备*。特定设备可包括管理组中的设备以及未分配设备。
- 手动指定设备地址或从列表中导入地址。您可以指定您要将任务分配给的设备的 NetBIOS 名称、IP 地址和 IP 子网。

步骤 4. 配置任务启动计划

配置启动任务的计划，例如，手动或在计算机空闲时。

步骤 5. 定义任务名称

输入任务的名称，例如“*激活 Kaspersky Endpoint Security for Windows*”。

步骤 6. 完成任务创建

退出向导。如有必要，选中“**向导完成时运行任务**”复选框。您可以在任务属性中监控任务进度。结果，Kaspersky Endpoint Security 将以静默模式在用户计算机上激活。

如何在 Web Console 和云控制台中激活应用程序

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
2. 单击“**添加**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 配置常规任务设置

配置常规任务设置：

1. 在“**应用程序**”下拉列表中，选择“**Kaspersky Endpoint Security for Windows 14.2.0**”。
2. 在“**任务类型**”下拉列表中，选择“**添加密钥**”。
3. 在“**任务名称**”字段中，输入简要说明，例如，“*激活 Kaspersky Endpoint Security for Windows*”。
4. 在“**要对其分配任务的设备**”块，选择任务范围。转到下一步。

步骤 2. 选择任务将分配到的设备

选择将要执行任务的计算机。下列选项可用：

- 将任务分配给管理组。在这种情况下，任务分配给先前创建的管理组中包括的计算机。
- 选择管理服务器在网络中检测到的计算机：*未分配设备*。特定设备可包括管理组中的设备以及未分配设备。
- 手动指定设备地址或从列表中导入地址。您可以指定您要将任务分配给的设备的 NetBIOS 名称、IP 地址和 IP 子网。

步骤 3. 选择授权许可

选择要用于激活应用程序的授权许可。转到下一步。

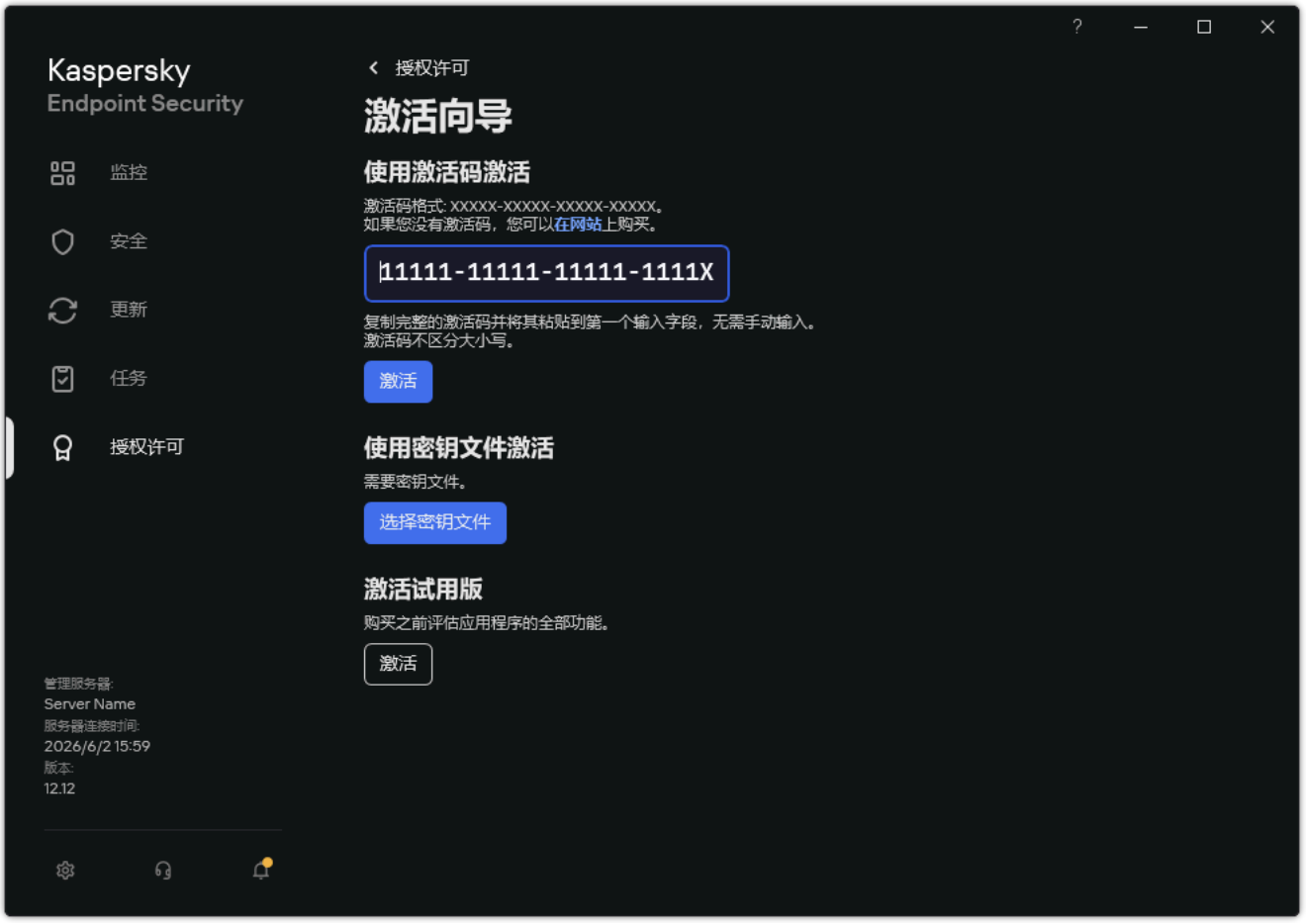
您可以向 Web Console 添加密钥（“**操作**”→“**授权许可**”）。

步骤 4. 完成任务创建

单击“**完成**”按钮完成向导。在任务列表中将显示一个新任务。要运行任务，请选中与任务对应的复选框，然后单击“**开始**”按钮。结果，Kaspersky Endpoint Security 将以静默模式在用户计算机上激活。

如何在应用程序界面中激活应用程序

1. 在应用程序主窗口中，转到“**授权许可**”区域。
2. 单击“**使用新授权许可激活应用程序**”。
   应用程序激活向导将启动。按照“激活向导”的说明进行操作。



激活应用程序

在“*添加密钥*”任务的属性中，可以将备用密钥添加到计算机。当活动密钥到期时，*备用密钥*将成为活动密钥。使用备用密钥可避免当授权许可到期时应用程序功能受限。

如何通过管理控制台 (MMC) 自动向计算机添加授权许可密钥

1. 在管理控制台中，转到文件夹“**卡巴斯基授权许可**”。
   将打开授权许可密钥列表。
2. 打开授权许可密钥属性。
3. 在“**常规**”区域中，选择“**自动分发授权许可密钥到受管理设备**”复选框。
4. 保存更改。

结果是密钥将自动分发到相应计算机。在将密钥作为活动密钥或备用密钥进行自动分发的过程中，会考虑授权许可对计算机数量的限制（在密钥属性中设置）。如果达到授权许可限制，会自动停止将该密钥分发到计算机。您可以在“**设备**”区域的密钥属性中查看已添加密钥的计算机数量以及其他数据。

如何通过 Web Console 和云控制台自动向计算机添加授权许可密钥

1. 在 Web Console 的主窗口中，选择“**操作**” → “**授权许可**” → “**授权许可**”。
   将打开授权许可密钥列表。
2. 打开授权许可密钥属性。
3. 在“**常规**”选项卡，启用“**自动分发授权许可密钥到受管理设备**”拨动开关。
4. 保存更改。

结果是密钥将自动分发到相应计算机。在将密钥作为活动密钥或备用密钥进行自动分发的过程中，会考虑授权许可对计算机数量的限制（在密钥属性中设置）。如果达到授权许可限制，会自动停止将该密钥分发到计算机。您可以在“**设备**”选项卡上的密钥属性中查看已添加密钥的计算机数量以及其他数据。

如果您正使用*激活码*激活应用程序，您需要互联网访问以连接到卡巴斯基激活服务器。如果您正使用*密钥文件*激活应用程序，不需要互联网访问。如果计算机位于无法访问互联网的隔离网段中，要使用激活码激活应用程序，您必须允许使用 Kaspersky Security Center 管理服务器作为代理服务器。也就是说，应用程序可以通过具有互联网访问权限的管理服务器来访问激活服务器。

如何在管理控制台 (MMC) 中允许使用管理服务器作为代理服务器来激活应用程序

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **应用程序设置**。
4. 选择**将 Kaspersky Security Center 用作代理服务器以进行激活**复选框。
5. 保存更改。

如何在 Web 控制台和云控制台中允许使用管理服务器作为代理服务器来激活应用程序

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。

4. 选择 **常规设置** → **KSC 整合**。

5. 选择**将 Kaspersky Security Center 用作代理服务器以进行激活**复选框。

6. 保存更改。

如果您无法使用*激活码*激活应用程序，您可以尝试使用卡巴斯基解决方案获得一个*密钥文件*并尝试使用不同的方法再次激活应用程序。

授权许可使用监控

您可以通过以下方式监控授权许可的使用：

- 查看组织的基础设施的"*授权许可密钥使用报告*"（**监控** → **报告**）。
- 在"**受管理设备**"→"**设备**"选项卡上查看计算机的状态。如果应用程序未激活，计算机将具有 ⚠ "*应用程序未激活*"状态。
- 查看计算机属性中的授权许可信息。
- 查看密钥属性（"**操作**" → "**授权许可**"）。

作为 Kaspersky Security Center 云控制台的一部分激活应用程序的细节

Kaspersky Security Center 云控制台提供了试用版。*试用版*是 Kaspersky Security Center 云控制台的特殊版本，旨在使用户熟悉该应用程序的功能。在此版本中，您可以在 30 天内在工作区中执行操作。所有托管的应用程序都自动在 Kaspersky Security Center 云控制台的试用授权许可下运行，包括 Kaspersky Endpoint Security。但是，当 Kaspersky Security Center 云控制台的试用授权许可到期时，您无法使用 Kaspersky Endpoint Security 自身的试用授权许可激活该应用程序。有关 Kaspersky Security Center 授权许可的详细信息，请参阅 Kaspersky Security Center 云控制台帮助。

> Kaspersky Security Center 云控制台试用版不允许以后切换到商业版本。30 天期限到期后，所有试用工作区及其所有内容都将被自动删除。

移除授权许可密钥

要删除授权许可密钥，您需要在计算机上运行一项特殊任务。您可以删除授权许可密钥，例如，重新排列授权许可单元。此外，当授权许可到期时，Kaspersky Endpoint Security 会通知您。如果您添加了短期授权许可密钥来试用该应用程序（例如，EDR Optimum 插件），则可以删除此授权许可密钥以摆脱通知并修复计算机的状态。

"*删除密钥*"任务允许从计算机中删除任何授权许可密钥。您可以删除活动授权许可密钥以及备用授权许可密钥。除了 Kaspersky Endpoint Security 激活授权许可密钥外，您还可以删除 Kaspersky Detection and Response 解决方案的授权许可密钥（例如，EDR Optimum 插件）。

如何在管理控制台 (MMC) 中删除授权许可密钥

1. 在 Kaspersky Security Center 管理控制台树中，选择“**任务**”。
   任务列表打开。
2. 单击“**新任务**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 选择任务类型

选择“**Kaspersky Endpoint Security for Windows (14.1)**”→ “**删除密钥**”。

步骤 2. 选择授权许可

选择您要删除的授权许可密钥。您可以从 Kaspersky Security Center 密钥存储中选择一个授权许可密钥，或者选择一个密钥文件。

步骤 3. 选择任务将分配到的设备

选择将要执行任务的计算机。下列选项可用：

- 将任务分配给管理组。在这种情况下，任务分配给先前创建的管理组中包括的计算机。
- 选择管理服务器在网络中检测到的计算机：*未分配设备*。特定设备可包括管理组中的设备以及未分配设备。
- 手动指定设备地址或从列表中导入地址。您可以指定您要将任务分配给的设备的 NetBIOS 名称、IP 地址和 IP 子网。

步骤 4. 配置任务启动计划

配置启动任务的计划，例如，手动或在计算机空闲时。

步骤 5. 定义任务名称

输入任务的名称，例如“*删除 Beta 密钥*”。

步骤 6. 完成任务创建

退出向导。如有必要，选中“**向导完成时运行任务**”复选框。您可以在任务属性中监控任务进度。

如何在 Web Console 中删除授权许可密钥

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
2. 单击“**添加**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 配置常规任务设置

配置常规任务设置：

1. 在“**应用程序**”下拉列表中，选择“**Kaspersky Endpoint Security for Windows 14.2.0**”。
2. 在“**任务类型**”下拉列表中，选择“**删除密钥**”。
3. 在“**任务名称**”字段中，输入简要说明，例如“*删除 Beta 密钥*”。
4. 在“**要对其分配任务的设备**”块，选择任务范围。转到下一步。

步骤 2. 选择任务将分配到的设备

选择将要执行任务的计算机。下列选项可用：

- 将任务分配给管理组。在这种情况下，任务分配给先前创建的管理组中包括的计算机。
- 选择管理服务器在网络中检测到的计算机：*未分配设备*。特定设备可包括管理组中的设备以及未分配设备。
- 手动指定设备地址或从列表中导入地址。您可以指定您要将任务分配给的设备的 NetBIOS 名称、IP 地址和 IP 子网。

步骤 3. 选择授权许可

选择您要删除的授权许可密钥。您可以从 Kaspersky Security Center 密钥存储中选择一个授权许可密钥，或者选择一个密钥文件。转到下一步。

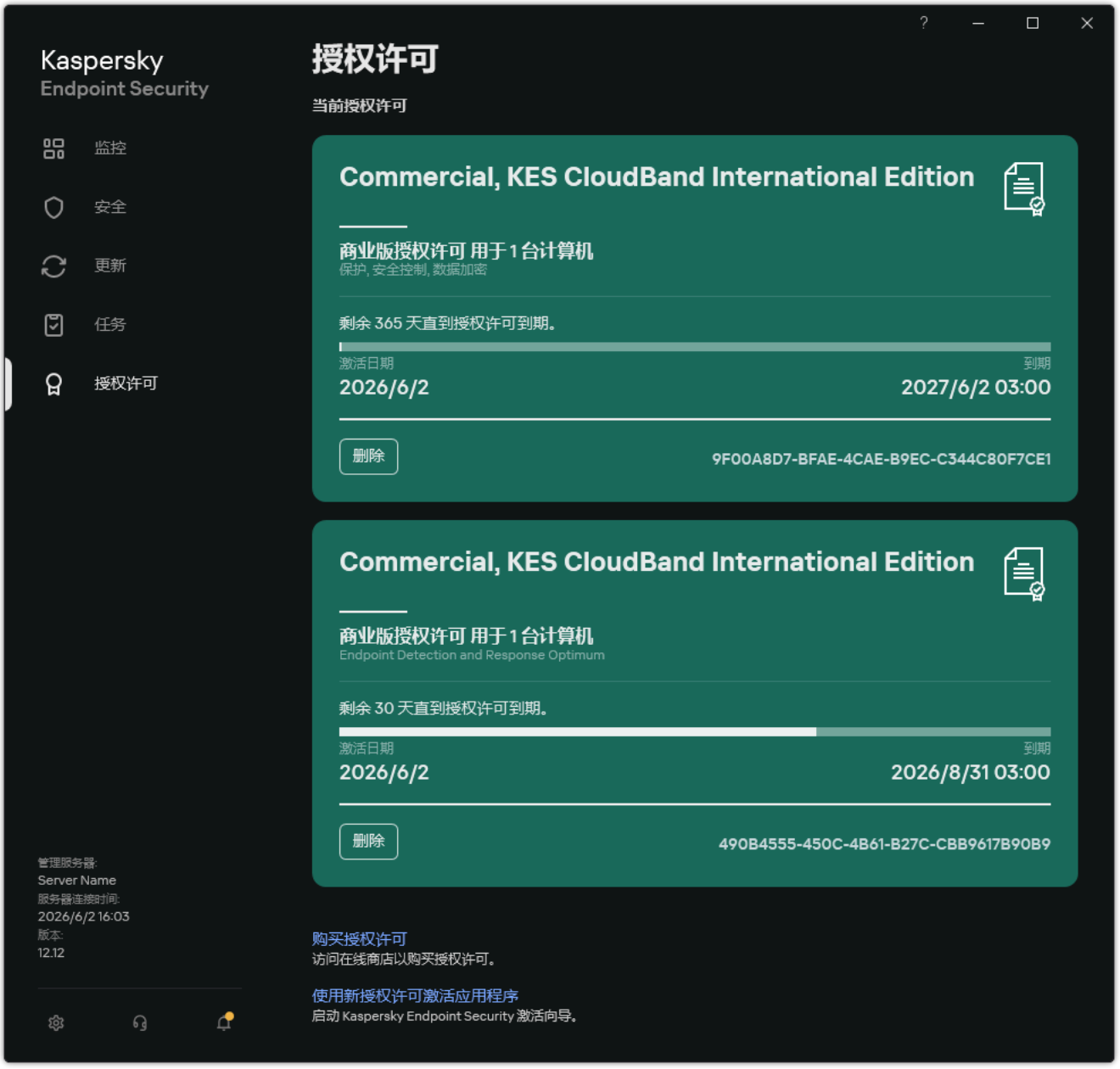
步骤 4. 完成任务创建

单击“**完成**”按钮完成向导。在任务列表中将显示一个新任务。要运行任务，请选中与任务对应的复选框，然后单击“**开始**”按钮。

如何在应用程序界面中删除授权许可密钥

1. 在应用程序主窗口中，转到“**授权许可**”区域。

2. 选择您要删除的密钥，然后单击“**删除**”。



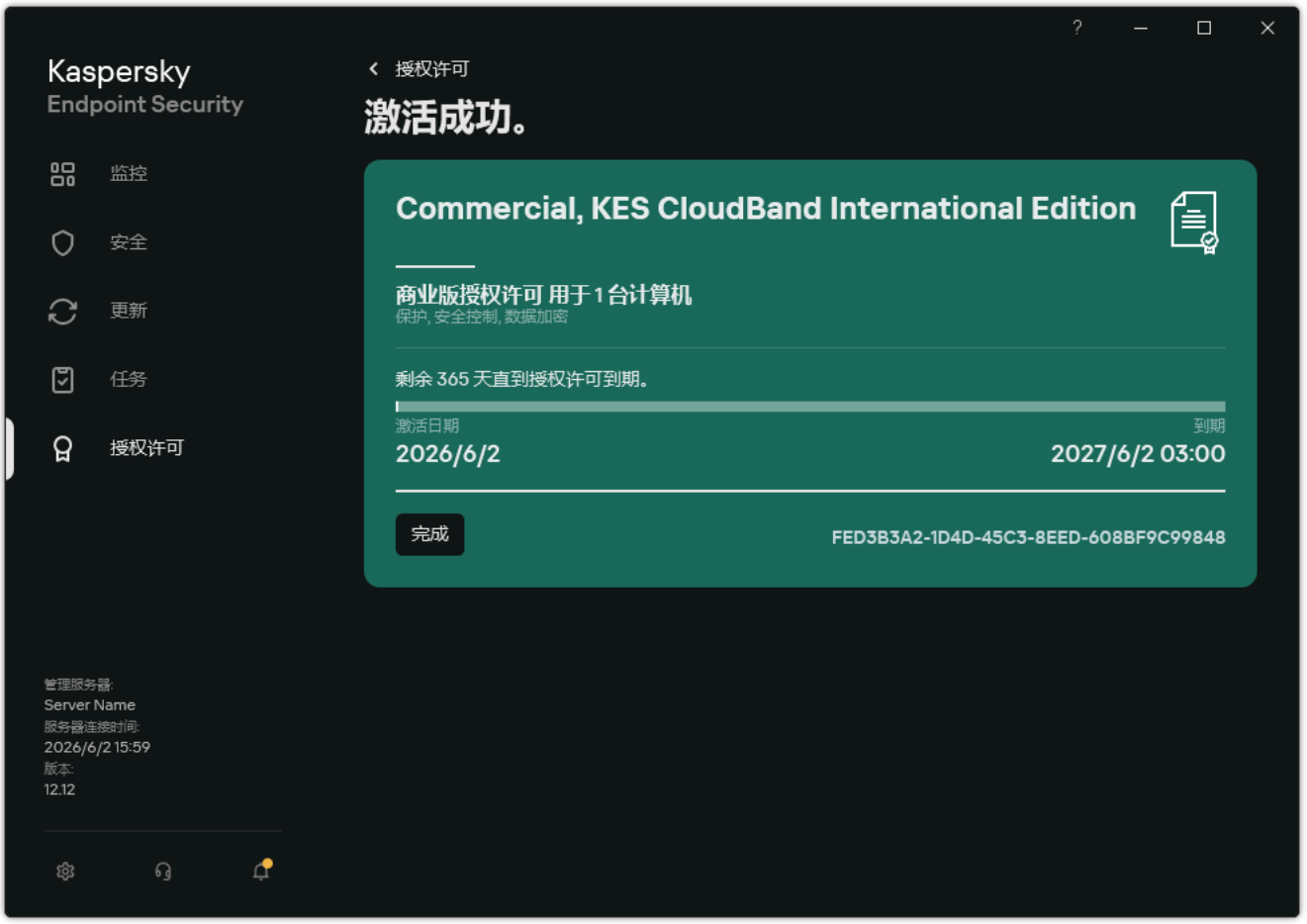
“授权许可”窗口

您还可以在命令行上删除授权许可密钥。

查看授权许可信息

要查看授权许可的相关信息：

在应用程序主窗口中，转到“**授权许可**”区域（参见下图）。



“授权许可”窗口

该区域显示以下详情：

- *密钥状态*。一台计算机上可以存储多个密钥。有两种类型的密钥：活动密钥和备用密钥。本应用程序不能拥有两个及以上活动密钥。只有活动密钥到期或使用**删除**按钮删除活动密钥后，备用密钥才变为活动密钥。
- *应用程序名称*。已购买的 Kaspersky 应用程序的全名。
- *授权许可类型*。以下授权许可类型可用：试用和商业。
- *功能*。在您的授权许可下提供的应用程序功能。功能可能包括保护、安全控制、数据加密等。授权许可证书中还提供了可用功能的列表。

- *有关授权许可的附加信息*。授权许可期限的开始日期和结束日期（仅适用于活动密钥），授权许可期限的剩余期限。

  授权许可到期日期根据操作系统中配置的时区进行显示。

- *密钥*。密钥是从激活码或密钥文件生成的唯一字母数字序列。

在“授权许可”窗口中，还可以执行下列操作之一：

- **购买授权许可 / 续费授权许可**。打开受保护设备在线商店网站，在其中可以购买或续费授权许可。为此，请输入您的公司信息并支付订单。

- “**使用新授权许可激活应用程序**”。启动应用程序激活向导。在此向导中可以使用激活码或密钥文件添加密钥。应用程序激活向导允许您添加一个活动密钥和一个（且仅有一个）备用密钥。

购买授权许可

您可以在安装程序后购买授权许可。购买授权许可后，您将收到用于激活应用程序的激活码或密钥文件。

要购买授权许可：

1. 在应用程序主窗口中，转到“**授权许可**”区域。

2. 执行下列操作之一：

   - 如果未添加任何密钥，或添加了试用版授权许可的密钥，请单击“**购买授权许可**”按钮。

   - 如果安装了商用版授权许可的密钥，请单击“**续费授权许可**”按钮。

   这时浏览器将打开 Kaspersky 在线商店的窗口，您可以在此网站中购买授权许可。

续费订阅

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应用程序，Kaspersky Endpoint Security 将自动检查激活服务器，以后台模式获取续费的密钥。如果激活服务器上有可用密钥，应用程序会替换先前授权许可继而添加此授权许可。通过这种方式，使用无限订阅的 Kaspersky Endpoint Security 无需用户介入进行更新。

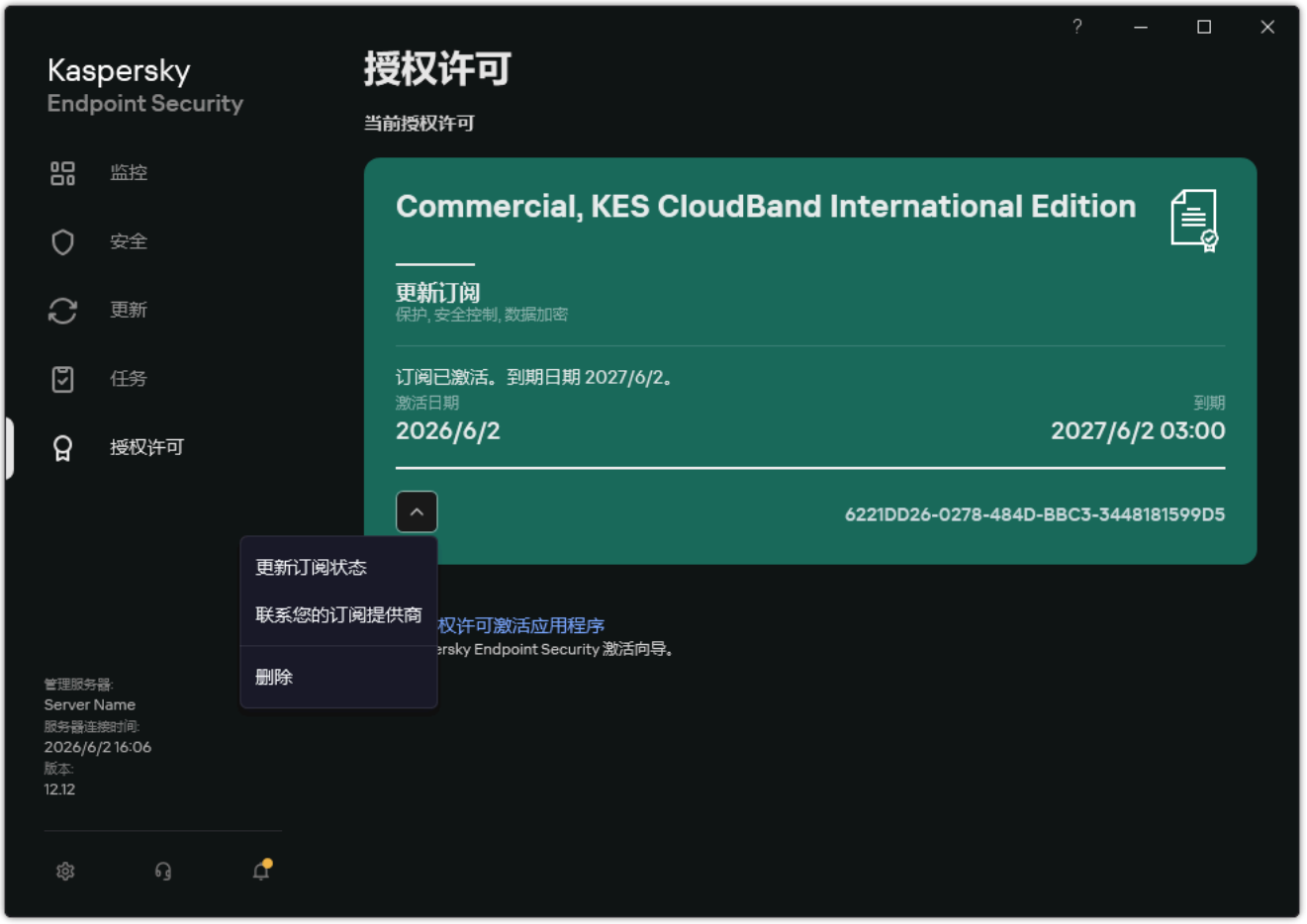
如果您在有限订阅下使用本应用程序，在订阅到期之日（或订阅续费宽限期到期之日），Kaspersky Endpoint Security 将通知您，并停止尝试自动续费订阅。在这种情况下，Kaspersky Endpoint Security 将与商用版应用程序过期一样的方式运行：应用程序运行但是没有更新且卡巴斯基安全网络不可用。

您可以在服务提供商的网站上续费订阅。

若要从程序界面中访问服务提供商网站，请执行以下操作：

1. 在应用程序主窗口中，转到“**授权许可**”区域。
2. 单击“**联系您的订阅提供商**”。

您可以手动更新订阅状态。如果在宽限期后对订阅进行续费并且订阅状态未自动更新时，您可能需要执行此操作。



续费订阅

入门

安装 Kaspersky Endpoint Security 后，您可以使用以下界面管理应用程序：

- 本地应用程序界面。
- Kaspersky Security Center 管理控制台。
- Kaspersky Security Center Web Console。
- Kaspersky Security Center 云控制台。

Kaspersky Security Center 管理控制台

Kaspersky Security Center 允许您远程安装和卸载、启动和停止 Kaspersky Endpoint Security，配置应用程序设置，更改可用应用程序组件的集合，添加密钥以及启动和停止更新和扫描任务。

可以使用 Kaspersky Security Center 管理插件通过 Kaspersky Endpoint Security 管理应用程序。

有关通过 Kaspersky Security Center 管理应用程序的详细信息，请参阅 Kaspersky Security Center 帮助。

Kaspersky Security Center Web Console 和 Kaspersky Security Center 云控制台

Kaspersky Security Center Web Console（以下简称“*Web Console*”）是用于集中执行主要任务来管理和维护组织网络的安全系统的 Web 应用程序。Web Console 是提供用户界面的 Kaspersky Security Center 组件。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（以下简称“*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。

Web Console 和云控制台允许您执行以下操作：

- 监控组织的安全系统的状态。
- 在网络内的设备上安装卡巴斯基应用程序。
- 管理已安装的应用程序。
- 查看有关安全系统状态的报告。

通过 Web Console、云控制台和 Kaspersky Security Center 管理控制台管理 Kaspersky Endpoint Security 都提供不同的管理功能。对于不同的控制台，可用的组件和任务也有所不同。

关于 Kaspersky Endpoint Security for Windows 管理插件

Kaspersky Endpoint Security for Windows 管理插件允许在 Kaspersky Endpoint Security 和 Kaspersky Security Center 之间进行交互。通过管理插件，您可以使用策略、任务和本地应用程序设置来管理 Kaspersky Endpoint Security。该 Web 插件提供了与 Kaspersky Security Center Web Console 进行交互的功能。

管理插件的版本会根据客户端计算机上所安装 Kaspersky Endpoint Security 应用程序版本的不同而有所不同。如果所安装的管理插件版本比已安装版本的 Kaspersky Endpoint Security 的功能少，则管理插件不会管理缺失功能的设置。用户可以在 Kaspersky Endpoint Security 本地界面修改这些设置。

默认情况下，该 Web 插件不安装在 Kaspersky Security Center Web Console 中。 必须在安装了Kaspersky Security Center Web Console 的计算机上安装 Web 插件。有权在浏览器中访问 Web Console 的所有管理员都可以使用该 Web 插件的功能。您可以在 Web Console 界面中查看已安装的 Web 插件列表：“**控制台设置**” → “**Web 插件**”。有关 Web 插件版本与 Web 控制台的兼容性的详细信息，请参阅 Kaspersky Security Center 帮助。

如果您将 Kaspersky Endpoint Security 作为 Kaspersky Endpoint Detection and Response Optimum 解决方案的一部分使用，则必须安装 Kaspersky Endpoint Detection and Response 管理插件。您需要管理插件来显示警报详细信息。*警报详情*是一种工具，用于查看所收集的有关检测到的威胁的全部信息。警报详情包括，例如，出现在计算机的文件历史。因此，要创建威胁响应任务，您需要 Kaspersky Endpoint Security 管理插件，而要查看警报详细信息，您需要 EDR 管理插件。

安装 Web 插件

您可以按如下方式安装该 Web 插件：

- 使用 Kaspersky Security Center Web Console 的快速启动向导安装 Web 插件。

  第一次将 Web 控制台连接到管理服务器时，Web 控制台会自动提示您运行快速启动向导。您还可以在 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 插件是否为最新，并下载必需的更新。有关 Kaspersky Security Center Web Console 的快速启动向导的详细信息，请参阅 Kaspersky Security Center 帮助。

- 在 Web 控制台中使用可用分发包列表安装 Web 插件。

  要安装 Web 插件，请在 Web Console 界面中选择 Kaspersky Endpoint Security Web 插件的分发包（“**控制台设置**” → “**Web 插件**”）。在新版本的 Kaspersky 应用程序发布后，可用分发包列表会自动更新。

- 将分发包从外部源下载到 Web 控制台。

  要安装 Web 插件，请在 Web Console 界面中添加 Kaspersky Endpoint Security for Windows Web 插件的分发包的 ZIP 存档（“**控制台设置**” → “**Web 插件**”）。例如，可以在 Kaspersky 网站下载 Web 插件的分发包。

从 Kaspersky Endpoint Security 12.11 for Windows 开始， Web 插件的安装过程发生了变化。分发包现在包含两个 Web 插件：*Kaspersky Endpoint Security for Windows 14.2.0* 以及 *Unified Protection and Management Plug-in*。这是由于卡巴斯基应用程序的管理过渡到使用单一的统一 Web 插件所致。统一的 Web 插件允许创建单一策略来管理多个卡巴斯基应用程序（例如，Kaspersky Endpoint Security for Windows、macOS 和 Linux）。过渡到统一的 Web 插件可能需要几个版本的时间。过渡完成后，分发包将仅包含以下内容：*Unified Protection and Management Plug-in*。

更新管理插件

要更新 Kaspersky Endpoint Security for Windows 管理插件，请下载该插件的最新版本（包含在分发包中），并运行插件安装向导。

如果有新版本的 Web 插件可用，Web 控制台将显示通知"*所用插件有更新*"。您可以继续从该 Web 控制台通知更新 Web 插件版本。您也可以在 Web 控制台界面中手动检查新 Web 插件更新（"**控制台设置**"→"**Web 插件**"）。更新过程中将自动删除以前版本的 Web 插件。

> Web 插件更新后，将保存已有项目（例如，策略或任务）。用于实现 Kaspersky Endpoint Security 新功能的新项目设置将显示在现有项目中，并采用默认值。

您可以按如下方式更新 Web 插件：

- 在在线模式下，在 Web 插件列表中更新 Web 插件。

  要更新 Web 插件，必须在 Web 控制台界面中选择 Kaspersky Endpoint Security Web 插件的分发包（"**控制台设置**"→"**Web 插件**"）。Web 控制台将在 Kaspersky 服务器中检查可用更新，并下载相关更新。

- 从文件更新 Web 插件。

  要更新 Web 插件，必须在 Web 控制台界面中选择 Kaspersky Endpoint Security for Windows Web 插件的分发包的 ZIP 存档（"**控制台设置**"→"**Web 插件**"）。例如，可以在 Kaspersky 网站下载 Web 插件的分发包。您只能将 Kaspersky Endpoint Security Web 插件更新到最新版本。Web 插件不能更新到较旧版本。

如果打开了任何项目（如策略或任务），则 Web 插件将检查其兼容性信息。如果 Web 插件的版本等于或晚于兼容性信息中指定的版本，则您可更改此项目的设置。否则您无法使用 Web 插件更改所选项目的设置。建议更新 Web 插件。

使用不同版本的管理插件时的特别考虑

只有当管理插件的版本等于或晚于 Kaspersky Endpoint Security 与管理插件兼容性信息中指定的版本时，您才可以通过 Kaspersky Security Center 管理 Kaspersky Endpoint Security。您可以在包括在分发包中的 installer.ini 档案中查看管理插件的最低要求版本。

> 如果打开了任何项目（如策略或任务），则管理插件将检查其兼容性信息。如果管理插件的版本等于或晚于兼容性信息中指定的版本，则您可更改此项目的设置。否则您无法使用管理插件更改所选项目的设置。建议升级管理插件。

如果在管理控制台中安装了 Kaspersky Endpoint Security 管理插件，在安装新版本的管理插件时请考虑以下事项：

- 以前版本的 Kaspersky Endpoint Security 管理插件将被删除。
- 新版本的 Kaspersky Endpoint Security 管理插件支持管理用户计算机上先前版本的 Kaspersky Endpoint Security for Windows。
- 您可以使用新版本的管理插件更改由以前版本的管理插件创建的策略、任务和其他项目中的设置。
- 对于新设置，新版本的管理插件会在第一次保存策略、策略配置文件或任务时分配默认值。

升级管理插件后，建议检查新设置的值并将其保存在策略和策略配置文件中。如果不执行此操作，用户计算机上的新 Kaspersky Endpoint Security 设置组将采用默认值并可以编辑（属性）。建议从顶级层级的策略和策略配置文件开始检查设置。还建议使用有权访问所有 Kaspersky Security Center 功能区域的用户账户。

要了解应用程序的新功能，请参阅版本说明或应用程序帮助。

- 如果新版本的管理插件的一组设置中添加了新参数，先前为该组设置的/属性定义的状态不会更改。

为与外部服务的交互使用加密协议时的特殊考虑

Kaspersky Endpoint Security 和 Kaspersky Security Center 利用 TLS（Transport Layer Security）使用一个加密的通信通道来配合使用卡巴斯基外部服务。Kaspersky Endpoint Security 将外部服务用于以下功能：

- 更新数据库和应用程序软件模块；
- 用激活码（激活 2.0）激活应用程序；
- 使用卡巴斯基安全网络。

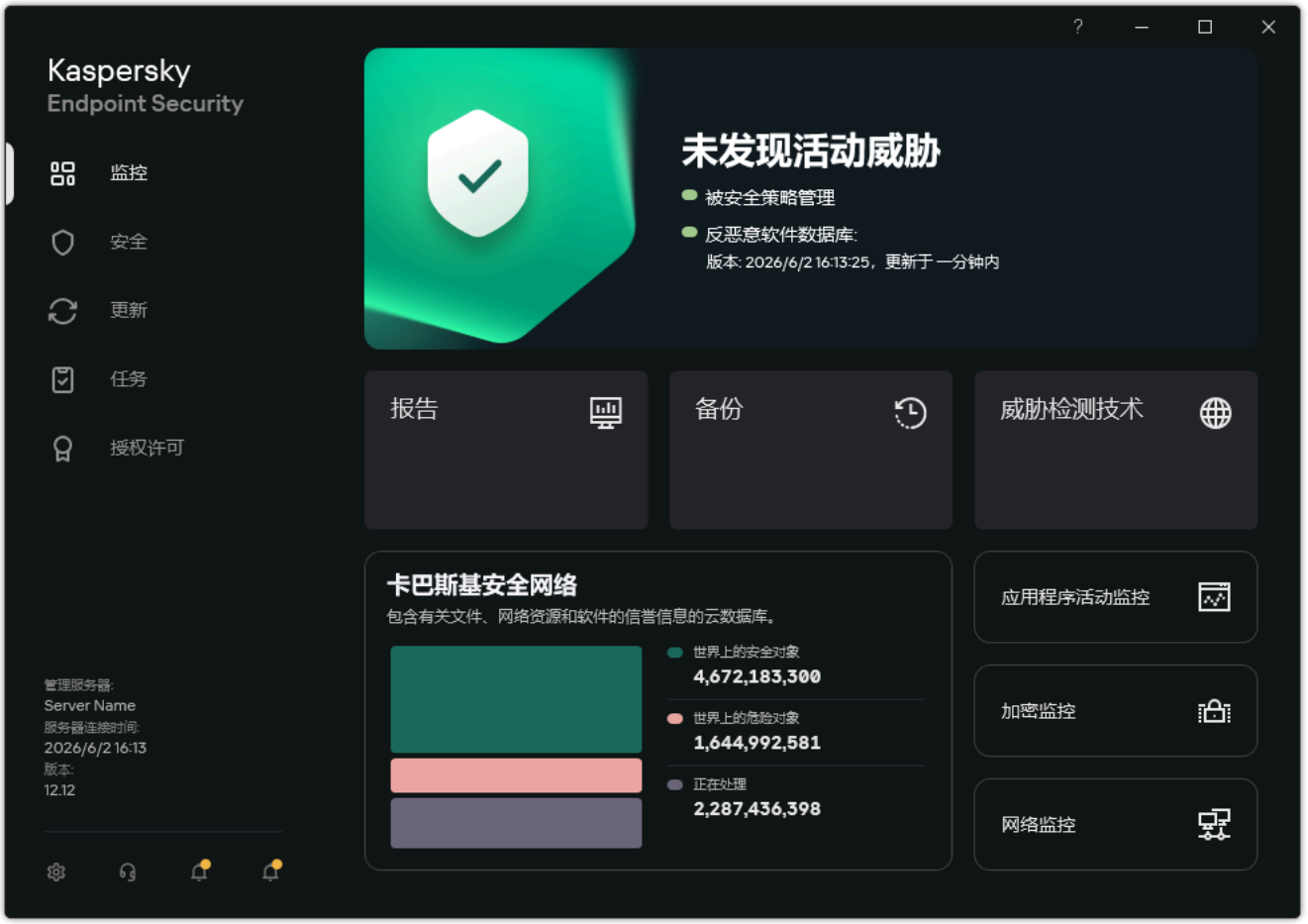
TLS 的使用通过提供以下功能来保护应用程序：

- 加密。消息内容是保密的，不向第三方用户披露。
- 完整性。消息收件人确定消息内容在发件人转发后未被修改。
- 身份验证。接收者确信通信是建立在一个可信的 Kaspersky 服务器上。

Kaspersky Endpoint Security 使用公钥证书进行服务器身份验证。使用证书需要 Public Key Infrastructure（PKI）。证书颁发机构是 PKI 的一部分。Kaspersky 使用自己的证书颁发机构，因为 Kaspersky 的服务是高度技术性的，不是公开的。在这种情况下，当 Thawte、VeriSign、GlobalTrust 等的根证书被吊销时，Kaspersky PKI 仍然可以正常运行而不会中断。

Kaspersky Endpoint Security 认为具有 MITM（支持 HTTPS 协议解析的软硬件工具）的环境是不安全的。使用 Kaspersky 服务时可能会遇到错误。例如，在使用Self-Signed Certificate时可能存在错误。这些错误可能是因为您的环境中的 HTTPS 检查工具无法识别 Kaspersky PKI。T要纠正这些问题，必须配置与外部服务交互的排除项。

程序界面



主应用程序窗口

监控	• "**报告**"。查看应用程序、单独组件和任务在操作过程中发生的事件。 • "**备份**"。查看已保存的应用程序检测到的受感染对象的副本列表。 • "**威胁检测技术**"。查看威胁检测技术和这些技术检测到的威胁数量信息。 • "**卡巴斯基安全网络**"。Kaspersky Endpoint Security 和卡巴斯基安全网络之间的连接状态，以及全球 KSN 统计信息。*卡巴斯基安全网络 (KSN)* 是一个云服务的基础架构。它可以访问在线卡巴斯基知识库。该知识库中包含了文件信誉、网页资源和软件的相关信息。使用卡巴斯基安全网络的数据可确保 Kaspersky Endpoint Security 能够更快地对新威胁作出响应，提高一些保护组件的性能，并减少误报风险。如果您正在参与卡巴斯基安全网络，KSN 服务为 Kaspersky Endpoint Security 提供有关已扫描网址的信誉的信息，以及有关已扫描文件的类别和信誉的信息。 • "**应用程序活动监控**"。查看已安装应用程序的操作信息。应用程序活动监控将保持对文件、注册表以及与应用程序关联的操作系统事件的跟踪。 • **网络监控**。实时查看计算机网络活动信息。 • "**加密监控**"。实时监控磁盘加密或解密过程。加密监控器在卡巴斯基磁盘加密组件或 BitLocker 驱动器加密组件被安装时可用。
安全	已安装组件的操作状态。您还可以继续配置组件或查看报告。
更新	管理 Kaspersky Endpoint Security 更新任务。您可以更新反病毒数据库和应用程序模块以及回滚上一次更新。管理员可以对用户隐藏分区或限制任务管理。
任务	管理 Kaspersky Endpoint Security 扫描任务。您可以运行恶意软件扫描和应用程序完整性检查。管理员可以从用户隐藏任务或限制任务管理。
授权许可	应用程序授权许可。您可以购买授权许可、激活应用程序或续费订阅。您也可以查看当前授权许可信息。
⚙	配置应用程序设置。管理员可以禁止对 Kaspersky Security Center 设置进行更改。
	应用程序相关信息：Kaspersky Endpoint Security 的当前版本、数据库发布日期、密钥和其他信息。您也可以转到提供有用的信息、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的 Kaspersky 信息资源。
	包含可用更新以及到加密文件和设备的访问请求信息的消息。

任务栏通知区域中的程序图标

Kaspersky Endpoint Security 安装完成后，应用程序图标将立即出现在 Microsoft Windows 任务栏通知区域。

> 如果任务栏通知区域的应用程序图标被隐藏，管理员禁止在策略中显示应用程序界面。

该图标有以下功能：

- 它指示程序活动。
- 是访问上下文菜单和应用程序主窗口的快捷方式。

提供以下应用程序图标状态以显示应用程序运行信息：

- 图标表示应用程序至关重要的保护组件已启用。如果需要用户执行操作（例如，在更新应用程序后重新启动计算机），则 Kaspersky Endpoint Security 将显示警告。
- 图标表示应用程序至关重要的保护组件已禁用或发生故障。例如，如果授权许可已过期或存在应用程序错误，则可能导致保护组件发生故障。Kaspersky Endpoint Security 将显示警告 并描述计算机保护中的问题。

应用程序图标的上下文菜单包含下列项：

- “**Kaspersky Endpoint Security for Windows**”。打开应用程序主窗口。在此窗口中，您可以调节应用程序组件和任务的运行，并查看已处理的文件和检测到的威胁的统计数据。
- **暂停保护 / 恢复保护**。暂停策略中不带锁标记 () 的所有保护和控制组件的运行。在执行此操作之前，建议禁用 Kaspersky Security Center 策略。

  在暂停保护和控制组件的运行之前，应用程序会请求 Kaspersky Endpoint Security 的访问密码（账户密码或临时密码）。您随后可以选择暂停时间段：特定一段时间、直至重新启动或用户请求后。

  如果已启用密码保护，则此上下文菜单项可用。要恢复保护和控制组件运行，请在应用程序的上下文菜单中单击“**恢复保护**”。

  > 暂停保护和控制组件的运行不会影响更新和恶意软件扫描任务的性能。应用程序也继续使用卡巴斯基安全网络。

- **禁用策略 / 启用策略**。在计算机上禁用 Kaspersky Security Center 策略。所有 Kaspersky Endpoint Security 设置均可进行配置，包括策略中已上锁的设置 ()。如果禁用策略，应用程序将请求访问 Kaspersky Endpoint Security 的密码（账户密码或临时密码）。如果已启用密码保护，则此上下文菜单项可用。要启用策略，请在应用程序的上下文菜单中选择“**启用策略**”。
- “**设置**”。打开应用程序设置窗口。
- “**支持**”。这将打开包含联系 Kaspersky 技术支持所需信息的窗口。
- “**关于**”。该项目可打开一个包含应用程序详细信息的窗口。

- “**退出**”。该项目可退出 Kaspersky Endpoint Security。点击该上下文菜单中的“退出”项会导致应用程序退出计算机的RAM。

应用程序图标上下文菜单

简化应用程序界面

如果将配置了“显示简化应用程序界面”的 Kaspersky Security Center 策略应用于已安装 Kaspersky Endpoint Security 的客户端计算机，则在该客户端计算机上不能使用应用程序主窗口。右键单击 Kaspersky Endpoint Security 图标可打开上下文菜单（如下图），其中包含以下项目：

- **禁用策略 / 启用策略**。在计算机上禁用 Kaspersky Security Center 策略。所有 Kaspersky Endpoint Security 设置均可进行配置，包括策略中已上锁的设置 (🔒)。如果禁用策略，应用程序将请求访问 Kaspersky Endpoint Security 的密码（账户密码或临时密码）。如果已启用密码保护，则此上下文菜单项可用。要启用策略，请在应用程序的上下文菜单中选择“**启用策略**”。

- “**任务**”。包含以下项的下拉列表：

  - “**应用程序完整性检查**”。

  - “**回滚数据库到其先前版本**”。

  - “**全盘扫描**”。

  - “**自定义扫描**”。

  - “**关键区域扫描**”。

  - “**更新**”。

- “**支持**”。这将打开包含联系 Kaspersky 技术支持所需信息的窗口。

- “**退出**”。该项目可退出 Kaspersky Endpoint Security。点击该上下文菜单中的“退出”项会导致应用程序退出计算机的RAM。

显示简化界面时应用程序图标的上下文菜单

配置应用程序界面的显示

您可以为用户配置应用程序界面显示模式。用户可以通过以下方式与应用程序进行交互：

- “**显示简化界面**”。在客户端计算机上，主应用程序窗口不可访问，只有 Windows 通知区域中的图标可用。在该图标的上下文菜单中，用户可以使用 Kaspersky Endpoint Security 执行有限数量的操作。Kaspersky Endpoint Security 也仅在应用程序图标上方显示需要用户操作的通知。

- “**显示用户界面**”。在客户端计算机上，Kaspersky Endpoint Security 的主窗口和 Windows 通知区域中的图标均可用。在该图标的上下文菜单中，用户可以使用 Kaspersky Endpoint Security 执行操作。Kaspersky Endpoint Security 还会在应用程序图标上方显示通知。

- “**不显示用户界面**”。在客户端计算机上，不显示 Kaspersky Endpoint Security 操作的迹象。Windows 通知区域中的图标和通知不可用。

如何在管理控制台 (MMC) 中配置应用程序界面显示模式

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **常规设置** → **界面**。

4. 在“**用户交互**”块中，配置应用程序界面的显示方式：

   - “**显示用户界面**”。在客户端计算机上，Kaspersky Endpoint Security 的主窗口和 Windows 通知区域中的图标均可用。在该图标的上下文菜单中，用户可以使用 Kaspersky Endpoint Security 执行操作。Kaspersky Endpoint Security 还会在应用程序图标上方显示通知。如有必要，您可以启用“**隐藏应用程序活动监控区域**”功能以隐藏有关计算机上应用程序活动的数据，从而限制用户对应用程序活动监控工具的访问。

   - “**显示简化界面**”。在客户端计算机上，主应用程序窗口不可访问，只有 Windows 通知区域中的图标可用。在该图标的上下文菜单中，用户可以使用 Kaspersky Endpoint Security 执行有限数量的操作。Kaspersky Endpoint Security 也仅在应用程序图标上方显示需要用户操作的通知。

   - “**不显示用户界面**”。在客户端计算机上，不显示 Kaspersky Endpoint Security 操作的迹象。Windows 通知区域中的图标和通知不可用。

5. 保存更改。

如何在 Web Console 和云控制台中配置应用程序界面显示模式

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **常规设置** → **用户交互**。

5. 在“**用户可见性**”块中，配置应用程序界面的显示方式：

- “**显示用户界面**”。如果禁用此功能，客户端计算机上不会显示 Kaspersky Endpoint Security 的任何运行迹象。Windows 通知区域中的图标和通知不可用。
- “**简化**”。在客户端计算机上，主应用程序窗口不可访问，只有 Windows 通知区域中的图标可用。在该图标的上下文菜单中，用户可以使用 Kaspersky Endpoint Security 执行有限数量的操作。Kaspersky Endpoint Security 也仅在应用程序图标上方显示需要用户操作的通知。
- “**完整**”。在客户端计算机上，Kaspersky Endpoint Security 的主窗口和 Windows 通知区域中的图标均可用。在该图标的上下文菜单中，用户可以使用 Kaspersky Endpoint Security 执行操作。Kaspersky Endpoint Security 还会在应用程序图标上方显示通知。
- “**隐藏应用程序活动监控区域**”。果要在用户的计算机上隐藏应用程序活动信息，您可以限制用户对应用程序活动监控工具的访问。

6. 保存更改。

准备应用程序以供使用

在客户端计算机上部署应用程序后，要从 Kaspersky Security Center Web Console 使用 Kaspersky Endpoint Security，需要执行以下操作：

- 创建并配置策略。

  您可以使用策略让同一 Kaspersky Endpoint Security 设置应用于一个管理组的所有客户端计算机中。Kaspersky Security Center 的快速启动向导会自动为 Kaspersky Endpoint Security 创建策略。

- 创建“*数据库和应用程序模块更新*”和“*恶意软件扫描*”任务。

  使计算机安全性保持最新需要“*数据库和应用程序模块更新*”任务。执行该任务时，Kaspersky Endpoint Security 将更新反病毒数据库和应用程序模块。“*数据库和应用程序模块更新*”任务由管理服务器快速启动向导自动创建。要创建“*数据库和应用程序模块更新*”任务，请在运行向导时安装 Kaspersky Endpoint Security for Windows Web 插件。

  及时检测威胁和其他恶意软件需要“*恶意软件扫描*”任务。您需要手动创建“*恶意软件扫描*”任务。

  如何在管理控制台 (MMC) 中创建“恶意软件扫描 ”任务

  1. 在 Kaspersky Security Center 管理控制台树中，选择“**任务**”。

     任务列表打开。

  2. 单击“**新任务**”。

  “任务向导”将启动。按照向导的说明进行操作。

步骤 1. 选择任务类型

选择“**Kaspersky Endpoint Security for Windows (14.1)**”→ “**恶意软件扫描**”。

步骤2. 扫描范围

创建 Kaspersky Endpoint Security 在执行扫描任务时要扫描的对象列表。

步骤3. Kaspersky Endpoint Security 操作

选择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。
- "**清除；如果清除失败则通知**"。如果选择该选项，Kaspersky Endpoint Security 将自动尝试对已经检测到的所有受感染的文件执行清除操作。如果清除失败，Kaspersky Endpoint Security 会将检测到的受感染文件的相关信息添加到活动威胁列表。
- "**通知**"。如果选择此选项，Kaspersky Endpoint Security 会在检测到受感染文件时将这些文件的相关信息添加到活动威胁列表。
- "**立即运行高级清除**"。如果选中该复选框，则 Kaspersky Endpoint Security 在扫描过程中将使用高级清除技术来处理活动威胁。

  *高级清除技术*致力于清除 RAM 中已启动进程，以及阻止 Kaspersky Endpoint Security 使用其他方式移除它们的恶意应用程序。结果就是威胁被消除。执行高级杀毒时，我们建议您不要开启新的进程或者编辑操作系统注册表。高级清除技术会占用相当多的操作系统资源，这可能会降低其他应用程序的运行速度。完成高级清除后，Kaspersky Endpoint Security 将重启计算机，且不提示用户进行确认。
- "**仅在计算机空闲时运行**"。计算机资源忙时推迟任务启动。如果计算机被锁定或屏幕保护开启，Kaspersky Endpoint Security 启动扫描任务。如果您中断了任务的执行，例如通过解锁计算机，Kaspersky Endpoint Security 将自动运行该任务，并从中断点继续运行。此计划选项允许您在使用计算机时节省计算机资源。

步骤 4. 选择任务将分配到的设备

选择将要执行任务的计算机。下列选项可用：

- 将任务分配给管理组。在这种情况下，任务分配给先前创建的管理组中包括的计算机。
- 选择管理服务器在网络中检测到的计算机：*未分配设备*。特定设备可包括管理组中的设备以及未分配设备。
- 手动指定设备地址或从列表中导入地址。您可以指定您要将任务分配给的设备的 NetBIOS 名称、IP 地址和 IP 子网。

步骤 5. 选择要运行任务的账户

选择要运行*恶意软件扫描*任务的账户。默认情况下，Kaspersky Endpoint Security 将使用本地用户账户的权限启动任务。如果扫描范围包括网络驱动器或访问受限的其他对象，请选择具有足够访问权限的用户账户。

步骤 6. 配置任务启动计划

配置任务启动计划，例如，手动或在将反病毒数据库下载到存储库之后。

步骤 7. 定义任务名称

输入任务的名称，例如“*每日全盘扫描*”。

步骤 8. 完成任务创建

退出向导。如有必要，选中“**向导完成时运行任务**”复选框。您可以在任务属性中监控任务进度。结果，将按照指定计划在用户计算机上执行“恶意软件扫描”任务。

如何在 Web Console 中创建“恶意软件扫描”任务

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
2. 单击“**添加**”。
   “任务向导”将启动。
3. 配置任务设置：
   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Endpoint Security for Windows 14.2.0**”。
   b. 在“**任务类型**”下拉列表中，选择“**恶意软件扫描**”。
   c. 在“**任务名称**”字段中，输入简要说明，例如“*每周扫描*”。
   d. 在“**要对其分配任务的设备**”块，选择任务范围。
4. 按照所选任务范围选项选择设备。转到下一步。
5. 选择要运行任务的账户。默认情况下，Kaspersky Endpoint Security 将使用本地用户账户的权限启动任务。
6. 退出向导。
   在任务列表中将显示一个新任务。

7. 要配置任务计划，请转到任务属性。
   建议将任务计划为每周至少运行一次。

8. 选中该任务旁边的复选框。

9. 单击“**开始**”。
   您可以监控任务的状态，以及成功完成任务或完成任务时发生错误的设备数量。

结果，将按照指定计划在用户计算机上执行“恶意软件扫描”任务。

- 优化 Kaspersky Endpoint Security 性能。

管理策略

*策略*是为管理组定义的一系列应用程序设置。您可以为一个应用程序配置多个具有不同值的策略。对于不同的管理组，应用程序可以在不同的设置下运行。每个管理组都有自己的应用程序策略。

每个策略设置都有 （“挂锁”）属性。此属性的状态决定了该设置是否会传递给管理组中的受管理设备：

- 如果“挂锁”是打开的（ ），此设置的值将不会传递给受管理设备。该设置可在应用程序的本地界面中进行修改。此类设置被称为*已解锁*。

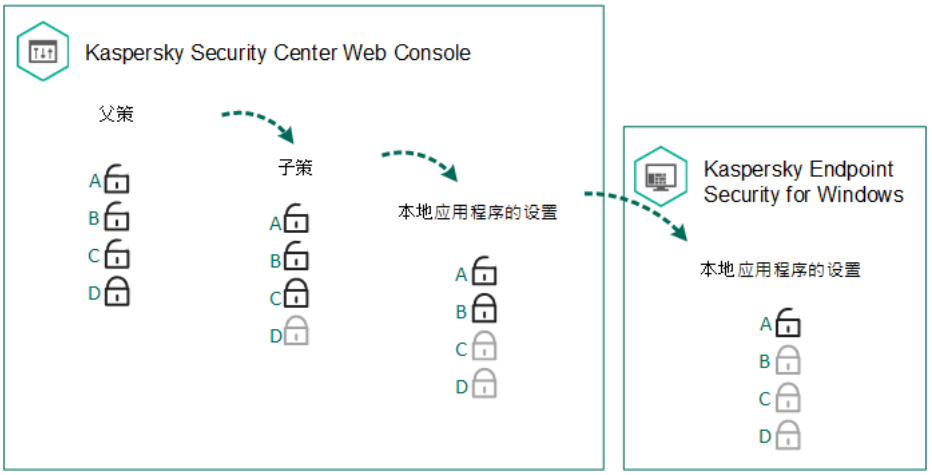
- 如果“挂锁”已关闭（ ），该设置的值将被传递并应用于受管理设备。此类设置被称为*已锁定*。被阻止的设置无法在应用程序的本地界面中进行修改。

在*同步*期间，策略设置由网络代理发送到客户端计算机。默认情况下，管理服务器在策略设置发生变化后立刻执行同步。使用客户端计算机上的 UDP 端口 15000 进行同步。默认情况下，管理服务器每 15 分钟执行一次同步。如果在策略设置发生变化后同步失败，将按照配置的计划执行下一次同步尝试。

设置继承

像管理组一样，策略按层次结构排列。*子策略*是用于嵌套层次结构级别的策略，即用于嵌套管理组和从属管理服务器的策略。

默认情况下，子策略从父策略继承设置。如果父策略中的设置具有 🔒（关闭的"挂锁"）属性，则在子策略和本地应用程序设置中，该设置的值将根据父策略被覆盖，并且该设置将被锁定。如果必要，您可以禁用从父策略继承设置。漫游策略不通过管理组的层次结构影响其他策略。



设置继承

为每个拥有 Kaspersky Security Center 管理服务器访问权限的用户指定访问策略设置的权限（读取、写入、执行），并为 Kaspersky Endpoint Security 的每个功能范围单独指定策略设置。要配置策略设置的访问权限，请转至 Kaspersky Security Center 管理服务器属性窗口的"**安全性**"部分（默认情况下，此部分隐藏在控制台界面中）。

策略修订

Kaspersky Security Center 跟踪策略修改并创建修订版本。一个*修订*是用户保存的一组修改后的参数。修订允许您比较和恢复策略参数的更改。除了修改后的参数集外，修订内容还包括进行更改的用户信息，以及时间、IP 地址、用户评论和其他相关数据。

要查看修订日志，请打开策略属性并转到"**修订历史**"部分。有关使用修订的详细信息，请参阅 Kaspersky Security Center 帮助。

创建策略

创建策略时，向导会建议与所选模式相关的设置。例如，对于 Light Agent 模式，您必须添加 Protection Server (SVM)。当使用应用程序保护 SQL 服务器时，您必须添加预定义的扫描排除项以确保服务器的运行不受干扰。选择模式后，向导会建议相关的策略设置。然后您可以在策略属性中编辑这些设置。

如何在管理控制台 (MMC) 中创建策略

1. 打开 Kaspersky Security Center Administration Console。
2. 在管理控制台树的"**受管理设备**"文件夹中，选择相关客户端计算机所属的管理组名称的文件夹。
3. 在工作区中选择"**策略**"选项卡。

4. 单击“**新策略**”。

   “策略向导”将启动。

5. 按照“策略向导”的说明进行操作。

步骤 1.

选择 **Kaspersky Endpoint Security for Windows （14.1）** 安装包。

步骤 2.

输入组策略的名称，例如，*办公室政策*。

您还可以使用策略向导按照已有的策略创建新策略。为此，在指定组策略名称时，选择“**使用早期版本应用程序的策略设置**”复选框。该向导还允许根据不同解决方案的策略创建 Kaspersky Endpoint Security (KES) 策略，例如 Kaspersky Security for Windows Server (KSWS) 或 Kaspersky Security for Virtualization Light Agent for Windows

步骤 3 加入卡巴斯基安全网络

请阅读并接受卡巴斯基安全网络 (KSN) 声明的条款。

步骤 4.

根据 Kaspersky Endpoint Security 的预期用途，您可以为以下应用程序模式配置策略：

- 保护主机的标准模式

  在此模式下，您可以选择如何配置策略：

  - “**使用默认设置创建策略**”。默认设置被认为是最佳的。此设置由 Kaspersky 专家推荐。默认设置提供建议的保护级别和最佳资源使用。

  - “**在向导中更改策略设置**”。该方法允许使用向导逐步管理策略设置。您还可以使用应用程序配置文件管理策略设置（参见下一步）。

- “用于抵御高级威胁和目标攻击的 Endpoint Detection and Response Agent”。

  Endpoint Detection and Response Agent 是安装在组织 IT 基础设施中的各个工作站和服务器上的应用程序，用于支持卡巴斯基的 Detection and Response 解决方案。下一步，您需要选择一个 EDR Agent 集成解决方案。

- “用于保护虚拟环境的 Light Agent”。

  要在 Light Agent 模式下使用应用程序，您需要配置与 SVM 虚拟机的连接。这些设置是应用程序在 Light Agent 模式下工作所必需的。

Kaspersky Endpoint Security 为所有应用程序模式和操作系统类型提供了通用策略。这意味着该策略涵盖了整个设置。然而，应用程序可能会忽略某些策略设置，因为 Kaspersky Endpoint Security 部署在某些功能不可用的模式下。例如，在 Endpoint Detection and Response Agent 模式下使用该应用程序时，只有与 Kaspersky Detection and Response 解决方案的集成以及与 KUMA 的集成相关的设置才可用。

> 我们建议针对不同的模式和操作系统类型使用不同的策略。

步骤 5. 导入设置

> 如果您在步骤 4 中选择手动策略配置，则可以执行此步骤。

您可以基于 CFG 配置文件中的 Kaspersky Endpoint Security 设置创建策略。导入应用程序配置文件时，向导无法访问所有策略设置。例如，应用程序设置中缺少策略配置文件。如果您想将所有设置和配置文件转移到该策略，您可以从 KLP 文件导入其他策略。

> 导入配置文件时，Kaspersky Endpoint Security 不会传输加密容器密码。如果在连接服务器时使用双向身份验证，则需要从头开始指定加密容器密码。

步骤 6 - 10.配置策略设置

> 如果您在步骤 4 中选择手动策略配置，则可以执行此步骤。

按照以下步骤管理策略设置。

步骤 11.配置受信任区域

配置受信任区域。您可以添加预定义扫描排除项和受信任的应用程序。预定义的扫描排除项和受信任的应用程序有助于在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上快速配置 Kaspersky Endpoint Security。这意味着您不需要在服务器上为应用程序手动设置信任区域。预定义的扫描排除项和受信任的应用程序还可以帮助您在 Light Agent 模式下快速配置 Citrix 和 VMware 虚拟环境中的 Kaspersky Endpoint Security。

步骤 12.选择策略状态

- “**活动**”。下次同步后，该策略将用作计算机上的活动策略。

  活动策略的设置在同步期间保存到客户端计算机上。您无法同时将多个策略应用到一台计算机，因此每个组只能有一个策略处于活动状态。

- “**不活动**”。备份策略。如有必要，不活动策略可切换为活动状态。

  您可以创建无限数量的不活动策略。不活动策略不影响网络中计算机的应用程序设置。不活动策略用作紧急情况（如病毒攻击）的后备。如果存在通过闪存驱动器进行的攻击，您可以激活用于阻止访问闪存驱动器的策略。在这种情况下，活动策略会自动变为不活动。

- “**漫游**”。当计算机离开组织网络周界时，将激活该策略。

结束向导。

如何在 Web Console 和云控制台中创建策略

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

2. 单击“**添加**”。

   “策略向导”将启动。

3. 选择 Kaspersky Endpoint Security 并单击“**下一步**”。

4. 请阅读并接受卡巴斯基安全网络 (KSN) 声明的条款，然后单击“**下一步**”。

5. 检查应用程序的模式：

   - 保护工作站和服务器的标准模式

   - “用于抵御高级威胁和目标攻击的 Endpoint Detection and Response Agent”。

     如果选择此模式，您可以创建一个策略将计算机与 Kaspersky Detection and Response 解决方案集成。该向导将提示您配置 Kaspersky Managed Detection and Response 以及 Kaspersky Anti Targeted Attack Platform (EDR) 的集成。

   - “用于保护虚拟环境的 Light Agent”。

     如果选择此模式，则在下一步中必须配置与 Protection Server (SVM) 的连接。这些设置是应用程序在 Light Agent 模式下工作所必需的。

   Kaspersky Endpoint Security 为所有应用程序模式和操作系统类型提供了通用策略。这意味着该策略涵盖了整个设置。然而，应用程序可能会忽略某些策略设置，因为 Kaspersky Endpoint Security 部署在某些功能不可用的模式下。例如，在 Endpoint Detection and Response Agent 模式下使用该应用程序时，只有与 Kaspersky Detection and Response 解决方案的集成以及与 KUMA 的集成相关的设置才可用。

   > 我们建议针对不同的模式和操作系统类型使用不同的策略。

6. 配置受信任区域。您可以添加预定义扫描排除项和受信任的应用程序。预定义的扫描排除项和受信任的应用程序有助于在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上快速配置 Kaspersky Endpoint Security。这意味着您不需要在服务器上为应用程序手动设置信任区域。预定义的扫描排除项和受信任的应用程序还可以帮助您在 Light Agent 模式下快速配置 Citrix 和 VMware 虚拟环境中的 Kaspersky Endpoint Security。

7. 在“**常规**”选项卡上，可以执行以下操作：

- 更改策略名称。
- 选择策略状态：
  - “**活动**”。下次同步后，该策略将用作计算机上的活动策略。

    活动策略的设置在同步期间保存到客户端计算机上。您无法同时将多个策略应用到一台计算机，因此每个组只能有一个策略处于活动状态。
  - “**不活动**”。备份策略。如有必要，不活动策略可切换为活动状态。

    您可以创建无限数量的不活动策略。不活动策略不影响网络中计算机的应用程序设置。不活动策略用作紧急情况（如病毒攻击）的后备。如果存在通过闪存驱动器进行的攻击，您可以激活用于阻止访问闪存驱动器的策略。在这种情况下，活动策略会自动变为不活动。
  - “**漫游**”。当计算机离开组织网络周界时，将激活该策略。
- 配置设置继承：
  - “**从父策略继承设置**”。如果打开此切换按钮，策略设置值将继承自顶级策略。如果为父策略设置了 🔒，则无法编辑策略设置。
  - “**在子策略中强制继承设置**”。如果开启该切换按钮，策略设置的值将传播到子策略。在子策略的属性中，“**从父策略继承设置**”切换按钮将自动打开，且无法关闭。子策略设置继承自父策略，除了标记有 🔓 的设置外。如果为父策略设置了 🔒，则无法编辑子策略设置。

8. 在“**应用程序设置**”选项卡上，您可以配置 Kaspersky Endpoint Security 策略设置。

9. 结束向导。

结果，在下次同步期间，将在客户端计算机上配置 Kaspersky Endpoint Security 设置。通过单击主屏幕上的 按钮，可以在 Kaspersky Endpoint Security 界面中查看有关应用于计算机的策略的信息（例如，策略名称）。为此，在网络代理策略的设置中，需要启用接收扩展策略数据。有关网络代理策略的详细信息，请参阅 Kaspersky Security Center 帮助。

策略的导出和导入

Kaspersky Endpoint Security 允许将策略及其设置和配置文件导出到 KLP 文件。然后，您可以使用策略导出/导入功能来备份策略、将策略迁移到另一台服务器，或者，例如，将策略从 Kaspersky Security Center Windows 迁移到 Kaspersky Security Center Linux。有关管理策略的详细信息，请参阅 Kaspersky Security Center 帮助。

如何在管理控制台 (MMC) 中导出和导入策略

1. 打开 Kaspersky Security Center Administration Console。

2. 在管理控制台树的“**受管理设备**”文件夹中，打开相关客户端计算机所属的管理组名称的文件夹。

3. 在工作区中选择“**策略**”选项卡。

4. 要导出策略：

   a. 单击要导出的策略。

   b. 单击窗口右侧的“**导出策略到文件**”链接。

   c. 在打开的窗口中，指定您要将策略导出到的 KLP 文件的名称，然后选择要保存此文件的文件夹。

   d. 保存文件。

5. 要导入策略：

   a. 单击“**从文件导入策略**”。

   b. 在打开的窗口中，选择您要导入的 KLP 策略文件。

   c. 打开文件。

   这增加了一个具有“*非活动策略*”状态的新策略。

如何在 Web Console 和云控制台中导出和导入策略

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

2. 要导出策略：

   a. 选中要导出的策略旁边的复选框。

   b. 单击**导出**按钮。

   c. 在打开的窗口中，指定您要将策略导出到的 KLP 文件的名称，然后选择要保存此文件的文件夹。

   d. 保存文件。

3. 要导入策略：

   a. 单击“**导入**”。

   b. 选择要导入的 KLP 策略文件。

   c. 策略成功处理后，选择要应用该策略的管理组。

   d. 单击“**完成**”按钮完成导入策略。

   这增加了一个具有“*不活动*”状态的新策略。

安全级别指示器

安全级别指示器显示在策略属性窗口的上部。该指示器的值可能如下：

- “**高保护级别**”。如果启用以下类别的所有组件，指示器为该值并变为绿色：
  - “**关键**”。此类别包含以下组件：
    - “文件威胁防护”。
    - “行为检测”。
    - “漏洞利用防御”。
    - “修复引擎”。
    - 针对外部管理对应用程序服务的保护。
  - “**重要**”。此类别包含以下组件：
    - “卡巴斯基安全网络”。
    - “Web 威胁防护”。
    - “邮件威胁防护”。
    - “主机入侵防御”。
    - “密码保护”。
- “**中保护级别**”。如果禁用了一个重要组件，指示器为该值并变为黄色。
- “**低保护级别**”。在以下任意一种情况下，指示器为该值并变为红色：
  - 一个或多个关键组件被禁用。
  - 两个或更多重要组件被禁用。

如果指示器的值为“**中保护级别**”或“**低保护级别**”，则指示器的右侧将显示一个链接，单击该链接可打开“**推荐的保护组件**”窗口。在此窗口中，可以启用任一推荐的保护组件。

升级应用程序后，保护级别指示器可能指示比升级前更低的保护级别。出现这种情况是因为应用程序的新版本引入了对计算机安全很重要的新组件或功能。升级应用程序后，您需要管理新设置以确保保护级别保持较高。

策略安全级别指标器

任务管理

您可以创建以下类型的任务来通过 Kaspersky Security Center 管理 Kaspersky Endpoint Security。

- 为单独的客户端计算机配置的本地任务。
- 为管理组中的客户端计算机配置的组任务。
- 面向一组所选计算机的任务。

您可以创建任意数量的组任务、面向一组所选计算机的任务或本地任务。有关使用管理组和计算机选择的详细信息，请参阅 Kaspersky Security Center 帮助。

Kaspersky Endpoint Security 支持以下任务：

- **恶意软件扫描**。Kaspersky Endpoint Security 扫描在任务设置中指定的计算机区域以查找病毒和其他威胁。Kaspersky Endpoint Security 运行需要“*恶意软件扫描*”任务，该任务在快速启动向导期间创建。建议将任务计划为每周至少运行一次。
- **添加密钥**。Kaspersky Endpoint Security 添加用于激活应用程序的密钥，包括附加密钥。在运行该任务前，请确保将执行该任务的计算机数量不超过授权许可允许的计算机数。
- **更改应用程序组件**。Kaspersky Endpoint Security 将根据任务设置中指定组件列表在客户端计算机上安装和删除组件。“文件威胁防护”组件无法删除。Kaspersky Endpoint Security 组件的最优集合有助于节省计算机资源。
- **清查**。Kaspersky Endpoint Security 将接收计算机上存储的所有应用程序可执行文件的相关信息。“*清查*”任务由“应用程序控制”组件执行。如果未安装“应用程序控制”组件，该任务将以错误结束。
- **数据库和应用程序模块更新**。Kaspersky Endpoint Security 更新数据库和应用程序模块。Kaspersky Endpoint Security 运行需要“*数据库和应用程序模块更新*”任务，该任务在快速启动向导期间创建。建议配置每天至少运行一次该任务的计划。

- **擦除数据**。Kaspersky Endpoint Security 立即或与 Kaspersky Security Center 长时间没有连接后删除用户计算机中的文件和文件夹。
- **更新回滚**。Kaspersky Endpoint Security 回滚最近的数据库和应用程序模块更新。例如，如果新数据库包含可能导致 Kaspersky Endpoint Security 阻止安全应用程序的错误数据，可能需要执行此任务。
- **应用程序完整性检查**。Kaspersky Endpoint Security 分析应用程序文件，检查文件是否损坏或被修改，并验证应用程序文件的数字签名。
- **管理身份验证代理账户**。Kaspersky Endpoint Security 会配置身份验证代理账户设置。使用加密驱动器需要身份验证代理。加载操作系统之前，用户需要使用代理完成身份验证。

如果应用程序由卡巴斯基作为 Endpoint Detection and Response 解决方案的一部分运行，您可以运行附加任务作为检测响应操作（responses）。例如，您可以使用"*终止进程*"任务远程终止进程。

> 仅当 Kaspersky Endpoint Security 正在运行时，才会在计算机上运行任务。

创建任务

如何在管理控制台 (MMC) 中创建任务

1. 打开 Kaspersky Security Center Administration Console。
2. 选择管理控制台树中的"**任务**"文件夹。
3. 单击"**新任务**"。
   "任务向导"将启动。
4. 按照"任务向导"的说明进行操作。

如何在 Web Console 和云控制台中创建任务

1. 在 Web Console 的主窗口中，选择"**任务**"。
   任务列表打开。
2. 单击"**添加**"。
   "任务向导"将启动。
3. 配置任务设置：
   a. 在"**应用程序**"下拉列表中，选择"**Kaspersky Endpoint Security for Windows 14.2.0**"。
   b. 在"**任务类型**"下拉列表中，选择要在用户计算机上运行的任务。
   c. 在"**任务名称**"字段中，输入简要说明。
   d. 在"**要对其分配任务的设备**"块，选择任务范围。
4. 按照所选任务范围选项选择设备。转到下一步。

5. 选择要运行任务的账户。默认情况下，Kaspersky Endpoint Security 将使用本地用户账户的权限启动任务。

6. 结束向导。

在任务列表中将显示一个新任务。该任务将具有默认设置。要配置任务设置，需要转到任务属性。要运行任务，需要选中与任务对应的复选框，然后单击“**开始**”按钮。启动任务后，您可以暂停任务并稍后恢复。

在任务列表中，您可以监视任务结果，其中包括任务状态和计算机上的任务性能统计。您还可以创建一组用于监控任务完成的事件（“**监控**”→“**事件分类**”）。有关事件选择的详细信息，请参阅 Kaspersky Security Center 帮助指南。任务执行结果还本地保存在 Windows 事件日志和 Kaspersky Endpoint Security 报告中。

管理任务访问权限

通过设置 Kaspersky Endpoint Security 的功能区访问权限，为每个拥有 Kaspersky Security Center 管理服务器访问权的用户定义 Kaspersky Endpoint Security 任务的访问权限（读取、写入、执行）。若要配置访问 Kaspersky Endpoint Security 功能区的权限，请转至 Kaspersky Security Center 管理服务器属性窗口的“**安全性**”区域。有关通过 Kaspersky Security Center 进行任务管理的详细信息，请参阅 Kaspersky Security Center 帮助。

您可以使用策略配置用户访问任务的权限（*任务管理模式*）。例如，您可以在 Kaspersky Endpoint Security 界面中隐藏组任务。

如何通过管理控制台 (MMC) 在 Kaspersky Endpoint Security 界面中配置任务管理模式

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **本地任务** → **任务管理**。

4. 配置任务管理模式（参见下表）。

5. 保存更改。

如何通过 Web Console 在 Kaspersky Endpoint Security 界面中配置任务管理模式

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **常规设置** → **用户交互**。

5. 在“**允许的操作**”下，配置任务管理模式（参见下表）。

6. 保存更改。

参数	描述
访问本地任务	如果选择此复选框，本地任务将显示在 Kaspersky Endpoint Security 的本地界面上。当没有其他策略限制时，用户可以配置并运行任务。然而，配置任务运行计划对该用户保持不可用。用户仅可以手动运行任务。 如果该复选框被清空，则停止使用本地任务。在该模式中，本地任务不根据计划运行。任务无法在 Kaspersky Endpoint Security 本地界面中启动或编辑，使用命令行工作时也无法进行。 用户仍可以通过在文件或文件夹的上下文菜单中选择"**扫描病毒**"选项开始文件或文件夹扫描。扫描任务将使用自定义扫描任务的默认设置值启动。
查看组任务	如果选择此复选框，组任务将显示在 Kaspersky Endpoint Security 的本地界面上。用户可以在应用程序界面中查看所有任务的列表。 如果清除该复选框，则 Kaspersky Endpoint Security 将显示空任务列表。
管理组任务	如果选中该复选框，则用户可以启动和停止在 Kaspersky Security Center 控制台中指定的组任务。用户可以在应用程序界面或简化应用程序界面中启动和停止任务。 如果清除该复选框，则 Kaspersky Endpoint Security 将自动启动计划任务，或者由管理员在 Kaspersky Security Center 控制台中手动启动任务。

配置本地应用程序设置

在 Kaspersky Security Center 中，您可以配置特定计算机上的 Kaspersky Endpoint Security 设置。这些设置是*本地应用程序设置*。某些设置可能无法进行编辑。这些设置在策略属性中被 🔒 属性锁定。

如何在管理控制台 (MMC) 中配置本地应用程序设置

1. 打开 Kaspersky Security Center Administration Console。
2. 在管理控制台树的"**受管理设备**"文件夹中，打开相关客户端计算机所属的管理组名称的文件夹。
3. 在工作区中选择"**设备**"选项卡。
4. 双击以打开计算机属性窗口。
5. 在计算机属性窗口中，选择"**应用程序**"区域。
6. 在计算机上安装的卡巴斯基应用程序列表中，选择 **Kaspersky Endpoint Security for Windows (14.1)** 并双击以打开应用程序属性。
7. 在"**常规设置**"区域中，配置 Kaspersky Endpoint Security 以及报告和存储的设置。

   应用程序属性窗口中的其余部分是 Kaspersky Security Center 的标准。《Kaspersky Security Center 帮助》提供了这些区域的说明。

   > 如果某个应用程序受到禁止更改特定设置的策略的限制，则在"**常规设置**"区域中配置应用程序设置时，您将无法编辑它们。

8. 保存更改。

如何在 Web Console 和云控制台中配置本地应用程序设置

1. 在 Web Console 的主窗口中，选择"**资产管理**" → "**资产(设备)**"。
2. 选择要为其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 Windows**”。
   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. 配置本地应用程序设置。

7. 保存更改。

本地应用程序设置与策略设置相同，但加密设置除外。

启动和停止 Kaspersky Endpoint Security

将 Kaspersky Endpoint Security 安装到用户的计算机后，该应用程序会自动启动。默认情况下，Kaspersky Endpoint Security 在操作系统启动后启动。在操作系统设置中无法配置应用程序的自动启动。

在操作系统启动后下载 Kaspersky Endpoint Security 反病毒数据库最多可能需要两分钟，具体取决于计算机的功能。在该期间计算机保护级别降低。在已启动的操作系统上启动 Kaspersky Endpoint Security 时，下载反病毒数据库不会导致计算机保护等级降低。

如何在管理控制台 (MMC) 中配置 Kaspersky Endpoint Security 的启动

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **常规设置** → **应用程序设置**。

4. 使用“**在计算机开启时启动应用程序(建议)**”复选框配置应用程序启动。

5. 保存更改。

如何在 Web Console 中配置 Kaspersky Endpoint Security 的启动

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **常规设置** → **用户交互**。

5. 使用“**在计算机启动时启动 Kaspersky Endpoint Security (建议)**”复选框配置应用程序启动。

6. 保存更改。

如何在应用程序界面中配置 Kaspersky Endpoint Security 的启动

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**应用程序设置**”。

Kaspersky Endpoint Security for Windows 设置

3. 使用“**在计算机开启时启动应用程序(建议)**”复选框配置应用程序启动。
4. 保存更改。

> Kaspersky 专家建议您不要手动停止 Kaspersky Endpoint Security，因为这样做会使计算机和您的个人数据暴露于威胁之中。如有必要，您可以根据需要暂停计算机保护而无需停止应用程序。

您可以使用“**保护状态**”小组件来监控应用程序状态。

如何在管理控制台 (MMC) 中启动或停止 Kaspersky Endpoint Security

1. 打开 Kaspersky Security Center Administration Console。
2. 在管理控制台树的“**受管理设备**”文件夹中，打开相关客户端计算机所属的管理组名称的文件夹。
3. 在工作区中选择“**设备**”选项卡。
4. 双击以打开计算机属性窗口。
5. 在计算机属性窗口中，选择“**应用程序**”区域。

6. 在计算机上安装的卡巴斯基应用程序列表中，选择 **Kaspersky Endpoint Security for Windows (14.1)** 并双击以打开应用程序属性。

7. 执行下列操作之一：

   - 要启动应用程序，请单击 Kaspersky 应用程序列表右侧的 按钮。
   - 要停止应用程序，请单击 Kaspersky 应用程序列表右侧的 按钮。

如何在 Web Console 中启动或停止 Kaspersky Endpoint Security

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**资产(设备)**”。
2. 单击您要在其上启动或停止 Kaspersky Endpoint Security 的计算机的名称。
   计算机属性窗口将打开。
3. 选择**应用程序**选项卡。
4. 选中与 **Kaspersky Endpoint Security for Windows** 对应的复选框。
5. 单击“**开始**”或“**停止**”按钮。

如何从命令行启动或停止 Kaspersky Endpoint Security

1. 以管理员身份运行命令行解释器 (cmd.exe)。
2. 转到可执行文件 klpsm.exe 所在的文件夹。
3. 要从命令行启动应用程序，请输入 `klpsm.exe start_avp_service`。
4. 要从命令行停止应用程序，请输入 `klpsm.exe stop_avp_service`。

> 要从命令行停止应用程序，请启用系统服务的外部管理。

通过命令行启动和停止应用程序

暂停和恢复计算机保护和控制

暂停计算机保护和控制意味着禁用 Kaspersky Endpoint Security 的所有保护和控制组件一段时间。

应用程序状态使用任务栏通知区域中应用程序图标进行显示。

- 图标表示计算机保护和控制已暂停。
- 图标表示计算机保护和控制已启用。

暂停或恢复计算机保护和控制不影响扫描或更新任务。

如果在暂停或恢复计算机保护和控制时已建立任何网络连接，系统会显示有关终止这些网络连接的通知。

暂停计算机保护和控制：

1. 在任务栏通知区域右键单击程序图标，调出上下文菜单中。
2. 在上下文菜单中，选择“**暂停保护**”（参见下图）。
   如果已启用密码保护，则此上下文菜单项可用。
3. 选择以下选项之一：
   - **暂停时间 <时间段>** – 经过下面的下拉列表中所指定的时间后将恢复计算机保护和控制。
   - **暂停至应用程序重启** – 重启应用程序或重启操作系统后将恢复计算机保护和控制。必须启用应用程序的自动启动才能使用该选项。
   - **暂停** – 在您决定重新启用时将恢复计算机保护和控制。
4. 单击“**暂停保护**”。

Kaspersky Endpoint Security 将暂停策略中不带锁标记 () 的所有保护和控制组件的运行。在执行此操作之前，建议禁用 Kaspersky Security Center 策略。

应用程序图标上下文菜单

恢复计算机保护和控制：

1. 在任务栏通知区域右键单击程序图标，调出上下文菜单中。
2. 在上下文菜单中，选择“**恢复保护**”。

如果您决定恢复计算机保护和控制，可以随时进行该操作，这与您之前选择的保护和控制暂停选项无关。

创建和使用配置文件

带有 Kaspersky Endpoint Security 设置的配置文件允许您完成以下任务：

- 通过命令行使用预定义的设置本地安装 Kaspersky Endpoint Security。
- 通过 Kaspersky Security Center 使用预定义的设置远程安装 Kaspersky Endpoint Security。
- 将应用程序设置转移到策略。
- 从一台计算机上将 Kaspersky Endpoint Security 设置迁移至其他计算机上（参见以下说明）。

导出配置文件

要创建配置文件，请执行以下操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**管理设置**”。
3. 单击“**导出**”。
4. 在打开的窗口中，指定您要保存配置文件的路径并输入其名称。

   若要使用配置文件本地或远程安装 Kaspersky Endpoint Security，您必须将其命名为 install.cfg。

5. 如有必要，请输入将应用程序配置导出到文件的密码。
   要保存配置文件，必须启用密码保护。用户必须具有“**导出设置**”权限。
6. 保存文件。

因此，应用程序会创建一个配置文件。配置文件可能包含用户账户详细信息，因此 Kaspersky Endpoint Security 会对该文件进行加密。您无法编辑配置文件。任何修改配置文件的尝试都会导致文件损坏。

导入配置文件

配置文件可能包含添加到应用程序中的用户账户的详细信息。如果您在创建该文件的同一台计算机上导入该文件，Kaspersky Endpoint Security 会导入用户账户的密码。如果您在另一台计算机上导入文件，则需要手动输入密码。

导入配置文件时，Kaspersky Endpoint Security 不会传输加密容器密码。如果在连接服务器时使用双向身份验证，则需要从头开始指定加密容器密码。

若要从配置文件导入 Kaspersky Endpoint Security 设置：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**管理设置**”。
3. 单击“**导入**”。
4. 在打开的窗口中，输入配置文件的路径。
5. 打开文件。

Kaspersky Endpoint Security 设置的所有值都将根据选定配置文件进行设置。

管理应用程序设置

恢复应用程序默认设置

您可以随时恢复卡巴斯基建议的应用程序设置。在设置被恢复后，应用程序将为所有保护组件设置“**建议**”安全级别。

要恢复应用程序默认设置：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**管理设置**”。
3. 单击“**恢复**”。
4. 保存更改。

管理应用程序设置

Kaspersky Endpoint Security 的性能以及与其他应用程序的兼容性

Kaspersky Endpoint Security 的性能是指它能够检测出的会对计算机造成损坏的威胁类型的数量，以及耗电量和计算机资源使用情况。

选择可检测对象的类型

Kaspersky Endpoint Security 将让您精调计算机保护并选择运行期间应用程序检测的对象类型。Kaspersky Endpoint Security 将始终扫描操作系统中的病毒、蠕虫和木马。您不能禁用对这些对象类型的扫描。此类恶意软件可能会给计算机带来巨大的损害。为了更好地保护您的计算机，您可以扩大可检测的对象类型范围，以便监控那些可能会被入侵者用来损害计算机或隐私数据的应用程序。

使用节能模式

对于便携式计算机来说，应用程序的电量消耗是一个关键的考虑因素。Kaspersky Endpoint Security 的计划任务通常会消耗大量的资源。当计算机使用电池运行时，您可以使用节能模式，更加节省电量。

在节能模式下，以下计划任务将自动延迟：

- 全盘扫描任务；
- 关键区域扫描任务；
- 自定义扫描任务；
- 完整性检查任务。

无论是否启用了节能模式，Kaspersky Endpoint Security 将在便携式电脑将在电池供电时暂停加密任务。便携式电脑从电池供电切换为电源供电时，程序将恢复加密任务。

允许其他应用程序使用计算机资源

扫描计算机时对计算机资源的消耗可能会增加 CPU 和硬盘驱动器子系统的负载。为了解决在 CPU 和硬盘驱动器子系统上的负载增加的条件下发生的同步操作的问题，Kaspersky Endpoint Security 可以将资源让给其他应用程序。

使用高级清除技术

如今的恶意应用程序能够侵入操作系统的最底层，从而无法清除。在操作系统中检测到恶意活动之后，Kaspersky Endpoint Security 将使用特殊的高级清除技术执行广泛的清除步骤。*高级清除技术*致力于清除 RAM 中已启动进程，以及阻止 Kaspersky Endpoint Security 使用其他方式移除它们的恶意应用程序。结果就是威胁被消除。执行高级杀毒时，我们建议您不要开启新的进程或者编辑操作系统注册表。高级清除技术会占用相当多的操作系统资源，这可能会降低其他应用程序的运行速度。

在运行 Microsoft Windows for workstations 的计算机上运行完高级杀毒过程后，Kaspersky Endpoint Security 将请求用户许可，重新启动计算机。系统重启后，Kaspersky Endpoint Security 将删除恶意软件文件并启动“快速”计算机全盘扫描。

由于 Kaspersky Endpoint Security 的特性，在运行 Microsoft Windows for servers 的计算机上无法提示重启。文件服务器的非计划重启将会导致文件服务器数据暂时不可用或未保存文件丢失等问题出现。建议您严格按照计划重启文件服务器。这就是为什么默认情况下文件服务器禁用高级清除技术的原因。

如果检测到文件服务器上有活动感染，系统将向 Kaspersky Security Center 发送一个事件，告知需要进行高级清除。要清除服务器的活动感染，请对服务器启用高级清除技术，并在服务器用户方便的时间启动"*恶意软件扫描*"组任务。

启用或禁用节能模式

*节能模式*功能可以减轻笔记本电脑的资源负担，延长待机时间，而不会显著降低安全级别。在节能模式下，应用程序会限制计划任务的启动。这样一来，节能模式就能确保笔记本电脑的安全级别和待机时间之间的平衡。

启用节能模式且计算机使用电池运行时，即使计划了以下任务，以下任务也不会运行：

- "*全盘扫描*"。
- "*关键区域扫描*"。
- "*自定义扫描*"。
- "*应用程序完整性检查*"。
- "*IOC 扫描*"。
- *数据库和应用程序模块更新*（仅限补丁）

> 只有当笔记本电脑使用电池供电且电池电量低于 30% 时，应用程序才会跳过计划的数据库更新。在其他所有情况下，无论笔记本电脑是连接电源还是使用电池供电，也无论应用程序是否处于节能模式，Kaspersky Endpoint Security软件都会按计划更新数据库。

如何在管理控制台(MMC)中启用或禁用节能模式

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择"**策略**"。
3. 选择必要的策略并双击以打开策略属性。
4. 在策略窗口中，选择 **常规设置** → **应用程序设置**。
5. 在"**性能**"块，使用"**使用电池供电时推迟计划任务**"复选框以启用或禁用节电模式。
6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 中启用或禁用节能模式

1. 在 Web Console 的主窗口中，选择"**资产管理**" → "**策略**"选项卡。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **常规设置** → **性能**。

5. 在“**使用电池供电时推迟或跳过计划任务**”块，使用“**使用电池供电时推迟或跳过计划任务(取决于操作系统)**”复选框以启用或禁用节电模式。

6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在应用程序界面中启用或禁用节能模式

1. 打开主应用程序窗口并单击 按钮。

2. 在应用程序设置窗口中，选择“**常规设置**” → “**应用程序设置**”。

Kaspersky Endpoint Security for Windows 设置

3. 在“**性能**”块，使用“**使用电池供电时推迟计划任务**”复选框以启用或禁用节电模式。

4. 保存更改。

启用或禁用允许其他应用程序使用资源

Kaspersky Endpoint Security 在扫描计算机时消耗计算机资源可能会增加 CPU 和硬盘驱动器子系统的负载。这可能会减慢其他应用程序的速度。为了优化性能，Kaspersky Endpoint Security 提供了*一种将资源传输到其他应用程序的模式*。在这种模式下，当 CPU 负载高时，操作系统可以降低 Kaspersky Endpoint Security 扫描任务线程的优先级。这允许将操作系统资源重新分配给其他应用程序。因此，扫描任务将获得更少的 CPU 时间。因此，Kaspersky Endpoint Security 将需要更长的时间来扫描计算机。默认情况下，程序已配置为允许其他应用程序使用资源。

如何在管理控制台（MMC）中启用或禁用为其他应用程序让出资源

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **应用程序设置**。
4. 在“**性能**”块，使用**为其他应用程序让出资源**复选框启用或禁用对其他应用程序的资源出让。
5. 保存更改。

如何在 Web Console 和云控制台中启用或禁用为其他应用程序让出资源

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **性能**。
5. 在“**为其他应用程序让出资源**”块，使用“**为其他应用程序让出资源**”切换开关以启用或禁用对其他应用程序的资源出让。
6. 保存更改。

如何在应用程序界面中启用或禁用为其他应用程序让出资源

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**应用程序设置**”。

Kaspersky Endpoint Security for Windows 设置

3. 在“**性能**”块，使用**为其他应用程序让出资源**复选框启用或禁用对其他应用程序的资源出让。
4. 保存更改。

优化 Kaspersky Endpoint Security 性能的最佳实践

当部署 Kaspersky Endpoint Security for Windows 时，您可以使用以下建议来配置计算机保护和优化性能。有关处理计算机性能问题的更多信息，请参阅技术支持知识库。

常规

根据以下建议配置应用程序的常规设置：

1. 将 Kaspersky Endpoint Security 升级至最新版本。
   较新版本的应用程序修复了错误，提高了稳定性，并优化了性能。

2. 使用默认设置启用保护组件。

   默认设置被认为是最佳的。此设置由 Kaspersky 专家推荐。默认设置提供建议的保护级别和最佳资源使用。如有必要，您可以恢复默认应用程序设置。

3. 启用应用程序性能优化功能。

   该应用程序具有性能优化特性：节能模式和为其他应用程序让出资源。确保这些选项已启用。

工作站上的恶意软件扫描

建议对工作站进行恶意软件扫描时启用后台扫描。“*后台扫描*”是 Kaspersky Endpoint Security 的一种扫描模式，不会向用户显示通知。后台扫描比其他类型的扫描（如全盘扫描）需要更少的计算机资源。在此模式下，Kaspersky Endpoint Security 扫描启动对象、引导扇区、内核内存和系统分区。后台扫描设置被认为是最佳的。此设置由 Kaspersky 专家推荐。因此，要对计算机执行恶意软件扫描，您可以只使用后台扫描模式，而不使用其他扫描任务。

如果后台扫描不适合您的需要，请按照以下建议配置*恶意软件扫描*任务：

1. 设置扫描计算机时 CPU 资源消耗的限制。

   您可以限制运行“*恶意软件扫描*”任务时的 CPU 使用率。为此，在应用程序设置中，指定扫描计算机时可利用的所有内核的最大 CPU 负载百分比。这可能会增加扫描计算机所需的时间。

2. 配置最佳计算机扫描计划。

   您可以将任务配置为在计算机以最小负载运行时运行。例如，您可以将任务配置为在夜间或周末运行。

   如果用户在工作时间之外关闭计算机，您可以启用网络唤醒功能。“Wake-on-LAN”功能允许通过本地网络发送特殊信号远程启动计算机。要使用此功能，必须在 BIOS 设置中启用“Wake-on-LAN”。您还可以在扫描完成后自动关闭计算机。

   如果您无法配置最佳扫描计划，请将任务设置为仅在计算机空闲时运行。如果计算机被锁定或屏幕保护开启，Kaspersky Endpoint Security 启动扫描任务。如果您中断了任务的执行，例如通过解锁计算机，Kaspersky Endpoint Security 将自动运行该任务，并从中断点继续运行。

3. 定义扫描范围。

   选择以下对象进行扫描（最小扫描范围）：

   - 内核内存
   - 正在运行的进程和启动对象
   - 引导扇区
   - %systemroot%（不包括子文件夹）
   - %systemroot%\System（不包括子文件夹）
   - %systemroot%\System32（不包括子文件夹）
   - %systemroot%\System32\drivers（不包括子文件夹）
   - %systemroot%\SysWOW64（不包括子文件夹）
   - %systemroot%\SysWOW64\drivers（不包括子文件夹）

4. 启用 iSwift 和 iChecker 技术。

   - iSwift 技术。

     该技术允许通过排除特定文件不扫描的方式提高扫描速度。该技术将使用特殊算法将文件排除在扫描范围之外，该算法会考虑 Kaspersky Endpoint Security 数据库的发布日期、文件的上次扫描日期以及对扫描设置的任何修改。iSwift 技术是对用于 NTFS 文件系统的 iChecker 技术的增强版。

   - iChecker 技术。

     该技术允许通过排除特定文件不扫描的方式提高扫描速度。该技术将使用特殊算法将文件排除在扫描范围之外，该算法会考虑 Kaspersky Endpoint Security 数据库的发布日期、文件的上次扫描日期以及对扫描设置的任何修改。iChecker 技术受到一些限制：它无法操作大型文件，并且仅能应用于具有应用程序可识别结构的文件（例如：EXE、DLL、LNK、TTF、INF、SYS、COM、CHM、ZIP 和 RAR）。

   > 您只能在管理控制台（MMC）和 Kaspersky Endpoint Security 界面中启用 iSwift 和 iChecker 技术。您无法在 Kaspersky Security Center Web Console 中启用这些技术。

5. 禁用对密码保护存档的扫描。

   如果启用了对密码保护存档的扫描，则在扫描存档之前会显示密码提示。由于建议在非工作时间安排任务，因此用户无法输入密码。您可以手动扫描受密码保护的压缩包。

6. 禁止同时启动多个扫描任务。

   如果当前扫描继续，Kaspersky Endpoint Security 将使新的扫描任务排队。这有助于优化计算机上的负载。

服务器上的恶意软件扫描

根据以下建议配置*恶意软件扫描*任务：

1. 设置扫描计算机时 CPU 资源消耗的限制。

   您可以限制运行“*恶意软件扫描*”任务时的 CPU 使用率。为此，在应用程序设置中，指定扫描计算机时可利用的所有内核的最大 CPU 负载百分比。这可能会增加扫描计算机所需的时间。

2. 配置最佳计算机扫描计划。

   您可以将任务配置为在计算机以最小负载运行时运行。例如，您可以将任务配置为在夜间或周末运行。

3. 启用 iSwift 和 iChecker 技术。

   - iSwift 技术。

     该技术允许通过排除特定文件不扫描的方式提高扫描速度。该技术将使用特殊算法将文件排除在扫描范围之外，该算法会考虑 Kaspersky Endpoint Security 数据库的发布日期、文件的上次扫描日期以及对扫描设置的任何修改。iSwift 技术是对用于 NTFS 文件系统的 iChecker 技术的增强版。

   - iChecker 技术。

     该技术允许通过排除特定文件不扫描的方式提高扫描速度。该技术将使用特殊算法将文件排除在扫描范围之外，该算法会考虑 Kaspersky Endpoint Security 数据库的发布日期、文件的上次扫描日期以及对扫描设置的任何修改。iChecker 技术受到一些限制：它无法操作大型文件，并且仅能应用于具有应用程序可识别结构的文件（例如：EXE、DLL、LNK、TTF、INF、SYS、COM、CHM、ZIP 和 RAR）。

您只能在管理控制台（MMC）和 Kaspersky Endpoint Security 界面中启用 iSwift 和 iChecker 技术。您无法在 Kaspersky Security Center Web Console 中启用这些技术。

4. 禁用对密码保护存档的扫描。

   如果启用了对密码保护存档的扫描，则在扫描存档之前会显示密码提示。由于建议在非工作时间安排任务，因此用户无法输入密码。您可以手动扫描受密码保护的压缩包。

5. 禁止同时启动多个扫描任务。

   如果当前扫描继续，Kaspersky Endpoint Security 将使新的扫描任务排队。这有助于优化计算机上的负载。

卡巴斯基安全网络

为了更有效地保护您的计算机，Kaspersky Endpoint Security 使用从全球用户处接收的数据。卡巴斯基安全网络设计用于收集此数据。

卡巴斯基安全网络 (KSN) 是一个云服务的基础架构。它可以访问在线卡巴斯基知识库。该知识库中包含了文件信誉、网页资源和软件的相关信息。使用卡巴斯基安全网络的数据可确保 Kaspersky Endpoint Security 能够更快地对新威胁作出响应，提高一些保护组件的性能，并减少误报风险。如果您正在参与卡巴斯基安全网络，KSN 服务为 Kaspersky Endpoint Security 提供有关已扫描网址的信誉的信息，以及有关已扫描文件的类别和信誉的信息。

根据以下建议编辑卡巴斯基安全网络设置：

1. 禁用扩展 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。

2. 配置卡巴斯基私有安全网络。

   *卡巴斯基私有安全网络*是让运行 Kaspersky Endpoint Security 或其他卡巴斯基应用程序的计算机的用户获得卡巴斯基信誉数据库以及其他统计数据的访问权限的解决方案，无需从他们自己的计算机向卡巴斯基发送数据。

3. 启用云模式。

   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。

恶意软件扫描

恶意软件扫描对于计算机安全至关重要。定期进行恶意软件扫描有助于防止因安全级别设置过低或者其他原因导致保护组件未能检测到的恶意软件进行传播。

Kaspersky Endpoint Security 不会扫描其内容位于 OneDrive 云存储中的文件，但会创建日志条目来说明尚未扫描这些文件。

全盘扫描

彻底地扫描整个计算机。Kaspersky Endpoint Security 扫描以下对象：

- 内核内存
- 操作系统启动时加载的对象
- 引导扇区
- 操作系统备份
- 所有硬盘和可移动驱动器

卡巴斯基专家建议不要更改"*全盘扫描*"任务的扫描范围。

为节省计算机资源，建议使用后台扫描任务而不是全盘扫描任务。这不会影响计算机的安全级别。

关键区域扫描

默认情况下, Kaspersky Endpoint Security 会扫描内核内存、运行进程和磁盘的引导扇区。

卡巴斯基专家建议不要更改"*关键区域扫描*"任务的扫描范围。

自定义扫描

Kaspersky Endpoint Security 将扫描用户选择的对象。您可以扫描下表中的任意对象：

- 系统内存
- 操作系统启动时加载的对象
- 操作系统备份
- 硬盘、可移动和网络驱动器
- 任何选定的文件

后台扫描

"*后台扫描*"是 Kaspersky Endpoint Security 的一种扫描模式，不会向用户显示通知。后台扫描比其他类型的扫描（如全盘扫描）需要更少的计算机资源。在此模式下，Kaspersky Endpoint Security 扫描启动对象、引导扇区、内核内存和系统分区。

应用程序完整性检查

Kaspersky Endpoint Security 将检查程序的模块是否损坏或者被修改，

扫描计算机

扫描对于计算机安全至关重要。定期进行恶意软件扫描有助于防止因安全级别设置过低或者其他原因导致保护组件未能检测到的恶意软件进行传播。该组件借助反病毒数据库、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。

Kaspersky Endpoint Security 预定义了以下标准任务： *全盘扫描*、*关键区域扫描*、*自定义扫描*。如果您的组织部署了 Kaspersky Security Center 管理系统，您可以创建一个*恶意软件扫描*任务并配置扫描。

如何在管理控制台 (MMC) 中创建扫描任务

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择"**任务**"。
3. 选择扫描任务并双击以打开任务属性。
   如果必要，请创建"*恶意软件扫描*"任务。
4. 在任务属性窗口中，选择"**设置**"区域。

5. 配置扫描任务（参见下表）。

   如果必要，配置扫描任务计划。

6. 保存更改。

7. 运行扫描任务。

Kaspersky Endpoint Security 将开始扫描计算机。如果用户中断了任务的执行，例如通过关闭计算机，Kaspersky Endpoint Security 将自动运行该任务，并从中断点继续运行。

如何在 Web Console 和云控制台中运行扫描任务

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

   任务列表打开。

2. 单击扫描任务。

   任务属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 配置扫描任务（参见下表）。

   如果必要，配置扫描任务计划。

5. 保存更改。

6. 运行扫描任务。

Kaspersky Endpoint Security 将开始扫描计算机。如果用户中断了任务的执行，例如通过关闭计算机，Kaspersky Endpoint Security 将自动运行该任务，并从中断点继续运行。

如何在应用程序界面中运行扫描任务

1. 在应用程序主窗口中，转到“**任务**”区域。

2. 在任务列表中，选择扫描任务并单击 ⚙ 按钮。

3. 配置扫描任务（参见下表）。

   如果必要，配置扫描任务计划。

4. 保存更改。

5. 运行扫描任务。

Kaspersky Endpoint Security 将开始扫描计算机。应用程序将显示扫描进度，扫描过的对象以及剩余扫描时间。您可以通过单击**停止**按钮随时停止任务。如果扫描任务未显示，这意味着管理员已禁止在策略中使用本地任务。

为了优化 Kaspersky Endpoint Security 在扫描计算机时的性能，您可以管理*全盘扫描*任务的高级设置，并限制 CPU 资源的使用。

在 Kaspersky Security Center 中，您还可以使用*后台扫描*任务而不是*全盘扫描*任务优化应用程序的性能。这不会影响计算机的安全级别。后台扫描无法被配置。

因此，Kaspersky Endpoint Security 扫描计算机，如果检测到威胁，则执行应用程序设置中配置的操作。通常，应用程序会尝试对受感染的文件进行清除。因此，受感染的文件可能会收到以下状态：

- "**已延期**"。无法对感染的文件进行清除。应用程序在计算机重新启动后删除受感染的文件。
- "**已记录**"。无法对感染的文件进行清除。该应用程序将有关检测到的受感染文件的信息添加到活动威胁列表中。
- **不支持写入**或**写入错误**。无法对感染的文件进行清除。应用程序没有写入权限。
- "**已处理**"。该应用程序之前检测到受感染的文件。应用程序在计算机重新启动后清除或删除受感染的文件。

扫描设置

参数	描述
安全级别	Kaspersky Endpoint Security 可以使用不同的设置组运行扫描。存储在应用程序中的设置组叫做*安全级别*： • "**高**"。Kaspersky Endpoint Security 扫描所有类型的文件。扫描复合文件时，应用程序会扫描存档、分发包、Office 格式的文件，但不会扫描受密码保护的存档。当设置此安全级别时，应用程序将使用**深度扫描**详细级别的启发式分析。 • "**建议**"。Kaspersky Endpoint Security 扫描所有类型的文件。扫描复合文件时，应用程序会扫描存档、分发包、Office 格式的文件，但不会扫描受密码保护的存档。当设置此安全级别时，应用程序将使用**中度扫描**详细级别的启发式分析。 • "**低**"。Kaspersky Endpoint Security 仅扫描指定的文件格式。扫描复合文件时，应用程序会扫描存档、分发包、Office 格式的文件，但不会扫描受密码保护的存档。当设置此安全级别时，应用程序将使用**轻度扫描**详细级别的启发式分析。 您可以选择某种预设的安全级别或手动配置安全性级别的设置。如果您改变了文件安全级别设置，仍可随时恢复到推荐的文件安全级别设置。
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。 "**清除；如果清除失败则通知**"。如果选择该选项，Kaspersky Endpoint Security 将自动尝试对已经检测到的所有受感染的文件执行清除操作。如果清除失败，Kaspersky Endpoint Security 会将检测到的受感染文件的相关信息添加到活动威胁列表。 "**通知**"。如果选择此选项，Kaspersky Endpoint Security 会在检测到受感染文件时将这些文件的相关信息添加到活动威胁列表。 在对感染的文件进行清除或删除操作之前，应用程序会创建一个备份，以免日后会需要恢复该文件或对该文件进行清除。 在检测到属于 Windows Store 应用程序一部分的受感染文件时，Kaspersky Endpoint Security 将尝试删除文件。
立即运行高级清除 *（仅在 Kaspersky Security Center 控制台可用）*	仅当在应用于计算机的策略的属性中启用"高级清除"功能后，才会在该计算机上运行病毒扫描任务期间执行高级清除。 如果选中该复选框，则在执行病毒扫描任务期间检测到活动感染后，Kaspersky Endpoint Security 会立即对其进行清除。在活动感染被清除后，Kaspersky Endpoint Security 会在不提示用户的情况下重启计算机。 如果清空该复选框，则在执行病毒扫描任务期间检测到活动感染后，Kaspersky Endpoint Security 不对其进行清除。Kaspersky Endpoint Security 在本地应用程序报告中和 Kaspersky Security Center 端生成活动感染事件。在启用高级清除功能的情况下再次运行病毒扫描任务时，可以对活动感染进行清除。这样，系统管理员可以选择适当的时间进行高级清除，然后自动重启计算机。
扫描范围	Kaspersky Endpoint Security 在运行扫描任务时扫描的对象列表。扫描范围内的对象可以包括内核内存、运行的进程、启动扇区、系统备份存储、硬盘驱动器、可移动驱动器或网络驱动器、文件夹或文件。 在 Kaspersky Endpoint Security for Windows 12.12 中，电子邮件被排除在应用程序扫描范围之外。对传入和传出电子邮件的扫描由邮件威胁防护组件执行。如果您使用的是较早版本的管理插件，即使策略中包含电子邮件，该应用程序也会将电子邮件排除在扫描范围之外。

参数	描述
扫描计划	"**手动**"。您可以在方便时手动启动扫描的运行模式。 "**根据计划**"。在该扫描任务运行模式下，应用程序将按照您创建的计划启动扫描任务。如果选择该扫描任务运行模式，您也可以手动启动扫描任务。
在应用程序启动此时间后延迟运行 N 分钟	应用程序启动后已推迟扫描任务的启动。在操作系统启动时，许多进程正在运行，因此推迟运行扫描任务而不是在 Kaspersky Endpoint Security 启动后立即运行扫描任务是有利的。
运行略过的任务	如果选中该复选框，Kaspersky Endpoint Security 将在可能的情况下尽快启动已忽略的任务。任务在某些情况下可能被略过，例如，计算机在启动计划任务时处于关闭状态。当应用程序有机会执行略过的任务时，它会在一定的时间间隔内随机运行任务，以分配计算机上的负载。 如果清除该复选框，Kaspersky Endpoint Security 不会运行已略过的任务。它将按照当前计划运行下一次任务。
仅在计算机空闲时运行	计算机资源忙时推迟任务启动。如果计算机被锁定或屏幕保护开启，Kaspersky Endpoint Security 启动扫描任务。如果您中断了任务的执行，例如通过解锁计算机，Kaspersky Endpoint Security 将自动运行该任务，并从中断点继续运行。此计划选项允许您在使用计算机时节省计算机资源。
运行扫描身份	默认下，扫描任务以您使用其权限在操作系统中注册的用户的名称运行。保护范围可能包含需要特殊权限才能访问的网络驱动器或其他对象。您可以在应用程序设置中指定拥有所需权限的用户，然后在该用户账户下运行扫描任务。
文件类型	Kaspersky Endpoint Security 将没有扩展名的文件视为可执行文件。应用程序总是扫描可执行文件，而与所选的要扫描的文件类型无关。 "**所有文件**"。如果启用该设置，Kaspersky Endpoint Security 将毫无例外地扫描所有文件（所有格式和扩展名）。 "**按格式扫描文件**"。如果启用该设置，则应用程序仅扫描被感染的文件。在扫描文件以查找恶意代码之前，系统将分析文件的内部头以确定文件的格式（例如，.txt、.doc 或 .exe）。该扫描也查找具有特殊文件扩展名的文件。 "**按扩展名扫描文件**"。如果启用该设置，则应用程序仅扫描被感染的文件。此时，系统将根据文件的扩展名确定文件格式。 默认情况下，Kaspersky Endpoint Security 按格式扫描文件。按扩展名扫描文件不太安全，因为恶意文件的扩展名可能不在潜在可感染列表中（例如，`.123`）。
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。
跳过扫描时间超过以下值的文件 N 秒	限制任务执行时间。超出指定时间后，Kaspersky Endpoint Security 将停止任务。任务未标记为已完成。下次 Kaspersky Endpoint Security 运行该任务时，它将按计划从头开始运行。
不同时运行多个扫描任务	如果扫描已在运行，则推迟启动扫描任务。如果当前扫描继续，Kaspersky Endpoint Security 将使新的扫描任务排队。这有助于优化计算机上的负载。例如，假设应用程序已根据计划启动了全盘扫描任务。如果有用户试图从应用程序界面启动快速扫描，Kaspersky Endpoint Security 会将此快速扫描任务排队，然后在完成全盘磁盘扫描任务后自动启动此任务。 然而，即使正在运行以下扫描任务之一，Kaspersky Endpoint Security 也会立即启动扫描任务： • 连接时扫描可移动驱动器。 • 从上下文菜单扫描。 • 在检测到妥协的指标（IoC）时开始的关键区域扫描。 如果清除此复选框，则 Kaspersky Endpoint Security 允许您同时运行多个扫描任务。运行多个扫描任务需要更多的计算机资源。
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	扫描第三方应用程序的分发包。
扫描 Microsoft Office 格式文件	扫描 Microsoft Office 文件（DOC、DOCX、XLS、PPT 和其他 Microsoft 扩展程序）。Office 格式文件也包括 OLE 对象。应用程序扫描小于 1 MB 的 office 格式文件，无论该复选框是否被选中。

参数	描述
扫描电子邮件格式文件	扫描电子邮件格式文件和电子邮件数据库。该应用程序扫描 MS Outlook 和 Windows Mail 邮件客户端使用的 PST 和 OST 文件以及 EML 文件。 Kaspersky Endpoint Security 不支持 64 位版本的 Microsoft Outlook 邮件客户端。这意味着，如果计算机上安装了 64 位版本的 Microsoft Outlook，即使邮件包含在扫描范围内，Kaspersky Endpoint Security 也不会扫描 Microsoft Outlook 文件（PST 和 OST 文件）。 如果选择该选框，Kaspersky Endpoint Security 将把邮件格式文件的各个部分分解（标题、正文、附件）后扫描威胁。 如果清空该选框，Kaspersky Endpoint Security 将把邮件格式的文件作为一个单独的文件扫描。 当在 PST 或 OST 文件中发现恶意对象时，Kaspersky Endpoint Security 会根据所选操作（例如，对文件清除或删除）使其无害。 当在其他邮件客户端（例如 Mozilla Thunderbird）的文件中检测到恶意文件时，Kaspersky Endpoint Security 只会标记受感染的邮件。您需要手动删除带有已感染附件的邮件。
扫描受密码保护的存档	如果选择该选框，应用程序将扫描密码保护的存档。在扫描存档中的文件前，系统将提示您输入密码。 如果清空该选框，应用程序将跳过扫描密码保护的存档。
复合文件大于指定值时不解压	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。
机器学习和特征码分析	机器学习和签名分析方法使用 Kaspersky Endpoint Security 数据库，其中包含已知威胁的描述以及消除它们的方法。使用此方法的保护提供了可接受的最低安全级别。 根据 Kaspersky 专家的推荐，机器学习和签名分析始终启用。
启发式分析	开发该技术的目的是检测使用当前版本的卡巴斯基应用程序数据库无法检测到的威胁。它可以检测可能受未知病毒或已知病毒新变种感染的文件。 当扫描文件以查找恶意代码时，启发式分析执行可执行文件中的指令。启发式分析执行的指令数量取决于启发式分析级别。启发式分析级别可在全面搜索新威胁、加载操作系统资源和启发式分析持续时间之间进行平衡。
iSwift 技术 *（仅在管理控制台（MMC）和 Kaspersky Endpoint Security 界面可用）*	该技术允许通过排除特定文件不扫描的方式提高扫描速度。该技术将使用特殊算法将文件排除在扫描范围之外，该算法会考虑 Kaspersky Endpoint Security 数据库的发布日期、文件的上次扫描日期以及对扫描设置的任何修改。iSwift 技术是对用于 NTFS 文件系统的 iChecker 技术的增强版。
iChecker 技术 *（仅在管理控制台（MMC）和 Kaspersky Endpoint Security 界面可用）*	该技术允许通过排除特定文件不扫描的方式提高扫描速度。该技术将使用特殊算法将文件排除在扫描范围之外，该算法会考虑 Kaspersky Endpoint Security 数据库的发布日期、文件的上次扫描日期以及对扫描设置的任何修改。iChecker 技术受到一些限制：它无法操作大型文件，并且仅能应用于具有应用程序可识别结构的文件（例如：EXE、DLL、LNK、TTF、INF、SYS、COM、CHM、ZIP 和 RAR）。

扫描连接到计算机的可移动驱动器

Kaspersky Endpoint Security 扫描您运行或复制的所有文件，即使该文件位于可移动驱动器（文件威胁保护组件）上。为了防止病毒和其他恶意软件的传播，您可以配置可移动驱动器连接到计算机时的自动扫描。Kaspersky Endpoint Security 将自动尝试对已经检测到的所有受感染的文件执行清除操作。如果清除失败，Kaspersky Endpoint Security 将删除文件。该组件通过运行实现了机器学习、启发式分析（高级别）和特征码分析的扫描来保证计算机的安全。Kaspersky Endpoint Security 还使用 iSwift 和 iChecker 扫描优化技术。该技术总是启用且无法被禁用。

如何在管理控制台 (MMC) 中配置运行可移动驱动器扫描

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **本地任务** → **可移动驱动器扫描**。

4. 在**连接可移动驱动器时的操作**下拉列表中，选择**详细扫描**或**快速扫描**。

5. 为可移动驱动器扫描配置高级选项（参见下表）。

6. 保存更改。

如何在 Web Console 和云控制台中配置可移动驱动器扫描的运行

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **主机威胁防护** → **可移动驱动器扫描**。

5. 使用**可移动驱动器扫描已启用**开关启用或禁用组件。

6. 在“**扫描类型**”块中，选择“**详细扫描**”或“**快速扫描**”。

7. 为可移动驱动器扫描配置高级选项（参见下表）。

8. 保存更改。

如何在应用程序界面中配置运行可移动驱动器扫描

1. 在应用程序主窗口中，转到“**任务**”区域。

2. 在任务列表中，选择扫描任务并单击 ⚙ 按钮。

3. 使用**可移动驱动器扫描**开关以启用或禁用在可移动驱动器连接到计算机时对其进行扫描。

4. 为可移动驱动器扫描配置高级选项（参见下表）。

5. 保存更改。

因此，Kaspersky Endpoint Security 会对不大于指定最大大小的可移动驱动器运行可移动驱动器扫描。如果“*可移动驱动器扫描*”任务未显示，这意味着管理员已在策略中禁止对本地任务的使用。

“可移动驱动器扫描”任务设置

参数	描述
扫描类型	“**详细扫描**”。如果选择此选项，Kaspersky Endpoint Security 将在连接可移动驱动器时扫描所有文件，包括嵌套在复合对象、存档、分发包和 Office 格式文件中的文件。Kaspersky Endpoint Security 不扫描邮件格式的文件或受密码保护的存档文件。 “**快速扫描**”。如果选择此选项，Kaspersky Endpoint Security 将在连接可移动驱动器后只扫描最容易被感染的特定格式的文件，并且不会解压缩复合对象。
最大驱动器大小 (MB)	如果选中该复选框，Kaspersky Endpoint Security 对于大小不超过指定最大驱动器大小的可移动驱动器，执行所选操作。如果可移动驱动器的大小超出配置的值，Kaspersky Endpoint Security 将跳过扫描。 如果清除该复选框，Kaspersky Endpoint Security 将对任意大小的可移动驱动器执行选定的操作。
隐藏扫描进度条	如果选中该复选框，Kaspersky Endpoint Security 将在单独的窗口和“**任务**”区域中显示可移动驱动器扫描进度。 如果清除该复选框，Kaspersky Endpoint Security 将在后台启动可移动驱动器扫描。
阻止用户停止扫描	如果选中了该复选框，则对于 Kaspersky Endpoint Security 本地界面中的可移动驱动器扫描任务，“**任务**”区域的“**停止**”按钮和“可移动驱动器扫描”窗口中的“**停止**”按钮不可用。

后台扫描

"*后台扫描*"是 Kaspersky Endpoint Security 的一种扫描模式，不会向用户显示通知。后台扫描比其他类型的扫描（如全盘扫描）需要更少的计算机资源。在此模式下，Kaspersky Endpoint Security 扫描启动对象、引导扇区、内核内存和系统分区。

为节省计算机资源，建议使用后台扫描任务而不是全盘扫描任务。这不会影响计算机的安全级别。这些任务具有相同的扫描范围。要优化计算机上的负载，应用程序不会同时运行全盘扫描任务和后台扫描任务。如果您已经运行了全盘扫描任务，Kaspersky Endpoint Security 在全盘扫描任务完成后的七天内不会启动后台扫描任务。

在以下情况下，启动后台扫描：

- 反病毒数据库更新后。
- Kaspersky Endpoint Security 启动 30 分钟后。
- 每六个小时一次。
- 当计算机空闲超过 5 分钟时（计算机被锁定或屏保开启）。

当满足以下任一条件时，计算机空闲时进行的后台扫描会中断：

- 计算机进入活动模式。

  > 如果后台扫描超过十天未运行，则扫描不会中断。

- 计算机（笔记本电脑）切换到电池模式。

> 执行后台扫描时，Kaspersky Endpoint Security 不扫描其内容位于 OneDrive 云存储中的文件。

如何在管理控制台 (MMC) 中启用后台扫描

1. 在 Kaspersky Security Center 管理控制台树中，选择"**策略**"。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **本地任务** → **后台扫描**。
4. 使用**启用后台扫描**开关启用或禁用后台扫描。
5. 保存更改。

如何在 Web Console 和云控制台中启用后台扫描

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

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. 在“**后台扫描**”下，使用“**后台扫描已启用**”切换开关启用或禁用后台扫描。

6. 保存更改。

如何在应用程序界面中启用后台扫描

1. 在应用程序主窗口中，转到“**任务**”区域。

2. 在任务列表中，选择扫描任务并单击 ⚙ 按钮。

3. 使用**后台扫描**开关启用或禁用背景扫描。

4. 保存更改。

如果*后台扫描*任务未显示，这意味着管理员已禁止在策略中使用本地任务。

从上下文菜单扫描

Kaspersky Endpoint Security 允许您从上下文菜单运行单个文件扫描来查找病毒和其他恶意软件（请参见下图）。

从上下文菜单执行扫描时，Kaspersky Endpoint Security 不扫描其内容位于 OneDrive 云存储中的文件。

从上下文菜单扫描

如何从管理控制台(MMC)的上下文菜单配置扫描

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **本地任务 → 从上下文菜单扫描**。

4. 配置从上下文菜单扫描（参见下表）。

5. 保存更改。

如何在 Web Console 和云控制台中配置从上下文菜单扫描

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
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. 在“**从上下文菜单扫描**”下，配置从上下文菜单扫描（参见下表）。
6. 保存更改。

如何在应用程序界面中配置从上下文菜单扫描

1. 在应用程序主窗口中，转到“**任务**”区域。
2. 在任务列表中，选择扫描任务并单击 ⚙ 按钮。
3. 配置从上下文菜单扫描（参见下表）。
4. 保存更改。

如果“*从上下文菜单扫描*”任务未显示，这意味着管理员已在策略中禁止对本地任务的使用。

“从上下文菜单扫描”任务设置

参数	描述
安全级别	Kaspersky Endpoint Security 可以使用不同的设置组运行扫描。存储在应用程序中的设置组叫做*安全级别*: • “**高**”。Kaspersky Endpoint Security 扫描所有类型的文件。扫描复合文件时，应用程序会扫描存档、分发包、Office 格式的文件，但不会扫描受密码保护的存档。当设置此安全级别时，应用程序将使用**深度扫描**详细级别的启发式分析。 • “**建议**”。Kaspersky Endpoint Security 扫描所有类型的文件。扫描复合文件时，应用程序会扫描存档、分发包、Office 格式的文件，但不会扫描受密码保护的存档。当设置此安全级别时，应用程序将使用**中度扫描**详细级别的启发式分析。 • “**低**”。Kaspersky Endpoint Security 仅扫描指定的文件格式。扫描复合文件时，应用程序会扫描存档、分发包、Office 格式的文件，但不会扫描受密码保护的存档。当设置此安全级别时，应用程序将使用**轻度扫描**详细级别的启发式分析。
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。 “**清除；如果清除失败则通知**”。如果选择该选项，Kaspersky Endpoint Security 将自动尝试对已经检测到的所有受感染的文件执行清除操作。如果清除失败，Kaspersky Endpoint Security 会将检测到的受感染文件的相关信息添加到活动威胁列表。 “**通知**”。如果选择此选项，Kaspersky Endpoint Security 会在检测到受感染文件时将这些文件的相关信息添加到活动威胁列表。
文件类型	Kaspersky Endpoint Security 将没有扩展名的文件视为可执行文件。应用程序总是扫描可执行文件，而与所选的要扫描的文件类型无关。 “**所有文件**”。如果启用该设置，Kaspersky Endpoint Security 将毫无例外地扫描所有文件（所有格式和扩展名）。 “**按格式扫描文件**”。如果启用该设置，则应用程序仅扫描被感染的文件。在扫描文件以查找恶意代码之前，系统将分析文件的内部头以确定文件的格式（例如，.txt、.doc 或 .exe）。该扫描也查找具有特殊文件扩展名的文件。 “**按扩展名扫描文件**”。如果启用该设置，则应用程序仅扫描被感染的文件。此时，系统将根据文件的扩展名确定文件格式。 默认情况下，Kaspersky Endpoint Security 按格式扫描文件。按扩展名扫描文件不太安全，因为恶意文件的扩展名可能不在潜在可感染列表中（例如，`.123`）。
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。
跳过扫描时间超过以下值的文件 N 秒	限制任务执行时间。超出指定时间后，Kaspersky Endpoint Security 将停止任务。任务未标记为已完成。下次 Kaspersky Endpoint Security 运行该任务时，它将按计划从头开始运行。

参数	描述
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	该选框用于启用或禁用对分发包的扫描。
扫描 Microsoft Office 格式文件	扫描 Microsoft Office 文件（DOC、DOCX、XLS、PPT 和其他 Microsoft 扩展程序）。Office 格式文件也包括 OLE 对象。应用程序扫描小于 1 MB 的 office 格式文件，无论该复选框是否被选中。
扫描电子邮件格式文件	扫描电子邮件格式文件和电子邮件数据库。该应用程序扫描 MS Outlook 和 Windows Mail 邮件客户端使用的 PST 和 OST 文件以及 EML 文件。 Kaspersky Endpoint Security 不支持 64 位版本的 Microsoft Outlook 邮件客户端。这意味着，如果计算机上安装了 64 位版本的 Microsoft Outlook，即使邮件包含在扫描范围内，Kaspersky Endpoint Security 也不会扫描 Microsoft Outlook 文件（PST 和 OST 文件）。 如果选择该选框，Kaspersky Endpoint Security 将把邮件格式文件的各个部分分解（标题、正文、附件）后扫描威胁。 如果清空该选框，Kaspersky Endpoint Security 将把邮件格式的文件作为一个单独的文件扫描。 当在 PST 或 OST 文件中发现恶意对象时，Kaspersky Endpoint Security 会根据所选操作（例如，对文件清除或删除）使其无害。 当在其他邮件客户端（例如 Mozilla Thunderbird）的文件中检测到恶意文件时，Kaspersky Endpoint Security 只会标记受感染的邮件。您需要手动删除带有已感染附件的邮件。
扫描受密码保护的存档	如果选择该选框，应用程序将扫描密码保护的存档。在扫描存档中的文件前，系统将提示您输入密码。 如果清空该选框，应用程序将跳过扫描密码保护的存档。
复合文件大于指定值时不解压	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。
机器学习和特征码分析	机器学习和签名分析方法使用 Kaspersky Endpoint Security 数据库，其中包含已知威胁的描述以及消除它们的方法。使用此方法的保护提供了可接受的最低安全级别。 根据 Kaspersky 专家的推荐，机器学习和签名分析始终启用。
启发式分析	开发该技术的目的是检测使用当前版本的卡巴斯基应用程序数据库无法检测到的威胁。它可以检测可能受未知病毒或已知病毒新变种感染的文件。 当扫描文件以查找恶意代码时，启发式分析执行可执行文件中的指令。启发式分析执行的指令数量取决于启发式分析级别。启发式分析级别可在全面搜索新威胁、加载操作系统资源和启发式分析持续时间之间进行平衡。
iSwift 技术	该技术允许通过排除特定文件不扫描的方式提高扫描速度。该技术将使用特殊算法将文件排除在扫描范围之外，该算法会考虑 Kaspersky Endpoint Security 数据库的发布日期、文件的上次扫描日期以及对扫描设置的任何修改。iSwift 技术是对用于 NTFS 文件系统的 iChecker 技术的增强版。
iChecker 技术	该技术允许通过排除特定文件不扫描的方式提高扫描速度。该技术将使用特殊算法将文件排除在扫描范围之外，该算法会考虑 Kaspersky Endpoint Security 数据库的发布日期、文件的上次扫描日期以及对扫描设置的任何修改。iChecker 技术受到一些限制：它无法操作大型文件，并且仅能应用于具有应用程序可识别结构的文件（例如：EXE、DLL、LNK、TTF、INF、SYS、COM、CHM、ZIP 和 RAR）。

应用程序完整性检查

Kaspersky Endpoint Security 将检查程序的模块是否损坏或者被修改，例如，如果应用程序库的数字签名错误，则该库被视为损坏。“*应用程序完整性检查*”任务用于检查应用程序文件。如果 Kaspersky Endpoint Security 检测到恶意对象但未清除它，请运行“*应用程序完整性检查*”任务。

您可以在 Kaspersky Security Center Web Console 和管理控制台中创建“*应用程序完整性检查*”任务。无法在 Kaspersky Security Center 云控制台中创建任务。

在以下情况下，应用程序完整性可能会被破坏：

- 恶意对象修改了 Kaspersky Endpoint Security 的文件。在这种情况下，使用操作系统的工具执行还原 Kaspersky Endpoint Security 的步骤。还原后，运行计算机全盘扫描并重复完整性检查。
- 数字签名已过期。在这种情况下，请更新 Kaspersky Endpoint Security。

如何通过管理控制台 (MMC) 运行应用程序完整性检查

1. 在 Kaspersky Security Center 管理控制台树中，选择“**任务**”。
   任务列表打开。
2. 单击“**新任务**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 选择任务类型

选择“**Kaspersky Endpoint Security for Windows (14.1)**”→ “**应用程序完整性检查**”。

步骤 2. 选择任务将分配到的设备

选择将要执行任务的计算机。下列选项可用：

- 将任务分配给管理组。在这种情况下，任务分配给先前创建的管理组中包括的计算机。
- 选择管理服务器在网络中检测到的计算机：*未分配设备*。特定设备可包括管理组中的设备以及未分配设备。
- 手动指定设备地址或从列表中导入地址。您可以指定您要将任务分配给的设备的 NetBIOS 名称、IP 地址和 IP 子网。

步骤 3. 配置任务启动计划

配置任务启动计划，例如，手动或当检测到病毒爆发时。

步骤 4. 定义任务名称

输入任务的名称，例如“*在计算机感染后执行完整性检查*”。

步骤 5. 完成任务创建

退出向导。如有必要，选中“**向导完成时运行任务**”复选框。您可以在任务属性中监控任务进度。结果，Kaspersky Endpoint Security 将检查应用程序的完整性。您还可以在任务属性中配置应用程序完整性检查计划（参见下表）。

如何通过 Web Console 运行应用程序完整性检查

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
2. 单击“**添加**”。
   “任务向导”将启动。
3. 配置任务设置：
   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Endpoint Security for Windows 14.2.0**”。
   b. 在“**任务类型**”下拉列表中，选择“**应用程序完整性检查**”。
   c. 在“**任务名称**”字段中，输入简要说明，例如，“*在计算机感染后检查应用程序的完整性*”。
   d. 在“**要对其分配任务的设备**”块，选择任务范围。
4. 按照所选任务范围选项选择设备。转到下一步。
5. 选择要运行任务的账户。默认情况下，Kaspersky Endpoint Security 将使用本地用户账户的权限启动任务。
6. 退出向导。
   在任务列表中将显示一个新任务。
7. 选中该任务旁边的复选框。

结果，Kaspersky Endpoint Security 将检查应用程序的完整性。您还可以在任务属性中配置应用程序完整性检查计划（参见下表）。

如何在应用程序界面中运行完整性检查

1. 在应用程序主窗口中，转到“**任务**”区域。
2. 这将打开任务列表；选择“*应用程序完整性检查*”任务并单击“**运行**”。

结果，Kaspersky Endpoint Security 将检查应用程序的完整性。您还可以在任务属性中配置应用程序完整性检查计划（参见下表）。如果“*应用程序完整性检查*”任务未显示，这意味着管理员已在策略中禁止对本地任务的使用。

参数	描述
扫描计划	"**手动**"。您可以在方便时手动启动扫描的运行模式。 "**根据计划**"。在该扫描任务运行模式下，应用程序将按照您创建的计划启动扫描任务。如果选择该扫描任务运行模式，您也可以手动启动扫描任务。
运行略过的任务	如果选中该复选框，Kaspersky Endpoint Security 将在可能的情况下尽快启动已忽略的任务。任务在某些情况下可能被略过，例如，计算机在启动计划任务时处于关闭状态。当应用程序有机会执行略过的任务时，它会在一定的时间间隔内随机运行任务，以分配计算机上的负载。 如果清除该复选框，Kaspersky Endpoint Security 不会运行已略过的任务。它将按照当前计划运行下一次任务。
仅在计算机空闲时运行	计算机资源忙时推迟任务启动。如果计算机被锁定或屏幕保护开启，Kaspersky Endpoint Security 启动扫描任务。如果您中断了任务的执行，例如通过解锁计算机，Kaspersky Endpoint Security 将自动运行该任务，并从中断点继续运行。此计划选项允许您在使用计算机时节省计算机资源。

编辑扫描范围

*扫描范围*是指向文件夹的路径列表，以及 Kaspersky Endpoint Security 在执行任务时扫描的路径。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。

> 要编辑扫描范围，我们建议使用"*自定义扫描*"任务。卡巴斯基专家建议不要更改"*全盘扫描*"和"*关键区域扫描*"任务的扫描范围。

Kaspersky Endpoint Security 具有以下预定义对象作为扫描范围的一部分：

- "**系统内存**"。
- "**正在运行的进程和启动对象**"。

  系统启动时运行的进程和应用程序可执行文件占用的内存。
- "**磁盘引导扇区**"。

  硬盘和可移动磁盘引导扇区。
- "**系统备份**"。

  系统卷信息文件夹的内容。
- "**所有外部设备**"。
- "**所有硬盘驱动器**"。
- "**所有网络驱动器**"。

> 在 Kaspersky Endpoint Security for Windows 12.12 中，电子邮件被排除在应用程序扫描范围之外。对传入和传出电子邮件的扫描由邮件威胁防护组件执行。如果您使用的是较早版本的管理插件，即使策略中包含电子邮件，该应用程序也会将电子邮件排除在扫描范围之外。

> 我们建议创建单独的扫描任务来扫描网络驱动器或共享文件夹。在"*恶意软件扫描*"任务的设置中，指定对此驱动器具有写入权限的用户；这对于减轻检测到的威胁是必要的。如果网络驱动器所在的服务器有自己的安全工具，请不要对该驱动器运行扫描任务。这样就可以避免两次检查对象，提高服务器的性能。

要从扫描范围中排除文件夹或文件，请将文件夹或文件添加到受信任区域。

如何在管理控制台 (MMC) 中编辑扫描范围

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**任务**”。
3. 选择扫描任务并双击以打开任务属性。
   如果必要，请创建“*恶意软件扫描*”任务。
4. 在任务属性窗口中，选择“**设置**”区域。
5. 在“**扫描范围**”区域中单击“**设置**”。
6. 在打开的窗口中，选择您要添加到扫描范围或从扫描范围排除的对象。
7. 如果您希望将新对象添加至扫描范围：
   a. 单击“**添加**”。
   b. 在**对象**字段，输入文件夹或文件的路径。
      使用掩码：
      - `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\*\*.txt` 将包括位于 C: 驱动器的文件夹（但不包括子文件夹）中所有具有 TXT 扩展名的文件的路径。
      - 两个连续 `*` 字符在文件或文件夹名称中代表任意一组字符（包括空集），包括 `\` 和 `/` 字符（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\**\*.txt` 将包括位于 `Folder` 嵌套子文件夹（除了 `Folder` 本身）中所有带 TXT 扩展名的文件的路径。掩码必须包含至少一个嵌套级别。掩码 `C:\**\*.txt` 不是有效掩码。
      - `?`（问号）字符代表任意单个字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\???.txt` 将包括位于 `Folder` 文件夹中所有带 TXT 扩展名且名称由三个字符构成的文件的路径。

      您可以在文件或文件夹路径中的任何位置使用掩码。例如，如果您希望扫描范围包括计算机上所有用户账户的下载文件夹，请输入 `C:\Users\*\Downloads\` 掩码。

      计算机的文件资源列表中的“**此 PC**”对象包括以下对象：**所有硬盘驱动器**、**所有网络驱动器** 和 **所有可移动驱动器**。

   您可以从扫描排除对象，而不用将其从对象列表删除。为此，清空对象旁边的复选框。
8. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中编辑扫描范围

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**任务**”。
   任务列表打开。
2. 单击扫描任务。
   任务属性窗口将打开。如果必要，请创建“*恶意软件扫描*”任务。

3. 选择**应用程序设置**选项卡。

4. 在**扫描范围**中，选择您要添加到扫描范围或从扫描范围排除的对象。

5. 如果您希望将新对象添加至扫描范围：

   a. 单击“**添加**”。

   b. 输入文件夹或文件的路径。

      使用掩码：

      - `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\*\*.txt` 将包括位于 C: 驱动器的文件夹（但不包括子文件夹）中所有具有 TXT 扩展名的文件的路径。

      - 两个连续 `*` 字符在文件或文件夹名称中代表任意一组字符（包括空集），包括 `\` 和 `/` 字符（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\**\*.txt` 将包括位于 `Folder` 嵌套子文件夹（除了 `Folder` 本身）中所有带 TXT 扩展名的文件的路径。掩码必须包含至少一个嵌套级别。掩码 `C:\**\*.txt` 不是有效掩码。

      - `?`（问号）字符代表任意单个字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\???.txt` 将包括位于 `Folder` 文件夹中所有带 TXT 扩展名且名称由三个字符构成的文件的路径。

      您可以在文件或文件夹路径中的任何位置使用掩码。例如，如果您希望扫描范围包括计算机上所有用户账户的下载文件夹，请输入 `C:\Users\*\Downloads\` 掩码。

   您可以从扫描排除对象，而不用将其从对象列表删除。为此，请将其旁边的切换开关设置为关闭位置。

6. 保存更改。

如何在应用程序界面中编辑扫描范围

1. 在应用程序主窗口中，转到“**任务**”区域。

2. 这将打开任务列表；选择“*自定义扫描*”任务并单击“**选择**”。

   您也可以为其他任务编辑扫描范围。卡巴斯基专家建议不要更改“*全盘扫描*”和“*关键区域扫描*”任务的扫描范围。

3. 在打开的窗口中，选择您要添加到扫描范围的对象。

4. 保存更改。

如果扫描任务未显示，这意味着管理员已禁止在策略中使用本地任务。

运行计划扫描

使用“*恶意软件扫描*”任务扫描恶意软件可能耗时较长，并且可能会增加 Kaspersky Endpoint Security 对计算机资源的使用。因此，推荐选择最佳时间运行该任务，以最大限度地减少对其他应用程序性能的影响。

例如，如果贵公司员工按固定时间表工作，您可以配置计算机扫描在夜间或周末运行。如果由于任何原因无法运行任务（例如，当时计算机处于关机状态），则可以配置跳过的任务，使其在计算机可用时尽快自动运行。此功能应谨慎使用，因为它可能会在早上电脑开机时减慢用户电脑上应用程序的运行速度。

如果您无法确定满足您需求的最佳扫描计划，您可以将扫描配置为在满足以下特殊条件之一时运行：

- 在数据库更新之后。

  Kaspersky Endpoint Security 使用更新的签名数据库运行计算机扫描。

- 在应用程序启动后。

  Kaspersky Endpoint Security 在应用程序启动后经过指定的时间后运行计算机扫描。在操作系统启动时，许多进程正在运行，因此推迟运行扫描任务而不是在 Kaspersky Endpoint Security 启动后立即运行扫描任务是有利的。

- “Wake-on-LAN”功能。

  Kaspersky Endpoint Security 按计划运行计算机扫描，即使计算机已关机。为此，应用程序使用操作系统的“Wake-on-LAN”功能。“Wake-on-LAN”功能允许通过本地网络发送特殊信号远程启动计算机。要使用此功能，必须在 BIOS 设置中启用“Wake-on-LAN”。

  您可以仅为 Kaspersky Security Center 的“*恶意软件扫描*”任务配置使用“Wake-on-LAN”运行扫描。无法在应用程序界面中启用“Wake-on-LAN”以扫描计算机。

- 在计算机空闲时扫描。

  当屏幕保护程序处于活动状态或屏幕被锁定时，Kaspersky Endpoint Security 会按计划运行计算机扫描。如果用户解锁计算机，Kaspersky Endpoint Security 将暂停扫描。在这种情况下，全盘扫描可能需要几天时间才能完成。

- 当任务被跳过。

  Kaspersky Endpoint Security 会在条件允许的情况下立即运行被跳过的任务。任务在某些情况下可能被略过，例如，计算机在启动计划任务时处于关闭状态。当应用程序有机会执行略过的任务时，它会在一定的时间间隔内随机运行任务，以分配计算机上的负载。

如何在 Web Console 和云控制台中配置扫描计划

1. 在 Web Console 的主窗口中，选择“**任务**”。

   任务列表打开。

2. 单击扫描任务。

   任务属性窗口将打开。

3. 在任务属性窗口中，选择“**计划**”选项卡。

4. 配置扫描任务计划。

5. 根据选定的频率，配置指定任务运行计划的高级设置（参见下表）。

6. 保存更改。

如何在应用程序界面中配置扫描计划

> 仅当策略未应用于计算机时，才能配置扫描计划。对于策略下的计算机，您可以在 Kaspersky Security Center 配置*恶意软件扫描*任务计划。

1. 在应用程序主窗口中，转到“**任务**”区域。

2. 在任务列表中，选择扫描任务并单击 ⚙ 按钮。

   您可以为运行全盘扫描、关键区域扫描或完整性检查配置计划。您仅可以手动运行自定义扫描。

3. 单击“**扫描计划**”。

4. 在打开的窗口中，配置扫描任务运行计划。

5. 根据选定的频率，配置指定任务运行计划的高级设置（参见下表）。

6. 保存更改。

扫描计划设置

参数	描述
扫描计划	“**手动**”。您可以在方便时手动启动扫描的运行模式。 “**根据计划**”。在该扫描任务运行模式下，应用程序将按照您创建的计划启动扫描任务。如果选择该扫描任务运行模式，您也可以手动启动扫描任务。
在应用程序启动此时间后延迟运行 N 分钟	应用程序启动后已推迟扫描任务的启动。在操作系统启动时，许多进程正在运行，因此推迟运行扫描任务而不是在 Kaspersky Endpoint Security 启动后立即运行扫描任务是有利的。
运行略过的任务	如果选中该复选框，Kaspersky Endpoint Security 将在可能的情况下尽快启动已忽略的任务。任务在某些情况下可能被略过，例如，计算机在启动计划任务时处于关闭状态。当应用程序有机会执行略过的任务时，它会在一定的时间间隔内随机运行任务，以分配计算机上的负载。 如果清除该复选框，Kaspersky Endpoint Security 不会运行已略过的任务。它将按照当前计划运行下一次任务。
仅在计算机空闲时运行	计算机资源忙时推迟任务启动。如果计算机被锁定或屏幕保护开启，Kaspersky Endpoint Security 启动扫描任务。如果您中断了任务的执行，例如通过解锁计算机，Kaspersky Endpoint Security 将自动运行该任务，并从中断点继续运行。此计划选项允许您在使用计算机时节省计算机资源。
使用任务启动自动随机延迟 *（仅在 Kaspersky Security Center 控制台可用）*	如果选中该复选框，则任务不会严格按计划运行，而是在一定的时间间隔内随机运行，即任务的开始时间是分散的。随机开始时间有助于避免任务按计划运行时大量计算机同时访问管理服务器。 随机开始时间的范围在创建任务时自动计算，具体取决于分配任务的计算机数量。随后，任务始终在其计算的开始时间运行。然而，无论何时修改任务设置或手动运行任务，计算的开始时间都会更改。 如果清除该复选框，则任务将完全在计划时间运行。
使用任务启动随机延迟间隔(分钟)	如果选中此复选框，则会在一定时间范围内的随机时间在计算机上运行任务。随机开始时间有助于避免任务按计划运行时大量计算机同时访问管理服务器。 如果清除该复选框，则任务将完全在计划时间运行。
如果任务运行超过该时间则停止(分钟) *（仅在 Kaspersky Security Center 控制台可用）*	限制任务执行时间。超出指定时间后，Kaspersky Endpoint Security 将停止任务。任务未标记为已完成。下次 Kaspersky Endpoint Security 运行该任务时，它将按计划从头开始运行。 要缩短任务执行时间，例如，您可以配置扫描范围或优化扫描。
使用 Wake-On-LAN 功能在任务启动之前开启设备(分钟) *（仅在 Kaspersky Security Center 控制台可用）*	如果选中该复选框，则在运行任务之前，计算机的操作系统将有一个指定的提前期来完成启动。默认提前期为 5 分钟。 如果要在所有计算机（包括已关机的计算机）上运行任务，请选中该复选框。
任务完成后关闭设备 *（仅在 Kaspersky Security Center 控制台可用）*	例如，您可以启用此功能在星期五下班后扫描计算机。当任务完成后，应用程序会在周末关闭计算机。
暂停任务	您可以指定一个时间间隔，在此期间将暂停执行先前计划的任务。指定时间段结束后，任务将继续执行。例如，为了最大限度地减少 Kaspersky Endpoint Security 软件在高峰使用期间对计算机性能的影响，这样做可能是必要的。
禁用计划开始于	如果选中该复选框，Kaspersky Endpoint Security 将从指定日期开始停止运行计划任务。任务将设置为 **手动** 模式。

以其他用户身份运行扫描

默认下，扫描任务以您使用其权限在操作系统中注册的用户的名称运行。保护范围可能包含需要特殊权限才能访问的网络驱动器或其他对象。您可以在应用程序设置中指定拥有所需权限的用户，然后在该用户账户下运行扫描任务。

您可以以其他用户身份运行以下扫描：

- 关键区域扫描。
- 全盘扫描。
- 自定义扫描。
- 从上下文菜单扫描。

您无法配置用户权限以运行可移动驱动器扫描、后台扫描或完整性检查。

如何在管理控制台 (MMC) 中以其他用户身份运行扫描

1. 打开 Kaspersky Security Center Administration Console。
2. 在管理控制台树的“**受管理设备**”文件夹中，打开相关客户端计算机所属的管理组名称的文件夹。
3. 在工作区中选择“**任务**”选项卡。
4. 选择扫描任务并双击以打开任务属性。
5. 在任务属性窗口中，选择“**账户**”区域。
6. 输入要使用其权限运行扫描任务的用户的账户凭证。
7. 保存更改。

如何在 Web Console 或云控制台中以其他用户身份运行扫描

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**任务**”。
   任务列表打开。
2. 单击扫描任务。
   任务属性窗口将打开。
3. 选择**设置**选项卡。
4. 在“**账户**”块中单击“**设置**”按钮。
5. 输入要使用其权限运行扫描任务的用户的账户凭证。
6. 保存更改。

如何在应用程序界面中以其他用户身份运行扫描

1. 在应用程序主窗口中，转到“**任务**”区域。
2. 在任务列表中，选择扫描任务并单击 ⚙ 按钮。
3. 在任务属性中，选择“**高级设置**” → “**运行扫描身份**”。
4. 在打开的窗口中，输入要使用其权限运行扫描任务的用户的账户凭证。
5. 保存更改。

如果扫描任务未显示，这意味着管理员已禁止在策略中使用本地任务。

扫描优化

扫描计算机时限制 CPU 使用率

您可以限制运行“*恶意软件扫描*”任务时的 CPU 使用率。这可能会增加扫描计算机所需的时间。

如何在管理控制台 (MMC) 中限制扫描计算机时的 CPU 使用率

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **应用程序设置**。
4. 在“**性能**”下，选择“**限制扫描任务的 CPU 使用率**”复选框并输入 CPU 资源消耗的平均值（百分比）。
5. 保存更改。

如何在 Web Console 和云控制台中限制扫描计算机时的 CPU 使用率

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **性能**。
5. 在“**限制扫描任务的 CPU 使用率**”下，设置切换开关到“**限制扫描任务的 CPU 使用率**”并输入 CPU 资源消耗的平均值（百分比）。
6. 保存更改。

如何在应用程序界面中限制扫描计算机时的 CPU 使用率

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**常规设置**” → “**应用程序设置**”。

Kaspersky Endpoint Security for Windows 设置

3. 在“**性能**”下，选择“**限制扫描任务的 CPU 使用率**”复选框并输入 CPU 资源消耗的平均值（百分比）。

4. 保存更改。

配置“恶意软件扫描”的高级任务设置。

您可以优化文件扫描：缩短扫描时间并提高 Kaspersky Endpoint Security 的操作速度。这可以通过仅扫描新文件和上次扫描后经过修改的文件来实现。此模式适用于简单文件和复合文件。您还可以设置单个文件的扫描限制。当指定的时间间隔到期时，Kaspersky Endpoint Security 将从当前扫描中排除该文件（除包含多个文件的存档和对象之外）。

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。

您也可以启用 iChecker 和 iSwift 技术。iChecker 和 iSwift 技术可以通过排除上次扫描后未修改的文件来优化文件的扫描速度。

如何在管理控制台 (MMC) 中优化扫描

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**任务**”。
3. 选择扫描任务并双击以打开任务属性。

   如果必要，请创建“*恶意软件扫描*”任务。
4. 在任务属性窗口中，选择“**设置**”区域。
5. 在“**安全级别**”块中单击“**设置**”按钮。

   这将打开扫描任务设置窗口。
6. 在“**优化**”块，配置扫描设置：
   - “**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。

     您还可以配置按类型扫描新文件。例如，您可以扫描所有分发包，并且只扫描新的压缩文件和 Office 格式文件。
   - **跳过扫描时间超过以下值的文件 N 秒**。限制任务执行时间。超出指定时间后，Kaspersky Endpoint Security 将停止任务。任务未标记为已完成。下次 Kaspersky Endpoint Security 运行该任务时，它将按计划从头开始运行。
   - “**不同时运行多个扫描任务**”。如果扫描已在运行，则推迟启动扫描任务。如果当前扫描继续，Kaspersky Endpoint Security 将使新的扫描任务排队。这有助于优化计算机上的负载。例如，假设应用程序已根据计划启动了全盘扫描任务。如果有用户试图从应用程序界面启动快速扫描，Kaspersky Endpoint Security 会将此快速扫描任务排队，然后在完成全盘磁盘扫描任务后自动启动此任务。
7. 单击“**附加**”。

   这将打开复合文件扫描设置窗口。
8. 在“**大小限制**”块中，选中“**复合文件大于指定值时不解压**”复选框。限制任务执行时间。超出指定时间后，Kaspersky Endpoint Security 将停止任务。任务未标记为已完成。下次 Kaspersky Endpoint Security 运行该任务时，它将按计划从头开始运行。

   > 无论是否选中“**复合文件大于指定值时不解压**”复选框，Kaspersky Endpoint Security 均会扫描从存档中提取的大型文件。
9. 单击“**确定**”。
10. 转到“**附加**”选项卡。

11. 在“**扫描技术**”块，选中您要在扫描期间使用技术的名称旁边的复选框。

    - “**iSwift 技术**”。该技术允许通过排除特定文件不扫描的方式提高扫描速度。该技术将使用特殊算法将文件排除在扫描范围之外，该算法会考虑 Kaspersky Endpoint Security 数据库的发布日期、文件的上次扫描日期以及对扫描设置的任何修改。iSwift 技术是对用于 NTFS 文件系统的 iChecker 技术的增强版。

    - “**iChecker 技术**”。该技术允许通过排除特定文件不扫描的方式提高扫描速度。该技术将使用特殊算法将文件排除在扫描范围之外，该算法会考虑 Kaspersky Endpoint Security 数据库的发布日期、文件的上次扫描日期以及对扫描设置的任何修改。iChecker 技术受到一些限制：它无法操作大型文件，并且仅能应用于具有应用程序可识别结构的文件（例如：EXE、DLL、LNK、TTF、INF、SYS、COM、CHM、ZIP 和 RAR）。

12. 保存更改。

如何在 Web Console 和云控制台中优化扫描

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

   任务列表打开。

2. 单击扫描任务。

   任务属性窗口将打开。如果必要，请创建“*恶意软件扫描*”任务。

3. 选择**应用程序设置**选项卡。

4. 在“**检测到威胁后的操作**”块中，选中“**仅扫描新建和已修改的文件**”复选框。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。

   您还可以配置按类型扫描新文件。例如，您可以扫描所有分发包，并且只扫描新的压缩文件和 Office 格式文件。

5. 在“**扫描优化**”块中，选中“**复合文件大于指定值时不解压**”复选框。限制任务执行时间。超出指定时间后，Kaspersky Endpoint Security 将停止任务。任务未标记为已完成。下次 Kaspersky Endpoint Security 运行该任务时，它将按计划从头开始运行。

   > 无论是否选中“**复合文件大于指定值时不解压**”复选框，Kaspersky Endpoint Security 均会扫描从存档中提取的大型文件。

6. 选择**不同时运行多个扫描任务**复选框。如果扫描已在运行，则推迟启动扫描任务。如果当前扫描继续，Kaspersky Endpoint Security 将使新的扫描任务排队。这有助于优化计算机上的负载。例如，假设应用程序已根据计划启动了全盘扫描任务。如果有用户试图从应用程序界面启动快速扫描，Kaspersky Endpoint Security 会将此快速扫描任务排队，然后在完成全盘磁盘扫描任务后自动启动此任务。

7. 在“**高级设置**”块中，选中“**跳过扫描时间超过以下值的文件(秒)**”复选框。限制任务执行时间。超出指定时间后，Kaspersky Endpoint Security 将停止任务。任务未标记为已完成。下次 Kaspersky Endpoint Security 运行该任务时，它将按计划从头开始运行。

8. 保存更改。

如何在应用程序界面中优化扫描

1. 在应用程序主窗口中，转到“**任务**”区域。

2. 在任务列表中，选择扫描任务并单击 ⚙ 按钮。

3. 单击“**高级设置**”。

4. 在“**优化**”块，配置扫描设置：

- “**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。

  您还可以配置按类型扫描新文件。例如，您可以扫描所有分发包，并且只扫描新的压缩文件和 Office 格式文件。

- **跳过扫描时间超过以下值的文件 N 秒**。限制任务执行时间。超出指定时间后，Kaspersky Endpoint Security 将停止任务。任务未标记为已完成。下次 Kaspersky Endpoint Security 运行该任务时，它将按计划从头开始运行。

- “**不同时运行多个扫描任务**”。如果扫描已在运行，则推迟启动扫描任务。如果当前扫描继续，Kaspersky Endpoint Security 将使新的扫描任务排队。这有助于优化计算机上的负载。例如，假设应用程序已根据计划启动了全盘扫描任务。如果有用户试图从应用程序界面启动快速扫描，Kaspersky Endpoint Security 会将此快速扫描任务排队，然后在完成全盘磁盘扫描任务后自动启动此任务。

5. 在“**大小限制**”块中，选中“**复合文件大于指定值时不解压**”复选框。限制任务执行时间。超出指定时间后，Kaspersky Endpoint Security 将停止任务。任务未标记为已完成。下次 Kaspersky Endpoint Security 运行该任务时，它将按计划从头开始运行。

   无论是否选中“**复合文件大于指定值时不解压**”复选框，Kaspersky Endpoint Security 均会扫描从存档中提取的大型文件。

6. 在“**扫描技术**”块，选中您要在扫描期间使用技术的名称旁边的复选框。

- “**iSwift 技术**”。该技术允许通过排除特定文件不扫描的方式提高扫描速度。该技术将使用特殊算法将文件排除在扫描范围之外，该算法会考虑 Kaspersky Endpoint Security 数据库的发布日期、文件的上次扫描日期以及对扫描设置的任何修改。iSwift 技术是对用于 NTFS 文件系统的 iChecker 技术的增强版。

- “**iChecker 技术**”。该技术允许通过排除特定文件不扫描的方式提高扫描速度。该技术将使用特殊算法将文件排除在扫描范围之外，该算法会考虑 Kaspersky Endpoint Security 数据库的发布日期、文件的上次扫描日期以及对扫描设置的任何修改。iChecker 技术受到一些限制：它无法操作大型文件，并且仅能应用于具有应用程序可识别结构的文件（例如：EXE、DLL、LNK、TTF、INF、SYS、COM、CHM、ZIP 和 RAR）。

7. 保存更改。

如果扫描任务未显示，这意味着管理员已禁止在策略中使用本地任务。

更新数据库和程序软件模块

更新 Kaspersky Endpoint Security 的数据库和程序模块可为您的计算机提供最新保护。新病毒和其他类型的恶意软件每天都在全世界出现。Kaspersky Endpoint Security 数据库包含有关威胁的信息和使其失效的方法。要快速检测到威胁，建议您定期更新数据库和应用程序模块。

在美国境内，本软件中将不再提供更新功能（包括提供反病毒签名更新和代码库更新）。

常规更新要求具有已生效的授权许可。如果当前没有授权许可，您将只能执行一次更新。

您的计算机必须连接到互联网才能成功下载来自卡巴斯基更新服务器的更新包。默认情况下，系统将自动确定互联网连接设置。如果您使用代理服务器，则需要配置代理服务器设置。

通过 HTTPS 协议下载更新。当无法通过 HTTPS 协议下载更新时，也可以通过 HTTP 协议下载。

当执行更新时，以下对象将下载并安装到您的计算机中：

- Kaspersky Endpoint Security 数据库。该程序使用包含病毒签名和其他威胁签名以及清除方法的数据库实现计算机保护。当搜索并为受感染文件清除时，保护组件将使用此信息。数据库将不断更新应对它们的方法和新威胁记录。因此，我们建议您定期更新数据库。

  除了 Kaspersky Endpoint Security 数据库之外，系统也会更新已启用程序组件以拦截网络流量的网络驱动程序。

- 程序模块。除了 Kaspersky Endpoint Security 数据库，您也可以更新程序模块。更新程序模块可以修补 Kaspersky Endpoint Security 中的漏洞、添加新功能或增强现有功能。

更新时，您的计算机上的程序模块和数据库将与最新版本更新源进行对比。如果您当前数据库和程序模块与相应的最新版本不同，缺少的更新部分将安装在您的计算机上。

如果数据库过时，更新包可能会很大，这可能会花费更多的互联网流量（最多达几十 MB）。

有关 Kaspersky Endpoint Security 数据库的当前状态的信息显示在主应用程序窗口中，或将光标悬停在通知区域中的应用程序图标上时看到的工具提示中。

有关更新任务运行期间更新结果和所有发生事件的信息将记录在 Kaspersky Endpoint Security 报告中。

如果应用程序正在 Light Agent 模式下运行，更新应用程序数据库和模块时将有特殊考虑。

数据库和应用程序模块更新方案

更新 Kaspersky Endpoint Security 的数据库和程序模块可为您的计算机提供最新保护。新病毒和其他类型的恶意软件每天都在全世界出现。Kaspersky Endpoint Security 数据库包含有关威胁的信息和使其失效的方法。要快速检测到威胁，建议您定期更新数据库和应用程序模块。

以下对象在用户的计算机上更新：

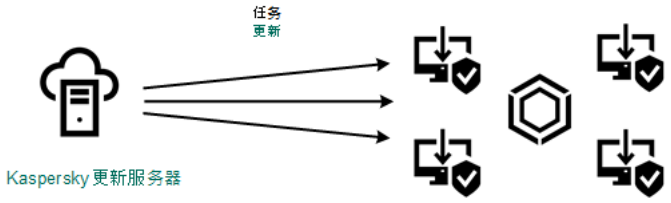
- 反病毒数据库。反病毒数据库包括恶意软件签名数据库、网络攻击描述、恶意和钓鱼网址数据库、广告栏数据库、垃圾邮件数据库以及其他数据。

- 程序模块。模块更新旨在消除应用程序中的漏洞和改进计算机保护方法。模块更新可能更改应用程序组件的行为和添加新功能。

Kaspersky Endpoint Security 支持下列数据库和应用程序模块更新方案：

- 从 Kaspersky 服务器更新。

  卡巴斯基更新服务器位于全球多个国家。这可确保更新的高可靠性。如果无法从一台服务器执行更新，Kaspersky Endpoint Security 会切换到下一台服务器。



从 Kaspersky 服务器更新

- 集中更新。

  集中更新可减少外部 Internet 流量，并提供方便的更新监控。

  集中更新包括以下步骤：

  1. 将更新包下载到组织网络内的存储库。

     更新包由名为“*将更新下载至管理服务器存储库*”的管理服务器任务下载到存储库。

  2. 将更新包下载到共享文件夹（可选）。

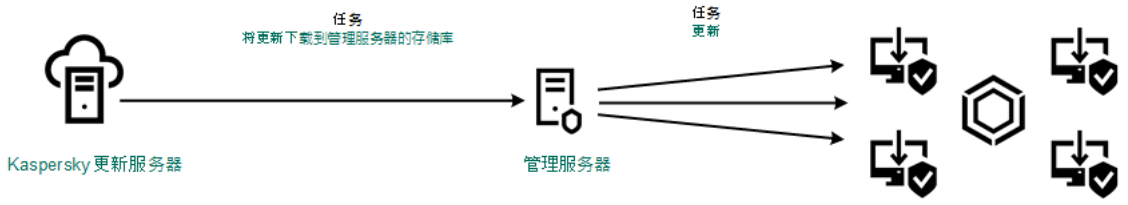
     您可以使用以下方法将更新包下载到共享文件夹：

     - 使用 Kaspersky Endpoint Security 的“*数据库和应用程序模块更新*”任务。该任务用于公司局域网中的一台计算机。

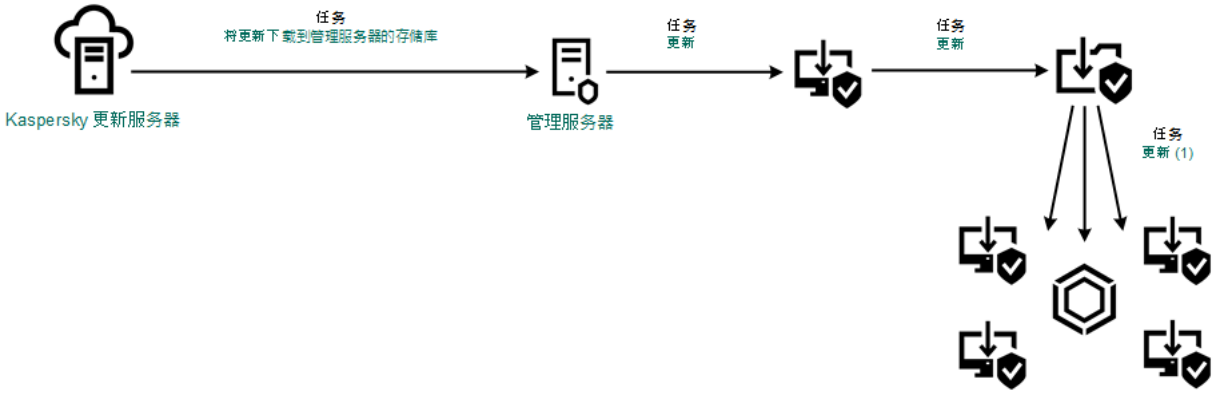
     - 使用 Kaspersky 更新实用程序。有关使用 Kaspersky 更新实用程序的详细信息，请参阅卡巴斯基知识库。

3. 将更新包分发到客户端计算机。

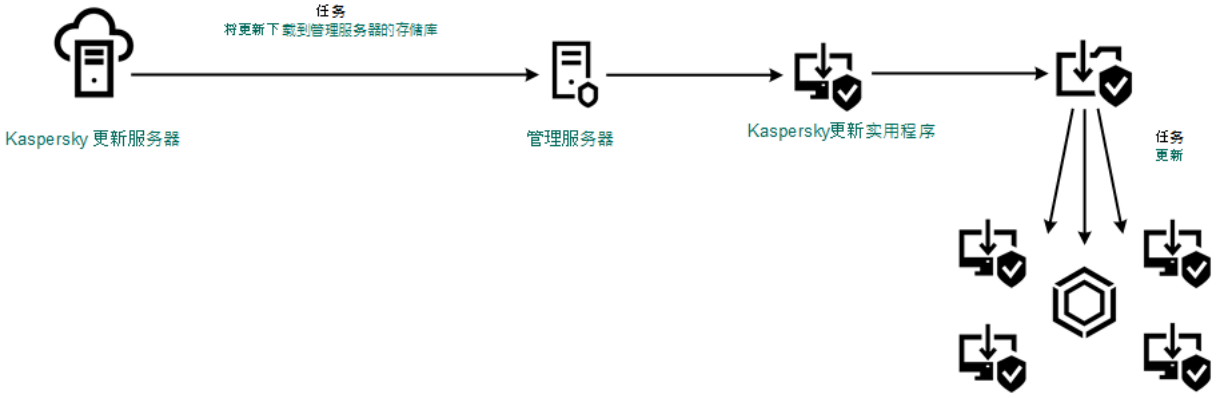
   更新包由 Kaspersky Endpoint Security 的“*数据库和应用程序模块更新*”任务分发到客户端计算机。您可以为每个管理组创建无限数量的更新任务。



从服务器存储库更新



从共享文件夹更新



使用 Kaspersky 更新实用程序更新

对于 Kaspersky Security Center，默认更新源列表包含 Kaspersky Security Center 管理服务器和卡巴斯基更新服务器。对于 Kaspersky Security Center 云控制台，默认更新源列表包含分发点和卡巴斯基更新服务器。有关分发点的详细信息，请参阅 Kaspersky Security Center 云控制台帮助。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。如果无法从一个更新源执行更新，Kaspersky Endpoint Security 会切换到下一个更新源。

更新通过标准网络协议从卡巴斯基更新服务器或其他 FTP 或 HTTP 服务器下载。如果访问更新源需要连接代理服务器，则在 Kaspersky Endpoint Security 策略设置中指定代理服务器设置。

从服务器存储库更新

为了节省 Internet 流量，您可以配置组织的 LAN 中的计算机从服务器存储库更新数据库和应用程序模块。为此，Kaspersky Security Center 必须将更新包从卡巴斯基更新服务器下载到存储库（FTP 或 HTTP 服务器、网络或本地文件夹）。组织的 LAN 中的其他计算机将能够从服务器存储库接收更新包。

配置从服务器存储库更新数据库和应用程序模块包括以下步骤：

1. 配置将更新包下载到管理服务器存储库（“*将更新下载至管理服务器存储库*”任务）。

   “*将更新下载至管理服务器存储库*”任务由管理服务器快速启动向导自动创建，并且此任务可能只有一个实例。默认情况下，Kaspersky Security Center 将更新包复制到文件夹 `\\<server name>\KLSHARE\Updates`。有关将更新下载至管理服务器存储库的详细信息，请参阅 Kaspersky Security Center 帮助。

2. 配置组织的 LAN 中的其余计算机从指定服务器存储库更新数据库和应用程序模块（“*数据库和应用程序模块更新*”任务）。

   如何从管理控制台 (MMC) 中的指定服务器存储配置 Kaspersky Endpoint Security 更新

   1. 打开 Kaspersky Security Center Administration Console。

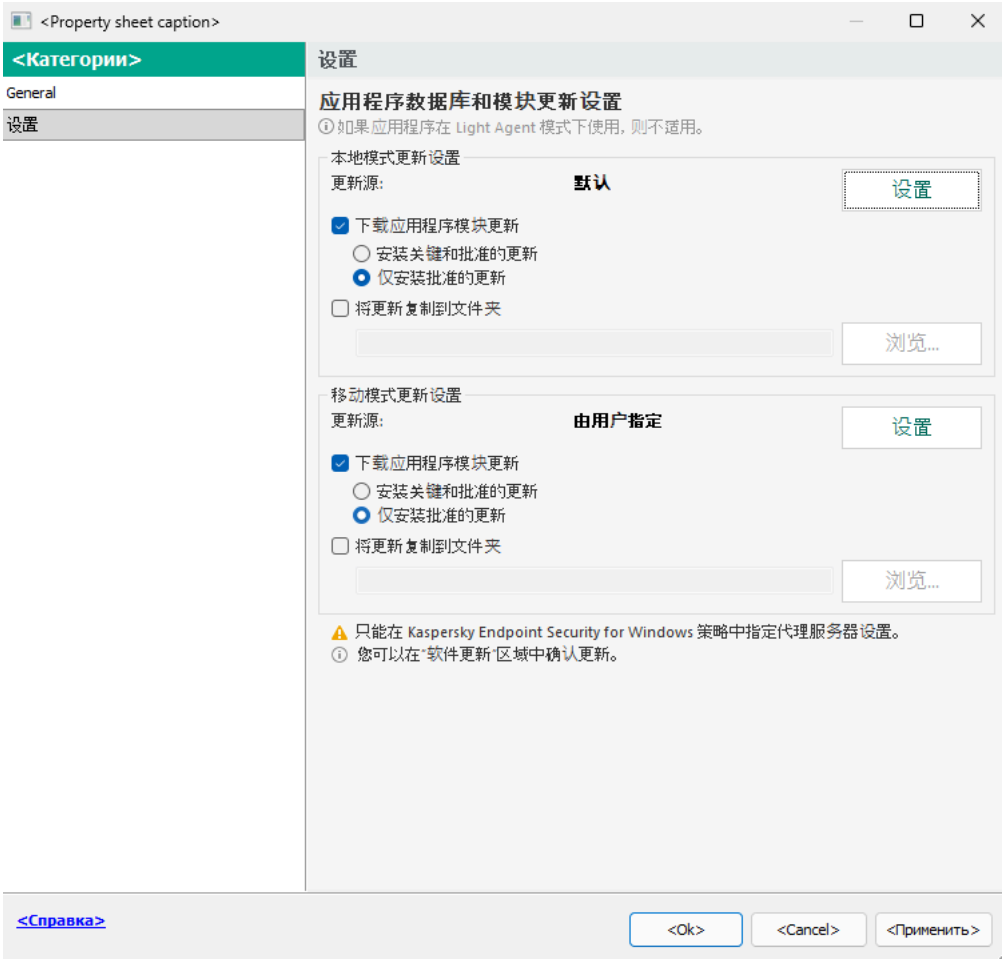
      在控制台树中，选择“**任务**”。

   2. 单击 Kaspersky Endpoint Security 的“**数据库和应用程序模块更新**”任务。

      任务属性窗口将打开。

      “*数据库和应用程序模块更新*”任务由管理服务器快速启动向导自动创建。要创建“*数据库和应用程序模块更新*”任务，请在运行向导时安装 Kaspersky Endpoint Security for Windows Web 插件。

   3. 在任务属性窗口中，选择“**设置**”区域。



数据库和应用程序模块更新 任务设置

   4. 在“**本地模式更新设置**”块中单击“**设置**”按钮。

   5. 在更新源列表中，确保来自“**Kaspersky Security Center**”源的更新已启用。此外，“**Kaspersky Security Center**”源必须具有最高优先级。

6. 如有必要，添加更新源：

   a. 在更新源列表中，单击“**添加**”按钮。

   b. 在“**更新源**”字段中，指定 Kaspersky Security Center 会将接收自 Kaspersky 服务器的更新包复制到的 FTP 或 HTTP 服务器、网络文件夹或者本地文件夹的地址。

   > 更新源的地址必须与您在配置将更新下载到服务器存储库（“*将更新下载至管理服务器存储库*”任务）时在“**更新存储文件夹**”字段中指定的地址匹配。

   c. 单击“**确定**”。

   您可以排除更新源而不将其从更新源列表中删除。为此，清空对象旁边的复选框。

更新来源

7. 使用“**上移**”和“**下移**”按钮配置更新源的优先级。

   如果无法从第一个更新源执行更新，Kaspersky Endpoint Security 会自动切换到下一个更新源。

8. 在任务属性窗口中，选择“**计划**”区域并配置任务运行模式。

9. 默认情况下，Kaspersky Endpoint Security 以手动模式运行任务。

10. 保存更改。

如何从 Web Console 中的指定服务器存储配置 Kaspersky Endpoint Security 更新

1. 在 Web Console 的主窗口中，选择“**任务**”。

   任务列表打开。

2. 单击 Kaspersky Endpoint Security 的“**更新**”任务。

   任务属性窗口将打开。

   “*更新*”任务由管理服务器快速启动向导自动创建。要创建“*更新*”任务，请在运行向导时安装 Kaspersky Endpoint Security for Windows Web 插件。

3. 选择“**应用程序设置**” → “**本地模式**”选项卡。

4. 在更新源列表中，确保来自“**Kaspersky Security Center**”源的更新已启用。此外，“**Kaspersky Security Center**”源必须具有最高优先级。

5. 如有必要，添加更新源：

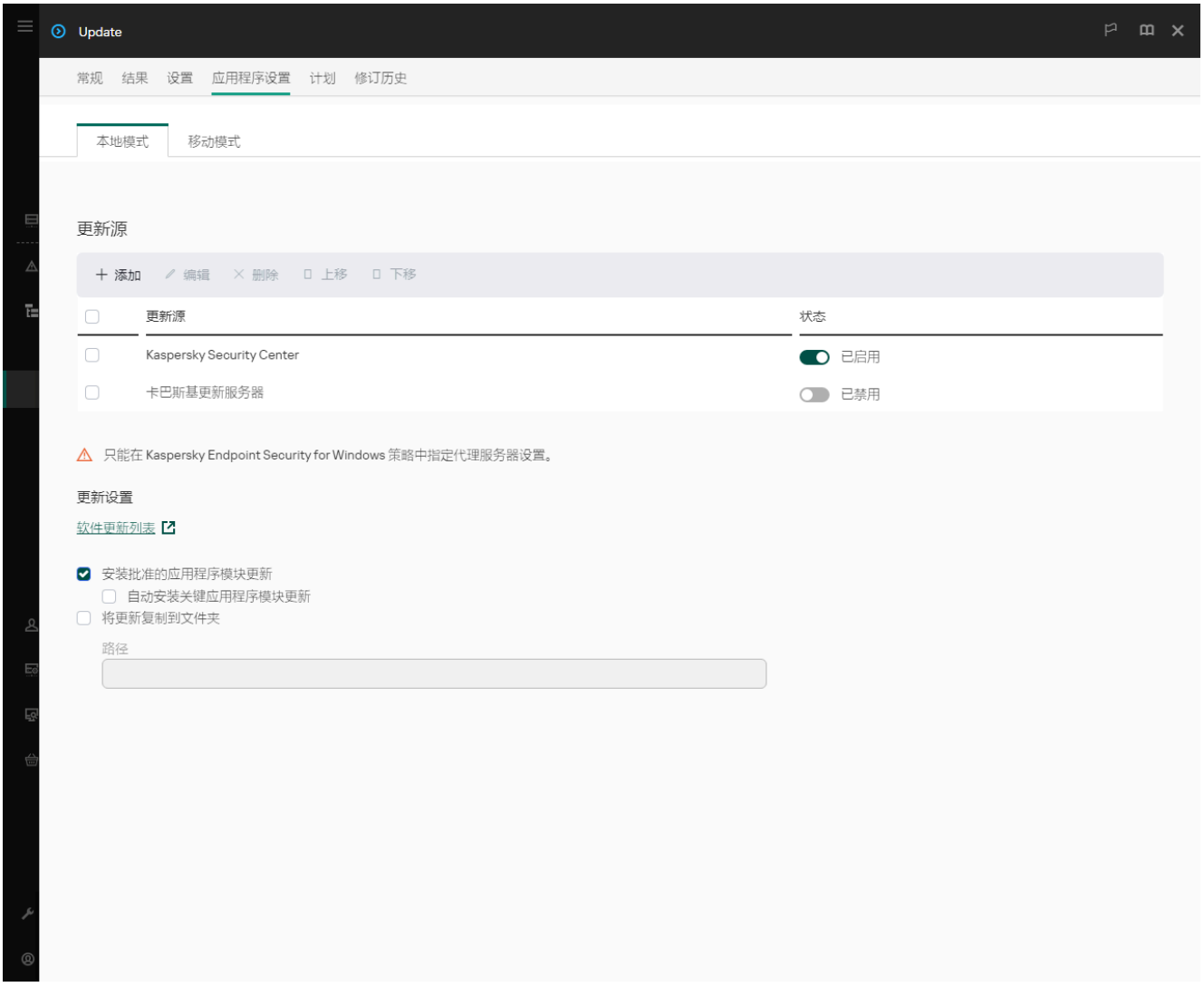
   a. 在更新源列表中，单击“**添加**”按钮。

   b. 在“**更新源**”字段中，指定 Kaspersky Security Center 会将接收自 Kaspersky 服务器的更新包复制到的 FTP 或 HTTP 服务器、网络文件夹或者本地文件夹的地址。

   > 更新源的地址必须与您在配置将更新下载到服务器存储库（“*将更新下载至管理服务器存储库*”任务）时在“**更新存储文件夹**”字段中指定的地址匹配。

   c. 单击“**保存**”。

   您可以排除更新源而不将其从更新源列表中删除。为此，请将其旁边的切换开关设置为关闭位置。



更新来源

6. 使用“**上移**”和“**下移**”按钮配置更新源的优先级。

   如果无法从第一个更新源执行更新，Kaspersky Endpoint Security 会自动切换到下一个更新源。

7. 在任务属性窗口中，选择“**计划**”区域并配置任务运行模式。

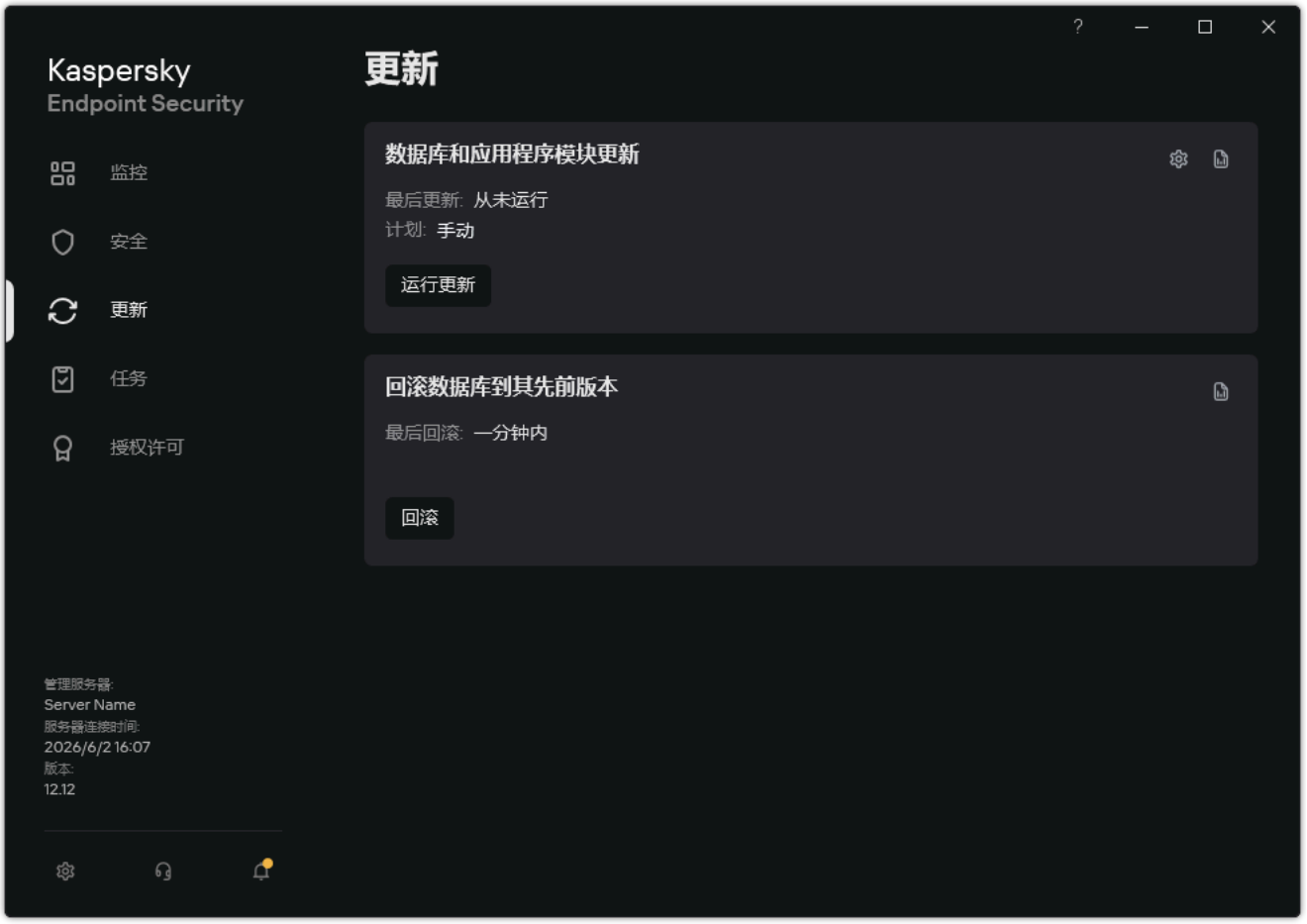
8. 默认情况下，Kaspersky Endpoint Security 以手动模式运行任务。

9. 保存更改。

如何从应用程序界面中的指定服务器存储配置 Kaspersky Endpoint Security 更新

> 您不能在应用程序界面中配置“*数据库和应用程序模块更新*”组任务。只有一个本地更新任务，*数据库和应用程序模块更新*，可供用户使用。如果“*数据库和应用程序模块更新*”任务未显示，这意味着管理员已在策略中禁止对本地任务的使用。

1. 在应用程序主窗口中，转到“**更新**”区域。



本地更新任务

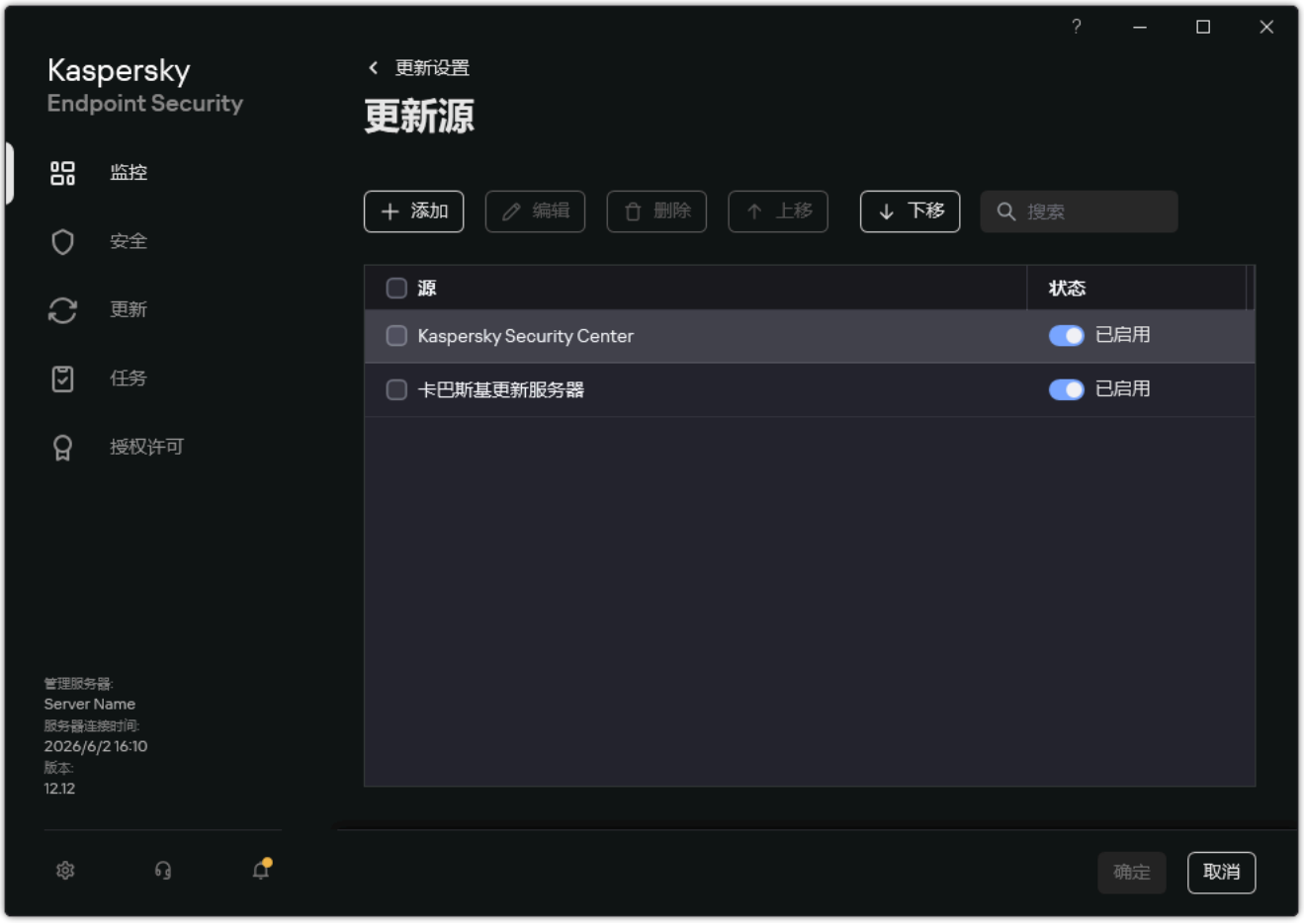
2. 这将打开任务列表；选择“*数据库和应用程序模块更新*”任务并单击 ⚙。
   任务属性窗口将打开。

3. 在任务属性窗口中，请单击“**选择更新源**”。

4. 在更新源列表中，确保来自“**Kaspersky Security Center**”源的更新已启用。此外，“**Kaspersky Security Center**”源必须具有最高优先级。

5. 如有必要，添加更新源：

   a. 在更新源列表中，单击“**添加**”按钮。



更新来源

   a. 指定 Kaspersky Security Center 会将接收自卡巴斯基更新服务器的更新包复制到的 FTP 或 HTTP 服务器、网络文件夹或者本地文件夹的地址。

   > 更新源的地址必须与您在配置将更新下载到服务器存储库（“*将更新下载至管理服务器存储库*”任务）时在“**更新存储文件夹**”字段中指定的地址匹配。

   b. 单击“**选择**”。

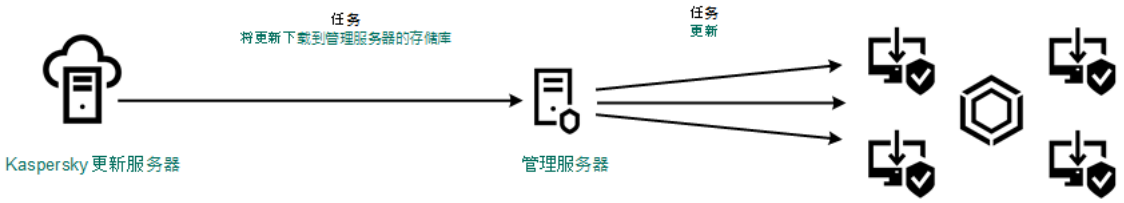
   您可以排除更新源而不将其从更新源列表中删除。为此，请将其旁边的切换开关设置为关闭位置。

6. 使用“**上移**”和“**下移**”按钮配置更新源的优先级。

   如果无法从第一个更新源执行更新，Kaspersky Endpoint Security 会自动切换到下一个更新源。

   > 如果计算机由 Kaspersky Security Center 管理，则无法为“*数据库和应用程序模块更新*”任务配置运行模式。您仅可以手动运行任务。

7. 保存更改。



从服务器存储库更新

从共享文件夹更新

为了节省流量，您可以配置组织的 LAN 中的计算机从共享文件夹更新数据库和应用程序模块。为此，组织的 LAN 中的一台计算机必须从 Kaspersky Security Center 管理服务器或从卡巴斯基更新服务器接收更新包，然后将收到的更新包复制到共享文件夹。组织的 LAN 中的其他计算机将能够从该共享文件夹接收更新包。

将更新包复制到共享文件夹的 Kaspersky Endpoint Security 应用程序的版本和本地化必须与从共享文件夹更新数据库的应用程序的版本和本地化相匹配。如果应用程序的版本或本地化不匹配，数据库更新可能会以错误结束。

配置从共享文件夹更新数据库和应用程序模块包括以下步骤：

1. 配置从服务器存储库进行数据库和应用程序模块更新。

2. 启用将更新包复制到位于本地网络上的一台计算机的共享文件夹中。

   如何在管理控制台（MMC）中启用将更新包复制到共享文件夹

   1. 打开 Kaspersky Security Center Administration Console。

   2. 在控制台树中，选择“**任务**”。

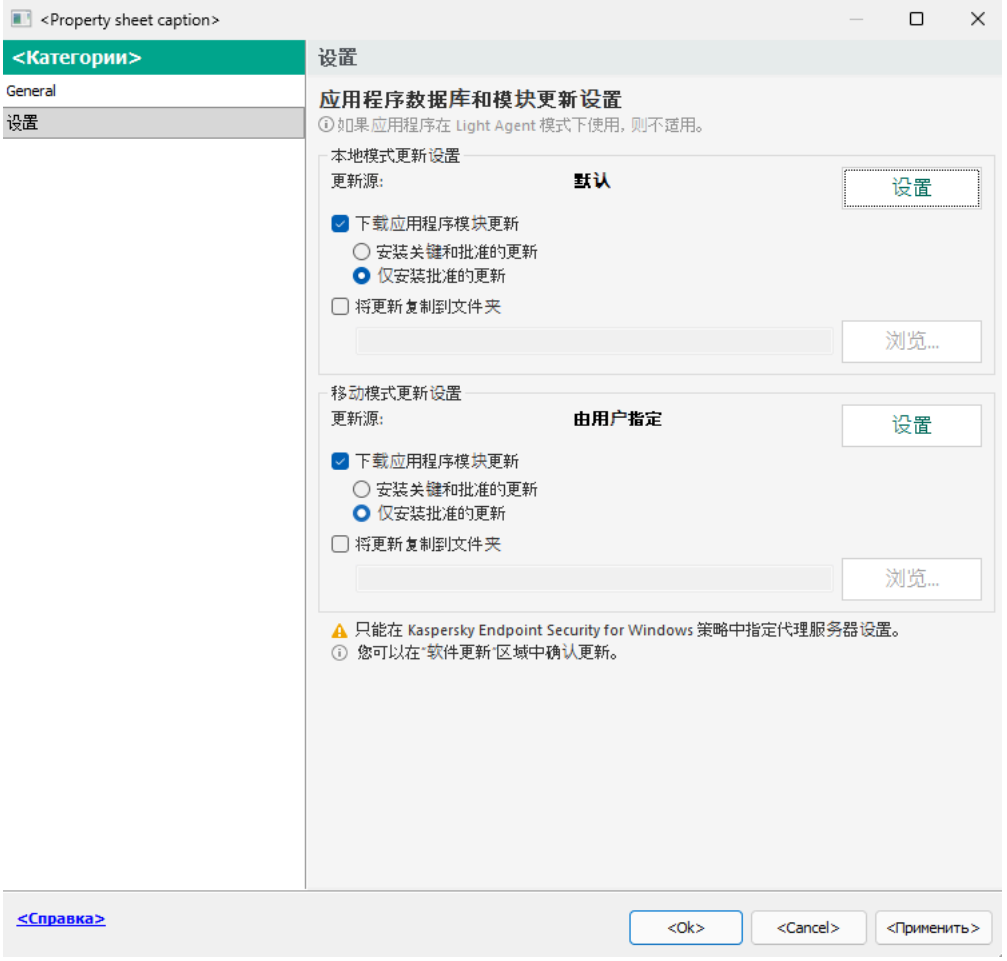
      必须为将用作更新源的计算机分配“*数据库和应用程序模块更新*”任务。

   3. 单击 Kaspersky Endpoint Security 的“**数据库和应用程序模块更新**”任务。

      任务属性窗口将打开。

      “*数据库和应用程序模块更新*”任务由管理服务器快速启动向导自动创建。要创建“*数据库和应用程序模块更新*”任务，请在运行向导时安装 Kaspersky Endpoint Security for Windows Web 插件。

4. 在任务属性窗口中，选择“**设置**”区域。



数据库和应用程序模块更新 任务设置

5. 在“**本地模式更新设置**”块中单击“**设置**”按钮。

6. 配置更新源。

   更新源可以是卡巴斯基更新服务器、Kaspersky Security Center 管理服务器、其他 FTP 或 HTTP 服务器、本地文件夹或网络文件夹。

7. 选择**将更新复制到文件夹**复选框。

8. 在“**文件夹路径**”字段中，输入共享文件夹的 UNC 路径（例如，`\\<server name>\KLSHARE\Updates`）。

   如果将该字段留空，Kaspersky Endpoint Security 会将更新包复制到文件夹 `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`。

9. 保存更改。

如何在 Web Console 和云控制台中启用将更新包复制到共享文件夹

1. 在 Web Console 的主窗口中，选择“**任务**”。

   任务列表打开。

   > 必须为将用作更新源的计算机分配“*更新*”任务。

2. 单击 Kaspersky Endpoint Security 的“**更新**”任务。

   任务属性窗口将打开。

“*更新*”任务由管理服务器快速启动向导自动创建。要创建“*更新*”任务，请在运行向导时安装 Kaspersky Endpoint Security for Windows Web 插件。

3. 选择“**应用程序设置**” → “**本地模式**”选项卡。

4. 配置更新源。

   更新源可以是卡巴斯基更新服务器、Kaspersky Security Center 管理服务器、其他 FTP 或 HTTP 服务器、本地文件夹或网络文件夹。

5. 选择**将更新复制到文件夹**复选框。

6. 在“**路径**”字段中，输入共享文件夹的 UNC 路径（例如，`\\<server name>\KLSHARE\Updates`）。

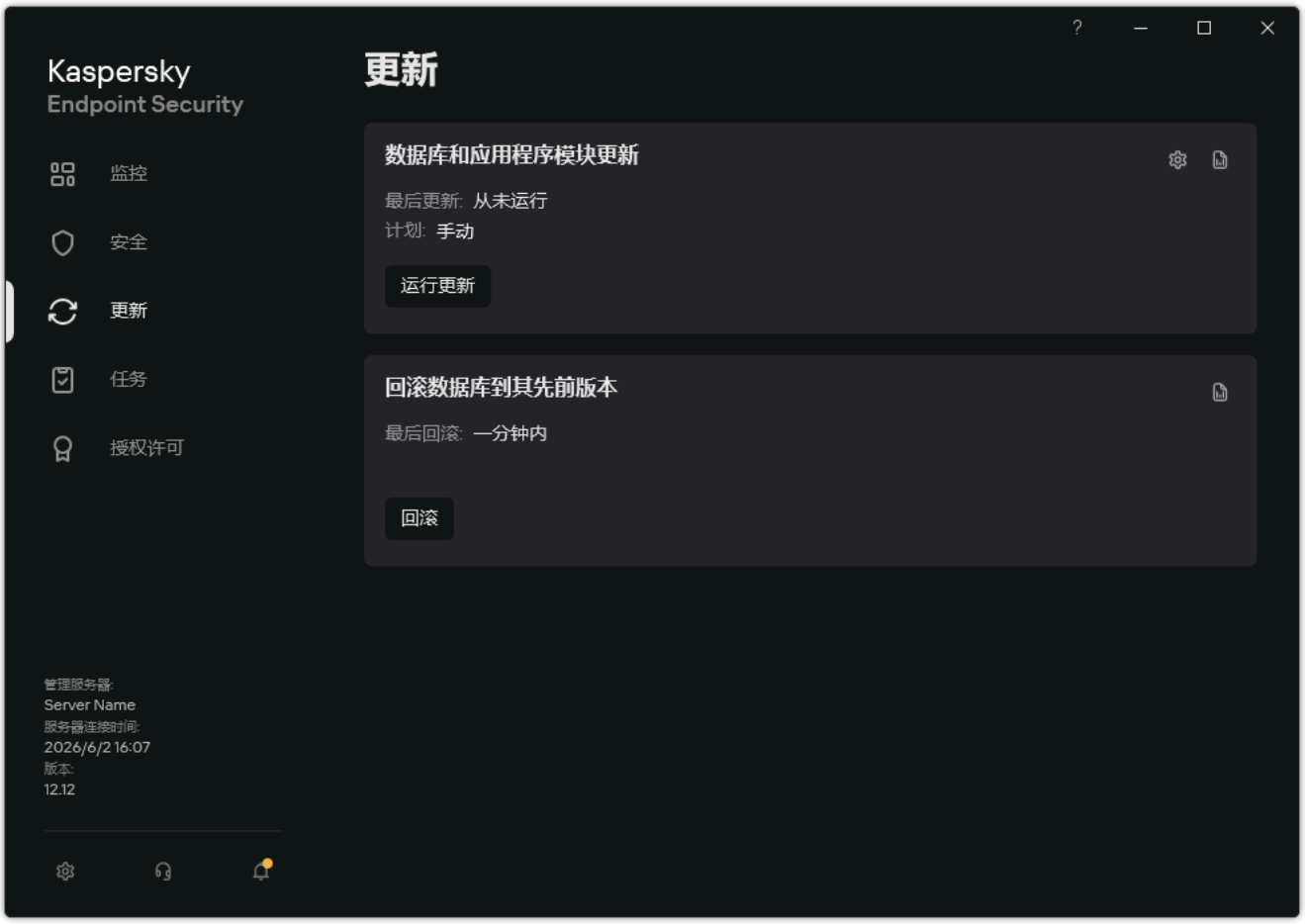
   如果将该字段留空，Kaspersky Endpoint Security 会将更新包复制到文件夹 `C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`。

7. 保存更改。

如何在应用程序界面中启用将更新包复制到共享文件夹

> 您不能在应用程序界面中配置“*数据库和应用程序模块更新*”组任务。只有一个本地更新任务，*数据库和应用程序模块更新*，可供用户使用。如果“*数据库和应用程序模块更新*”任务未显示，这意味着管理员已在策略中禁止对本地任务的使用。

1. 在应用程序主窗口中，转到“**更新**”区域。



本地更新任务

2. 这将打开任务列表；选择“*数据库和应用程序模块更新*”任务并单击 ⚙。

   任务属性窗口将打开。

3. 在“**分发更新**”块中，选中“**将更新复制到文件夹**”复选框。

4. 输入共享文件夹的 UNC 路径（例如，`\\<server name>\KLSHARE\Updates`）。

5. 保存更改。

3. 配置组织的 LAN 中的其余计算机从指定共享文件夹更新数据库和应用程序模块。

如何在管理控制台（MMC）中配置从共享文件夹更新

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。

2. 单击“**添加**”。
   “任务向导”将启动。

3. 配置任务设置：

   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Endpoint Security for Windows 14.2.0**”。

   b. 在“**任务类型**”下拉列表中，选择“**数据库和应用程序模块更新**”。

4. 在 Kaspersky Security Center 管理控制台树中，选择“**任务**”。
   任务列表打开。

5. 单击“**新任务**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 选择任务类型

选择“**Kaspersky Endpoint Security for Windows (14.1)**”→ “**数据库和应用程序模块更新**”。

步骤 2. 选择更新源

添加新的更新源：共享文件夹。源地址必须与您之前配置将更新包复制到共享文件夹时在“**文件夹路径**”字段中指定的地址相匹配。使用“**上移**”和“**下移**”按钮配置更新源的优先级。

步骤 3. 选择任务将分配到的设备

选择将要执行任务的计算机。下列选项可用：

- 将任务分配给管理组。在这种情况下，任务分配给先前创建的管理组中包括的计算机。
- 选择管理服务器在网络中检测到的计算机：*未分配设备*。特定设备可包括管理组中的设备以及未分配设备。
- 手动指定设备地址或从列表中导入地址。您可以指定您要将任务分配给的设备的 NetBIOS 名称、IP 地址和 IP 子网。

> 必须为组织的 LAN 中除用作更新源的计算机之外的计算机分配"*数据库和应用程序模块更新*"任务。

步骤 4. 选择要运行任务的账户

选择要运行*数据库和应用程序模块更新*任务的账户。默认情况下，Kaspersky Endpoint Security 将使用本地用户账户的权限启动任务。

步骤 5. 配置任务启动计划

配置任务启动计划，例如，手动或在将反病毒数据库下载到存储库之后。

步骤 6. 定义任务名称

输入任务的名称，例如*从共享文件夹更新*。

步骤 7. 完成任务创建

退出向导。如有必要，选中"**向导完成时运行任务**"复选框。您可以在任务属性中监控任务进度。结果，将根据指定计划在用户计算机上执行更新任务。

如何在 Web Console 和云控制台中配置从共享文件夹更新

1. 在 Web Console 的主窗口中，选择"**任务**"。

   任务列表打开。

2. 单击"**添加**"。

   "任务向导"将启动。

3. 配置任务设置：

   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Endpoint Security for Windows 14.2.0**”。

   b. 在“**任务类型**”下拉列表中，选择“**更新**”。

   c. 在“**任务名称**”字段中，输入简要说明，例如，“*从共享文件夹更新*”。

   d. 在“**要对其分配任务的设备**”块，选择任务范围。

   > 必须为组织的 LAN 中除用作更新源的计算机之外的计算机分配“*更新*”任务。

4. 按照所选任务范围选项选择设备，然后转到下一步。

5. 退出向导。
   在任务表中将显示一个新任务。

6. 单击新创建的“*更新*”任务。
   任务属性窗口将打开。

7. 选择“**应用程序设置**” → “**本地模式**”选项卡。

8. 在“**更新源**”块中单击“**添加**”按钮。

9. 在打开的窗口中，输入共享文件夹的路径。

   > 源地址必须与您之前配置将更新包复制到共享文件夹时在“**路径**”字段中指定的地址相匹配（请参见上述说明）。

10. 单击“**确定**”。

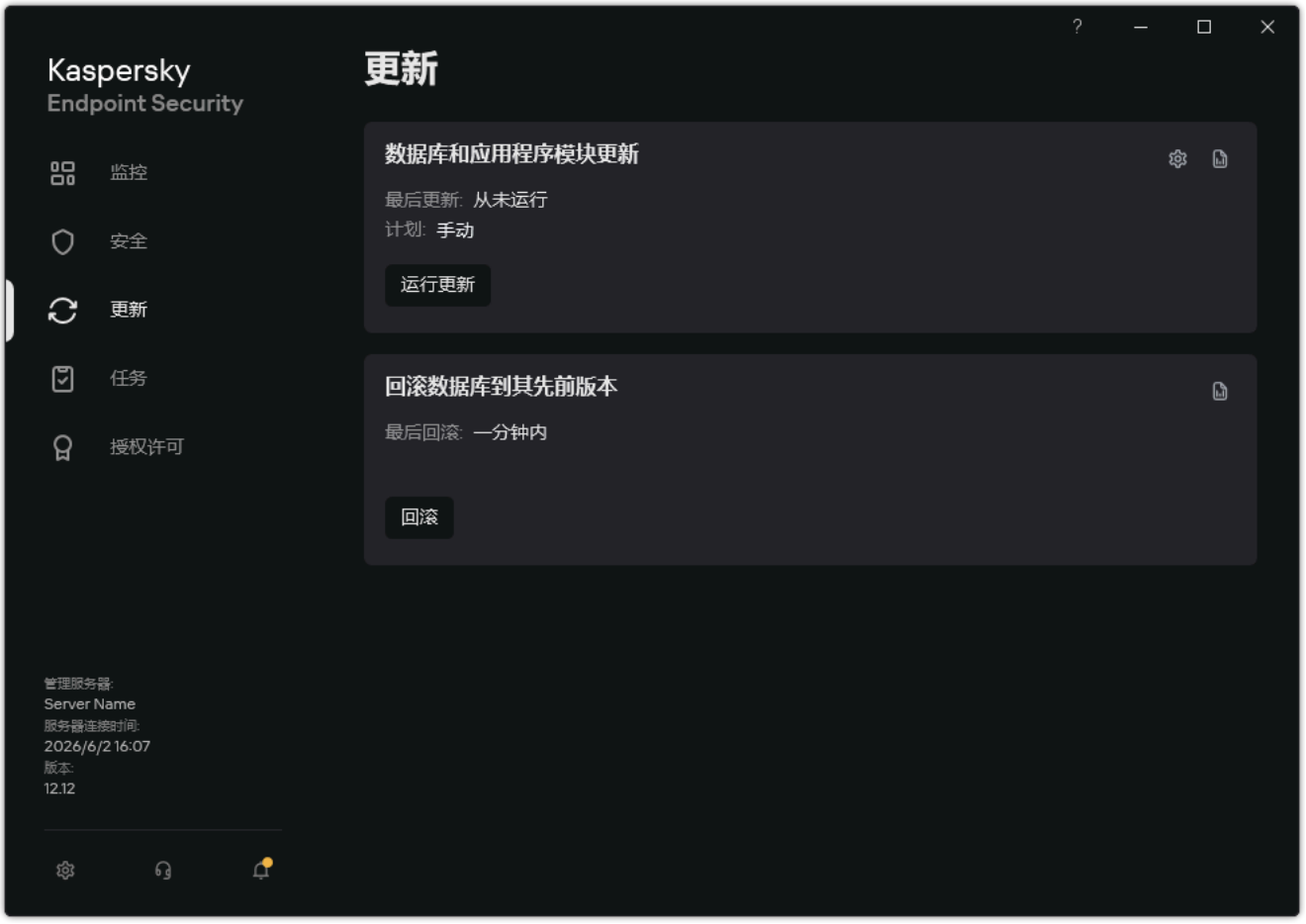
11. 使用“**上移**”和“**下移**”按钮配置更新源的优先级。

12. 保存更改。

如何在应用程序界面中配置从共享文件夹更新

> 您不能在应用程序界面中配置“*数据库和应用程序模块更新*”组任务。只有一个本地更新任务，*数据库和应用程序模块更新*，可供用户使用。如果“*数据库和应用程序模块更新*”任务未显示，这意味着管理员已在策略中禁止对本地任务的使用。

1. 在应用程序主窗口中，转到“**更新**”区域。



本地更新任务

2. 这将打开任务列表；选择“*数据库和应用程序模块更新*”任务并单击 ⚙。
   任务属性窗口将打开。

3. 单击“**选择更新源**”。

4. 在打开的窗口中，单击“**添加**”按钮。

5. 在打开的窗口中，输入共享文件夹的路径。

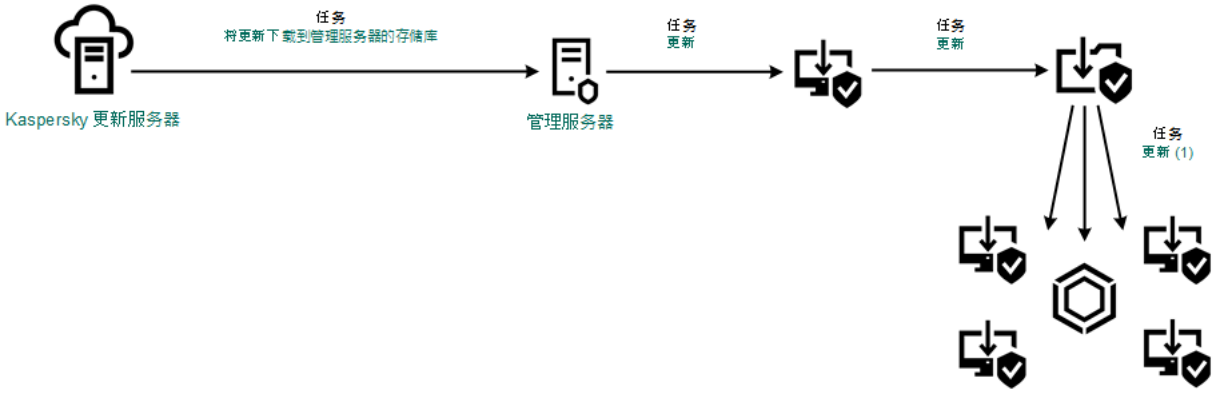
   > 源地址必须与您之前在配置将更新包复制到共享文件夹时指定的地址相匹配（请参见上述说明）。

6. 单击“**选择**”。

7. 使用“**上移**”和“**下移**”按钮配置更新源的优先级。

   如果无法从第一个更新源执行更新，Kaspersky Endpoint Security 会自动切换到下一个更新源。

8. 保存更改。



从共享文件夹更新

使用 Kaspersky 更新实用程序更新

为了节省 Internet 流量，您可以使用 Kaspersky 更新实用程序配置从共享文件夹更新组织 LAN 中的计算机上的数据库和应用程序模块。为此，组织的 LAN 中的一台计算机必须从 Kaspersky Security Center 管理服务器或从卡巴斯基更新服务器接收更新包，然后使用实用程序将收到的更新包复制到共享文件夹。组织的 LAN 中的其他计算机将能够从该共享文件夹接收更新包。

> 将更新包复制到共享文件夹的 Kaspersky Endpoint Security 应用程序的版本和本地化必须与从共享文件夹更新数据库的应用程序的版本和本地化相匹配。如果应用程序的版本或本地化不匹配，数据库更新可能会以错误结束。

配置从共享文件夹更新数据库和应用程序模块包括以下步骤：

1. 配置从服务器存储库进行数据库和应用程序模块更新。

2. 在组织的 LAN 的一台计算机上安装 Kaspersky 更新实用程序。

3. 在 Kaspersky 更新实用程序设置中配置将更新包复制到共享文件夹。

   您可以从 Kaspersky 技术支持网站 下载 Kaspersky 更新实用程序分发包。安装该实用程序后，选择更新源（例如，管理服务器存储库）和 Kaspersky 更新实用程序将更新包复制到的共享文件夹。有关使用 Kaspersky 更新实用程序的详细信息，请参阅卡巴斯基知识库 。

4. 配置组织的 LAN 中的其余计算机从指定共享文件夹更新数据库和应用程序模块。

   如何在管理控制台（MMC）中配置从共享文件夹更新

   1. 打开 Kaspersky Security Center Administration Console。

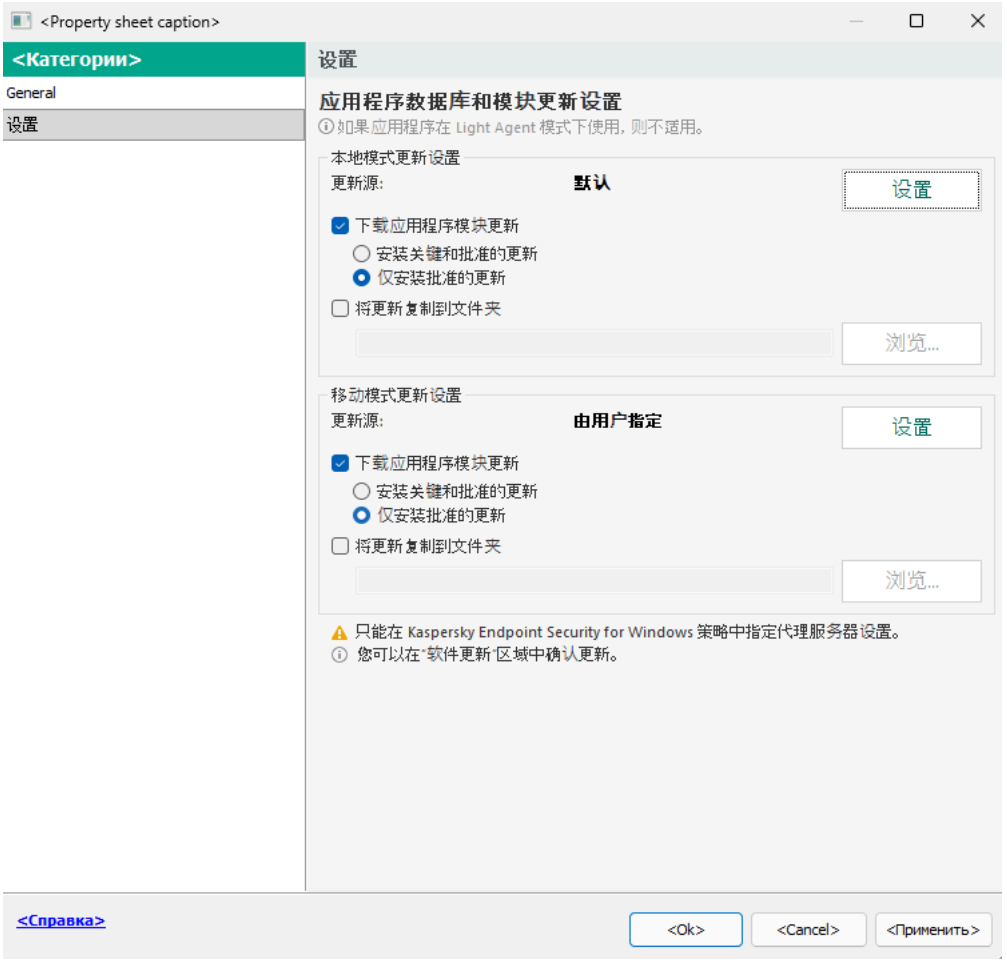
   2. 在控制台树中，选择“**任务**”。

   3. 单击 Kaspersky Endpoint Security 的“**数据库和应用程序模块更新**”任务。

      任务属性窗口将打开。

“*数据库和应用程序模块更新*”任务由管理服务器快速启动向导自动创建。要创建“*数据库和应用程序模块更新*”任务，请在运行向导时安装 Kaspersky Endpoint Security for Windows Web 插件。

4. 在任务属性窗口中，选择“**设置**”区域。



数据库和应用程序模块更新 任务设置

5. 在“**本地模式更新设置**”块中单击“**设置**”按钮。

6. 在更新源列表中，单击“**添加**”按钮。

7. 在打开的窗口中，输入共享文件夹的 UNC 路径（例如，`\\<server name>\KLSHARE\Updates`）。

   源地址必须与 Kaspersky 更新实用程序设置中指示的地址匹配。

8. 单击“**确定**”。

9. 使用“**上移**”和“**下移**”按钮配置更新源的优先级。
   如果无法从第一个更新源执行更新，Kaspersky Endpoint Security 会自动切换到下一个更新源。

10. 保存更改。

如何在 Web Console 和云控制台中配置从共享文件夹更新

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。

2. 单击 Kaspersky Endpoint Security 的“**更新**”任务。

任务属性窗口将打开。

“*更新*”任务由管理服务器快速启动向导自动创建。要创建“*更新*”任务，请在运行向导时安装 Kaspersky Endpoint Security for Windows Web 插件。

3. 选择“**应用程序设置**” → “**本地模式**”选项卡。

4. 在更新源列表中，单击“**添加**”按钮。

5. 在打开的窗口中，输入共享文件夹的 UNC 路径（例如，`\\<server name>\KLSHARE\Updates`）。

   源地址必须与 Kaspersky 更新实用程序设置中指示的地址匹配。

6. 单击“**确定**”。

7. 使用“**上移**”和“**下移**”按钮配置更新源的优先级。

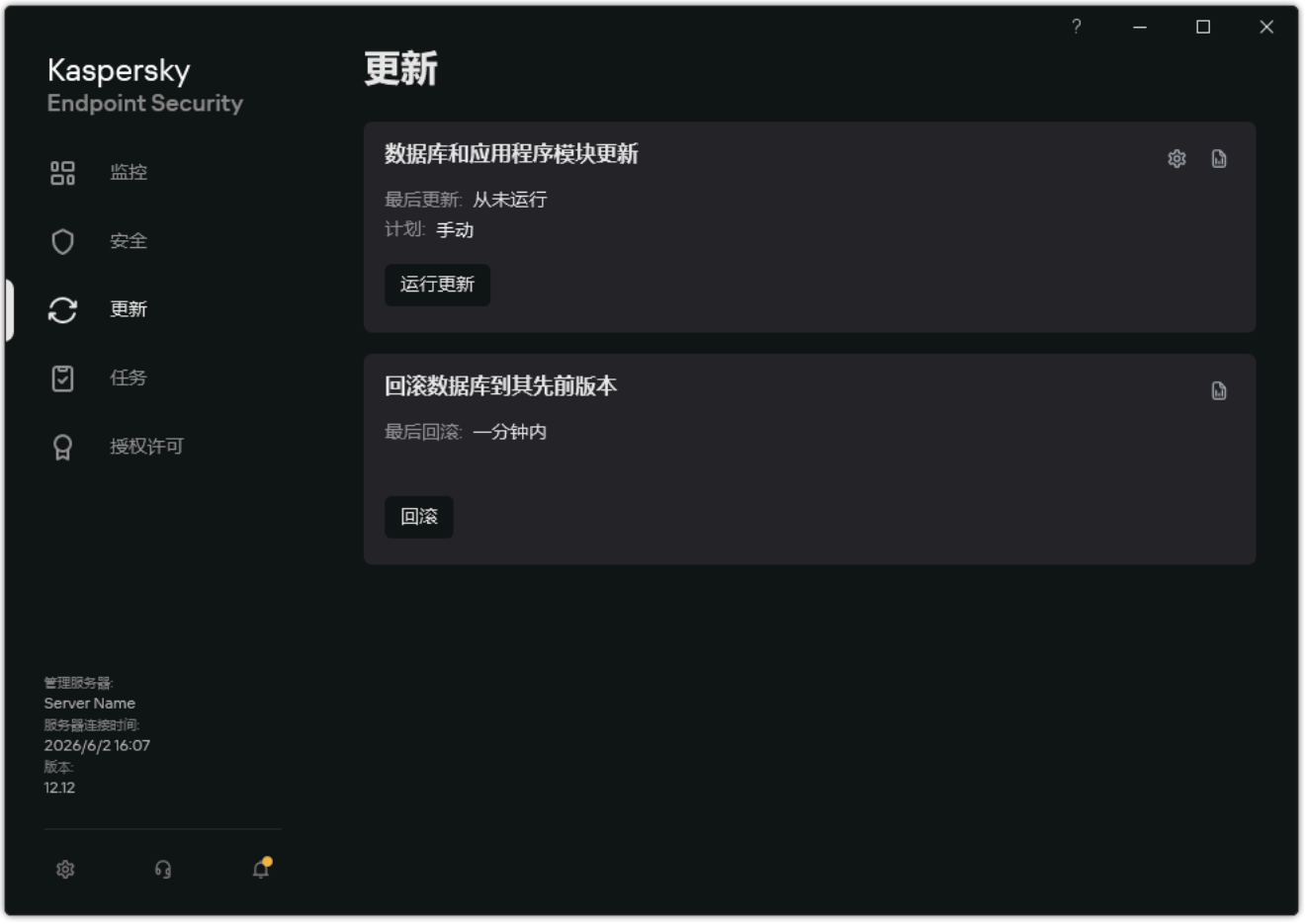
   如果无法从第一个更新源执行更新，Kaspersky Endpoint Security 会自动切换到下一个更新源。

8. 保存更改。

如何在应用程序界面中配置从共享文件夹更新

您不能在应用程序界面中配置“数据库和应用程序模块更新”组任务。只有一个本地更新任务，数据库和应用程序模块更新，可供用户使用。如果“数据库和应用程序模块更新”任务未显示，这意味着管理员已在策略中禁止对本地任务的使用。

1. 在应用程序主窗口中，转到“**更新**”区域。

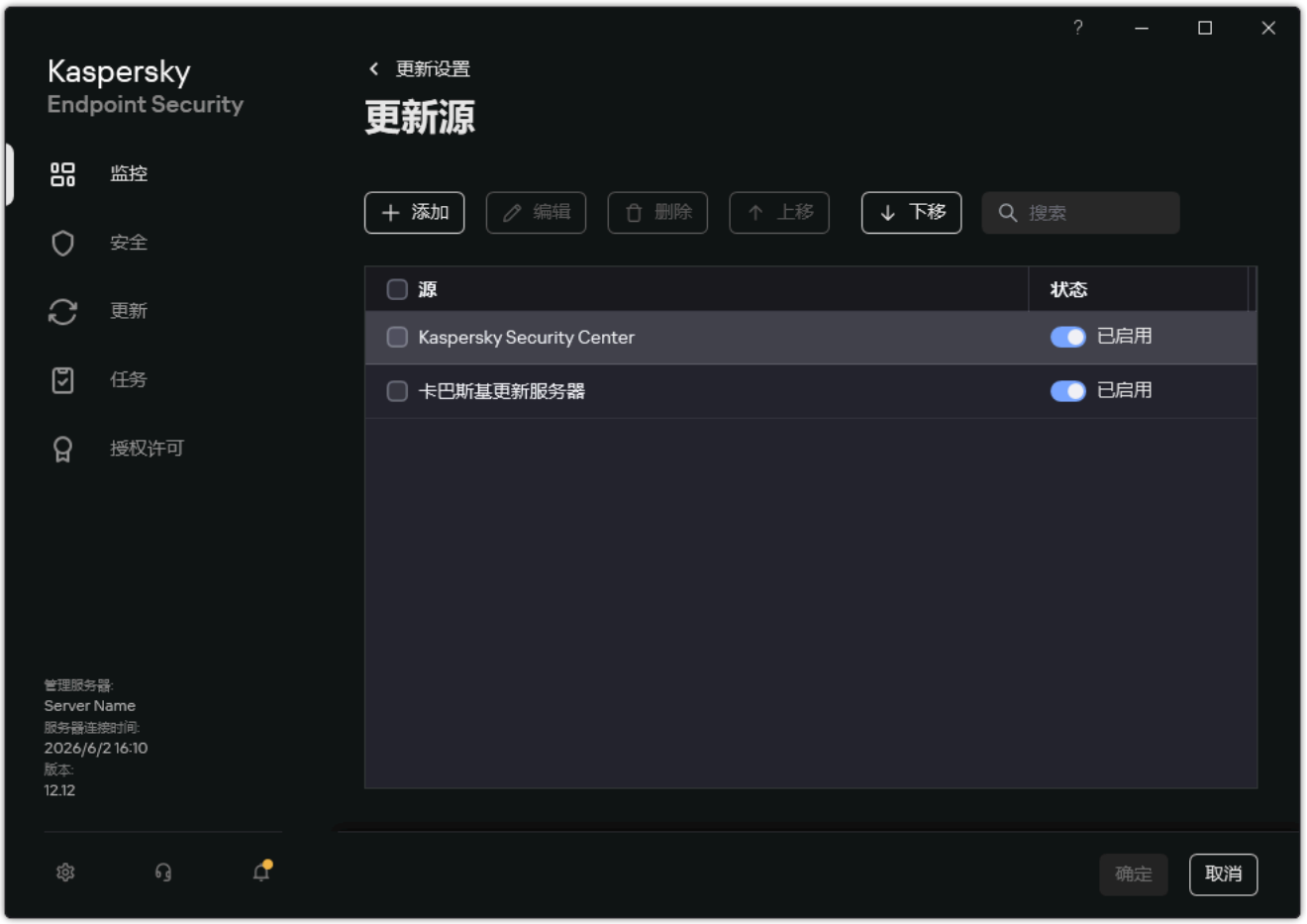


本地更新任务

2. 这将打开任务列表；选择“*数据库和应用程序模块更新*”任务并单击 ⚙。
   任务属性窗口将打开。

3. 在任务属性窗口中，请单击“**选择更新源**”。

4. 在更新源列表中，单击“**添加**”按钮。



更新来源

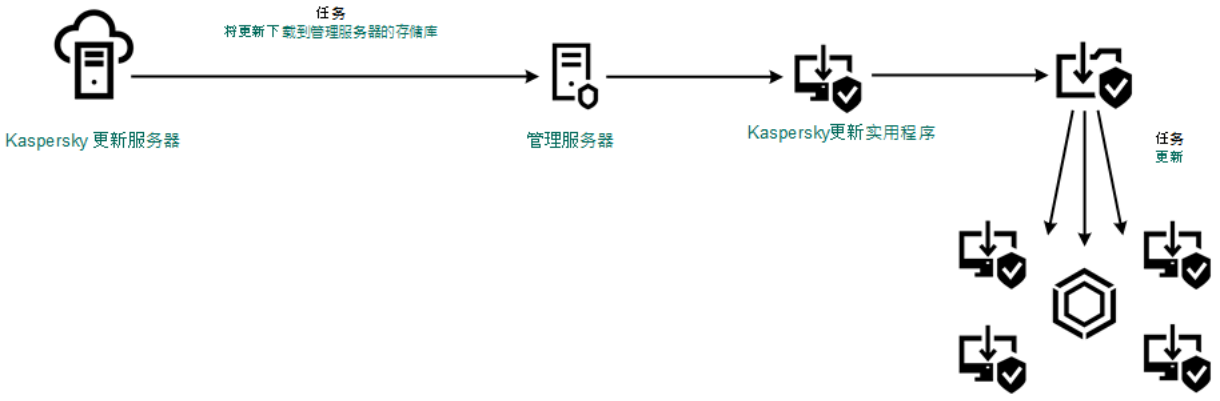
5. 输入共享文件夹的 UNC 路径（例如，`\\<server name>\KLSHARE\Updates`）。

> 源地址必须与 Kaspersky 更新实用程序设置中指示的地址匹配。

6. 单击“**选择**”。

7. 使用“**上移**”和“**下移**”按钮配置更新源的优先级。
   如果无法从第一个更新源执行更新，Kaspersky Endpoint Security 会自动切换到下一个更新源。

8. 保存更改。



使用 Kaspersky 更新实用程序更新

在移动模式下更新

*移动模式*是计算机离开组织网络周界（*离线计算机*）时 Kaspersky Endpoint Security 的运行模式。有关使用离线计算机以及与漫游用户一起工作的详细信息，请参阅 Kaspersky Security Center 帮助。

组织网络外部的离线计算机无法连接到管理服务器来更新数据库和应用程序模块。默认情况下，只有卡巴斯基更新服务器用作移动模式下更新数据库和应用程序模块的更新源。是否使用代理服务器连接到 Internet 由特殊漫游策略确定。漫游策略必须单独创建。当 Kaspersky Endpoint Security 切换到移动模式后，更新任务每两小时启动一次。

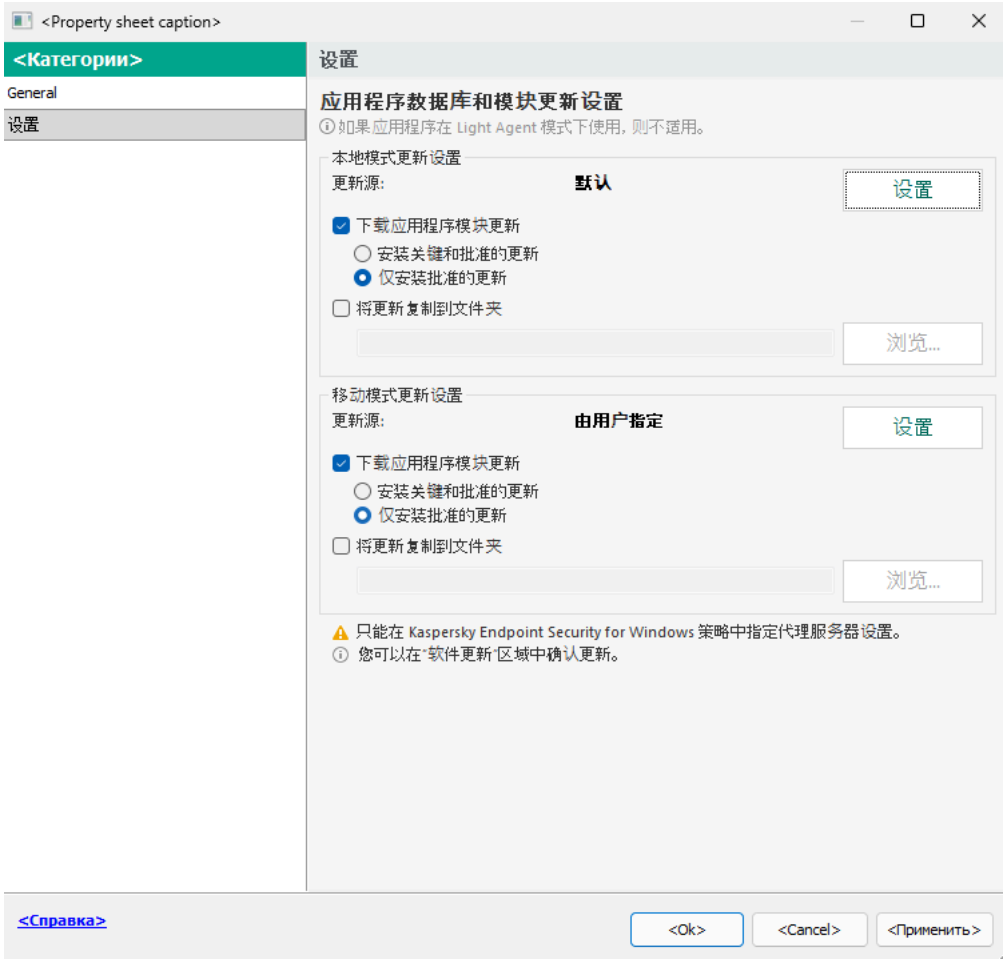
如何在管理控制台（MMC）中配置移动模式更新设置

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**任务**”。
3. 单击 Kaspersky Endpoint Security 的“**数据库和应用程序模块更新**”任务。

   任务属性窗口将打开。

   “*数据库和应用程序模块更新*”任务由管理服务器快速启动向导自动创建。要创建“*数据库和应用程序模块更新*”任务，请在运行向导时安装 Kaspersky Endpoint Security for Windows Web 插件。

4. 在任务属性窗口中，选择“**设置**”区域。



数据库和应用程序模块更新 任务设置

5. 在“**移动模式更新设置**”块中单击“**设置**”按钮。

6. 配置更新源。更新源可以是卡巴斯基更新服务器、其他 FTP 和 HTTP 服务器、本地文件夹或网络文件夹。

7. 保存更改。

如何在 Web Console 和云控制台中配置移动模式的更新设置

1. 在 Web Console 的主窗口中，选择“**任务**”。

   任务列表打开。

2. 单击 Kaspersky Endpoint Security 的“**更新**”任务。

   任务属性窗口将打开。

   “*更新*”任务由管理服务器快速启动向导自动创建。要创建“*更新*”任务，请在运行向导时安装 Kaspersky Endpoint Security for Windows Web 插件。

3. 选择“**应用程序设置**” → “**移动模式**”选项卡。

4. 配置更新源。更新源可以是卡巴斯基更新服务器、其他 FTP 和 HTTP 服务器、本地文件夹或网络文件夹。

5. 保存更改。

结果，当用户计算机切换到移动模式时，数据库和应用程序模块将获得更新。

开始和停止更新任务

无论选定的更新任务运行模式是什么，您都可以随时启动或停止 Kaspersky Endpoint Security 更新任务。

要启动或停止更新任务，请执行以下操作：

1. 在应用程序主窗口中，转到“**更新**”区域。
2. 在“**数据库和应用程序模块更新**”块，单击“**更新**”按钮以开始更新任务。

   Kaspersky Endpoint Security 将开始更新应用程序模块和数据库。应用程序将显示任务进度、已下载文件大小和更新源。您可以通过单击**停止更新**按钮随时停止任务。

要在显示简化的应用程序界面时启动或停止更新任务：

1. 在任务栏通知区域右键单击程序图标，调出上下文菜单中。
2. 在上下文菜单中的“**任务**”下拉列表中，执行以下操作之一：
   - 选择未运行的更新任务以将其启动
   - 选择正在运行的更新任务以将其停止
   - 选择暂停的更新任务以将其恢复或重新启动

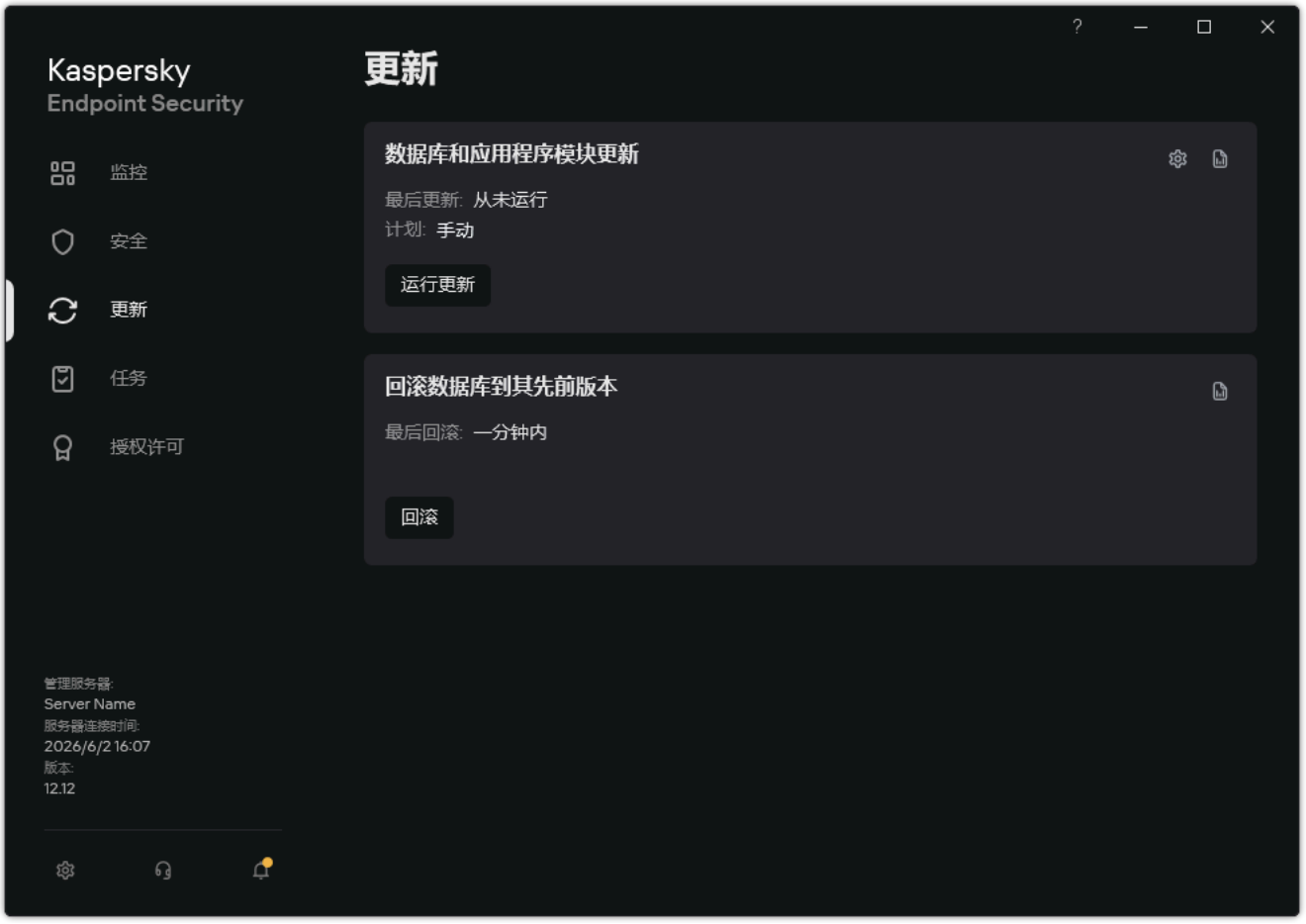
在不同用户帐户权限下开始更新任务

默认情况下，Kaspersky Endpoint Security 使用您用来登陆操作系统的帐户执行更新任务。但是，Kaspersky Endpoint Security 可以从用户没有访问权限的更新源（例如，含有更新包的共享文件夹）进行更新，或者从没有配置过代理服务器身份验证的更新源进行更新。在应用程序设置中，您可以指定一个拥有以上权限的用户，然后使用该用户帐户开始 Kaspersky Endpoint Security 更新任务。

要使用不同的用户帐户开始更新任务，请执行以下操作：

> 您不能在应用程序界面中配置“*数据库和应用程序模块更新*”组任务。只有一个本地更新任务，*数据库和应用程序模块更新*，可供用户使用。如果“*数据库和应用程序模块更新*”任务未显示，这意味着管理员已在策略中禁止对本地任务的使用。

1. 在应用程序主窗口中，转到“**更新**”区域。



本地更新任务

2. 这将打开任务列表；选择“*数据库和应用程序模块更新*”任务并单击 ⚙。
   任务属性窗口将打开。

3. 单击“**以用户权限运行数据库更新**”。

4. 在打开的窗口中，选择“**其他用户**”。

5. 输入具有访问更新源必要权限的用户的账户凭证。

6. 保存更改。

选择更新任务运行模式

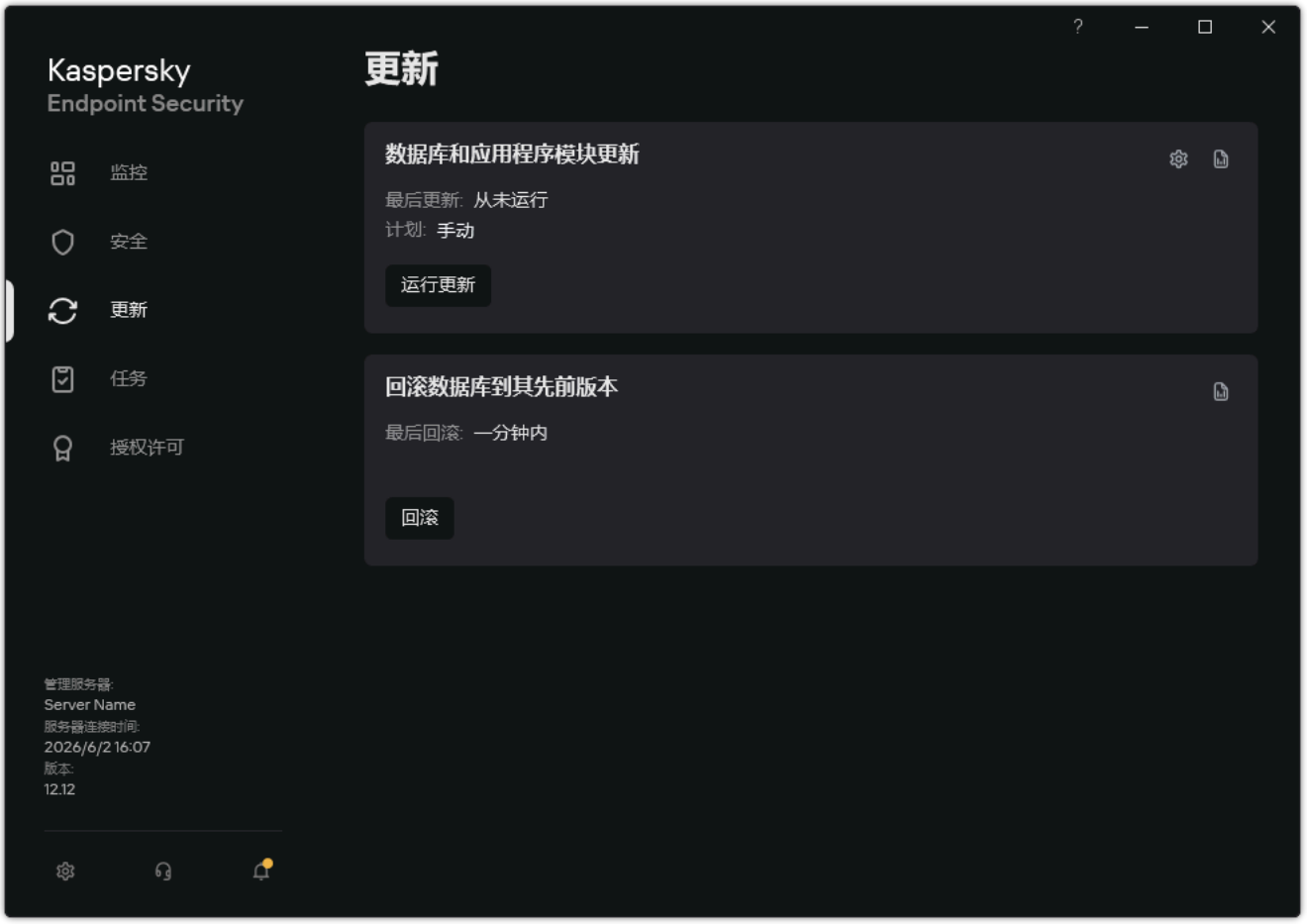
如果出于任何原因无法运行更新任务（例如，计算机当时没有打开），您可以配置被跳过的任务在可能执行时立即自动开始。

如果您选择了“**根据计划**”更新任务运行模式，而且 Kaspersky Endpoint Security 的启动时间与更新任务启动计划相匹配，您可以在程序启动后推迟更新任务的启动。更新任务只能在 Kaspersky Endpoint Security 启动后经过特定时间间隔后运行。

要选择更新任务运行模式，请执行以下操作：

> 您不能在应用程序界面中配置“*数据库和应用程序模块更新*”组任务。只有一个本地更新任务，*数据库和应用程序模块更新*，可供用户使用。如果“*数据库和应用程序模块更新*”任务未显示，这意味着管理员已在策略中禁止对本地任务的使用。

1. 在应用程序主窗口中，转到“**更新**”区域。



本地更新任务

2. 这将打开任务列表；选择“*数据库和应用程序模块更新*”任务并单击 ⚙。

   任务属性窗口将打开。

3. 单击“**运行模式**”。

4. 在打开的窗口中，选择更新任务运行模式：

   - 如果您希望 Kaspersky Endpoint Security 根据是否能够从更新源获取更新包来运行更新任务，请选择“**自动**”。Kaspersky Endpoint Security 检查更新包的频率在病毒爆发时会增加，在其他时候会减少。

   - 如果您希望手动开始更新任务，请选择“**手动**”。

- 如果您希望为更新任务配置一个启动计划，请选择其他选项。为更新任务启动配置高级设置：
  - 在“**在应用程序启动此时间后延迟运行 N 分钟**”字段中，指定更新任务在 Kaspersky Endpoint Security 启动后的开始时间间隔。
  - 如果您想让 Kaspersky Endpoint Security 优先运行略过的更新任务，选择**计算机关闭时，在第二天运行计划扫描**。当应用程序有机会执行略过的任务时，它会在一定的时间间隔内随机运行任务，以分配计算机上的负载。

5. 保存更改。

添加更新源

*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。

> 如果卡巴斯基更新服务器不可用，Kaspersky Endpoint Security 可以使用备用域来更新其数据库和应用程序软件模块。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“*数据库和应用程序模块更新*”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。

> 如果应用程序正在 Light Agent 模式下运行，一个 SVM 上的文件夹选为更新源。

如何在管理控制台（MMC）中添加更新源

1. 打开 Kaspersky Security Center Administration Console。

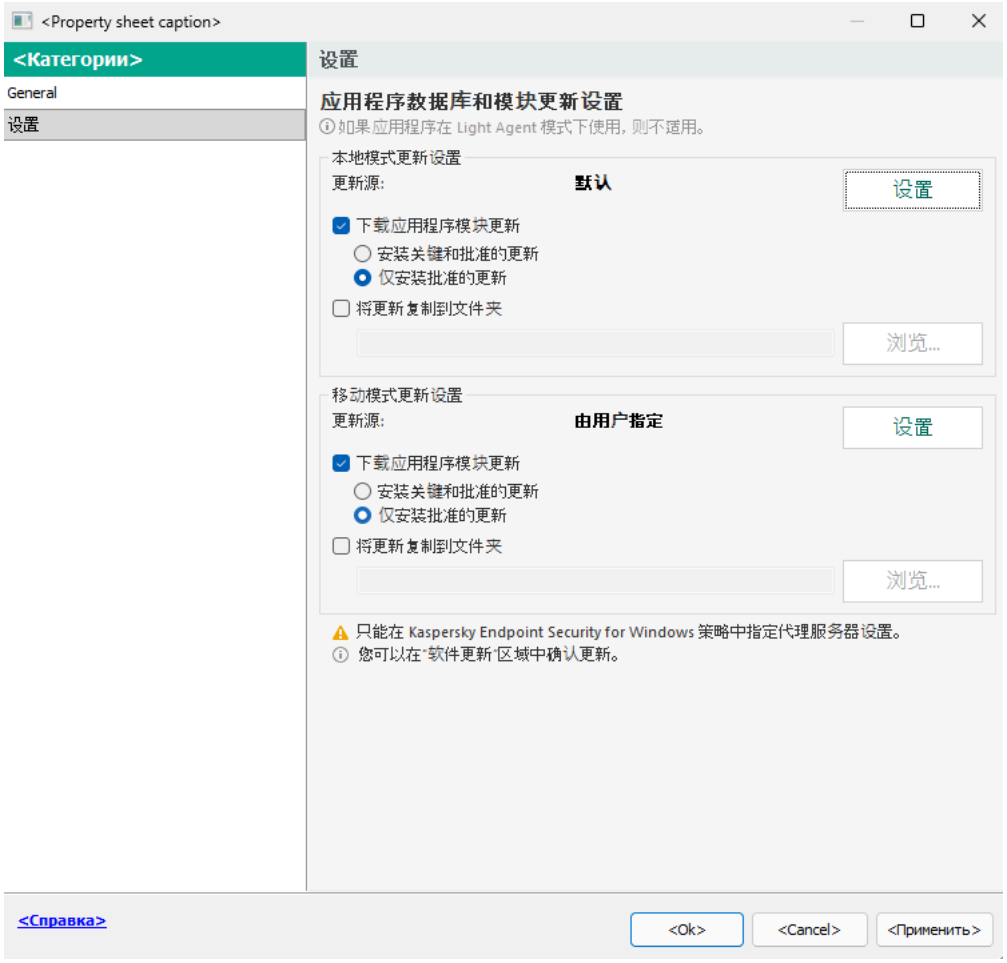
   在控制台树中，选择“**任务**”。

2. 单击 Kaspersky Endpoint Security 的“**数据库和应用程序模块更新**”任务。

   任务属性窗口将打开。

   “*数据库和应用程序模块更新*”任务由管理服务器快速启动向导自动创建。要创建“*数据库和应用程序模块更新*”任务，请在运行向导时安装 Kaspersky Endpoint Security for Windows Web 插件。

3. 在任务属性窗口中，选择“**设置**”区域。



数据库和应用程序模块更新 任务设置

4. 在“**本地模式更新设置**”块中单击“**设置**”按钮。

更新来源

5. 在更新源列表中，单击“**添加**”按钮。

6. 在“**更新源**”字段中，指定包含更新包的 FTP 或 HTTP 服务器、网络文件夹或本地文件夹的地址。更新源使用以下路径格式：

- 对于 FTP 或 HTTP 服务器，请输入它的网址或 IP 地址。

例如，`http://dnl-01.geo.kaspersky.com/` 或 `93.191.13.103`。

对于 FTP 服务器，可以用以下格式在地址内指定身份验证设置：`ftp://<user name>:<password>@<node>:<port>`。

- 对于网络文件夹，输入 UNC 路径。

  例如，`\\Server\Share\Update distribution`。

- 对于本地文件夹，输入该文件夹的完整路径。

  例如，`C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`。

您可以排除更新源而不将其从更新源列表中删除。为此，清空对象旁边的复选框。

7. 单击“**确定**”。

8. 使用“**上移**”和“**下移**”按钮配置更新源的优先级。

   如果无法从第一个更新源执行更新，Kaspersky Endpoint Security 会自动切换到下一个更新源。

9. 如有需要，为移动模式添加更新源。*移动模式*是计算机离开组织网络周界（*离线计算机*）时 Kaspersky Endpoint Security 的运行模式。

10. 保存更改。

如何在 Web Console 和云控制台中添加更新源

1. 在 Web Console 的主窗口中，选择“**任务**”。

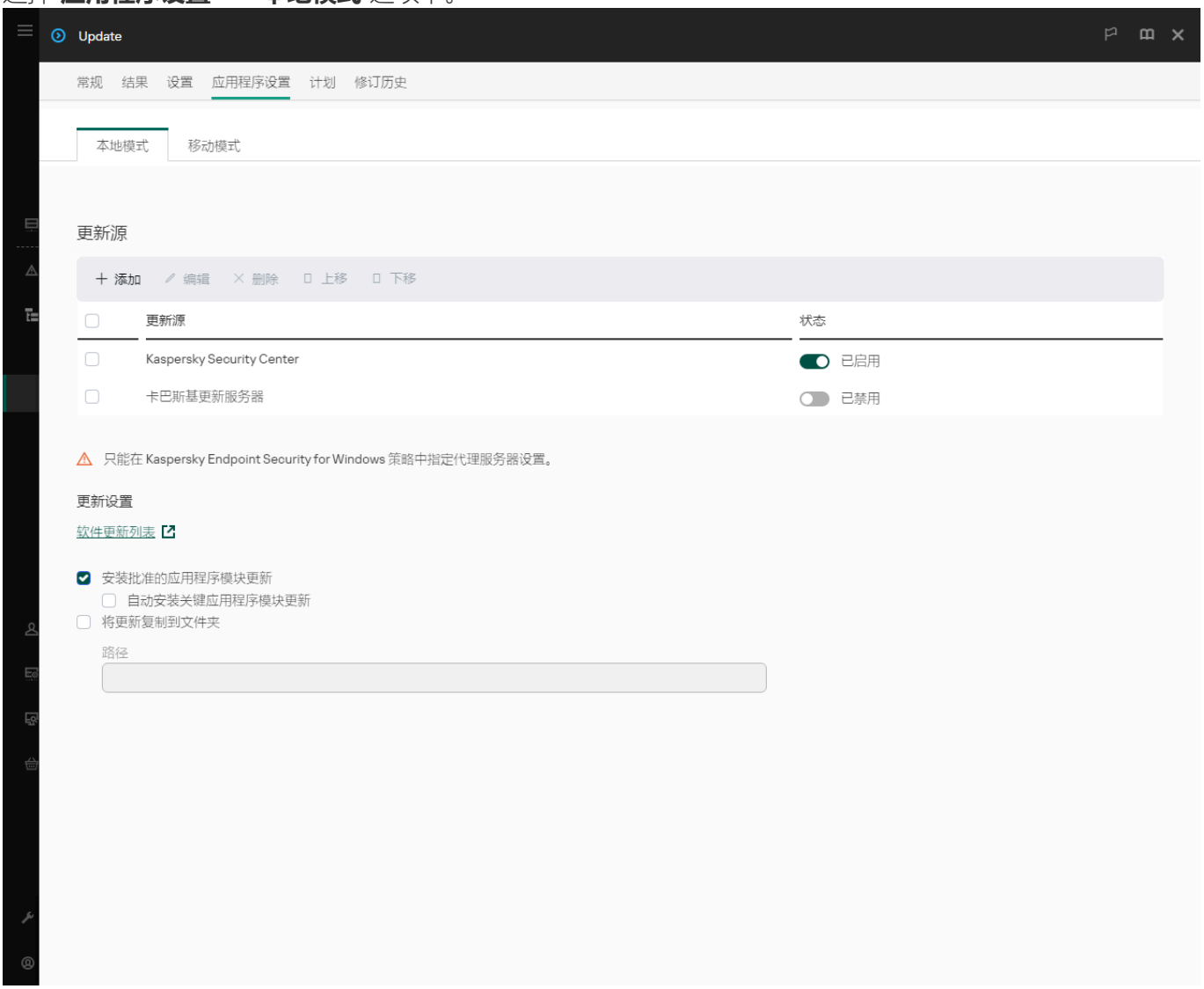
   任务列表打开。

2. 单击 Kaspersky Endpoint Security 的“**更新**”任务。

   任务属性窗口将打开。

   “*更新*”任务由管理服务器快速启动向导自动创建。要创建“*更新*”任务，请在运行向导时安装 Kaspersky Endpoint Security for Windows Web 插件。

3. 选择“**应用程序设置**” → “**本地模式**”选项卡。



更新来源

4. 在更新源列表中，单击“**添加**”按钮。

5. 在打开的窗口中，指定包含更新包的 FTP 或 HTTP 服务器、网络文件夹或本地文件夹的地址。
   更新源使用以下路径格式：

   - 对于 FTP 或 HTTP 服务器，请输入它的网址或 IP 地址。
     例如，`http://dnl-01.geo.kaspersky.com/` 或 `93.191.13.103`。
     对于 FTP 服务器，可以用以下格式在地址内指定身份验证设置：`ftp://<user name>:<password>@<node>:<port>`。

   - 对于网络文件夹，输入 UNC 路径。
     例如，`\\Server\Share\Update distribution`。

   - 对于本地文件夹，输入该文件夹的完整路径。
     例如，`C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`。

   您可以排除更新源而不将其从更新源列表中删除。为此，请将其旁边的切换开关设置为关闭位置。

6. 单击“**确定**”。

7. 使用“**上移**”和“**下移**”按钮配置更新源的优先级。

   如果无法从第一个更新源执行更新，Kaspersky Endpoint Security 会自动切换到下一个更新源。

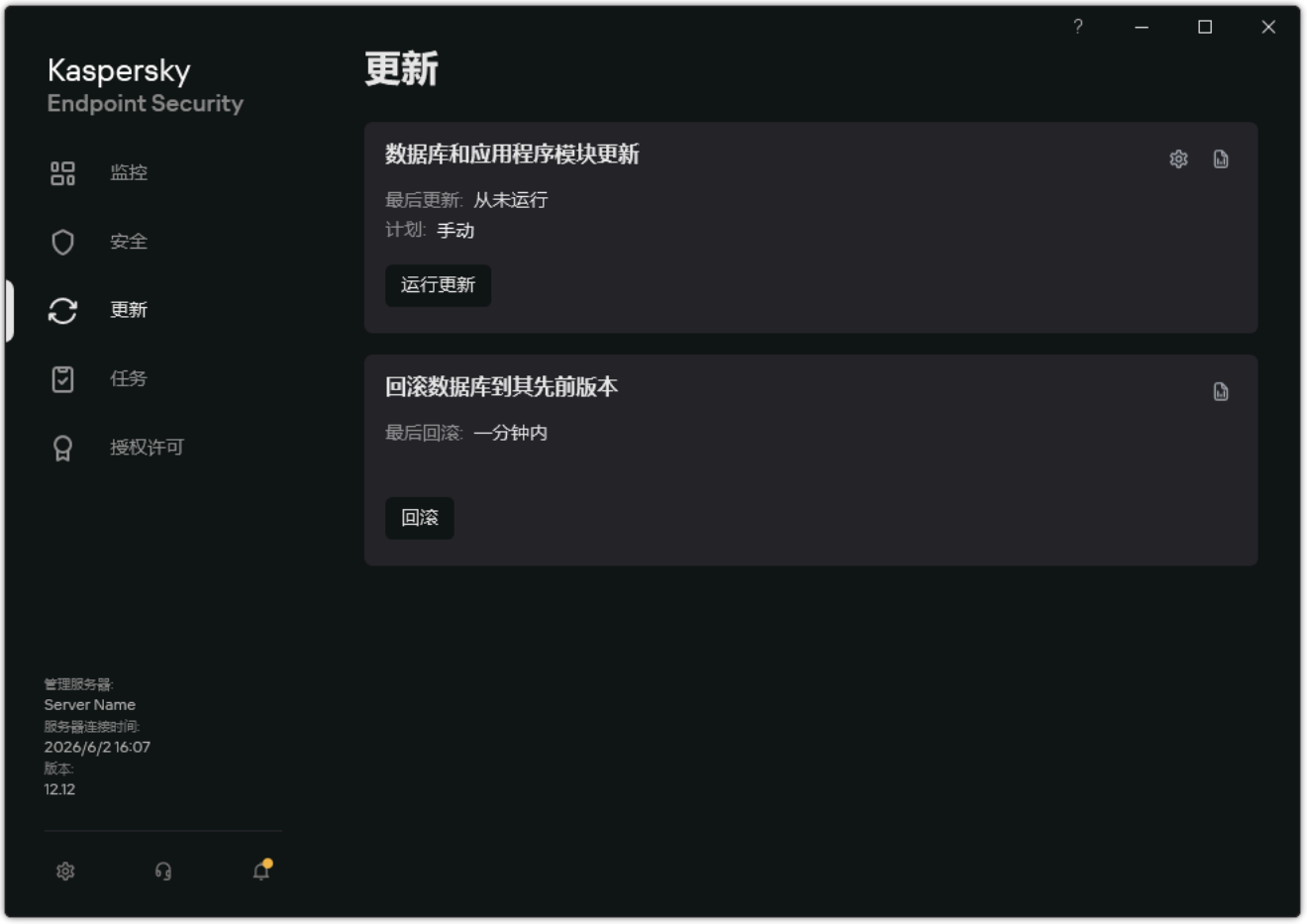
8. 如有需要，为移动模式添加更新源。*移动模式*是计算机离开组织网络周界（*离线计算机*）时 Kaspersky Endpoint Security 的运行模式。

9. 保存更改。

如何在应用程序界面中添加更新源

> 您不能在应用程序界面中配置“*数据库和应用程序模块更新*”组任务。只有一个本地更新任务，*数据库和应用程序模块更新*，可供用户使用。如果“*数据库和应用程序模块更新*”任务未显示，这意味着管理员已在策略中禁止对本地任务的使用。

1. 在应用程序主窗口中，转到“**更新**”区域。



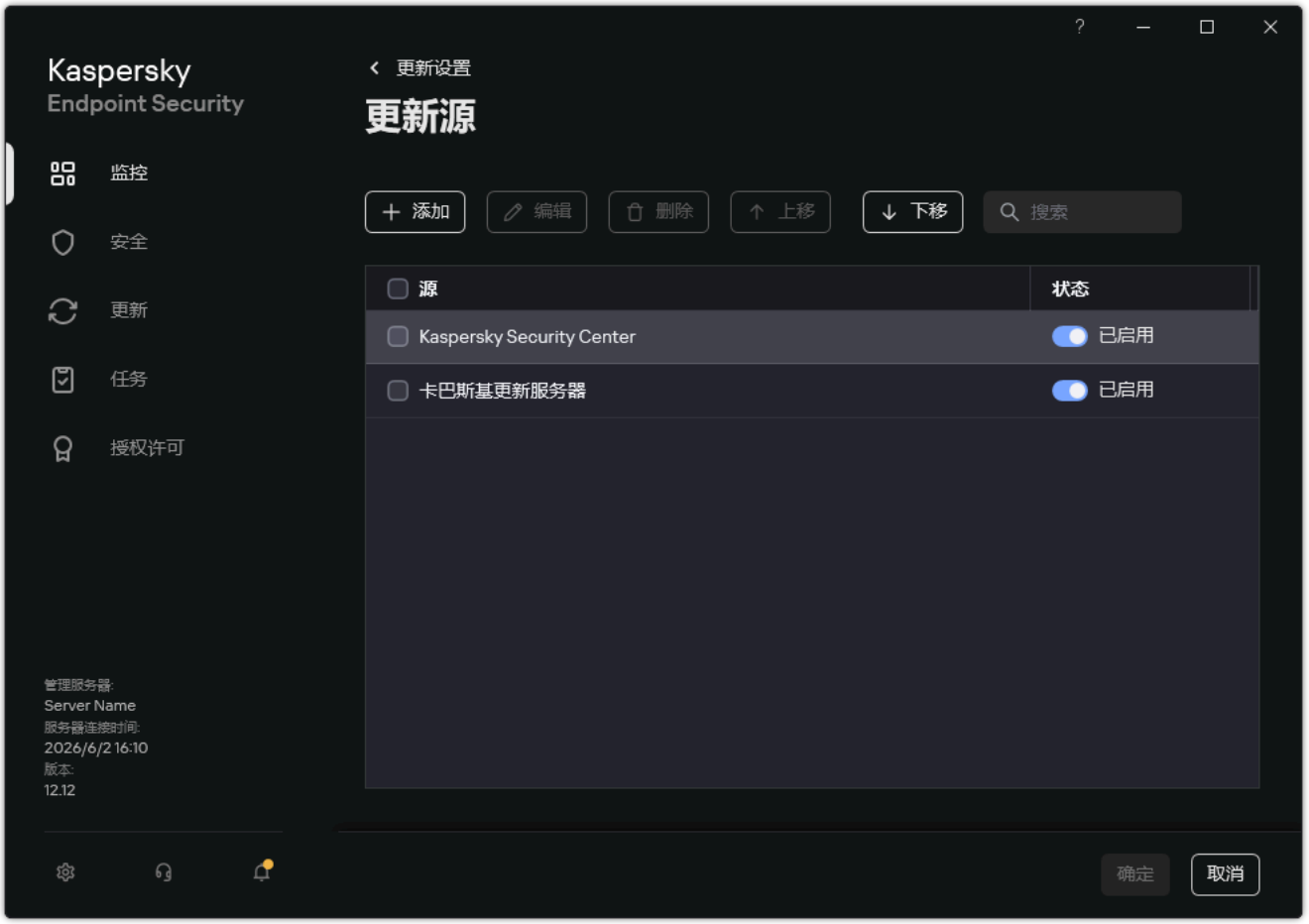
本地更新任务

2. 这将打开任务列表；选择“*数据库和应用程序模块更新*”任务并单击 ⚙。

   任务属性窗口将打开。

3. 单击“**选择更新源**”。

4. 在打开的窗口中，单击“**添加**”按钮。



更新来源

5. 在打开的窗口中，指定包含更新包的 FTP 或 HTTP 服务器、网络文件夹或本地文件夹的地址。
   更新源使用以下路径格式：

   - 对于 FTP 或 HTTP 服务器，请输入它的网址或 IP 地址。
     例如，`http://dnl-01.geo.kaspersky.com/` 或 `93.191.13.103`。
     对于 FTP 服务器，可以用以下格式在地址内指定身份验证设置：`ftp://<user name>:<password>@<node>:<port>`。
   - 对于网络文件夹，输入 UNC 路径。
     例如，`\\Server\Share\Update distribution`。
   - 对于本地文件夹，输入该文件夹的完整路径。
     例如，`C:\Documents and Settings\All Users\Application Data\Kaspersky Lab\AVP12\Update distribution\`。

6. 单击“**选择**”。

7. 使用“**上移**”和“**下移**”按钮配置更新源的优先级。

8. 保存更改。

更新应用程序模块

应用程序模块更新可修复错误、提高性能并添加新功能。当新的应用程序模块更新可用时，您需要确认更新的安装。您可以在应用程序界面或 Kaspersky Security Center 确认应用程序模块更新的安装。无论何时有更新可用，应用程序都会在 Kaspersky Endpoint Security 的主窗口中显示通知：。如果应用程序模块更新需要查看和接受最终用户授权许可协议，应用程序将在最终用户授权许可协议被接受后，安装更新。

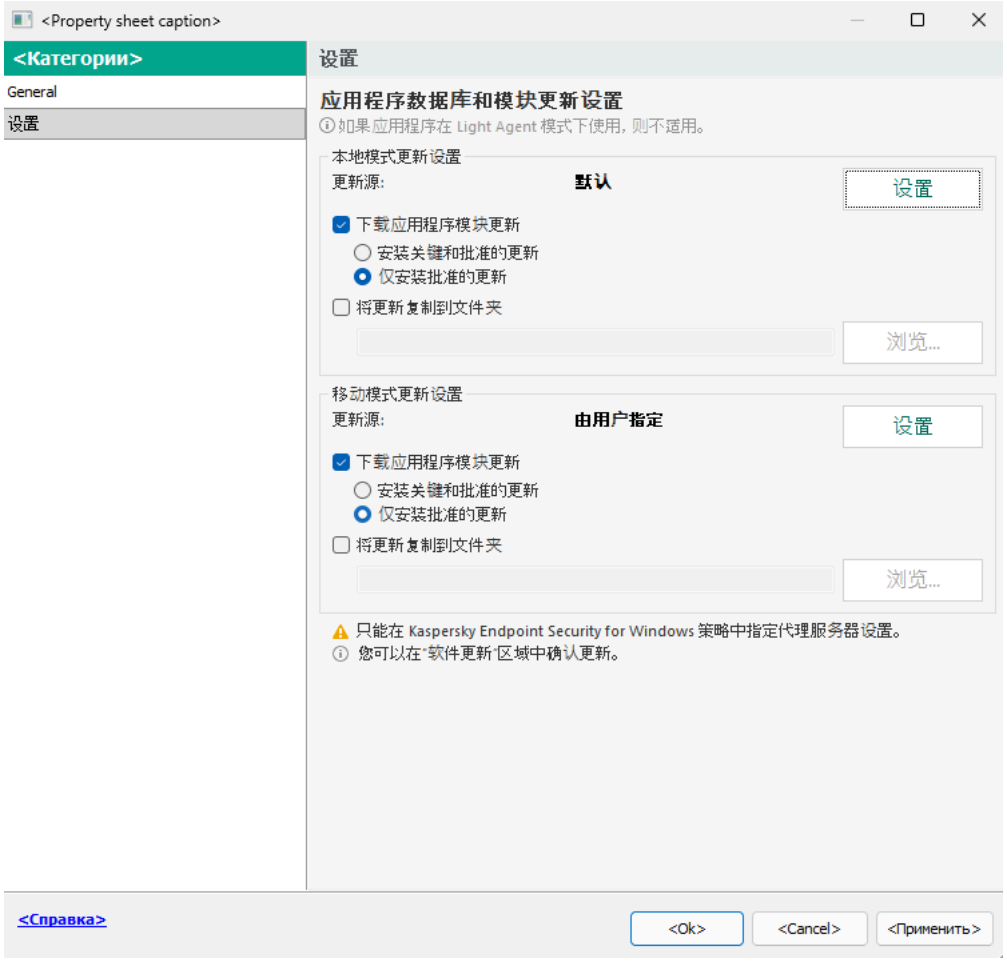
安装应用程序更新后，您可能需要重启计算机。

如何在管理控制台 (MMC) 中配置应用程序模块更新

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**任务**”。
3. 单击 Kaspersky Endpoint Security 的“**数据库和应用程序模块更新**”任务。

   任务属性窗口将打开。

   “*数据库和应用程序模块更新*”任务由管理服务器快速启动向导自动创建。要创建“*数据库和应用程序模块更新*”任务，请在运行向导时安装 Kaspersky Endpoint Security for Windows Web 插件。
4. 在任务属性窗口中，选择“**设置**”区域。



数据库和应用程序模块更新 任务设置

5. 在“**本地模式更新设置**”块中，选中“**下载应用程序模块更新**”复选框。

   如果要阻止下载应用程序模块更新，请清除“**下载应用程序模块更新**”复选框并禁止用户使用本地任务。

6. 选择您要安装的应用程序模块更新。

   - “**安装关键和批准的更新**”。如果选择此选项，当有应用程序模块更新可用时，仅在这些更新通过应用程序界面或在 Kaspersky Security Center 一侧被本地批准后，Kaspersky Endpoint Security 才会自动安装关键更新和所有其他应用程序模块更新。

   - “**仅安装批准的更新**”。如果选择该选项，当有应用程序模块更新可用时，仅在这些更新通过应用程序界面或在 Kaspersky Security Center 一侧被本地批准后，Kaspersky Endpoint Security 才会安装它们。默认情况下已选定该选项。

7. 如果有必要，为移动模式配置应用程序模块更新。*移动模式*是计算机离开组织网络周界（*离线计算机*）时 Kaspersky Endpoint Security 的运行模式。

8. 保存更改。

如何在 Web Console 和云控制台中配置应用程序模块更新

1. 在 Web Console 的主窗口中，选择“**任务**”。

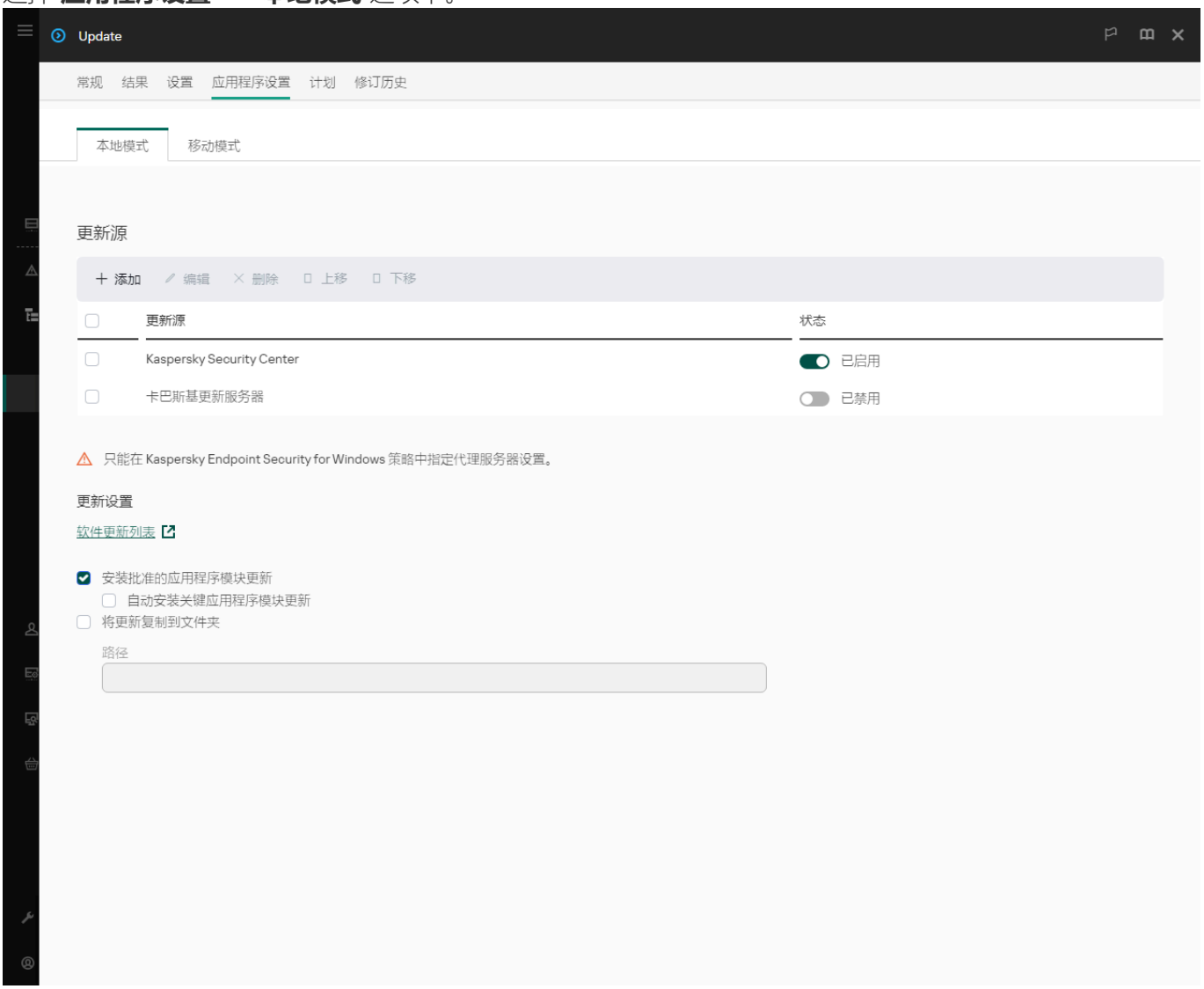
   任务列表打开。

2. 单击 Kaspersky Endpoint Security 的“**数据库和应用程序模块更新**”任务。

   任务属性窗口将打开。

   “*数据库和应用程序模块更新*”任务由管理服务器快速启动向导自动创建。要创建“*数据库和应用程序模块更新*”任务，请在运行向导时安装 Kaspersky Endpoint Security for Windows Web 插件。

3. 选择“**应用程序设置**” → “**本地模式**”选项卡。



更新 任务设置

4. 在“**更新设置**”下，选择您要安装的应用程序模块更新：

   - “**安装批准的应用程序模块更新**”。如果选择该选项，当有应用程序模块更新可用时，仅在这些更新通过应用程序界面或在 Kaspersky Security Center 一侧被本地批准后，Kaspersky Endpoint Security 才会安装它们。默认情况下已选定该选项。

   - “**自动安装关键应用程序模块更新**”。如果选择此选项，当有应用程序模块更新可用时，仅在这些更新通过应用程序界面或在 Kaspersky Security Center 一侧被本地批准后，Kaspersky Endpoint Security 才会自动安装关键更新和所有其他应用程序模块更新。

   如果您要阻止下载应用程序模块更新，请清除“**安装批准的应用程序模块更新**”和“**自动安装关键应用程序模块更新**”复选框并禁止用户使用本地任务。

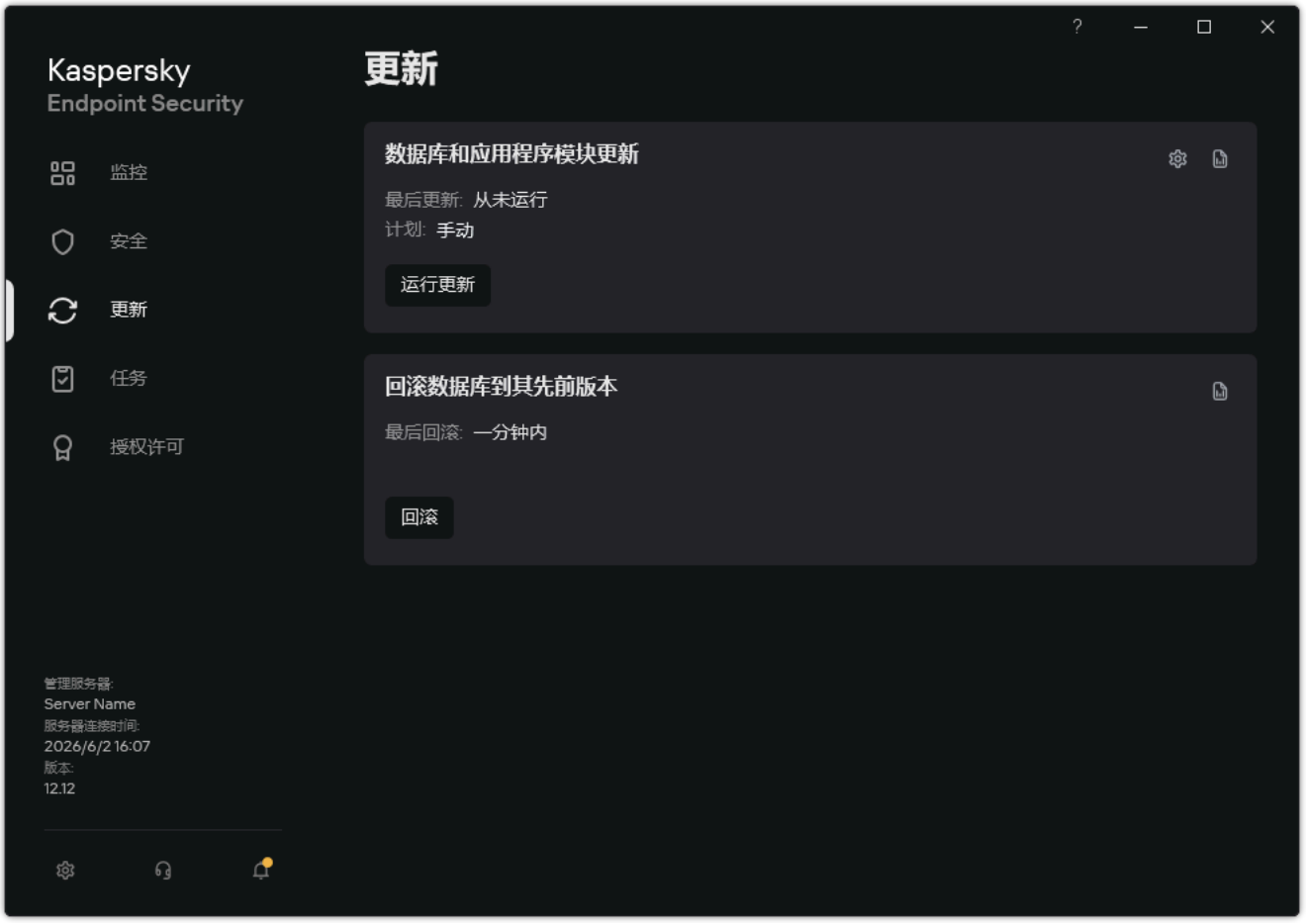
5. 如果有必要，为移动模式配置应用程序模块更新。*移动模式*是计算机离开组织网络周界（*离线计算机*）时 Kaspersky Endpoint Security 的运行模式。

6. 保存更改。

如何在应用程序界面中配置应用程序模块更新

> 您不能在应用程序界面中配置“*数据库和应用程序模块更新*”组任务。只有一个本地更新任务，*数据库和应用程序模块更新*，可供用户使用。如果“*数据库和应用程序模块更新*”任务未显示，这意味着管理员已在策略中禁止对本地任务的使用。

1. 在应用程序主窗口中，转到“**更新**”区域。



本地更新任务

2. 这将打开任务列表；选择“*数据库和应用程序模块更新*”任务并单击 ⚙。
   任务属性窗口将打开。

3. 在“**下载和安装应用程序模块更新**”块中，选中“**下载应用程序模块更新**”复选框。

4. 选择您要安装的应用程序模块更新。

   - “**安装关键和批准的更新**”。如果选择此选项，当有应用程序模块更新可用时，仅在这些更新通过应用程序界面或在 Kaspersky Security Center 一侧被本地批准后，Kaspersky Endpoint Security 才会自动安装关键更新和所有其他应用程序模块更新。

   - “**仅安装批准的更新**”。如果选择该选项，当有应用程序模块更新可用时，仅在这些更新通过应用程序界面或在 Kaspersky Security Center 一侧被本地批准后，Kaspersky Endpoint Security 才会安装它们。默认情况下已选定该选项。

5. 保存更改。

使用代理服务器进行更新

您可能需要指定代理服务器设置才能从更新源下载数据库和应用程序模块更新。如果有多个更新源，代理服务器设置将适用于所有源。如果某些更新源不需要代理服务器，可以在策略属性中禁用代理服务器。Kaspersky Endpoint Security 还将使用代理服务器访问卡巴斯基安全网络和激活服务器。

要配置通过代理服务器连接到更新源：

1. 在 Web Console 的主窗口中单击 ⚙。
   “管理服务器”属性窗口将打开。
2. 转到**配置互联网访问**区域。
3. 选择**使用代理服务器**复选框。
4. 配置代理服务器连接设置：代理服务器地址、端口和身份验证设置（用户名和密码）。
5. 保存更改。

要对特定管理组禁止使用代理服务器：

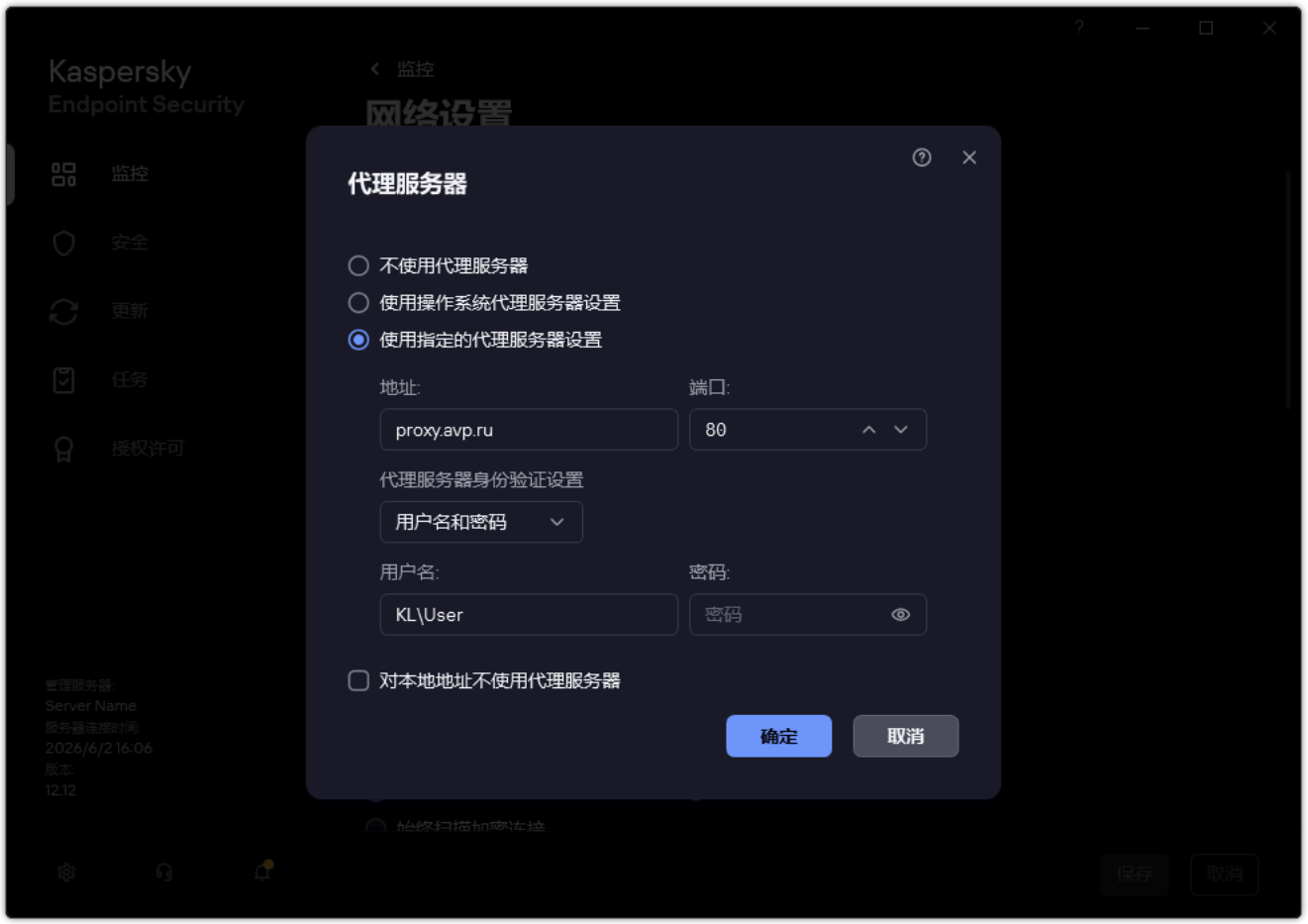
1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **网络设置**。
5. 在“**代理服务器**”块中单击“**设置**”按钮。
6. 在打开的窗口中，选中“**对本地地址不使用代理服务器**”复选框。
7. 保存更改。

要在应用程序界面配置代理服务器设置：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**网络设置**”。

应用程序网络设置

3. 在“**代理服务器**”区域，单击“**代理服务器设置**”链接。



代理服务器连接设置

4. 在打开的窗口中，选择以下选项之一以确定代理服务器地址：

   - “**使用操作系统代理服务器设置**”。

     默认情况下已选定该选项。Kaspersky Endpoint Security 使用在操作系统设置中定义的代理服务器设置。

   - “**使用指定的代理服务器设置**”。

     如果您选择该选项，配置连接到代理服务器的设置：代理服务器地址和端口。

5. 选择您希望应用程序在代理服务器上进行身份验证的方式。默认情况下，应用程序使用当前用户的域 NTLM 身份验证。

6. 如果您希望在从共享文件夹更新数据库和应用程序模块时禁用代理服务器，请选中“**对本地地址不使用代理服务器**”复选框。

7. 保存更改。

结果，Kaspersky Endpoint Security 将使用代理服务器下载应用程序模块和数据库更新。Kaspersky Endpoint Security 还将使用代理服务器访问 KSN 和卡巴斯基激活服务器。如果代理服务器需要身份验证但是用户账户凭证未正确提供，Kaspersky Endpoint Security 将提示您输入用户名和密码。

上次更新回滚

在数据库和程序模块进行第一次更新以后，就能够将数据库和程序模块回滚至前一版本的功能。

每次用户开始更新程序时，Kaspersky Endpoint Security 会为当前数据库和程序模块创建一个备份副本。让您能够在必要时将数据库和程序模块回滚至它们的前一版本。回滚上次更新是有用的，例如，如果新的数据库版本导致误报，从而导致 Kaspersky Endpoint Security 阻止安全应用程序。

Light Agent 模式下的 Kaspersky Endpoint Security 不支持“*更新回滚*”任务。

如何在管理控制台 (MMC) 中回滚上一次更新

1. 在 Kaspersky Security Center 管理控制台树中，选择“**任务**”。
   任务列表打开。
2. 单击“**新任务**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 选择任务类型

1. 选择“**Kaspersky Endpoint Security for Windows (14.1)**”→ “**更新回滚**”。

步骤 2. 选择任务将分配到的设备

选择将要执行任务的计算机。下列选项可用：

- 将任务分配给管理组。在这种情况下，任务分配给先前创建的管理组中包括的计算机。
- 选择管理服务器在网络中检测到的计算机：*未分配设备*。特定设备可包括管理组中的设备以及未分配设备。
- 手动指定设备地址或从列表中导入地址。您可以指定您要将任务分配给的设备的 NetBIOS 名称、IP 地址和 IP 子网。

步骤 3. 配置任务启动计划

配置任务计划，例如，手动。

步骤 4. 定义任务名称

输入任务的名称。

步骤 5. 完成任务创建

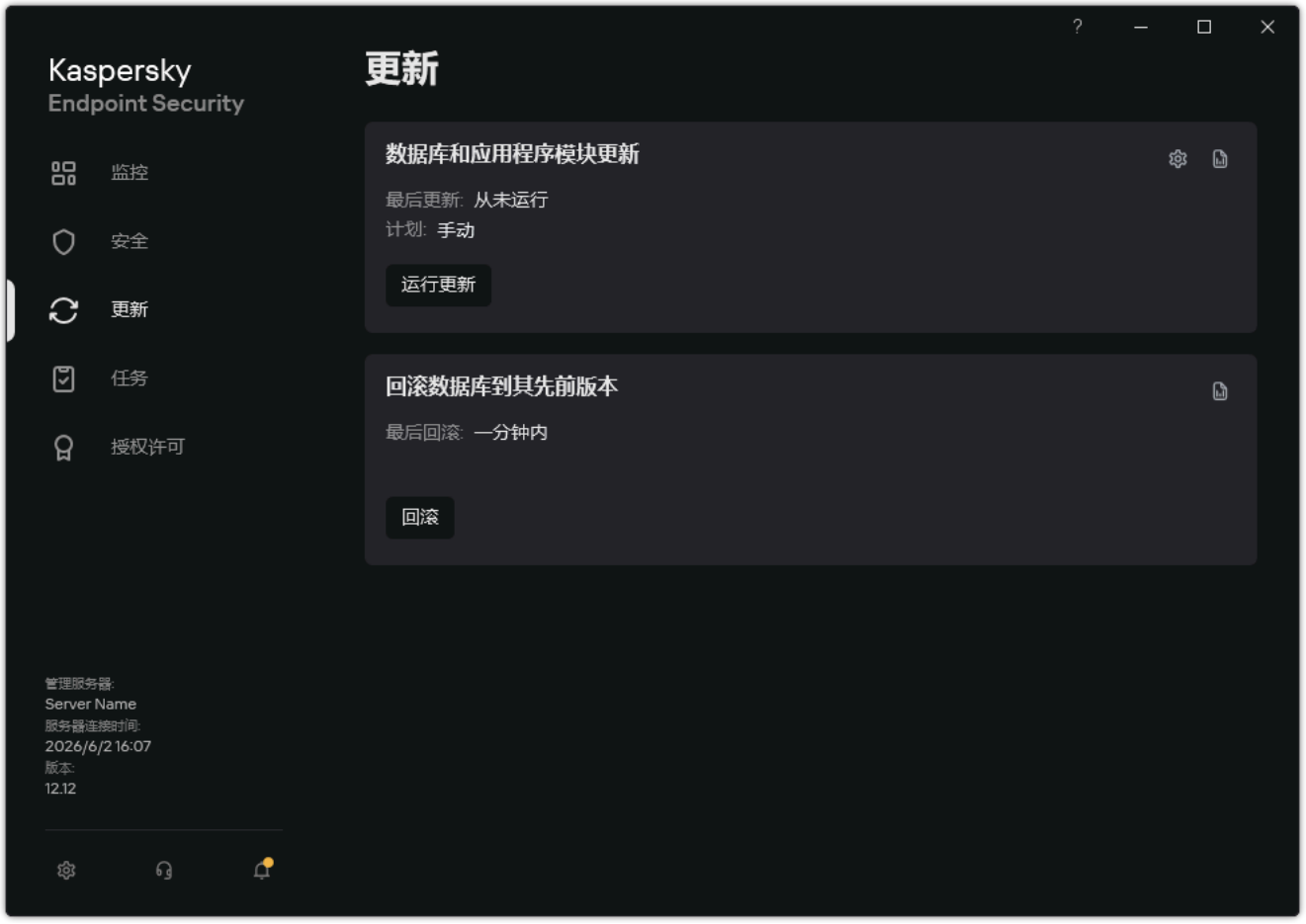
退出向导。如有必要，选中“**向导完成时运行任务**”复选框。您可以在任务属性中监控任务进度。

如何在 Web Console 中回滚上次更新

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
2. 单击“**添加**”。
   “任务向导”将启动。
3. 配置任务设置：
   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Endpoint Security for Windows 14.2.0**”。
   b. 在“**任务类型**”下拉列表中，选择“**更新回滚**”。
   c. 在“**任务名称**”字段中，输入简要说明，例如“*更新回滚*”。
   d. 在“**要对其分配任务的设备**”块，选择任务范围。
4. 按照所选任务范围选项选择设备。转到下一步。
5. 选择要运行任务的账户。默认情况下，Kaspersky Endpoint Security 将使用本地用户账户的权限启动任务。
6. 退出向导。
7. 在任务列表中将显示一个新任务。
8. 选中该任务旁边的复选框。
9. 单击“**开始**”。

如何在应用程序界面中回滚上一次更新

1. 在应用程序主窗口中，转到“**更新**”区域。



本地更新任务

2. 在**回滚数据库到其先前版本**块中，单击**回滚**按钮。

Kaspersky Endpoint Security 将开始回滚上一次数据库更新。应用程序将显示回滚进度、已下载文件大小和更新源。您可以通过单击**停止更新**按钮随时停止任务。

高级清除技术

要处理活动威胁，Kaspersky Endpoint Security 使用高级清除技术。高级清除针对工作站和服务器具有不同功能。您可以在“*恶意软件扫描*”任务设置和应用程序设置中配置高级清除。

如果 Kaspersky Endpoint Security 无法停止执行恶意软件，您可以使用高级清除技术。适用于受策略约束的计算机，高级清除被默认禁用，因为该技术使用大量的计算资源。 对于不受策略约束的计算机，高级清除默认启用。

> 高级清除针对工作站和服务器具有不同功能。要在服务器上使用该技术，您必须在“*恶意软件扫描*”任务的属性中启用即时高级清除。在工作站上使用此技术时不需要此先决条件。

如何在管理控制台(MMC)中启用或禁用高级清除技术

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **应用程序设置**。
4. 在“**常规**”块，选中或清空“**启用高级清除技术**”复选框以启用或禁用高级清除技术。
5. 保存更改。

如何在 Web Console 和云控制台中启用或禁用高级清除技术

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择“**常规设置**” → “**检测设置**”。
5. 在“**高级清除技术**”块，开启或关闭“**高级清除技术已启用**”切换开关以启用或禁用高级清除技术。
6. 保存更改。

如何在应用程序界面中启用或禁用高级清除技术

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**应用程序设置**”。

Kaspersky Endpoint Security for Windows 设置

3. 在“**常规**”块，选中或清空“**使用高级清除技术(需要大量计算机资源)**”复选框以启用或禁用高级清除技术。
4. 保存更改。

因此，在进行高级清除时，用户无法使用大多数操作系统功能。当清除完成时，计算机将被重启。

清除工作站上的活动威胁

要在工作站上处理活动威胁，在应用程序设置中启用高级清除技术。下一步，在“*恶意软件扫描*”任务属性中配置用户经验。在任务属性中有**立即运行高级清除**复选框。如果设置了该标志，Kaspersky Endpoint Security 将执行清除而不通知用户。当清除完成时，计算机将被重启。如果未设置该标志，Kaspersky Endpoint Security 将显示关于活动威胁的通知（参见下图）。您无法不处理该文件而关闭该通知。

仅当在应用于计算机的策略的属性中启用“高级清除”功能后，才会在该计算机上运行病毒扫描任务期间执行高级清除。

通知活动威胁

清除服务器上的活动威胁

要在服务器上处理活动威胁，您需要做以下操作：

- 在应用程序设置中启用高级清除技术；
- 在“*恶意软件扫描*”任务属性中启用即时高级清除。

如果 Kaspersky Endpoint Security 安装在运行 Windows for Servers 的计算机上，Kaspersky Endpoint Security 不显示通知。因此，您无法选择操作以清除活动威胁。要清除威胁，您需要在应用程序设置中启用高级清除技术以及在“*恶意软件扫描*”任务设置中立即启动高级清除。然后您需要启动“*恶意软件扫描*”任务。

消除未处理的威胁

Kaspersky Endpoint Security 将记录由于某种原因而未能处理的文件的信息。此信息在活动威胁列表中以事件的形式记录（参见下表）。

活动威胁列表

如果 Kaspersky Endpoint Security 在扫描计算机病毒和其他恶意软件时对受感染的文件进行了清除或消除了威胁，则认为该文件*已处理*。

如果 Kaspersky Endpoint Security 在扫描计算机中的病毒和其他威胁时由于某种原因未能按照指定的应用程序设置对某个文件执行操作，Kaspersky Endpoint Security 会将该文件移至活动威胁列表。

在下列情况中可能出现此状况：

- 扫描的文件不可用（例如，文件位于网络驱动器或没有写权限的可移动驱动器上）。
- 在“*恶意软件扫描*”任务设置中，检测到威胁后的操作被设置为“**通知**”。然后，当屏幕上显示已感染文件的通知时，用户选择“**忽略**”。

如果有任何未处理的威胁，Kaspersky Endpoint Security 更改其图标到 。在应用程序主窗口中，威胁通知被显示（参见下图）。在 Kaspersky Security Center 控制台中，计算机的状态更改为“*严重*”。

如何在管理控制台 (MMC) 中处理威胁

1. 在管理控制台中，转到文件夹“**管理服务器**”→“**高级**”→“**存储库**”→“**活动威胁**”。

   活动威胁列表打开。

2. 选择您要处理的对象。

3. 选择如何处理威胁：

- “**清除**”。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。

- “**删除**”。如果选择此选项，应用程序将删除从活动威胁存储库中检测到的受感染文件。在这种情况下，应用程序会将检测到的文件保存在计算机内存中。要消除计算机中的威胁，请选择“**清除**”。

如何在 Web Console 和云控制台中处理威胁

1. 在 Web Console 的主窗口中，选择“**操作**” → “**存储库**” → “**活动威胁**”。

   活动威胁列表打开。

2. 选择您要处理的对象。

3. 选择如何处理威胁：

- “**清除**”。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。

- “**删除**”。如果选择此选项，应用程序将删除从活动威胁存储库中检测到的受感染文件。在这种情况下，应用程序会将检测到的文件保存在计算机内存中。要消除计算机中的威胁，请选择“**清除**”。

如何在应用程序界面中处理威胁

1. 在应用程序主窗口中，在“**监控**”区域，单击“**保护存在风险**”瓦片。

   活动威胁列表打开。

2. 选择您要处理的对象。

3. 选择如何处理威胁：

- “**解决**”。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。

- “**添加到排除项**”。如果选择此操作，Kaspersky Endpoint Security 建议将文件添加到扫描排除项列表中。排除项设置是自动配置的。如果添加排除项不可用，则表示管理员已禁用在策略设置中添加排除项。

- “**忽略**”。如果选择该选项，Kaspersky Endpoint Security 将从活动威胁列表中删除此条目。如果列表上没有活动威胁，计算机状态将变为“*确定*”。如果对象再次被检测到，Kaspersky Endpoint Security 将向活动威胁列表新添一个条目。

- “**打开所在文件夹**”。如果选择此选项，Kaspersky Endpoint Security 将在文件管理程序中打开包含此物件的文件夹。然后您可以手动删除对象或将对象移到在保护范围内的文件夹中。

- “**了解更多**”。如果选择此选项，Kaspersky Endpoint Security 将打开卡巴斯基漏洞和威胁数据库网站。

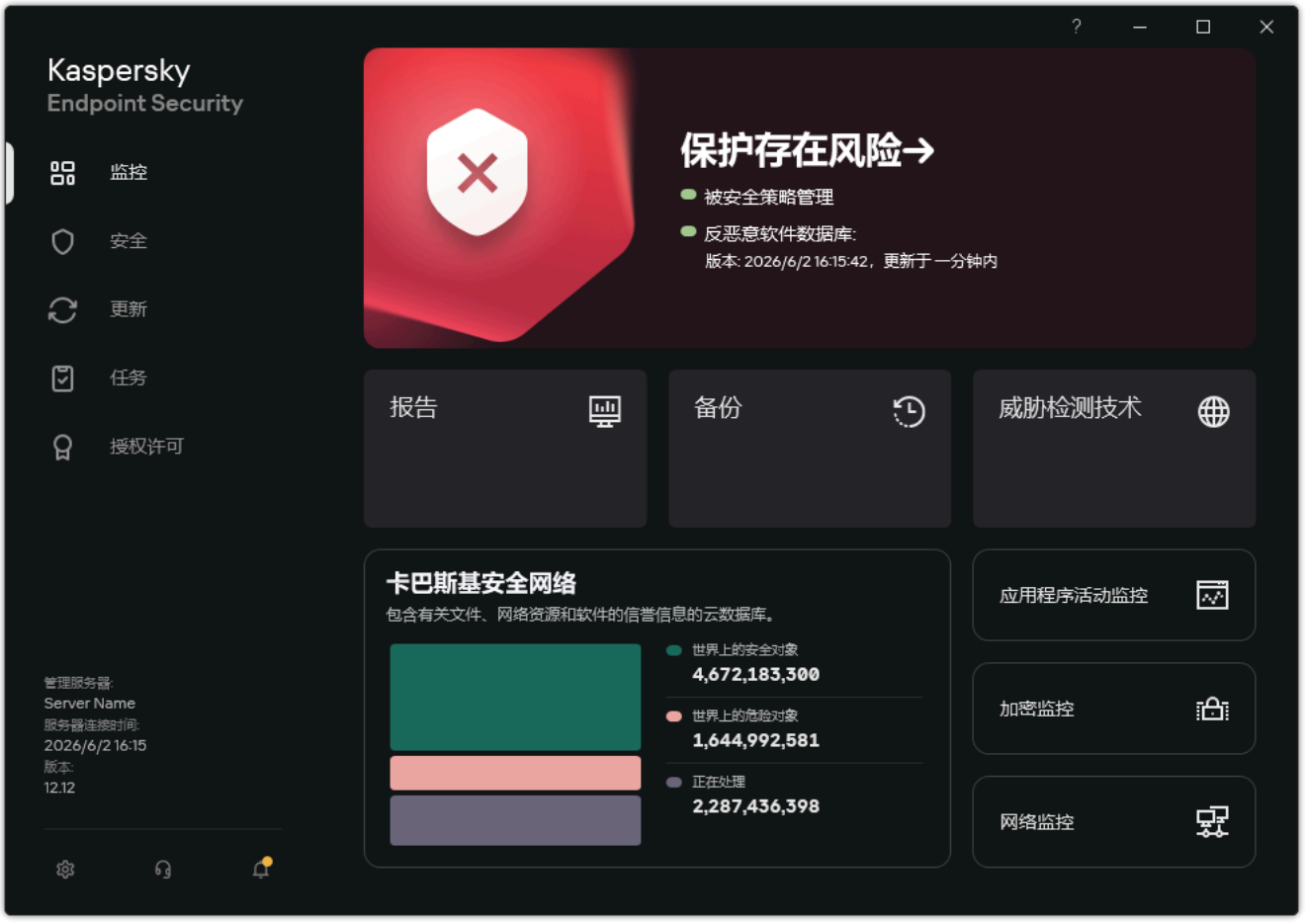
要在 Kaspersky Security Center 控制台中处理活动威胁，您必须启用将有关未处理文件的信息传输到管理服务器。默认情况下启用数据传输。

如何在管理控制台 (MMC) 中启用未处理文件数据的传输

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **报告和存储**。
4. 在“**到管理服务器的数据传输**”块中单击“**设置**”按钮。
5. 选择**未处理的文件**复选框。
6. 保存更改。

如何在 Web Console 中启用未处理文件数据的传输

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **KSC 整合**。
5. 在“**到管理服务器的数据传输**”块中，选中“**关于未处理的文件**”复选框。
6. 保存更改。



当检测到威胁时，主应用程序窗口

计算机保护

文件威胁防护

文件威胁防护组件可防止计算机文件系统受到感染。默认情况下，文件威胁防护组件永久驻留在计算机的 RAM 中，并实时扫描所有打开、保存和启动的文件。该组件扫描所有计算机驱动器（包括连接的驱动器）上的文件。该组件借助反病毒数据库、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。

该组件将扫描用户或应用程序访问的文件。如果检测到恶意文件，Kaspersky Endpoint Security 将阻止文件操作。应用程序随后将根据“文件威胁防护”组件的设置来清除或删除恶意文件。

当尝试访问其内容驻留在 OneDrive 云存储中的文件时，Kaspersky Endpoint Security 会下载并扫描文件内容。

启用和禁用文件威胁防护

默认情况下，“文件威胁防护”组件已启用并在 Kaspersky 专家建议的模式下运行。对于文件威胁防护，Kaspersky Endpoint Security 可以应用不同的设置组。存储在应用程序中的设置组叫做“*安全级别*”：**高**、**建议**、**低**。**建议**安全级别设置将被视为 Kaspersky 专家建议的最佳设置（参加下表）。您可以选择某种预设的安全级别或手动配置安全性级别的设置。如果您改变了文件安全级别设置，仍可随时恢复到推荐的文件安全级别设置。

文件威胁防护组件使用从其他应用程序组件接收的数据。启用那些组件是可选的。提供附加数据的组件包括：

- 卡巴斯基安全网络。
- 主机入侵防御。
- 行为检测。

如何在管理控制台(MMC)中启用或禁用文件威胁防护组件

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **基本威胁防护** → **文件威胁防护**。
4. 使用“**文件威胁防护**”复选框启用或禁用组件。

5. 如果您启用了组件，在“**安全级别**”块做以下之一：

- 如果您希望应用一种预设的安全级别，请使用滑动条选择：

  - “**高**”。选择该文件安全级别后，“文件威胁防护”组件将对打开、保存和运行的所有文件实施最严格的控制。“文件威胁防护”组件会扫描计算机的所有硬盘驱动器、可移动驱动器和网络驱动器上的所有文件类型。它还扫描存档、安装包和嵌入式 OLE 对象。

  - “**建议**”。该文件安全级别被 Kaspersky 专家推荐。“文件威胁防护”组件仅扫描计算机的所有硬盘驱动器、可移动驱动器和网络驱动器上的指定文件格式，以及嵌入式 OLE 对象。“文件威胁防护”组件不扫描压缩包或安装包。

  - “**低**”。该文件安全级别的设置确保最大的扫描速度。“文件威胁防护”组件仅扫描计算机的所有硬盘驱动器、可移动驱动器以及网络驱动器上拥有指定扩展名的文件。“文件威胁防护”组件不扫描复合文件。

- 如果您要配置自定义安全级别，单击**设置**按钮并定义您自己的组件设置。

  您可以通过单击“**默认**”按钮恢复预设安全级别的值。

6. 在“**检测到威胁后的操作**”块中选择 Kaspersky Endpoint Security 对恶意对象所采取的操作：

- “**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。

- “**清除；如果清除失败则阻止**”。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，应用程序将阻止这些文件。

- “**阻止**”。如果选择该选项，应用程序将自动阻止受感染的文件，而不尝试对其进行清除或删除。

- “**通知**”。如果选择此选项，Kaspersky Endpoint Security 会在检测到受感染文件时将这些文件的相关信息添加到活动威胁列表。

> 在对感染的文件进行清除或删除操作之前，应用程序会创建一个备份，以免日后会需要恢复该文件或对该文件进行清除。

7. 保存更改。

如何在 Web Console 和云控制台中启用或禁用文件威胁防护组件

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **主机威胁防护** → **文件威胁防护**。

5. 使用**文件威胁防护已启用**开关启用或禁用组件。

6. 如果您希望将新对象添加至保护范围：

   a. 在“**高级设置**”下，选择“**保护范围**”选项卡。

   b. 单击“**添加**”。

c. 在打开的窗口中，选择您要添加到保护范围的对象。

使用掩码：

- `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\*\*.txt` 将包括位于 C: 驱动器的文件夹（但不包括子文件夹）中所有具有 TXT 扩展名的文件的路径。

- 两个连续 `*` 字符在文件或文件夹名称中代表任意一组字符（包括空集），包括 `\` 和 `/` 字符（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\**\*.txt` 将包括位于 `Folder` 嵌套子文件夹（除了 `Folder` 本身）中所有带 TXT 扩展名的文件的路径。掩码必须包含至少一个嵌套级别。掩码 `C:\**\*.txt` 不是有效掩码。

- `?`（问号）字符代表任意单个字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\???.txt` 将包括位于 `Folder` 文件夹中所有带 TXT 扩展名且名称由三个字符构成的文件的路径。

您可以在文件或文件夹路径中的任何位置使用掩码。例如，如果您希望扫描范围包括计算机上所有用户账户的下载文件夹，请输入 `C:\Users\*\Downloads\` 掩码。

您可以从保护排除对象，而不用将其从保护范围对象列表中删除。为此，请将其旁边的切换开关设置为关闭位置。

d. 保存更改。

7. 在“**检测到威胁后的操作**”块中选择 Kaspersky Endpoint Security 对恶意对象所采取的操作：

- “**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。

- “**清除；如果清除失败则阻止**”。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，应用程序将阻止这些文件。

- “**阻止**”。如果选择该选项，应用程序将自动阻止受感染的文件，而不尝试对其进行清除或删除。

> 在对感染的文件进行清除或删除操作之前，应用程序会创建一个备份，以免日后会需要恢复该文件或对该文件进行清除。

8. 如有必要，请编辑文件威胁防护的高级设置。

9. 保存更改。

如何在应用程序界面中启用或禁用文件威胁防护组件

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**文件威胁防护**”。

3. 使用**文件威胁防护**开关启用或禁用组件。

4. 如果您启用了组件，在“**安全级别**”块做以下之一：

- 如果您希望应用一种预设的安全级别，请使用滑动条选择：
  - “**高**”。选择该文件安全级别后，“文件威胁防护”组件将对打开、保存和运行的所有文件实施最严格的控制。“文件威胁防护”组件会扫描计算机的所有硬盘驱动器、可移动驱动器和网络驱动器上的所有文件类型。它还扫描存档、安装包和嵌入式 OLE 对象。
  - “**建议**”。该文件安全级别被 Kaspersky 专家推荐。“文件威胁防护”组件仅扫描计算机的所有硬盘驱动器、可移动驱动器和网络驱动器上的指定文件格式，以及嵌入式 OLE 对象。“文件威胁防护”组件不扫描压缩包或安装包。
  - “**低**”。该文件安全级别的设置确保最大的扫描速度。“文件威胁防护”组件仅扫描计算机的所有硬盘驱动器、可移动驱动器以及网络驱动器上拥有指定扩展名的文件。“文件威胁防护”组件不扫描复合文件。
- 如果您要配置自定义安全级别，单击“**高级设置**”按钮并定义您自己的组件设置。

  您可以通过单击“**恢复推荐的安全级别**”按钮恢复预设安全级别的值。

5. 在“**检测到威胁后的操作**”块中选择 Kaspersky Endpoint Security 对恶意对象所采取的操作：

- “**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。
- “**清除；如果清除失败则阻止**”。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，应用程序将阻止这些文件。
- “**阻止**”。如果选择该选项，应用程序将自动阻止受感染的文件，而不尝试对其进行清除或删除。
- “**通知**”。如果选择此选项，Kaspersky Endpoint Security 会在检测到受感染文件时将这些文件的相关信息添加到活动威胁列表。

> 在对感染的文件进行清除或删除操作之前，应用程序会创建一个备份，以免日后会需要恢复该文件或对该文件进行清除。

6. 保存更改。

Kaspersky 专家推荐的文件威胁防护设置（推荐的安全级别）

参数	值	描述
文件类型	**按格式扫描文件**	如果启用该设置，则应用程序仅扫描被感染的文件。在扫描文件以查找恶意代码之前，系统将分析文件的内部头以确定文件的格式（例如，.txt、.doc 或 .exe）。该扫描也查找具有特殊文件扩展名的文件。
启发式分析	**轻度扫描**	开发该技术的目的是检测使用当前版本的卡巴斯基应用程序数据库无法检测到的威胁。它可以检测可能受未知病毒或已知病毒新变种感染的文件。 当扫描文件以查找恶意代码时，启发式分析执行可执行文件中的指令。启发式分析执行的指令数量取决于启发式分析级别。启发式分析级别可在全面搜索新威胁、加载操作系统资源和启发式分析持续时间之间进行平衡。
仅扫描新建和已修改的文件	**启用**	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。
使用 iSwift 技术	**启用**	该技术允许通过排除特定文件不扫描的方式提高扫描速度。该技术将使用特殊算法将文件排除在扫描范围之外，该算法会考虑 Kaspersky Endpoint Security 数据库的发布日期、文件的上次扫描日期以及对扫描设置的任何修改。iSwift 技术是对用于 NTFS 文件系统的 iChecker 技术的增强版。
使用 iChecker 技术	**启用**	该技术允许通过排除特定文件不扫描的方式提高扫描速度。该技术将使用特殊算法将文件排除在扫描范围之外，该算法会考虑 Kaspersky Endpoint Security 数据库的发布日期、文件的上次扫描日期以及对扫描设置的任何修改。iChecker 技术受到一些限制：它无法操作大型文件，并且仅能应用于具有应用程序可识别结构的文件（例如：EXE、DLL、LNK、TTF、INF、SYS、COM、CHM、ZIP 和 RAR）。

参数	值	描述
扫描 Microsoft Office 格式文件	**启用**	扫描 Microsoft Office 文件（DOC、DOCX、XLS、PPT 和其他 Microsoft 扩展程序）。Office 格式文件也包括 OLE 对象。应用程序扫描小于 1 MB 的 office 格式文件，无论该复选框是否被选中。
扫描电子邮件格式文件	**启用**	扫描电子邮件格式的文件。应用程序扫描 MSG 和 EML 文件。电子邮件格式的文件也包括 OLE 对象和 MHT 文件。Kaspersky Endpoint Security 扫描小于 1 MB 的电子邮件格式的文件，无论该复选框是否被选中。
扫描模式	**智能模式**	在该模式中，文件威胁防护将基于对象所做操作进行分析以扫描对象。例如，当操作某个 Microsoft Office 文档时，Kaspersky Endpoint Security 将在其首次打开和最后一次关闭时扫描该文件。覆盖文件的中间操作不会引起文件扫描。
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。

自动暂停文件威胁防护

您可以配置“文件威胁防护”在指定时间或处理特定应用程序时自动暂停。

只有“文件威胁防护”与某些应用程序冲突时，才应将其暂停作为最后手段。如果组件在运行过程中产生任何冲突，建议您联系 Kaspersky 技术支持。支持专家将帮助您设置“文件威胁防护”组件以便与您的计算机上的其他应用程序同时运行。

要配置“文件威胁防护”的自动暂停：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**文件威胁防护**”。
3. 单击“**高级设置**”。
4. 在“**暂停文件威胁防护**”区域，单击“**暂停文件威胁防护**”链接。
5. 在打开的窗口中，配置暂停文件威胁防护的设置：
   a. 配置计划以自动暂停文件威胁防护。
   b. 创建其操作可以导致文件威胁防护暂停的应用程序的列表。
6. 保存更改。

更改“文件威胁防护”组件对受感染文件执行的操作

默认情况下，“文件威胁防护”组件将自动尝试对已经检测到的所有受感染文件执行清除操作。如果清除失败，“文件威胁防护”组件将删除这些文件。

要更改“文件威胁防护”组件对受感染文件执行的操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**文件威胁防护**”。

3. 在“**检测到威胁后的操作**”块，选择相关选项：

   - “**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。

   - “**清除；如果清除失败则阻止**”。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，应用程序将阻止这些文件。

   - “**阻止**”。如果选择该选项，应用程序将自动阻止受感染的文件，而不试图对其进行清除或删除。

   在对感染的文件进行清除或删除操作之前，应用程序会创建一个备份，以免日后会需要恢复该文件或对该文件进行清除。

4. 保存更改。

构成“文件威胁防护”组件的保护范围

保护范围是指组件启用时的扫描对象。不同组件的保护范围有不同的参数。要扫描的文件的位置和类型是“文件威胁防护”组件保护范围的属性。默认情况下，“文件威胁防护”组件仅扫描从硬盘、可移动驱动器和网络驱动器运行的潜在受感染文件。

在选择要扫描的文件类型时，请考虑以下信息：

1. 将恶意代码引入某些格式的文件并随后将其激活的可能性很低（例如 TXT格式）。同时，有些文件格式包含可执行代码（如 .exe、.dll）。可执行代码还可能包含在并非用于此用途的格式（例如 DOC 格式）的文件中。这些文件中，恶意代码入侵并激活的可能性高。

2. 入侵者可能会把可执行文件的扩展名重命名为 .txt，然后将其中的病毒或其他恶意应用程序发送到您的计算机中。如果您按照扩展名选择扫描文件，程序将在扫描期间忽略该文件。如果选择按格式扫描文件，则 Kaspersky Endpoint Security 会分析文件标头，和扩展名无关。如果此分析显示文件具有可执行文件的格式（例如，EXE），则应用程序将对其进行扫描。

要创建保护范围，请执行以下操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**文件威胁防护**”。

3. 单击“**高级设置**”。

4. 在“**文件类型**”块中，指定您希望“文件威胁防护”组件扫描的文件类型：

- “**所有文件**”。如果启用该设置，Kaspersky Endpoint Security 将毫无例外地扫描所有文件（所有格式和扩展名）。
- “**按格式扫描文件**”。如果启用该设置，则应用程序仅扫描被感染的文件。在扫描文件以查找恶意代码之前，系统将分析文件的内部头以确定文件的格式（例如，.txt、.doc 或 .exe）。该扫描也查找具有特殊文件扩展名的文件。
- “**按扩展名扫描文件**”。如果启用该设置，则应用程序仅扫描被感染的文件。此时，系统将根据文件的扩展名确定文件格式。

5. 单击**编辑保护范围**链接。

6. 在打开的窗口中，选择您要添加到保护范围或从保护范围排除的对象。

> 您无法删除或编辑包括在默认保护范围中的对象。

7. 如果您希望将新对象添加至保护范围：

   a. 单击“**添加**”。

   文件夹树打开。

   b. 在**路径**字段，输入文件夹或文件的路径。

   使用掩码：

   - `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\*\*.txt` 将包括位于 C: 驱动器的文件夹（但不包括子文件夹）中所有具有 TXT 扩展名的文件的路径。
   - 两个连续 `*` 字符在文件或文件夹名称中代表任意一组字符（包括空集），包括 `\` 和 `/` 字符（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\**\*.txt` 将包括位于 `Folder` 嵌套子文件夹（除了 `Folder` 本身）中所有带 TXT 扩展名的文件的路径。掩码必须包含至少一个嵌套级别。掩码 `C:\**\*.txt` 不是有效掩码。
   - `?`（问号）字符代表任意单个字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\???.txt` 将包括位于 `Folder` 文件夹中所有带 TXT 扩展名且名称由三个字符构成的文件的路径。

   您可以在文件或文件夹路径中的任何位置使用掩码。例如，如果您希望扫描范围包括计算机上所有用户账户的下载文件夹，请输入 `C:\Users\*\Downloads\` 掩码。

   计算机的文件资源列表中的“**此 PC**”对象包括以下对象：**所有硬盘驱动器**、**所有网络驱动器** 和 **所有可移动驱动器**。

   您可以从扫描排除对象，而不用将其从对象列表删除。为此，清空对象旁边的复选框。

8. 保存更改。

使用扫描方法

Kaspersky Endpoint Security 使用一种称为机器学习和特征码分析的扫描技术。在特征码分析中，Kaspersky Endpoint Security 会将检测对象与其数据库中的记录进行匹配。根据 Kaspersky 专家的推荐，机器学习和签名分析始终启用。

您可以使用启发式分析提高保护效率。当扫描文件以查找恶意代码时，启发式分析执行可执行文件中的指令。启发式分析执行的指令数量取决于启发式分析级别。启发式分析级别可在全面搜索新威胁、加载操作系统资源和启发式分析持续时间之间进行平衡。

要配置“文件威胁防护”组件运行中启发式分析的使用：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**文件威胁防护**”。
3. 单击“**高级设置**”。
4. 如果您想让应用程序使用启发式分析来防护文件威胁，在**启发式分析**块选择**扫描方式**复选框。然后使用滑块设置启发式分析的级别：**轻度扫描**、**中度扫描**或**深度扫描**。
5. 保存更改。

在“文件威胁防护”组件的运行中使用扫描技术

要配置“文件威胁防护”组件运行中扫描技术的使用：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**文件威胁防护**”。
3. 单击“**高级设置**”。
4. 在“**扫描技术**”块，选中您要在文件威胁防护中使用的技术的名称旁边的复选框。
   - “**使用 iSwift 技术**”。该技术允许通过排除特定文件不扫描的方式提高扫描速度。该技术将使用特殊算法将文件排除在扫描范围之外，该算法会考虑 Kaspersky Endpoint Security 数据库的发布日期、文件的上次扫描日期以及对扫描设置的任何修改。iSwift 技术是对用于 NTFS 文件系统的 iChecker 技术的增强版。
   - “**使用 iChecker 技术**”。该技术允许通过排除特定文件不扫描的方式提高扫描速度。该技术将使用特殊算法将文件排除在扫描范围之外，该算法会考虑 Kaspersky Endpoint Security 数据库的发布日期、文件的上次扫描日期以及对扫描设置的任何修改。iChecker 技术受到一些限制：它无法操作大型文件，并且仅能应用于具有应用程序可识别结构的文件（例如：EXE、DLL、LNK、TTF、INF、SYS、COM、CHM、ZIP 和 RAR）。
5. 保存更改。

优化文件扫描

您可以通过减少扫描时间和提高 Kaspersky Endpoint Security 的运行速度来优化“文件威胁防护”组件执行的文件扫描。这可以通过仅扫描新文件和上次扫描后经过修改的文件来实现。此模式适用于简单文件和复合文件。

您也可以启用 iChecker 和 iSwift 技术，在扫描中排除最近一次扫描后未修改的文件，从而优化文件扫描速度。

要优化文件扫描，请执行以下操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**文件威胁防护**”。
3. 单击“**高级设置**”。
4. 在“**优化**”块中，选中“**仅扫描新建和已修改的文件**”复选框。
5. 保存更改。

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。

用于处理受感染复合文件（杀毒或删除）的方法取决于文件类型。

“文件威胁防护”组件会清除 ZIP、GZIP、BZIP、RAR、TAR、ARJ、CAB、LHA、JAR 和 ICE 格式的复合文件并删除所有其它格式的文件（邮件数据库除外）。

要配置复合文件的扫描，请执行以下步骤：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**文件威胁防护**”。
3. 单击“**高级设置**”。
4. 在“**扫描复合文件**”块中，指定您想要扫描的复合文件类型：存档、分发包、邮件或 Office 格式文件。
5. 如果仅扫描新建和已修改的文件被禁用，配置扫描每种复合文件的设置：扫描所有该类型的文件或仅扫描新文件。

   如果仅扫描新建和已修改的文件被启用，Kaspersky Endpoint Security 仅扫描所有类型的新建和已修改的复合文件。

6. 配置复合文件扫描的高级设置。

- “**复合文件大于指定值时不解压**”。

  如果选中该复选框，Kaspersky Endpoint Security 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，Kaspersky Endpoint Security 将扫描所有大小的复合文件。

  > 无论是否选中“**复合文件大于指定值时不解压**”复选框，Kaspersky Endpoint Security 均会扫描从存档中提取的大型文件。

- “**在后台解压复合文件**”。

  如果选中该复选框，Kaspersky Endpoint Security 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，Kaspersky Endpoint Security 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，Kaspersky Endpoint Security 才会提供对这些文件的访问权限。

7. 保存更改。

更改扫描模式

*扫描模式*是指触发“文件威胁防护”组件进行文件扫描的条件。默认情况下，Kaspersky Endpoint Security 以智能模式扫描文件。在此文件扫描模式下，“文件威胁防护”组件将确定是否在用户、应用程序（以用户身份在登录的帐户下或用不同帐户）或操作系统对文件执行分析操作后扫描文件。例如，当操作某个 Microsoft Office Word 文档时，Kaspersky Endpoint Security 将在其首次打开和最后一次关闭时扫描该文件。覆盖文件的中间操作不会引起文件扫描。

要更改文件扫描模式，请执行以下操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**文件威胁防护**”。

3. 单击“**高级设置**”。

4. 在“**扫描模式**”块，选择所需的模式：

   - “**智能模式**”。在该模式中，文件威胁防护将基于对象所做操作进行分析以扫描对象。例如，当操作某个 Microsoft Office 文档时，Kaspersky Endpoint Security 将在其首次打开和最后一次关闭时扫描该文件。覆盖文件的中间操作不会引起文件扫描。

   - “**在访问和修改时**”。在该模式中，文件威胁防护将在出现打开/修改文件的尝试时扫描对象。

   - “**在访问时**”。在该模式中，文件威胁防护将在出现打开对象的尝试时进行扫描。

   - “**执行时**”。在该模式中，文件威胁防护仅在出现运行文件的尝试时扫描对象。

5. 保存更改。

容器扫描

*容器*是一个隔离的环境，应用程序可以在其中运行而无需与操作系统直接交互。使用容器存在以下风险：

- 黑客可能能够利用容器化漏洞来破坏容器内的应用程序。
- 黑客可能会利用容器环境的不安全配置来获取对计算机上的数据的未经授权的访问或破坏系统的完整性。
- 成功攻击容器可以让黑客获得计算机上的数据。
- 黑客可能利用网络漏洞来拦截网络流量。

Kaspersky Endpoint Security 不仅扫描磁盘上的文件，还扫描容器内的文件。也就是说，Kaspersky Endpoint Security 是一个用于检测容器内部恶意活动的外部工具。这可以维持容器的性能并防止与容器内的其他应用程序发生冲突。不支持在容器内安装 Kaspersky Endpoint Security。

除了提供容器安全之外，Kaspersky Endpoint Security 还允许使用应用程序控制管理容器内的应用程序。容器的应用程序控制配置方式与计算机上安装的应用程序的配置方式相同。系统完整性监控还支持容器。

容器要求

- 该容器必须是 Docker 容器。不支持其他容器化工具。
- 容器必须以进程隔离模式运行。不支持 Hyper-V 隔离模式。
- 容器必须放置在 Windows Server 2016、2019 或 2022 服务器上（Docker Host）。
- 容器必须包含 Windows 映像 (Docker Image）。不支持 Windows 10 和 11。不支持 Linux 镜像。

检测到威胁后的操作

如果在容器内检测到威胁，该应用程序将应用为文件威胁防护组件选择的操作。容器扫描有附加设置（请参阅下面的说明）。如果检测到威胁，应用程序会阻止恶意活动并执行选定的操作（例如，尝试对对象清除）。如果无法清除检测到的对象， Kaspersky Endpoint Security 可以停止该容器。默认情况下，容器停止功能是禁用的。

如何在管理控制台 (MMC) 中配置容器扫描

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **基本威胁防护** → **文件威胁防护**。
4. 单击“**设置**”。
5. 这将打开一个窗口；在该窗口中，选择“**附加**”选项卡。

6. 在“**扫描在 Windows 容器中执行的文件操作**”块，配置容器扫描设置：

   - “**如果清除失败，则停止容器**”。应用程序可能没有足够的对检测到的对象进行读写的权限。在这种情况下，不可能对检测到的对象进行清除或删除。如果选中此复选框，应用程序将阻止检测到的对象并停止容器。如果清除此复选框，应用程序将仅阻止检测到的对象。

   - “**不扫描在 Windows 容器中执行的文件操作**”。如果选中该复选框，应用程序仅在容器启动时扫描容器。如果清除该复选框，应用程序将实时连续扫描容器。

7. 保存更改。

如何在 Web Console 和云控制台中配置容器扫描

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

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

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. 在“**高级设置**”下，选择“**性能**”选项卡。

6. 在“**扫描优化**”块，配置容器扫描设置：

   - “**如果清除失败则停止容器**”。应用程序可能没有足够的对检测到的对象进行读写的权限。在这种情况下，不可能对检测到的对象进行清除或删除。如果选中此复选框，应用程序将阻止检测到的对象并停止容器。如果清除此复选框，应用程序将仅阻止检测到的对象。

   - “**不扫描在 Windows 容器中执行的文件操作**”。如果选中该复选框，应用程序仅在容器启动时扫描容器。如果清除该复选框，应用程序将实时连续扫描容器。

7. 保存更改。

如何在应用程序界面中配置容器扫描

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**文件威胁防护**”。

3. 在“**扫描在 Windows 容器中执行的文件操作**”块，配置容器扫描设置：

   - “**如果清除失败，则停止容器**”。应用程序可能没有足够的对检测到的对象进行读写的权限。在这种情况下，不可能对检测到的对象进行清除或删除。如果选中此复选框，应用程序将阻止检测到的对象并停止容器。如果清除此复选框，应用程序将仅阻止检测到的对象。

   - “**不扫描在 Windows 容器中执行的文件操作**”。如果选中该复选框，应用程序仅在容器启动时扫描容器。如果清除该复选框，应用程序将实时连续扫描容器。

4. 保存更改。

主机入侵防御

如果 Kaspersky Endpoint Security 安装在运行 Windows for Workstations 的计算机上，则该组件可用。如果 Kaspersky Endpoint Security 安装在运行 Windows for Servers 的计算机上，则该组件不可用。

“主机入侵防御”组件可避免应用程序执行可能给操作系统带来危险的操作，并确保控制对操作系统资源和个人数据的访问。该组件借助反病毒数据库和卡巴斯基安全网络云服务来提供计算机保护。

该组件通过*应用程序权限*来控制应用程序的操作。应用程序权限包括以下访问参数：

- 对操作系统资源（例如，自动启动选项、注册表项）的访问权限
- 对个人数据（例如文件和应用程序）的访问权限

应用程序的网络活动由防火墙组件使用*网络规则*控制。

在应用程序首次启动期间，“主机入侵防御”组件执行以下操作：

1. 使用下载的反病毒数据库检查应用程序的安全性。
2. 在卡巴斯基安全网络中检查应用程序安全性。

   建议您加入卡巴斯基安全网络以帮助“主机入侵防御”组件更有效地工作。

3. 将应用程序置于其中一个信任组中：*受信任*、*低限制*、*高限制*、*不信任*。

   信任组定义了在控制应用程序活动时 Kaspersky Endpoint Security 所引用的权限。Kaspersky Endpoint Security 会将应用程序放置在某个信任组中，具体取决于该应用程序可能对计算机造成的危险级别。

   Kaspersky Endpoint Security 将应用程序放置在“防火墙”和“主机入侵防御”组件的信任组中。您不能仅更改“防火墙”或“主机入侵防御”的信任组。

   如果您拒绝加入 KSN 或没有网络，Kaspersky Endpoint Security 会根据“主机入侵防御”组件的设置将应用程序放置在某个信任组中。从 KSN 收到应用程序的信誉后，可以自动更改信任组。

4. 根据信任组阻止应用程序操作。例如，“*高限制*”信任组中的应用程序被拒绝访问操作系统模块。

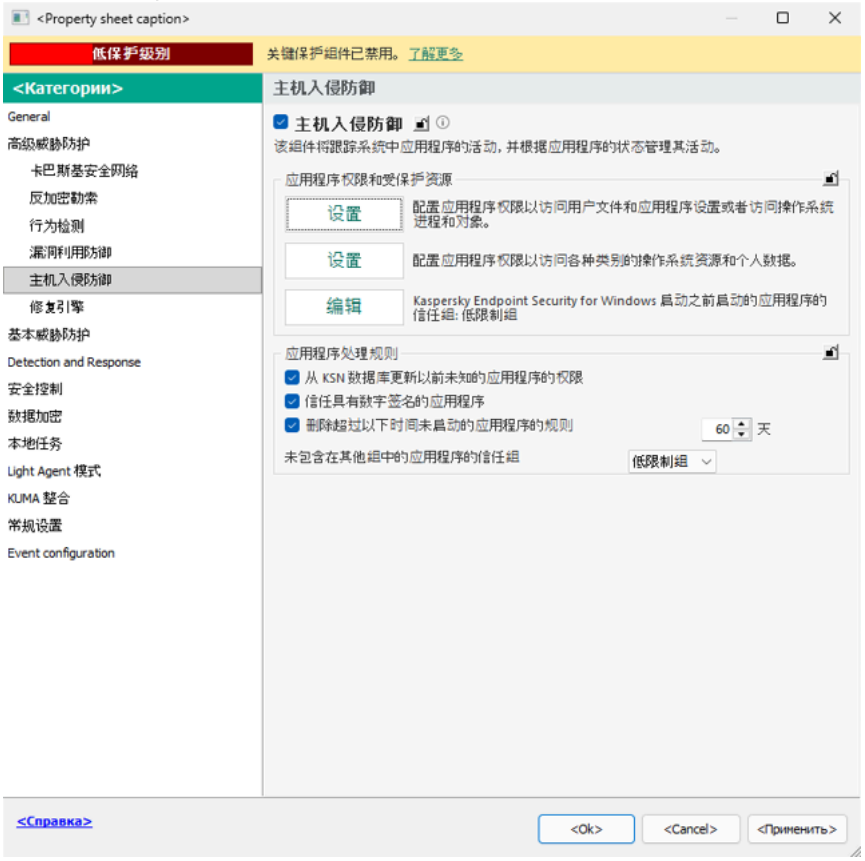
当应用程序下一次启动时，Kaspersky Endpoint Security 会检查该应用程序的完整性。如果应用程序未更改，则该组件对其应用当前应用程序权限。如果应用程序已经过修改，Kaspersky Endpoint Security 会分析应用程序，就像它首次启动时一样。

启用和禁用主机入侵防御

默认情况下，“主机入侵防御”组件已启用并在 Kaspersky 专家建议的模式下运行。

如何在管理控制台(MMC)中启用或禁用主机入侵防御组件

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **高级威胁防护** → **主机入侵防御**。



入侵防御设置

4. 使用“**主机入侵防御**”复选框启用或禁用组件。
5. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中启用或禁用主机入侵防御组件

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **主机威胁防护** → **主机入侵防御**。

5. 使用**主机入侵防御已启用**开关启用或禁用组件。

6. 保存更改。

如何在应用程序界面中启用或禁用主机入侵防御组件

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**高级威胁防护**” → “**主机入侵防御**”。

3. 使用**主机入侵防御**开关启用或禁用组件。

4. 保存更改。

如果启用了主机入侵防御组件，Kaspersky Endpoint Security 会将应用程序放置在某个信任组中，具体取决于该应用程序可能对计算机造成的危险级别。Kaspersky Endpoint Security 将根据其信任组阻止应用程序的操作。

管理应用程序信任组

每个应用程序首次启动时，“主机入侵防御”组件都会检查该应用程序的安全性并将其置于某个信任组中。

在应用程序扫描的第一阶段，Kaspersky Endpoint Security 将搜索已知应用程序的内部数据库查看是否存在匹配的条目，同时向卡巴斯基安全网络数据库发送请求（如果互联网连接可用）。根据内部数据库和卡巴斯基安全网络数据库的搜索结果，应用程序将被放置到某个信任组中：随后每次应用程序启动时，Kaspersky Endpoint Security 会向 KSN 数据库发送新查询，如果 KSN 数据库中该应用程序的信誉发生变化则将应用程序放置到不同信任组中。

您可以选择 Kaspersky Endpoint Security 自动将所有未知应用程序放置到的信任组。在 Kaspersky Endpoint Security 启动之前运行的应用程序会自动添加到在主机入侵防御设置中设置的信任组中。

> 对于先于 Kaspersky Endpoint Security 启动的应用程序，只有网络活动受到控制。按照防火墙设置中定义的网络规则执行控制。

更改应用程序的信任组

每个应用程序首次启动时，“主机入侵防御”组件都会检查该应用程序的安全性并将其置于某个信任组中。

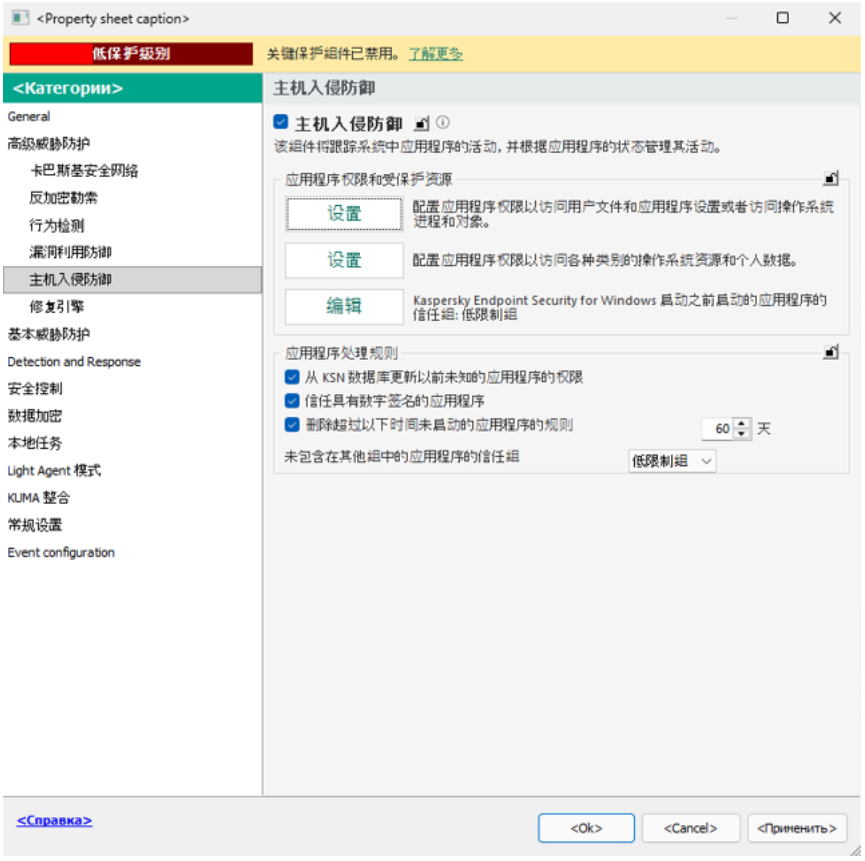
> Kaspersky 专家建议您不要将应用程序从自动分配的受信任组移动到不同的受信任组。作为替代，如有必要，您可以修改单个应用程序的权限。

如何在管理控制台 (MMC) 中更改应用程序信任组

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **高级威胁防护** → **主机入侵防御**。



入侵防御设置

4. 在“**应用程序权限和受保护资源**”块中单击“**设置**”按钮。

   这将打开应用程序权限配置窗口和受保护资源列表。

5. 选择**应用程序权限**选项卡。

6. 单击“**添加**”。

7. 在打开的窗口中，输入标准以搜索您要更改其信任组的应用程序。

   您可以输入应用程序名称或供应商名称。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。

8. 单击“**刷新**”。

   Kaspersky Endpoint Security 将在安装于受管理计算机上的应用程序列表中搜索应用程序。Kaspersky Endpoint Security 将显示满足您的搜索标准的应用程序列表。

9. 选择需要的应用程序。

10. 在**将选定应用程序添加至信任组**下拉列表中，为应用程序选择信任组。

11. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中更改应用程序信任组

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **主机威胁防护** → **主机入侵防御**。

5. 在“**应用程序权限和受保护资源**”区域，单击“**应用程序权限和受保护资源**”链接。

   这将打开应用程序权限配置窗口和受保护资源列表。

6. 选择**应用程序权限**选项卡。

   您将在窗口的左边看到信任组列表，窗口的右边显示它们的属性。

7. 单击“**添加**”。

   这将启动添加应用程序到信任组向导。

8. 为应用程序选择相关的信任组。

9. 选择“**应用程序**”类型。转到下一步。

   如果您要为多个应用程序更改信任组，选择“**组**”类型并为应用程序组定义名称。

10. 在打开的应用程序列表，选择您要更改其信任组的应用程序。

    使用过滤器。您可以输入应用程序名称或供应商名称。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。

11. 退出向导。

    应用程序将被添加到信任组。

12. 保存更改。

如何在应用程序界面中更改应用程序信任组

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**高级威胁防护**” → “**主机入侵防御**”。

3. 单击“**管理应用程序**”。

   这将打开已安装的应用程序列表。

4. 选择需要的应用程序。

5. 在应用程序的上下文菜单中，单击“**限制**” → “**<信任组>**”。

6. 保存更改。

结果，应用程序将被放置到其他信任组。Kaspersky Endpoint Security 将根据其信任组阻止应用程序的操作。*(用户定义)*状态将被分配到该应用程序。如果应用程序在卡巴斯基安全网络中的信誉被更改，主机入侵防御组件将使该应用程序的信任组保持不变。

配置信任组权限

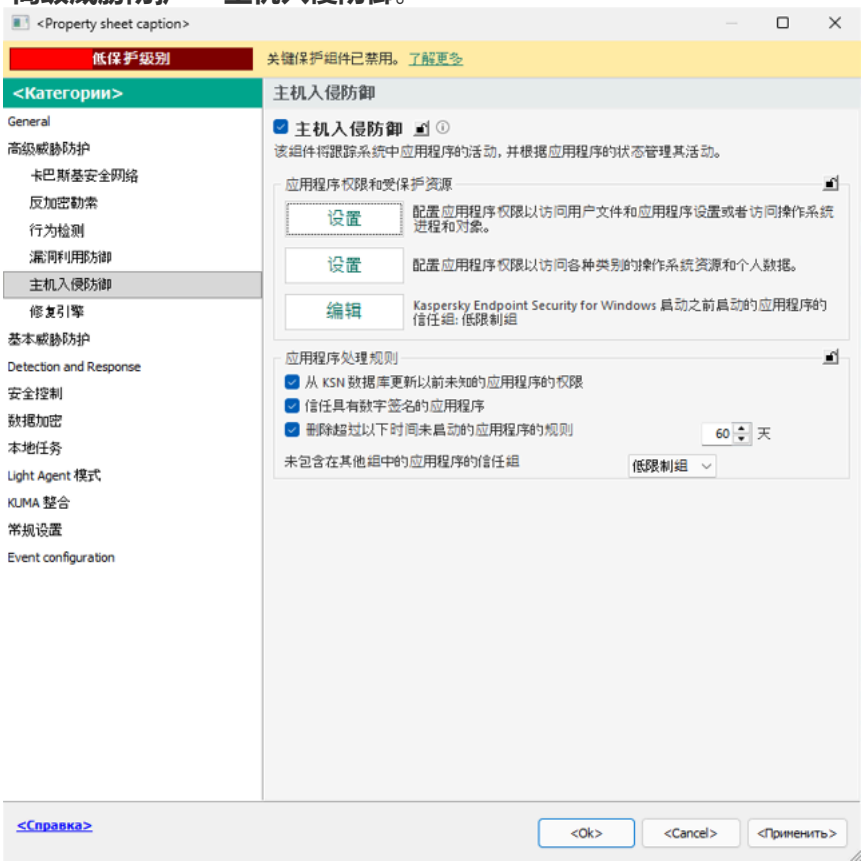
默认将为不同的信任组创建最佳应用程序权限。信任组中的应用程序组的权限设置会继承信任组权限设置的值。

如何在管理控制台 (MMC) 中更改信任组权限

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **高级威胁防护** → **主机入侵防御**。



入侵防御设置

4. 在“**应用程序权限和受保护资源**”块中单击“**设置**”按钮。
   这将打开应用程序权限配置窗口和受保护资源列表。

5. 转到“**应用程序权限**”选项卡。

6. 选择必要的信任组。

7. 在信任组的上下文菜单中，选择“**组权限**”。
   这将打开信任组属性。

8. 执行下列操作之一：

   - 如果您要编辑控制对操作系统注册表、用户文件和应用程序设置的操作的信任组权限，请选择“**文件和系统注册表**”。

   - 如果您要编辑控制对操作系统进程和对象的访问的信任组权限，请选择“**权限**”选项卡。

   > 应用程序的网络活动由防火墙组件使用*网络规则*控制。

9. 对于相关资源，在对应的操作列，右击打开上下文菜单并选择必要的选项：**继承**、**允许** (✓)或**阻止**(⊘)。

10. 如果您要监控对计算机资源的使用，请选择**记录事件** (/)。

    Kaspersky Endpoint Security 将记录主机入侵防御组件的操作信息。报告包含应用程序对对计算机资源的操作信息（允许或禁止）。报告也包含使用每个资源的应用程序信息。

11. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中更改信任组权限

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **主机威胁防护** → **主机入侵防御**。

5. 在“**应用程序权限和受保护资源**”区域，单击“**应用程序权限和受保护资源**”链接。

   这将打开应用程序权限配置窗口和受保护资源列表。

6. 转到“**应用程序权限**”选项卡。

   您将在窗口的左边看到信任组列表，窗口的右边显示它们的属性。

7. 在窗口左侧，选择相关信任组。

8. 在窗口右侧，在下拉列表中，做以下之一：

   - 如果您要编辑控制对操作系统注册表、用户文件和应用程序设置的操作的信任组权限，请选择“**文件和系统注册表**”。

   - 如果您要编辑控制对操作系统进程和对象的访问的信任组权限，请选择“**权限**”选项卡。

   应用程序的网络活动由防火墙组件使用*网络规则*控制。

9. 对于相关资源，在对应的操作列，选择必要的选项：**继承**、**允许** ( )、**阻止** ( )。

10. 如果您要监控对计算机资源的使用，请选择**记录事件** (/)。

    Kaspersky Endpoint Security 将记录主机入侵防御组件的操作信息。报告包含应用程序对对计算机资源的操作信息（允许或禁止）。报告也包含使用每个资源的应用程序信息。

11. 保存更改。

如何在应用程序界面中更改信任组权限

1. 打开主应用程序窗口并单击 按钮。

2. 在应用程序设置窗口中，选择“**高级威胁防护**” → “**主机入侵防御**”。

3. 单击“**管理应用程序**”。

   这将打开已安装的应用程序列表。

4. 选择必要的信任组。

5. 在信任组的上下文菜单中，选择“**详情和规则**”。

   这将打开信任组属性。

6. 执行下列操作之一：

   - 如果您要编辑控制对操作系统注册表、用户文件和应用程序设置的操作的信任组权限，请选择“**文件和系统注册表**”。
   - 如果您要编辑控制对操作系统进程和对象的访问的信任组权限，请选择“**权限**”选项卡。

   应用程序的网络活动由防火墙组件使用*网络规则*控制。

7. 对于相关资源，在对应的操作列，右击打开上下文菜单并选择必要的选项：**继承**、**允许**（）或**拒绝**（）。

8. 如果您要监控对计算机资源的使用，请选择**记录事件**（）。

   Kaspersky Endpoint Security 将记录主机入侵防御组件的操作信息。报告包含应用程序对对计算机资源的操作信息（允许或禁止）。报告也包含使用每个资源的应用程序信息。

9. 保存更改。

信任组权限将被更改。Kaspersky Endpoint Security 将根据其信任组阻止应用程序的操作。状态（*自定义设置*）将被分配到信任组。

选择在 Kaspersky Endpoint Security 启动之前启动的应用程序受信任组

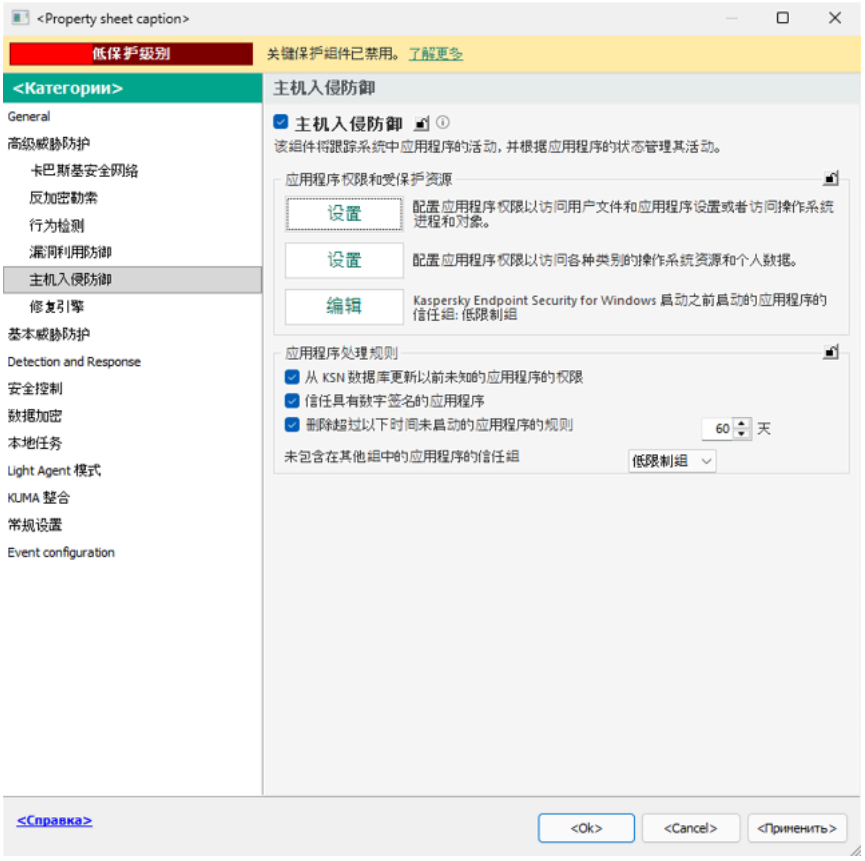
对于先于 Kaspersky Endpoint Security 启动的应用程序，只有网络活动受到控制。按照防火墙设置中定义的网络规则执行控制。若要指定必须为此类应用程序的网络活动应用哪些网络规则，您必须选择受信任组。

如何在管理控制台(MMC)中为在 Kaspersky Endpoint Security 之前启动的应用程序选择信任组

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **高级威胁防护** → **主机入侵防御**。



入侵防御设置

4. 在“**应用程序权限和受保护资源**”块中单击“**编辑**”按钮。

5. 对于 **Kaspersky Endpoint Security 启动之前启动的应用程序的信任组**设置，选择适当的信任组。

6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中为在 Kaspersky Endpoint Security 之前启动的应用程序选择信任组

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **主机威胁防护** → **主机入侵防御**。

5. 对于 **Kaspersky Endpoint Security 启动之前启动的应用程序的信任组**设置，选择适当的信任组。

6. 保存更改。

如何在应用程序界面中为在 Kaspersky Endpoint Security 之前启动的应用程序选择信任组

1. 打开主应用程序窗口并单击 按钮。

2. 在应用程序设置窗口中，选择“**高级威胁防护**” → “**主机入侵防御**”。

3. 在“**Kaspersky Endpoint Security 启动之前启动的应用程序的信任组**”块中，选择适当的信任组。

4. 保存更改。

结果，在 Kaspersky Endpoint Security 之前启动的应用程序将被放置到其他信任组。Kaspersky Endpoint Security 将根据其信任组阻止应用程序的操作。

为未知应用程序选择信任组

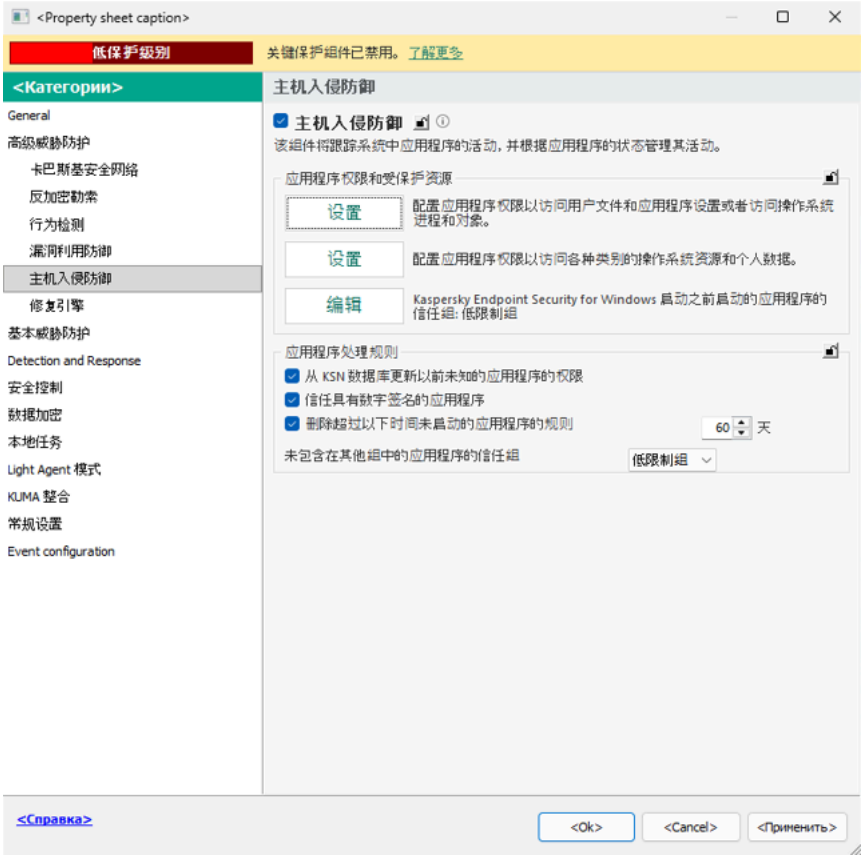
在应用程序第一次启动过程中，主机入侵防御组件为应用程序决定信任组。如果您没有互联网连接或卡巴斯基安全网络没有该应用程序的信息，Kaspersky Endpoint Security 默认会将该应用程序放置在*低限制*组。当先前未知的应用程序的信息在 KSN 中被检测到时，Kaspersky Endpoint Security 将更新该应用程序的权限。随后您可以手动编辑应用程序权限。

如何在管理控制台 (MMC) 中为未知应用程序选择信任组

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **高级威胁防护 → 主机入侵防御**。



入侵防御设置

4. 在**应用程序处理规则**块，使用**未包含在其他组中的应用程序的信任组**下拉列表选择必要的信任组。

   如果启用了参与卡巴斯基安全网络，Kaspersky Endpoint Security 会在每次应用程序启动时向 KSN 请求有关应用程序的信誉。根据收到的响应，应用程序可能会被移动至与“主机入侵防御”组件设置中指定的信任组不同的信任组中。

5. 使用**从 KSN 数据库更新以前未知的应用程序的权限**复选框配置未知应用程序权限的自动更新。

6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中为未知应用程序选择信任组

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

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **主机威胁防护** → **主机入侵防御**。
5. 在**应用程序处理规则**块，使用**未包含在其他组中的应用程序的信任组**下拉列表选择必要的信任组。

   如果启用了参与卡巴斯基安全网络，Kaspersky Endpoint Security 会在每次应用程序启动时向 KSN 请求有关应用程序的信誉。根据收到的响应，应用程序可能会被移动至与“主机入侵防御”组件设置中指定的信任组不同的信任组中。
6. 使用**从 KSN 数据库更新以前未知的应用程序的权限**复选框配置未知应用程序权限的自动更新。
7. 保存更改。

如何在应用程序界面中为未知应用程序选择信任组

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**高级威胁防护**” → “**主机入侵防御**”。
3. 在“**应用程序处理规则**”块中，选择适当的信任组。

   如果启用了参与卡巴斯基安全网络，Kaspersky Endpoint Security 会在每次应用程序启动时向 KSN 请求有关应用程序的信誉。根据收到的响应，应用程序可能会被移动至与“主机入侵防御”组件设置中指定的信任组不同的信任组中。
4. 使用**从 KSN 为之前未知应用程序更新规则**复选框配置未知应用程序权限的自动更新。
5. 保存更改。

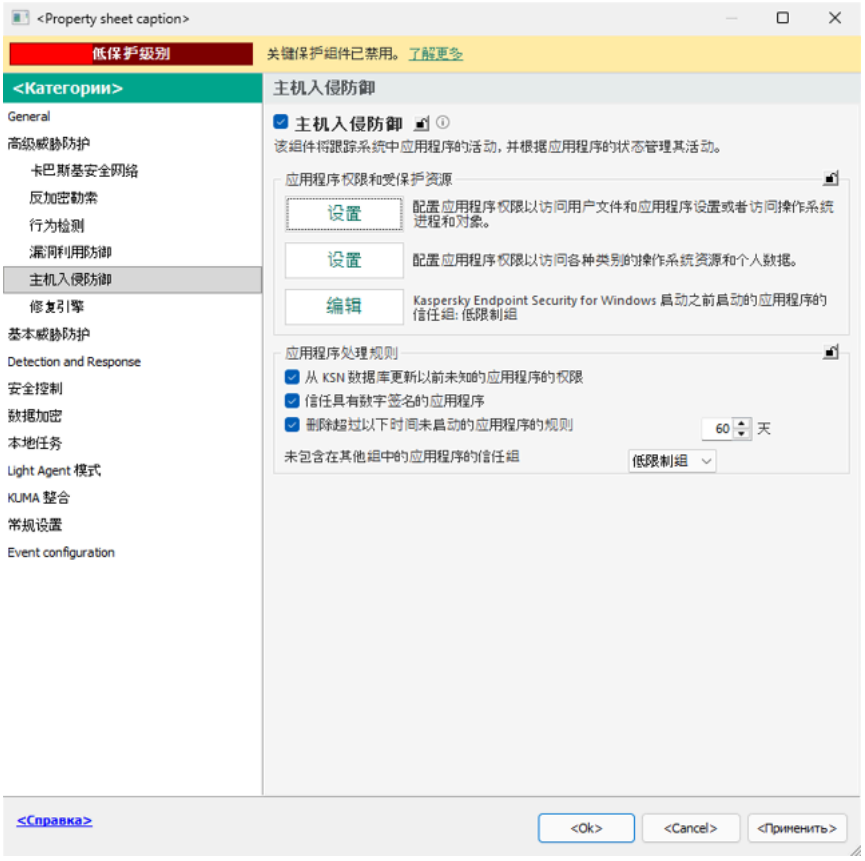
为数字签名的应用程序选择信任组

Kaspersky Endpoint Security 总是将带有 Microsoft 证书签名或卡巴斯基证书签名的应用程序放入“*受信任*”组。

如何在管理控制台 (MMC) 中为数字签名的应用程序选择信任组

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **高级威胁防护** → **主机入侵防御**。



入侵防御设置

4. 在“**应用程序处理规则**”块中，使用“**信任具有数字签名的应用程序**”复选框启用或禁用将包含受信任供应商数字签名的应用程序自动分配到“受信任组”信任组。

   *受信任供应商*是被 Kaspersky 包含在受信任组中的软件供应商。您也可以手动添加供应商证书到受信任系统证书存储。

   如果清空该选框，“主机入侵防御”组件将不再信任经过数字签名的应用程序，并使用其他参数以确定它们的信任组。

5. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中为数字签名的应用程序选择信任组

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **主机威胁防护** → **主机入侵防御**。

5. 在“**应用程序处理规则**”块中，使用“**信任具有数字签名的应用程序**”复选框启用或禁用将包含受信任供应商数字签名的应用程序自动分配到“受信任组”信任组。

   *受信任供应商*是被 Kaspersky 包含在受信任组中的软件供应商。您也可以手动添加供应商证书到受信任系统证书存储。

   如果清空该选框，“主机入侵防御”组件将不再信任经过数字签名的应用程序，并使用其他参数以确定它们的信任组。

6. 保存更改。

如何在应用程序界面中为数字签名的应用程序选择信任组

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**高级威胁防护**” → “**主机入侵防御**”。

3. 在“**应用程序处理规则**”块中，使用“**信任具有数字签名的应用程序**”复选框启用或禁用将包含受信任供应商数字签名的应用程序自动分配到“受信任组”信任组。

   *受信任供应商*是被 Kaspersky 包含在受信任组中的软件供应商。您也可以手动添加供应商证书到受信任系统证书存储。

   如果清空该选框，“主机入侵防御”组件将不再信任经过数字签名的应用程序，并使用其他参数以确定它们的信任组。

4. 保存更改。

管理应用程序权限

默认情况下，应用程序的活动基于 Kaspersky Endpoint Security 在此应用程序第一次启动时将其分配到的特别信任组定义的应用程序权限来控制。如有必要，您可以为整个信任组、单个应用程序或信任组内的一组应用程序编辑应用程序权限。

手动定义的应用程序权限比信任组的应用程序权限具有更高的优先级。换言之，如果手动定义的应用程序权限与信任组定义的应用程序权限不同，主机入侵防御组件根据手动定义的应用程序权限控制应用程序活动。

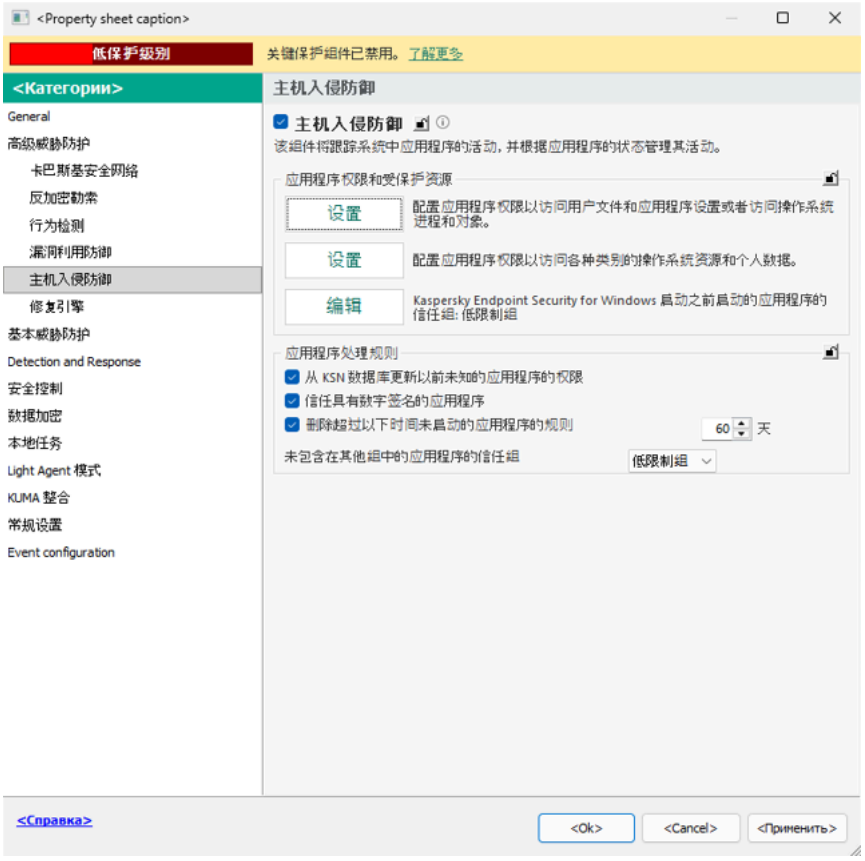
您为应用程序创建的规则被子应用程序继承。例如，如果您拒绝所有 cmd.exe 的网络活动，使用 cmd.exe 启动的 notepad.exe 的所有网络活动也将被拒绝。如果应用程序不是该应用程序的子程序，则规则不被继承。

如何在管理控制台 (MMC) 中更改应用程序权限

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **高级威胁防护** → **主机入侵防御**。



入侵防御设置

4. 在“**应用程序权限和受保护资源**”块中单击“**设置**”按钮。

   这将打开应用程序权限配置窗口和受保护资源列表。

5. 转到“**应用程序权限**”选项卡。

6. 单击“**添加**”。

7. 在打开的窗口中，输入标准以搜索您要更改其应用程序权限的应用程序。

   您可以输入应用程序名称或供应商名称。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。

8. 单击“**刷新**”。

   Kaspersky Endpoint Security 将在安装于受管理计算机上的应用程序列表中搜索应用程序。Kaspersky Endpoint Security 将显示满足您的搜索标准的应用程序列表。

9. 选择需要的应用程序。

10. 在**将选定应用程序添加至信任组**下拉列表中，选择**默认组**并单击**确定**。

    应用程序将被添加到默认组。

11. 选择相关应用程序并从应用程序的上下文菜单中选择**应用程序权限**。

    这将打开应用程序属性。

12. 执行下列操作之一：

    - 如果您要编辑控制对操作系统注册表、用户文件和应用程序设置的操作的信任组权限，请选择“**文件和系统注册表**”。
    - 如果您要编辑控制对操作系统进程和对象的访问的信任组权限，请选择“**权限**”选项卡。

    应用程序的网络活动由防火墙组件使用*网络规则*控制。

13. 对于相关资源，在对应的操作列，右击打开上下文菜单并选择必要的选项：**继承**、**允许** (✓)或**阻止**(⊘)。
14. 如果您要监控对计算机资源的使用，请选择**记录事件** (✓ / ⊘)。

    Kaspersky Endpoint Security 将记录主机入侵防御组件的操作信息。报告包含应用程序对对计算机资源的操作信息（允许或禁止）。报告也包含使用每个资源的应用程序信息。

15. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中更改应用程序权限

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

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。
4. 选择 **主机威胁防护** → **主机入侵防御**。
5. 在“**应用程序权限和受保护资源**”区域，单击“**应用程序权限和受保护资源**”链接。

   这将打开应用程序权限配置窗口和受保护资源列表。

6. 转到“**应用程序权限**”选项卡。

   您将在窗口的左边看到信任组列表，窗口的右边显示它们的属性。

7. 单击“**添加**”。

   这将启动添加应用程序到信任组向导。

8. 为应用程序选择相关的信任组。
9. 选择“**应用程序**”类型。转到下一步。

   如果您要为多个应用程序更改信任组，选择“**组**”类型并为应用程序组定义名称。

10. 在打开的应用程序列表，选择您要更改其应用程序权限的应用程序。

    使用过滤器。您可以输入应用程序名称或供应商名称。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。

11. 退出向导。

    应用程序将被添加到信任组。

12. 在窗口左侧，选择相关应用程序。

13. 在窗口右侧，在下拉列表中，做以下之一：

    - 如果您要编辑控制对操作系统注册表、用户文件和应用程序设置的操作的信任组权限，请选择“**文件和系统注册表**”。
    - 如果您要编辑控制对操作系统进程和对象的访问的信任组权限，请选择“**权限**”选项卡。

    应用程序的网络活动由防火墙组件使用*网络规则*控制。

14. 对于相关资源，在对应的操作列，选择必要的选项：**继承**、**允许** ( )、**阻止** ( )。
15. 如果您要监控对计算机资源的使用，请选择**记录事件** (/)。

    Kaspersky Endpoint Security 将记录主机入侵防御组件的操作信息。报告包含应用程序对对计算机资源的操作信息（允许或禁止）。报告也包含使用每个资源的应用程序信息。

16. 保存更改。

如何在应用程序界面中更改应用程序权限

1. 打开主应用程序窗口并单击 按钮。
2. 在应用程序设置窗口中，选择“**高级威胁防护**” → “**主机入侵防御**”。
3. 单击“**管理应用程序**”。

   这将打开已安装的应用程序列表。

4. 选择需要的应用程序。
5. 在应用程序的上下文菜单中，选择“**详情和规则**”。

   这将打开应用程序属性。

6. 执行下列操作之一：

   - 如果您要编辑控制对操作系统注册表、用户文件和应用程序设置的操作的信任组权限，请选择“**文件和系统注册表**”。
   - 如果您要编辑控制对操作系统进程和对象的访问的信任组权限，请选择“**权限**”选项卡。

7. 对于相关资源，在对应的操作列，右击打开上下文菜单并选择必要的选项：**继承**、**允许** ( )或**拒绝**( )。
8. 如果您要监控对计算机资源的使用，请选择**记录事件** ( )。

   Kaspersky Endpoint Security 将记录主机入侵防御组件的操作信息。报告包含应用程序对对计算机资源的操作信息（允许或禁止）。报告也包含使用每个资源的应用程序信息。

9. 选择**排除项**选项卡并配置应用程序的高级设置（参加你下表）。
10. 保存更改。

参数	描述
不扫描应用程序打开的文件	应用程序打开的所有文件被从 Kaspersky Endpoint Security 的扫描中排除。例如，如果您正使用应用程序备份文件，该功能帮助降低 Kaspersky Endpoint Security 的资源消耗。
不监控应用程序活动	Kaspersky Endpoint Security 将不监控应用程序文件和其在操作系统中的网络活动。您可以为 Kaspersky Endpoint Security 的不同组件配置应用程序活动监控： • "**不监控保护和控制组件**"。应用程序活动被以下组件监控：行为检测、漏洞利用防御、主机入侵防御、修复引擎和防火墙。 • "**不监控 Managed Detection and Response 和 Endpoint Detection and Response**"。应用程序活动由内置 MDR 代理和内置 EDR (KATA) 代理监控。 • "**不拦截 Endpoint Detection and Response 的控制台交互式输入**"。Kaspersky Endpoint Security 不会发送有关在控制台上管理应用程序的遥测数据。遥测数据由 Kaspersky Anti Targeted Attack Platform (EDR)使用。
不继承父进程(应用程序)的限制	为父进程配置的限制将不被 Kaspersky Endpoint Security 应用到子进程。父进程由配置了应用程序权限（主机入侵防御）和应用程序网络规则（防火墙）的应用程序启动。
不监控子应用程序活动	Kaspersky Endpoint Security 将不监控被该应用程序启动的应用程序的文件活动或网络活动。您可以递归地应用排除。这样应用程序就不会监控整个子应用程序链的活动。
允许与 Kaspersky Endpoint Security 的界面进行交互	Kaspersky Endpoint Security 自我保护阻止所有从远程计算机管理应用程序服务的尝试。如果选择该复选框，则允许远程访问应用程序通过 Kaspersky Endpoint Security 界面管理 Kaspersky Endpoint Security 设置。
不扫描加密流量 / 不扫描所有流量	应用程序发起的网络流量将被 Kaspersky Endpoint Security 从扫描排除。您可以从扫描排除所有流量，也可以仅排除加密流量。您也可以从扫描排除单个 IP 地址和端口号。 如果为受信任应用程序指定哈希值而不是路径，则 Kaspersky Endpoint Security 14.0 或更早版本不支持排除网络流量。

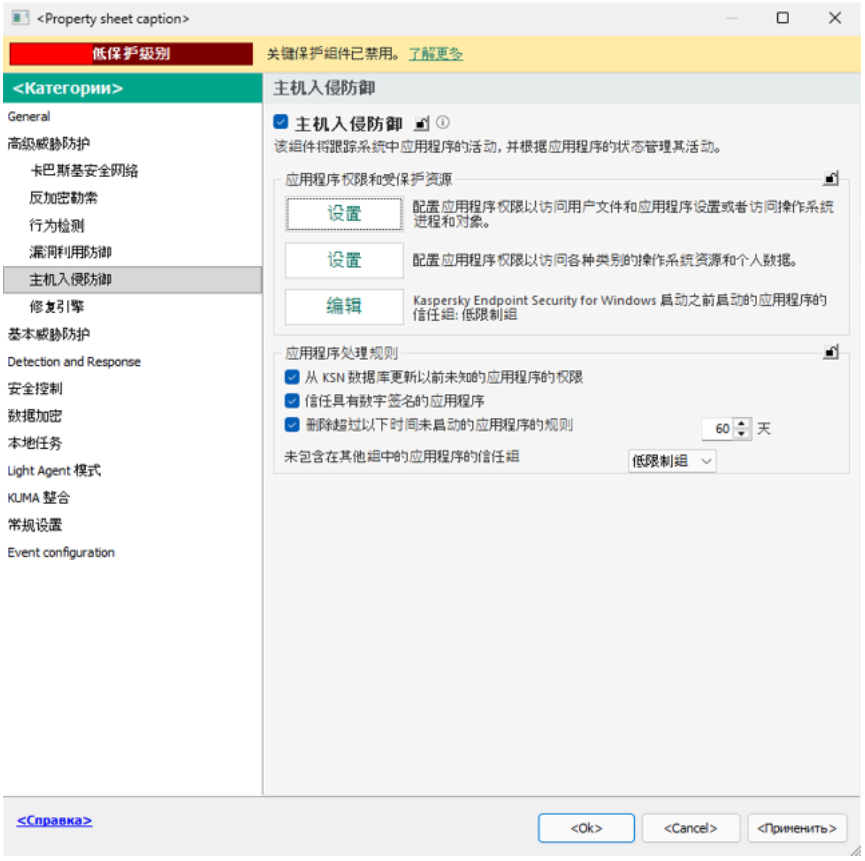
保护操作系统资源和个人数据

"主机入侵防御"组件管理应用程序对各种类别的操作系统资源和个人数据执行操作的权限。Kaspersky 专家已建立受保护资源的预设类别。例如，*操作系统*类别具有*启动设置*子类别，该子类别列出与应用程序自动运行相关的所有注册表键。您无法编辑或删除受保护资源的预设类别，或这些类别中的受保护资源。

如何在管理控制台 (MMC) 中添加受保护资源

1. 在 Kaspersky Security Center 管理控制台树中，选择"**策略**"。
2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **高级威胁防护** → **主机入侵防御**。



入侵防御设置

4. 在“**应用程序权限和受保护资源**”块中单击“**设置**”按钮。

   这将打开应用程序权限配置窗口和受保护资源列表。

5. 转到“**受保护资源**”选项卡。

   您将在窗口左侧看到受保护资源列表，以及根据特定的信任组访问这些资源的对应权限。

6. 选择您要向其添加新受保护资源的受保护资源的类别。

   如果您要添加子类别，单击**添加** → **类别**。

7. 单击**添加**按钮。在下拉列表中，选择您要添加的资源类型：**文件或文件夹**或**注册表键**。

8. 在打开的窗口中，选择一个文件、文件夹或注册表键。

   您可以查看应用程序访问所添加资源的权限。为此，在窗口左侧选择添加的资源，Kaspersky Endpoint Security 将显示每个信任组的访问权限。您也可以使用新资源旁边的复选框禁用应用程序对资源操作的控制。

9. 要将此策略应用到计算机，请关闭 🔒 挂锁图标并保存更改。

如何在 Web Console 和云控制台中添加受保护资源

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **主机威胁防护** → **主机入侵防御**。

5. 在“**应用程序权限和受保护资源**”区域，单击“**应用程序权限和受保护资源**”链接。

   这将打开应用程序权限配置窗口和受保护资源列表。

6. 转到“**受保护资源**”选项卡。

   您将在窗口左侧看到受保护资源列表，以及根据特定的信任组访问这些资源的对应权限。

7. 单击“**添加**”。

   新资源向导启动。

8. 在“**组名称**”块，选择您要向其添加新受保护资源的受保护资源的类别。

   如果您要添加子类别，选择“**受保护资源的类别**”选项。

9. 选择您要添加的资源类型：**文件或文件夹**或**注册表键**。

10. 选择一个文件、文件夹或注册表键。

11. 退出向导。

    您可以查看应用程序访问所添加资源的权限。为此，在窗口左侧选择添加的资源，Kaspersky Endpoint Security 将显示每个信任组的访问权限。您也可以使用**状态**栏中的复选框禁用应用程序对资源操作的控制。

12. 保存更改。

如何在应用程序界面中添加受保护资源

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**高级威胁防护**” → “**主机入侵防御**”。

3. 单击“**管理资源**”。

   受保护资源列表打开。

4. 选择您要向其添加新受保护资源的受保护资源的类别。

   如果您要添加子类别，单击**添加** → **类别**。

5. 单击**添加**按钮。在下拉列表中，选择您要添加的资源类型：**文件或文件夹**或**注册表键**。

6. 在打开的窗口中，选择一个文件、文件夹或注册表键。

   您可以查看应用程序访问所添加资源的权限。为此，在窗口左侧选择添加的资源，Kaspersky Endpoint Security 将显示一个应用程序列表以及每个应用程序的访问权限。您也可以使用**状态**栏的**启用控制**按钮来禁用应用程序对资源操作的控制。

7. 保存更改。

Kaspersky Endpoint Security 将控制对所添加的操作系统资源和个人数据的访问。Kaspersky Endpoint Security 基于分配给应用程序的信任组控制应用程序对资源的访问。您还可以更改应用程序的信任组。

删除有关未使用的应用程序的信息

Kaspersky Endpoint Security 使用应用程序权限来控制应用程序的活动。应用程序权限由其信任组确定。Kaspersky Endpoint Security 在应用程序第一次启动时将其放置在信任组。您可以手动更改应用程序的信任组。您还可以手动配置单个应用程序的权限。Kaspersky Endpoint Security 存储有关应用程序的以下信息：应用程序的信任组和应用程序的权限。

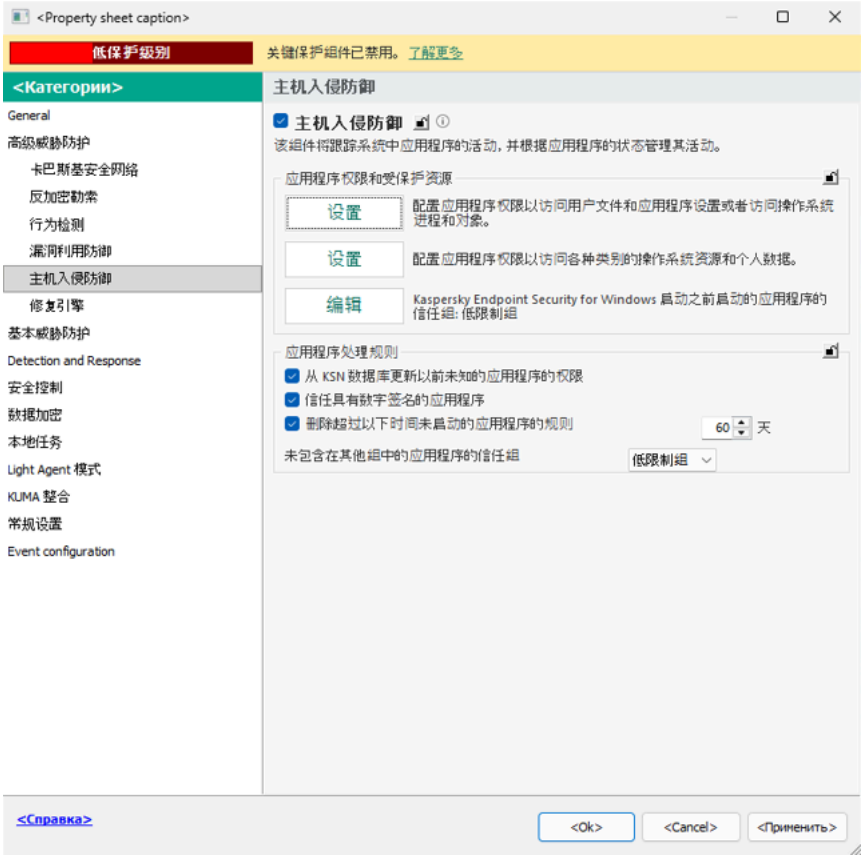
Kaspersky Endpoint Security 会自动删除有关未使用的应用程序的信息以节省计算机资源。Kaspersky Endpoint Security 根据以下规则删除应用程序信息：

- 如果应用程序的信任组和权限已自动确定，Kaspersky Endpoint Security 将在 30 天后删除有关此应用程序的信息。不能更改应用程序信息的存储期限或关闭自动删除。
- 如果您手动将应用程序放入信任组或配置其访问权限，Kaspersky Endpoint Security 将在 60 天（默认存储期限）后删除有关此应用程序的信息。您可以更改应用程序信息的存储期限，或关闭自动删除（请参见下面说明）。

当启动其信息已被删除的应用程序时，Kaspersky Endpoint Security 会像首次启动该应用程序一样对其进行分析。

如何在管理控制台(MMC)中配置对无用应用程序信息的自动检测

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **高级威胁防护** → **主机入侵防御**。



入侵防御设置

4. 在“**应用程序处理规则**”块中执行以下操作之一：
   - 如果要配置自动删除，请选择 **删除超过以下时间未启动的应用程序的规则 N 天** 复选框并输入天数。

     您手动放入信任组或手动配置其访问权限的应用程序的相关信息在定义的天数后将被 Kaspersky Endpoint Security 删除。有关已自动确定其信任组和应用程序权限的应用程序的信息也将在 30 天后被 Kaspersky Endpoint Security 删除。

- 如果您要关闭自动删除，请清空“**删除超过以下时间未启动的应用程序的规则 N 天**”复选框。

  您手动放入信任组或手动配置其访问权限的应用程序的相关信息将被 Kaspersky Endpoint Security 无限期存储，没有任何存储期限。Kaspersky Endpoint Security 在 30 天后将只删除已自动确定其信任组和应用程序权限的应用程序的相关信息。

5. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中配置对无用应用程序信息的自动检测

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **主机威胁防护** → **主机入侵防御**。

5. 在“**应用程序处理规则**”块中执行以下操作之一：

   - 如果要配置自动删除，请选择**删除超过以下天数未启动的应用程序的规则 (1 至 90)**复选框并输入天数。

     您手动放入信任组或手动配置其访问权限的应用程序的相关信息在定义的天数后将被 Kaspersky Endpoint Security 删除。有关已自动确定其信任组和应用程序权限的应用程序的信息也将在 30 天后被 Kaspersky Endpoint Security 删除。

   - 如果您要关闭自动删除，请清空“ **删除超过以下天数未启动的应用程序的规则 (1 至 90)**”复选框。

     您手动放入信任组或手动配置其访问权限的应用程序的相关信息将被 Kaspersky Endpoint Security 无限期存储，没有任何存储期限。Kaspersky Endpoint Security 在 30 天后将只删除已自动确定其信任组和应用程序权限的应用程序的相关信息。

6. 保存更改。

如何在应用程序界面中配置对无用应用程序信息的自动检测

1. 打开主应用程序窗口并单击 按钮。

2. 在应用程序设置窗口中，选择“**高级威胁防护**” → “**主机入侵防御**”。

3. 在“**应用程序处理规则**”块中执行以下操作之一：

   - 如果要配置自动删除，请选择 **删除超过以下时间未启动的应用程序的规则 N 天(从 1 到 90)** 复选框并输入天数。

     您手动放入信任组或手动配置其访问权限的应用程序的相关信息在定义的天数后将被 Kaspersky Endpoint Security 删除。有关已自动确定其信任组和应用程序权限的应用程序的信息也将在 30 天后被 Kaspersky Endpoint Security 删除。

   - 如果您要关闭自动删除，请清空“**删除超过以下时间未启动的应用程序的规则 N 天(从 1 到 90)**”复选框。

     您手动放入信任组或手动配置其访问权限的应用程序的相关信息将被 Kaspersky Endpoint Security 无限期存储，没有任何存储期限。Kaspersky Endpoint Security 在 30 天后将只删除已自动确定其信任组和应用程序权限的应用程序的相关信息。

4. 保存更改。

监控主机入侵防御

您可以接收主机入侵防御组件的操作报告。报告包含应用程序对对计算机资源的操作信息（允许或禁止）。报告也包含使用每个资源的应用程序信息。

要监控主机入侵防御操作，您需要启用报告写入。例如，您可以在主机入侵防御组件设置中启用转发个别应用程序报告。

当配置主机入侵防御监控时，当转发事件到 Kaspersky Security Center 时请考虑潜在的网络负载。您也可以启用仅保存报告到 Kaspersky Endpoint Security 本地日志中。

保护对音频和视频的访问

基于 Arm 架构的计算机不支持音频信号保护功能和网络摄像头访问保护功能。

网络罪犯可以使用特殊的程序获取对音频和视频设备的访问（例如麦克风和网络摄像头）。Kaspersky Endpoint Security 控制应用程序接收的音频流或视频流并保护数据免遭截取。

默认情况下，Kaspersky Endpoint Security 仅允许“*受信任*”组的应用程序接收音频和视频流。“*低限制*”、“*高限制*”和“*不信任*”组的应用程序不被允许接收来自设备的音频流和视频流。您可以手动允许应用程序接收音频流和视频流。

音频流保护的特殊功能

音频流保护具有以下特殊特性：

- 必须启用“主机入侵防御”组件，该功能才有效。
- 如果在“主机入侵防御”组件启动之前该应用程序开始接受音频流，则 Kaspersky Endpoint Security 允许该应用程序接收音频流且不显示任何通知。
- 如果您在应用程序开始接收音频流之后将该应用程序移动至“*不信任*组”或“*高限制*组”，Kaspersky Endpoint Security 将允许应用程序接收音频流且不显示任何通知。
- 应用程序访问录音设备的设置被更改后（例如，如果阻止了该应用程序接收音频流），则必须重启该应用程序才能阻止其继续接收音频流。
- 控制对录音设备音频流的访问不取决于应用程序的摄像头访问设置。
- Kaspersky Endpoint Security 仅保护对内置麦克风和外置麦克风的访问。不支持其他音频流设备。

- Kaspersky Endpoint Security 无法保证对其他诸如单反相机、便携式录像机和动作捕捉相机中音频流的保护。
- 当您在安装 Kaspersky Endpoint Security 之后首次运行音频和视频录制或播放应用程序时，音频和视频播放或录制可能会被中断。为了确保该功能能够控制应用程序对录音设备的访问，这是必要的。Kaspersky Endpoint Security 首次运行时控制音频硬件的系统设备将重新启动。

应用程序网络摄像头访问保护的特殊功能

摄像头访问保护功能拥有以下特别考虑和限制：

- 应用程序将控制从处理摄像头数据而来的视频和静止图像。
- 应用程序将控制视频流，如果其作为摄像头接收视频流的一部分。
- 应用程序仅控制在 Windows 设备管理器中显示为“图像设备”通过 USB 或 IEEE1394 连接的摄像头。
- Kaspersky Endpoint Security 支持以下摄像头：
  - Logitech HD Webcam C270
  - Logitech HD Webcam C310
  - Logitech Webcam C210
  - Logitech Webcam Pro 9000
  - Logitech HD Webcam C525
  - Microsoft LifeCam VX-1000
  - Microsoft LifeCam VX-2000
  - Microsoft LifeCam VX-3000
  - Microsoft LifeCam VX-800
  - Microsoft LifeCam Cinema

  Kaspersky 不保证支持不在列表中的摄像头。

BadUSB 攻击防护

某些病毒会修改 USB 设备的固件以欺骗操作系统，将 USB 伪装为键盘。结果，病毒可能在您的用户账户下执行命令以下载恶意软件。

BadUSB 攻击防护组件可以防止受感染的模拟键盘 USB 设备连接至计算机。

当 USB 设备连接至计算机并被操作系统识别为键盘时，应用程序将提示用户从该键盘输入其生成的数字代码或使用屏幕键盘（如果可用）（参见下图）。这个步骤称为键盘授权。

如果代码输入正确，应用程序会将识别参数（键盘的 VID/PID 及其连接的端口号）保存在已授权键盘列表中。重启操作系统后重新连接键盘时无需重复键盘授权。

经授权的键盘连接至该计算机不同的 USB 端口时，应用程序将提示为该键盘再次授权。

如果错误输入数字代码，则程序将生成新的代码。您可以配置尝试输入数字代码的次数。如果数字代码多次输入错误或键盘授权窗口关闭（参见下图），应用程序将阻止从该键盘输入。当达到 USB 设备阻止时间或者操作系统重启后，程序将再次提示用户重新执行键盘授权。

程序将允许使用经过授权的键盘并阻止未经授权的键盘。

默认情况下，未安装“BadUSB 攻击防护”组件。如果需要“BadUSB 攻击防护”组件，可以在安装应用程序前在安装包的属性中添加该组件，或者在安装应用程序后更改可用应用程序组件。

键盘授权

启用和禁用 BadUSB 攻击防护

在 BadUSB 攻击防护组件安装前被计算机识别为键盘的 USB 设备在该组件安装后仍将被认定为经过授权。

如何在管理控制台(MMC)中启用或禁用 BadUSB 攻击防护组件

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **基本威胁防护** → **BadUSB 攻击防护**。
4. 使用“**BadUSB 攻击防护**”复选框启用或禁用组件。

5. 在“**连接时的 USB 设备授权**”块，调整输入授权代码的安全设置：

   - “**USB 设备授权尝试的最大数量**”。如果授权码输入不正确达到指定次数，则自动阻止 USB 设备。有效值为 1 到 10。例如，如果允许 5 次尝试输入授权码，则在第五次尝试失败后，应用程序将阻止 USB 设备。Kaspersky Endpoint Security 显示 USB 设备的阻塞持续时间。此时间过后，您还可以再尝试 5 次输入授权代码。

   - “**达到最大尝试数量的超时时间(分钟)**”。在指定次数的授权码输入失败后，USB 设备将被阻止。有效值为 1 到 180（分钟）。

6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中启用或禁用 BadUSB 攻击防护组件

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **主机威胁防护** → **BadUSB 攻击防护**。

5. 使用**BadUSB 攻击防护已启用**开关启用或禁用组件。

6. 在“**USB 设备授权**”块，调整输入授权代码的安全设置：

   - “**USB 设备授权尝试的最大次数**”。如果授权码输入不正确达到指定次数，则自动阻止 USB 设备。有效值为 1 到 10。例如，如果允许 5 次尝试输入授权码，则在第五次尝试失败后，应用程序将阻止 USB 设备。Kaspersky Endpoint Security 显示 USB 设备的阻塞持续时间。此时间过后，您还可以再尝试 5 次输入授权代码。

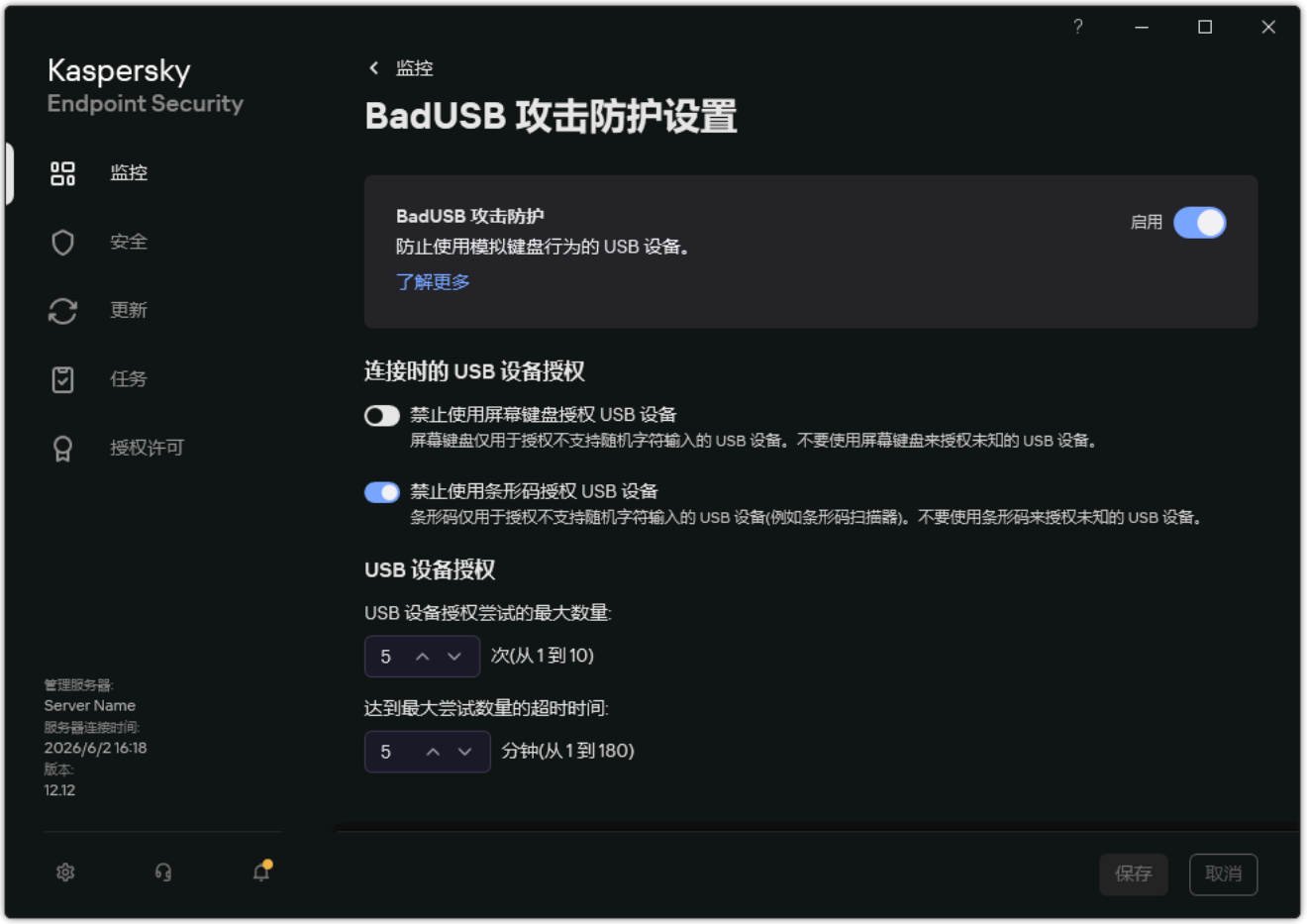
   - “**达到最大尝试次数的超时(分钟)**”。在指定次数的授权码输入失败后，USB 设备将被阻止。有效值为 1 到 180（分钟）。

7. 保存更改。

如何在应用程序界面中启用或禁用 BadUSB 攻击防护组件

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “BadUSB **攻击防护**”。



BadUSB 攻击防护组件设置

3. 使用**BadUSB 攻击防护**开关启用或禁用组件。

4. 在“**连接时的 USB 设备授权**”块，调整输入授权代码的安全设置：

   - “**USB 设备授权尝试的最大数量**”。如果授权码输入不正确达到指定次数，则自动阻止 USB 设备。有效值为 1 到 10。例如，如果允许 5 次尝试输入授权码，则在第五次尝试失败后，应用程序将阻止 USB 设备。Kaspersky Endpoint Security 显示 USB 设备的阻塞持续时间。此时间过后，您还可以再尝试 5 次输入授权代码。

   - “**达到最大尝试数量的超时时间**”。在指定次数的授权码输入失败后，USB 设备将被阻止。有效值为 1 到 180（分钟）。

5. 保存更改。

结果，如果 BadUSB 攻击防护被启用，Kaspersky Endpoint Security 请求已连接的被操作系统识别为键盘的 USB 设备的授权。键盘经过授权前用户无法使用该键盘。

使用屏幕键盘授权 USB 设备

屏幕键盘应仅用于不支持随机字符输入的 USB 设备的授权（例如条形码扫描器）。不建议使用屏幕键盘授权未知的 USB 设备。

如何在管理控制台(MMC) 中允许或禁止使用屏幕键盘进行授权

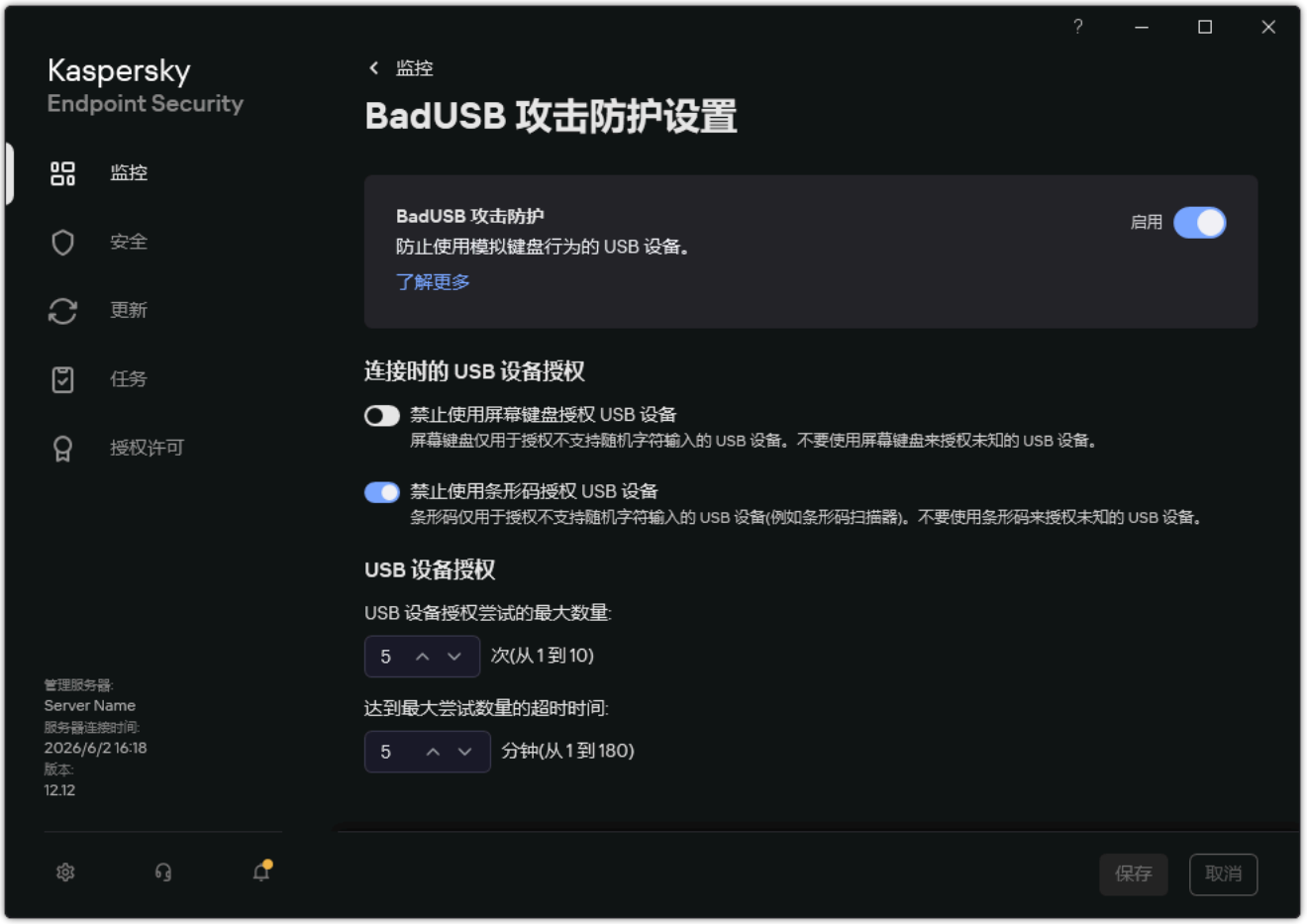
1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **基本威胁防护** → **BadUSB 攻击防护**。
4. 使用“**禁止使用屏幕键盘授权 USB 设备**”复选框来阻止或允许使用屏幕键盘进行授权。
5. 保存更改。

如何在 Web Console 和云控制台中允许或禁止使用屏幕键盘进行授权

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **主机威胁防护** → **BadUSB 攻击防护**。
5. 使用“**禁止使用屏幕键盘授权 USB 设备**”切换开关来阻止或允许使用屏幕键盘进行授权。
6. 保存更改。

如何在应用程序界面中允许或禁止使用屏幕键盘进行授权

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “BadUSB **攻击防护**”。



BadUSB 攻击防护组件设置

3. 使用“**禁止使用屏幕键盘授权 USB 设备**”切换开关来阻止或允许使用屏幕键盘进行授权。

4. 保存更改。

USB 设备授权

条形码扫描器授权

当将条形码扫描器连接到计算机时， BadUSB 攻击防护组件会将此设备识别为输入设备并提示您执行授权。要授权条形码扫描器，您必须扫描屏幕上显示的条形码。应用程序程以大多数条形码和二维码扫描器支持的 Code39 格式生成条形码。

Kaspersky Endpoint Security 还支持另一种条形码扫描器授权方法。如果您使用触摸屏设备，则可以使用屏幕键盘输入代码。为此，您需要允许使用屏幕键盘。例如，对于收银机内置的固定条形码扫描器，这种方法很方便。禁止使用其他条形码扫描器授权方法。

默认情况下，应用程序不使用条形码来授权 USB 设备。

如何在管理控制台(MMC)中启用通过条形码来授权 USB 设备

1. 打开 Kaspersky Security Center Administration Console。

2. 在控制台树中，选择“**策略**”。

3. 选择必要的策略并双击以打开策略属性。

4. 在策略窗口中，选择 **基本威胁防护** → **BadUSB 攻击防护**。

5. 使用“**禁止使用条形码授权 USB 设备**”复选框来阻止或允许使用条形码进行授权。

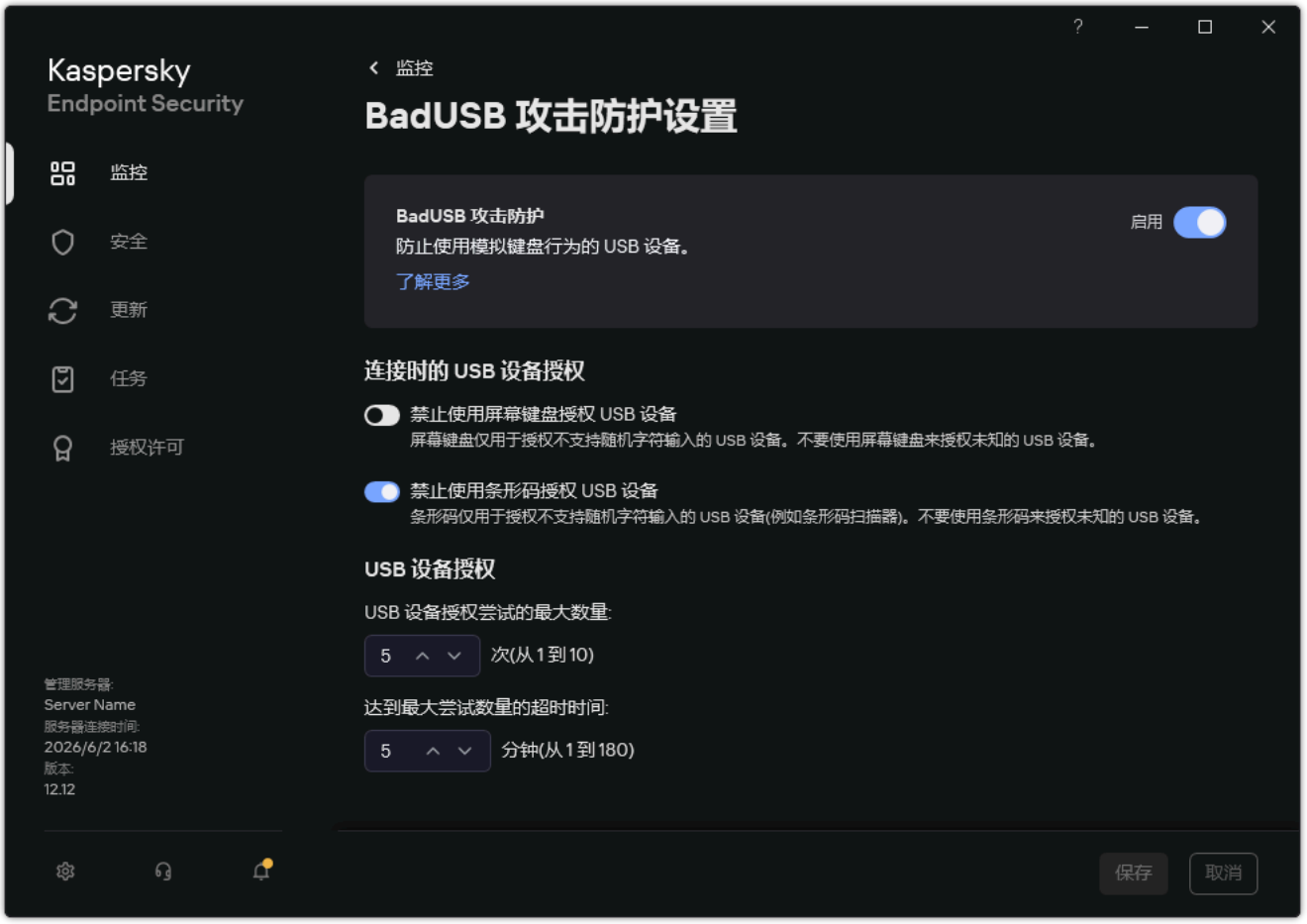
6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中启用通过条形码授权 USB 设备

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”选项卡。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **主机威胁防护** → **BadUSB 攻击防护**。
5. 使用“**禁止使用条形码授权 USB 设备**”切换开关来阻止或允许使用条形码进行授权。
6. 要将此策略应用到计算机，请关闭 🔒 挂锁图标并保存更改。

如何在应用程序界面中启用通过条形码来授权 USB 设备

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**BadUSB 攻击防护**”。



BadUSB 攻击防护组件设置

3. 使用“**禁止使用条形码授权 USB 设备**”切换开关来阻止或允许使用条形码进行授权。

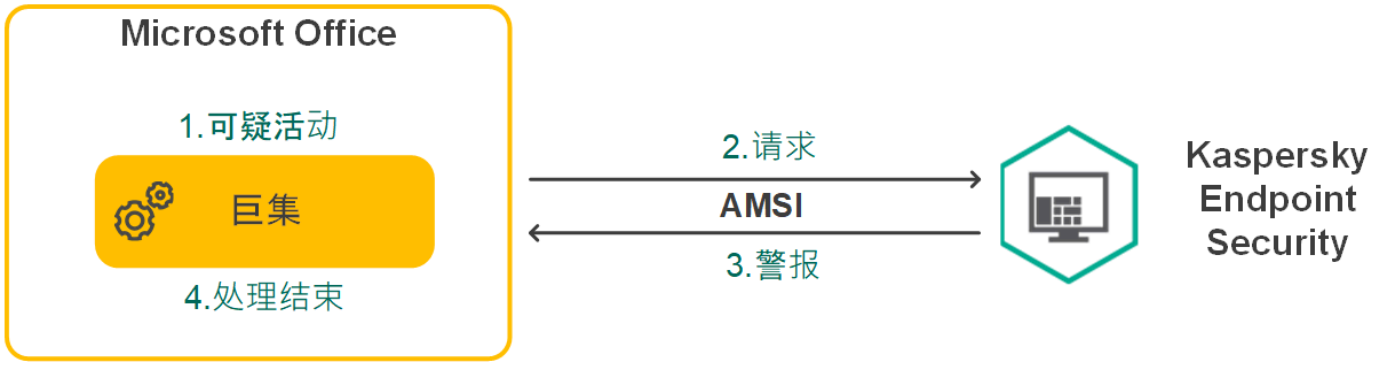
4. 保存更改。

条形码扫描器授权

AMSI 保护

AMSI 保护组件旨在支持 Microsoft 的反恶意软件扫描接口。*反恶意软件扫描接口 (AMSI)* 允许具有 AMSI 支持的第三方应用程序将对象（例如，PowerShell 脚本）发送到 Kaspersky Endpoint Security 进行附加扫描，然后接收这些对象的扫描结果。例如，第三方应用程序可能包括 Microsoft Office 应用程序（请参见下图）。有关 AMSI 的详细信息，请参阅 Microsoft 文档。

AMSI 保护组件只能检测威胁并将检测到的威胁通知给第三方应用程序。在收到威胁通知后，第三方应用程序不允许恶意操作（例如，它会终止操作）。



AMSI 操作示例

> AMSI 保护组件可能会拒绝第三方应用程序的请求，例如，如果该应用程序超出了指定间隔内的最大请求数。Kaspersky Endpoint Security 将有关来自第三方应用程序的被拒绝请求的信息发送至管理服务器。AMSI 保护组件不会拒绝来自已启用与 AMSI 保护组件持续集成的第三方应用程序的请求。

AMSI 保护组件可用于以下适用于工作站和服务器的操作系统：

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multi-session
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise
- Windows Server 2016 Essentials / Standard / Datacenter (包括 Server Core 模式)

- Windows Server 2019 Essentials / Standard / Datacenter (包括 Server Core 模式)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (包括 Server Core 模式)
- Windows Server 2025 Standard / Datacenter

启用和禁用 AMSI 保护

默认情况下， AMSI 保护已启用并以卡巴斯基推荐的模式工作（见下表）。

如何在管理控制台(MMC)中启用或禁用 AMSI 保护

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **基本威胁防护** → **AMSI 扫描程序**。
4. 使用“**AMSI 扫描程序**”复选框启用或禁用组件。
5. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

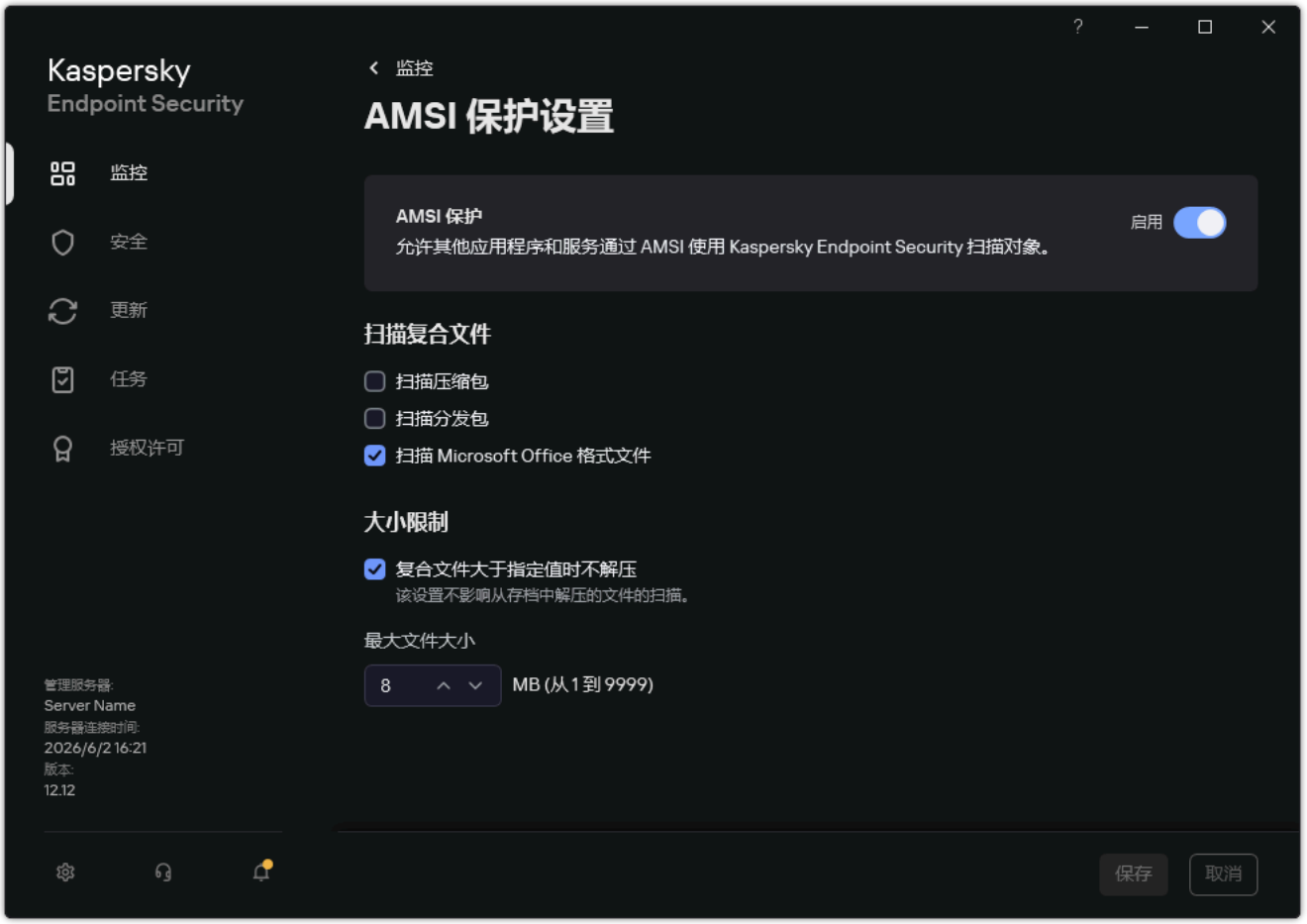
如何在 Web Console 和云控制台中启用或禁用 AMSI 保护

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **主机威胁防护** → **AMSI 保护**。
5. 使用**AMSI 保护已启用**开关启用或禁用组件。
6. 保存更改。要在计算机上应用该策略，请关闭“挂锁”。

如何在应用程序界面中启用或禁用 AMSI 保护

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**AMSI 保护**”。



AMSI 保护设置

3. 使用**AMSI 保护**开关启用或禁用组件。

4. 保存更改。

卡巴斯基专家推荐的 AMSI 保护设置

参数	值	描述
扫描压缩包	**禁用**	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	**禁用**	扫描第三方应用程序的分发包。
扫描 Microsoft Office 格式文件	**启用**	扫描 Microsoft Office 文件（DOC、DOCX、XLS、PPT 和其他 Microsoft 扩展程序）。Office 格式文件也包括 OLE 对象。应用程序扫描小于 1 MB 的 office 格式文件，无论该复选框是否被选中。
复合文件大于指定值时不解压	**最大文件大小 8 MB**	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。

通过 AMSI 保护优化文件扫描

您可以优化文件扫描：缩短扫描时间并提高 Kaspersky Endpoint Security 的操作速度。您可以选择需要扫描的复合文件：存档、分发包或 office 格式的文件。您还可以限制要扫描的复合文件的大小。“AMSI 保护”组件不会解压缩大于指定大小的复合文件。

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。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。

如何在管理控制台(MMC)中优化通过 AMSI 保护进行的文件扫描

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **基本威胁防护** → **AMSI 扫描程序**。
4. 在“**扫描复合文件**”块中，指定您希望扫描的复合文件类型：存档、分发包或 Office 格式文件。
5. 在“**大小限制**”块中执行以下操作之一：
   - 要阻止“AMSI 保护”组件解压缩大型复合文件，请选中“**复合文件大于指定值时不解压**”复选框，并指定所需值。“AMSI 保护”组件不会解压缩大于指定大小的复合文件。
   - 要允许“AMSI 保护”组件解压缩大型复合文件，请取消选中“**复合文件大于指定值时不解压**”复选框。

   无论是否选中“**复合文件大于指定值时不解压**”复选框，“AMSI 保护”组件均会扫描从存档中提取的大型文件。

6. 保存更改。要在计算机上应用该策略，请关闭“挂锁”。

如何在 Web Console 和云控制台中优化通过 AMSI 保护进行的文件扫描

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **主机威胁防护** → **AMSI 保护**。
5. 在“**扫描复合文件**”块中，指定您希望扫描的复合文件类型：存档、分发包或 Office 格式文件。
6. 在“**扫描优化**”块中执行以下操作之一：
   - 要阻止“AMSI 保护”组件解压缩大型复合文件，请选中“**已启用大小限制**”复选框，并指定所需值。“AMSI 保护”组件不会解压缩大于指定大小的复合文件。
   - 要允许“AMSI 保护”组件解压缩大型复合文件，请取消选中“**已启用大小限制**”复选框。

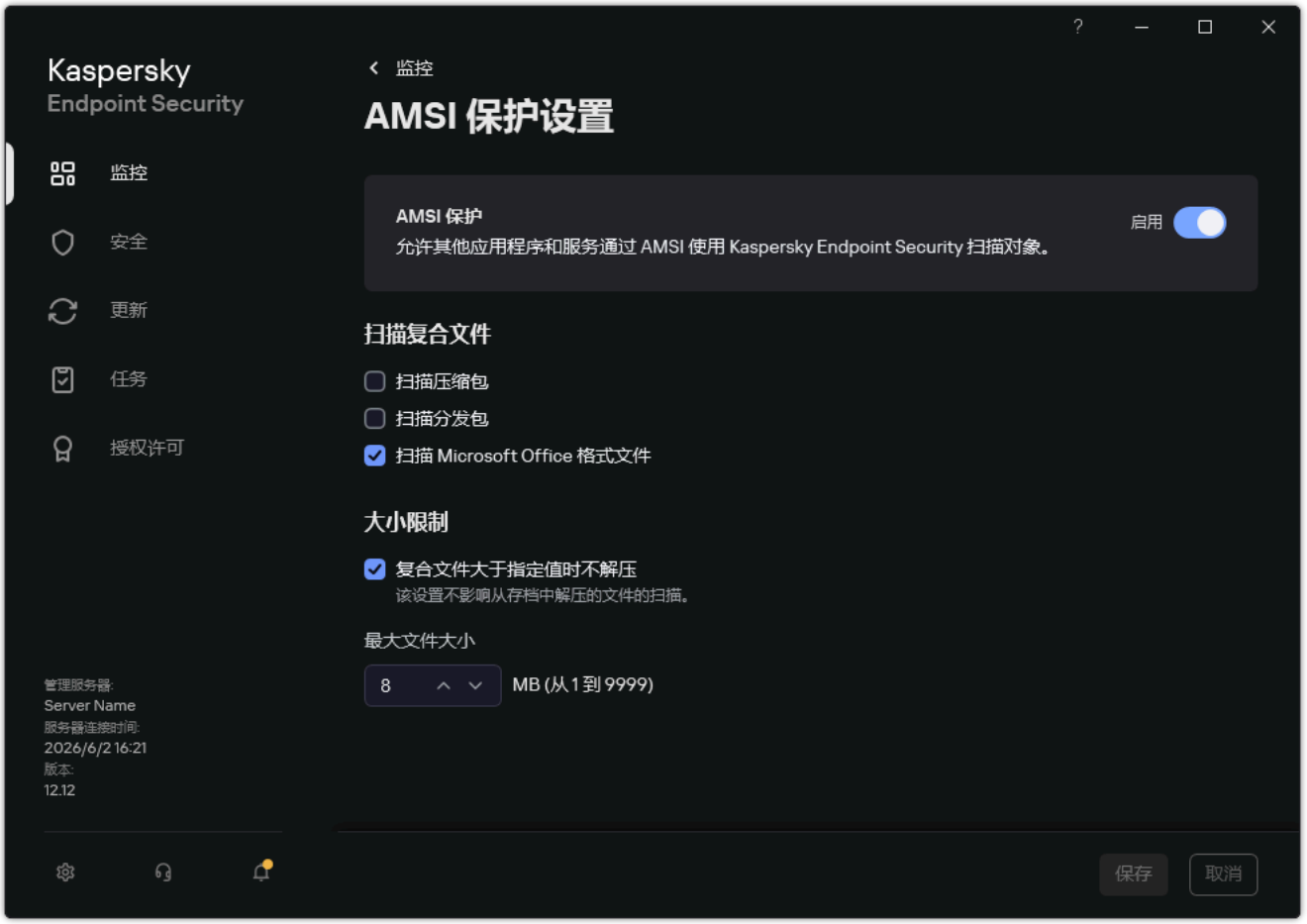
   无论是否选中“**已启用大小限制**”复选框，“AMSI 保护”组件均会扫描从存档中提取的大型文件。

7. 保存更改。要在计算机上应用该策略，请关闭“挂锁”。

如何在应用程序界面中优化通过 AMSI 保护进行的文件扫描

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**AMSI 保护**”。



AMSI 保护设置

3. 在“**扫描复合文件**”块中，指定您希望扫描的复合文件类型：存档、分发包或 Office 格式文件。

4. 在“**大小限制**”块中执行以下操作之一：

   - 要阻止“AMSI 保护”组件解压缩大型复合文件，请选中“**复合文件大于指定值时不解压**”复选框，并指定所需值。“AMSI 保护”组件不会解压缩大于指定大小的复合文件。

   - 要允许“AMSI 保护”组件解压缩大型复合文件，请取消选中“**复合文件大于指定值时不解压**”复选框。

   > 无论是否选中“**复合文件大于指定值时不解压**”复选框，“AMSI 保护”组件均会扫描从存档中提取的大型文件。

5. 保存更改。

Web 威胁防护

“Web 威胁防护”组件可防止从 Internet 下载恶意文件，同时阻止恶意网站和钓鱼网站。该组件借助反病毒数据库、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。

Kaspersky Endpoint Security 扫描 HTTP、HTTPS 和 FTP 流量。Kaspersky Endpoint Security 扫描 URL 和 IP 地址。

要使用 Web 威胁防护，您必须完成应用程序的初始配置：

- 对于 HTTPS 流量监控，启用加密连接扫描（默认情况下启用）。
- 选择 Kaspersky Endpoint Security 必须监控的端口（默认情况下，应用程序监控所有端口）。
- 选择您希望 Kaspersky Endpoint Security 监控其流量的应用程序。大多数浏览器已经存在于卡巴斯基推荐的应用程序列表中。如果列表中缺少您的浏览器，请手动添加。
- 我们建议将网页交互脚本注入到 Web 流量中（默认情况下，脚本注入是禁用的）。该脚本启用将 Web 威胁防护事件注册到应用程序事件日期、OS 事件日志和报告。

当用户尝试打开恶意网站或钓鱼网站时，Kaspersky Endpoint Security 将阻止访问并显示警告。

启用和禁用 Web 威胁防护

默认情况下，“Web 威胁防护”组件已启用并在 Kaspersky 专家建议的模式下运行。对于 Web 威胁防护，应用程序可以应用不同的设置组。存储在应用程序中的设置组叫做“*安全级别*”：**高**、**建议**、**低**。**建议**Web 流量安全级别设置将被视为 Kaspersky 专家建议的最佳设置（参加下表）。您可以选择预安装的通过 HTTP 和 FTP 协议接收或传输的 Web 流量安全级别之一，或配置自定义 Web 流量安全级别。如果您更改了 Web 流量安全级别设置，您仍可随时转换到推荐的 Web 流量安全级别设置。

> 您仅可以在管理控制台(MMC)或应用程序本地界面中选择或配置安全级别。您无法在 Web Console 或云控制台中选择或配置安全级别。

如何在管理控制台(MMC)中启用或禁用 Web 威胁防护组件

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **基本威胁防护** → **Web 威胁防护**。
4. 使用“**Web 威胁防护**”复选框启用或禁用组件。
5. 如果您启用了组件，在“**安全级别**”块做以下之一：
   - 如果您希望应用一种预设的安全级别，请使用滑动条选择：
     - “**高**”。在此安全级别下，“Web 威胁防护”组件对计算机通过 HTTP 和 FTP 收到的 Web 流量执行最大限度的扫描。“Web 威胁防护”使用整个程序应用数据库详细扫描所有 Web 流量对象，并尽可能执行最深度的启发式分析。
     - “**建议**”。在应用程序的性能和 Web 流量的安全性之间提供最佳平衡的安全级别。“Web 威胁防护”组件执行“中度扫描”扫描级别的启发式分析。Kaspersky 专家推荐使用此 Web 流量安全级别。推荐安全级别的设置值在下表中提供。
     - “**低**”。此 Web 流量安全级别的设置可确保 Web 流量的最快扫描。“Web 威胁防护”组件执行“轻度扫描”扫描级别的启发式分析。

- 如果您要配置自定义安全级别，单击**设置**按钮并定义您自己的组件设置。

  您可以通过单击“**默认**”按钮恢复预设安全级别的值。

6. 在“**检测到威胁后的操作**”块中选择 Kaspersky Endpoint Security 对恶意 Web 流量对象所采取的操作：

   - “**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。

   - “**通知**”。如果选择此选项并且在 Web 流量中检测到受感染对象，Kaspersky Endpoint Security 将允许将该对象下载到计算机，但会将受感染对象的相关信息添加到活动威胁列表中。

7. 保存更改。

如何在 Web Console 和云控制台中启用或禁用 Web 威胁防护组件

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **通信和 Web 保护** → **Web 威胁防护**。

5. 使用**Web 威胁防护已启用**开关启用或禁用组件。

6. 在“**检测到威胁后的操作**”块中选择 Kaspersky Endpoint Security 对恶意 Web 流量对象所采取的操作：

   - “**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。

   - “**允许、通知或提示操作(取决于操作系统)**”。如果选择此选项并且在 Web 流量中检测到受感染对象，Kaspersky Endpoint Security 将允许将该对象下载到计算机，但会将受感染对象的相关信息添加到活动威胁列表中。

7. 如果有需要的话，创建受信任 Web 资源列表。

8. 保存更改。

如何启用或禁用“Web 威胁防护”组件

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**Web 威胁防护**”。

3. 使用**Web 威胁防护**开关启用或禁用组件。

4. 如果您启用了组件，在“**安全级别**”块做以下之一：

- 如果您希望应用一种预设的安全级别，请使用滑动条选择：
  - “**高**”。在此安全级别下，“Web 威胁防护”组件对计算机通过 HTTP 和 FTP 收到的 Web 流量执行最大限度的扫描。“Web 威胁防护”使用整个程序应用数据库详细扫描所有 Web 流量对象，并尽可能执行最深度的启发式分析。
  - “**建议**”。在应用程序的性能和 Web 流量的安全性之间提供最佳平衡的安全级别。“Web 威胁防护”组件执行“中度扫描”扫描级别的启发式分析。Kaspersky 专家推荐使用此 Web 流量安全级别。推荐安全级别的设置值在下表中提供。
  - “**低**”。此 Web 流量安全级别的设置可确保 Web 流量的最快扫描。“Web 威胁防护”组件执行“轻度扫描”扫描级别的启发式分析。
- 如果您要配置自定义安全级别，单击“**高级设置**”按钮并定义您自己的组件设置。

  您可以通过单击“**恢复推荐的安全级别**”按钮恢复预设安全级别的值。

5. 在“**检测到威胁后的操作**”块中选择 Kaspersky Endpoint Security 对恶意 Web 流量对象所采取的操作：
   - “**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。
   - “**通知**”。如果选择此选项并且在 Web 流量中检测到受感染对象，Kaspersky Endpoint Security 将允许将该对象下载到计算机，但会将受感染对象的相关信息添加到活动威胁列表中。

6. 保存更改。

Kaspersky 专家推荐的 Web 威胁防护设置（推荐的安全级别）

参数	值	描述
检查网址是否在恶意网址数据库中	**启用**	扫描链接以决定它们是否被包含在恶意网址数据库中，这样您可以跟踪被列入拒绝列表的网站。恶意网址数据库由 Kaspersky 维护，包含在程序安装包中，并通过 Kaspersky Endpoint Security 数据库更新进行补充。
检查网址是否在钓鱼网址数据库中	**启用**	钓鱼网址数据库包含当前用于启动钓鱼攻击的已知网站的地址。Kaspersky 使用从国际组织 Anti-Phishing Working Group 获取的网址补充该钓鱼链接数据库。钓鱼地址数据库包含在程序安装包中，并通过 Kaspersky Endpoint Security 数据库更新进行补充。
使用启发式分析 (Web 威胁防护)	**中度扫描**	开发该技术的目的是检测使用当前版本的卡巴斯基应用程序数据库无法检测到的威胁。它可以检测可能受未知病毒或已知病毒新变种感染的文件。 当 Web 流量被扫描以查找病毒和其他威胁应用程序时，启发式分析执行可执行文件中的指令。启发式分析执行的指令数量取决于启发式分析级别。启发式分析级别可在全面搜索新威胁、加载操作系统资源和启发式分析持续时间之间进行平衡。
使用启发式分析 (反钓鱼)	**启用**	开发该技术的目的是检测使用当前版本的卡巴斯基应用程序数据库无法检测到的威胁。它可以检测可能受未知病毒或已知病毒新变种感染的文件。
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。

配置恶意网址检测方法

Web 威胁防护使用反病毒数据库、卡巴斯基安全网络云服务和启发式分析检测恶意网址。

> 您仅可以在管理控制台(MMC)或应用程序本地界面中选择恶意网址检测方法。您无法在 Web Console 或云控制台中选择恶意网址检测方法。默认选项是使用启发式分析检查网址是否在恶意网址数据库中（中度扫描）。

使用恶意网址数据库进行扫描

扫描链接以决定它们是否被包含在恶意网址数据库中，这样您可以跟踪被列入拒绝列表的网站。恶意网址数据库由 Kaspersky 维护，包含在程序安装包中，并通过 Kaspersky Endpoint Security 数据库更新进行补充。

> Kaspersky Endpoint Security 扫描所有链接以决定它们是否在恶意网址数据库中。应用程序的安全连接扫描设置不影响链接扫描功能。换句话说，如果加密连接扫描被禁用，Kaspersky Endpoint Security 检查链接是否在恶意网址数据库中，即便网络流量是通过加密连接传输的。

如何使用管理控制台(MMC)启用或禁用检查网址是否在恶意网址数据库中

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **基本威胁防护** → **Web 威胁防护**。
4. 在“**安全级别**”块中单击“**设置**”按钮。
5. 在打开的窗口中，在“**扫描方式**”下，选择或清空“**检查网址是否在恶意网址数据库中**”复选框以启用或禁用检查网址是否在恶意网址数据库中。
6. 保存更改。

如何在应用程序界面中启用或禁用检查网址是否在恶意网址数据库中

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**Web 威胁防护**”。
3. 单击“**高级设置**”。
4. 在“**扫描方式**”块中，选择或清空“**检查网址是否在恶意网址数据库中**”复选框以启用或禁用检查网址是否在恶意网址数据库中。
5. 保存更改。

启发式分析

在启发式分析中，Kaspersky Endpoint Security 将分析应用程序在操作系统中的活动。启发式分析可以检测 Kaspersky Endpoint Security 数据库中尚无记录的安全威胁。

当 Web 流量被扫描以查找病毒和其他威胁应用程序时，启发式分析执行可执行文件中的指令。启发式分析执行的指令数量取决于启发式分析级别。启发式分析级别可在全面搜索新威胁、加载操作系统资源和启发式分析持续时间之间进行平衡。

如何在管理控制台(MMC)中启用或禁用使用启发式分析

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **基本威胁防护** → **Web 威胁防护**。
4. 在“**安全级别**”块中单击“**设置**”按钮。
5. 如果您想让应用程序在扫描 Web 流量以查找病毒和其他恶意软件时使用启发式分析，请在打开的窗口的“**扫描方式**”块中选择“**使用启发式分析**”复选框。
6. 使用滑块设置启发式分析的级别：**轻度扫描**、**中度扫描**或**深度扫描**。

   当 Web 流量被扫描以查找病毒和其他威胁应用程序时，启发式分析执行可执行文件中的指令。启发式分析执行的指令数量取决于启发式分析级别。启发式分析级别可在全面搜索新威胁、加载操作系统资源和启发式分析持续时间之间进行平衡。
7. 保存更改。

如何在应用程序界面中启用或禁用启发式分析

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**Web 威胁防护**”。
3. 单击“**高级设置**”。
4. 如果您想让应用程序在扫描 Web 流量以查找病毒和其他恶意软件时使用启发式分析，请在**扫描方式**块选择**使用启发式分析**复选框。

   当 Web 流量被扫描以查找病毒和其他威胁应用程序时，启发式分析执行可执行文件中的指令。启发式分析执行的指令数量取决于启发式分析级别。启发式分析级别可在全面搜索新威胁、加载操作系统资源和启发式分析持续时间之间进行平衡。
5. 保存更改。

反钓鱼

Web 威胁防护检查链接以查看它们是否属于钓鱼网址。这将帮助防止*钓鱼攻击*。钓鱼攻击常常带有伪装，比如从您银行发来的带有银行官方网站链接的电子邮件消息。单击此链接，您将进入银行网站的完整复制网站，甚至可以在浏览器地址栏看到其真实地址，即使您在假网站上。从此刻起，您在网站上的所有操作都将被跟踪，进而用来窃取您的金钱。

由于钓鱼网站的链接不仅能通过电子邮件消息传送，而且还可能来自其他来源（例如聊天软件），因此"Web 威胁防护"组件将在 Web 流量扫描级别监视访问钓鱼网站的尝试并阻止对此类网站的访问。Kaspersky Endpoint Security 分发套装中包含了钓鱼网址列表。

> 您可以仅在管理控制台(MMC)中或者应用程序本地界面中配置反钓鱼。您无法在 Web Console 或云控制台中配置反钓鱼。默认下，带有启发式分析的反钓鱼被启用。

如何在管理控制台(MMC)中启用或禁用反钓鱼

1. 在 Kaspersky Security Center 管理控制台树中，选择"**策略**"。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **基本威胁防护** → **Web 威胁防护**。
4. 在"**安全级别**"块中单击"**设置**"按钮。
5. 在打开的窗口中，在"**反钓鱼设置**"块，选择或清空"**检查网址是否在钓鱼网址数据库中**"复选框以启用或禁用反钓鱼。

   钓鱼网址数据库包含当前用于启动钓鱼攻击的已知网站的地址。Kaspersky 使用从国际组织 Anti-Phishing Working Group 获取的网址补充该钓鱼链接数据库。钓鱼地址数据库包含在程序安装包中，并通过 Kaspersky Endpoint Security 数据库更新进行补充。
6. 如果您想让应用程序在扫描网页以查找钓鱼链接时使用启发式分析，请选择**使用启发式分析**复选框。

   在启发式分析中，Kaspersky Endpoint Security 将分析应用程序在操作系统中的活动。启发式分析可以检测 Kaspersky Endpoint Security 数据库中尚无记录的安全威胁。

   如果您除了反病毒数据库和启发式分析外还想扫描链接，您可以使用卡巴斯基安全网络信誉数据库。
7. 保存更改。

如何在应用程序界面中启用或禁用反钓鱼

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择"**基本威胁防护**" → "**Web 威胁防护**"。
3. 单击"**高级设置**"。
4. 如果您想让 Web 威胁防护组件检查链接是否在钓鱼网址数据库中，请在**反钓鱼**块中选择"**检查网址是否在钓鱼网址数据库中**"复选框。钓鱼网址数据库包含当前用于启动钓鱼攻击的已知网站的地址。Kaspersky 使用从国际组织 Anti-Phishing Working Group 获取的网址补充该钓鱼链接数据库。钓鱼地址数据库包含在程序安装包中，并通过 Kaspersky Endpoint Security 数据库更新进行补充。
5. 如果您想让应用程序在扫描网页以查找钓鱼链接时使用启发式分析，请选择**使用启发式分析**复选框。

在启发式分析中，Kaspersky Endpoint Security 将分析应用程序在操作系统中的活动。启发式分析可以检测 Kaspersky Endpoint Security 数据库中尚无记录的安全威胁。

如果您除了反病毒数据库和启发式分析外还想扫描链接，您可以使用卡巴斯基安全网络信誉数据库。

6. 保存更改。

创建受信任网址列表

除了恶意和钓鱼网站，Web 威胁防护还可以阻止其他网站。例如，Web 威胁防护阻止不满足 RFC 标准的 HTTP 流量。您可以为您信任其内容的网址创建一个列表。“Web 威胁防护”组件不会分析来自受信任网址的信息，不会检查它们中是否含有病毒或其他威胁。在一些情况下本选项十分有用，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。

网址可以是某特定网页的地址，也可以是某网站的地址。

更改策略中的受信任网址列表可能会受到父策略属性的阻止。要更改列表，您需要允许更改以下设置：Web Console 中的受信任区域（“挂锁”必须处于解锁状态）。

管理控制台(MMC) 和 Web Console 中受信任区域的分组方式不同。同样，防止受信任区域参数更改的方式也不同（“挂锁”不同）。我们建议仅使用 Web Console 来管理应用程序。如果在不同的控制台中配置受信任区域，管理插件可能会将“挂锁”重置为其默认状态。

如何使用管理控制台(MMC)添加受信任网址

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **基本威胁防护** → **Web 威胁防护**。

4. 在“**安全级别**”块中单击“**设置**”按钮。

5. 在打开的窗口中，选择“**受信任网址**”选项卡。

6. 选择**不扫描受信任网址的 Web 流量**复选框。

   如果选中此选项，“Web 威胁防护”组件将不再扫描其网址包含在受信任网址列表中的网页或网站的内容。您可以将网页/网站的特定地址和地址掩码添加至受信任网址列表。

7. 为您信任其内容的网页或网址创建列表。

   输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。

   您也可以从 XML 文件导入受信任网址列表。

8. 保存更改。

如何在 Web Console 和云控制台中添加受信任网址

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **通信和 Web 保护** → **Web 威胁防护**。
5. 单击“**受信任网址**”。
6. 为您信任其内容的网页或网址创建列表。
   输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。
   您也可以从 JSON 文件导入受信任网址列表。
7. 保存更改。

如何在应用程序界面中添加受信任网址

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**Web 威胁防护**”。
3. 单击“**高级设置**”。
4. 选择“**不扫描来自 受信任网址的 Web 流量**”复选框。
   如果选中此选项，“Web 威胁防护”组件将不再扫描其网址包含在受信任网址列表中的网页或网站的内容。您可以将网页/网站的特定地址和地址掩码添加至受信任网址列表。
5. 为您信任其内容的网页或网址创建列表。
   输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。
   您也可以从 XML 文件导入受信任网址列表。
6. 保存更改。

作为结果，Web 威胁防护不扫描受信任网址的流量。用户总是可以打开受信任网址并从该网址下载文件。如果您无法访问该网址，请检查“加密连接扫描”、“Web 控制”和“网络端口监控”组件的设置。如果 Kaspersky Endpoint Security 检测到从受信任网址下载的文件是恶意的，您可以添加此文件到排除项。

您也可以为加密连接创建排除项常规列表。此种情况下，在 Web 威胁防护、邮件威胁防护和 Web 控制组件正常运行的情况下，Kaspersky Endpoint Security 不扫描受信任网址的 HTTPS 流量。

导出和导入受信任网址列表

可以将受信任网址列表导出到 XML 文件。然后可以修改文件，例如，添加大量相同类型的网址。还可以使用导出/导入功能备份受信任网址列表或将列表迁移到其他服务器。

如何在管理控制台(MMC)中导出和导入受信任网址列表

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **基本威胁防护** → **Web 威胁防护**。
4. 在“**安全级别**”块中单击“**设置**”按钮。
5. 在打开的窗口中，选择“**受信任网址**”选项卡。
6. 要导出受信任网址列表：
   a. 选择您要导出的受信任网址。要选择多个端口，使用 **CTRL** 或 **SHIFT** 键。
      如果您未选择任何受信任网址，Kaspersky Endpoint Security 将导出所有网址。
   b. 单击**导出**链接。
   c. 在打开的窗口中，指定您要将受信任网址列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。
   d. 保存文件。
      Kaspersky Endpoint Security 会将整个受信任网址列表导出到 XML 文件。
7. 要导入受信任地址的列表：
   a. 单击**导入**链接。
      在打开的窗口中，选择要从中导入受信任地址列表的 XML 文件。
   b. 打开文件。
      如果计算机已经具有受信任地址的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 XML 文件向其中添加新条目。
8. 保存更改。

如何在 Web Console 和云控制台中导出和导入受信任网址列表

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **通信和 Web 保护** → **Web 威胁防护**。
5. 要在**规则列表**块导出排除项列表：
   a. 选择您要导出的受信任网址。
   b. 单击“ → **导出**”按钮。
      Kaspersky Endpoint Security 导出受信任网址列表到默认下载文件夹中的 JSON 文件。

6. 要在**规则列表**块导入排除项列表：

   a. 单击“ → **导入**”按钮。

      在打开的窗口中，选择要从中导入受信任地址列表的 JSON 文件。

   b. 打开文件。

      如果计算机已经具有受信任地址的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 JSON 文件向其中添加新条目。

7. 保存更改。

邮件威胁防护

“邮件威胁防护”组件扫描传入和传出电子邮件的附件是否有病毒和其他威胁。该组件借助反病毒数据库、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。

邮件威胁防护可以扫描传入和传出的邮件。该应用程序在以下邮件客户端中支持 POP3、SMTP、IMAP 和 NNTP：

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

> 要扫描 Mozilla Thunderbird、MyOffice Mail 和 R7-Office Organizer 邮件客户端中的流量，您需要将卡巴斯基证书添加到证书存储并选择自己的证书存储。

邮件威胁防护不支持其他协议和邮件客户端。

邮件威胁防护可能并不总是能够获得邮件的*协议级*访问权限（例如，使用 Microsoft Exchange 解决方案时）。为此，邮件威胁防护包括 Microsoft Office Outlook 扩展程序。该扩展程序允许在*邮件客户端级别*扫描邮件。邮件威胁防护扩展程序支持 Outlook 2010、2013、2016、2019、2021、2024 和 365 的 32 位和 64 位版本。在基于 Arm 的计算机上，邮件威胁防护扩展程序支持 32 位和 64 位版本的 Outlook 2016、Outlook 2021、Outlook 2024 和 Outlook 365 for Arm64。

> 如果在浏览器中打开邮件客户端，“邮件威胁防护”组件不会扫描邮件。

当在附件中检测到恶意文件时，Kaspersky Endpoint Security 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>*。

启用和禁用邮件威胁防护

默认情况下，“邮件威胁防护”组件已启用并在 Kaspersky 专家建议的模式下运行。对于邮件威胁防护，应用程序可以应用不同的设置组。存储在应用程序中的设置组叫做“*安全级别*”：**高**、**建议**、**低**。**建议**邮件安全级别设置将被视为 Kaspersky 专家建议的最佳设置（参加下表）。您可以选择预安装的邮件安全级别之一或配置自定义邮件安全级别。如果您改变了邮件安全级别设置，您仍可随时转换到推荐的邮件安全级别设置。

当使用 Mozilla Thunderbird 邮件客户端时，如果使用过滤器将电子邮件移出“收件箱”文件夹，则“邮件威胁防护”组件不扫描经由 IMAP 协议发送的电子邮件以查找病毒和其他威胁。

如何在管理控制台(MMC)中启用或禁用邮件威胁防护组件

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **基本威胁防护** → **邮件威胁防护**。
4. 使用“**邮件威胁防护**”复选框启用或禁用组件。
5. 如果您启用了组件，在“**安全级别**”块做以下之一：
   - 如果您希望应用一种预设的安全级别，请使用滑动条选择：
     - “**高**”。选择此电子邮件安全级别时，“邮件威胁防护”组件会最彻底地扫描电子邮件。“邮件威胁防护”组件将扫描发送和接收的电子邮件消息，并执行深度启发式分析。“高”邮件安全级别被推荐用于高风险环境。这种情况的一个例子就是，未获得集中式电子邮件保护的家庭网络连接免费的电子邮件服务。
     - “**建议**”。在应用程序性能和电子邮件安全性之间提供最佳平衡的电子邮件安全级别。“邮件威胁防护”组件将扫描发送和接收的电子邮件，并执行中度启发式分析。Kaspersky 专家推荐采用这一邮件流量安全级别。推荐安全级别的设置值在下表中提供。
     - “**低**”。选择此电子邮件安全级别时，“邮件威胁防护”组件只扫描接收的电子邮件消息，执行轻度启发式分析，不扫描电子邮件的压缩包附件。在这一邮件安全级别中，“邮件威胁防护”组件将使用最少的操作系统资源，以最大速度扫描电子邮件。在保护良好的环境中工作时，推荐使用“低”邮件安全级别。这类环境的例子包括具有集中式电子邮件保护的企业局域网。
   - 如果您要配置自定义安全级别，单击**设置**按钮并定义您自己的组件设置。

     您可以通过单击“**默认**”按钮恢复预设安全级别的值。

6. 在“**检测到威胁后的操作**”块中选择 Kaspersky Endpoint Security 对恶意对象所采取的操作：

   - “**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的对象时，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>*。

   - “**清除；如果清除失败则阻止**”。在入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。在出站邮件中检测到受感染的对象时，应用程序会尝试对检测到的对象进行清除。如果无法清除对象，应用程序会阻止邮件的传输，邮件客户端会显示错误。

   - “**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。

7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中启用或禁用邮件威胁防护组件

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **通信和 Web 保护** → **邮件威胁防护**。

5. 使用**邮件威胁防护已启用**开关启用或禁用组件。

6. 在“**检测到威胁后的操作**”块中选择 Kaspersky Endpoint Security 对恶意对象所采取的操作：

   - “**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的对象时，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>*。

   - “**清除；如果清除失败则阻止**”。在入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。在出站邮件中检测到受感染的对象时，应用程序会尝试对检测到的对象进行清除。如果无法清除对象，应用程序会阻止邮件的传输，邮件客户端会显示错误。

   - “**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。

7. 如有必要，请编辑邮件威胁防护的高级设置。

8. 保存更改。

如何在应用程序界面中启用或禁用邮件威胁防护组件

1. 打开主应用程序窗口并单击 按钮。

2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**邮件威胁防护**”。

3. 使用**邮件威胁防护**开关启用或禁用组件。

4. 如果您启用了组件，在“**安全级别**”块做以下之一：

- 如果您希望应用一种预设的安全级别，请使用滑动条选择：
  - “**高**”。选择此电子邮件安全级别时，“邮件威胁防护”组件会最彻底地扫描电子邮件。“邮件威胁防护”组件将扫描发送和接收的电子邮件消息，并执行深度启发式分析。“高”邮件安全级别被推荐用于高风险环境。这种情况的一个例子就是，未获得集中式电子邮件保护的家庭网络连接免费的电子邮件服务。
  - “**建议**”。在应用程序性能和电子邮件安全性之间提供最佳平衡的电子邮件安全级别。“邮件威胁防护”组件将扫描发送和接收的电子邮件，并执行中度启发式分析。Kaspersky 专家推荐采用这一邮件流量安全级别。推荐安全级别的设置值在下表中提供。
  - “**低**”。选择此电子邮件安全级别时，“邮件威胁防护”组件只扫描接收的电子邮件消息，执行轻度启发式分析，不扫描电子邮件的压缩包附件。在这一邮件安全级别中，“邮件威胁防护”组件将使用最少的操作系统资源，以最大速度扫描电子邮件。在保护良好的环境中工作时，推荐使用“低”邮件安全级别。这类环境的例子包括具有集中式电子邮件保护的企业局域网。
- 如果您要配置自定义安全级别，单击“**高级设置**”按钮并定义您自己的组件设置。

  您可以通过单击“**恢复推荐的安全级别**”按钮恢复预设安全级别的值。

5. 在“**检测到威胁后的操作**”块中选择 Kaspersky Endpoint Security 对恶意对象所采取的操作：

- “**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的对象时，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>*。
- “**清除；如果清除失败则阻止**”。在入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。在出站邮件中检测到受感染的对象时，应用程序会尝试对检测到的对象进行清除。如果无法清除对象，应用程序会阻止邮件的传输，邮件客户端会显示错误。
- “**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。

6. 保存更改。

Kaspersky 专家推荐的邮件威胁防护设置（推荐的安全级别）

参数	值	描述
保护范围	**传入和传出邮件**	*保护范围*包括组件在运行时检查的对象：接收和发送的消息或仅接收的消息。 为了保护您的计算机，您仅需要扫描接收邮件消息。您可以开启扫描发送邮件消息以防范发送在存档中的受感染文件。如果您要防范发送的特殊格式的文件，例如音频和视频文件，您也可以开启扫描发送邮件消息。
连接 Microsoft Outlook 扩展程序	**启用**	如果选中该复选框，则在 Microsoft Outlook 中集成的扩展程序一侧启用对通过 POP3、SMTP、NNTP、IMAP 协议传输的电子邮件的扫描。 如果使用 Microsoft Outlook 的扩展程序扫描邮件，建议使用Cached Exchange Mode。有关缓存 Exchange 模式的详细信息和对其用途的建议，请参阅 Microsoft 知识库。
扫描附加的压缩包	**启用**	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 Microsoft Office 格式的附加文件	**启用**	扫描 Microsoft Office 文件（DOC、DOCX、XLS、PPT 和其他 Microsoft 扩展程序）。Office 格式文件也包括 OLE 对象。应用程序扫描小于 1 MB 的 office 格式文件，无论该复选框是否被选中。
附件过滤器	**重命名选定类型的附件**	如果您选择该选项，邮件威胁防护组件将使用下划线字符（例如，attachment.doc_）替换上一个在指定类型的附加文件中找到的扩充字符。因此，为了打开文件，用户必须重命名文件。

参数	值	描述
启发式分析	**中度扫描**	开发该技术的目的是检测使用当前版本的卡巴斯基应用程序数据库无法检测到的威胁。它可以检测可能受未知病毒或已知病毒新变种感染的文件。 当扫描文件以查找恶意代码时，启发式分析执行可执行文件中的指令。启发式分析执行的指令数量取决于启发式分析级别。启发式分析级别可在全面搜索新威胁、加载操作系统资源和启发式分析持续时间之间进行平衡。
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的对象时，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>*。

更改对受感染电子邮件采取的操作

默认情况下，“邮件威胁防护”组件将自动尝试对已经检测到的所有受感染电子邮件执行清除操作。如果清除失败，“邮件威胁防护”组件会删除感染的电子邮件。

更改对受感染电子邮件执行的操作，请执行以下操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**邮件威胁防护**”。
3. 在“**检测到威胁后的操作**”块中选择 Kaspersky Endpoint Security 对检测到的感染邮件执行的操作：
   - “**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的对象时，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>*。
   - “**清除；如果清除失败则阻止**”。在入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。在出站邮件中检测到受感染的对象时，应用程序会尝试对检测到的对象进行清除。如果无法清除对象，应用程序会阻止邮件的传输，邮件客户端会显示错误。
   - “**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。
4. 保存更改。

构成“邮件威胁防护”组件的保护范围

*保护范围*是指活动时被该组件扫描的对象。不同组件的保护范围有不同的参数。“邮件威胁防护”组件的保护范围属性包括将“邮件威胁防护”组件集成至邮件客户端的设置，以及被“邮件威胁防护”组件扫描流量的电子邮件类型和电子邮件协议。默认情况下，Kaspersky Endpoint Security 通过 POP3、SMTP、NNTP 和 IMAP 协议扫描收件箱和发件箱邮件，并且该扫描与 Microsoft Office Outlook 电子邮件客户端相集成。

要构成“邮件威胁防护”组件的保护范围：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**邮件威胁防护**”。
3. 单击“**高级设置**”。
4. 在**保护范围**块，选择要扫描的消息：
   - “**传入和传出邮件**”。
   - “**仅传入的邮件**”。

   为了保护您的计算机，您仅需要扫描接收邮件消息。您可以开启扫描发送邮件消息以防范发送在存档中的受感染文件。如果您要防范发送的特殊格式的文件，例如音频和视频文件，您也可以开启扫描发送邮件消息。

   > 如果您选择仅扫描接收的邮件，建议为所有发送的邮件执行一次性扫描，因为有可能您的计算机存有邮件蠕虫病毒并且会通过邮件传播。这有助于避免因未监视计算机大量电子邮件散播而造成的问题。

5. 在“**连接**”块中执行下列操作：
   - 如果您希望“邮件威胁防护”组件在经由 POP3、SMTP、NNTP 和 IMAP 协议传送的电子邮件到达计算机之前进行扫描，请选中“**扫描 POP3、SMTP、NNTP 和 IMAP 流量**”复选框。

     如果您不希望“邮件威胁防护”组件在经由 POP3、SMTP、NNTP 和 IMAP 协议传送的电子邮件到达计算机之前进行扫描，请清空“**扫描 POP3、SMTP、NNTP 和 IMAP 流量**”复选框。在这种情况下，如果选定了“**连接 Microsoft Outlook 扩展程序**”复选框，用户计算机上接收到邮件时，邮件将经过 Microsoft Office Outlook 邮件客户端中嵌入的“邮件威胁防护”扩展插件的扫描。

     > I如果使用的邮件客户端不是 Microsoft Office Outlook，则如果清除了**扫描 POP3、SMTP、NNTP 和 IMAP 流量**复选框，则邮件威胁防护组件不会扫描通过 POP3、SMTP、NNTP 和 IMAP 协议传输的邮件。

   - 如果您希望允许从 Microsoft Office Outlook 访问“邮件威胁防护”组件设置并且希望经由 POP3、SMTP、NNTP、IMAP 和 MAPI 协议发送的邮件在到达计算机后由嵌入在 Microsoft Office Outlook 的扩展插件进行扫描，请选中“**连接 Microsoft Outlook 扩展程序**”复选框。

     如果您希望阻止从 Microsoft Office Outlook 访问“邮件威胁防护”组件设置并且禁止经由 POP3、SMTP、NNTP、IMAP 和 MAPI 协议发送的邮件在到达计算机后由嵌入在 Microsoft Office Outlook 的扩展插件进行扫描，请清除“**连接 Microsoft Outlook 扩展程序**”复选框。

     > “邮件威胁防护”扩展程序在安装 Kaspersky Endpoint Security 时嵌入在 Microsoft Office Outlook 邮件客户端中。

6. 保存更改。

扫描附加于电子邮件中的复合文件

您可以启用或禁用扫描邮件附件，限制要扫描的邮件附件的最大大小并限制邮件附件最大扫描时长。

若要配置对附加于电子邮件中的复合文件的扫描：

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**邮件威胁防护**”。

3. 单击“**高级设置**”。

4. 在“**扫描复合文件**”块，配置扫描设置：

   - “**扫描 Microsoft Office 格式的附加文件**”。扫描 Microsoft Office 文件（DOC、DOCX、XLS、PPT 和其他 Microsoft 扩展程序）。Office 格式文件也包括 OLE 对象。应用程序扫描小于 1 MB 的 office 格式文件，无论该复选框是否被选中。

   - “**扫描附加的压缩包**”。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。

     > 如果在扫描过程中，应用程序检测到邮件文本中的存档密码，则该密码将用于扫描存档内容以查找恶意应用程序。在这种情况下，不会保存密码。在扫描过程中，存档被解包。如果在解包过程中发生应用程序错误，您可以手动删除保存到以下路径的解包文件：%systemroot%\temp。文件具有 PR 前缀。

   - **不扫描大于该值的存档 N MB (从 1 到 9999)**。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。

   - **限制检查存档的时间到 N 秒 (从 1 到 9999)**。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。

5. 保存更改。

邮件消息附件过滤器

> 附件过滤器不适用于传出电子邮件。

恶意应用程序会以电子邮件附件的形式传播。您可以根据邮件附件类型配置筛选，银边指定类型的文件可以被自动重命名或删除。通过重命名某种类型的附件，Kaspersky Endpoint Security 可以保护您的计算机，防御恶意应用程序的自动执行。

要配置附件的过滤，请执行以下操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**邮件威胁防护**”。

3. 单击“**高级设置**”。

4. 在“**附件过滤器**”块中执行以下操作之一：

   - “**禁用过滤**”。如果选择此选项，“邮件威胁防护”组件将不过滤属于电子邮件附件的文件。
   - “**重命名选定类型的附件**”。如果您选择该选项，邮件威胁防护组件将使用下划线字符（例如，attachment.doc_）替换上一个在指定类型的附加文件中找到的扩充字符。因此，为了打开文件，用户必须重命名文件。
   - “**删除选定类型的附件**”。如果选择此选项，“邮件威胁防护”组件将从电子邮件中删除指定的附件类型。

5. 如果您在上个步骤中选择了“**重命名选定类型的附件**”选项或者“**删除选定类型的附件**”选项，则选择相应类型文件旁的复选框。

6. 保存更改。

导出和导入附件过滤的扩展名

您可以将附件过滤扩展名列表导出到 XML 文件。还可以使用导出/导入功能备份扩展名列表或将列表迁移到其他服务器。

如何在管理控制台(MMC)中导出和导入附件过滤扩展名列表

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **通信和 Web 保护** → **邮件威胁防护**。

5. 要在**附件过滤器**块导出扩展名列表：

   a. 选择您要导出的扩展名。

   b. 单击**导出**链接。

   c. 在打开的窗口中，指定您要将扩展名列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。

   d. 保存文件。
      Kaspersky Endpoint Security 会将整个扩展名列表导出到 XML 文件。

6. 要在**附件过滤器**块导入扩展名列表：

   a. 单击**导入**链接。

   b. 在打开的窗口中，选择要从中导入扩展名列表的 XML 文件。

c. 打开文件。

如果计算机已经具有扩展名的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 XML 文件向其中添加新条目。

7. 保存更改。

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **基本威胁防护** → **邮件威胁防护**。

4. 在“**安全级别**”块中单击“**设置**”按钮。

5. 这将打开一个窗口；在该窗口中，选择“**附件过滤器**”选项卡。

6. 要导出扩展名列表：

   a. 选择您要导出的扩展名。要选择多个端口，使用 **CTRL** 或 **SHIFT** 键。

   b. 单击**导出**链接。

   c. 在打开的窗口中，指定您要将扩展名列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。

   d. 保存文件。

   Kaspersky Endpoint Security 会将整个扩展名列表导出到 XML 文件。

7. 要导入扩展名列表：

   a. 单击**导入**链接。

   b. 在打开的窗口中，选择要从中导入扩展名列表的 XML 文件。

   c. 打开文件。

   如果计算机已经具有扩展名的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 XML 文件向其中添加新条目。

8. 保存更改。

扫描 Microsoft Office Outlook 中的电子邮件

在 Kaspersky Endpoint Security 安装期间，“邮件威胁防护”扩展程序嵌入到 Microsoft Office Outlook（以下简称 Outlook）中。该扩展程序允许在邮件客户端级别而不是协议级别扫描邮件。除了消息之外，该扩展程序还允许您扫描通过 MAPI 接口从 Microsoft Exchange 存储库接收的对象（例如，日历中的对象）。此扫描在邮件客户端中进行。

您可从 Outlook 内部快速打开“邮件威胁防护”组件设置，指定在何时扫描电子邮件以查找病毒和其他威胁。

邮件威胁防护扩展程序支持 Outlook 2010、2013、2016、2019、2021、2024 和 365 的 32 位和 64 位版本。

在基于 Arm 的计算机上，邮件威胁防护扩展程序支持 32 位和 64 位版本的 Outlook 2016、Outlook 2021、Outlook 2024 和 Outlook 365 for Arm64。

在 Outlook 中，接收的电子邮件首先由“邮件威胁防护”组件进行扫描（如果在 Kaspersky Endpoint Security 界面中选定了“POP3、SMTP、NNTP 和 IMAP 流量”复选框），然后由 Outlook 的“邮件威胁防护”扩展程序进行扫描。如果“邮件威胁防护”组件在邮件中检测到恶意对象，会就此事件向您发出警报。

如果在 Kaspersky Endpoint Security 界面中选定了“已链接 Microsoft Office Outlook 扩展程序”，则可以直接在 Outlook 中配置“邮件威胁防护”组件设置（参见下图）。

Outlook 中的邮件威胁防护组件设置

发送的电子邮件首先由 Outlook 的“邮件威胁防护”扩展程序进行扫描，然后由“邮件威胁防护”组件进行扫描。

如果使用 Outlook 的邮件威胁防护扩展程序扫描邮件，建议使用缓存的交换模式。有关缓存 Exchange 模式的详细信息和对其用途的建议，请参阅 Microsoft 知识库。

要配置 Outlook 的邮件威胁防护扩展程序的操作模式：

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **基本威胁防护** → **邮件威胁防护**。
4. 在“**安全级别**”块中单击“**设置**”按钮。
5. 在打开的窗口中，在“**连接**”块，点击“**设置**”按钮。

6. 在“**电子邮件保护**”窗口中，执行以下操作之一：

- 如果您想让 Outlook 的邮件威胁防护扩展程序扫描邮箱中的传入消息，选择**接收时扫描**复选框。
- 如果您想让 Outlook 的邮件威胁防护扩展程序在用户打开邮箱中的传入消息时扫描它们，选择**读取时扫描**复选框。
- 如果您想让 Outlook 的邮件威胁防护扩展程序扫描发送的传出消息，选择**发送时扫描**复选框。

7. 保存更改。

在 Thunderbird、MyOffice 和 R7-Office 中扫描电子邮件

“邮件威胁防护”组件扫描传入和传出电子邮件的附件是否有病毒和其他威胁。对于 Mozilla Thunderbird、MyOffice Mail 和 R7-Office Organizer 邮件客户端，应用程序只能在*协议级别*（POP3、SMTP、IMAP、NNTP）访问邮件。

要扫描 Mozilla Thunderbird、MyOffice Mail 和 R7-Office Organizer 邮件客户端中的流量，您需要将卡巴斯基证书添加到证书存储并选择自己的证书存储。

如果在浏览器中打开邮件客户端，“邮件威胁防护”组件不会扫描邮件。

实时邮件威胁防护

邮件威胁防护可以扫描传入和传出的邮件。默认情况下，“邮件威胁防护”组件将自动尝试对已经检测到的所有受感染电子邮件执行清除操作。如果清除失败，“邮件威胁防护”组件会删除感染的电子邮件。当在附件中检测到恶意文件时，Kaspersky Endpoint Security 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>*。

当使用 Mozilla Thunderbird 邮件客户端时，如果使用过滤器将电子邮件移出“收件箱”文件夹，则“邮件威胁防护”组件不扫描经由 IMAP 协议发送的电子邮件以查找病毒和其他威胁。

邮件数据库中的恶意软件扫描

*恶意软件扫描*任务允许扫描邮件格式文件。如果在这些邮件客户端的文件中检测到恶意对象，Kaspersky Endpoint Security 只会将检测到的对象的信息添加到活动威胁列表中。无论任务设置如何，应用程序都不会对邮件数据库中的受感染文件清除或删除。

消除活动威胁

邮件威胁防护可在协议级别防止计算机感染，但如果计算机在安装 Kaspersky Endpoint Security 之前已被感染，则应用程序可能只在邮件数据库中检测威胁。邮件威胁防护不包含专门用于将邮件拆分成各个部分（邮件头、邮件正文、附件）的组件，比如对于 Microsoft Office Outlook。因此，应用程序无法删除或清除检测到的对象。Kaspersky Endpoint Security 仅将有关受感染对象的信息添加到活动威胁列表中。

要消除活动威胁：

1. 在邮件客户端界面中手动查找并删除包含检测到的对象的邮件。

   应用程序在活动威胁列表中显示有关检测到的对象的信息。

   检测到的对象卡片示例：

!	**HEUR:Trojan.PDF.Phish.gen** 对象：`C:\Users\admin\AppData\Roaming\Thunderbird\Profiles\ov56jpz0.default-release\Mail\mail.company.ru\Inbox// [From USER NAME <company@mail.com>][Date 25 Sep 2025 20:05:36] [Subj Mail title X] Object.pdf`

2. 执行数据库压缩操作。

   当用户在界面中删除邮件时，邮件客户端只会添加一个删除标记。邮件客户端只有在数据库压缩后才会真正删除邮件。有关数据库压缩的详细信息，请参阅邮件客户端的帮助文档（例如，Mozilla Thunderbird）。

3. 再次运行“*恶意软件扫描*”任务，并确保威胁已不存在。

网络威胁防护

*网络威胁防护组件*组件（也称Intrusion Detection System，IDS）监控入站网络流量以查找网络攻击的活动特征。当应用程序在用户计算机上检测到网络攻击企图时，它将阻止与攻击计算机的网络连接。应用程序数据库提供了当前已知类型的网络攻击以及应对方法的描述。“网络威胁防护”组件检测到的网络攻击列表在数据库和应用程序模块更新期间更新。

启用和禁用网络威胁防护

默认情况下，“网络威胁防护”已启用并在最优模式下运行。Kaspersky Endpoint Security 监测入站网络流量以查找网络攻击的活动特征并阻止攻击。

如何在管理控制台（MMC）中启用或禁用网络威胁防护

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **基本威胁防护** → **网络威胁防护**。

4. 使用“**网络威胁防护**”复选框启用或禁用组件。

5. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中启用或禁用网络威胁防护

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **通信和 Web 保护** → **网络威胁防护**。
5. 使用**网络威胁防护已启用**开关启用或禁用组件。
6. 保存更改。

如何在应用程序界面中启用或禁用网络威胁防护

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**网络威胁防护**”。

网络威胁防护设置

3. 使用**网络威胁防护**开关启用或禁用组件。
4. 保存更改。

阻止攻击计算机

如果启用网络威胁防护组件，Kaspersky Endpoint Security 会自动阻止网络威胁。此外，应用程序可以阻止攻击计算机并在一定时间内限制网络数据包的发送。默认情况下，Kaspersky Endpoint Security 会阻止计算机一小时。

如何在管理控制台（MMC）中阻止攻击计算机

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **基本威胁防护** → **网络威胁防护**。
4. 在“**网络威胁防护设置**”下，选择“**阻止攻击设备 N 分钟**”复选框。

   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。
5. 在“**阻止攻击设备 N 分钟**”复选框右侧的字段中为攻击计算机设置不同的阻止持续时间。
6. 保存更改。

如何在 Web Console 和云控制台中阻止攻击计算机

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

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **通信和 Web 保护** → **网络威胁防护**。
5. 在“**检测到威胁后的操作**”块中，选中“**阻止攻击和攻击设备(分钟)**”复选框。

   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。
6. 更改攻击计算机的阻止持续时间。
7. 保存更改。

如何在应用程序的用户界面中阻止攻击计算机

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**网络威胁防护**”。

网络威胁防护设置

3. 打开“**阻止攻击设备 N 分钟**”拨动开关。

   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。

4. 在“**阻止攻击设备 N 分钟**”拨动开关下方的字段中为攻击计算机设置不同的阻止持续时间。

5. 保存更改。

结果，当 Kaspersky Endpoint Security 检测到针对用户计算机的网络攻击企图时，它将阻止与攻击计算机的网络连接。Kaspersky Endpoint Security 创建“*检测到网络攻击*”事件。事件包含有关攻击计算机的信息：IP 和 MAC 地址。

> 您可以在应用程序的用户界面或 Kaspersky Security Center 控制台版本 15.1 中查看攻击计算机的 MAC 地址。

关于网络攻击检测的通知

当指定时间用完时，Kaspersky Endpoint Security 会解除对计算机的阻止。Kaspersky Security Center 控制台不提供用于监控报告中“*检测到网络攻击*”事件以外的被阻止计算机的工具。您只能在应用程序界面中查看阻止计算机的列表。此功能由“*网络监控*”工具提供。您还可以使用网络监控工具来解锁计算机。

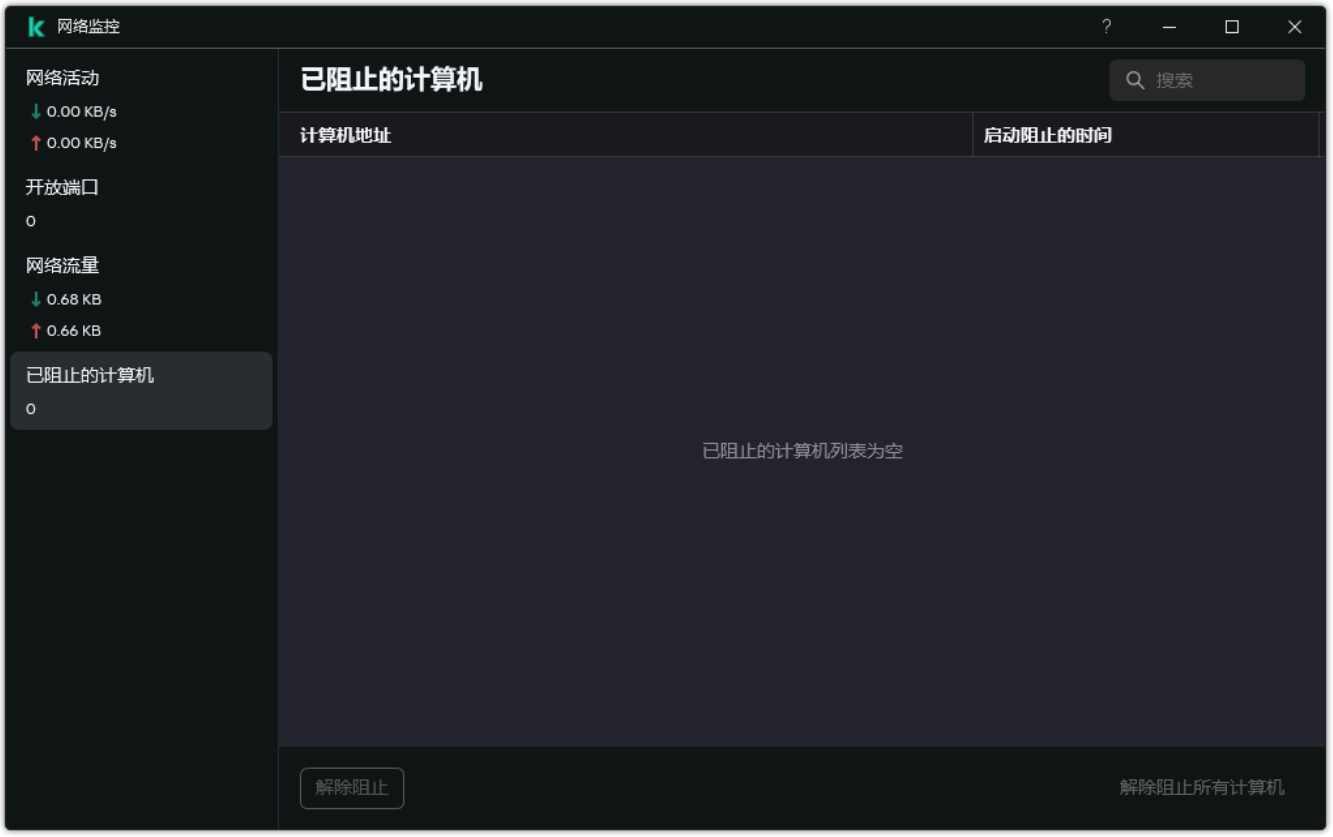
要解锁计算机：

1. 在应用程序主窗口中，在“**监控**”区域，单击“**网络监控**”瓦片。
2. 转到“**已阻止的计算机**”选项卡。

   这将打开被阻止计算机的列表（见下图）。

   > 当应用程序重启和网络威胁防护设置被更改时，Kaspersky Endpoint Security 清空阻止列表。

3. 选择您要取消阻止的计算机，然后单击“**解除阻止**”。



被阻止的计算机列表

配置排除在阻止外的地址

Kaspersky Endpoint Security 可以识别网络攻击并阻止不安全的传输大量数据包的网络连接（例如，从摄像头）。要使用收信人设备，您可以添加这些设备的 IP 地址到排除项列表。您还可以选择用于通信并允许特定网络活动的协议和端口。

Kaspersky Endpoint Security 12.2 中添加了选择排除项的协议和端口的功能。确保应用程序和管理插件已更新至版本 12.2 或更高版本。如果您使用的是早期版本的应用程序或管理插件，Kaspersky Endpoint Security 只能通过 IP 地址允许网络活动。

更改阻止排除项列表可能会受到父策略属性的阻止。要更改列表，您需要允许更改以下设置：Web Console 中的受信任区域（“挂锁”必须处于解锁状态）。

管理控制台(MMC) 和 Web Console 中受信任区域的分组方式不同。同样，防止受信任区域参数更改的方式也不同（“挂锁”不同）。我们建议仅使用 Web Console 来管理应用程序。如果在不同的控制台中配置受信任区域，管理插件可能会将“挂锁”重置为其默认状态。

如何在管理控制台（MMC）中配置排除项地址

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **基本威胁防护** → **网络威胁防护**。

4. 在“**网络威胁防护设置**”块中单击“**排除项**”按钮。

5. 在打开的窗口中，单击“**添加**”按钮。

6. 输入不阻止网络攻击的计算机的 IP 地址。
   如果需要，选择用于传输数据的协议和端口。

7. 保存更改。

如何在 Web Console 和云控制台中配置排除项地址

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **通信和 Web 保护** → **网络威胁防护**。

5. 在窗口上部，单击“**受信任 IP 地址**”链接。

6. 在打开的窗口中，单击“**添加**”按钮。

7. 输入不阻止网络攻击的计算机的 IP 地址。
   如有必要，请指定子网。

8. 保存更改。

如何在应用程序的用户界面中配置排除项地址

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**网络威胁防护**”。

网络威胁防护设置

3. 单击**管理排除项**链接。
4. 在打开的窗口中，单击“**添加**”按钮。
5. 输入不阻止网络攻击的计算机的 IP 地址。
   如果需要，选择用于传输数据的协议和端口。
6. 保存更改。

导出和导入扩展名排除列表

可以将排除列表导出到 XML 文件。然后可以修改文件，例如，添加大量相同类型的地址。还可以使用导出/导入功能备份排除列表或将列表迁移到其他服务器。

如何在管理控制台（MMC）中导出和导入排除列表

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **基本威胁防护** → **网络威胁防护**。

4. 在“**网络威胁防护设置**”块中单击“**排除项**”按钮。

5. 要导出规则列表：

   a. 选择您要导出的排除项。要选择多个端口，使用 **CTRL** 或 **SHIFT** 键。
   如果您未选择任何排除项，Kaspersky Endpoint Security 将导出所有排除项。

   b. 单击“ → **导出**”按钮。

   c. 在打开的窗口中，指定您要将排除项列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。

   d. 保存文件。
   Kaspersky Endpoint Security 会将整个排除项列表导出到 XML 文件。

6. 要导入排除项列表：

   a. 单击“ → **导入**”按钮。

   b. 在打开的窗口中，选择要从中导入排除项列表的 XML 文件。

   c. 打开文件。
   如果计算机已经具有排除项的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 XML 文件向其中添加新条目。

7. 保存更改。

如何在 Web Console 和云控制台中导出和导入排除列表

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **通信和 Web 保护** → **网络威胁防护**。

5. 在窗口上部，单击“**受信任 IP 地址**”链接。
排除项列表打开。

6. 要导出规则列表：

   a. 选择您要导出的排除项。

   b. 单击“ → **导出**”按钮。
   Kaspersky Endpoint Security 导出排除项列表到默认下载文件夹中的 JSON 文件。

7. 要导入排除项列表：

   a. 单击“ → **导入**”按钮。

      在打开的窗口中，选择要从中导入排除项列表的 JSON 文件。

   b. 打开文件。

      如果计算机已经具有排除项的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 JSON 文件向其中添加新条目。

8. 保存更改。

按类型配置网络威胁防护

Kaspersky Endpoint Security 允许您管理对以下类型的网络攻击的保护：

- *网络 Flooding* 是对网络资源或组织（例如 Web 服务器）的攻击。该攻击包括发送大量的请求以让网络资源过载。当发生此类事情时，用户无法访问组织的网络资源。

- *端口扫描*攻击包括扫描计算机上的 UDP 端口、TCP 端口和网络服务。该攻击允许攻击者识别计算机的漏洞程度，然后再发起更危险的网络攻击。端口扫描也允许攻击者识别计算机上的操作系统并选择针对性的网络攻击。

- *MAC 欺骗攻击*包括更改网络设备（网卡）的 MAC 地址。结果，攻击者可以将发送到某台设备的数据重定向到另一台设备，并获得对该数据的访问权限。Kaspersky Endpoint Security 允许您阻止 MAC 欺骗攻击并接收关于攻击的通知。

如果一些您允许的应用程序执行了类似某些类型攻击的操作，您可以禁用对这些类型攻击的检测。这将帮助避免误报。

默认下，Kaspersky Endpoint Security 不监控网络 Flooding、端口扫描和 MAC 欺骗攻击。

> 我们不建议在 Microsoft Hyper-V 基础架构中的虚拟机上启用 MAC 欺骗保护。由于 Microsoft Hyper-V 平台的特殊性，Kaspersky Industrial CyberSecurity for Nodes 可能会因误报结果而阻止 Hypervisor。

如何在管理控制台（MMC）中按类型配置网络威胁防护

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **基本威胁防护** → **网络威胁防护**。

4. 使用“**将端口扫描和网络 Flooding 视为攻击**”复选框启用或禁用对这些攻击的检测。

   如果启用此功能，Kaspersky Endpoint Security 会监控网络流量以检测端口扫描和网络泛洪。如果检测到此类行为，应用程序会通知用户并将相应事件发送到 Kaspersky Security Center。该应用程序提供有关发出请求的计算机的信息。此信息对于及时响应是必要的。但是，Kaspersky Endpoint Security 不会阻止发出请求的计算机，因为此类流量可能在公司网络上很常见。

5. 在**MAC 欺骗防护模式**区块，选择以下选项之一：

   - “**不跟踪 MAC 欺骗**”。
   - “**通知**”。
   - “**阻止**”。

6. 保存更改。

如何在 Web Console 和云控制台中按类型配置网络威胁防护

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **通信和 Web 保护** → **网络威胁防护**。
5. 使用“**将端口扫描和网络 Flooding 视为攻击**”复选框启用或禁用对这些攻击的检测。
   如果启用此功能，Kaspersky Endpoint Security 会监控网络流量以检测端口扫描和网络泛洪。如果检测到此类行为，应用程序会通知用户并将相应事件发送到 Kaspersky Security Center。该应用程序提供有关发出请求的计算机的信息。此信息对于及时响应是必要的。但是，Kaspersky Endpoint Security 不会阻止发出请求的计算机，因为此类流量可能在公司网络上很常见。
6. 在**MAC 欺骗防护**区块，选择以下选项之一：

   - “MAC **欺骗防护已启用**”。
   - “**通知**”。
   - “**阻止**”。

7. 保存更改。

如何在应用程序界面中按类型配置网络威胁防护

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**网络威胁防护**”。

网络威胁防护设置

3. 使用**将端口扫描和网络 Flooding 视为攻击**开关以启用或禁用对这些攻击的检测。

   如果启用此功能，Kaspersky Endpoint Security 会监控网络流量以检测端口扫描和网络泛洪。如果检测到此类行为，应用程序会通知用户并将相应事件发送到 Kaspersky Security Center。该应用程序提供有关发出请求的计算机的信息。此信息对于及时响应是必要的。但是，Kaspersky Endpoint Security 不会阻止发出请求的计算机，因为此类流量可能在公司网络上很常见。

4. 使用**MAC 欺骗防护**开关以启用或禁用对这些攻击的检测。

5. 在**在检测到 MAC 欺骗攻击时的操作**区块，选择以下选项之一：

   - “**通知**”。
   - “**阻止**”。

6. 保存更改。

防火墙

在互联网或局域网上工作时，防火墙组件会阻止未经授权的计算机连接。防火墙还控制计算机上应用程序的网络活动。这允许您保护公司局域网免受身份盗窃和其他攻击。该组件借助反病毒数据库、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。

网络代理被用于与 Kaspersky Security Center 的交互。防火墙自动创建应用程序和网络代理工作所需的网络规则。结果，防火墙打开计算机上的若干个端口。打开哪些端口取决于计算机的角色（例如，分发点）。要了解要在计算机上打开的端口，请参阅 Kaspersky Security Center 帮助。

网络规则

您可以在以下级别配置网络规则：

- *网络数据包规则*。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。Kaspersky Endpoint Security 具有预定义的网络数据包规则，其中权限由 Kaspersky 专家推荐。
- *应用程序网络规则*。应用程序网络规则将对特定应用程序的网络活动进行限制。它们不仅将网络数据包的特征列入重要参考因素，还把接收或发送该网络数据包的应用程序列入重要参考因素中。

应用程序对操作系统资源、进程和个人数据的受控访问由“主机入侵防御”组件通过*应用程序权限*提供。

在应用程序首次启动期间，“防火墙”执行以下操作：

1. 使用下载的反病毒数据库检查应用程序的安全性。
2. 在卡巴斯基安全网络中检查应用程序安全性。

   建议您加入卡巴斯基安全网络以帮助“防火墙”更有效地工作。
3. 将应用程序置于其中一个信任组中：*受信任*、*低限制*、*高限制*、*不信任*。

   信任组定义了在控制应用程序活动时 Kaspersky Endpoint Security 所引用的权限。Kaspersky Endpoint Security 会将应用程序放置在某个信任组中，具体取决于该应用程序可能对计算机造成的危险级别。

   Kaspersky Endpoint Security 将应用程序放置在“防火墙”和“主机入侵防御”组件的信任组中。您不能仅更改“防火墙”或“主机入侵防御”的信任组。

   如果您拒绝加入 KSN 或没有网络，Kaspersky Endpoint Security 会根据“主机入侵防御”组件的设置将应用程序放置在某个信任组中。从 KSN 收到应用程序的信誉后，可以自动更改信任组。
4. 它根据信任组阻止应用程序的网络活动。例如，不允许“*高限制*”信任组中的应用程序使用任何网络连接。

当应用程序下一次启动时，Kaspersky Endpoint Security 会检查该应用程序的完整性。如果应用程序未更改，则该组件对其应用当前网络规则。如果应用程序已经过修改，Kaspersky Endpoint Security 会分析应用程序，就像它首次启动时一样。

网络规则优先级

每条规则都有优先级。规则在列表中的位置越高，优先级越高。如果将网络活动添加到多条规则中，“防火墙”会根据优先级最高的规则来管理网络活动。

网络数据包规则的优先级比应用程序网络规则高。如果网络数据包规则和应用程序网络规则指定了同一类别的网络活动，则该网络活动将根据网络数据包规则进行处理。

应用程序的网络规则以特定方式工作。应用程序的网络规则包括基于网络状态的访问规则：*公用网络*、*本地网络*、*受信任网络*。例如，默认情况下，“*高限制*”信任组中的应用程序在所有状态的网络中均不允许进行任何网络活动。如果为单个应用程序（父应用程序）指定了网络规则，则其他应用程序的子进程将依据父应用程序的网络规则运行。如果没有为应用程序指定网络规则，则子进程将依据应用程序信任组的网络访问规则运行。

例如，对于除浏览器 X 之外的所有应用程序，您已禁止所有状态的网络中的任何网络活动。如果从浏览器 X（父应用程序）中启动浏览器 Y 的安装（子进程），则浏览器 Y 安装程序将能够访问网络并下载必要的文件。安装之后，浏览器 Y 将根据防火墙设置被拒绝任何网络连接。要禁止作为子进程的浏览器 Y 安装程序的网络活动，必须为浏览器 Y 的安装程序添加网络规则。

网络连接类型

“防火墙”允许您根据网络连接的类型来控制网络活动。Kaspersky Endpoint Security 从计算机的操作系统接收网络连接类型。操作系统中的网络连接类型由用户在建立连接时设置。您可以在 Kaspersky Endpoint Security 设置中更改网络连接的类型。“防火墙”将根据 Kaspersky Endpoint Security 设置中而不是操作系统中指定的网络类型来监控网络活动。

有以下网络连接类型可用：

- “**公用网络**”。网络不受反病毒应用程序、防火墙或过滤器保护（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，防火墙可阻止对此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访问数据和远程访问该计算机的桌面。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。

  防火墙默认给互联网分配“*公用网络*”类型。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**”。其中的计算机不会暴露于攻击或未经授权的数据访问尝试的安全网络。防火墙允许在具有此状态的网络中进行任何网络活动。

启用或禁用防火墙

默认情况下，防火墙为启动状态，各种功能均配置为最优模式。

如何在管理控制台（MMC）中启用或禁用防火墙

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择“**基本威胁防护**”→“**防火墙**”。
4. 使用“**防火墙**”复选框启用或禁用组件。
5. 保存更改。

如何在 Web Console 和云控制台中启用或禁用防火墙

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择“**通信和 Web 保护**”→“**防火墙**”。
5. 使用**防火墙已启用**开关启用或禁用组件。
6. 保存更改。

如何在应用程序界面中启用或禁用防火墙

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**防火墙**”。
3. 使用**防火墙**开关启用或禁用组件。
4. 保存更改。

因此，如果启用防火墙，Kaspersky Endpoint Security 将控制网络活动，并阻止未经授权的网络连接到您的计算机，以及阻止您计算机上应用程序的未经授权的网络活动。网络活动也由网络威胁防护组件控制。网络威胁防护组件（也称为入侵检测系统）监测入站网络流量以查找网络攻击的活动特征。

> Kaspersky Endpoint Security 在其报告中记录网络攻击事件，而不考虑防火墙设置。即使防火墙使用规则阻止网络连接，从而防止网络攻击，网络威胁防护组件也会注册网络攻击事件。需要生成有关组织中计算机上网络攻击的统计信息。

更改网络连接类型

防火墙默认给互联网分配“*公用网络*”类型。您无法更改互联网的类型。

要更改网络连接类型，请执行以下操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**防火墙**”。
3. 单击“**可用网络**”。
4. 选择您想要更改其类型的网络连接。
5. 在“**网络类型**”栏，选择网络连接类型：
   - “**公用网络**”。网络不受反病毒应用程序、防火墙或过滤器保护（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，防火墙可阻止对此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访问数据和远程访问该计算机的桌面。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。
   - “**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**”。其中的计算机不会暴露于攻击或未经授权的数据访问尝试的安全网络。防火墙允许在具有此状态的网络中进行任何网络活动。
6. 保存更改。

管理网络数据包规则

您在管理网络数据包规则时可执行以下操作：

- 创建新的网络数据包规则。

  您可以通过创建一个可应用于网络数据包和数据流的条件集和操作集来创建新的网络数据包规则。

- 启用或禁用网络数据包规则。

  默认情况下，由防火墙创建的所有网络数据包规则处于“*启用*”状态。当启用网络数据包规则时，防火墙应用此规则。

  您可以禁用网络数据包规则列表中选择的任何网络数据包规则。当禁用网络数据包规则时，防火墙临时不应用此规则。

  > 默认情况下，新添加到网络数据包规则列表中的自定义网络数据包规则处于“*启用*”状态。

- 编辑现有网络数据包规则的设置。

  当您创建新的网络数据包规则之后，您始终可以重新编辑其设置并根据需要进行修改。

- 更改网络数据包规则的防火墙操作。

  在网络数据包规则列表中，您可以编辑防火墙在检测到与特定网络数据包规则匹配的网络活动时的操作。

- 更改网络数据包规则的优先级。

  您可以提高或降低列表中选择的网络数据包规则的优先级。

- 删除网络数据包规则。

您可以删除网络数据包规则以停止防火墙将此规则应用于检测网络活动，并停止将此规则显示在“*禁用*”状态的网络数据包规则列表中。

创建网络数据包规则

防火墙根据网络包规则过滤计算机上的所有网络活动。网络包规则包含防火墙用于控制计算机网络连接的条件（例如方向、协议）。网络包规则还指定防火墙对符合规则的连接执行的操作（允许或阻止连接）。

创建网络包规则的建议

您可以指定一个 IP 地址或一个 IP 地址范围来过滤网络活动。您还可以指定 DNS 名称，但我们建议使用 IP 地址和 IP 地址范围。在网络包名称中使用 DNS 名称可能不安全，因为 DNS 服务器的所有者可以修改 DNS 记录的参数。恶意的操作者还可以伪造 DNS 消息并绕过防火墙规则。

您可以使用 Web 控制规则按 DNS 名称控制网络连接。如果需要在防火墙规则中指定 DNS 名称：

- 确保企业局域网的安全。
- 确保缓存和权威 DNS 服务器的安全。
- 启用 DNS 记录防修改保护。

在创建网络数据包规则时，请记住，它们的优先级比应用程序网络规则高。

创建网络包规则的方法

您可以用以下方法之一创建网络数据包规则：

- 使用网络监控工具。

  *网络监控器*是一个用于实时查看用户计算机网络活动信息的工具。这个方法很方便，因为您不需要配置所有的规则设置。一些防火墙设置将被从网络监控数据自动插入。网络监控仅在应用程序界面可用。

- 配置防火墙设置。

  这允许您微调防火墙设置。您可以为任何网络活动创建规则，即便当前没有网络活动。

如何使用网络监控工具在应用程序界面中创建网络数据包规则

1. 在应用程序主窗口中，在“**监控**”区域，单击“**网络监控**”瓦片。
2. 转到“**网络活动**”选项卡。

   “**网络活动**”选项卡将显示计算机的所有当前活动网络连接。接收和发送的网络连接都将显示出来。

3. 在网络连接上下文菜单中，选择**创建网络包规则**。

   这将打开网络规则属性。

4. 为包规则设置**活动**状态。

5. 在**名称**字段手动输入网络服务名称。

6. 配置网络规则设置（参见下表）。
   您可以通过单击**网络规则模板**链接选择预定义的规则模板。规则模板描述了最常使用的网络连接。所有网络规则设置将被自动填充。

7. 如果您希望将网络规则的操作反映在“报告”中，请选中“**记录事件**”复选框。

8. 单击“**保存**”。
   网络规则将被添加到列表。

9. 使用**上移** / **下移**按钮设置网络规则的优先级。

10. 保存更改。

如何使用防火墙设置在应用程序界面中创建网络数据包规则

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**防火墙**”。

3. 单击“**包规则**”。
   这将打开防火墙设置的默认网络规则列表。

4. 使用“**添加**”下拉列表，选择规则在列表中的位置：列表顶部、列表底部或所选规则旁边。
   规则在列表中的位置决定了规则的优先级。列表顶部的规则具有最高优先级。

5. 为包规则设置**活动**状态。

6. 在**名称**字段手动输入网络服务名称。

7. 配置网络规则设置（参见下表）。
   您可以通过单击**网络规则模板**链接选择预定义的规则模板。规则模板描述了最常使用的网络连接。所有网络规则设置将被自动填充。

8. 如果您希望将网络规则的操作反映在“报告”中，请选中“**记录事件**”复选框。

9. 单击“**保存**”。
   网络规则将被添加到列表。

10. 使用**上移** / **下移**按钮设置网络规则的优先级。

11. 保存更改。

如何在管理控制台 (MMC) 中创建网络数据包规则

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择“**基本威胁防护**”→“**防火墙**”。

4. 在“**防火墙设置**”块中单击“**设置**”按钮。
   这将打开网络数据包规则列表和应用程序网络规则列表。

5. 转到“**网络数据包规则**”选项卡。
   这将打开防火墙设置的默认网络规则列表。

6. 使用“**添加**”下拉列表，选择规则在列表中的位置：列表顶部、列表底部或所选规则旁边。
   规则在列表中的位置决定了规则的优先级。列表顶部的规则具有最高优先级。

7. 在**名称**字段手动输入网络服务名称。

8. 配置网络规则设置（参见下表）。
   您可以通过单击 按钮选择预定义的规则模板。规则模板描述了最常使用的网络连接。
   所有网络规则设置将被自动填充。

9. 如果您希望将网络规则的操作反映在“报告”中，请选中“**记录事件**”复选框。

10. 保存新网络规则。

11. 使用**上移** / **下移**按钮设置网络规则的优先级。

12. 保存更改。

防火墙将根据规则控制网络数据包。您可以在防火墙操作中禁用一个包规则而不将其从列表删除。为此，清空对象旁边的复选框。

如何在 Web Console 和云控制台中创建网络包规则

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

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

3. 选择**应用程序设置**选项卡。

4. 选择“**通信和 Web 保护**”→“**防火墙**”。

5. 选择**网络数据包规则**选项卡。
   这将打开防火墙设置的默认网络规则列表。

6. 单击“**添加**”。
   这将打开新网络规则的表单。

7. 在**规则名称**字段手动输入网络服务名称。

8. 配置网络规则设置（参见下表）。
   您可以通过单击**选择规则模板**链接选择预定义的规则模板。规则模板描述了最常使用的网络连接。
   所有网络规则设置将被自动填充。

9. 如果您希望将网络规则的操作反映在“报告”中，请选中“**记录事件**”复选框。

10. 保存网络规则。

    网络规则将被添加到列表。

11. 使用**移动**按钮设置网络规则的优先级。

12. 保存更改。

防火墙将根据规则控制网络数据包。您可以在防火墙操作中禁用一个包规则而不将其从列表删除。使用**状态**栏的开关启用或禁用包规则。

"网络数据包规则"设置

参数	描述
操作	"**允许**"。 "**阻止**"。 "**根据应用程序规则**"。如果该选项被选择，防火墙应用应用程序网络规则到网络连接。
协议	在所选协议上控制网络活动：TCP、UDP、ICMP、ICMPv6、IGMP 和 GRE。 如果选择的是 ICMP 或 ICMPv6 端口，您可以定义 ICMP 数据包类型和代码。 如果选择的是 TCP 或 UDP 协议类型，您可以指定其连接受监控的本地和远程计算机端口号。端口号的值范围是 0–65535。在每个字段中，您可以输入多个值，并用"`,`"分隔，或者使用"`-`"指定值范围。例如： • `100,101` • `100-130` • `100,110-130`
方向	"**入站(包)**"。防火墙应用网络规则到所有入站网络包。 "**入站**"。防火墙应用网络规则到所有通过由远程计算机发起的网络连接发送的网络包。 "**入站/出站**"。防火墙应用网络规则到所有入站和出站网络包。 "**出站(包)**"。防火墙应用网络规则到所有出站网络包。 "**出站**"。防火墙应用网络规则到所有通过由用户计算机发起的网络连接发送的网络包。
网络适配器	您可以发送和/或接收网络包的网络适配器。指定网络适配器的设置可以区分相同 IP 地址发送或接收的网络数据包。
生存时间 (TTL)	通过网络数据包的生存期（Time to Live，TTL）来限制对网络数据包的控制。
远程地址	发送和/或接收网络数据包的远程计算机的网络地址。防火墙将网络规则应用于指定范围的远程网地址。您可以包含所有 IP 地址到网络规则，创建 IP 地址的单独列表，指定 IP 地址范围，或选择一个子网(受信任网络、本地网络、公共网络)。您还可以指定计算机的 DNS 名称，而不是其 IP 地址。您应该仅对 LAN 计算机或内部服务使用 DNS 名称。与云服务（如 Microsoft Azure）和其他互联网资源的交互应由 Web 控件组件处理。 如果您在网络数据包规则中添加了无法确定 IP 地址的 DNS 名称，Kaspersky Endpoint Security 将显示警告。在 Web Console 的网络数据包规则列表中，列中添加了错误的描述。在管理控制台（MMC）中，错误描述不可用。此类数据包规则以颜色突出显示。
本地地址	发送和/或接收网络数据包的计算机的网络地址。防火墙将网络规则应用于指定范围的本地网地址。您可以包含所有 IP 地址到网络规则，创建 IP 地址的单独列表，或指定一个 IP 地址范围。 仅当指定了远程地址列表时，应用程序才会存储本地地址。也就是说，已为"**远程地址**"选择了"**来自列表的地址**"值，并且至少已添加一个地址。 有时候无法获得应用程序的本地地址。如果是这种情况，该参数被忽略。

启用或禁用网络数据包规则

要启用或禁用网络数据包规则，请执行以下操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**防火墙**”。
3. 单击“**包规则**”。
   这将打开防火墙设置的默认网络数据包规则列表。
4. 在列表中选择所需的网络数据包规则。
5. 使用**状态**栏的开关启用或禁用规则。
6. 保存更改。

更改网络数据包规则的防火墙操作

要更改应用于网络数据包规则的防火墙操作，请执行以下操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**防火墙**”。
3. 单击“**包规则**”。
   这将打开防火墙设置的默认网络数据包规则列表。
4. 在列表中选择该规则，并单击“**编辑**”按钮。
5. 在“**操作**”下拉列表中选择防火墙在检测到此类网络活动后的操作：
   - “**允许**”。
   - “**阻止**”。
   - “**根据应用程序规则**”。如果该选项被选择，防火墙应用应用程序网络规则到网络连接。
6. 保存更改。

更改网络数据包规则的优先级

网络数据包规则的优先级取决于其在网络包规则列表中的位置。包规则列表中位于最上方的优先级最高。

每个手工创建的网络数据包规则都将被添加到包规则列表尾部，拥有最低的优先级。

防火墙将按照网络数据包规则列表中规则的显示顺序自上而下执行规则。根据应用于特定网络连接的每个已处理网络数据包规则，防火墙会允许或阻止对该网络连接设置中指定的地址和端口的网络访问。

要更改网络数据包规则优先级，请执行以下操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**防火墙**”。
3. 单击“**包规则**”。
   这将打开防火墙设置的默认网络数据包规则列表。
4. 在列表中选择您希望更改其优先级的网络数据包规则。
5. 使用**上移** / **下移**按钮设置网络规则的优先级。
6. 保存更改。

导出和导入网络包规则

您可以将网络包规则列表导出到 XML 文件。然后可以修改文件，例如，添加大量相同类型的规则。还可以使用导出/导入功能备份网络包规则列表或将列表迁移到其他服务器。

如何在管理控制台(MMC)中导出和导入网络包规则列表

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择“**基本威胁防护**”→“**防火墙**”。
4. 在“**防火墙设置**”块中单击“**设置**”按钮。
   这将打开网络数据包规则列表和应用程序网络规则列表。
5. 转到“**网络数据包规则**”选项卡。
6. 要导出网络包规则列表：
   a. 选择您要导出的规则。要选择多个端口，使用 **CTRL** 或 **SHIFT** 键。
      如果您未选择任何规则，Kaspersky Endpoint Security 将导出所有规则。
   b. 单击**导出**链接。
   c. 在打开的窗口中，指定您要将规则列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。
   d. 保存文件。
      Kaspersky Endpoint Security 会将整个规则列表导出到 XML 文件。
7. 要导入网络包规则列表：
   a. 单击**导入**链接。
      在打开的窗口中，选择要从中导入规则列表的 XML 文件。

b. 打开文件。

如果计算机已经具有规则的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 XML 文件向其中添加新条目。

8. 保存更改。

如何在 Web Console 和云控制台中导出和导入网络包规则列表

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择“**通信和 Web 保护**”→“**防火墙**”。

5. 要在**网络数据包规则**块导出规则列表：

   a. 选择您要导出的规则。

   b. 单击“ → **导出**”按钮。

   Kaspersky Endpoint Security 导出规则列表到默认下载文件夹中的 JSON 文件。

6. 要在**网络数据包规则**块导入规则列表：

   a. 单击“ → **导入**”按钮。

   在打开的窗口中，选择要从中导入规则列表的 JSON 文件。

   b. 打开文件。

   如果计算机已经具有规则的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 JSON 文件向其中添加新条目。

7. 保存更改。

用 XML 定义网络数据包规则

防火墙允许以 XML 格式导出网络数据包规则。然后可以修改文件，例如，添加大量相同类型的规则。

XML 文件包含两个主要节点：`Rules`和`Resources`。`Rules`节点列出网络数据包规则。此节点包含默认配置的规则（*预定义规则*）以及用户添加的规则（*自定义规则*）。

网络数据包规则标记

```
<key name="0000">
        <tDWORD name="RuleId">100</tDWORD>
        <tDWORD name="RuleState">1</tDWORD>
        <tDWORD name="RuleTypeId">4</tDWORD>
        <tQWORD name="AppIdEx">0</tQWORD>
        <tDWORD name="ResIdEx">812</tDWORD>
        <tDWORD name="ResIdEx2">0</tDWORD>
        <tDWORD name="AccessFlag">2</tDWORD>
</key>
```

XML 格式的网络数据包规则设置

参数	描述	值
`<key name="0000">`	规则优先级。值越低，优先级越高。	整数 优先级值必须由 4 位数字组成。XML 文件中的节点必须按优先级值排列，从 `0000` 开始。
`RuleId`	规则 ID。	**预定义规则** `100` – **通过 TCP 请求 DNS 服务器**。 `101` – **通过 UDP 请求 DNS 服务器**。 `102` – **发送电子邮件消息**。 `110` – **任何网络活动**（受信任网络）。 `125` – **任何网络活动**（本地网络）。 `130` – **远程桌面网络活动**。 `131` – **通过本地端口的 TCP 连接**。 `132` – **通过本地端口的 UDP 连接**。 `133` – **传入的 TCP 流**。 `134` – **传入的 UDP 流**。 `137` – ICMP **目的地无法接通传入响应**。 `138` – ICMP **回显应答传入数据包**。 `140` – ICMP **超时传入响应**。 `142` – **传入的** ICMP **流**。 `266` – ICMPv6 **回显请求传入数据包**。
`RuleState`	规则状态。	`0` – 预定义规则已禁用 `1` – 预定义规则已启用 `2` – 自定义规则已禁用 `3` – 自定义规则已启用
`RuleTypeId`	规则类型 ID。	`4` – 网络数据包规则。
`AppIdEx`	网络数据包规则所属的应用程序的 ID。	如果规则不属于任何应用程序，则值是 `0`。
`ResIdEx`	具有规则设置的资源的主 ID。您可以使用此标识符在“`Resources`”节点中查找具有规则设置的块。	整数
`ResIdEx2`	网络类型 ID。	`0` – **任何地址**。 `50` – **受信任网络**。 `51` – **本地网络**。 `52` – **公用网络**。 `<Network Identifier>` – **来自列表的地址**（地址是手动定义的）。
`AccessFlag`	**操作**参数的值。	`0` – **允许**。 `2` – **根据应用程序规则**。 `3` – **阻止**。 `4` – **允许** 和 **记录事件**。 `6` – **根据应用程序规则** 和 **记录事件**。 `7` – **阻止** 和 **记录事件**。
`</key>`		

“`Resources`”节点包含网络数据包规则设置。自定义网络数据包规则设置列于“`<key name="0004">`”块中。

自定义网络数据包规则标记

```
<key name="0026">
        <key name="Data">
                <key name="RemotePorts"> </key>
                <key name="LocalPorts"> </key>
                <key name="AdapterBindings">
```

```
                        <key name="0000">
                                <key name="IpAddresses">
                                        <key name="0000">
                                                <key name="IP">
                                                        <key name="V6">
                                                                <tQWORD name="Hi">0</tQWORD>
                                                                <tQWORD name="Lo">0</tQWORD>
                                                                <tDWORD name="Zone">0</tDWORD>
                                                                <tSTRING name="ZoneStr"/>
                                                        </key>
                                                        <tBYTE name="Version">4</tBYTE>
                                                        <tDWORD name="V4">16909060</tDWORD>
                                                        <tBYTE name="Mask">32</tBYTE>
                                                </key>
                                                <key name="AddressIP"> </key>
                                                <tSTRING name="Address"/>
                                        </key>
                                </key>
                                <key name="MacAddresses">
                                        <key name="0000">
                                                <tDWORD name="Type">0</tDWORD>
                                                <tQWORD name="AddressData0">1108152157446</tQWORD>
                                                <tQWORD name="AddressData1">0</tQWORD>
                                        </key>
                                </key>
                                <tSTRING name="AdapterName">ADAPTER TEST 123</tSTRING>
                                <tDWORD name="InterfaceType">3</tDWORD>
                        </key>
                </key>
                <tTYPE_ID name="unique">3213697024</tTYPE_ID>
                <tBYTE name="Proto">2</tBYTE>
                <tBYTE name="Direction">2</tBYTE>
                <tBYTE name="IcmpType">0</tBYTE>
                <tBYTE name="IcmpCode">0</tBYTE>
                <tDWORD name="Flags">1</tDWORD>
                <tBYTE name="TTL">255</tBYTE>
        </key>
        <key name="Childs"> </key>
        <tDWORD name="Id">1073747214</tDWORD>
        <tDWORD name="ParentID">7</tDWORD>
        <tDWORD name="Flags">38</tDWORD>
        <tSTRING name="Name">TEST1</tSTRING>
</key>
```

自定义网络数据包规则设置

参数	描述	值
`<key name="Data">`	参数 ID 块。	整数
`RemotePorts`	**远程端口**参数的值。	远程端口范围列表。
`LocalPorts`	**本地端口**参数的值。	本地端口范围列表。
`AdapterBindings`	**网络适配器**参数的值。	`IpAddresses` – **IP 地址**参数的值。 `MacAddresses` – **MAC 地址**参数的值。 `AdapterName` – 网络适配器的名称。 `InterfaceType` – **接口类型**参数的值： • `0` – **其他**。 • `1` – **LoopBack**。 • `2` – **有线网络(以太网)**。 • `3` – **无线网络(Wi-Fi)**。 • `4` – **隧道**。 • `5` – **PPP 连接**。 • `6` – **PPPoE 连接**。 • `7` – **VPN 连接**。 • `8` – **Modem 连接**。
`unique`	结构的内部 ID。	整数 建议保持此参数不变。

参数	描述	值
`Proto`	**协议**参数的值。	`0` – 已禁用。 `1` – ICMP。 `2` – IGMP。 `6` – TCP。 `17` – UDP。 `47` – GRE。 `58` – ICMPv6。
`Direction`	**方向**参数的值。	`1` – **入站(包)**。 `2` – **出站(包)**。 `3` – **入站/出站**。 `4` – **入站**。 `5` – **出站**。

参数	描述	值
`IcmpType`	**ICMP 类型**参数的值。	**ICMP 协议** `0` – **Echo Reply**（ICMP）或已禁用。 `3` – **Destination Unreachable**（ICMP）。 `4` – **Source Quench**。 `5` – **Redirect**。 `6` – **Alternate Host Address**。 `8` – **Echo Request**。 `9` – **Router Advertisement**。 `10` – **Router Solicitation**。 `11` – **Time Exceeded**。 `12` – **Parameter Problem**。 `13` – **Timestamp**。 `14` – **Timestamp Reply**。 `15` – **Information Request**。 `16` – **Information Reply**。 `17` – **Address Mask Request**。 `18` – **Address Mask Reply**。 `30` – **Traceroute**。 `31` – **Datagram Conversion Error**。 `32` – **Mobile Host Redirect**。 `33` – **IPv6 Where-Are-You**。 `34` – **IPv6 I-Am-Here**。 `35` – **Mobile Registration Request**。 `36` – **Mobile Registration Reply**。 `37` – **Domain Name Request**。 `38` – **Domain Name Reply**。 `40` – **Photuris**。 **ICMPv6 协议** `1` – **Destination Unreachable**。 `2` – **Packet Too Big**。 `3` – **Time Exceeded**。 `4` – **Parameter Problem**。 `128` – **Echo Request**。 `129` – **Echo Reply**。 `130` – **Multicast Listener Query**。 `131` – **Multicast Listener Report**。 `132` – **Multicast Listener Done**。 `133` – **Router Solicitation**。 `134` – **Router Advertisement**。 `135` – **Neighbor Solicitation**。 `136` – **Neighbor Advertisement**。 `137` – **Redirect Message**。 `138` – **Router Renumbering**。 `139` – **ICMP Node Information Query**。 `141` – **Inverse Neighbor Discovery Solicitation Message**。 `142` – **Inverse Neighbor Discovery Advertisement Message**。 `143` – **Version 2 Multicast Listener Report**。

参数	描述	值
		144 – Home Agent Address Discovery Request Message。 145 – Home Agent Address Discovery Reply Message。 146 – Mobile Prefix Solicitation。 147 – Mobile Prefix Advertisement。 148 – Certification Path Solicitation Message。 149 – Certification Path Advertisement Message。 151 – Multicast Router Advertisement。 152 – Multicast Router Solicitation。 153 – Multicast Router Termination。
IcmpCode	ICMP **代码**参数的值。	0 – **代码** 0 或已禁用。 1 – **代码** 1。 2 – **代码** 2。
Flags	结构属性指针。	整数 建议保持此参数不变。
TTL	**生存时间**(TTL)参数的值。	以秒为单位的值。如果禁用，则值为 0。
</key>		
Id	资源的主 ID（参见“Rules”节点）。	整数
ParentID	父组 ID。	整数 建议保持此参数不变。
Flags	规则状态。	6 – 规则已禁用。 38 – 规则已启用。
Name	网络数据包规则名称。	字符串

管理应用程序网络规则

默认情况下，Kaspersky Endpoint Security 将按照其所监控的文件或网络活动所对应的软件的供应商名称对安装在计算机上的所有应用程序进行分组。应用程序组将依次被归类到“信任组”中。所有应用程序和应用程序组都将继承来自其父组的属性：应用程序控制规则、应用程序网络规则及其执行优先级。

像“主机入侵防御”组件一样，默认情况下，“防火墙”组件在过滤应用程序组内所有应用程序的网络活动时将应用该应用程序组的网络规则。应用程序组网络规则将定义组中应用程序访问不同网络连接的权限。

默认情况下，防火墙将为计算机上的 Kaspersky Endpoint Security 检测到的每个应用程序组创建网络规则集。您可以更改应用于默认创建的应用程序组网络规则的防火墙操作。您不能编辑、删除、禁用或更改默认情况下创建的应用程序组网络规则的优先级。

您也可以为单个应用程序创建网络规则。此类规则将拥有比该应用程序所属网络规则组高的优先级。

创建应用程序网络规则

默认情况下，应用程序的活动由 Kaspersky Endpoint Security 在此应用程序第一次启动时将其分配到的信任组定义的网络规则来控制。如有必要，您可以为整个信任组、单个应用程序或信任组内的一组应用程序创建网络规则。

手动定义的网络规则比信任组的网络规则具有更高的优先级。换言之，如果手动定义的应用程序规则与信任组定义的应用程序规则不同，防火墙根据手动定义的应用程序规则控制应用程序活动。

默认下，防火墙为每个应用程序创建以下网络规则：

- 受信任网络中的任何网络活动。
- 本地网络中的任何网络活动。
- 公共网络中的任何网络活动。

Kaspersky Endpoint Security 根据以下预定义的网络规则控制应用程序的网络活动：

- 受信任和低限制：所有网络活动被允许。
- 高限制和不受信任：所有网络活动被阻止。

预定义应用程序规则无法被编辑或删除。

您可以用以下方法之一创建应用程序网络规则：

- 使用网络监控工具。

  *网络监控器*是一个用于实时查看用户计算机网络活动信息的工具。这个方法很方便，因为您不需要配置所有的规则设置。一些防火墙设置将被从网络监控数据自动插入。网络监控仅在应用程序界面可用。

- 配置防火墙设置。

  这允许您微调防火墙设置。您可以为任何网络活动创建规则，即便当前没有网络活动。

> 当创建应用程序网络规则时，网络包规则比应用程序网络规则具有更高的优先级。

如何使用网络监控工具在应用程序界面中创建应用程序网络规则

1. 在应用程序主窗口中，在“**监控**”区域，单击“**网络监控**”瓦片。
2. 转到“**网络活动**”或“**开放端口**”选项卡。

   “**网络活动**”选项卡将显示计算机的所有当前活动网络连接。接收和发送的网络连接都将显示出来。

   “**开放端口**”选项卡列出了计算机的所有开放网络端口。
3. 在网络连接上下文菜单中，选择**创建应用程序网络规则**。

   应用程序规则和属性窗口打开。
4. 选择**网络规则**选项卡。

   这将打开防火墙设置的默认网络规则列表。

5. 单击“**添加**”。
   这将打开网络规则属性。

6. 在**名称**字段手动输入网络服务名称。

7. 配置网络规则设置（参见下表）。
   您可以通过单击**网络规则模板**链接选择预定义的规则模板。规则模板描述了最常使用的网络连接。所有网络规则设置将被自动填充。

8. 如果您希望将网络规则的操作反映在“报告”中，请选中“**记录事件**”复选框。

9. 单击“**保存**”。
   网络规则将被添加到列表。

10. 使用**上移** / **下移**按钮设置网络规则的优先级。

11. 保存更改。

如何使用防火墙设置在应用程序界面中创建应用程序网络规则

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**防火墙**”。

3. 单击“**应用程序规则**”。
   这将打开防火墙设置的默认网络规则列表。

4. 在应用程序列表中，选择您想为其创建网络规则的应用程序或应用程序组。

5. 右键单击以打开上下文菜单并选择“**详情和规则**”。
   应用程序规则和属性窗口打开。

6. 选择**网络规则**选项卡。

7. 单击“**添加**”。
   这将打开网络规则属性。

8. 在**名称**字段手动输入网络服务名称。

9. 配置网络规则设置（参见下表）。
   您可以通过单击**网络规则模板**链接选择预定义的规则模板。规则模板描述了最常使用的网络连接。所有网络规则设置将被自动填充。

10. 如果您希望将网络规则的操作反映在“报告”中，请选中“**记录事件**”复选框。

11. 单击“**保存**”。
    网络规则将被添加到列表。

12. 使用**上移** / **下移**按钮设置网络规则的优先级。

13. 保存更改。

如何在管理控制台 (MMC) 中创建应用程序网络规则

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择“**基本威胁防护**”→“**防火墙**”。
4. 在“**防火墙设置**”块中单击“**设置**”按钮。

   这将打开网络数据包规则列表和应用程序网络规则列表。
5. 转到“**应用程序网络规则**”选项卡。
6. 单击“**添加**”。
7. 在打开的窗口中，输入标准以查找您要为其创建网络规则的应用程序。

   您可以输入应用程序名称或供应商名称。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 * 以及 ? 字符。
8. 单击“**刷新**”。

   Kaspersky Endpoint Security 将在安装于受管理计算机上的应用程序列表中搜索应用程序。Kaspersky Endpoint Security 将显示满足您的搜索标准的应用程序列表。
9. 选择需要的应用程序。
10. 在**将选定应用程序添加至信任组**下拉列表中，选择**默认组**并单击**确定**。

    应用程序将被添加到默认组。
11. 选择相关应用程序并从应用程序的上下文菜单中选择**应用程序权限**。

    应用程序规则和属性窗口打开。
12. 选择**网络规则**选项卡。

    这将打开防火墙设置的默认网络规则列表。
13. 单击“**添加**”。

    这将打开网络规则属性。
14. 在**名称**字段手动输入网络服务名称。
15. 配置网络规则设置（参见下表）。

    您可以通过单击 按钮选择预定义的规则模板。规则模板描述了最常使用的网络连接。

    所有网络规则设置将被自动填充。
16. 如果您希望将网络规则的操作反映在“报告”中，请选中“**记录事件**”复选框。
17. 保存新网络规则。
18. 使用**上移** / **下移**按钮设置网络规则的优先级。
19. 保存更改。

如何在 Web Console 和云控制台中创建应用程序网络规则

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择“**通信和 Web 保护**”→“**防火墙**”。
5. 在“**应用程序权限和受保护资源**”区域，单击“**应用程序权限**”链接。
   这将打开应用程序权限配置窗口和受保护资源列表。
6. 转到“**应用程序权限**”选项卡。
   您将在窗口的左边看到信任组列表，窗口的右边显示它们的属性。
7. 在“**应用程序**”块中单击“**添加**”按钮。
   这将启动添加应用程序到信任组向导。
8. 为应用程序选择相关的信任组。
9. 选择“**应用程序**”类型。转到下一步。
   如果您要为多个应用程序创建网络规则，选择**组**类型并为应用程序组定义名称。
10. 在打开的应用程序列表中，选择您想为其创建或编辑网络规则的应用程序。
    使用过滤器。您可以输入应用程序名称或供应商名称。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 * 以及 ? 字符。
11. 退出向导。
    应用程序将被添加到信任组。
12. 在窗口左侧，选择相关应用程序。
13. 在窗口右侧从下拉列表，选择“**网络规则**”。
    这将打开防火墙设置的默认网络规则列表。
14. 单击“**添加**”。
    这将打开应用程序规则属性。
15. 在**规则名称**字段手动输入网络服务名称。
16. 配置网络规则设置（参见下表）。
    您可以通过单击**选择规则模板**链接选择预定义的规则模板。规则模板描述了最常使用的网络连接。
    所有网络规则设置将被自动填充。
17. 如果您希望将网络规则的操作反映在“报告”中，请选中“**记录事件**”复选框。
18. 保存网络规则。
    网络规则将被添加到列表。

19. 使用**移动**按钮设置网络规则的优先级。

20. 保存更改。

"应用程序网络规则"设置

参数	描述
操作	"**允许**"。 "**阻止**"。
协议	在所选协议上控制网络活动：TCP、UDP、ICMP、ICMPv6、IGMP 和 GRE。 如果选择的是 ICMP 或 ICMPv6 端口，您可以定义 ICMP 数据包类型和代码。 如果选择的是 TCP 或 UDP 协议类型，您可以指定其连接受监控的本地和远程计算机端口号。端口号的值范围是 0–65535。在每个字段中，您可以输入多个值，并用"`,`"分隔，或者使用"`-`"指定值范围。例如： • `100,101` • `100-130` • `100,110-130`
方向	"**入站**"。 "**入站/出站**"。 "**出站**"。
远程地址	发送和/或接收网络数据包的远程计算机的网络地址。防火墙将网络规则应用于指定范围的远程网地址。您可以包含所有 IP 地址到网络规则，创建 IP 地址的单独列表，指定 IP 地址范围，或选择一个子网(受信任网络、本地网络、公共网络)。您还可以指定计算机的 DNS 名称，而不是其 IP 地址。您应该仅对 LAN 计算机或内部服务使用 DNS 名称。与云服务（如 Microsoft Azure）和其他互联网资源的交互应由 Web 控件组件处理。 如果您在网络数据包规则中添加了无法确定 IP 地址的 DNS 名称，Kaspersky Endpoint Security 将显示警告。在 Web Console 的网络数据包规则列表中，列中添加了错误的描述。在管理控制台（MMC）中，错误描述不可用。此类数据包规则以颜色突出显示。
本地地址	发送和/或接收网络数据包的计算机的网络地址。防火墙将网络规则应用于指定范围的本地网地址。您可以包含所有 IP 地址到网络规则，创建 IP 地址的单独列表，或指定一个 IP 地址范围。 仅当指定了远程地址列表时，应用程序才会存储本地地址。也就是说，已为"**远程地址**"选择了"**来自列表的地址**"值，并且至少已添加一个地址。 有时候无法获得应用程序的本地地址。如果是这种情况，该参数被忽略。

启用和禁用应用程序网络规则

要启用或禁用应用程序网络规则，请执行以下操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择"**基本威胁防护**" → "**防火墙**"。

3. 单击"**应用程序规则**"。
   这将打开应用程序规则列表。

4. 在应用程序列表中，选择您想为其创建或编辑网络规则的应用程序或应用程序组。

5. 右键单击以打开上下文菜单并选择"**详情和规则**"。
   应用程序规则和属性窗口打开。

6. 选择**网络规则**选项卡。

7. 在应用程序组的网络规则列表中，选择相关的网络规则。

   “网络规则属性”窗口打开。

8. 为网络规则设置**活动**或**非活动**状态。

   您不能禁用默认情况下由防火墙创建的应用程序组网络规则。

9. 保存更改。

更改应用程序网络规则的防火墙操作

您可以更改应用于应用程序或应用程序组的所有网络规则的默认创建的防火墙操作，也可以为应用程序或应用程序组更改单个自定义网络规则的防火墙操作。

若要为应用程序或应用程序组更改所有网络规则的防火墙操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**防火墙**”。

3. 单击“**应用程序规则**”。

   这将打开应用程序规则列表。

4. 如果您希望更改默认创建的应用至所有网络规则的防火墙操作，则选择列表中应用程序或应用程序组。手动创建的网络规则将保持不变。

5. 右击打开上下文菜单，选择**网络规则**，然后选择您要分配的操作：

   - “**继承**”。
   - “**允许**”。
   - “**阻止**”。

6. 保存更改。

要更改应用程序或应用程序组网络规则的防火墙响应，请执行以下操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**防火墙**”。

3. 单击“**应用程序规则**”。

   这将打开应用程序规则列表。

4. 在列表中选择您想为其更改一个网络规则操作的应用程序或应用程序组。

5. 右键单击以打开上下文菜单并选择“**详情和规则**”。

   应用程序规则和属性窗口打开。

6. 选择**网络规则**选项卡。

7. 选择您要为其更改防火墙操作的网络规则。

8. 在“**权限**”列中，单击右键显示上下文菜单，然后选择您要分配的操作：
   - “**继承**”。
   - “**允许**”。
   - “**拒绝**”。
   - “**记录事件**”。
9. 保存更改。

更改应用程序网络规则的优先级

网络规则的优先级取决于其在网络规则列表中的位置。防火墙执行按照网络规则列表中规则的显示顺序自上而下执行规则。根据应用于特定网络连接的每个已处理网络规则，防火墙会允许或阻止对该网络连接设置中指定的地址和端口的网络访问。

手动创建的网络规则拥有比默认网络规则高的优先级。

> 您不能更改默认情况下创建的应用程序组网络规则的优先级。

要更改网络规则的优先级，请执行以下操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**基本威胁防护**” → “**防火墙**”。
3. 单击“**应用程序规则**”。
   这将打开应用程序规则列表。
4. 在应用程序列表中，选择您要更改网络规则优先级的应用程序或应用程序组。
5. 右键单击以打开上下文菜单并选择“**详情和规则**”。
   应用程序规则和属性窗口打开。
6. 选择**网络规则**选项卡。
7. 选择您想要更改其优先级的网络规则。
8. 使用**上移** / **下移**按钮设置网络规则的优先级。
9. 保存更改。

网络监控器

*网络监控器*是一个用于实时查看用户计算机网络活动信息的工具。

要启动网络监控器，请执行以下操作：

在应用程序主窗口中，在“**监控**”区域，单击“**网络监控**”瓦片。

“网络监控”窗口将开启。在该窗口中，计算机网络活动的相关信息将显示在四个选项卡上：

- “**网络活动**”选项卡将显示计算机的所有当前活动网络连接。接收和发送的网络连接都将显示出来。在此选项卡上，您还可以为防火墙操作创建网络包规则。
- “**开放端口**”选项卡列出了计算机的所有开放网络端口。在此选项卡上，您还可以为防火墙操作创建网络包规则和应用程序规则。
- “**网络流量**”选项卡显示用户计算机和在用户当前连接的网络上的其他计算机之间发送和接收的网络流量。
- “**已阻止的计算机**”选项卡列出了“网络威胁防护”组件在检测到从某些 IP 地址发起的网络攻击企图后阻止其网络活动的远程计算机的 IP 地址。

漏洞利用防御

“漏洞利用防御”组件可检测利用计算机漏洞来利用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。

漏洞利用防御组件还会监控可能威胁计算机安全的应用程序进程的网络端口。应用程序通过反病毒数据库获取有关此类进程的信息。

启用和禁用漏洞利用防御

默认情况下，漏洞利用防御被启用并工作在最优模式。Kaspersky Endpoint Security 监控易受攻击的应用程序运行的可执行文件。如果 Kaspersky Endpoint Security 检测到某个易于感染的应用程序的可执行文件被除用户以外的事物运行，Kaspersky Endpoint Security 将执行所选操作（例如，阻止操作）。

如何在管理控制台（MMC）中启用或禁用漏洞利用防御

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **高级威胁防护** → **漏洞利用防御**。
4. 使用“**漏洞利用防御**”复选框启用或禁用组件。

5. 在“**检测到漏洞时**”块中选择相关操作：

   - “**阻止**”。如果选择此项，在检测到漏洞时，Kaspersky Endpoint Security 会阻止此漏洞的操作，并生成一条包含此漏洞相关信息的日志条目。

   - “**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。

6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中启用或禁用漏洞利用防御

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **主机威胁防护** → **行为分析** → **漏洞利用防御**。

5. 使用**漏洞利用防御**开关启用或禁用组件。

6. 在“**检测到威胁后的操作**”块中选择相关操作：

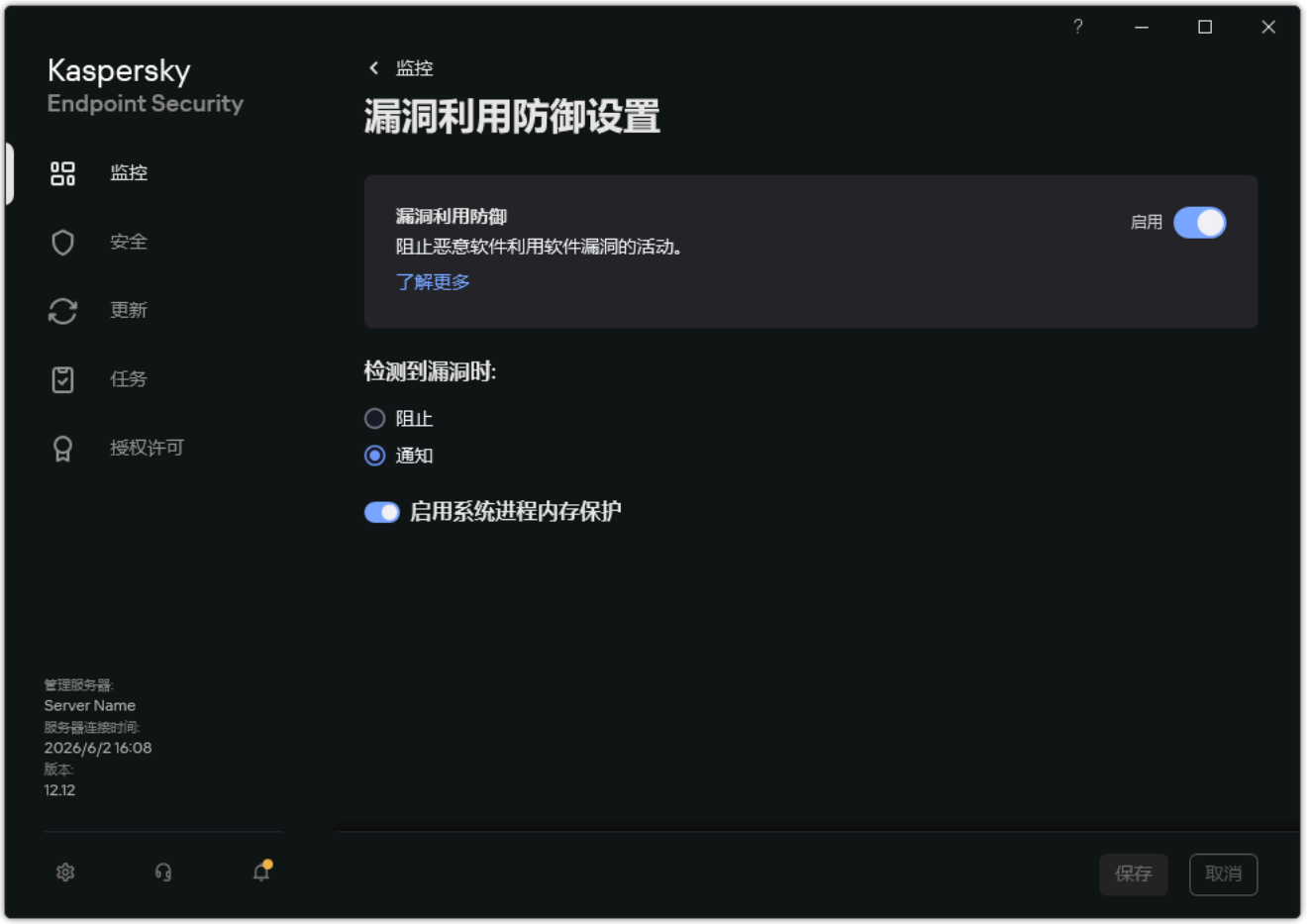
   - “**阻止**”。如果选择此项，在检测到漏洞时，Kaspersky Endpoint Security 会阻止此漏洞的操作，并生成一条包含此漏洞相关信息的日志条目。

   - “**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。

7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在应用程序界面中启用或禁用漏洞利用防御

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**高级威胁防护**” → “**漏洞利用防御**”。



漏洞利用防御设置

3. 使用**漏洞利用防御**开关启用或禁用组件。

4. 在“**检测到漏洞时**”块中选择相关操作：

   - “**阻止**”。如果选择此项，在检测到漏洞时，Kaspersky Endpoint Security 会阻止此漏洞的操作，并生成一条包含此漏洞相关信息的日志条目。

   - “**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。

5. 保存更改。

通知活动威胁

系统进程内存保护

默认情况下，启用系统进程内存保护。Kaspersky Endpoint Security 会阻止尝试访问系统进程的外部进程。

如何在管理控制台（MMC）中启用或禁用系统进程内存保护

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **高级威胁防护** → **漏洞利用防御**。

4. 使用“**启用系统进程内存保护**”复选框启用或禁用选项。

5. 保存更改。

如何在 Web Console 和云控制台中启用或禁用系统进程内存保护

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **主机威胁防护** → **行为分析** → **漏洞利用防御**。

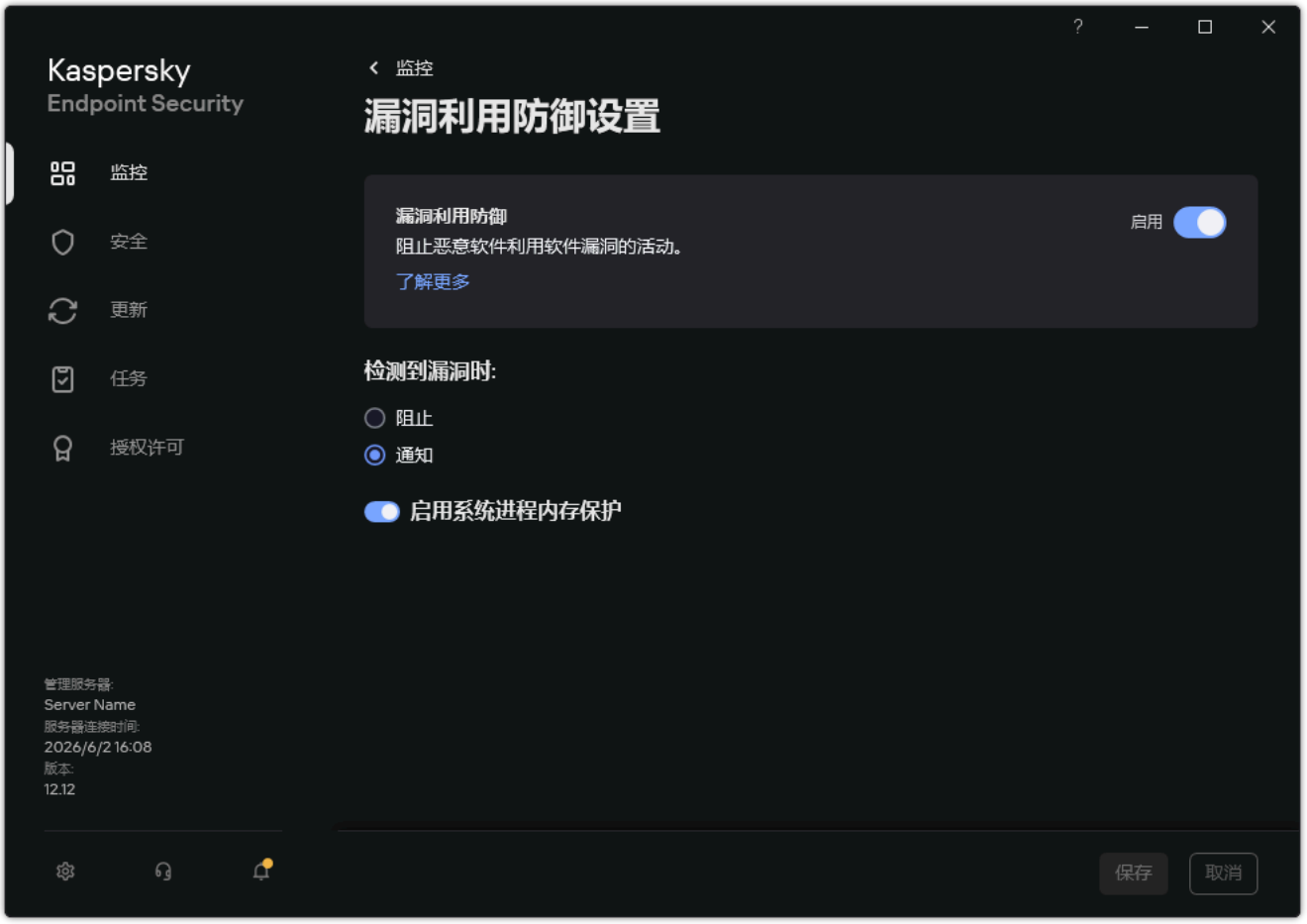
5. 使用**系统进程内存保护已启用**开关启用或禁用该功能。

6. 保存更改。

如何在应用程序界面中启用或禁用系统进程内存保护

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**高级威胁防护**” → “**漏洞利用防御**”。



漏洞利用防御设置

3. 使用**启用系统进程内存保护**开关启用或禁用该功能。

4. 保存更改。

行为检测

“行为检测”组件接收您计算机上的应用程序操作的信息，并将此信息提供给其他保护组件以提高性能。“行为检测”组件将行为流签名 (BSS) 用于应用程序。如果应用程序操作匹配行为流签名，Kaspersky Endpoint Security 将执行选定的响应操作。Kaspersky Endpoint Security 功能基于行为流签名，并为计算机提供主动防御。

行为检测组件还会监控可能威胁计算机安全的应用程序进程的网络端口。应用程序通过反病毒数据库获取有关此类进程的信息。

默认情况下，行为检测已启用并在 Kaspersky 专家建议的模式下运行。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。

除非绝对必要，否则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。保护组件可请求“行为检测”组件收集的数据以检测威胁。

如何在管理控制台(MMC)中启用或禁用行为检测

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**策略**”。
3. 选择必要的策略并双击以打开策略属性。
4. 在策略窗口中，选择 **高级威胁防护** → **行为检测**。
5. 使用“**行为检测**”复选框启用或禁用组件。
6. 在“**检测到恶意软件活动时的操作**”块中选择相关操作：
   - “**删除**”。如果选择此项目，在检测到恶意活动时，Kaspersky Endpoint Security 会删除恶意应用程序的可执行文件，同时在备份区创建该文件的备份副本。
   - “**阻止**”。如果选择此项目，在检测到恶意活动时，Kaspersky Endpoint Security 会终止该应用程序。
   - “**通知**”。如果选择此项目并且检测到应用程序的恶意软件活动，Kaspersky Endpoint Security 将应用程序恶意软件活动的相关信息添加至活动威胁列表。
7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中启用或禁用行为检测

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **主机威胁防护** → **行为分析** → **行为检测**
5. 使用**行为检测已启用**开关启用或禁用组件。
6. 在“**检测到威胁后的操作**”块中选择相关操作：
   - “**删除**”。如果选择此项目，在检测到恶意活动时，Kaspersky Endpoint Security 会删除恶意应用程序的可执行文件，同时在备份区创建该文件的备份副本。
   - “**阻止**”。如果选择此项目，在检测到恶意活动时，Kaspersky Endpoint Security 会终止该应用程序。
   - “**通知**”。如果选择此项目并且检测到应用程序的恶意软件活动，Kaspersky Endpoint Security 将应用程序恶意软件活动的相关信息添加至活动威胁列表。

7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在应用程序界面中启用或禁用行为检测

1. 打开主应用程序窗口并单击 按钮。

2. 在应用程序设置窗口中，选择“**高级威胁防护**” → “**行为检测**”。

行为检测设置

3. 使用**行为检测**开关启用或禁用组件。

4. 在“**检测到恶意软件活动时的操作**”块中选择相关操作：

   - “**删除**”。如果选择此项目，在检测到恶意活动时，Kaspersky Endpoint Security 会删除恶意应用程序的可执行文件，同时在备份区创建该文件的备份副本。

   - “**阻止**”。如果选择此项目，在检测到恶意活动时，Kaspersky Endpoint Security 会终止该应用程序。

   - “**通知**”。如果选择此项目并且检测到应用程序的恶意软件活动，Kaspersky Endpoint Security 将应用程序恶意软件活动的相关信息添加至活动威胁列表。

5. 保存更改。

结果，如果行为检测被启用，Kaspersky Endpoint Security 将使用行为流签名分析操作系统中的应用程序活动。

反加密

从 Kaspersky Endpoint Security 12.12 for Windows 开始，以前作为行为检测组件一部分的共享文件夹对外部加密的保护功能，现在已成为一个独立的组件，反加密。

该组件只能监控针对存储在文件系统为 NTFS 的大容量存储设备上并且未使用 EFS 加密的文件所进行的操作。

反加密组件分析共享文件夹中的活动。如果该活动与外部加密的典型行为流签名匹配，Kaspersky Endpoint Security 将执行选定操作。

要使反加密组件正常工作，您必须启用行为检测组件。

如果 Kaspersky Endpoint Security 检测到修改共享文件夹中的文件的尝试，则会执行以下操作：

- 阻止对启动恶意活动的会话的文件修改（该文件将是只读的）。
- 创建被修改的文件的备份副本。
- 添加条目至本地应用程序界面报告并将有关检测到的恶意活动的信息发送到 Kaspersky Security Center。
- 此外，如果启用了“修复引擎”组件，将从备份副本还原被修改的文件。

启用和禁用共享文件夹对外部加密的防护

默认情况下，共享文件夹针对外部加密的保护已启用，并按照卡巴斯基专家的推荐运行。要配置此功能，您可以创建保护范围并在必要时配置排除。默认情况下，应用程序会自动识别共享文件夹并监控所有文件夹中的文件活动。当检测到尝试对共享文件夹中的文件进行外部加密时，Kaspersky Endpoint Security 会阻止远程用户的会话一小时（默认情况下）。

安装 Kaspersky Endpoint Security 后，共享文件夹对外部加密的防护将受到限制，直到计算机重启为止。

如何在管理控制台 (MMC) 中启用或禁用共享文件夹对外部加密的防护

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **高级威胁防护** → **反加密勒索**。
4. 使用“**反加密勒索**”复选框启用或禁用对典型外部加密活动的检测。

5. 选择当检测到尝试修改共享文件夹中的文件时应用程序将采取的相关操作：

- **阻止连接时间 N 分钟**。如果选择此选项，当 Kaspersky Endpoint Security 检测到有人试图修改共享文件夹中的文件时，它将阻止启动恶意活动的会话对文件修改的访问，并创建已修改文件的备份副本。

  如果启用了“修复引擎”组件，并且选择“**阻止连接时间 N 分钟**”选项，被修改的文件将被从备份副本恢复。

- “**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 会将有关此尝试的信息添加到活动威胁列表中，并添加条目到本地应用程序界面报告，并将有关检测到的恶意活动的信息发送到 Kaspersky Security Center。

6. 如果有必要，编辑保护范围并定义排除项。

7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中启用或禁用共享文件夹对外部加密的防护

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **主机威胁防护** → **行为分析** → **反加密**。

5. 使用**反加密已启用**开关启用或禁用对典型外部加密活动的检测。

6. 选择当检测到尝试修改共享文件夹中的文件时应用程序将采取的相关操作：

- **阻止连接(分钟) N 分钟**。如果选择此选项，当 Kaspersky Endpoint Security 检测到有人试图修改共享文件夹中的文件时，它将阻止启动恶意活动的会话对文件修改的访问，并创建已修改文件的备份副本。

  如果启用了“修复引擎”组件，并且选择“**阻止连接(分钟) N 分钟**”选项，被修改的文件将被从备份副本恢复。

- “**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 会将有关此尝试的信息添加到活动威胁列表中，并添加条目到本地应用程序界面报告，并将有关检测到的恶意活动的信息发送到 Kaspersky Security Center。

7. 如果有必要，编辑保护范围并定义排除项。

8. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在应用程序界面中启用和禁用保护共享文件夹防止外部加密

1. 打开主应用程序窗口并单击 按钮。

2. 在应用程序设置窗口中，选择“**高级威胁防护**” → “**反加密程序**”。

3. 使用“**共享文件夹对外部加密的防护**”复选框启用或禁用对典型外部加密活动的检测。

4. 使用“**共享文件夹对外部加密的防护**”复选框启用或禁用对典型外部加密活动的检测。

5. 选择当检测到尝试修改共享文件夹中的文件时应用程序将采取的相关操作：

   - **阻止连接时长(分钟) N 分钟**。如果选择此选项，当 Kaspersky Endpoint Security 检测到有人试图修改共享文件夹中的文件时，它将阻止启动恶意活动的会话对文件修改的访问，并创建已修改文件的备份副本。

     > 如果启用了“修复引擎”组件，并且选择“**阻止连接时长(分钟) N 分钟**”选项，被修改的文件将被从备份副本恢复。

   - “**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 会将有关此尝试的信息添加到活动威胁列表中，并添加条目到本地应用程序界面报告，并将有关检测到的恶意活动的信息发送到 Kaspersky Security Center。

6. 如果有必要，编辑保护范围并定义排除项。

7. 保存更改。

配置不受信任的计算机的阻止期限

*不受信任的计算机*是正在从事恶意活动或数据加密的远程计算机。默认情况下，Kaspersky Endpoint Security 会阻止远程用户的会话一小时。当阻止期限到期时，Kaspersky Endpoint Security 会将计算机从阻止列表中删除并恢复对共享文件夹的访问。

如何在管理控制台 (MMC) 中配置不受信任的计算机的阻止期限

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **高级威胁防护** → **反加密勒索**。

4. 在“**检测到威胁后的操作**”块中，选择“ **阻止连接时间 N 分钟**”。

5. 配置正在从事恶意活动或数据加密的不受信任的计算机的阻止期限。

6. 保存更改。

如何在 Web Console 和云控制台中配置不受信任的计算机的阻止期限

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **主机威胁防护** → **行为分析** → **反加密**。

5. 在“**检测到威胁后的操作**”下，配置正在从事恶意活动或数据加密的不受信任的计算机的阻止期限。

6. 保存更改。

如果在应用程序界面中配置不受信任的计算机的阻止期限

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**高级威胁防护**” → “**反加密程序**”。
3. 在“**检测到威胁后的操作**”块中，选择“**阻止连接时长(分钟)**”。
4. 配置正在从事恶意活动或数据加密的不受信任的计算机的阻止期限。
5. 保存更改。

结果，远程计算机将被锁定。要解锁远程计算机，您可以重新启动 Kaspersky Endpoint Security。

编辑保护范围

*保护范围*是 Kaspersky Endpoint Security 监控文件活动的共享文件夹路径列表。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。默认情况下，应用程序会自动识别共享文件夹并监控所有文件夹中的文件活动。

如果您的组织在使用共享文件夹交换文件时使用数据加密，则从保护范围排除文件夹可以减少误报量。例如，当用户处理共享文件夹中具有 ENC 扩展名的文件时，行为检测可能会引发误报。这种活动与外部加密的典型行为模式相匹配。如果您在共享文件夹中有加密文件以保护数据，请将该文件夹添加到排除项。

> 您还可以排除不得处理外部加密尝试的计算机。

如何在管理控制台 (MMC) 中编辑保护范围

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **高级威胁防护** → **反加密勒索**。
4. 在“**保护范围**”块中，选择“**仅指定的共享文件夹**”。
5. 在文件夹列表中，单击“**添加**”。
6. 这将打开一个窗口；在该窗口中，输入要包含在保护范围内的共享文件夹的路径（例如，`C:\Share`）。

   > 要将共享文件夹添加到保护范围，请使用本地路径。

7. 单击“**正常**”。
8. 如有必要，定义保护范围排除项：
   a. 在“**扫描排除项**”块中单击“**按掩码**”按钮。
   b. 在打开的窗口中，单击“**添加**”按钮。

c. 在显示的窗口中，以“`*.<file extension>`”格式或文件夹路径指定文件扩展名。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。

应用程序不支持某些排除项文件扩展名。因此，您可以指定排除项为 `*.docx` 或者 `**\Folder\**`。

您可以从扫描排除对象，而不用将其从保护范围对象列表中删除。为此，清空对象旁边的复选框。

9. 保存更改。

如何在 Web Console 和云控制台中编辑保护范围

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

策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。
4. 选择 **主机威胁防护** → **行为分析** → **反加密**。
5. 在“**保护范围**”块中，选择“**仅指定的共享文件夹**”。
6. 在文件夹列表中，单击“**添加**”。
7. 这将打开一个窗口；在该窗口中，输入要包含在保护范围内的共享文件夹的路径（例如，`C:\Share`）。

> 要将共享文件夹添加到保护范围，请使用本地路径。

8. 单击“**确定**”。
9. 如有必要，定义保护范围排除项：

a. 在窗口上部，单击“**扫描排除项**”链接。

b. 在打开的窗口中，单击“**添加**”按钮。

c. 在显示的窗口中，以“`*.<file extension>`”格式或文件夹路径指定文件扩展名。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。

应用程序不支持某些排除项文件扩展名。因此，您可以指定排除项为 `*.docx` 或者 `**\Folder\**`。

您可以从扫描排除对象，而不用将其从保护范围对象列表中删除。为此，清空对象旁边的复选框。

10. 保存更改。

如何在应用程序界面中编辑保护范围

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**高级威胁防护**” → “**反加密程序**”。
3. 在“**保护范围**”块中，选择“**仅指定的共享文件夹**”。
4. 在文件夹列表中，单击“**添加**”。

5. 这将打开一个窗口；在该窗口中，输入要包含在保护范围内的共享文件夹的路径（例如，`C:\Share`）。

> 要将共享文件夹添加到保护范围，请使用本地路径。

6. 单击“**确定**”。

7. 如有必要，定义保护范围排除项：

   a. 在窗口上部，单击“**按掩码的排除项**”链接。

   b. 在打开的窗口中，单击“**添加**”按钮。

   c. 在显示的窗口中，以“`*.<file extension>`”格式或文件夹路径指定文件扩展名。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。

      应用程序不支持某些排除项文件扩展名。因此，您可以指定排除项为 `*.docx` 或者 `**\Folder\**`。

   您可以从扫描排除对象，而不用将其从保护范围对象列表中删除。为此，清空对象旁边的复选框。

8. 保存更改。

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**常规设置**” → “**排除项和检测对象类型**”。

3. 在“**排除项**”区域，单击“**管理排除项**”链接。

4. 单击“**添加**”。

5. 单击“**浏览**”并选择共享文件夹。

   您也可以手动输入路径。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符：

   - `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\*\*.txt` 将包括位于 C: 驱动器的文件夹（但不包括子文件夹）中所有具有 TXT 扩展名的文件的路径。

   - 两个连续 `*` 字符在文件或文件夹名称中代表任意一组字符（包括空集），包括 `\` 和 `/` 字符（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\**\*.txt` 将包括位于 `Folder` 嵌套子文件夹（除了 `Folder` 本身）中所有带 TXT 扩展名的文件的路径。掩码必须包含至少一个嵌套级别。掩码 `C:\**\*.txt` 不是有效掩码。

   - `?`（问号）字符代表任意单个字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\???.txt` 将包括位于 `Folder` 文件夹中所有带 TXT 扩展名且名称由三个字符构成的文件的路径。

   您可以在文件路径的开头、中间或末尾使用掩码。例如，您如果要将所有用户的文件夹添加到排除项，请输入 `?:\Users\*\Folder\` 掩码。

6. 在“**保护组件**”块中，选中“**行为检测**”组件。

7. 如有必要，在“**注释**”字段，输入您创建的扫描排除项的简短描述。

8. 为排除项选择**活动**状态。

   您可以随时使用开关停止排除项。

9. 保存更改。

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 转到**受信任区域**区域。

5. 在打开的窗口中，单击“**恶意软件扫描排除项**”链接。

6. 如果要为公司内的所有计算机创建排除项的综合列表，请选中“**继承时合并值**”复选框。将合并父策略和子策略中的排除项列表。如果启用继承时合并值，则将合并列表。父策略中的排除项以只读视图的形式显示在子策略中。无法更改或删除父策略的排除项。

7. 如果您要让用户创建排除项本地列表，选择“**允许使用本地排除项**”复选框。这样，除了策略中生成的排除项常规列表，用户可以创建他们自己的排除项本地列表。管理员可以使用 Kaspersky Security Center 在计算机属性中查看、添加、编辑或删除列表项目。

   如果复选框被清空，用户仅可以访问策略中生成的排除项常规列表。此外，如果清除此复选框，Kaspersky Endpoint Security 会在应用程序的用户界面中隐藏扫描排除项的综合列表。

8. 点击“**添加**”并选择一个操作：

   - “**类别**”。您可以将扫描排除项分组到不同的类别中。要创建新类别，请输入类别名称并向该类别添加至少一个扫描排除项。

   - “**新建排除项**”。Kaspersky Endpoint Security 会将新的扫描排除项添加到列表的根目录中。

   - “**从列表选择排除项**”。为了在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上快速配置 Kaspersky Endpoint Security，应用程序包括*预定义的扫描排除项*。还添加了预定义的扫描排除项，以支持 Citrix 和 VMware 虚拟环境中的应用程序设置。您必须根据受保护服务器的用途选择预定义的扫描排除项。

9. 选择您要添加排除项的方式：**文件或文件夹路径**。

10. 请输入共享文件夹的路径。

您也可以手动输入路径。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符：

- `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\*\*.txt` 将包括位于 C: 驱动器的文件夹（但不包括子文件夹）中所有具有 TXT 扩展名的文件的路径。

- 两个连续 `*` 字符在文件或文件夹名称中代表任意一组字符（包括空集），包括 `\` 和 `/` 字符（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\**\*.txt` 将包括位于 `Folder` 嵌套子文件夹（除了 `Folder` 本身）中所有带 TXT 扩展名的文件的路径。掩码必须包含至少一个嵌套级别。掩码 `C:\**\*.txt` 不是有效掩码。

- `?`（问号）字符代表任意单个字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\???.txt` 将包括位于 `Folder` 文件夹中所有带 TXT 扩展名且名称由三个字符构成的文件的路径。

您可以在文件路径的开头、中间或末尾使用掩码。例如，您如果要将所有用户的文件夹添加到排除项，请输入 `C:\Users\*\Folder\` 掩码。

11. 在“**将排除项应用于**”块中，选中“**行为检测**”组件。

12. 如有必要，在“**注释**”字段，输入您创建的扫描排除项的简短描述。

13. 为排除项选择**添加到排除项**状态。

    您可以随时使用开关停止排除项。

14. 保存更改。

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **常规设置** → **排除项和对象类型**。

4. 在“**扫描排除项和受信任应用程序** → **扫描排除项**”块中单击“**设置**”按钮。

   这将打开包含排除项列表的窗口。

5. 如果要为公司内的所有计算机创建排除项的综合列表，请选中“**继承时合并值**”复选框。将合并父策略和子策略中的排除项列表。如果启用继承时合并值，则将合并列表。父策略中的排除项以只读视图的形式显示在子策略中。无法更改或删除父策略的排除项。

6. 如果您要让用户创建排除项本地列表，选择“**允许使用本地排除项**”复选框。这样，除了策略中生成的排除项常规列表，用户可以创建他们自己的排除项本地列表。管理员可以使用 Kaspersky Security Center 在计算机属性中查看、添加、编辑或删除列表项目。

   如果复选框被清空，用户仅可以访问策略中生成的排除项常规列表。此外，如果清除此复选框，Kaspersky Endpoint Security 会在应用程序的用户界面中隐藏扫描排除项的综合列表。

7. 点击“**添加**”并选择一个操作：

   - “**类别**”。您可以将扫描排除项分组到不同的类别中。要创建新类别，请输入类别名称并向该类别添加至少一个扫描排除项。

   - “**新建排除项**”。Kaspersky Endpoint Security 会将新的扫描排除项添加到列表的根目录中。

   - “**从列表选择排除项**”。为了在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上快速配置 Kaspersky Endpoint Security，应用程序包括*预定义的扫描排除项*。还添加了预定义的扫描排除项，以支持 Citrix 和 VMware 虚拟环境中的应用程序设置。您必须根据受保护服务器的用途选择预定义的扫描排除项。

8. 单击“**添加**”。

9. 在“**属性**”块中，选中“**文件或文件夹**”复选框。

10. 单击“**扫描排除项说明(单击下划线项目进行编辑)**”块中的“**选择文件或文件夹。**”链接，打开“**文件或文件夹名称**”窗口。

11. 单击“**浏览**”并选择共享文件夹。

    您也可以手动输入路径。输入掩码时，Kaspersky Endpoint Security 支持 * 字符和 ? 字符：

    - `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\*\*.txt` 将包括位于 C: 驱动器的文件夹（但不包括子文件夹）中所有具有 TXT 扩展名的文件的路径。

    - 两个连续 `*` 字符在文件或文件夹名称中代表任意一组字符（包括空集），包括 `\` 和 `/` 字符（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\**\*.txt` 将包括位于 `Folder` 嵌套子文件夹（除了 `Folder` 本身）中所有带 TXT 扩展名的文件的路径。掩码必须包含至少一个嵌套级别。掩码 `C:\**\*.txt` 不是有效掩码。

    - `?`（问号）字符代表任意单个字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\???.txt` 将包括位于 `Folder` 文件夹中所有带 TXT 扩展名且名称由三个字符构成的文件的路径。

    您可以在文件路径的开头、中间或末尾使用掩码。例如，您如果要将所有用户的文件夹添加到排除项，请输入 `?:\Users\*\Folder\` 掩码。

12. 如有必要，在“**注释**”字段，输入您创建的扫描排除项的简短描述。

13. 单击“**扫描排除项说明(单击下划线项目进行编辑)**”块中的链接，打开“**保护组件**”窗口。

14. 选中“**行为检测**”组件旁边的复选框。

15. 保存更改。

添加受信任的计算机以进行外部数据加密

如果您的组织在其文件交换工作流程中使用外部数据加密，则必须创建受信任的计算机列表。Kaspersky Endpoint Security 不监控受信任的计算机的数据加密。

必须启用审计登录服务，才能从共享文件夹对外部加密的防护中排除地址。默认情况下，审计登录服务已禁用（有关启用审计登录服务的详细信息，请访问 Microsoft 网站）。

如果远程计算机在 Kaspersky Endpoint Security 启动前启动，从共享文件夹保护中排除地址的功能将不适用于该远程计算机。您可以在 Kaspersky Endpoint Security 启动后重启该远程计算机，确保从共享文件夹保护中排除地址的功能在该远程计算机上有效。

更改受信任计算机列表可能受到父策略属性的阻止。要更改列表，您需要允许更改以下设置：Web Console 中的受信任区域（“挂锁”必须处于解锁状态）。

管理控制台(MMC) 和 Web Console 中受信任区域的分组方式不同。同样，防止受信任区域参数更改的方式也不同（“挂锁”不同）。我们建议仅使用 Web Console 来管理应用程序。如果在不同的控制台中配置受信任区域，管理插件可能会将“挂锁”重置为其默认状态。

如何在管理控制台 (MMC) 中添加允许外部数据加密的受信任的计算机

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **高级威胁防护** → **反加密勒索**。
4. 在“**扫描排除项**”块中单击“**按名称或 IP 地址**”按钮。
5. 在打开的窗口中，单击“**按名称或 IP 地址**”按钮。
6. 输入不应处理其外部加密尝试的计算机的 IP 地址、IP 地址范围或名称。

   例如：

   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
7. 保存更改。

如何在 Web Console 和云控制台中添加允许外部数据加密的受信任的计算机

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **主机威胁防护** → **行为分析** → **反加密**。
5. 在窗口上部，单击“**按名称或 IP 地址的排除项**”链接。
6. 在打开的窗口中，单击“**添加**”按钮。
7. 输入不应处理其外部加密尝试的计算机的 IP 地址、IP 地址范围或名称。
   例如：
   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
8. 保存更改。

如何在应用程序界面中添加允许外部数据加密的受信任的计算机

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**高级威胁防护**” → “**反加密程序**”。
3. 在窗口上部，单击“**按名称或 IP 地址的排除项**”链接。
4. 在打开的窗口中，单击“**添加**”按钮。
5. 输入不应处理其外部加密尝试的计算机的 IP 地址、IP 地址范围或名称。
   例如：
   - `192.168.0.0 - 192.168.255.255`
   - `192.168.0.0/24`
   - `192.168.2-3.0-128`
   - `2001:db8:fd0c::/64`
   - `2001:db8:fd0c:: - 2001:db8:fd0c:ffff:ffff:ffff:ffff:ffff`
6. 保存更改。

从共享文件夹对外部加密的防护中导出和导入排除项列表

可以将排除列表导出到 XML 文件。然后可以修改文件，例如，添加大量相同类型的地址。还可以使用导出/导入功能备份排除列表或将列表迁移到其他服务器。

如何在管理控制台（MMC）中导出和导入排除列表

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **高级威胁防护** → **反加密勒索**。
4. 在“**扫描排除项**”块中单击“**按名称或 IP 地址**”按钮。
5. 要导出规则列表：
   a. 选择您要导出的排除项。要选择多个端口，使用 **CTRL** 或 **SHIFT** 键。
      如果您未选择任何排除项，Kaspersky Endpoint Security 将导出所有排除项。
   b. 单击“ → **导出**”按钮。
   c. 在打开的窗口中，指定您要将排除项列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。
   d. 保存文件。
      Kaspersky Endpoint Security 会将整个排除项列表导出到 XML 文件。
6. 要导入排除项列表：
   a. 单击“ → **导入**”按钮。
   b. 在打开的窗口中，选择要从中导入排除项列表的 XML 文件。
   c. 打开文件。
      如果计算机已经具有排除项的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 XML 文件向其中添加新条目。
7. 保存更改。

如何在 Web Console 和云控制台中导出和导入排除列表

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **主机威胁防护** → **行为分析** → **反加密**。
5. 单击**按名称或 IP 地址的排除项**链接。

6. 要导出规则列表：

   a. 选择您要导出的排除项。

   b. 单击“ → **导出**”按钮。

      Kaspersky Endpoint Security 导出排除项列表到默认下载文件夹中的 JSON 文件。

7. 要导入排除项列表：

   a. 单击“ → **导入**”按钮。

      在打开的窗口中，选择要从中导入排除项列表的 JSON 文件。

   b. 打开文件。

      如果计算机已经具有排除项的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 JSON 文件向其中添加新条目。

8. 保存更改。

修复引擎

修复引擎组件允许 Kaspersky Endpoint Security 回滚恶意软件在操作系统中执行的操作。

回滚操作系统中的恶意软件活动时，Kaspersky Endpoint Security 将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（在除网络驱动器外的所有介质上）创建的可执行文件。
  - 删除已被恶意软件入侵的程序所创建的可执行文件。
  - 恢复被恶意软件修改或删除的文件。

  文件恢复功能有一些限制.

- **注册表活动**

  Kaspersky Endpoint Security 执行以下操作：

  - 删除由恶意软件创建的注册表项。
  - 不会恢复被恶意软件修改或删除的注册表项。

- **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。
  - 终止被恶意应用程序渗透的进程。
  - 不恢复被恶意软件挂起的进程。

- **网络活动**
  Kaspersky Endpoint Security 执行以下操作：
  - 阻止恶意软件的网络活动。
  - 阻止被恶意软件入侵的进程的网络活动。

“文件威胁防护”或“行为检测”组件或在恶意软件扫描过程中可以启动恶意软件操作回滚。

回滚恶意软件操作会影响一组严格定义的数据。回滚对操作系统或计算机数据完整性无不良影响。

如何在管理控制台(MMC)中启用或禁用修复引擎

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **高级威胁防护** → **修复引擎**。
4. 使用“**修复引擎**”复选框启用或禁用组件。
5. 保存更改。

如何在 Web Console 和云控制台中启用或禁用修复引擎组件

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

如何在应用程序界面中启用或禁用修复引擎组件

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**高级威胁防护**” → “**修复引擎**”。
3. 使用**修复引擎**开关启用或禁用组件。
4. 保存更改。

结果，如果启用修复引擎，Kaspersky Endpoint Security 将回滚恶意应用程序在操作系统中所做的操作。

卡巴斯基安全网络

为了更有效地保护您的计算机，Kaspersky Endpoint Security 使用从全球用户处接收的数据。卡巴斯基安全网络设计用于收集此数据。

KSN 功能可能无法在美国的应用程序中使用。

卡巴斯基安全网络 (KSN) 是一个云服务的基础架构。它可以访问在线卡巴斯基知识库。该知识库中包含了文件信誉、网页资源和软件的相关信息。使用卡巴斯基安全网络的数据可确保 Kaspersky Endpoint Security 能够更快地对新威胁作出响应，提高一些保护组件的性能，并减少误报风险。如果您正在参与卡巴斯基安全网络，KSN 服务为 Kaspersky Endpoint Security 提供有关已扫描网址的信誉的信息，以及有关已扫描文件的类别和信誉的信息。有关配置对 KSN 的访问的更多详细信息，请参阅 Kaspersky Security Center 帮助。

卡巴斯基安全网络的使用是自愿的。应用程序将在初始配置期间提示您使用 KSN。用户可以随时开始或停止加入 KSN。

有关在参与 KSN 期间生成的卡巴斯基统计信息的发送详情，以及有关此类信息的存储和销毁，请参阅卡巴斯基安全网络声明和卡巴斯基网站。含有卡巴斯基安全网络声明文本的 ksn_<语言 ID>.txt 文件包括在应用程序分发包中。

卡巴斯基信誉数据库的基础设施

Kaspersky Endpoint Security 支持以下用于使用卡巴斯基信誉数据库的基础设施解决方案：

- *卡巴斯基安全网络（KSN）*是大多数卡巴斯基应用程序使用的解决方案。KSN 参与者从卡巴斯基接收信息，并向卡巴斯基发送用户计算机上检测到的对象的信息，以便 卡巴斯基分析人员进行额外分析，并包括在卡巴斯基安全网络的信誉和统计数据库中。
- *卡巴斯基私有安全网络*是让运行 Kaspersky Endpoint Security 或其他卡巴斯基应用程序的计算机的用户获得卡巴斯基信誉数据库以及其他统计数据的访问权限的解决方案，无需从他们自己的计算机向卡巴斯基发送数据。KPSN 专为因以下任一原因无法参与卡巴斯基安全网络的公司客户所设计：
  - 本地工作站未连接 Internet。
  - 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。

启用和禁用卡巴斯基安全网络

默认情况下，Kaspersky Endpoint Security 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。

如何在管理控制台(MMC)中启用或禁用 KSN 使用

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **高级威胁防护** → **卡巴斯基安全网络**。
4. 使用**卡巴斯基安全网络**开关启用或禁用组件。

   如果您启用了 KSN，Kaspersky Endpoint Security 将显示卡巴斯基安全网络声明。如果您同意，请阅读并接受卡巴斯基安全网络 (KSN) 声明使用条款。
5. 如有必要，清空“**启用扩展 KSN 模式**”复选框。默认启用扩展 KSN 模式。
6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中启用或禁用 KSN 使用

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

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **卡巴斯基安全网络**。
5. 使用**使用卡巴斯基安全网络 (KSN) 已启用**开关启用或禁用组件。

   如果您启用了 KSN，Kaspersky Endpoint Security 将显示卡巴斯基安全网络声明。如果您同意，请阅读并接受卡巴斯基安全网络 (KSN) 声明使用条款。
6. 如果需要，关掉“**使用扩展 KSN 模式**”开关。默认启用扩展 KSN 模式。
7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在应用程序界面中启用或禁用 KSN 使用

1. 打开主应用程序窗口并单击 按钮。
2. 在应用程序设置窗口中，选择“**高级威胁防护**” → “**卡巴斯基安全网络**”。
3. 使用**卡巴斯基安全网络**开关启用或禁用组件。

   如果您启用了 KSN，Kaspersky Endpoint Security 将显示卡巴斯基安全网络声明。如果您同意，请阅读并接受卡巴斯基安全网络 (KSN) 声明使用条款。
4. 如果需要，关掉“**启用扩展 KSN 模式**”开关。默认启用扩展 KSN 模式。
5. 保存更改。

结果，如果启用 KSN，Kaspersky Endpoint Security 使用从卡巴斯基安全网络接收的文件、Web 资源的信誉信息。

卡巴斯基私有安全网络的限制

*卡巴斯基私有安全网络*是让运行 Kaspersky Endpoint Security 或其他卡巴斯基应用程序的计算机的用户获得卡巴斯基信誉数据库以及其他统计数据的访问权限的解决方案，无需从他们自己的计算机向卡巴斯基发送数据。卡巴斯基私有安全网络允许您使用自己的本地信誉数据库来检查对象（文件或网址）的信誉。添加到本地信誉数据库的对象的信誉比添加到 KSN/KPSN 的对象的信誉具有更高的优先级。例如，假设 Kaspersky Endpoint Security 正在扫描计算机并请求 KSN/KPSN 中文件的信誉。如果文件在本地信誉数据库中具有"*不信任*"的信誉，但在 KSN/KPSN 中具有"*受信任*"信誉，Kaspersky Endpoint Security 将检测到该文件为"*不信任*"，并将采取为检测到的威胁定义的操作。

但是，在某些情况下，Kaspersky Endpoint Security 可能不会请求 KSN/KPSN 中对象的信誉。如果是这种情况，Kaspersky Endpoint Security 将不会从 KPSN 的本地信誉数据库接收数据。Kaspersky Endpoint Security 可能不会请求 KSN/KPSN 中对象的信誉，原因如下：

- Kaspersky 应用程序正在使用离线信誉数据库。离线信誉数据库旨在优化 Kaspersky 应用程序运行期间的资源，并保护计算机上至关重要的对象。离线信誉数据库由 Kaspersky 专家根据卡巴斯基安全网络的数据创建。Kaspersky 应用程序使用特定应用程序的防病毒数据库更新脱机信誉数据库。如果脱机信誉数据库包含有关正在扫描的对象的信息，则应用程序不会从 KSN/KPSN 请求此对象的信誉。
- 扫描排除（受信任区域）在应用程序设置中配置。如果是这种情况，则应用程序不会考虑对象在本地信誉数据库中的信誉。
- 应用程序使用扫描优化技术，如 iSwift 或 iChecker，或正在缓存信誉请求到 KSN / KPSN。如果是这种情况，应用程序可能不会请求以前扫描的对象的信誉。
- 为了优化其工作负载，应用程序扫描特定格式和大小的文件。相关格式和尺寸限制列表由 Kaspersky 专家确定。该列表与应用程序的反病毒数据库一起更新。您还可以在应用程序界面中配置扫描优化设置，例如文件威胁保护组件。
- Light Agent 模式下的 Kaspersky Endpoint Security 通过 KSN 代理服务器与 KSN 服务器通信。不支持与 KSN 直接通信。

为保护组件启用和禁用云模式

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。

从卡巴斯基私人安全网络版本 3.0 开始，在使用卡巴斯基专属安全网络时，云模式功能可用。

如果应用程序正运行在 Light Agent 模式，云模式不可用。

如何在管理控制台(MMC)中启用或禁用保护组件的云模式

1. 在 Kaspersky Security Center 管理控制台树中，选择"**策略**"。
2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **高级威胁防护** → **卡巴斯基安全网络**。

4. 使用“**启用云模式**”复选框启用或禁用组件。

5. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中启用或禁用保护组件的云模式

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **常规设置** → **卡巴斯基安全网络**。

5. 使用**使用云模式**开关启用或禁用组件。

6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在应用程序界面中启用或禁用保护组件的云模式

1. 打开主应用程序窗口并单击 按钮。

2. 在应用程序设置窗口中，选择“**高级威胁防护**” → “**卡巴斯基安全网络**”。

3. 使用**启用云模式**开关启用或禁用组件。

4. 保存更改。

结果，Kaspersky Endpoint Security 在下一次更新中下载轻量版本或完整版本的反病毒数据库。

> 如果反病毒数据库的轻量级版本不可用，Kaspersky Endpoint Security 会自动切换到反病毒数据库的高级版本。

KSN 代理设置

受 Kaspersky Security Center 管理服务器管理的用户计算机可以直接或通过“KSN Proxy”服务与 KSN 交互。

> 如果应用程序正运行在 Light Agent 模式，不支持与 KSN 直接通信。Kaspersky Endpoint Security 通过 KSN 代理服务器与 KSN 服务器通信。

KSN Proxy服务提供以下功能：

- 用户计算机可查询 KSN 并将信息提交给 KSN，甚至无需访问互联网即可实现。
- KSN Proxy服务会缓存已处理的数据，从而降低外部网络通信信道的负载，并提高用户计算机所请求信息的接收速度。

默认情况下，在启用 KSN 并接受 KSN 声明后，应用程序使用代理服务器连接到卡巴斯基安全网络。应用程序使用的代理服务器是通过 TCP 端口 13111 的 Kaspersky Security Center 管理服务器。因此，如果 KSN 代理不可用，则需要验证以下内容：

- `ksnproxy` 服务正在管理服务器上运行。
- 计算机上的防火墙未阻止端口 13111。

您可以按如下方式配置 KSN Proxy的使用：启用或禁用 KSN Proxy，并配置连接的端口。为此，您需要打开管理服务器属性。有关"KSN Proxy"配置的详细信息，请参阅 Kaspersky Security Center 帮助。您还可以在 Kaspersky Endpoint Security 策略中为单个计算机启用或禁用 KSN Proxy。

如何在管理控制台(MMC)中启用或禁用 KSN 代理

1. 在 Kaspersky Security Center 管理控制台树中，选择"**策略**"。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **高级威胁防护** → **卡巴斯基安全网络**。
4. 在"**KSN 代理设置**"块，使用"**使用管理服务器作为 KSN 代理服务器**"复选框启用或禁用 KSN 代理。
5. 如有必要，选中"**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**"复选框。

   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）。
6. 保存更改。

如何在 Web 控制台中启用或禁用 KSN 代理

1. 在 Web Console 的主窗口中，选择"**资产管理**" → "**策略**"。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **卡巴斯基安全网络**。
5. 使用"**使用管理服务器作为 KSN 代理服务器**"复选框启用或禁用"KSN Proxy"。
6. 如有必要，选中"**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**"复选框。

   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）。默认下，复选框被清除。
7. 要将此策略应用到计算机，请关闭 🔒 挂锁图标并保存更改。

KSN Proxy地址与管理服务器地址匹配。更改管理服务器域名时，需要手动更新 KSN Proxy地址。

要配置 KSN 代理地址，请执行以下操作：

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择"**高级**" → "**远程安装**" → "**安装包**"文件夹。

3. 在“**安装包**”文件夹的上下文菜单中，选择“**属性**”。

4. 在所打开窗口的“**常规**”选项卡，指定 KSN 代理服务器的新地址。

5. 保存更改。

在卡巴斯基安全网络中检查文件信誉

如果您怀疑某个文件的安全性，可以在卡巴斯基安全网络中检查其信誉。

如果您已接受卡巴斯基安全网络声明的条款，则可以检查文件的信誉。

若要在卡巴斯基安全网络中检查文件信誉：

打开文件上下文菜单，然后选择“**查看在 KSN 中的信誉**”选项（请参见下图）。

文件上下文菜单

Kaspersky Endpoint Security 显示文件信誉：

受信任(卡巴斯基安全网络)。如果满足以下一个或多个条件，则应用程序认为文件受信任：

- 该文件由受信任的供应商进行数字签名；
- 该文件在卡巴斯基安全网络中享有可信声誉；
- 用户已将该文件放置在“受信任”组中。

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。虽然这些应用程序并不具备任何恶意功能，但它们可被入侵者利用。有关可被犯罪分子用来破坏计算机或用户个人数据的合法软件的详细信息，请访问 卡巴斯基 IT 百科全书网站。您可以将这些应用程序添加到受信任列表。

不受信任(卡巴斯基安全网络)。造成威胁的病毒或其他应用程序。

未知(卡巴斯基安全网络)。卡巴斯基安全网络不包含文件的任何信息。您可以使用反病毒数据库扫描文件（上下文菜单中的“**扫描病毒**”选项）。

Kaspersky Endpoint Security 显示用于确定文件信誉的 KSN 解决方案：*卡巴斯基安全网络* 或 *卡巴斯基私人安全网络*。

Kaspersky Endpoint Security 还会显示有关文件的其他信息（请参见下图）。

卡巴斯基安全网络中的文件信誉

加密连接扫描

安装后，Kaspersky Endpoint Security 会将 Kaspersky 证书添加到受信任证书的系统存储中（Windows 证书存储）。Kaspersky Endpoint Security 使用该证书扫描加密连接。Kaspersky Endpoint Security 还包括使用 Firefox 和 Thunderbird 中的受信任证书系统存储来扫描这些应用程序的流量。

Web 控制、邮件威胁防护、Web 威胁防护、行为检测和漏洞利用防御组件可以解密和扫描通过使用以下协议建立的加密连接传输的网络流量：

- SSL 3.0。
- TLS 1.0、TLS 1.1、TLS 1.2、TLS 1.3。

启用加密连接扫描

默认情况下，Kaspersky Endpoint Security 并不总是扫描加密连接，而是仅在保护组件请求时才扫描。

如何在管理控制台 (MMC) 中启用加密连接扫描

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**策略**”。
3. 选择必要的策略并双击以打开策略属性。
4. 在策略窗口中，选择 **常规设置** → **网络设置**。

5. 在“**加密连接扫描**”块中，选择加密连接扫描模式：

- “**扫描加密连接**”。Kaspersky Endpoint Security 将无法访问地址以 `https://` 开头的网站的内容。
- “**根据保护组件的请求扫描加密连接**”。Kaspersky Endpoint Security 只有在得到文件威胁防护、Web 威胁防护和 Web 控制组件的请求时才扫描加密流量。
- “**始终扫描加密连接**”。即使保护组件被禁用，Kaspersky Endpoint Security 也将扫描加密网络流量。

> Kaspersky Endpoint Security 不扫描由禁用了流量扫描的受信任应用程序建立的加密连接。Kaspersky Endpoint Security 不扫描预定义的受信任网站的加密连接。预定义的受信任网站列表由 Kaspersky 专家创建。该列表与应用程序的反病毒数据库一起更新。您仅可以在 Kaspersky Endpoint Security 界面查看预定义的受信任网站列表。您无法在 Kaspersky Security Center 控制台查看列表。

6. 如有必要，添加扫描排除项：受信任地址和应用程序。
7. 配置用于扫描加密连接的设置（参见下表）。
8. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中启用加密连接扫描

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”选项卡。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **网络设置**。
5. 在“**加密连接扫描**”下，开启“**加密连接扫描已启用**”开关。
   如果关闭此切换开关，Kaspersky Endpoint Security 将无法访问地址以 `https://` 开头的网站的内容。
6. 点击“**设置**”并选择加密连接扫描模式：

- “**根据保护组件的请求扫描加密连接**”。Kaspersky Endpoint Security 只有在得到文件威胁防护、Web 威胁防护和 Web 控制组件的请求时才扫描加密流量。
- “**始终扫描加密连接**”。即使保护组件被禁用，Kaspersky Endpoint Security 也将扫描加密网络流量。

> Kaspersky Endpoint Security 不扫描由禁用了流量扫描的受信任应用程序建立的加密连接。Kaspersky Endpoint Security 不扫描预定义的受信任网站的加密连接。预定义的受信任网站列表由 Kaspersky 专家创建。该列表与应用程序的反病毒数据库一起更新。您仅可以在 Kaspersky Endpoint Security 界面查看预定义的受信任网站列表。您无法在 Kaspersky Security Center 控制台查看列表。

7. 如有必要，添加扫描排除项：受信任地址和应用程序。
8. 配置用于扫描加密连接的设置（参见下表）。
9. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在应用程序界面中启用加密连接扫描

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**常规设置**” → “**网络设置**”。

加密连接扫描设置

3. 在“**加密连接扫描**”块中，选择加密连接扫描模式：

- “**不扫描加密连接**”。Kaspersky Endpoint Security 将无法访问地址以 `https://` 开头的网站的内容。
- “**根据保护组件的请求扫描加密连接**”。Kaspersky Endpoint Security 只有在得到文件威胁防护、Web 威胁防护和 Web 控制组件的请求时才扫描加密流量。
- “**始终扫描加密连接**”。即使保护组件被禁用，Kaspersky Endpoint Security 也将扫描加密网络流量。

> Kaspersky Endpoint Security 不扫描由禁用了流量扫描的受信任应用程序建立的加密连接。Kaspersky Endpoint Security 不扫描预定义的受信任网站的加密连接。预定义的受信任网站列表由 Kaspersky 专家创建。该列表与应用程序的反病毒数据库一起更新。您仅可以在 Kaspersky Endpoint Security 界面查看预定义的受信任网站列表。您无法在 Kaspersky Security Center 控制台查看列表。

4. 如有必要，添加扫描排除项：受信任地址和应用程序。

5. 配置用于扫描加密连接的设置（参见下表）。

扫描加密连接的附加设置

6. 保存更改。

加密连接扫描设置

参数	描述
受信任根证书	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。要添加到系统证书存储，您可以使用 Active Directory 组策略。
访问带有不受信任证书的域	• "**允许**"。当访问具有不受信任证书的域时，Kaspersky Endpoint Security 将允许网络连接。 在浏览器中打开具有未受信任证书的域时，Kaspersky Endpoint Security 会显示一个 HTML 页面，其中显示警告和不建议访问该域的原因。用户可以单击 HTML 警告页面中的链接来获取对所请求 Web 资源的访问权限。 如果第三方应用程序或服务与具有不受信任的证书的域建立连接，Kaspersky Endpoint Security 将创建自己的证书来扫描流量。新证书具有"*不信任组*"状态。这对于警告第三方应用程序不受信任的连接是必要的，因为在这种情况下无法显示 HTML 页面，并且连接可以在后台模式下建立。 • "**阻止**"。当访问具有不受信任证书的域时，Kaspersky Endpoint Security 将阻止网络连接。在浏览器中打开具有未受信任证书的域时，Kaspersky Endpoint Security 会显示一个 HTML 页面，其中显示阻止该域的原因。
访问带有加密连接扫描错误的域	• "**阻止**"。如果发生加密连接扫描错误，Kaspersky Endpoint Security 会阻止网络连接。 • "**允许并添加域到排除项**"。在发生加密连接扫描错误时，Kaspersky Endpoint Security 将导致错误的域添加到具有扫描错误的域列表中，并且在访问此域时不监控加密网络流量。您只能在应用程序的本地界面中查看具有加密连接扫描错误的域列表。要清除列表内容，您需要选择"**阻止**"。Kaspersky Endpoint Security 也为加密连接扫描错误生成事件。
阻止 SSL 2.0 连接	如果选中该复选框，应用程序将监控并阻止通过 SSL 2.0 协议建立的网络连接。 如果清除该复选框，应用程序将不会阻止通过 SSL 2.0 协议建立的网络连接。但是，应用程序不会监控通过该协议的网络流量。
阻止 SSL 3.0 连接	如果选中该复选框，应用程序将阻止通过 SSL 3.0 协议建立的网络连接。 如果清除该复选框，应用程序将不会阻止通过 SSL 3.0 协议建立的网络连接。应用程序监控通过该协议的网络流量。应用程序的所有组件均不受限制地运行。
阻止 TLS 1.0 连接	如果选中该复选框，应用程序将阻止通过 TLS 1.0 协议建立的网络连接。 如果清除该复选框，应用程序将不会阻止通过 TLS 1.0 协议建立的网络连接。应用程序监控通过该协议的网络流量。应用程序的所有组件均不受限制地运行。

参数	描述
解密与使用 EV 证书的网站之间的加密连接	EV 证书（Extended Validation Certificate）确认网站的真实性并增强连接的安全性。浏览器在地址栏中使用锁定图标来指示网站具有 EV 证书。浏览器还可能将地址栏的全部或部分填充绿色。 如果选中该复选框，应用程序将解密并监控与使用 EV 证书的网站的加密连接。 如果清除该复选框，应用程序无权访问 HTTPS 流量的内容。为此，应用程序仅基于网址（例如 `https://bing.com`）监控 HTTPS 流量。 如果您第一次打开具有 EV 证书的网站，则无论是否选中该复选框，加密连接都将被解密。

安装受信任根证书

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。要添加到系统证书存储，您可以使用 Active Directory 组策略。

更改受信任根证书列表可能受到父策略属性的阻止。要更改列表，您需要允许更改以下设置：Web Console 中的受信任区域（“挂锁”必须处于解锁状态）。

管理控制台(MMC) 和 Web Console 中受信任区域的分组方式不同。同样，防止受信任区域参数更改的方式也不同（“挂锁”不同）。我们建议仅使用 Web Console 来管理应用程序。如果在不同的控制台中配置受信任区域，管理插件可能会将“挂锁”重置为其默认状态。

如何在管理控制台(MMC)中安装受信任根证书

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **网络设置**。
4. 在“**受信任根证书**”块中单击“**添加**”按钮。
5. 这打开了一个窗户；在该窗口中，选择一个受信任的根证书。

   Kaspersky Endpoint Security 支持带有 PEM、DER 和 CRT 扩展名的证书。
6. 保存更改。

如何在 Web 控制台和云控制台中安装受信任根证书

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

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。

4. 选择 **常规设置** → **网络设置**。

5. 单击**受信任根证书**链接。

6. 这将打开一个窗口；在该窗口中，单击“**添加**”并选择一个受信任的根证书。
   Kaspersky Endpoint Security 支持带有 PEM、DER 和 CRT 扩展名的证书。

7. 保存更改。

如何在应用程序界面中安装受信任根证书

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**常规设置**” → “**网络设置**”。

3. 在“**加密连接扫描**”块中单击“**显示证书**”按钮。

4. 这将打开一个窗口；在该窗口中，单击“**添加**”并选择一个受信任的根证书。
   Kaspersky Endpoint Security 支持带有 PEM、DER 和 CRT 扩展名的证书。

5. 保存更改。

因此，在扫描流量时，除了系统证书存储之外，Kaspersky Endpoint Security 还使用自己的证书存储。

扫描带有不受信任证书的加密连接

安装后，Kaspersky Endpoint Security 会将 Kaspersky 证书添加到受信任证书的系统存储中（Windows 证书存储）。Kaspersky Endpoint Security 使用该证书扫描加密连接。在访问具有不受信任证书的域时，您可以允许或拒绝用户访问域（参见以下说明）。

如果您已允许用户访问具有不受信任证书的域，Kaspersky Endpoint Security 执行以下操作：

- 当在*浏览器*中访问具有不受信任证书的域时，Kaspersky Endpoint Security 使用卡巴斯基证书扫描流量。Kaspersky Endpoint Security 会显示一个 HTML 页面，其中包含警告和有关不建议访问相关域的原因的信息（请参见下图）。用户可以单击 HTML 警告页面中的链接来获取对所请求 Web 资源的访问权限。单击此链接后，在随后一个小时内访问同一域中的其他资源时，Kaspersky Endpoint Security 不会显示关于不受信任证书的警告。Kaspersky Endpoint Security 还会生成一个关于使用不受信任的证书建立加密连接的事件。

  > 在某些情况下，Kaspersky Endpoint Security 从技术上无法在浏览器中显示带有警告的 HTML 页面（见下图）。例如，如果 Web 资源使用过时版本的网络协议和非标准端口。在这些情况下，Kaspersky Endpoint Security 会阻止访问该域，并且浏览器将显示标准 `ERR_CONNECTION_RESET` 窗户。要访问 Web 资源，您可以将域添加到排除项或使用受信任的证书。

- 如果*第三方应用程序或服务*与具有不受信任的证书的域建立连接，Kaspersky Endpoint Security 将创建自己的证书来扫描流量。新证书具有*不受信任*状态。这对于警告第三方应用程序不受信任的连接是必要的，因为在这种情况下无法显示 HTML 页面，并且连接可以在后台模式下建立。因此，如果第三方应用程序具有内置证书验证工具，连接可能被终止。在这种情况下，您必须与域的所有者联系，并建立受信任的连接。如果无法建立受信任连接，您可以将该第三方应用程序添加到受信任应用程序列表中。Kaspersky Endpoint Security 还会生成一个关于使用不受信任的证书建立加密连接的事件。

如果在管理控制台(MMC)配置对具有不受信任证书的加密连接的扫描

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **网络设置**。
4. 在“**加密连接扫描**”块中单击“**高级设置**”按钮。
5. 在打开的窗口中，选择访问具有不受信任证书的域时的应用程序运行模式：“**允许**”或者“**阻止**”。
6. 保存更改。

如果在 Web 控制台配置对具有不受信任证书的加密连接的扫描

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **网络设置**。
5. 在“**加密连接扫描**”区域，单击“**设置**”链接。
6. 在打开的窗口中，选择访问具有不受信任证书的域时的应用程序运行模式：“**允许连接**”或者“**阻止连接**”。
7. 保存更改。

如果在应用程序界面配置对具有不受信任证书的加密连接的扫描

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**网络设置**”。
3. 在“**加密连接扫描**”块，选择访问具有不受信任证书的域时的应用程序运行模式：“**允许**”或者“**阻止**”。
4. 保存更改。

在访问具有不受信任证书的域时发出警告

将卡巴斯基证书添加到自己的证书存储

浏览器和邮件客户端使用证书来验证 Web 资源的安全性和真实性。该证书还提供 Web 资源和用户之间的数据加密。大多数浏览器和邮件客户端使用受信任的证书存储（Windows 证书存储）。例如，Google Chrome。一些浏览器和邮件客户端默认使用自己的证书存储，而不是 Windows 证书存储。例如，Firefox 和 Thunderbird。

安装后，Kaspersky Endpoint Security 会将 Kaspersky 证书添加到受信任证书的系统存储中（Windows 证书存储）。如果您的组织中部署了 Kaspersky Security Center，并且将策略应用于计算机，则 Kaspersky Endpoint Security 会自动启用 Firefox 和 Thunderbird 中的 Windows 证书存储来扫描这些应用程序的流量。如果策略未应用于计算机，您可以选择浏览器和邮件客户端将使用的证书存储。如果您选择了自己的证书存储，请手动将卡巴斯基证书添加到存储中。这将有助于避免在处理 HTTPS 流量时出错。

要扫描 Mozilla Firefox 浏览器和 Thunderbird 邮件客户端中的流量，您必须"启用加密连接扫描"。如果"加密连接扫描"被禁用，应用程序不扫描 Mozilla Firefox 浏览器和 Thunderbird 邮件客户端中的流量。还应启用加密连接扫描来扫描 MyOffice Mail 和 R7-Office Organizer 邮件客户端中的流量。

将证书添加到浏览器或邮件代理自己的证书存储之前，请从 Windows 控制面板（Internet 属性）导出卡巴斯基证书。您可以在以下位置了解有关将证书添加到存储的更多信息：Mozilla 技术支持网站。

只能在应用程序的本地接口中选择证书存储。

要在浏览器和邮件客户端中选择用于扫描加密连接的证书存储：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择"**常规设置**" → "**网络设置**"。
3. 在"**加密连接扫描**"块中，选中"**要使用自己的证书存储扫描应用程序中的加密连接，请使用**"复选框。
4. 选择一个证书存储。
   - "**Windows 证书存储(推荐)**"。在 Kaspersky Endpoint Security 安装期间，Kaspersky 根证书被添加到该存储。
   - "**自己的证书存储**"。Mozilla Firefox 和 Thunderbird 使用它们自己的证书存储。如果 Mozilla 证书存储被选择，您需要通过浏览器属性手动添加 Kaspersky 根证书到该存储。

     MyOffice Mail 和 R7-Office Organizer 邮件客户端也使用自己的证书存储。
5. 保存更改。

从扫描中排除加密连接

大多数网络资源使用加密连接。Kaspersky 专家建议您启用"加密连接扫描"。如果加密连接扫描干扰与工作相关的活动，您可以将网站添加到被称为"*受信任地址*"的排除项中。此种情况下，在 Web 威胁防护、邮件威胁防护和 Web 控制组件正常运行的情况下，Kaspersky Endpoint Security 不扫描受信任网址的 HTTPS 流量。

如果受信任应用程序使用加密连接，您可以对此应用程序禁用加密连接扫描。例如，您可以对使用自己的证书执行双因素身份验证的云存储应用程序禁用加密连接扫描。

> 更改受信任地址列表可能受到父策略属性的阻止。要更改列表，您需要允许更改以下设置：Web Console 中的受信任区域（“挂锁”必须处于解锁状态）。

> 管理控制台(MMC) 和 Web Console 中受信任区域的分组方式不同。同样，防止受信任区域参数更改的方式也不同（“挂锁”不同）。我们建议仅使用 Web Console 来管理应用程序。如果在不同的控制台中配置受信任区域，管理插件可能会将“挂锁”重置为其默认状态。

如何从管理控制台 (MMC) 中的加密连接扫描中排除网址

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **网络设置**。
4. 在“**加密连接扫描**”块中单击“**配置受信任地址**”按钮。
5. 单击“**添加**”。
6. 如果您不希望 Kaspersky Endpoint Security 扫描在访问该域时建立的加密连接，请输入域名或 IP 地址。

   Kaspersky Endpoint Security 支持使用 `*` 字符在域名中输入掩码。

   > Kaspersky Endpoint Security 不支持 IP 地址的 `*` 符号。您可以使用子网掩码选择一个 IP 地址范围（例如，198.51.100.0/24）。

   例如：

   - `domain.com` – 该记录包括以下地址：`https://domain.com`、`https://www.domain.com`、`https://domain.com/page123`。该记录不包括子域（例如，`subdomain.domain.com`）。
   - `subdomain.domain.com` – 该记录包括以下地址：`https://subdomain.domain.com`、`https://subdomain.domain.com/page123`。该记录不包括 `domain.com` 域。
   - `*.domain.com` – 该记录包括以下地址：`https://movies.domain.com`、`https://images.domain.com/page123`。该记录不包括 `domain.com` 域。
7. 保存更改。

如何从 Web 控制台和云控制台中的加密连接扫描中排除网址

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

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **网络设置**。

5. 在“**加密连接扫描**”块中单击“**受信任域**”按钮。

6. 单击“**添加**”。

7. 如果您不希望 Kaspersky Endpoint Security 扫描在访问该域时建立的加密连接，请输入域名或 IP 地址。

   Kaspersky Endpoint Security 支持使用 `*` 字符在域名中输入掩码。

   > Kaspersky Endpoint Security 不支持 IP 地址的 `*` 符号。您可以使用子网掩码选择一个 IP 地址范围（例如，198.51.100.0/24）。

   例如：

   - `domain.com` – 该记录包括以下地址：`https://domain.com`、`https://www.domain.com`、`https://domain.com/page123`。该记录不包括子域（例如，`subdomain.domain.com`）。
   - `subdomain.domain.com` – 该记录包括以下地址：`https://subdomain.domain.com`、`https://subdomain.domain.com/page123`。该记录不包括 `domain.com` 域。
   - `*.domain.com` – 该记录包括以下地址：`https://movies.domain.com`、`https://images.domain.com/page123`。该记录不包括 `domain.com` 域。

8. 保存更改。

如何从应用程序界面中的加密连接扫描中排除网址

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**网络设置**”。

应用程序网络设置

3. 在“**加密连接扫描**”块中单击“**配置受信任地址**”按钮。
4. 单击“**添加**”。
5. 如果您不希望 Kaspersky Endpoint Security 扫描在访问该域时建立的加密连接，请输入域名或 IP 地址。Kaspersky Endpoint Security 支持使用 `*` 字符在域名中输入掩码。

> Kaspersky Endpoint Security 不支持 IP 地址的 `*` 符号。您可以使用子网掩码选择一个 IP 地址范围（例如，198.51.100.0/24）。

例如：

- `domain.com` – 该记录包括以下地址：`https://domain.com`、`https://www.domain.com`、`https://domain.com/page123`。该记录不包括子域（例如，`subdomain.domain.com`）。
- `subdomain.domain.com` – 该记录包括以下地址：`https://subdomain.domain.com`、`https://subdomain.domain.com/page123`。该记录不包括 `domain.com` 域。
- `*.domain.com` – 该记录包括以下地址：`https://movies.domain.com`、`https://images.domain.com/page123`。该记录不包括 `domain.com` 域。

6. 保存更改。

默认情况下，当发生错误时，Kaspersky Endpoint Security 将不扫描加密连接，并将该网站添加到专门设置的“*有扫描错误的域*”列表中。Kaspersky Endpoint Security 会为每个用户编制单独的列表，并且不会将数据发送到 Kaspersky Security Center。您可以启用当发生扫描错误时阻止连接。您只能在应用程序的本地界面中查看具有加密连接扫描错误的域列表。

要查看有扫描错误的域列表：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**网络设置**”。
3. 在“**加密连接扫描**”块中单击“**有扫描错误的域**”按钮。

   将打开有扫描错误的域列表。要重置该列表，请在策略中启用当发生扫描错误时阻止连接，应用策略，然后将参数重置为其初始值，并再次应用策略。

Kaspersky 专家会创建“*全局排除项*”列表。不管应用程序设置如何，Kaspersky Endpoint Security 始终不会对该列表中的受信任网站进行检查。

要查看加密流量扫描的全局排除项：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**网络设置**”。
3. 在“**加密连接扫描**”块中，单击“受信任网站列表”链接。

   这打开由 Kaspersky 专家编辑的网站列表。Kaspersky Endpoint Security 不扫描列表中网站的受保护连接。当更新 Kaspersky Endpoint Security 数据库和模块时，该列表可能也更新。

擦除数据

Kaspersky Endpoint Security 允许您使用任务来远程删除用户计算机中的数据。

Kaspersky Endpoint Security 删除数据的方式如下：

- 在静默模式下；
- 在硬盘驱动器和可移动驱动器上；
- 对于计算机上的所有用户账户。

即使授权许可过期后，Kaspersky Endpoint Security 也会执行“*擦除数据*”任务，无论使用哪种授权许可类型。

“数据擦除”模式

通过该任务可在以下模式中删除数据：

- 立即删除数据。

  例如，您可以在此模式下删除过期数据以释放磁盘空间。

- 延迟删除数据。

  例如，此模式可用于保护笔记本电脑上的数据，以防其丢失或被盗。您可以配置成当笔记本电脑超出公司网络边界并且长时间未与 Kaspersky Security Center 同步时自动删除数据。

无法在任务属性中设置删除数据的计划。您只能在手动启动任务后立即删除数据，或者配置延迟的数据删除（如果未与 Kaspersky Security Center 连接）。

限制

数据擦除具有以下限制：

- 只有 Kaspersky Security Center 管理员可以管理“*擦除数据*”任务。您无法在 Kaspersky Endpoint Security 的本地界面中配置或启动任务。
- 对于 NTFS 文件系统，Kaspersky Endpoint Security 仅删除主数据流的名称。交换数据流名称不能删除。
- 删除符号链接文件时，Kaspersky Endpoint Security 还会删除在符号链接中指定了路径的文件。

创建擦除数据任务

要删除用户计算机上的数据：

1. 在 Web Console 的主窗口中，选择“**任务**”。

   任务列表打开。

2. 单击“**添加**”。

   “任务向导”将启动。

3. 配置任务设置：

   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Endpoint Security for Windows 14.2.0**”。

   b. 在“**任务类型**”下拉列表中，选择“**擦除数据**”。

   c. 在“**任务名称**”字段中，输入简要说明，例如，“*擦除数据（反盗窃）*”。

   d. 在“**要对其分配任务的设备**”块，选择任务范围。

4. 按照所选任务范围选项选择设备。转到下一步。

   如果将新计算机添加到任务范围内的管理组，则只有在添加新计算机后的 5 分钟内完成任务，才会在新计算机上运行立即删除数据任务。

5. 退出向导。

   在任务列表中将显示一个新任务。

6. 单击 Kaspersky Endpoint Security 的“**擦除数据**”任务。

   任务属性窗口将打开。

7. 选择**应用程序设置**选项卡。

8. 选择数据删除方法：

   - “**通过操作系统删除**”。Kaspersky Endpoint Security 使用操作系统资源删除文件，而不将文件发送到回收站。
   - “**完全删除，无法恢复**”。Kaspersky Endpoint Security 使用随机数据覆盖文件。删除数据后，几乎不可能恢复数据。

9. 如果要延迟删除数据，请选中“**与 Kaspersky Security Center 无连接超过以下时间时自动擦除数据 N 天**”复选框。定义天数。

   每次在定义的时间段内与 Kaspersky Security Center 无连接时，将执行延迟删除数据任务。

   配置延迟数据删除时，请记住员工可能有不同的工作时间表。还要考虑离线用户的工作计划。有关使用离线计算机以及与漫游用户一起工作的详细信息，请参阅 Kaspersky Security Center 帮助。

   如果计算机关闭并且连接中断的时间超过配置的持续时间，则计算机启动后，Kaspersky Endpoint Security 不会立即删除数据。应用程序等待与 Kaspersky Security Center 同步一小时。这对于防止用户在外出度假前关闭计算机时未经授权删除其计算机上的数据是必要的。

   如果清除该复选框，则在与 Kaspersky Security Center 同步后将立即执行该任务。

10. 创建要删除的对象列表：

- “**文件夹**”。Kaspersky Endpoint Security 会删除文件夹及其子文件夹中的所有文件。输入文件夹路径时，Kaspersky Endpoint Security 不支持掩码和环境变量。
- “**按扩展名选择文件**”。Kaspersky Endpoint Security 将搜索所有计算机驱动器（包括可移动驱动器）中具有指定扩展名的文件。使用“`;`”或“`,`”字符可指定多个扩展名。
- “**预定义范围**”。Kaspersky Endpoint Security 将从以下区域删除文件：
  - “**文档**”。操作系统的“*文档*”文件夹及其子文件夹中的文件。
  - “**Cookie**”。浏览器在其中保存用户访问过的网站的数据（如用户授权数据）的文件。
  - “**桌面**”。操作系统的“*桌面*”文件夹及其子文件夹中的文件。
  - “**临时 Internet Explorer 文件**”。与 Internet Explorer 操作有关的临时文件，如网页副本、图像和媒体文件。
  - “**临时文件**”。与计算机上安装的应用程序的操作有关的临时文件。例如，Microsoft Office 应用程序会创建包含文档备份副本的临时文件。
  - “**Outlook 文件**”。与 Outlook 邮件客户端操作有关的文件：数据文件 (PST)、离线数据文件 (OST)、离线地址簿文件 (OAB) 和个人地址簿文件 (PAB)。
  - “**用户配置文件**”。存储本地用户账户的操作系统设置的文件和文件夹集。

您可以在每个选项卡上创建要删除的对象列表。Kaspersky Endpoint Security 将创建一个综合列表，并在任务完成后删除此列表中的文件。

> 您无法删除 Kaspersky Endpoint Security 运行所需的文件。

11. 保存更改。

12. 选中该任务旁边的复选框。

13. 单击“**开始**”。

结果，将根据所选模式删除用户计算机上的数据：立即删除或无连接时删除。如果 Kaspersky Endpoint Security 无法删除文件，例如用户当前正在使用文件时，应用程序不会尝试再次删除该文件。要完成数据删除，请再次运行该任务。

计算机控制

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（请参见下图）。

要使用 Web 控制，您必须完成应用程序的初始配置：

- 对于 HTTPS 流量监控，启用加密连接扫描（默认情况下启用）。
- 选择 Kaspersky Endpoint Security 必须监控的端口（默认情况下，应用程序监控所有端口）。
- 选择您希望 Kaspersky Endpoint Security 监控其流量的应用程序。大多数浏览器已经存在于卡巴斯基推荐的应用程序列表中。如果列表中缺少您的浏览器，请手动添加。
- 我们建议将网页交互脚本注入到 Web 流量中（默认情况下，脚本注入是禁用的）。该脚本启用将 Web 控制事件注册到应用程序事件日期、OS 事件日志和报告。

管理对网站的访问的方法

“Web 控制”允许您使用以下方法配置对网站的访问：

- **网站类别**。网站按照卡巴斯基安全网络云服务、启发式分析和已知网站数据库（包含在应用程序数据库中）进行分类。例如，您可以限制用户对“*社交网络*”类别或其他类别的访问。
- **数据类型**。例如，您可以限制用户访问网站上的数据，并隐藏图像。Kaspersky Endpoint Security 根据文件格式确定数据类型，而不是基于其扩展名。

  Kaspersky Endpoint Security 不扫描压缩文件内的文件。例如，如果图像文件放在压缩文件中，Kaspersky Endpoint Security 会识别“*存档*”数据类型而不是“*图形*”。

- **单个地址**。您可以输入网址或使用掩码。

可以同时使用多种方法来管理对网站的访问。例如，您可以仅针对“*基于 Web 的邮件*”网站类别限制对“*Office 应用程序文件*”数据类型的访问。

网站访问规则

“Web 控制”通过使用*访问规则*管理用户对网站的访问。您可以为网站访问规则配置以下高级设置：

- 规则适用的用户。

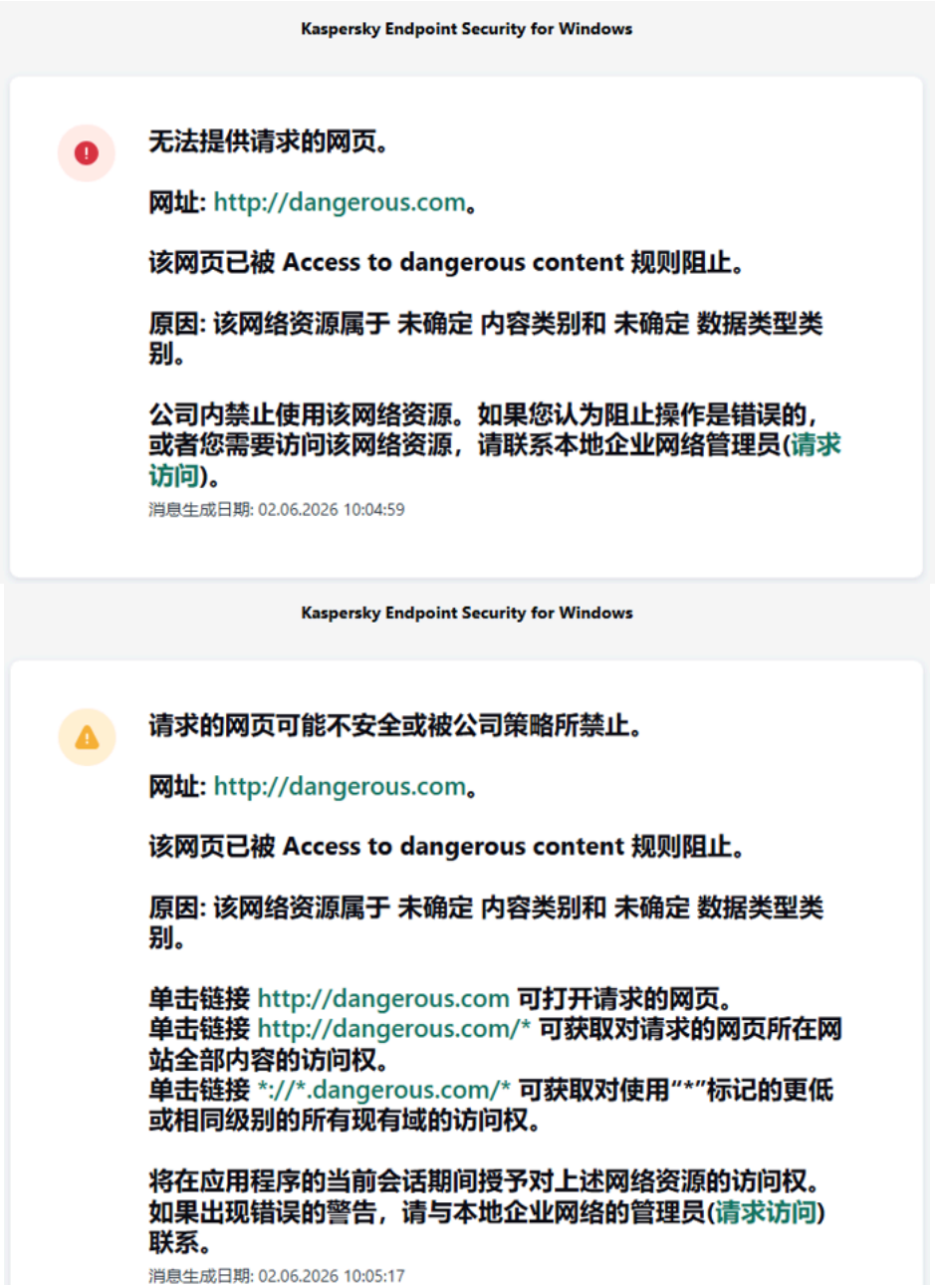
  例如，您可以限制公司内除 IT 部门以外的所有用户通过浏览器访问 Internet。

- 规则计划。

  例如，您可以限制只能在工作时间通过浏览器访问 Internet。

访问规则优先级

每条规则都有优先级。规则在列表中的位置越高，优先级越高。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。例如，Kaspersky Endpoint Security 可能将公司门户识别为社交网络。要限制对社交网络的访问并提供对公司 Web 门户的访问权限，请创建两条规则：一条针对“*社交网络*”网站类别的阻止规则和一条针对公司 Web 门户的允许规则。公司 Web 门户访问规则的优先级必须高于社交网络访问规则的优先级。



“Web 控制”消息

添加 Web 资源访问规则

*Web 资源访问规则*是 Kaspersky Endpoint Security 在用户访问 Web 资源时应用的一组过滤器和操作。访问规则可以包括规则计划。

不建议创建超过 1000 条的 Web 资源访问规则，因为这可能导致系统变得不稳定。

网页资源访问规则是用户在规则计划中指明的时间范围内访问规则中描述的网页资源时，Kaspersky Endpoint Security 执行的一组过滤和操作。通过过滤，您可以精确指定由 Web 控制组件控制其访问权限的网页资源池。

系统提供以下过滤：

- **按内容过滤**。Web 控制将按照内容和数据类型分类网页资源。对于内容和数据属于按这些类别定义的类型的网页资源，您可以控制用户对它们的访问权限。用户访问属于选定内容类别和/或数据类型类别的网页资源时，Kaspersky Endpoint Security 会执行规则中指定的操作。

- **按网页资源地址过滤**。您可以控制用户对所有网页资源地址或单个网页资源地址和/或网页资源地址组的访问权限。

  如果指定了按内容过滤和按网页资源地址过滤，而指定的网页资源地址和/或网页资源地址组属于选定的内容类别或数据类型类别，Kaspersky Endpoint Security 不会控制对选定内容类别和/或数据类型类别中所有网页资源的访问权限。相反，应用程序仅控制对指定网页资源地址和/或网页资源地址组的访问权限。

- **按用户和用户组的名称过滤**。您可以指定根据规则控制其对网页资源的访问的用户和/或用户组的名称。

- **规则计划**。您可以指定规则计划。规则计划确定了 Kaspersky Endpoint Security 监控对该规则涵盖的网络资源的访问的时间跨度。

安装 Kaspersky Endpoint Security 后，Web 控制组件的规则列表将不为空。"*默认规则*"是预设的。此规则应用于未被其他规则覆盖的任何 Web 资源，并允许或阻止所有用户访问这些 Web 资源。

每条规则都有优先级。规则在列表中的位置越高，优先级越高。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。例如，Kaspersky Endpoint Security 可能将公司门户识别为社交网络。要限制对社交网络的访问并提供对公司 Web 门户的访问权限，请创建两条规则：一条针对"*社交网络*"网站类别的阻止规则和一条针对公司 Web 门户的允许规则。公司 Web 门户访问规则的优先级必须高于社交网络访问规则的优先级。

如何在管理控制台 (MMC) 中添加 Web 资源访问规则

1. 在 Kaspersky Security Center 管理控制台树中，选择"**策略**"。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **安全控制** → **Web 控制**。

4. 选择**Web 控制**复选框。

5. 在"**Web 控制设置**"块中单击"**添加**"按钮。

   "**网络资源访问规则**"窗口将打开。

6. 配置 Web 资源访问规则（请参阅下表）。

7. 如果您希望 Web 控制在应用策略后立即终止与禁止的 Web 资源的连接，请选择“**应用规则后终止活动用户浏览器会话**”复选框。

   Web 控制仅允许在 Web 浏览器中立即断开 Web 资源。对于其他应用程序，Web 控制仅限制新连接。

   如果清除该复选框，Web 控制将仅限制与禁止的 Web 资源的新连接。Web 控制不会终止活动连接。

8. 保存更改。

如何在 Web Console 和云控制台中添加 Web 资源访问规则

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **安全控制** → **Web 控制**。
5. 开启 **Web 控制已启用**切换开关。
6. 在“**规则列表**”块中单击“**添加**”按钮。
7. 配置 Web 资源访问规则（请参阅下表）。
8. 如果您希望 Web 控制在应用策略后立即终止与禁止的 Web 资源的连接，请选择“**应用规则后终止活动用户浏览器会话**”复选框。

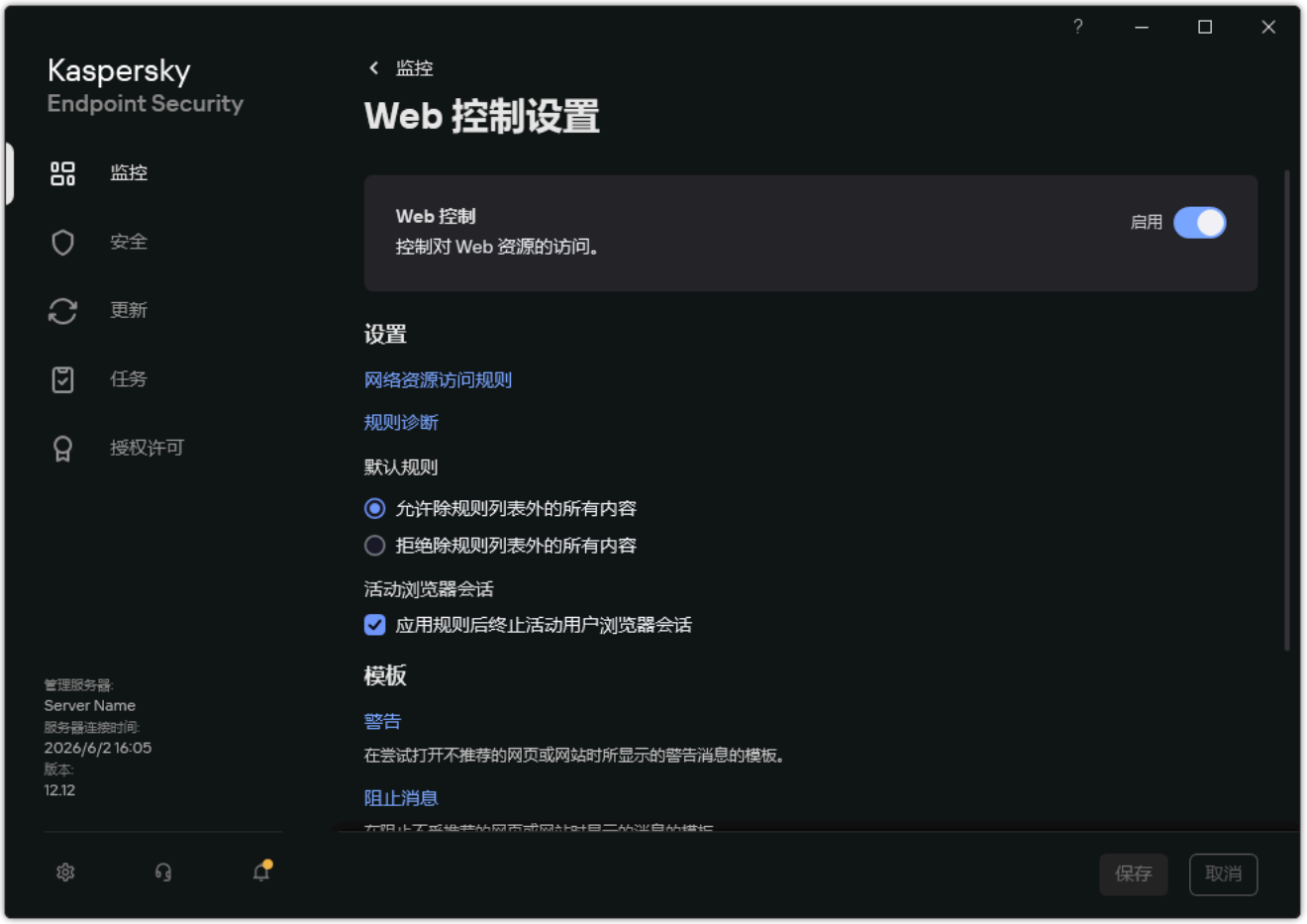
   Web 控制仅允许在 Web 浏览器中立即断开 Web 资源。对于其他应用程序，Web 控制仅限制新连接。

   如果清除该复选框，Web 控制将仅限制与禁止的 Web 资源的新连接。Web 控制不会终止活动连接。

9. 保存更改。

如何在应用程序界面中添加 Web 资源访问规则

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**安全控制**” → “**Web 控制**”。



Web 控制设置

3. 开启 **Web 控制**切换开关。
4. 在“**设置**”块中单击“**网络资源访问规则**”按钮。
5. 在打开的窗口中，单击“**添加**”按钮。

   “**网络资源访问规则**”窗口将打开。
6. 配置 Web 资源访问规则（请参阅下表）。
7. 如果您希望 Web 控制在应用策略后立即终止与禁止的 Web 资源的连接，请选择“**应用规则后终止活动用户浏览器会话**”复选框。

   > Web 控制仅允许在 Web 浏览器中立即断开 Web 资源。对于其他应用程序，Web 控制仅限制新连接。

   如果清除该复选框，Web 控制将仅限制与禁止的 Web 资源的新连接。Web 控制不会终止活动连接。
8. 保存更改。

结果，新的 Web 控制规则被添加到列表中。如有必要，请更改 Web 控制规则的优先级。您也可以随时使用切换开关禁用 Web 资源访问规则，而无需将其从列表中删除。

参数	描述
规则名称	Web 控制规则名称。
状态	• "**启用**"。 • "**禁用**"。 您可以随时使用开关禁用 Web 资源访问规则。
操作	• "**允许**"。Web 控制允许访问与规则参数匹配的 Web 资源。 • "**阻止**"。Web 控制阻止访问与规则参数匹配的 Web 资源，并显示拒绝访问网站的消息。 • "**警告**"。当用户试图访问与规则匹配的 Web 资源时，Web 控制会显示一条警告，表示不建议访问该 Web 资源。通过警告消息链接，用户可获取对所请求的网页资源的访问权限。
过滤器内容	• "**根据内容类别**"。您可以通过类别（例如，"*社交网络*"类别）控制用户对 Web 资源的访问。 • "**根据数据类型**"。您可以根据其发布的数据的数据类型（例如，*图形*）控制用户对 Web 资源的访问。
地址	• "**应用于所有地址**"。Web 控制将不根据地址过滤 Web 资源。 • "**应用于个别地址**"。Web 控制将仅过滤列表中的 Web 资源地址。您可以输入网址或使用掩码。您也可以从 TXT 文件导出 Web 资源地址列表。您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。 如果禁用加密连接扫描，则对于 HTTPS 协议只能按服务器名称过滤。
用户	• "**应用于所有用户**"。Web 控制将不为特定用户过滤 Web 资源。 • "**应用于个别用户和/或组**"。Web 控制将仅对特定用户过滤 Web 资源。您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。
规则计划	规则计划确定了 Kaspersky Endpoint Security 监控对该规则涵盖的网络资源的访问的时间跨度。例如，您可以限制只能在工作时间通过浏览器访问 Internet。

按 Web 资源地址过滤

若要控制对单个 Web 资源的访问，必须创建 Web 控制规则，创建网址列表，然后选择 Web 控制操作。创建网址列表时，您可以输入 URL 地址或使用掩码。

规则可以包括规则计划和规则所应用的用户列表。例如，您可以限制仅在工作时间访问网站，或者允许特定组中的用户访问网站。

如何在管理控制台（MMC）中启用 Web 资源地址过滤器

1. 在 Kaspersky Security Center 管理控制台树中，选择"**策略**"。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **安全控制** → **Web 控制**。
4. 选择**Web 控制**复选框。
5. 在"**Web 控制设置**"块中单击"**添加**"按钮。

   "**网络资源访问规则**"窗口将打开。
6. 配置 Web 资源访问规则：

   a. 在"**名称**"字段中输入规则的名称。

   b. 在"**应用于地址**"下拉列表中，选择"**应用于个别地址**"。

c. 创建 Web 资源地址列表。您可以输入网址或使用掩码。您也可以从 TXT 文件导出 Web 资源地址列表。

> 如果禁用加密连接扫描，则对于 HTTPS 协议只能按服务器名称过滤。

d. 在“**应用于用户**”下拉列表，为用户选择相关过滤器：

- “**应用于所有用户**”。Web 控制将不根据地址过滤 Web 资源。
- “**应用于个别用户或组**”。Web 控制将仅过滤列表中的 Web 资源地址。您可以输入网址或使用掩码。您也可以从 TXT 文件导出 Web 资源地址列表。您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

e. 在“**操作**”下拉列表中，选择一个选项：

- “**允许**”。Web 控制允许访问与规则参数匹配的 Web 资源。
- “**阻止**”。Web 控制阻止访问与规则参数匹配的 Web 资源，并显示拒绝访问网站的消息。
- “**警告**”。当用户试图访问与规则匹配的 Web 资源时，Web 控制会显示一条警告，表示不建议访问该 Web 资源。通过警告消息链接，用户可获取对所请求的网页资源的访问权限。

f. 在“**规则计划**”下拉列表中，选择一个计划或创建新计划。

7. 如果您希望 Web 控制在应用策略后立即终止与禁止的 Web 资源的连接，请选择“**应用规则后终止活动用户浏览器会话**”复选框。

> Web 控制仅允许在 Web 浏览器中立即断开 Web 资源。对于其他应用程序，Web 控制仅限制新连接。

如果清除该复选框，Web 控制将仅限制与禁止的 Web 资源的新连接。Web 控制不会终止活动连接。

8. 保存更改。

如何在 Web Console 和云控制台中启用 Web 资源地址过滤器

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **安全控制** → **Web 控制**。
5. 开启 **Web 控制已启用**切换开关。
6. 在“**规则列表**”块中单击“**添加**”按钮。

7. 配置 Web 资源访问规则：

   a. 在“**规则名称**”字段中输入规则的名称。

   b. 为 Web 资源访问规则选择**已启用**状态。

      您可以随时使用切换开关禁用 Web 资源访问规则，而无需将其从列表中删除。

   c. 在“**操作**”块，选择相关选项：

      - “**允许**”。Web 控制允许访问与规则参数匹配的 Web 资源。
      - “**阻止**”。Web 控制阻止访问与规则参数匹配的 Web 资源，并显示拒绝访问网站的消息。
      - “**通知**”。当用户试图访问与规则匹配的 Web 资源时，Web 控制会显示一条警告，表示不建议访问该 Web 资源。通过警告消息链接，用户可获取对所请求的网页资源的访问权限。

   d. 在“**范围**”下，选择“**个别网站**”。

   e. 配置内容过滤器：

      - “**个别地址**”。创建 Web 资源地址列表。您可以输入网址或使用掩码。您也可以从 TXT 文件导出 Web 资源地址列表。

        > 如果禁用加密连接扫描，则对于 HTTPS 协议只能按服务器名称过滤。

      - “**数据类型**”。您可以根据其发布的数据的数据类型（例如，*图形*）控制用户对 Web 资源的访问。

   f. 在“**用户或组**”下，选择希望 Web 控制应用规则的用户。

      Web 控制将仅过滤列表中的 Web 资源地址。您可以输入网址或使用掩码。您也可以从 TXT 文件导出 Web 资源地址列表。您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

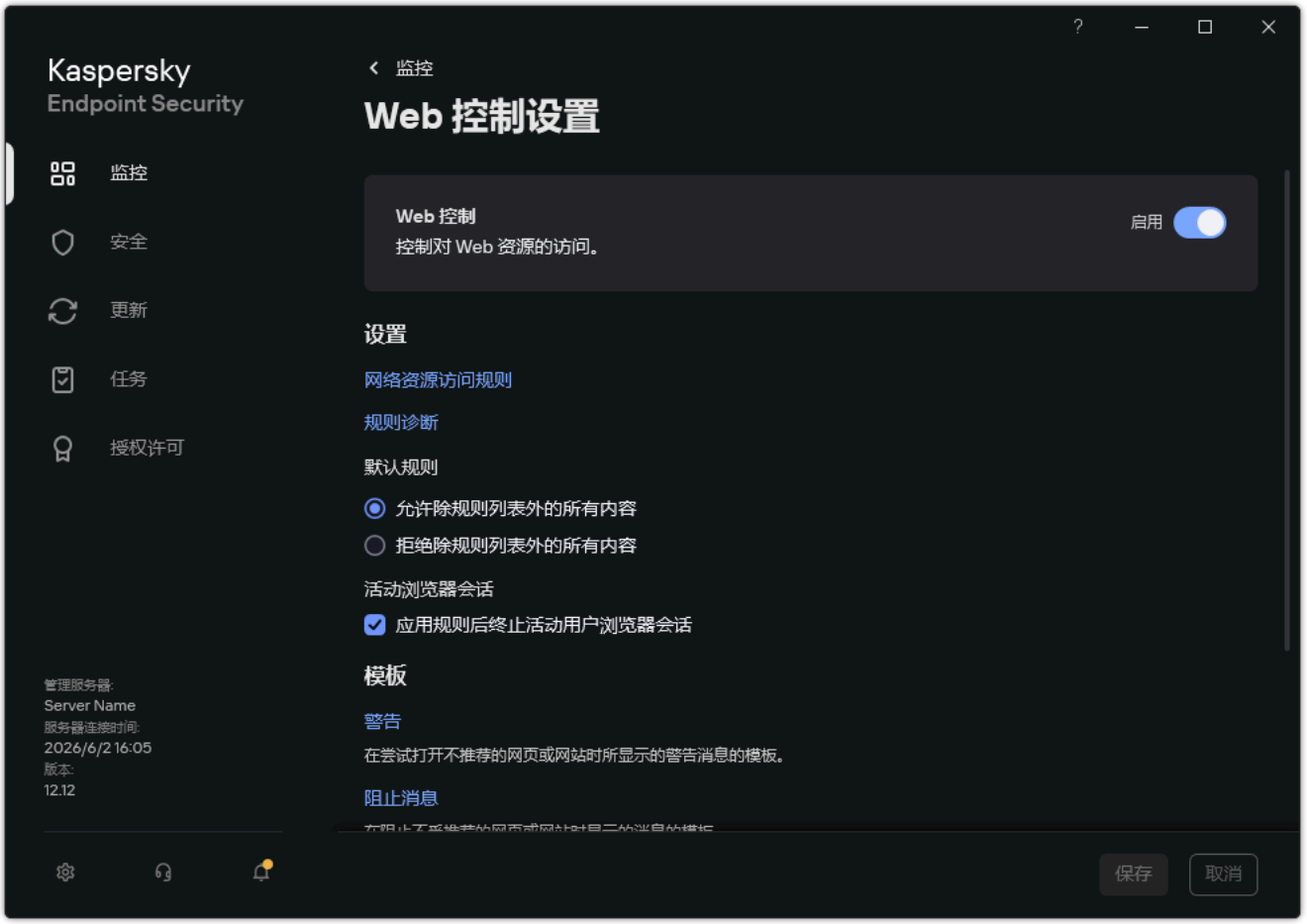
   g. 在“**访问计划**”块，选择计划或创建新计划。

8. 保存更改。

如何在应用程序界面中启用 Web 资源地址过滤器

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**安全控制**” → “**Web 控制**”。



Web 控制设置

3. 在“**设置**”块中单击“**网络资源访问规则**”按钮。

4. 在打开的窗口中，单击“**添加**”按钮。
   “**网络资源访问规则**”窗口将打开。

5. 在“**规则名称**”字段中输入规则的名称。

6. 为 Web 资源访问规则选择**启用**状态。
   您可以随时使用开关禁用 Web 资源访问规则。

7. 在“**操作**”块，选择相关选项：

   - “**允许**”。Web 控制允许访问与规则参数匹配的 Web 资源。
   - “**阻止**”。Web 控制阻止访问与规则参数匹配的 Web 资源，并显示拒绝访问网站的消息。
   - “**警告**”。当用户试图访问与规则匹配的 Web 资源时，Web 控制会显示一条警告，表示不建议访问该 Web 资源。通过警告消息链接，用户可获取对所请求的网页资源的访问权限。

8. 在“**地址**”下，选择“**应用于个别地址**”。
   创建 Web 资源地址列表。您可以输入网址或使用掩码。您也可以从 TXT 文件导出 Web 资源地址列表。

如果禁用加密连接扫描，则对于 HTTPS 协议只能按服务器名称过滤。

9. 在**用户**块，为用户选择相关的过滤器：

   - "**应用于所有用户**"。Web 控制将不为特定用户过滤 Web 资源。
   - "**应用于个别用户和/或组**"。Web 控制将仅过滤列表中的 Web 资源地址。您可以输入网址或使用掩码。您也可以从 TXT 文件导出 Web 资源地址列表。您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

10. 在"**规则计划**"下拉列表中，选择一个计划或创建新计划。

11. 如果您希望 Web 控制在应用策略后立即终止与禁止的 Web 资源的连接，请选择"**应用规则后终止活动用户浏览器会话**"复选框。

    Web 控制仅允许在 Web 浏览器中立即断开 Web 资源。对于其他应用程序，Web 控制仅限制新连接。

    如果清除该复选框，Web 控制将仅限制与禁止的 Web 资源的新连接。Web 控制不会终止活动连接。

12. 保存更改。

结果，新的 Web 控制规则被添加到列表中。如有必要，请更改 Web 控制规则的优先级。您也可以随时使用切换开关禁用 Web 资源访问规则，而无需将其从列表中删除。

按 Web 资源内容过滤

要控制按 Web 资源内容访问，Web 控制提供了一个类别过滤器和一个数据类型过滤器。

网站按照卡巴斯基安全网络云服务、启发式分析和已知网站数据库（包含在应用程序数据库中）进行分类。例如，您可以限制用户对"*社交网络*"类别或其他类别的访问。

您可以根据数据类型限制用户访问网站，例如隐藏图像。Kaspersky Endpoint Security 根据文件格式确定数据类型，而不是基于其扩展名。Web 控制区分以下数据类型：

- 视频
- 声音
- Office 应用程序文件
- 可执行文件
- 存档

- 图形
- 脚本

> Kaspersky Endpoint Security 不扫描压缩文件内的文件。例如，如果图像文件放在压缩文件中，Kaspersky Endpoint Security 会识别“*存档*”数据类型而不是“*图形*”。

规则可以包括规则计划和规则所应用的用户列表。例如，您可以限制仅在工作时间访问网站，或者允许特定组中的用户访问网站。

如何在管理控制台（MMC）中启用 Web 资源内容过滤器

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **安全控制** → **Web 控制**。
4. 选择**Web 控制**复选框。
5. 在“**Web 控制设置**”块中单击“**添加**”按钮。
   “**网络资源访问规则**”窗口将打开。
6. 配置 Web 资源访问规则：
   a. 在“**名称**”字段中输入规则的名称。
   b. 在“**过滤内容**”下拉列表，选择相关的内容过滤器：
      - “**根据内容类别**”。您可以通过类别（例如，“*社交网络*”类别）控制用户对 Web 资源的访问。
      - “**根据数据类型**”。您可以根据其发布的数据的数据类型（例如，*图形*）控制用户对 Web 资源的访问。
      - “**根据内容类别和数据类型**”。启用了按内容类别和数据类型进行过滤。

      选择过滤器后，配置过滤器参数。
   c. 在“**应用于用户**”下拉列表，为用户选择相关过滤器：
      - “**应用于所有用户**”。Web 控制将不根据地址过滤 Web 资源。
      - “**应用于个别用户或组**”。Web 控制将仅过滤列表中的 Web 资源地址。您可以输入网址或使用掩码。您也可以从 TXT 文件导出 Web 资源地址列表。您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

d. 在“**操作**”下拉列表中，选择一个选项：

- “**允许**”。Web 控制允许访问与规则参数匹配的 Web 资源。
- “**阻止**”。Web 控制阻止访问与规则参数匹配的 Web 资源，并显示拒绝访问网站的消息。
- “**警告**”。当用户试图访问与规则匹配的 Web 资源时，Web 控制会显示一条警告，表示不建议访问该 Web 资源。通过警告消息链接，用户可获取对所请求的网页资源的访问权限。

e. 在“**规则计划**”下拉列表中，选择一个计划或创建新计划。

7. 如果您希望 Web 控制在应用策略后立即终止与禁止的 Web 资源的连接，请选择“**应用规则后终止活动用户浏览器会话**”复选框。

> Web 控制仅允许在 Web 浏览器中立即断开 Web 资源。对于其他应用程序，Web 控制仅限制新连接。

如果清除该复选框，Web 控制将仅限制与禁止的 Web 资源的新连接。Web 控制不会终止活动连接。

8. 保存更改。

如何在 Web Console 和云控制台中启用 Web 资源内容过滤器

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **安全控制** → **Web 控制**。
5. 开启 **Web 控制已启用**切换开关。
6. 在“**规则列表**”块中单击“**添加**”按钮。
7. 配置 Web 资源访问规则：

   a. 在“**规则名称**”字段中输入规则的名称。

   b. 为 Web 资源访问规则选择**已启用**状态。
   您可以随时使用开关禁用 Web 资源访问规则。

   c. 在“**操作**”块，选择相关选项：

   - “**允许**”。Web 控制允许访问与规则参数匹配的 Web 资源。
   - “**阻止**”。Web 控制阻止访问与规则参数匹配的 Web 资源，并显示拒绝访问网站的消息。
   - “**通知**”。当用户试图访问与规则匹配的 Web 资源时，Web 控制会显示一条警告，表示不建议访问该 Web 资源。通过警告消息链接，用户可获取对所请求的网页资源的访问权限。

   d. 在“**范围**”下，选择“**内容类别**”。

e. 配置内容过滤器：

- “**内容类别**”。您可以通过类别（例如，“*社交网络*”类别）控制用户对 Web 资源的访问。
- “**数据类型**”。您可以根据其发布的数据的数据类型（例如，*图形*）控制用户对 Web 资源的访问。

f. 在“**用户或组**”下，选择希望 Web 控制应用规则的用户。

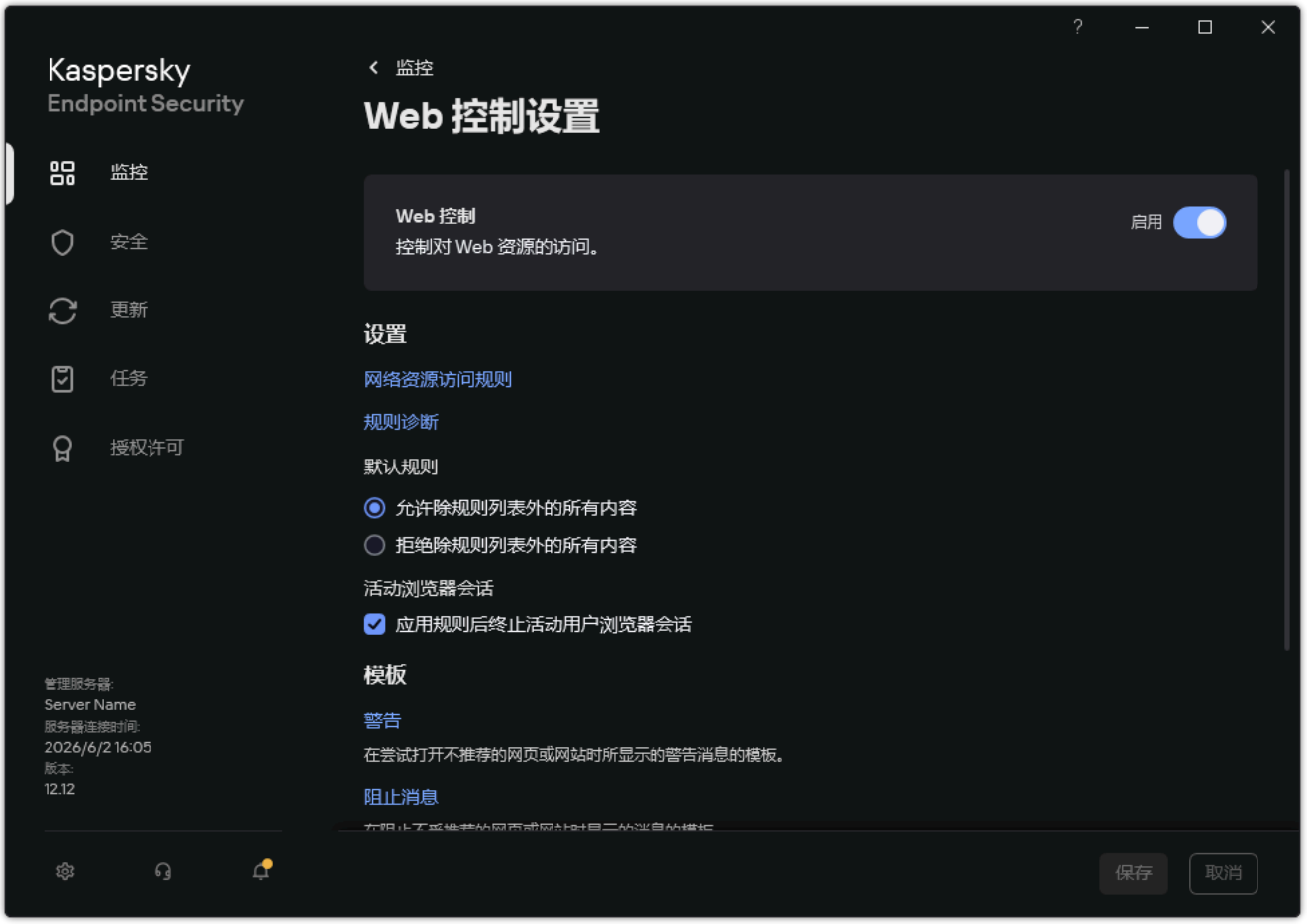
Web 控制将仅过滤列表中的 Web 资源地址。您可以输入网址或使用掩码。您也可以从 TXT 文件导出 Web 资源地址列表。您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

g. 在“**访问计划**”块，选择计划或创建新计划。

8. 保存更改。

如何在应用程序界面中启用 Web 资源内容过滤器

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**安全控制**” → “**Web 控制**”。



Web 控制设置

3. 在“**设置**”块中单击“**网络资源访问规则**”按钮。
4. 在打开的窗口中，单击“**添加**”按钮。

“**网络资源访问规则**”窗口将打开。

5. 在“**规则名称**”字段中输入规则的名称。

6. 为 Web 资源访问规则选择**启用**状态。

   您可以随时使用开关禁用 Web 资源访问规则。

7. 在“**操作**”块，选择相关选项：

   - “**允许**”。Web 控制允许访问与规则参数匹配的 Web 资源。
   - “**阻止**”。Web 控制阻止访问与规则参数匹配的 Web 资源，并显示拒绝访问网站的消息。
   - “**警告**”。当用户试图访问与规则匹配的 Web 资源时，Web 控制会显示一条警告，表示不建议访问该 Web 资源。通过警告消息链接，用户可获取对所请求的网页资源的访问权限。

8. 在**过滤器内容**块，选择相关内容过滤器：

   - “**根据内容类别**”。您可以通过类别（例如，“*社交网络*”类别）控制用户对 Web 资源的访问。
   - “**根据数据类型**”。您可以根据其发布的数据的数据类型（例如，*图形*）控制用户对 Web 资源的访问。

   要配置内容过滤器：

   a. 单击**设置**链接。

   b. 选择所需内容类别和/或数据类型名称旁边的复选框。

      选择某个内容类别和/或数据类型类别旁的复选框就意味着 Kaspersky Endpoint Security 将应用规则以控制对属于选定的内容类别和/或数据类型类别的网页资源的访问。

   c. 返回窗口以配置 Web 资源访问规则。

9. 在**用户**块，为用户选择相关的过滤器：

   - “**应用于所有用户**”。Web 控制将不根据地址过滤 Web 资源。
   - “**应用于个别用户和/或组**”。Web 控制将仅过滤列表中的 Web 资源地址。您可以输入网址或使用掩码。您也可以从 TXT 文件导出 Web 资源地址列表。您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。要创建您要对其应用规则的用户列表：

     a. 单击“**添加**”。

     b. 在打开的窗口中，选择您要应用 Web 资源访问规则的用户或用户组。

     c. 返回窗口以配置 Web 资源访问规则。

10. 在“**规则计划**”下拉列表中，选择所需日程表的名称，或根据选定的规则日程表生成新日程表。为此，请执行下列操作：

    a. 单击“**编辑或添加新的**”。

    b. 在打开的窗口中，单击“**添加**”按钮。

    c. 在打开的窗口中，输入规则计划名称。

    d. 为用户配置 Web 资源访问计划。

    e. 返回窗口以配置 Web 资源访问规则。

11. 如果您希望 Web 控制在应用策略后立即终止与禁止的 Web 资源的连接，请选择“**应用规则后终止活动用户浏览器会话**”复选框。

> Web 控制仅允许在 Web 浏览器中立即断开 Web 资源。对于其他应用程序，Web 控制仅限制新连接。

如果清除该复选框，Web 控制将仅限制与禁止的 Web 资源的新连接。Web 控制不会终止活动连接。

12. 保存更改。

结果，新的 Web 控制规则被添加到列表中。如有必要，请更改 Web 控制规则的优先级。您也可以随时使用切换开关禁用 Web 资源访问规则，而无需将其从列表中删除。

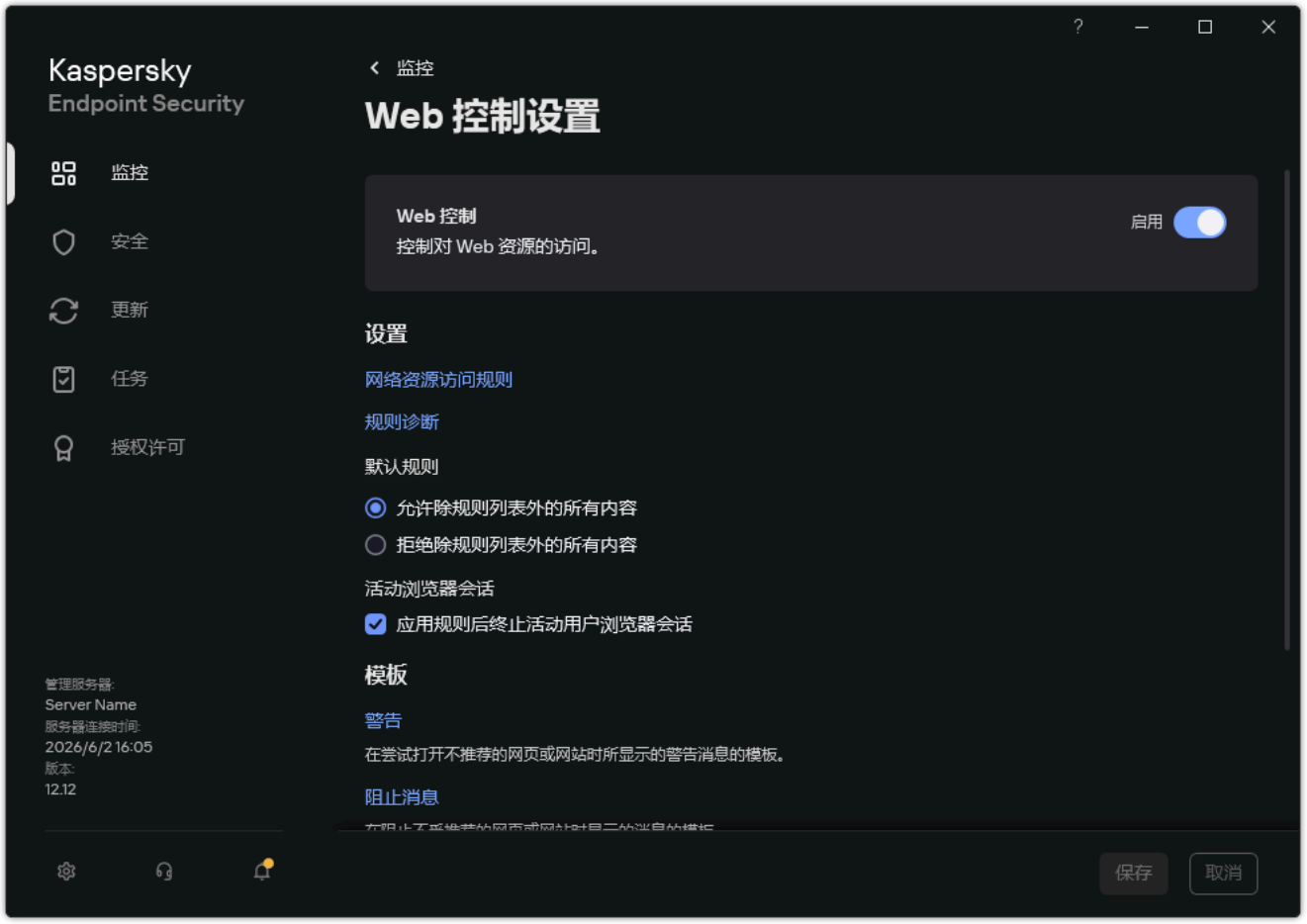
测试网页资源访问规则

配置 Web 控制时，您可能会无意中阻止对用户工作所需的 Web 资源的访问。若要找出阻止访问 Web 资源的 Web 控制规则，您可以使用 *Web 控制规则诊断*工具。Web 控制规则诊断仅在 Kaspersky Endpoint Security 的界面中可用。在 Kaspersky Security Center 控制台中，您无法找到包含给定资源的 Web 控制规则。

如果用户相信该 Web 资源被阻止是错误的，可以单击 Web 资源阻止通知中的链接，将预先生成的消息发送给公司局域网管理员。

要测试网络资源访问规则，请执行下列操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**安全控制**” → “**Web 控制**”。



Web 控制设置

3. 在“**设置**”区域，单击“**规则诊断**”链接。

   “**规则诊断**”窗口将打开。

4. 如果您想要测试 Kaspersky Endpoint Security 用于控制特定网页资源访问权限的规则，请选择“**指定地址**”复选框。后在下面的字段中输入网页资源的地址。

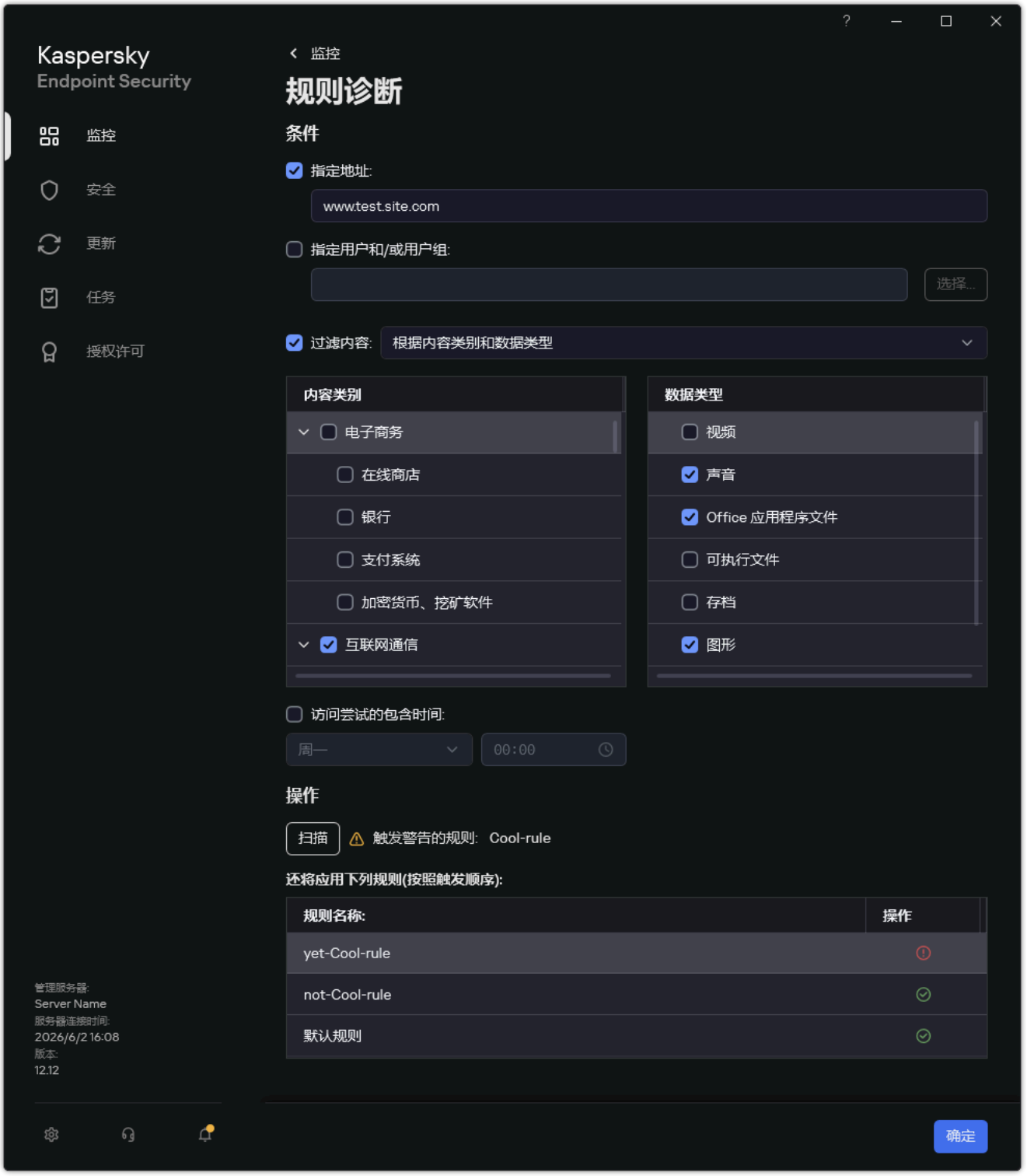
5. 如果您想要测试 Kaspersky Endpoint Security 用于为指定用户和/或用户组控制网页资源访问权限的规则，请指定用户和/或用户组列表。

6. 如果您想要测试 Kaspersky Endpoint Security 用于控制特定内容类别和/或数据类型类别的网页资源访问权限的规则，选择“**过滤内容**”复选框并在下拉列表中选择需要的选项（“**根据内容类别**”、“**根据数据类型**”或“**根据内容类别和数据类型**”）。

7. 如果您要在测试规则时考虑尝试访问规则诊断条件中指定的网页资源的时间和星期几，请选择“**访问尝试的包含时间**”复选框。然后，请指定星期几和时间。

8. 单击“**扫描**”。

测试完成后将显示一条消息，其中包含有关 Kaspersky Endpoint Security 采取的操作（允许、阻止或警告）的信息，该操作是程序根据访问指定网络资源的尝试所触发的第一个规则而采取的。要触发的第一个规则是在 Web 控制规则列表中具有比其他满足诊断条件的规则更高排名的规则。该消息显示在“**扫描**”按钮的右侧。下表列出了其余触发规则，它们指定了 Kaspersky Endpoint Security 采取的操作。这些规则按优先级递减的顺序排列。



Web 资源访问测试结果

导出和导入 Web 控制规则

可以将 Web 控制规则列表导出到 XML or JSON 文件。然后可以修改文件，例如，添加大量相同类型的地址。还可以使用导出/导入功能备份 Web 控制规则列表或将列表迁移到其他服务器。

如何在管理控制台(MMC)中导出和导入 Web 控制规则列表

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **安全控制** → **Web 控制**。

4. 要导出 Web 控制规则列表：

   a. 选择您要导出的规则。要选择多个端口，使用 **CTRL** 或 **SHIFT** 键。

      如果您未选择任何规则，Kaspersky Endpoint Security 将导出所有规则。

   b. 单击**导出**链接。

   c. 在打开的窗口中，指定您要将规则列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。

   d. 保存文件。

      Kaspersky Endpoint Security 会将整个规则列表导出到 XML 文件。

5. 要导入 Web 控制规则列表：

   a. 单击**导入**链接。

      在打开的窗口中，选择要从中导入规则列表的 XML 文件。

   b. 打开文件。

      如果计算机已经具有规则的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 XML 文件向其中添加新条目。

6. 保存更改。

如何在 Web Console 和云控制台中导出和导入 Web 控制规则列表

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **安全控制** → **Web 控制**。

5. 要在**规则列表**块导出规则列表：

   a. 选择您要导出的规则。

   b. 单击“ → **导出**”按钮。

      Kaspersky Endpoint Security 导出规则列表到默认下载文件夹中的 JSON 文件。

6. 要在**规则列表**块导入规则列表：

   a. 单击“ → **导入**”按钮。

      在打开的窗口中，选择要从中导入规则列表的 JSON 文件。

   b. 打开文件。

      如果计算机已经具有规则的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 JSON 文件向其中添加新条目。

7. 保存更改。

导出和导入 Web 控件规则的 Web 资源地址

如果您在 Web 资源访问规则中创建了 Web 资源地址列表，则可将其导出到文件：

- 在管理控制台(MMC)中以 TXT 格式
- 在应用程序界面中以 CSV 格式

随后，您可以从该文件导入列表，从而不必在配置访问规则时创建新的网页资源地址列表。例如，在创建具有相似参数的访问规则时，用于导出和导入网页资源地址列表的选项会非常有用。

您还可以导出/导入所有 Web 控制规则，而不仅仅是单个规则的 Web 资源地址。

> 无法在 Web Console 或云控制台中导出/导入 Web 控制规则的 Web 资源地址。

如何在管理控制台(MMC)中导出/导入 Web 控制规则的 Web 资源地址

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **安全控制** → **Web 控制**。
4. 在“**Web 控制设置**”块，选择您要将其 Web 资源地址列表导出或导入的规则。

   将显示 Web 控制规则属性。
5. 要导出 Web 资源列表，在地址列表中做以下操作：
   a. 选择您要导出的地址。

      如果您未选择任何地址，Kaspersky Endpoint Security 将导出所有地址。
   b. 单击 按钮。
   c. 在打开的窗口中，输入您要将 Web 资源地址列表导出到的 TXT 文件的名称，然后选择要保存此文件的文件夹。
   d. 保存文件。

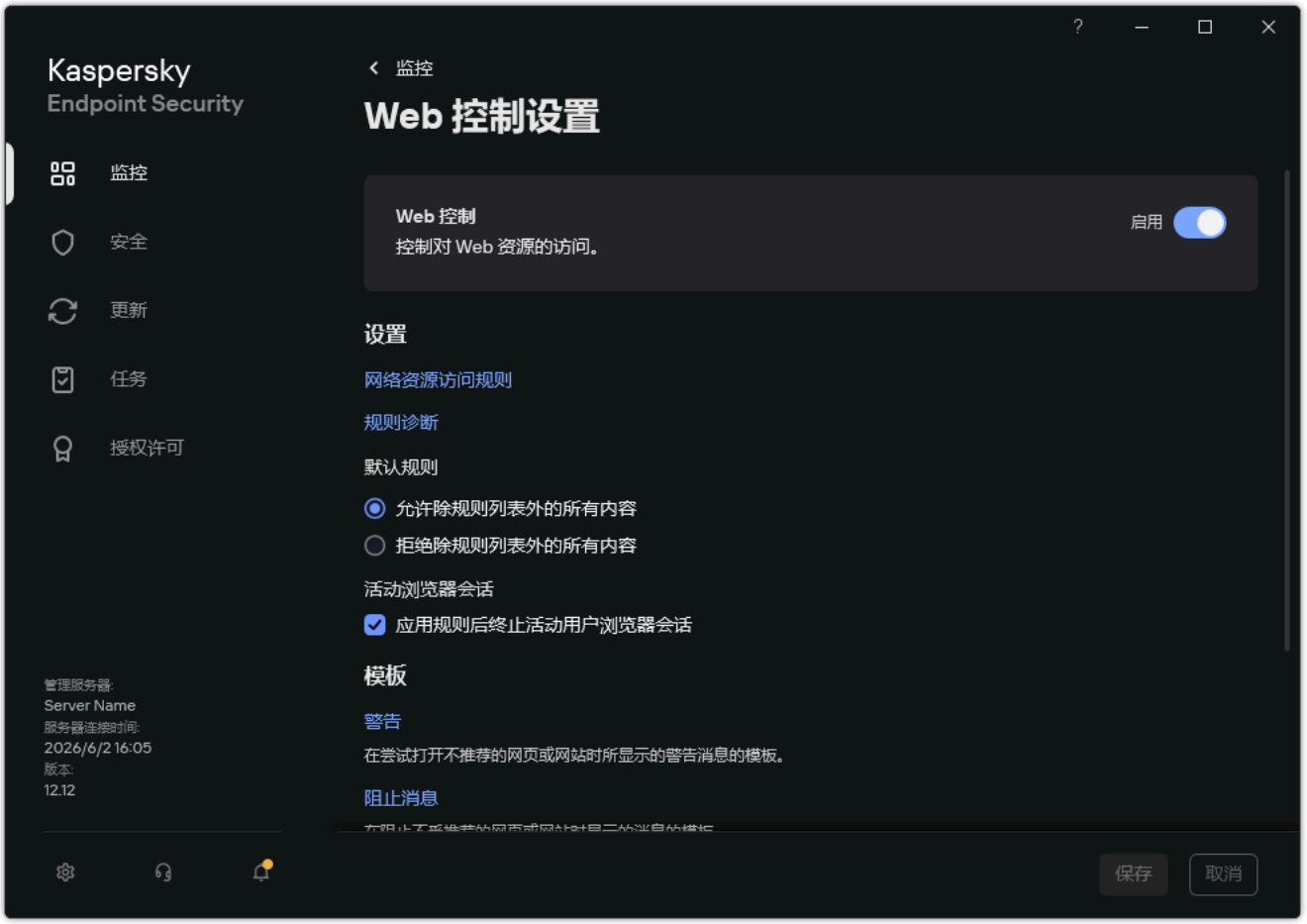
      Kaspersky Endpoint Security 导出 Web 资源地址列表到 TXT 文件。
6. 要导入 Web 资源列表，在地址列表中做以下操作：
   a. 单击 按钮。

      在打开的窗口中，选择要从中导入 Web 资源列表的 TXT 文件。
   b. 打开文件。

      如果计算机已经具有地址列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 TXT 文件向其中添加新条目。
7. 保存更改。

如何在应用程序界面中导出/导入 Web 控制规则的 Web 资源地址

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**安全控制**” → “**Web 控制**”。



Web 控制设置

3. 在“**设置**”块中单击“**网络资源访问规则**”按钮。
4. 选择您要将其网页资源地址列表导出或导入到文件的规则。
5. 要导出受信任网址列表，在**地址**块中做以下操作：
   a. 选择您要导出的地址。
      如果您未选择任何地址，Kaspersky Endpoint Security 将导出所有地址。
   b. 单击“**导出**”。
   c. 在打开的窗口中，输入您要将 Web 资源地址列表导出到的 CSV 文件的名称，然后选择要保存此文件的文件夹。
   d. 保存文件。
      Kaspersky Endpoint Security 导出 Web 资源地址列表到 CSV 文件。
6. 要导入 Web 资源列表，在**地址**块中做以下操作：
   a. 单击“**导入**”。
      在打开的窗口中，选择要从中导入 Web 资源列表的 CSV 文件。

b. 打开文件。

如果计算机已经具有地址列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 CSV 文件向其中添加新条目。

7. 保存更改。

监控用户 Internet 活动

Kaspersky Endpoint Security 允许您记录用户对所有网站（包括允许的网站）的访问数据。这使您可以获取完整的浏览器历史记录视图。Kaspersky Endpoint Security 将用户活动事件发送到 Kaspersky Security Center、Kaspersky Endpoint Security 本地日志和 Windows 事件日志。要在 Kaspersky Security Center 中接收事件，您需要在管理控制台或 Web Console 中配置策略中的事件设置。您还可以配置通过电子邮件传输 Web 控制事件以及在用户计算机上显示屏幕通知。

支持监控功能的浏览器：Microsoft Edge、Microsoft Internet Explorer、Google Chrome、Yandex Browser、Mozilla Firefox。用户活动监控在其他浏览器中不起作用。

Kaspersky Endpoint Security 会创建以下用户 Internet 活动事件：

- 阻止网站（*严重*状态）。
- 访问非推荐网站（*警告*状态）。
- 访问允许的网站（*信息*状态）。

启用用户互联网活动监控之前，您必须做以下操作：

- 注入网页交互脚本到 Web 流量（参见以下说明）。该脚本确保 Web 控制事件的注册。
- 对于 HTTPS 流量监控，您需要启用加密连接扫描。

注入网页交互脚本

如何在管理控制台 (MMC) 中将网页交互脚本注入到 Web 流量中

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **网络设置**。
4. 在“**加密连接扫描**”块中，选中“**注入脚本到 Web 流量从而与网页交互**”复选框。
5. 保存更改。

如何在 Web Console 和 Cloud 控制台中将网页交互脚本注入到 Web 流量中

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 在策略窗口中，选择 **常规设置** → **网络设置**。
5. 在“**监控互联网连接**”下，开启“**监控互联网连接已启用**”开关。
6. 保存更改。

如何在应用程序界面中注入网页交互脚本到 Web 流量

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**网络设置**”。

应用程序网络设置

3. 在“**流量处理**”块中，选中“**注入脚本到 Web 流量从而与网页交互**”复选框。
4. 保存更改。

结果，Kaspersky Endpoint Security 将注入网页交互脚本到 Web 流量。该脚本启用将 Web 控制事件注册到应用程序事件日期、OS 事件日志和报告。

配置 Web 控制事件的日志记录

要配置用户计算机上的 Web 控制事件的日志记录：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**界面**”。
3. 在“**通知**”块中单击“**配置通知**”按钮。
4. 在打开的窗口中选择“**Web 控制**”区域。

   这将打开 Web 控制事件和通知方法的表。
5. 为每个事件配置通知方法：“**保存在本地报告中**”或“**保存在 Windows 事件日志中**”。

   要记录允许的网站访问事件，您还需要配置 Web 控制（请参见下面的说明）。

   在事件表中，您还可以启用屏幕通知和电子邮件通知。要通过电子邮件发送通知，您需要配置 SMTP 服务器设置。有关通过电子邮件发送通知的详细信息，请参阅 Kaspersky Security Center 帮助。
6. 保存更改。

结果，Kaspersky Endpoint Security开始记录用户 Internet 活动事件。

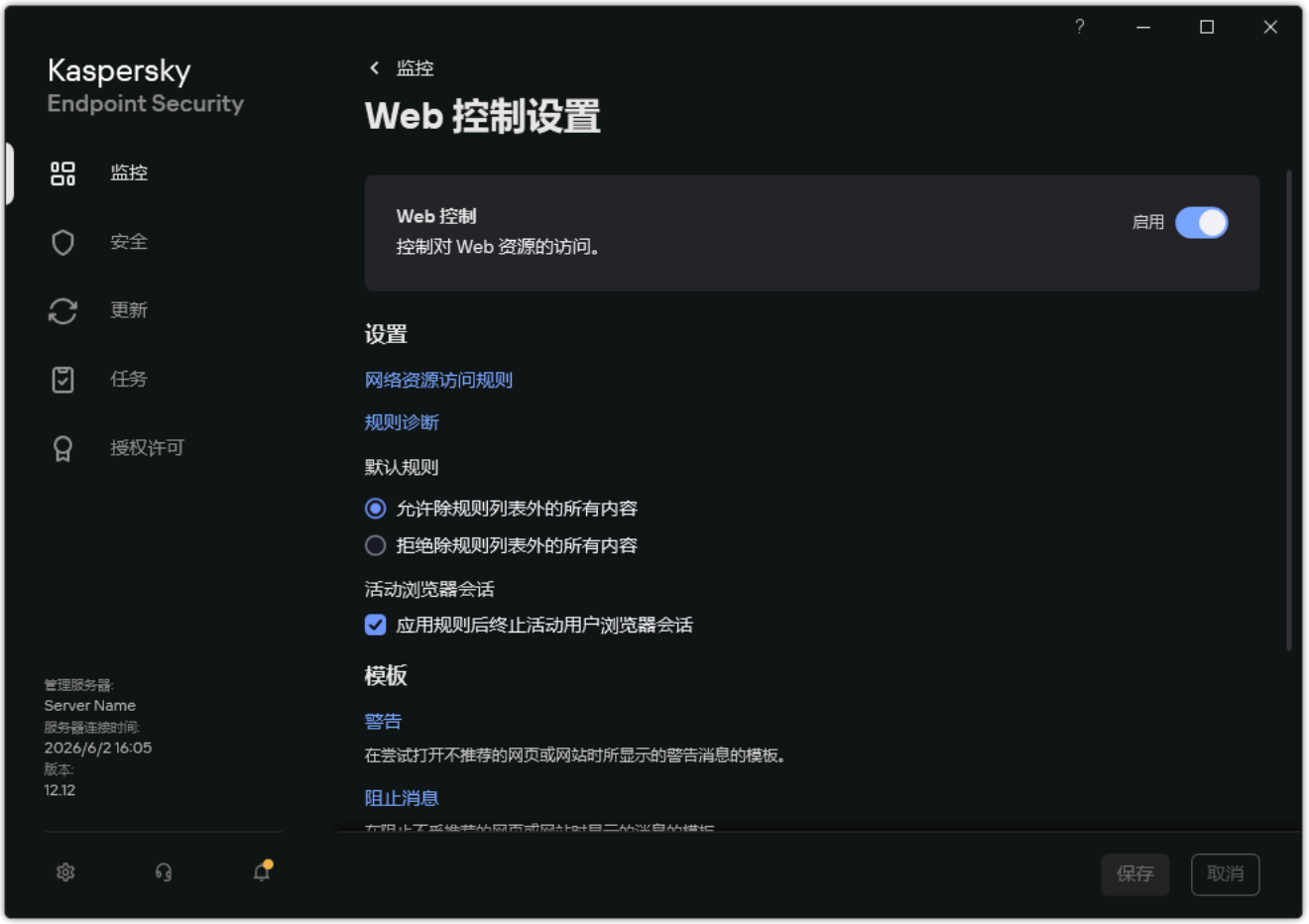
“Web 控制”将用户活动事件发送到 Kaspersky Security Center，如下所示：

- 如果您使用 Kaspersky Security Center，“Web 控制”会针对构成网页的所有对象发送事件。因此，当一个网页被阻止时，可能会创建多个事件。例如，在阻止网页 http://www.example.com 时，Kaspersky Endpoint Security 可能会发送以下对象的事件：http://www.example.com、http://www.example.com/icon.ico、http://www.example.com/file.js 等。
- 如果您使用 Kaspersky Security Center 云控制台，“Web 控制”会对事件进行分组并仅发送网站的协议和域。例如，如果用户访问非推荐网页 http://www.example.com/main、http://www.example.com/contact、http://www.example.com/gallery，Kaspersky Endpoint Security 将只发送一个针对 http://www.example.com 对象的事件。

访问允许的网站时记录事件

要启用访问允许的网站的事件记录：

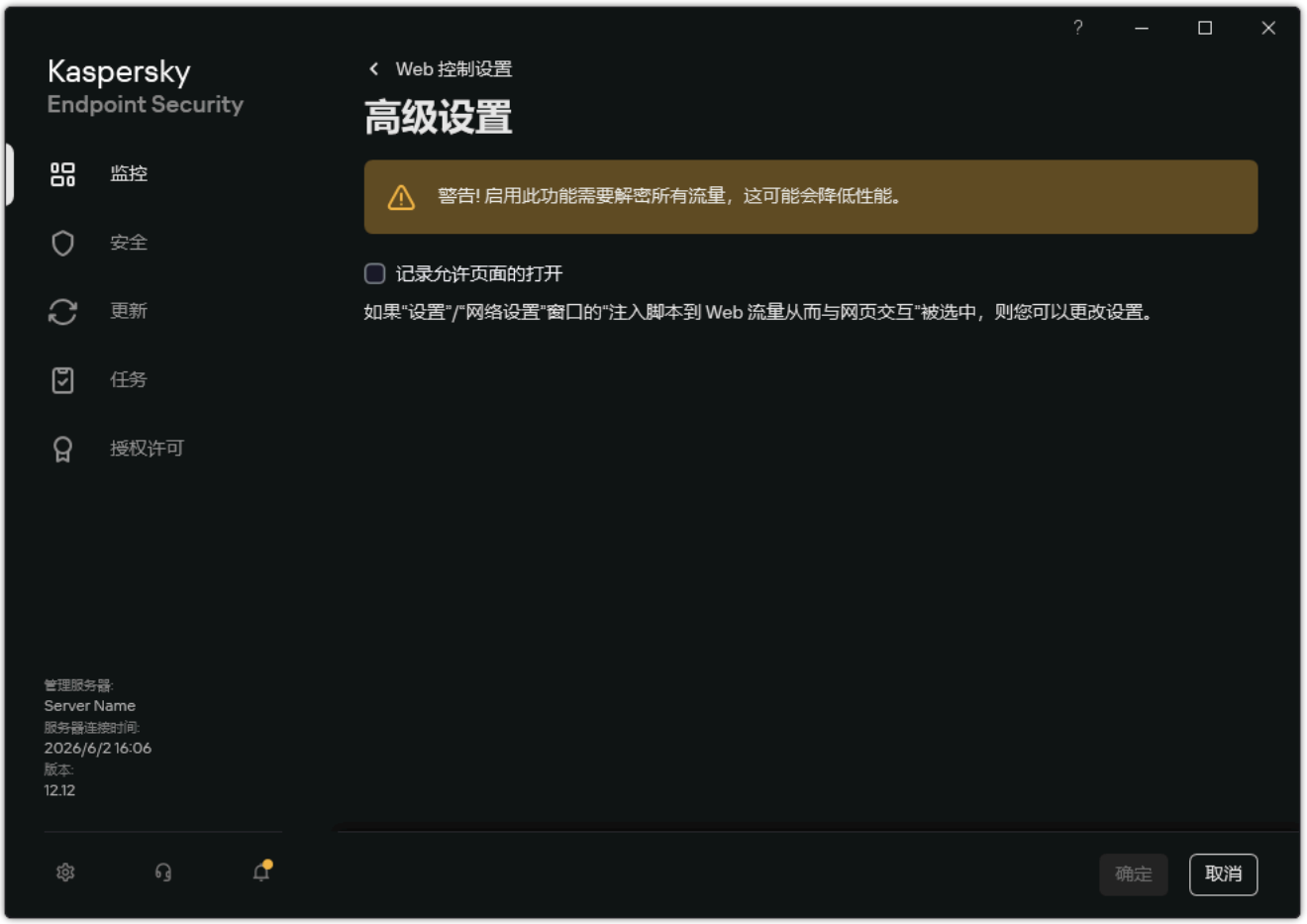
1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**安全控制**” → “**Web 控制**”。



Web 控制设置

3. 在“**附加**”块中单击“**高级设置**”按钮。

4. 在打开的窗口中，选中“**记录允许页面的打开**”复选框。



Web 控制高级设置

5. 保存更改。

结果，您将能够查看完整的浏览器历史记录。

编辑 Web 控制消息模板

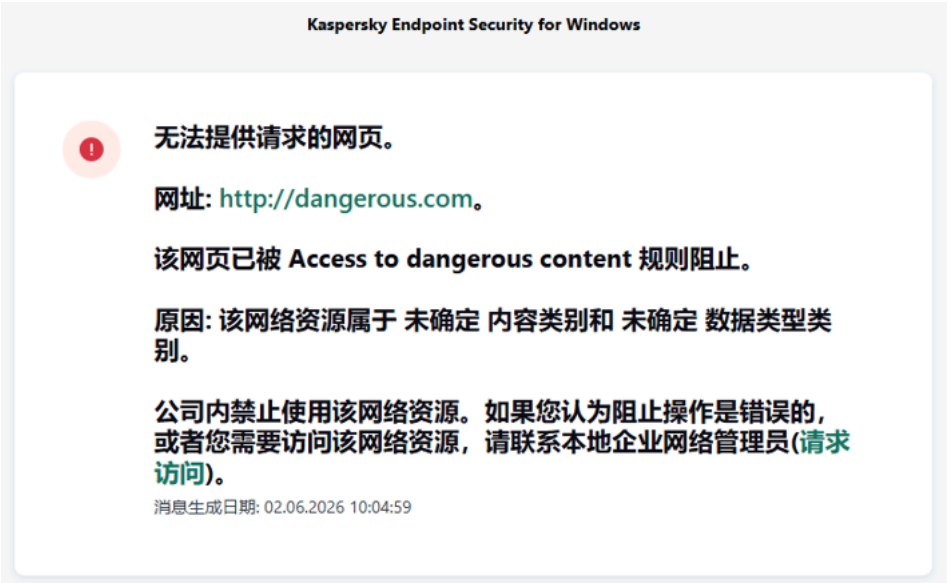
根据在 Web 控制规则属性中指定的操作的类型，当用户尝试访问互联网资源时，Kaspersky Endpoint Security 显示下列类型之一的消息（应用程序用 HTTP 服务器响应消息替换 HTML 页面）：

- 警告消息。该消息将警告访问该网页资源的用户该网页资源不受欢迎并且/或者违反公司安全策略。如果在描述该网页资源的规则的设置中选择了“**警告**”选项，则 Kaspersky Endpoint Security 显示警告消息。

  如果用户相信该警告是错误的，用户可以单击警告消息中的链接，打开预先生成的反馈消息并将其发送给公司局域网管理员。

- 通知阻止网页资源的消息。如果在描述该网页资源的规则的设置中选择了“**阻止**”选项，则 Kaspersky Endpoint Security 显示一条消息，通知您阻止了一个网页资源（参见下图）。

如果用户相信该网页被阻止是错误的，可以单击网页资源阻止通知中的链接，打开预先生成的消息并将其发送给公司局域网管理员。



关于网页资源阻止的消息

我们为警告消息、通知网页资源被阻止的消息以及要发送给局域网管理员的消息提供了专用模板。提供了特殊变量来管理消息模板（例如，`%USER_NAME%`）。变量允许将单个消息模板用于不同的计算机。生成消息时，Kaspersky Endpoint Security 从操作系统设置中检索变量的值，并将其插入到与特定计算机、用户和事件匹配的消息中。

如何在管理控制台 (MMC) 中更改 Web 控制消息模板

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **安全控制** → **Web 控制**。
4. 在“**消息模板设置**”块中单击“**模板**”按钮。
5. 配置 Web 控制消息模板：
   - “**警告**”。该条目字段包含一个消息模板，尝试访问不需要的网页资源触发警告消息规则时就会显示警告消息。
   - “**阻止消息**”。该条目字段包含某个阻止访问网页资源的规则被触发时要显示的消息的模板。
   - “**给管理员的消息**”。用户认为被错误地阻止了访问资源时要发送给局域网管理员的消息模板。在用户请求提供访问权限后，Kaspersky Endpoint Security 向 Kaspersky Security Center 发送一个事件： **发送给管理员的网页访问阻止消息**。事件描述包含一条给管理员的消息，其中包含替换变量。您可以使用预定义事件分类“**用户请求**”在 Kaspersky Security Center 控制台中查看这些事件。如果您的组织没有部署 Kaspersky Security Center 或者没有连接到管理服务器，应用程序将向管理员发送一条消息到指定的电子邮件地址。

   要将变量添加到模板文本中，请将光标放在所需的位置，单击“**变量**”，然后从可用选项列表中选择所需的变量。

   您还可以使用“**默认**”按钮恢复默认模板文本。
6. 保存更改。

如何在 Web Console 和云控制台中更改 Web 控制消息模板

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **安全控制** → **Web 控制**。

5. 在“**消息模板**”块，点击“**关于网站阻止的消息**”链接并配置 Web 控制消息的模板：

   - “**警告**”。该条目字段包含一个消息模板，尝试访问不需要的网页资源触发警告消息规则时就会显示警告消息。

   - “**阻止消息**”。该条目字段包含某个阻止访问网页资源的规则被触发时要显示的消息的模板。

   - “**给管理员的消息**”。用户认为被错误地阻止了访问资源时要发送给局域网管理员的消息模板。在用户请求提供访问权限后，Kaspersky Endpoint Security 向 Kaspersky Security Center 发送一个事件： **发送给管理员的网页访问阻止消息**。事件描述包含一条给管理员的消息，其中包含替换变量。您可以使用预定义事件分类“**用户请求**”在 Kaspersky Security Center 控制台中查看这些事件。如果您的组织没有部署 Kaspersky Security Center 或者没有连接到管理服务器，应用程序将向管理员发送一条消息到指定的电子邮件地址。

   要将变量添加到模板文本中，请将光标放在所需的位置，单击“**添加变量**”，然后从可用选项列表中选择所需的变量。

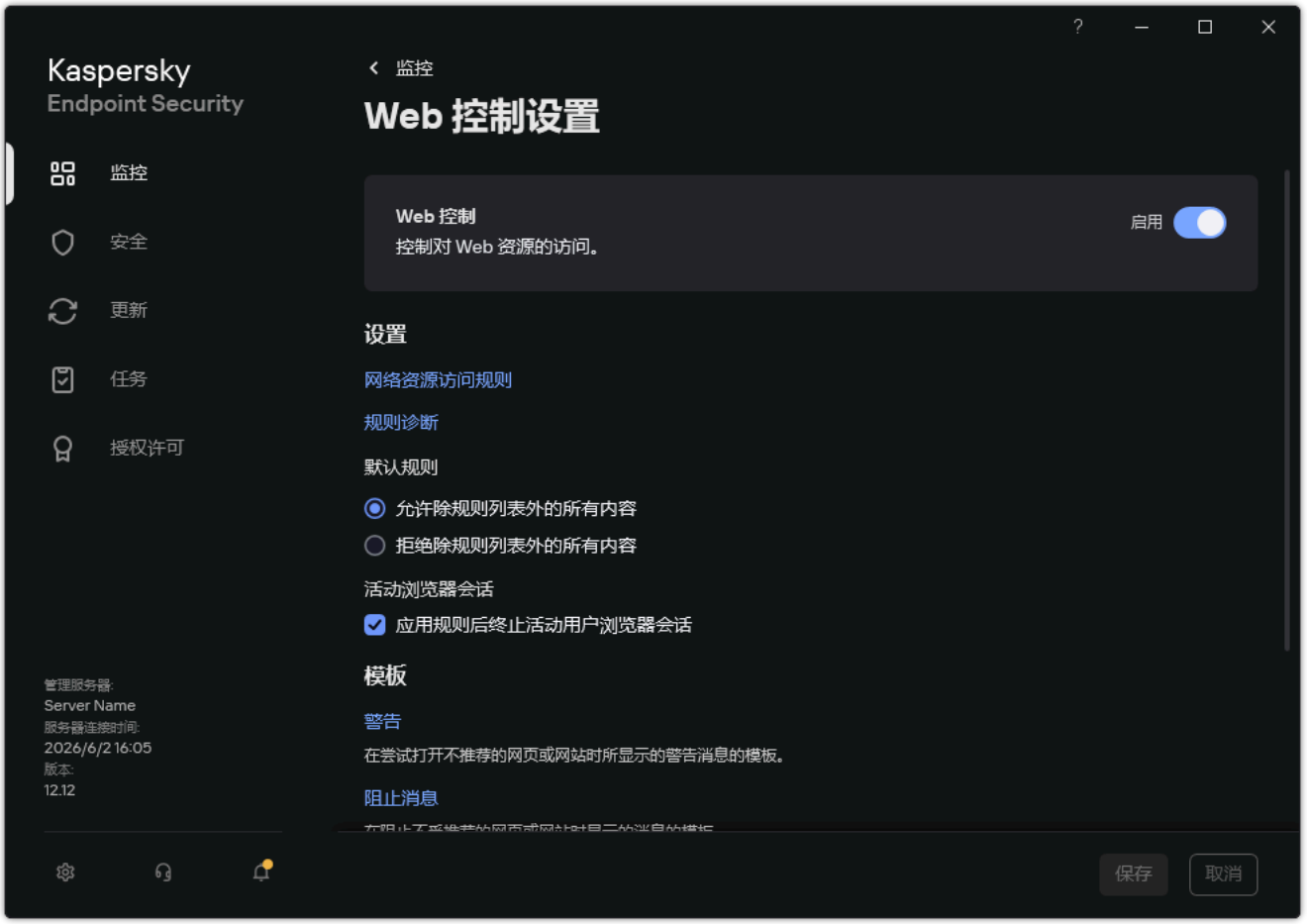
   您还可以使用“**重置为默认值**”按钮恢复默认模板文本。

6. 保存更改。

如何在应用程序界面中更改 Web 控制消息模板

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**安全控制**” → “**Web 控制**”。



Web 控制设置

3. 在**模板**块，为 Web 控制消息配置模板：

   - “**警告**”。该条目字段包含一个消息模板，尝试访问不需要的网页资源触发警告消息规则时就会显示警告消息。

   - “**阻止消息**”。该条目字段包含某个阻止访问网页资源的规则被触发时要显示的消息的模板。

   - “**给管理员的消息**”。用户认为被错误地阻止了访问资源时要发送给局域网管理员的消息模板。在用户请求提供访问权限后，Kaspersky Endpoint Security 向 Kaspersky Security Center 发送一个事件： **发送给管理员的网页访问阻止消息**。事件描述包含一条给管理员的消息，其中包含替换变量。您可以使用预定义事件分类“**用户请求**”在 Kaspersky Security Center 控制台中查看这些事件。如果您的组织没有部署 Kaspersky Security Center 或者没有连接到管理服务器，应用程序将向管理员发送一条消息到指定的电子邮件地址。

   要将变量添加到模板文本中，请将光标放在所需的位置，单击“**添加变量**”，然后从可用选项列表中选择所需的变量。

   您还可以使用“**重置**”按钮恢复默认模板文本。

4. 保存更改。

编辑网页资源地址的掩码

如果您在创建网络资源访问规则时需要输入多个相似的网页资源地址，则使用*网页资源地址掩码*（也称为“地址掩码”）会非常有用。如果创建得当，一个地址掩码可以替换大量的网页资源地址。

创建地址掩码时遵循以下规则：

1. `*` 字符将替换包含零或更多个字符的任意序列。

   例如，如果输入 `*abc*` 地址掩码，则访问规则将应用于包含序列 `abc` 的所有网络资源。例如：`http://www.example.com/page_0-9abcdef.html`。

2. 一个 `*.` 字符序列(即*域掩码*)允许您选择一个地址的所有域。`*.` 域掩码代表任何域名、子域名或空白行。

   例如：`*.example.com` 掩码代表以下地址：

   - `http://pictures.example.com`。域掩码 `*.` 代表`pictures.`。
   - `http://user.pictures.example.com`。域掩码 `*.` 代表 `pictures.` 和 `user.`。
   - `http://example.com`。域掩码 `*.` 解释为空行。

3. 位于地址掩码开头的`www.` 字符序列被解释为 `*.` 序列。

   例如：地址掩码 `www.example.com` 将被解释为 `*.example.com`。该掩码覆盖地址 `www2.example.com` 和 `www.pictures.example.com`。

4. 如果地址掩码不以 `*` 字符开头，则地址掩码的内容等同于以 `*.` 为前缀的内容。

5. 如果地址掩码以 `/` 或 `*` 之外的字符结尾，则地址掩码的内容等同于以 `/*` 为后缀的内容。

   例如：地址掩码 `http://www.example.com` 涵盖像 `http://www.example.com/abc` 这样的地址，其中 `a`、`b` 和 `c` 为任意字符。

6. 如果地址掩码以 `/` 字符结尾，则地址掩码的内容等同于以 `/*` 为后缀的内容。

7. 地址掩码末尾的字符序列 `/*` 将被解释为 `/*` 或空字符串。

8. 网页资源地址根据地址掩码进行验证，同时会考虑使用的协议（http 或 https）：

   - 如果地址掩码不含网络协议，该地址掩码将涵盖使用任意网络协议的地址。

     例如：地址掩码 `example.com` 涵盖地址 `http://example.com` 和 `https://example.com`。

   - 如果地址掩码包含网络协议，该地址仅涵盖使用地址掩码中网络协议的地址。

     例如：地址掩码 `http://*.example.com` 涵盖地址 `http://www.example.com`，但不涵盖 `https://www.example.com`。

9. 用双引号引起来的地址掩码表示除 `*` 字符（如果初始包含在地址掩码中）外，不考虑其他任何替代项。规则 5 和 7 不会应用至双引号中的地址掩码（请参阅下表中的示例 14-18）。

10. 在比较网页资源的地址掩码时，不会考虑用户名和密码、连接端口以及字符大小写。

编号	地址掩码	要验证的网页资源地址	是地址掩码涵盖的地址	注释
1	*.example.com	http://www.123example.com	否	参见规则 1。
2	*.example.com	http://www.123.example.com	是	参见规则 2。
3	*example.com	http://www.123example.com	是	参见规则 1。
4	*example.com	http://www.123.example.com	是	参见规则 1。
5	http://www.*.example.com	http://www.123example.com	否	参见规则 1。
6	www.example.com	http://www.example.com	是	参见规则 3、2、1。
7	www.example.com	https://www.example.com	是	参见规则 3、2、1。
8	http://www.*.example.com	http://123.example.com	是	参见规则 3、4、1。
9	www.example.com	http://www.example.com/abc	是	参见规则 3、5、1。
10	example.com	http://www.example.com	是	参见规则 3、1。
11	http://example.com/	http://example.com/abc	是	参见规则 6。
12	http://example.com/*	http://example.com	是	参见规则 7。
13	http://example.com	https://example.com	否	参见规则 8。
14	"example.com"	http://www.example.com	否	参见规则 9。
15	"http://www.example.com"	http://www.example.com/abc	否	参见规则 9。
16	"*.example.com"	http://www.example.com	是	参见规则 1、9。
17	"http://www.example.com/*"	http://www.example.com/abc	是	参见规则 1、9。
18	"www.example.com"	http://www.example.com; https://www.example.com	是	参见规则 9、8。
19	www.example.com/abc/123	http://www.example.com/abc	否	地址掩码包含的信息量多于网页资源地址。

虚拟机的 Web 控制

Web 控制控制计算机上的流量以及计算机上本地部署的虚拟机的流量。无需在本地虚拟机上安装 Kaspersky Endpoint Security 应用程序即可实现此功能。这意味着，如果用户尝试在*虚拟机*的浏览器中打开被 Web 控制规则阻止的网站，安装在*计算机*主机操作系统上的应用程序拒绝访问该网站。

Web 控制在不同的虚拟机上的工作方式不同。

Oracle VM VirtualBox

Kaspersky Endpoint Security 支持 Oracle VM VirtualBox 虚拟机上的 Web 控制规则，不受限制。该应用程序可以控制虚拟机的所有流量。如果在 Web 控制规则中配置了按用户过滤，则应用程序可以正常工作，因为虚拟机的所有进程均由本地用户启动。

VMware Workstation

Kaspersky Endpoint Security 支持 VMware Workstation 虚拟机上的 Web 控制规则，但有限制。该应用程序不支持配置了按用户过滤的规则。虚拟机进程在系统用户（SYSTEM）下运行。这使得无法识别尝试在虚拟机上打开网站的用户。

Microsoft Hyper-V

Kaspersky Endpoint Security 不支持 Microsoft Hyper-V 虚拟机上的 Web 控制规则。

Web 控制消息模板中的变量

您可以在用户消息模板或管理员消息模板中使用以下变量：

- **用户** – `%USER_NAME%`。

  生成该消息的计算机上的当前用户账户名称，以“`<device name>\<user alias>`”格式（例如，`DESKTOP-123\John.Smith`）。

- **网络资源地址** – `%CANONIC_REQUEST_URL%`。

  被阻止的 Web 资源的地址。

- **规则名称** – `%RULE%`。

  阻止该 Web 资源的规则名称。

- **用于发送消息的电子邮件** – `%COMPLAIN_EMAIL%`。

  用于接收关于 Web 资源被阻止反馈的电子邮件地址。点击电子邮件地址会打开一个窗口，用户可以在该窗口中向管理员发送消息。

- **内容类别的名称** – `%CONTENT_CATEGORY_LIST%`。

  被阻止资源所属的网站类别（例如，*支付系统*）。

- **数据类型类别的名称** – `%TYPE_CATEGORY_LIST%`。

  被阻止的 Web 资源的数据类型类别（例如，*图形文件*）。

- **到所请求网络资源的链接** – `%CONTINUE_PAGE%`。

  指向所请求网页的链接（例如，`http://www.example.com/pagename.html`）。

- **网站链接** – `%CONTINUE_SITE%`。

  指向包含所请求网页的网站的链接（例如，`http://www.example.com/`）。

- **用于访问域的链接** – %CONTINUE_DOMAIN%。

  点击此链接即可访问该域名下的所有现有网页。例如，如果被阻止网页的地址是 http://www.example.com， %CONTINUE_DOMAIN% 变量被替换为 http://*.example.com 链接。点击此链接即可访问基本域名 http://www.example.com/ 下的所有网址，包括子域名。例如 http://start.example.com/* 或者 http://domain.domain.example.com/*，其中 * 字符代表任意字符序列（包括空字符串）。

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（例如，硬盘驱动器、相机或 Wi-Fi 模块）的访问。这样可以在连接此类设备时保护计算机免受感染，并防止数据丢失或数据泄漏。

如果设备控制被启用，应用程序转发已连接的设备信息到 Kaspersky Security Center。您可以在 Kaspersky Security Center 的“**高级**” → “**存储库**” → “**硬件**”文件夹中查看已连接设备列表。

设备访问级别

“设备控制”控制以下级别的访问权限：

- **设备类型**。例如，打印机、可移动驱动器和 CD/DVD 驱动器。

  您可以按如下方式配置设备访问权限：

  - 允许 – ✓。
  - 阻止 – ⊘。
  - 根据规则（仅对打印机和便携式设备） – 。
  - 取决于连接总线（除了 Wi-Fi） – 。
  - 阻止但带有例外（仅 Wi-Fi） – .

- **连接总线**。“*连接总线*”是用于将设备连接到计算机的接口（例如 USB 或 FireWire）。如果为设备类型选择了“**取决于连接总线**”模式，应用程序根据连接接口（例如 USB）允许或拒绝访问设备。

  您可以按如下方式配置设备访问权限：

  - 允许 – ✓。
  - 阻止 – ⊘。

- **受信任设备**。*受信任的设备*是指在受信任设备设置中指定的用户可随时进行完全访问的设备。

您可以根据以下数据添加受信任设备：

- “**按 ID 添加设备**”。每个设备都有一个唯一的标识符（硬件 ID 或 HWID）。您可以使用操作系统工具在设备属性中查看 ID。设备 ID 示例：`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`。如果要添加多个特定设备，则按 ID 添加设备很方便。

- “**按型号添加设备**”。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在设备属性中查看 ID。用于输入 VID 和 PID 的模板：`VID_1234&PID_5678`。如果在组织中使用特定型号的设备，则按型号添加设备很方便。这样，您可以添加该型号的所有设备。

- “**按 ID 掩码添加设备**”。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。`*` 字符可替换任意一组字符。输入掩码时，Kaspersky Endpoint Security 不支持 `?` 字符。例如，`WDC_C*`。

- “**按型号掩码列出的设备**”。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。`*` 字符可替换任意一组字符。输入掩码时，Kaspersky Endpoint Security 不支持 `?` 字符。例如，`VID_05AC&PID_*`。

“设备控制”通过使用*访问规则*来管理用户对设备的访问。“设备控制”还允许您保存设备连接/断开连接事件。要保存事件，您需要在策略中配置事件注册。

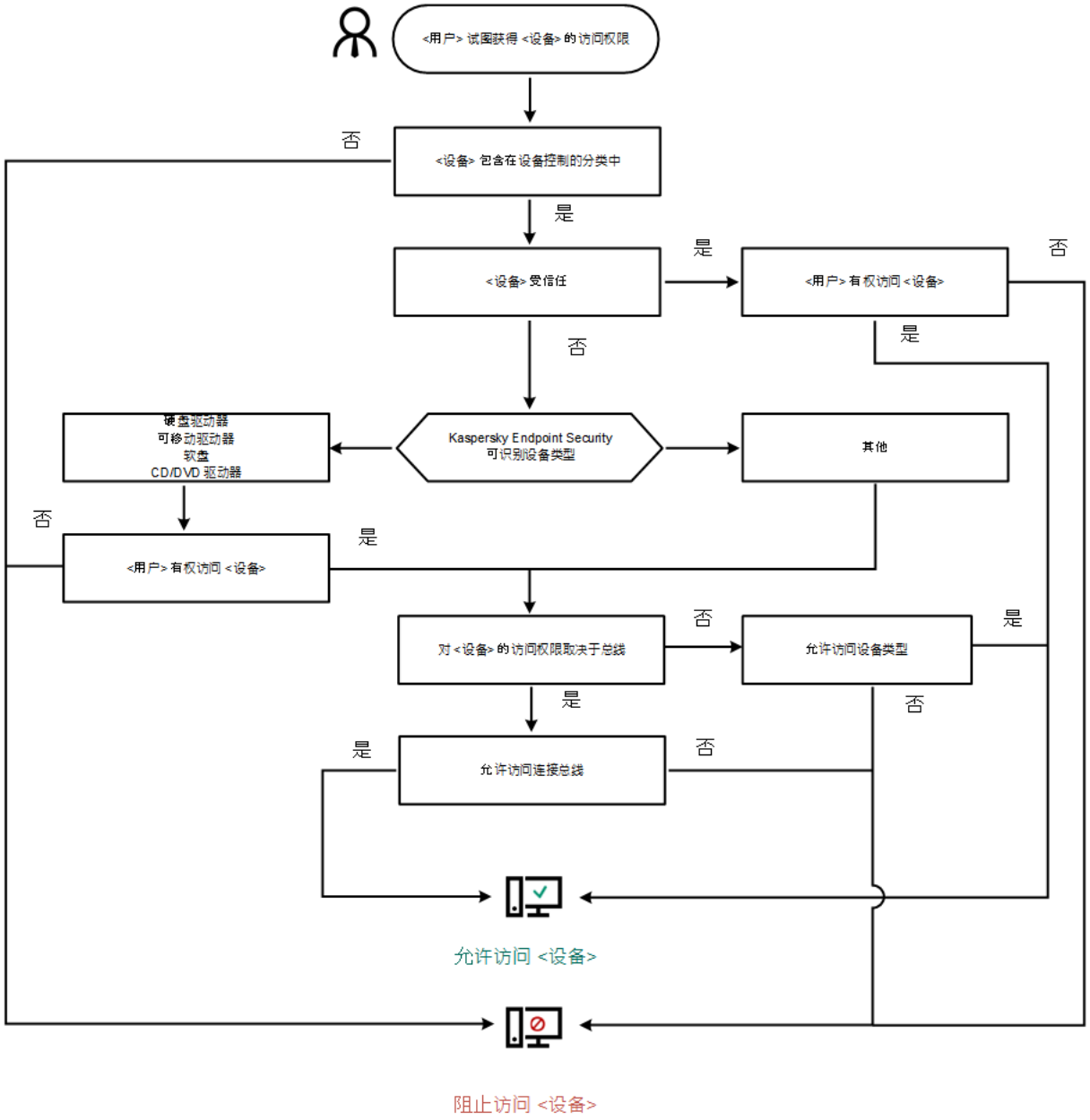
> 如果对设备的访问权限取决于连接总线（状态），Kaspersky Endpoint Security 不会保存设备连接/断开连接事件。要使 Kaspersky Endpoint Security 保存设备连接/断开连接事件，请允许访问相应的设备类型（状态）或将设备添加到信任列表。

当被“设备控制”阻止的设备连接到计算机时，Kaspersky Endpoint Security 将阻止访问并显示通知（请参见下图）。

“设备控制”通知

设备控制运行算法

Kaspersky Endpoint Security 在用户将设备连接到计算机之后做出是否允许访问该设备的决定（请参见下图）。



设备控制运行算法

如果已连接设备并允许访问，您可以编辑访问规则并阻止访问。在这种情况下，下次有人尝试访问该设备（例如查看文件夹树或执行读取或写入操作）时，Kaspersky Endpoint Security 会阻止访问。没有文件系统的设备仅在该设备下一次连接时被阻止。

如果已安装有 Kaspersky Endpoint Security 的计算机上的用户需要请求被错误阻止的设备的访问权限，则向该用户发送请求访问说明。

关于访问规则

*设备访问规则*包含一组设置，用于确定用户如何访问安装到或连接到计算机的设备。这些设置包含到特定设备的访问权限，访问计划和读写权限。您不能添加在设备控制分类之外的设备。此类设备允许所有用户访问。

设备访问规则

访问规则的设置组根据设备类型的不同而不同（请参见下表）。

访问规则设置

设备	访问控制	设备访问计划	用户和/或用户组的分配	优先级	读/写权限
硬盘驱动器	✓	✓	✓	✓	✓
可移动驱动器 （包括 USB 闪存驱动器）	✓	✓	✓	✓	✓
软盘	✓	✓	✓	✓	✓
CD/DVD 驱动器	✓	✓	✓	✓	✓
便携式设备(MTP)	✓	✓	✓	✓	✓
本地打印机	✓	–	✓	✓	–
网络打印机	✓	–	✓	✓	–
调制解调器	✓	–	–	–	–
磁带设备	✓	–	–	–	–
多功能设备	✓	–	–	–	–
智能卡读取器	✓	–	–	–	–
Windows CE USB ActiveSync 设备	✓	–	–	–	–
外部网络适配器	✓	–	–	–	–
蓝牙	✓	–	–	–	–
摄像头和扫描仪	✓	–	–	–	–

Wi-Fi 网络的访问规则

Wi-Fi 网络访问规则确定允许（✓ 状态）还是禁止（⊘ 状态）使用 Wi-Fi 网络。你您可以将*受信任的 Wi-Fi 网络*（ 状态）添加到规则中。允许无限制使用受信任的 Wi-Fi 网络。默认情况下，Wi-Fi 网络访问规则允许访问任何 Wi-Fi 网络。

连接总线访问规则

如果根据设备类型为访问规则选择了“**取决于连接总线**”值，应用程序根据连接接口允许或拒绝对设备的访问。默认情况下，程序将为设备控制组件分类中存在的所有连接总线创建允许访问总线的规则。

连接总线访问规则确定允许（✓ 状态）还是禁止（⊘ 状态）连接设备。设备类型访问规则的优先级高于连接总线访问规则的优先级。

> 无法使用设备控制锁定键盘和鼠标。如果您禁止访问 USB 连接总线，用户将继续使用通过 USB 连接的键盘和鼠标进行工作。“BadUSB 攻击防护”组件用于防止受感染的模拟键盘的 USB 设备连接至计算机。

按类型管理设备访问

设备控制允许按类型管理对设备的访问。设备类型在设备连接时由操作系统确定。您可以使用操作系统内置的设备管理器工具查找设备类型。要管理对设备的访问，您必须配置规则。*设备访问规则*包含一组设置，用于确定用户如何访问安装到或连接到计算机的设备。这些设置包含到特定设备的访问权限，访问计划和读写权限。您不能添加在设备控制分类之外的设备。此类设备允许所有用户访问。

默认情况下，设备控制允许所有用户访问所有设备。

您可以按如下方式配置对设备的访问：

- "**允许**"。

  Kaspersky Endpoint Security 授予所有用户对设备的完全访问权限。

- "**阻止**"。

  Kaspersky Endpoint Security 阻止设备连接。应用程序仅允许受信任设备连接。

- "**取决于连接总线**"。

  Kaspersky Endpoint Security 确定设备的连接接口并根据设备的总线连接状态限制对设备的访问。应用程序还允许连接受信任设备。

- "**根据规则**"。

  对于某些设备类型，您可以指定允许使用设备的单个用户或一组用户，设置访问设备的时间表，并配置读写权限。应用程序还允许连接受信任设备。

配置对"**硬盘驱动器**"类型设备的访问时要小心。如果阻止对系统磁盘的访问，则应用程序可能会在启动操作系统时导致崩溃 (BSOD)。

如果设备不符合设备控制分类方案，则无法限制对该设备的访问。

如何在管理控制台(MMC)中按类型管理对设备的访问

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择"**策略**"。
3. 选择必要的策略并双击以打开策略属性。
4. 在策略窗口中，选择 **安全控制** → **设备控制**。
5. 在"**设备控制设置**"下，选择"**设备类型**"选项卡。

   "**设备类型**"选项卡显示包含在设备控制分类的所有设备的访问规则。
6. 配置设备的访问规则：

   a. 选择访问模式：**允许**、**阻止**、**取决于连接总线**、**根据规则**。

      要选择"**根据规则**"访问模式，必须双击以打开访问规则属性。

   b. 如果您选择"**取决于连接总线**"访问模式，必须在"**连接总线**"选项卡上配置连接接口的访问规则。

c. 对于存储设备（例如，可移动媒体），您可以为单个用户配置访问权限。您还可以设置访问设备的时间表并配置读写权限。

   您可以将设备添加到受信任列表。*受信任的设备*是指在受信任设备设置中指定的用户可随时进行完全访问的设备。

d. 如有需要，配置打印规则。

e. 如有需要，配置蓝牙设备访问规则。

f. 如有需要，配置计算机 Wi-Fi 连接规则。

7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中按类型管理对设备的访问

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **安全控制** → **设备控制**。

5. 在“**设备访问规则**”下，选择“**设备和 Wi-Fi 网络**”选项卡。

   该表列出了设备控制组件分类中存在的所有设备的访问规则。

6. 配置设备的访问规则：

   a. 选择访问模式：**允许**、**阻止**、**取决于总线**、**自定义**。

      如果下拉菜单中缺少访问模式，请双击设备类型打开访问规则属性。

   b. 如果您选择“**取决于总线**”访问模式，必须在“**连接总线**”选项卡上配置连接接口的访问规则。

   c. 对于存储设备（例如，可移动媒体），您可以为单个用户配置访问权限。您还可以设置访问设备的时间表并配置读写权限。

      您可以将设备添加到受信任列表。*受信任的设备*是指在受信任设备设置中指定的用户可随时进行完全访问的设备。

   d. 如有需要，配置打印规则。

   e. 如有需要，配置蓝牙设备访问规则。

   f. 如有需要，配置计算机 Wi-Fi 连接规则。

7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在应用程序界面中管理对设备的访问

1. 打开主应用程序窗口并单击 按钮。

2. 在应用程序设置窗口中，选择“**安全控制**” → “**设备控制**”。

3. 在“**访问设置**”区域，单击“**设备和 Wi-Fi 网络**”链接。

   该表列出了设备控制组件分类中存在的所有设备的访问规则。

4. 配置设备的访问规则：

   a. 选择访问模式：**允许**、**阻止**、**取决于连接总线**、**根据规则**。

      如果下拉菜单中缺少访问模式，请双击设备类型打开访问规则属性。

   b. 如果您选择“**取决于连接总线**”访问模式，必须在“**连接总线**”选项卡上配置连接接口的访问规则。

   c. 对于存储设备（例如，可移动媒体），您可以为单个用户配置访问权限。您还可以设置访问设备的时间表并配置读写权限。

      您可以将设备添加到受信任列表。*受信任的设备*是指在受信任设备设置中指定的用户可随时进行完全访问的设备。

   d. 如有需要，配置打印规则。

   e. 如有需要，配置蓝牙设备访问规则。

   f. 如有需要，配置计算机 Wi-Fi 连接规则。

5. 保存更改。

因此，当用户尝试访问设备时，应用程序会根据规则阻止访问。Kaspersky Endpoint Security 也会记录相应的事件。如果您想授予单个设备的访问权限，您可以将这些设备添加到受信任设备列表中。

通过连接总线管理对设备的访问

要编辑连接总线访问规则，请执行以下操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**安全控制**” → “**设备控制**”。

3. 在“**访问设置**”块中单击“**连接总线**”按钮。

   打开的窗口显示包含在设备控制组件分类的所有连接总线的访问规则。

4. 选择您想要编辑的访问规则。

5. 在**访问**栏，选择是否允许访问连接总线：**允许**或**阻止**。

   如果您已更改对连接总线**串行端口**（COM）或**并行端口**（LPT）的访问，则必须重新启动计算机以激活访问规则。

6. 保存更改。

区分用户对设备的访问权限

您可以按设备类型或受信任设备配置用户访问权限。

根据设备类型区分用户访问权限

设备控制允许配置用户对*存储设备*上数据的访问权限。对于这样的设备，您可以配置写入和读取权限。设备控制支持以下类型的*存储设备*：

- 硬盘驱动器。
- 可移动驱动器 （包括 USB 闪存驱动器）。
- 软盘。
- CD/DVD 驱动器。
- 便携式设备(MTP)。便携式设备 (MTP) 包括例如移动设备、照相机、媒体播放器等。

例如，通过这种方式，您可以仅允许管理员组使用可移动媒体。对于其他设备类型，您可以拒绝或允许所有用户访问。您还可以配置用户使用打印机的访问权限。

如何在管理控制台(MMC)中配置用户对存储设备上的数据的访问权限

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**策略**”。
3. 选择必要的策略并双击以打开策略属性。
4. 在策略窗口中，选择 **安全控制** → **设备控制**。
5. 在“**设备控制设置**”下，选择“**设备类型**”选项卡。

   “**设备类型**”选项卡显示包含在设备控制分类的所有设备的访问规则。
6. 要配置存储设备访问规则，请双击打开规则列表。
7. 配置存储设备访问规则：

   a. 在“**访问规则**”块中单击“**添加**”按钮。

      这将打开添加新存储设备访问规则的窗口。

   b. 在“**规则优先级**”字段，设置*规则写入*优先级。规则包含以下属性：用户账户、计划、权限（读/写）和优先级。

      规则具有特定优先级。如果用户被添加到若干组，Kaspersky Endpoint Security 基于具有最高优先级的规则规范设备访问。Kaspersky Endpoint Security 允许您分配 0 到 10000 的优先级。值越高，优先级越高。也就是说，0 值具有最低优先级。

例如，您可以授予只读权限到 Everyone 组并授予读/写权限到管理员组。为此，给管理员组分配优先级 1，给 Everyone 组分配优先级 0。

阻止规则的优先级高于允许规则的优先级。换句话说，如果一个用户被添加到若干组且所有规则的优先级一样，Kaspersky Endpoint Security 基于任何现有的阻止规则规范设备访问。

c. 在“**用户和组规则**”下，选择用户或用户组。您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

d. 单击“**正常**”。

8. 在“**所选访问规则的计划**”下，为用户配置存储设备访问计划。

   例如，您可以允许用户仅在工作时间使用存储设备。

9. 在文件管理器中配置用户对存储设备的访问权限（**读取/写入**）。

10. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中配置用户对存储设备上数据的访问权限

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **安全控制** → **设备控制**。

5. 在“**设备访问规则**”块，在访问规则表中，打开存储设备访问规则的属性。

6. 在“**设备访问规则**”块中，选择“**自定义**”。

7. 配置存储设备访问规则：

   a. 在“**用户及其权限**”块中单击“**添加**”按钮。

   这将打开添加新存储设备访问规则的窗口。

   b. 在“**优先级**”字段，设置*规则写入*优先级。规则包含以下属性：用户账户、计划、权限（读/写）和优先级。

   规则具有特定优先级。如果用户被添加到若干组，Kaspersky Endpoint Security 基于具有最高优先级的规则规范设备访问。Kaspersky Endpoint Security 允许您分配 0 到 10000 的优先级。值越高，优先级越高。也就是说，0 值具有最低优先级。

   例如，您可以授予只读权限到 Everyone 组并授予读/写权限到管理员组。为此，给管理员组分配优先级 1，给 Everyone 组分配优先级 0。

   阻止规则的优先级高于允许规则的优先级。换句话说，如果一个用户被添加到若干组且所有规则的优先级一样，Kaspersky Endpoint Security 基于任何现有的阻止规则规范设备访问。

   c. 在“**用户或组**”下，选择用户或用户组。您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

   d. 在“**访问计划**”下，为用户配置存储设备访问计划。

   例如，您可以允许用户仅在工作时间使用存储设备。

e. 在文件管理器中配置用户对存储设备的访问权限（**读取/写入**）。

f. 单击“**保存**”。

8. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在应用程序界面中配置用户对存储设备上数据的访问权限

1. 打开主应用程序窗口并单击 按钮。

2. 在应用程序设置窗口中，选择“**安全控制**” → “**设备控制**”。

3. 在“**访问设置**”区域，单击“**设备和 Wi-Fi 网络**”链接。
   该表列出了设备控制组件分类中存在的所有设备的访问规则。

4. 要配置存储设备访问规则，请右键单击打开规则列表。

5. 配置存储设备访问规则：

   a. 在“**用户权限**”块中单击“**添加**”按钮。
   这将打开添加新存储设备访问规则的窗口。

   b. 在“**优先级**”字段，设置*规则写入*优先级。规则包含以下属性：用户账户、计划、权限（读/写）和优先级。
   规则具有特定优先级。如果用户被添加到若干组，Kaspersky Endpoint Security 基于具有最高优先级的规则规范设备访问。Kaspersky Endpoint Security 允许您分配 0 到 10000 的优先级。值越高，优先级越高。也就是说，0 值具有最低优先级。
   例如，您可以授予只读权限到 Everyone 组并授予读/写权限到管理员组。为此，给管理员组分配优先级 1，给 Everyone 组分配优先级 0。
   阻止规则的优先级高于允许规则的优先级。换句话说，如果一个用户被添加到若干组且所有规则的优先级一样，Kaspersky Endpoint Security 基于任何现有的阻止规则规范设备访问。

   c. 在“**用户**”下，选择用户或用户组。您可以在 Active Directory 中选择用户或手动输入本地用户名。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

   d. 单击“**确定**”。

6. 在“**设备访问计划**”下，为用户配置存储设备访问计划。
   例如，您可以允许用户仅在工作时间使用存储设备。

7. 在文件管理器中配置用户对存储设备的访问权限（**读取/写入**）。

8. 保存更改。

区分用户对受信任设备的访问权限

*受信任的设备*是指在受信任设备设置中指定的用户可随时进行完全访问的设备。要使用受信任设备，您可以为单个用户、一组用户或组织的所有用户授予访问权限。您可以在受信任设备属性中配置用户访问权限。

管理对移动设备的访问

Kaspersky Endpoint Security 允许您控制对运行 Android 和 iOS 的移动设备上的数据的访问。移动设备属于便携式设备 (MTP) 类别。因此，要配置对移动设备的数据访问，您需要编辑便携式设备（MTP）的访问设置。

当某个移动设备连接到计算机时，操作系统会确定设备类型。如果计算机上安装了 Android Debug Bridge(ADB)、iTunes 或其等效应用程序，操作系统会将移动设备识别为 ADB 或 iTunes 设备。在所有其他情况下，操作系统可能将移动设备类型识别为用于文件传输的便携式设备 (MTP)、用于图像传输的 PTP 设备（相机）或其他设备。设备类型取决于移动设备的型号和所选的 USB 连接模式。Kaspersky Endpoint Security 允许您在 ADB 应用程序、iTunes 或文件管理器中为移动设备上的数据配置单独的访问权限。在所有其他情况下，设备控制允许根据便携式设备（MTP）访问规则访问移动设备。

对移动设备的访问

移动设备属于便携式设备 (MTP) 类别，因此它们的设置相同。你可以选择以下访问移动设备的模式之一：

- **允许**。Kaspersky Endpoint Security 允许完全访问移动设备。您可以使用文件管理器或 ADB 和 iTunes 应用程序在移动设备上打开、创建、修改、复制或删除文件。您还可以通过将移动设备连接到计算机的 USB 端口来为设备的电池充电。
- **阻止**。Kaspersky Endpoint Security 在文件管理器以及 ADB 和 iTunes 应用程序中限制对移动设备的访问。该应用程序只允许访问受信任的移动设备。您还可以通过将移动设备连接到计算机的 USB 端口来为设备的电池充电。
- **取决于连接总线**。Kaspersky Endpoint Security 允许根据 USB 连接状态（**允许**或**阻止**）连接到移动设备。
- **根据规则**。Kaspersky Endpoint Security 根据规则限制对移动设备的访问。在规则中，您可以配置访问权限（读/写），选择可以访问移动设备的用户或用户组，并配置移动设备的访问计划。您还可以限制通过 ADB 和 iTunes 应用程序对移动设备数据的访问。

配置移动设备访问规则

便携式设备（MTP）、ADB 设备和 iTunes 设备的访问规则配置不同。对于便携式设备（MTP）和 ADB 设备，您可以为单个用户或用户组配置规则，并为规则的应用时间创建时间表。对于 iTunes 设备，您不能这样做。您只能允许或拒绝所有用户通过 iTunes 应用程序访问数据。

如何在管理控制台（MMC）中配置移动设备访问规则

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **安全控制** → **设备控制**。
4. 在“**设备控制设置**”下，选择“**设备类型**”选项卡。

   该表列出了设备控制组件分类中存在的所有设备的访问规则。

5. 在上下文菜单中，对于“**便携式设备(MTP)**”设备类型，配置移动设备访问模式：**允许**、**阻止**或者**取决于连接总线**。

6. 要配置移动设备访问规则，请双击打开规则列表。

7. 配置移动设备访问规则：

   a. 在“**访问规则**”块中单击“**添加**”按钮。

      这将打开添加新移动设备访问规则的窗口。

   b. 在“**优先级**”字段，设置规则写入优先级。规则包含以下属性：用户账户、计划、权限（读/写/ADB 访问）和优先级。

      规则具有特定优先级。如果用户被添加到若干组，Kaspersky Endpoint Security 基于具有最高优先级的规则规范设备访问。Kaspersky Endpoint Security 允许您分配 0 到 10000 的优先级。值越高，优先级越高。也就是说，0 值具有最低优先级。

      例如，您可以授予只读权限到 Everyone 组并授予读/写权限到管理员组。为此，给管理员组分配优先级 1，给 Everyone 组分配优先级 0。

      阻止规则的优先级高于允许规则的优先级。换句话说，如果一个用户被添加到若干组且所有规则的优先级一样，Kaspersky Endpoint Security 基于任何现有的阻止规则规范设备访问。

   c. 在“**用户和组规则**”下，选择用户或用户组。您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

   d. 单击“**确定**”。

8. 在“**所选访问规则的计划**”下，为用户配置移动设备访问计划。

   无法为 ADB 设备配置单独的访问计划。您可以为 ADB 设备和便携式设备 (MTP) 配置通用访问计划。

9. 在文件管理器中配置用户对移动设备的访问权限（**读取 / 写入**）。

10. 使用“**通过 ADB 访问**”复选框配置通过 ADB 应用程序对移动设备上数据的访问。

    如果清除该复选框，当连接移动设备时，ADB 应用程序将无法检测到该设备。

11. 在“**通过 iTunes 访问**”下，配置通过 iTunes 应用程序对移动设备上数据的访问。

    Kaspersky Endpoint Security 通过 iTunes 应用程序为所有用户应用移动设备访问设置。无法为 iTunes 设备配置单独的访问计划。

12. 保存更改。

如何在 Web Console 和云控制台中配置移动设备访问规则

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **安全控制** → **设备控制**。

5. 在“**设备访问规则**”区域，单击“**设备和 Wi-Fi 网络**”链接。

   该表列出了设备控制组件分类中存在的所有设备的访问规则。

6. 选择“**便携式设备(MTP)**”设备类型。

   这将打开便携式设备 (MTP) 访问权限。

7. 配置移动设备访问模式：**允许**、**阻止**、**取决于总线**或者**自定义**。

8. 使用“**所有用户都可以通过 iTunes 访问已启用**”切换开关，配置通过 iTunes 应用程序对移动设备上数据的访问。

   > Kaspersky Endpoint Security 通过 iTunes 应用程序为所有用户应用移动设备访问设置。无法为 iTunes 设备配置单独的访问计划。

9. 如果您选择“**自定义**”模式，则必须为设备添加访问规则。为此，在“**用户及其权限**”下，单击“**添加**”按钮并配置移动设备访问规则：

   a. 在“**优先级**”字段，设置规则写入优先级。规则包含以下属性：用户账户、计划、权限（读/写/ADB 访问）和优先级。

      规则具有特定优先级。如果用户被添加到若干组，Kaspersky Endpoint Security 基于具有最高优先级的规则规范设备访问。Kaspersky Endpoint Security 允许您分配 0 到 10000 的优先级。值越高，优先级越高。也就是说，0 值具有最低优先级。

      例如，您可以授予只读权限到 Everyone 组并授予读/写权限到管理员组。为此，给管理员组分配优先级 1，给 Everyone 组分配优先级 0。

      阻止规则的优先级高于允许规则的优先级。换句话说，如果一个用户被添加到若干组且所有规则的优先级一样，Kaspersky Endpoint Security 基于任何现有的阻止规则规范设备访问。

   b. 在“**用户或组**”下，选择要访问移动设备的用户或用户组。您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

   c. 在“**访问计划**”下，为用户配置移动设备访问计划。

      > 无法为 ADB 设备配置单独的访问计划。您可以为 ADB 设备和便携式设备 (MTP) 配置通用访问计划。

   d. 在文件管理器中配置用户对移动设备的访问权限（**读取 / 写入**）。

   e. 使用“**通过 ADB 访问**”复选框配置通过 ADB 应用程序对移动设备上数据的访问。

      如果清除该复选框，当连接移动设备时，ADB 应用程序将无法检测到该设备。

10. 保存更改。

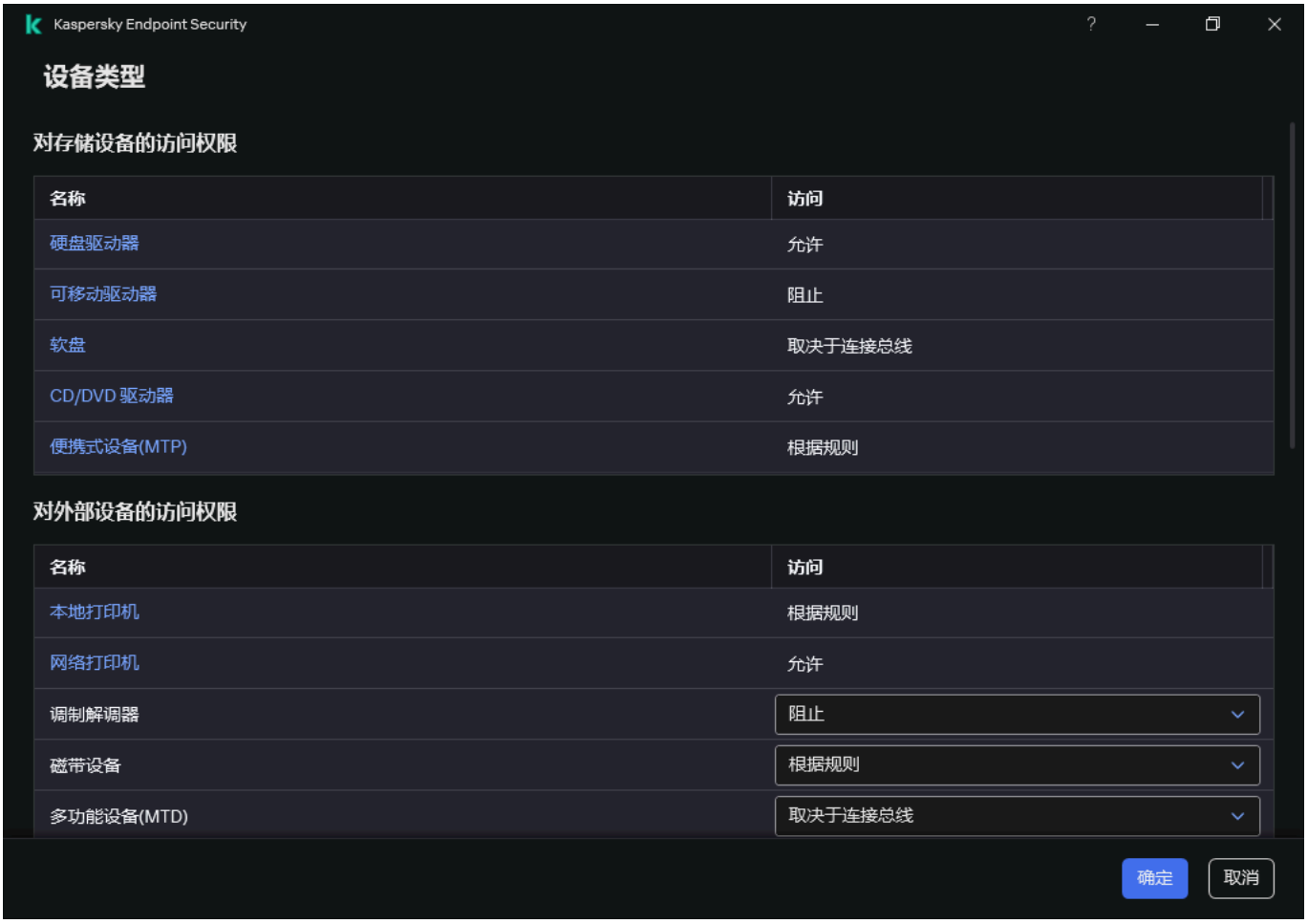
如何在应用程序界面中配置移动设备访问规则

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**安全控制**” → “**设备控制**”。

3. 在“**访问设置**”块中单击“**设备和 Wi-Fi 网络**”按钮。

打开的窗口显示包含在设备控制组件分类的所有设备的访问规则。



设备控制组件中的设备类型

4. 在“**对存储设备的访问权限**”区域，单击“**便携式设备(MTP)**”链接。

   这将打开一个包含便携式设备 (MTP) 访问规则的窗口。

5. 在“**访问**”下，配置移动设备访问模式：**允许**、**阻止**、**取决于连接总线**或者**根据规则**。

6. 如果您选择“**根据规则**”模式，则必须为设备添加访问规则：

   a. 在“**用户权限**”块中单击“**添加**”按钮。

      这将打开添加新移动设备访问规则的窗口。

   b. 在“**优先级**”字段，设置规则写入优先级。规则包含以下属性：用户账户、计划、权限（读/写/ADB 访问）和优先级。

      规则具有特定优先级。如果用户被添加到若干组，Kaspersky Endpoint Security 基于具有最高优先级的规则规范设备访问。Kaspersky Endpoint Security 允许您分配 0 到 10000 的优先级。值越高，优先级越高。也就是说，0 值具有最低优先级。

      例如，您可以授予只读权限到 Everyone 组并授予读/写权限到管理员组。为此，给管理员组分配优先级 1，给 Everyone 组分配优先级 0。

      阻止规则的优先级高于允许规则的优先级。换句话说，如果一个用户被添加到若干组且所有规则的优先级一样，Kaspersky Endpoint Security 基于任何现有的阻止规则规范设备访问。

   c. 在“**状态**”下，打开移动设备访问规则。

d. 在“**访问规则**”下，为用户配置移动设备访问权限。

- 在文件管理器中配置用户对移动设备的访问权限（**读取 / 写入**）。
- 使用“**通过 ADB 访问**”复选框配置通过 ADB 应用程序对移动设备上数据的访问。
  如果清除该复选框，当连接移动设备时，ADB 应用程序将无法检测到该设备。

e. 在“**用户**”下，选择要访问移动设备的用户或用户组。您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

f. 在“**设备访问计划**”下，为用户配置设备访问计划。

> 无法为 ADB 设备配置单独的访问计划。您可以为 ADB 设备和便携式设备 (MTP) 配置通用访问计划。

g. 在“**通过 iTunes 访问**”下，配置通过 iTunes 应用程序对移动设备上数据的访问。

> Kaspersky Endpoint Security 通过 iTunes 应用程序为所有用户应用移动设备访问设置。无法为 iTunes 设备配置单独的访问计划。

7. 保存更改。

因此，用户对移动设备的访问会根据规则受到限制。如果您在 ADB 和 iTunes 应用程序中禁止访问移动设备，当您连接移动设备时，ADB 和 iTunes 应用程序将无法检测到该移动设备。

受信任的移动设备

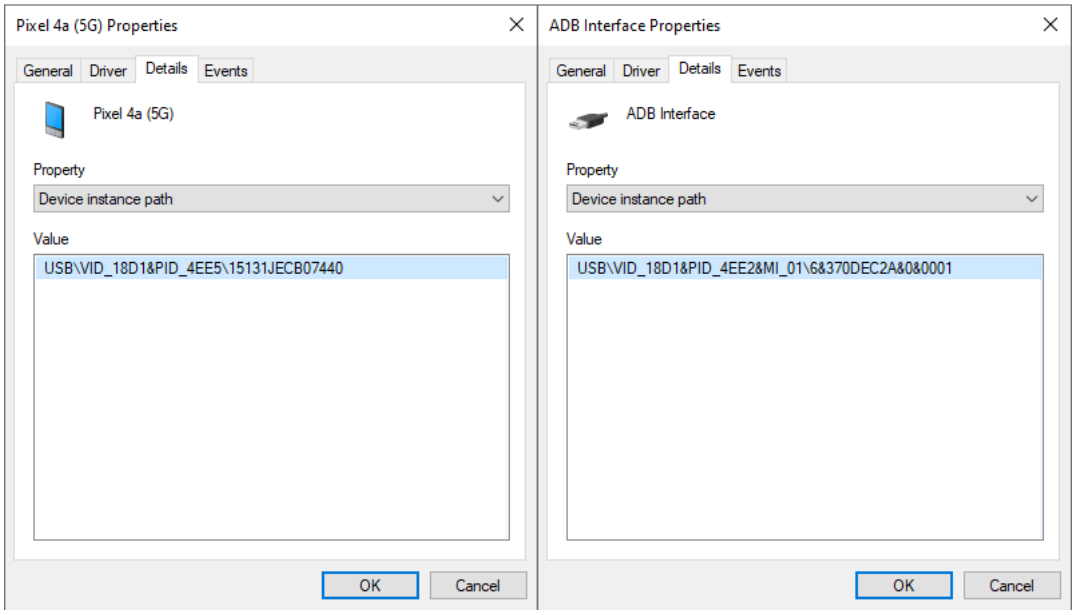
*受信任的设备*是指在受信任设备设置中指定的用户可随时进行完全访问的设备。

添加受信任的移动设备的过程与添加其他类型的受信任设备完全相同。您可以按 ID 或设备型号添加移动设备。

要按 ID 添加受信任的移动设备，您需要一个唯一的 ID（Hardware ID – HWID）。您可以使用操作系统工具在设备属性中找到 ID（参见下图）。设备管理器工具允许您执行此操作。便携式设备（MTP）和 ADB、iTunes 设备的 ID 即使对于相同的移动设备也是不同的。便携式设备 (MTP) 的 ID 可能如下所示： `15131JECB07440`。ADB 设备的 ID 可能如下所示： `6&370DEC2A&0&0001`。如果要添加多个特定设备，则按 ID 添加设备很方便。您也可以使用掩码。

> 如果在将设备连接到计算机后安装了 ADB 或 iTunes 应用程序，则该设备的唯一 ID 可能会重置。这意味着 Kaspersky Endpoint Security 会将此设备识别为新设备。如果该设备受信任，请再次将其添加到受信任列表。

要按设备型号添加受信任的移动设备，您需要其Vendor ID（VID）和Product ID（PID）。您可以使用操作系统工具在设备属性中找到 ID（参见下图）。用于输入 VID 和 PID 的模板：`VID_18D1&PID_4EE5`。如果在组织中使用特定型号的设备，则按型号添加设备很方便。这样，您可以添加该型号的所有设备。



设备管理器中的设备 ID

管理对蓝牙设备的访问

Kaspersky Endpoint Security 允许管理对蓝牙设备的访问。蓝牙设备包括无线键盘、鼠标、耳机、打印机等。您还可以使用蓝牙进行通信，例如使用移动设备。

当蓝牙设备连接或断开连接时，应用程序可能会创建有关该设备的多个事件。原因是操作系统可能会将一个蓝牙设备检测为多个不同类型的设备。Kaspersky Endpoint Security 还管理蓝牙适配器，通过该适配器将设备作为单独的设备进行连接。这就是应用程序为每个检测到的设备创建事件的原因。

您可以选择以下访问移动设备的模式之一：

- **允许且不记录**。Kaspersky Endpoint Security 允许连接任何蓝牙设备，并且不会在事件日志中保存有关连接的信息。您可以连接蓝牙输入设备（键盘、鼠标等）、通过蓝牙发送数据、管理其他蓝牙设备（耳机等）。
- **允许**。Kaspersky Endpoint Security 允许连接任何蓝牙设备。您可以连接蓝牙输入设备（键盘、鼠标等）、通过蓝牙发送数据、管理其他蓝牙设备（耳机等）。
- **阻止**。Kaspersky Endpoint Security 限制对蓝牙设备的访问。您可以仅允许连接蓝牙输入设备（即“Human Interface Devices”类）。这些设备包括键盘、鼠标、操纵杆等。

无法创建受信任的蓝牙设备列表。如果您对蓝牙设备的访问受到限制，则只能连接蓝牙输入设备。

如何在管理控制台（MMC）中配置移动设备访问规则

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**策略**”。

3. 选择必要的策略并双击以打开策略属性。

4. 在策略窗口中，选择 **安全控制** → **设备控制**。

5. 在“**设备控制设置**”下，选择“**设备类型**”选项卡。
   该表列出了设备控制组件分类中存在的所有设备的访问规则。

6. 在“**蓝牙**”设备类型的上下文菜单中，配置蓝牙设备访问模式：**允许**、**阻止**或者**允许且不记录**。

7. 如果您选择**阻止**模式，您可以只允许连接蓝牙输入设备（键盘、鼠标等）。为此，在“**排除项**”下，选择“**输入设备(鼠标和键盘)**”复选框。

8. 要将此策略应用到计算机，请关闭挂锁图标并保存更改。

如何在 Web Console 和云控制台中配置蓝牙设备访问规则

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **安全控制** → **设备控制**。

5. 在“**设备访问规则**”区域，单击“**设备和 Wi-Fi 网络**”链接。
   该表列出了设备控制组件分类中存在的所有设备的访问规则。

6. 选择“**蓝牙设备**”设备类型。
   这将打开蓝牙设备访问设置。

7. 配置蓝牙设备访问模式：**允许**, **阻止**, **允许且不记录**。

8. 如果您选择**阻止**模式，您可以只允许连接蓝牙输入设备（键盘、鼠标等）。为此，在“**排除项**”下，选择“**输入设备(鼠标和键盘)**”复选框。

9. 要将此策略应用到计算机，请关闭挂锁图标并保存更改。

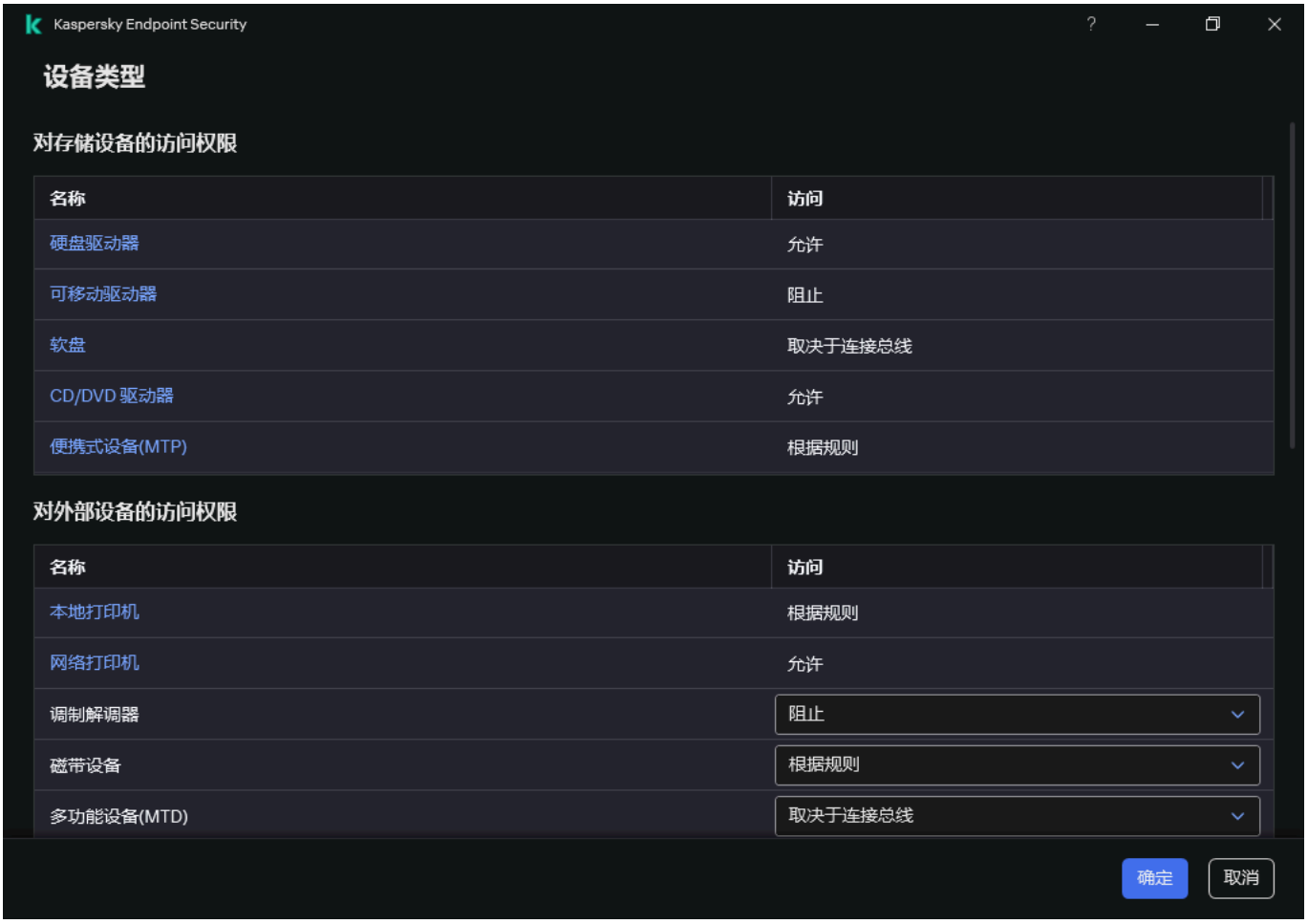
如何在应用程序界面中配置蓝牙设备访问规则

1. 打开主应用程序窗口并单击按钮。

2. 在应用程序设置窗口中，选择“**安全控制**” → “**设备控制**”。

3. 在“**访问设置**”块中单击“**设备和 Wi-Fi 网络**”按钮。

打开的窗口显示包含在设备控制组件分类的所有设备的访问规则。



设备控制组件中的设备类型

4. 在“**对外部设备的访问权限**”区域，单击“**蓝牙**”链接。
   这将打开蓝牙设备访问设置。

5. 在“**访问**”下，配置蓝牙设备访问模式：**允许**、**阻止**或者**允许且不记录**。

6. 如果您选择**阻止**模式，您可以只允许连接蓝牙输入设备（键盘、鼠标等）。为此，在“**排除项**”下，选择“**输入设备(鼠标和键盘)**”复选框。

7. 保存更改。

打印控制

基于 Arm 架构的计算机不支持打印控制。

您可以使用打印控制来配置用户对本地和网络打印机的访问。

本地打印机控制

Kaspersky Endpoint Security 允许在两个级别上配置对本地打印机的访问：*连接*和*打印*。

Kaspersky Endpoint Security 通过以下总线控制本地打印机连接：USB、串行端口（COM）、并行端口（LPT）。

> Kaspersky Endpoint Security 仅在总线级别控制本地打印机与 COM 和 LPT 端口的连接。因此，要阻止通过 COM 和 LPT 端口的打印机连接，您需要为本地打印机选择"取决于连接总线"访问模式并禁止连接到 COM 和 LPT 总线。

对于连接到 USB 的打印机，应用程序在两个级别上进行控制：设备类型（本地打印机）和连接总线（USB）。

你可以选择以下模式之一通过 USB 访问本地打印机：

- **允许**。Kaspersky Endpoint Security 向所有用户授予对本地打印机的完全访问权限。用户可以使用操作系统提供的方式连接打印机和打印文档。
- **阻止**。Kaspersky Endpoint Security 阻止本地打印机的连接。该应用程序仅允许连接受信任的打印机。
- **取决于连接总线**。Kaspersky Endpoint Security 允许根据USB 总线连接状态（**允许**或**阻止**）连接到本地打印机。
- **根据规则**。要控制打印，您必须添加*打印规则*。在规则中，您可以选择要允许或阻止在本地打印机上打印文档的用户或用户组。

网络打印机控制

Kaspersky Endpoint Security 允许配置对网络打印机上打印的访问。您可以选择以下网络打印机访问模式之一：

- **允许且不记录**。 Kaspersky Endpoint Security 不控制网络打印机上的打印。该应用程序向所有用户授予打印访问权限，并且不会将有关打印的信息保存到事件日志中。
- **允许**。Kaspersky Endpoint Security 向所有用户授予在网络打印机上打印的权限。
- **阻止**。Kaspersky Endpoint Security 限制所有用户访问网络打印机。该应用程序仅允许访问受信任的打印机。
- **根据规则**。Kaspersky Endpoint Security 根据打印规则授予打印访问权限。在规则中，您可以选择允许或禁止在网络打印机上打印文档的用户或用户组。

为打印机添加打印规则

如何在管理控制台 (MMC) 中添加打印规则

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **安全控制** → **设备控制**。

4. 在“**设备控制设置**”下，选择“**设备类型**”选项卡。
   该表列出了设备控制组件分类中存在的所有设备的访问规则。

5. 在“**本地打印机**”和“**网络打印机**”设备类型的上下文菜单中，配置相关打印机的访问模式：**允许**、**阻止**、**允许且不记录**（仅适用于网络打印机）或**取决于连接总线**（仅适用于本地打印机）。

6. 要在本地和网络打印机上配置打印规则，请双击规则列表以打开它们。

7. 选择“**根据规则**”作为打印机访问模式。

8. 选择您要应用打印规则的用户或用户组。

   a. 单击“**添加**”。
      这将打开添加新打印规则的窗口。

   b. 将优先级分配到规则条目。规则条目包括以下属性：用户账户、操作（允许/阻止）和优先级。
      规则具有特定优先级。如果用户被添加到若干组，Kaspersky Endpoint Security 基于具有最高优先级的规则规范设备访问。Kaspersky Endpoint Security 允许您分配 0 到 10000 的优先级。值越高，优先级越高。也就是说，0 值具有最低优先级。
      例如，您可以授予只读权限到 Everyone 组并授予读/写权限到管理员组。为此，给管理员组分配优先级 1，给 Everyone 组分配优先级 0。
      阻止规则的优先级高于允许规则的优先级。换句话说，如果一个用户被添加到若干组且所有规则的优先级一样，Kaspersky Endpoint Security 基于任何现有的阻止规则规范设备访问。

   c. 在“**操作**”下，配置用户对打印机打印的访问权限。

   d. 单击“**用户和组**”，选择要访问打印的用户或用户组。您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

   e. 单击“**确定**”。

9. 保存更改。

如何在 Web Console 和云控制台中添加打印规则

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **安全控制** → **设备控制**。

5. 在“**设备访问规则**”区域，单击“**设备和 Wi-Fi 网络**”链接。

   该表列出了设备控制组件分类中存在的所有设备的访问规则。

6. 选择“**本地打印机**”或者“**网络打印机**”设备类型。

   这将打开打印机访问规则。

7. 配置相关打印机的访问模式： **允许**、**阻止**、**允许且不记录**（仅适用于网络打印机）、**取决于总线** （仅适用于本地打印机）或**自定义**。

8. 如果您选择“**自定义**”模式，则必须为本地或网络打印机添加打印规则。若要执行此操作，请单击打印规则表格中的“**添加**”按钮。

   这将打开新打印规则的设置。

9. 将优先级分配到规则条目。规则条目包括以下属性：用户账户、操作（允许/阻止）和优先级。

   规则具有特定优先级。如果用户被添加到若干组，Kaspersky Endpoint Security 基于具有最高优先级的规则规范设备访问。Kaspersky Endpoint Security 允许您分配 0 到 10000 的优先级。值越高，优先级越高。也就是说，0 值具有最低优先级。

   例如，您可以授予只读权限到 Everyone 组并授予读/写权限到管理员组。为此，给管理员组分配优先级 1，给 Everyone 组分配优先级 0。

   阻止规则的优先级高于允许规则的优先级。换句话说，如果一个用户被添加到若干组且所有规则的优先级一样，Kaspersky Endpoint Security 基于任何现有的阻止规则规范设备访问。

10. 在“**操作**”下，配置用户对打印机打印的访问权限。

11. 在“**用户或组**”下，选择要访问打印的用户或用户组。您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

12. 保存更改。

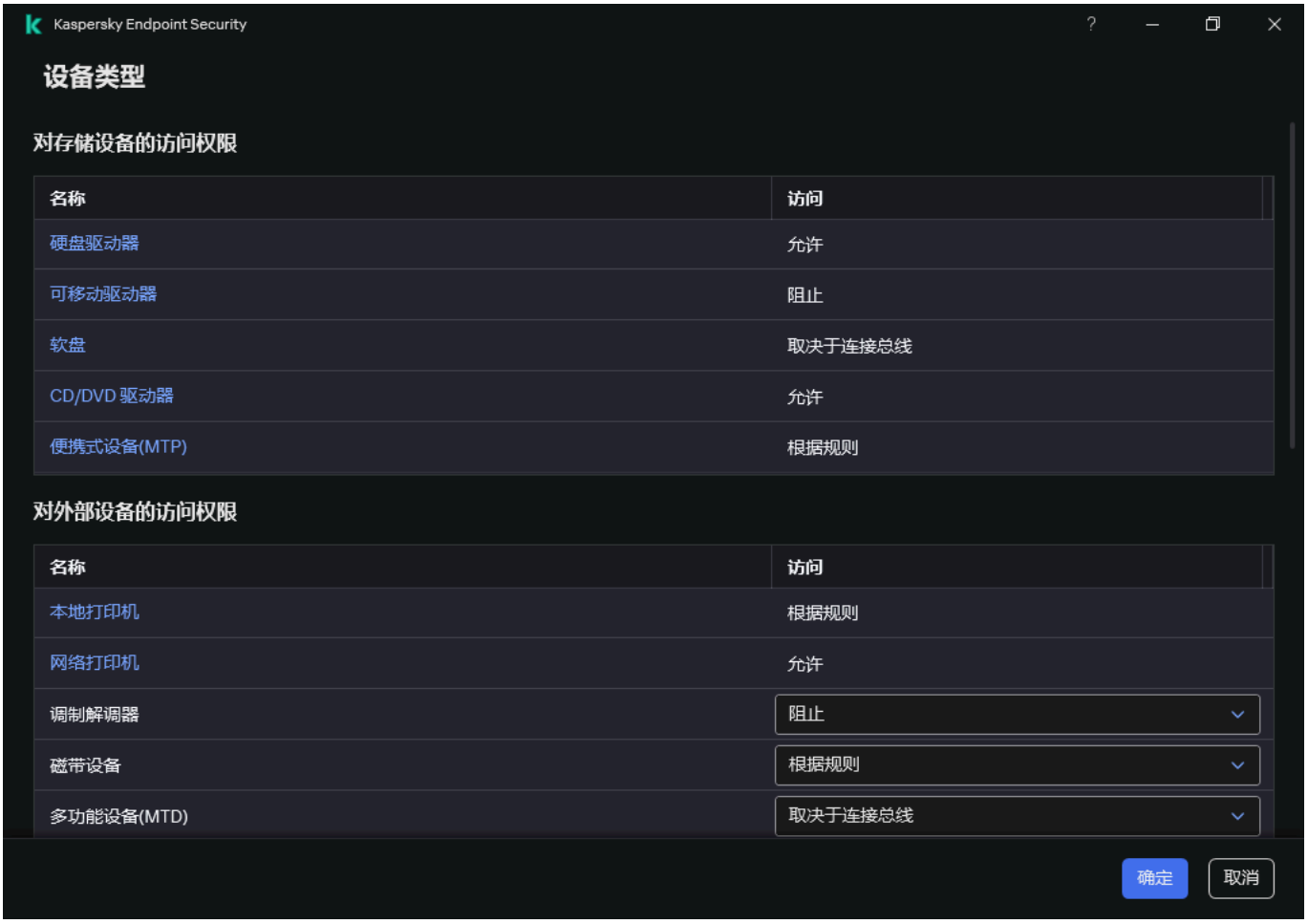
如何在应用程序界面中添加打印规则

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**安全控制**” → “**设备控制**”。

3. 在“**访问设置**”块中单击“**设备和 Wi-Fi 网络**”按钮。

打开的窗口显示包含在设备控制组件分类的所有设备的访问规则。



设备控制组件中的设备类型

4. 在“**对外部设备的访问权限**”下，单击“**本地打印机**”或者“**网络打印机**”。

   这将打开打印机访问规则窗口。

5. 在**访问本地打印机**或者**访问网络打印机**下，配置打印机的访问模式：**允许**、**阻止**、**允许且不记录**（仅适用于网络打印机）、**取决于连接总线**（仅适用于本地打印机）或**根据规则**。

6. 如果您选择“**根据规则**”模式，则必须为打印机添加打印规则。选择您要应用打印规则的用户或用户组。

   a. 单击“**添加**”。

      这将打开添加新打印规则的窗口。

   b. 将优先级分配到规则条目。规则条目包括以下属性：用户账户、权限（允许/阻止）和优先级。

      规则具有特定优先级。如果用户被添加到若干组，Kaspersky Endpoint Security 基于具有最高优先级的规则规范设备访问。Kaspersky Endpoint Security 允许您分配 0 到 10000 的优先级。值越高，优先级越高。也就是说，0 值具有最低优先级。

      例如，您可以授予只读权限到 Everyone 组并授予读/写权限到管理员组。为此，给管理员组分配优先级 1，给 Everyone 组分配优先级 0。

      阻止规则的优先级高于允许规则的优先级。换句话说，如果一个用户被添加到若干组且所有规则的优先级一样，Kaspersky Endpoint Security 基于任何现有的阻止规则规范设备访问。

c. 在“**操作**”下，配置用户访问打印的权限。

d. 在“**用户和组**”下，选择要访问打印的用户或用户组。您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

7. 保存更改。

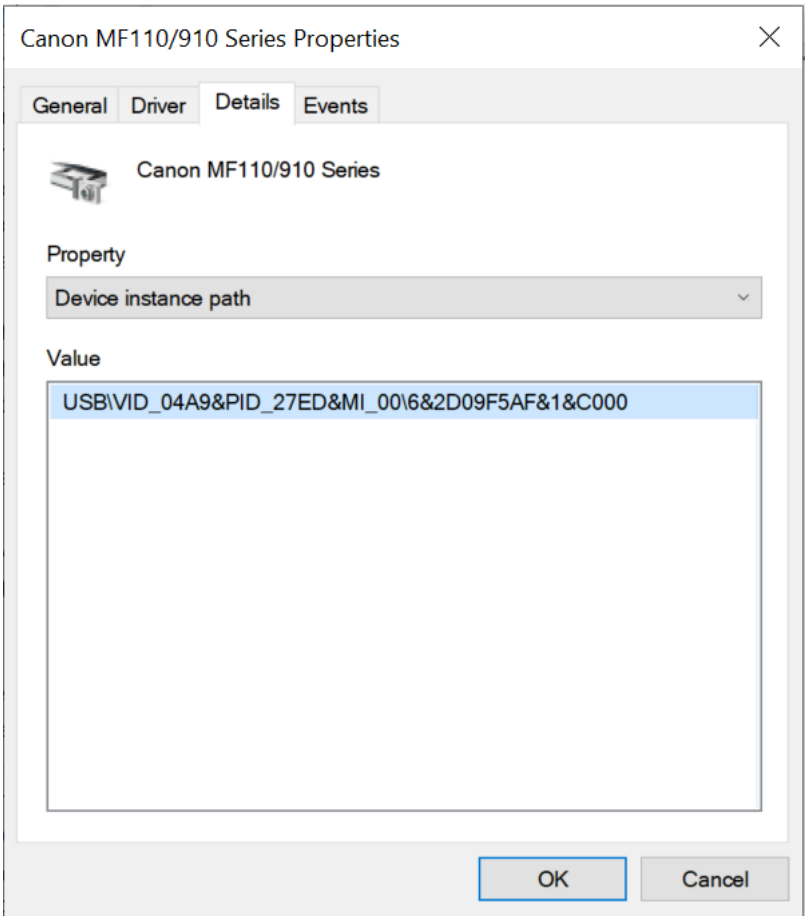
受信任的打印机

*受信任的设备*是指在受信任设备设置中指定的用户可随时进行完全访问的设备。

添加受信任打印机的过程与添加其他类型的受信任设备完全相同。您可以按 ID 或设备型号添加本地打印机。您只能按设备 ID 添加网络打印机。

要按 ID 添加受信任的本地打印机，您需要一个唯一的 ID（Hardware ID – HWID）。您可以使用操作系统工具在设备属性中找到 ID（参见下图）。Device Manager工具允许您执行此操作。本地打印机的 ID 可能如下所示：`6&2D09F5AF&1&C000`。如果要添加多个特定设备，则按 ID 添加设备很方便。您也可以使用掩码。

要按设备型号添加受信任的本地打印机，您需要其Vendor ID（VID）和Product ID（PID）。您可以使用操作系统工具在设备属性中找到 ID（参见下图）。用于输入 VID 和 PID 的模板：`VID_04A9&PID_27FD`。如果在组织中使用特定型号的设备，则按型号添加设备很方便。这样，您可以添加该型号的所有设备。



设备管理器中的设备 ID

要添加受信任的网络打印机，您需要其设备 ID。对于网络打印机，设备 ID 可以是打印机的网络名称（共享打印机的名称）、打印机的 IP 地址或打印机的 URL。

Wi-Fi 连接控制

设备控制允许管理计算机（笔记本电脑）的 Wi-Fi 连接。公共 Wi-Fi 网络可能不安全，使用此类网络可能会导致数据丢失。设备控制允许您阻止用户连接到 Wi-Fi 或仅允许连接到受信任的网络。例如，您可以只允许连接到足够安全的公司 Wi-Fi 网络。设备控制将阻止访问除受信任列表中指定的 Wi-Fi 网络之外的所有网络。

在运行 Windows 11 的计算机上，您需要启用定位服务才能控制 Wi-Fi 连接。为此，您需要启用操作系统设置中的"**定位服务**"开关（**设置** → **隐私&安全** → **位置**）。如果禁用定位服务，Kaspersky Endpoint Security 将不会控制与 Wi-Fi 网络的连接。

如何在管理控制台 (MMC) 中限制 Wi-Fi 连接

1. 在 Kaspersky Security Center 管理控制台树中，选择"**策略**"。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **安全控制** → **设备控制**。
4. 在"**设备控制设置**"下，选择"**设备类型**"选项卡。

   该表列出了设备控制组件分类中存在的所有设备的访问规则。
5. 在"**Wi-Fi**"设备类型的上下文菜单中，选择连接到 Wi-Fi 时执行的设备控制操作：**允许**（✓）、**阻止**（⊘）或**阻止但带有例外**（）。
6. 如果您选择了"**阻止但带有例外**"选项，请创建受信任的 Wi-Fi 网络列表：

   a. 双击打开受信任的 Wi-Fi 网络列表。

   b. 在"**受信任的 Wi-Fi 网络**"块中单击"**添加**"按钮。

   c. 这将打开一个窗口；在该窗口中，配置受信任的 Wi-Fi 网络（参见下图）：

   - "**网络名称**"。Wi-Fi 网络的名称或 SSID（Service Set Identifier）。
   - "**身份验证类型**"。连接到 Wi-Fi 网络时使用的身份验证类型。

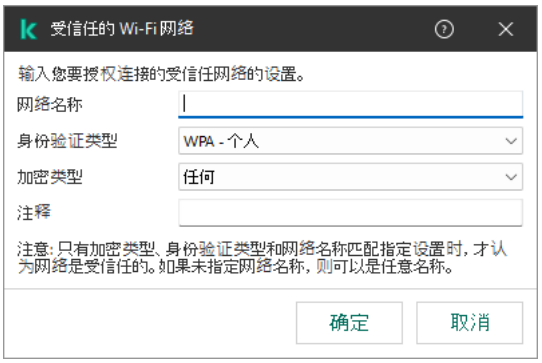
     从 Kaspersky Endpoint Security for Windows 版本 12.0 开始，WPA3 协议支持已添加到应用程序中。如果在计算机上应用 Kaspersky Endpoint Security 12.2 版策略，则在 Kaspersky Endpoint Security 11.11.0 及更早版本的计算机上选择 WPA2 协议；12.0 到 12.1 版本选择 WPA2 / WPA3；12.2 及更高版本选择 WPA3。

   - "**加密类型**"。用于保护 Wi-Fi 流量的加密类型。
   - "**注释**"。有关添加的 Wi-Fi 网络的更多信息。

   您可以在路由器设置中查看受信任的 Wi-Fi 网络的设置。

   如果某个 Wi-Fi 网络的设置匹配规则中指定的所有设置则其被认定为受信任。

7. 保存更改。



受信任的 Wi-Fi 网络设置

如何在 Web Console 和云控制台中限制 Wi-Fi 连接

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **安全控制** → **设备控制**。

5. 在“**设备访问规则**”下，选择“**设备和 Wi-Fi 网络**”选项卡。
   该表列出了设备控制组件分类中存在的所有设备的访问规则。

6. 在“**Wi-Fi 网络**”区域，单击“**Wi-Fi**”链接。

7. 在打开的窗口中，选择连接到 Wi-Fi 时采取的设备控制操作：**允许**、**阻止**或**阻止但带有排除项**。

8. 如果您选择了“**阻止但带有排除项**”选项，请创建受信任的 Wi-Fi 网络列表：

   a. 双击打开受信任的 Wi-Fi 网络列表。

   b. 在“**受信任的 Wi-Fi 网络**”块中单击“**添加**”按钮。

   c. 这将打开一个窗口；在该窗口中，配置受信任的 Wi-Fi 网络（参见下图）：

   - “**名称**”。Wi-Fi 网络的名称或 SSID（Service Set Identifier）。
   - “**身份验证类型**”。连接到 Wi-Fi 网络时使用的身份验证类型。

     > 从 Kaspersky Endpoint Security for Windows 版本 12.0 开始，WPA3 协议支持已添加到应用程序中。如果在计算机上应用 Kaspersky Endpoint Security 12.2 版策略，则在 Kaspersky Endpoint Security 11.11.0 及更早版本的计算机上选择 WPA2 协议；12.0 到 12.1 版本选择 WPA2 / WPA3；12.2 及更高版本选择 WPA3。

   - “**加密类型**”。用于保护 Wi-Fi 流量的加密类型。
   - “**注释**”。有关添加的 Wi-Fi 网络的更多信息。

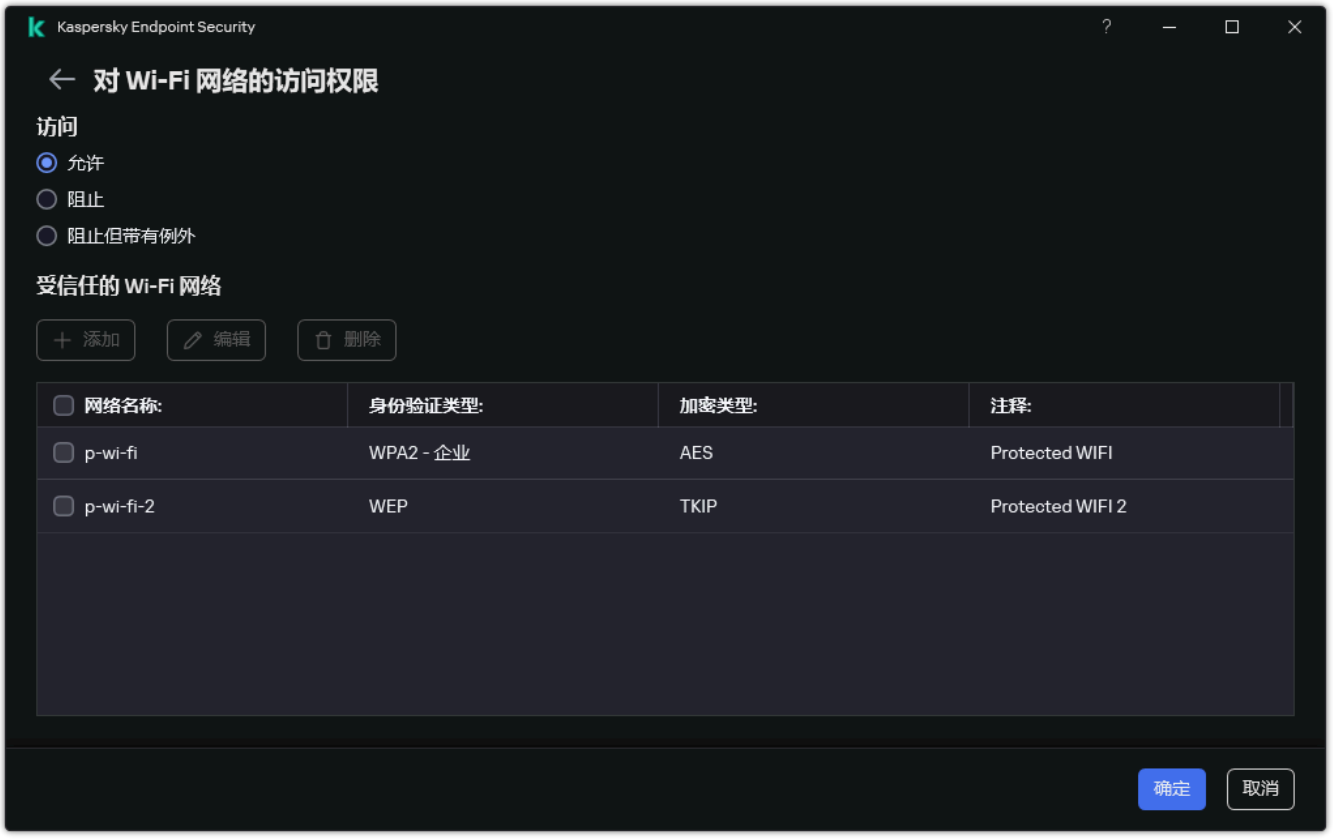
   您可以在路由器设置中查看受信任的 Wi-Fi 网络的设置。

如果某个 Wi-Fi 网络的设置匹配规则中指定的所有设置则其被认定为受信任。

9. 保存更改。

如何在应用程序界面中限制 Wi-Fi 连接

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**安全控制**” → “**设备控制**”。
3. 在“**访问设置**”块中单击“**设备和 Wi-Fi 网络**”按钮。
   打开的窗口显示包含在设备控制组件分类的所有设备的访问规则。
4. 在“**对 Wi-Fi 网络的访问权限**”区域，单击“**Wi-Fi**”链接。
   打开的窗口显示 Wi-Fi 网络访问规则。



Wi-Fi 访问设置

5. 在“**访问**”中，选择连接到 Wi-Fi 时采取的设备控制操作：**允许**、**阻止**或**阻止但带有例外**。

6. 如果您选择了“**阻止但带有例外**”选项，请创建受信任的 Wi-Fi 网络列表：

   a. 在“**受信任的 Wi-Fi 网络**”块中单击“**添加**”按钮。

   b. 这将打开一个窗口；在该窗口中，配置受信任的 Wi-Fi 网络（参见下图）：

   - “**网络名称**”。Wi-Fi 网络的名称或 SSID（Service Set Identifier）。
   - “**身份验证类型**”。连接到 Wi-Fi 网络时使用的身份验证类型。

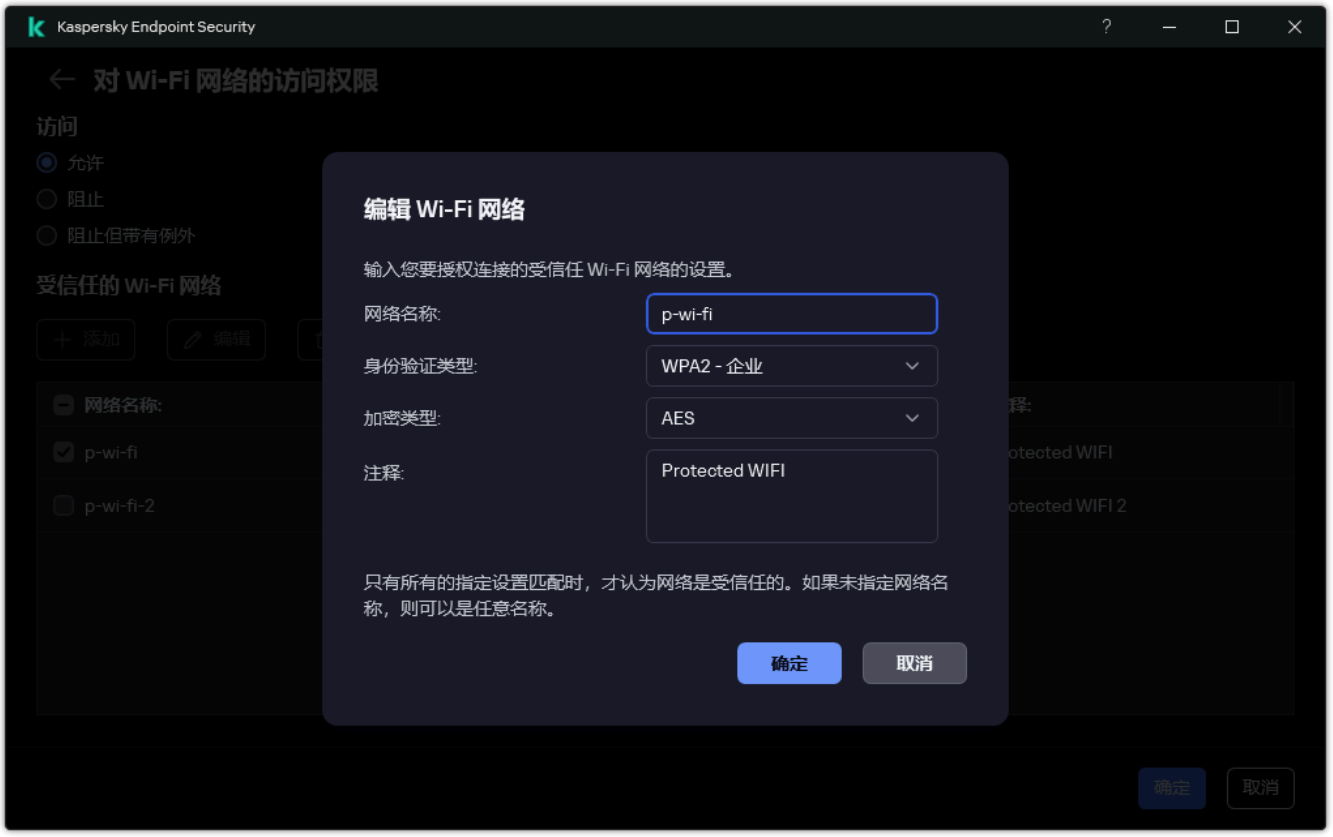
     > 从 Kaspersky Endpoint Security for Windows 版本 12.0 开始，WPA3 协议支持已添加到应用程序中。如果在计算机上应用 Kaspersky Endpoint Security 12.2 版策略，则在 Kaspersky Endpoint Security 11.11.0 及更早版本的计算机上选择 WPA2 协议；12.0 到 12.1 版本选择 WPA2 / WPA3；12.2 及更高版本选择 WPA3。

   - “**加密类型**”。用于保护 Wi-Fi 流量的加密类型。
   - “**注释**”。有关添加的 Wi-Fi 网络的更多信息。

   您可以在路由器设置中查看受信任的 Wi-Fi 网络的设置。

   > 如果某个 Wi-Fi 网络的设置匹配规则中指定的所有设置则其被认定为受信任。

7. 保存更改。



受信任的 Wi-Fi 网络设置

因此，当用户尝试连接到未列为受信任的 Wi-Fi 网络时，应用程序会阻止连接并显示通知（参见下图）。

"设备控制"通知

监控可移动驱动器的使用

监控可移动驱动器的使用包括：

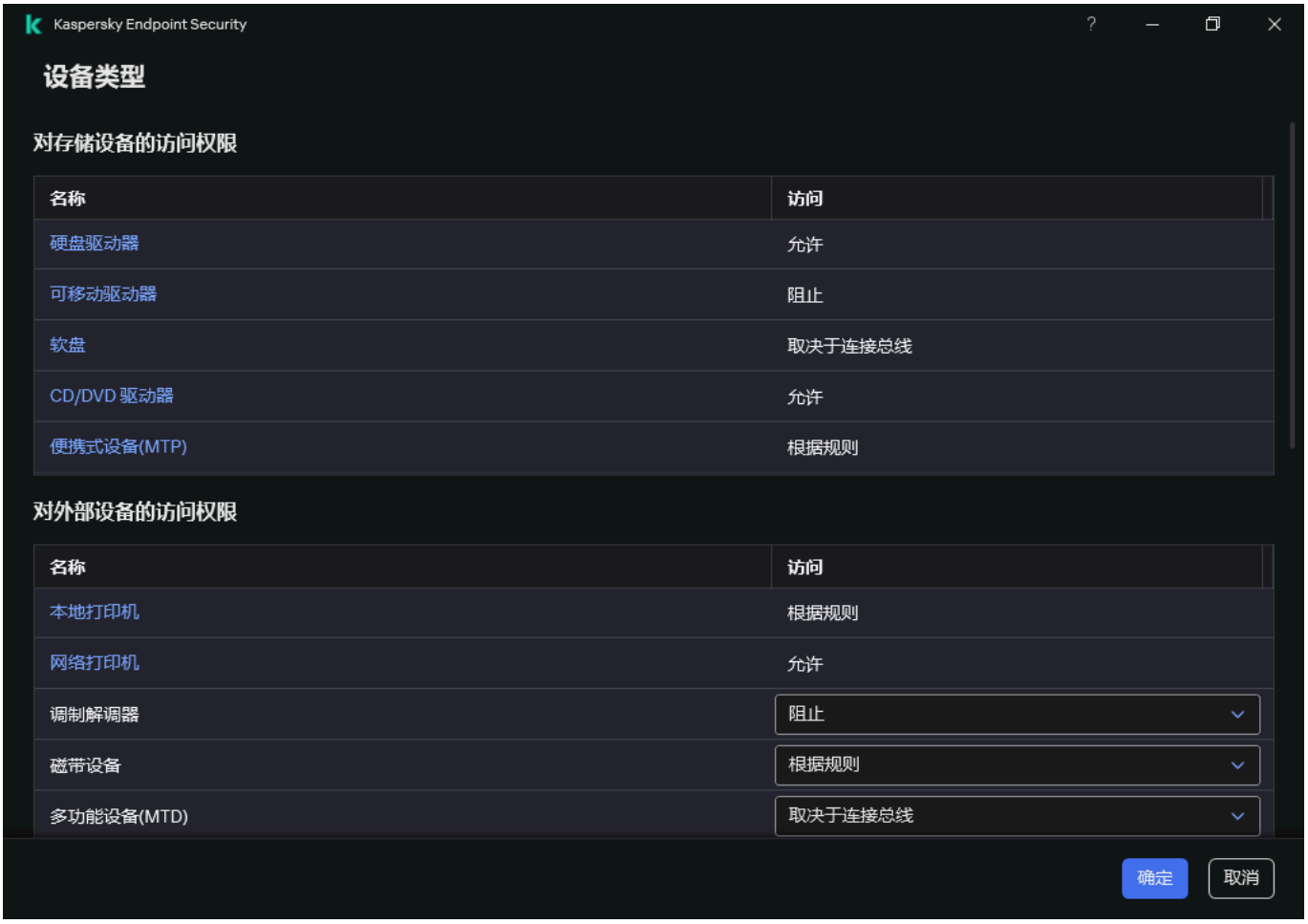
- 监控可移动驱动器上文件的操作。
- 监控受信任的可移动驱动器的连接和断开。

  Kaspersky Endpoint Security 允许监控所有受信任设备的连接和断开，而不仅仅是可移动驱动器。您可以在设备控制组件的通知设置中打开事件日志记录。事件具有"*信息性消息*"严重级别。

要启用对可移动驱动器使用的监控：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择"**安全控制**" → "**设备控制**"。
3. 在"**访问设置**"块中单击"**设备和 Wi-Fi 网络**"按钮。

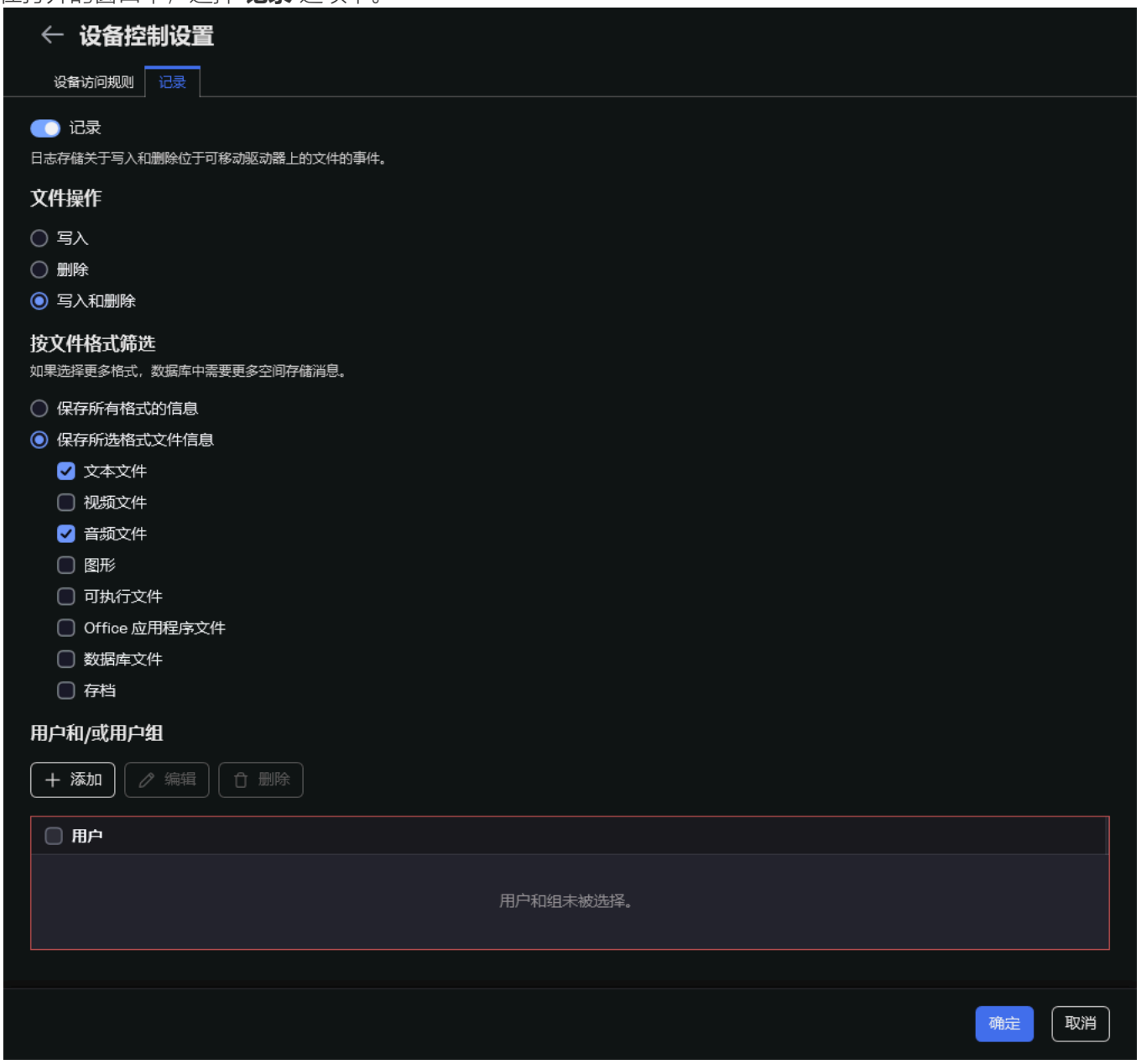
打开的窗口显示包含在设备控制组件分类的所有设备的访问规则。



设备控制组件中的设备类型

4. 在“**对存储设备的访问权限**”块中，选择“**可移动驱动器**”。

5. 在打开的窗口中，选择“**记录**”选项卡。



可移动驱动器使用监控的设置

6. 开启 **记录**切换开关。

7. 在**文件操作**块下，选择您要监控的操作：**写入**、**删除**。

8. 在**按文件格式筛选**块，选择其操作要被设备控制所记录的文件格式。

9. 选择您要监控其使用可移动驱动器的用户或用户组。

10. 保存更改。

结果，当用户在可移动驱动器上写入文件或删除文件时，Kaspersky Endpoint Security 会将此类操作的信息写入事件日志并将事件发送至 Kaspersky Security Center。您可以在 Kaspersky Security Center 管理控制台中查看移动驱动器上与文件关联的事件，其位于**事件**选项卡上**管理服务器**节点的工作区中。要使事件显示在本地 Kaspersky Endpoint Security 事件日志中，您必须选择“设备控制”组件的“通知设置”中的“**文件操作已执行**”复选框。

更改缓存持续时间

设备控制组件注册与被监视设备相关的事件，例如设备的连接和断开、从设备读取文件、将文件写入设备以及其他事件。设备控制然后根据 Kaspersky Endpoint Security 设置允许或阻止操作。

设备控制保存特定时间段（称为*缓存期*）的事件信息。如果缓存了有关某个事件的信息，并且此事件重复发生，则无需通知 Kaspersky Endpoint Security，也无需显示另一个授予对相应操作（例如连接设备）的访问权限的提示。这使得使用设备更方便。

如果以下所有事件设置都与缓存中的记录匹配，则将事件视为重复事件：

- 设备 ID
- 尝试访问的用户帐户的 SID
- 设备类别
- 使用设备执行的操作
- 此操作的应用程序权限：允许或拒绝
- 用于执行操作的进程的路径
- 正在访问的文件

在更改缓存周期之前，禁用 Kaspersky Endpoint Security 自我保护。更改缓存周期后，启用自我保护。

要更改缓存周期：

1. 打开计算机上的注册表编辑器。
2. 在注册表编辑器中，转到以下部分：
   - 对于 64 位操作系统：
     `[HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\environment]`
   - 对于 32 位操作系统：
     `[HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\protected\KES\environment]`
3. 打开 `DeviceControlEventsCachePeriod` 进行编辑。
4. 定义在删除此信息之前，设备控件必须保存有关事件的信息的分钟数。

对受信任设备的操作

*受信任的设备*是指在受信任设备设置中指定的用户可随时进行完全访问的设备。

要使用受信任设备，您可以为单个用户、一组用户或组织的所有用户授予访问权限。

例如，如果您的组织不允许使用可移动驱动器，但是管理员在工作中使用可移动驱动器，您可以仅允许一组管理员使用可移动驱动器。为此，请将可移动驱动器添加到受信任列表，并配置用户访问权限。

不建议添加超过 5000 个受信任设备，因为这可能会导致系统不稳定。

Kaspersky Endpoint Security 允许您通过以下方式将设备添加到受信任列表：

- 如果您的组织中未部署 Kaspersky Security Center，您可以将设备连接到计算机，然后在应用程序设置中将其添加到受信任列表中。要将受信任设备的列表分发到组织内的所有计算机，您可以在策略中启用合并受信任设备列表，也可以使用导出/导入过程。
- 如果您的组织中部署了 Kaspersky Security Center，您可以远程检测所有已连接的设备，并在策略中创建受信任设备的列表。受信任设备列表将在应用该策略的所有计算机上可用。

Kaspersky Endpoint Security 允许控制受信任设备的使用（连接和断开）。您可以在设备控制组件的通知设置中打开事件日志记录。事件具有“*信息性消息*”严重级别。

在应用程序界面中向受信任列表添加设备

默认情况下，在将设备添加到受信任设备列表中后，所有用户（“所有人”用户组）都被授予访问该设备的权限。

若要在应用程序界面中向受信任列表添加设备，请执行以下操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**安全控制**” → “**设备控制**”。
3. 在“**访问设置**”块中单击“**受信任设备**”按钮。
   这将打开受信任设备列表。
4. 单击“**选择**”。
   这将打开已连接设备列表。设备列表依赖于在“**显示已连接的设备**”下拉列表中选择的值。
5. 在设备列表中，选择您要添加到受信任列表的设备。

   Kaspersky Endpoint Security 不支持添加“**软盘**”类型的设备到受信任列表。

6. 在**注释**字段，您可以提供关于受信任设备的任何相关信息。
7. 选择您要允许其访问受信任设备的用户或用户组。
   您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。
8. 保存更改。

在 Kaspersky Security Center 中向受信任列表添加设备

如果计算机上已安装 Kaspersky Endpoint Security 并且已启用"设备控制"，则 Kaspersky Security Center 会收到有关设备的信息。无法将设备添加到受信任列表，除非 Kaspersky Security Center 中有该设备的信息。

您可以根据以下数据将设备添加到受信任列表中：

- "**按 ID 添加设备**"。每个设备都有一个唯一的标识符（硬件 ID 或 HWID）。您可以使用操作系统工具在设备属性中查看 ID。设备 ID 示例：`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`。如果要添加多个特定设备，则按 ID 添加设备很方便。

- "**按型号添加设备**"。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在设备属性中查看 ID。用于输入 VID 和 PID 的模板：`VID_1234&PID_5678`。如果在组织中使用特定型号的设备，则按型号添加设备很方便。这样，您可以添加该型号的所有设备。

- "**按 ID 掩码添加设备**"。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。`*` 字符可替换任意一组字符。输入掩码时，Kaspersky Endpoint Security 不支持 `?` 字符。例如，`WDC_C*`。

- "**按型号掩码列出的设备**"。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。`*` 字符可替换任意一组字符。输入掩码时，Kaspersky Endpoint Security 不支持 `?` 字符。例如，`VID_05AC&PID_*`。

更改受信任设备列表可能会受到父策略属性的阻止。要更改列表，您需要允许更改以下设置：Web Console 中的受信任区域（"挂锁"必须处于解锁状态）。

管理控制台(MMC) 和 Web Console 中受信任区域的分组方式不同。同样，防止受信任区域参数更改的方式也不同（"挂锁"不同）。我们建议仅使用 Web Console 来管理应用程序。如果在不同的控制台中配置受信任区域，管理插件可能会将"挂锁"重置为其默认状态。

要将设备添加到受信任设备列表：

1. 在 Kaspersky Security Center 管理控制台树中，选择"**策略**"。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **安全控制** → **设备控制**。
4. 在窗口右侧，选择"**受信任设备**"选项卡。
5. 如果要为公司内的所有计算机创建受信任设备的综合列表，请选中"**继承时合并值**"复选框。

   将合并父策略和子策略中的受信任设备列表。如果启用继承时合并值，则将合并列表。父策略中的受信任设备以只读视图的形式显示在子策略中。无法更改或删除父策略的受信任设备。
6. 单击"**添加**"按钮，然后选择将设备添加到受信任列表的方法。

7. 要筛选设备，请从“**设备类型**”下拉列表中选择一种设备类型（例如，“**可移动驱动器**”）。

> Kaspersky Endpoint Security 不支持添加“**软盘**”类型的设备到受信任列表。

8. 在“**名称/型号**”字段中，输入设备 ID、型号（VID 和 PID）或掩码，具体取决于所选的添加方法。

> 按型号掩码（VID 和 PID）添加设备的操作方式如下：如果输入的型号掩码与任何型号都不匹配，则 Kaspersky Endpoint Security 会检查设备 ID (HWID) 是否与该掩码匹配。Kaspersky Endpoint Security 只检查设备 ID 中决定了设备的制造商和类型的部分 (`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`)。如果型号掩码与设备 ID 的此部分匹配，则与该掩码匹配的设备将被添加到计算机上的受信任设备列表中。同时，当单击“**刷新**”按钮时，Kaspersky Security Center 中的设备列表将保持空白。要正确显示设备列表，可以按设备 ID 掩码添加设备。

9. 要筛选设备，请在“**计算机**”字段中输入设备所连接的计算机的名称或名称掩码。

   `*` 字符可替换任意一组字符。`?` 字符可替换任意单个字符。

10. 单击“**刷新**”按钮。

    该表显示满足定义的筛选条件的设备列表。

11. 选中您想要添加到受信任列表中的设备名称旁边的复选框。

12. 在“**注释**”字段中，输入将设备添加到受信任列表的原因的说明。

13. 单击“**允许用户和/或用户组**”字段右侧的“**选择**”按钮。

14. 您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

    默认情况下，允许 Everyone 组访问受信任设备。

15. 保存更改。

连接设备后，Kaspersky Endpoint Security 会检查授权用户的受信任设备列表。如果设备受信任，即使对设备类型或连接总线的访问被拒绝，Kaspersky Endpoint Security 也会允许以所有权限访问该设备。如果设备不受信任并且访问被拒绝，您可以请求访问锁定的设备。

导出和导入受信任设备的列表

要将受信任设备的列表分发到组织中的所有计算机，可以使用导出/导入过程。

例如，如果您需要分发受信任的可移动驱动器的列表，需要执行以下操作：

1. 按顺序将可移动驱动器连接到计算机。

2. 在 Kaspersky Endpoint Security 设置中，将可移动驱动器添加到受信任列表。如果需要，配置用户访问权限。例如，仅允许管理员访问可移动驱动器。

3. 在 Kaspersky Endpoint Security 设置中导出受信任设备的列表（请参见以下说明）。

4. 将受信任设备列表文件分发到组织中的其他计算机。例如，将文件放置在共享文件夹中。

5. 在组织的其他计算机上的 Kaspersky Endpoint Security 设置中导入受信任设备的列表（请参见以下说明）。

要导入或导出受信任设备的列表：

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**安全控制**” → “**设备控制**”。

3. 在“**访问设置**”块中单击“**受信任设备**”按钮。
   这将打开受信任设备列表。

4. 要导出受信任设备的列表：

   a. 选择您要导出的受信任设备。

   b. 单击“**导出**”。

   c. 在打开的窗口中，指定您要将受信任设备列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。

   d. 保存文件。
      Kaspersky Endpoint Security 会将整个受信任设备列表导出到 XML 文件。

5. 要导入受信任设备的列表：

   a. 在**导入**下拉列表，选择相关操作：**导入并添加到现有**或**导入并替换现有**。

   b. 在打开的窗口中，选择要从中导入受信任设备列表的 XML 文件。

   c. 打开文件。

6. 保存更改。

连接设备后，Kaspersky Endpoint Security 会检查授权用户的受信任设备列表。如果设备受信任，即使对设备类型或连接总线的访问被拒绝，Kaspersky Endpoint Security 也会允许以所有权限访问该设备。

获取访问被阻止设备的权限

配置“设备控制”时，可能会意外阻止对工作所需设备的访问。

如果未在组织中部署 Kaspersky Security Center，可以在 Kaspersky Endpoint Security 的设置中提供对设备的访问权限。例如，可以将设备添加到受信任列表或暂时禁用“设备控制”。

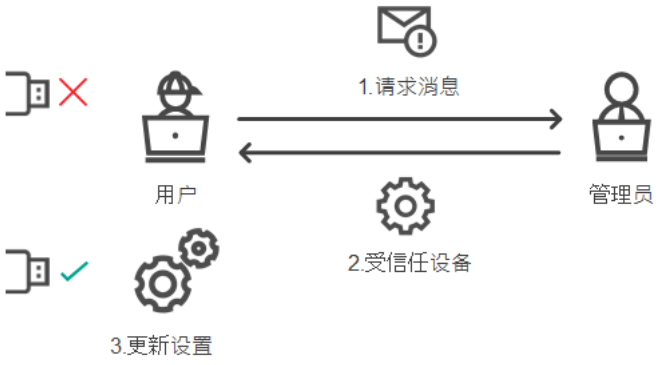
如果组织中已部署 Kaspersky Security Center 并且已将某个策略应用于计算机，则可以在管理控制台中提供对设备的访问权限。

授予访问权限的在线模式

只有在组织中部署了 Kaspersky Security Center 且已将某个策略应用于计算机时，才能以在线模式授予对阻止的设备的访问权限。计算机必须能够与管理服务器建立连接。

在线模式下授予访问权限包括以下步骤：

1. 用户向管理员发送包含访问请求的消息。
2. 管理员在 Kaspersky Security Center 控制台中收到一条包含请求的消息。
   Kaspersky Security Center 控制台有预设的事件分类“*用户请求*”以便于跟踪来自用户的消息。
3. 管理员将设备添加到受信任列表。
   您可以在管理组的策略中或单个计算机的本地应用程序设置中添加受信任设备。
4. 管理员在用户的计算机上更新 Kaspersky Endpoint Security 的设置。



在线模式下授予设备访问权限的示意图

授予访问权限的离线模式

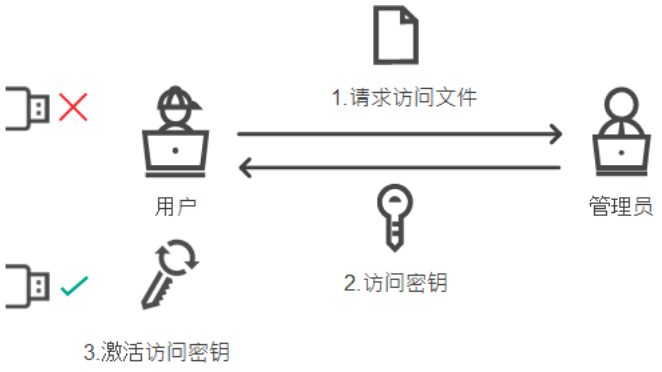
只有在组织中部署了 Kaspersky Security Center 且已将某个策略应用于计算机时，才能以离线模式授予对阻止的设备的访问权限。在策略设置的“**设备控制**”部分中，必须选中“**允许临时访问请求**”复选框。

如果需要授予对阻止的设备的临时访问权限，但无法将设备添加到受信任列表，则可以在离线模式下授予对设备的访问权限。这样，即使计算机没有网络访问权限，或者计算机位于公司网络外部，您也可以授予对阻止的设备的访问权限。

离线模式下授予访问权限包括以下步骤：

1. 用户创建请求访问文件并将其发送给管理员。
2. 管理员根据请求访问文件创建访问密钥并将其发送给用户。

3. 用户激活访问密钥。



离线模式下授予设备访问权限的示意图

授予访问权限的在线模式

只有在组织中部署了 Kaspersky Security Center 且已将某个策略应用于计算机时，才能以在线模式授予对阻止的设备的访问权限。计算机必须能够与管理服务器建立连接。

某用户请求访问阻止的设备，如下所示：

1. 将设备连接到计算机。

   Kaspersky Endpoint Security 将显示一条通知，指示对设备的访问被阻止（请参见下图）。

2. 单击**请求访问**链接。

   这将打开一个包含给管理员的消息的窗口。此消息包含有关阻止的设备的信息。

3. 单击"**发送**"。

"设备控制"通知

接下来，Kaspersky Security Center 控制台中的管理员接收"*发送给管理员的设备访问阻止消息*"事件。该事件包含用户名、计算机名、有关用户尝试访问的设备详情以及其他信息。您可以配置向管理员通知此类事件的方式，例如，选择电子邮件通知。Kaspersky Security Center 控制台有预设的事件分类"*用户请求*"以便于跟踪来自用户的消息。

若要允许访问，您必须将设备添加到受信任列表中。在计算机上更新 Kaspersky Endpoint Security 设置后，用户将获得对设备的访问权限。

授予访问权限的离线模式

只有在组织中部署了 Kaspersky Security Center 且已将某个策略应用于计算机时，才能以离线模式授予对阻止的设备的访问权限。在策略设置的“**设备控制**”部分中，必须选中“**允许临时访问请求**”复选框。

某用户请求访问阻止的设备，如下所示：

1. 将设备连接到计算机。

   Kaspersky Endpoint Security 将显示一条通知，指示对设备的访问被阻止（请参见下图）。

2. 单击**请求临时访问**链接。

   这将打开包含已连接设备列表的窗口。

3. 在已连接设备的列表中，选择您想要获取其访问权限的设备。

4. 单击“**生成请求访问文件**”。

5. 在“**访问持续时间**”字段中，指定您想要访问设备的时长。

6. 将文件保存到计算机内存中。

结果，带 *.akey 扩展名的请求访问文件将下载到计算机内存中。使用任何可用方法将设备请求访问文件发送给公司 LAN 管理员。

“设备控制”通知

管理员如何在管理控制台（MMC）中为被阻止的设备创建访问密钥

1. 打开 Kaspersky Security Center Administration Console。

2. 在管理控制台树的“**受管理设备**”文件夹中，打开相关客户端计算机所属的管理组名称的文件夹。

3. 在工作区中选择“**设备**”选项卡。

4. 在客户端计算机列表中，选择其用户需要被授予阻止的设备临时访问权限的计算机。

5. 在计算机的上下文菜单中，选择“**授予离线模式下的访问权限**”条目。

6. 这将打开一个窗口；在该窗口中，选择“**设备控制**”选项卡。

7. 单击“**浏览**”按钮并下载从用户处收到的请求访问文件。
   您将看到有关用户请求访问的阻止的设备的信息。

8. 如果必要，更改“**访问持续时间**”设置的值。
   默认情况下，“**访问持续时间**”设置采用用户在创建访问请求文件时指示的值。

9. 指定“**激活截止日期**”设置的值。
   该设置定义用户可使用提供的访问密钥激活被阻止设备访问权限的时间段。

10. 将访问密钥文件保存到计算机内存中。

管理员如何在 Web Console 和云控制台中为被阻止的设备创建访问密钥

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**资产(设备)**”。

2. 在客户端计算机列表中，选择其用户需要被授予阻止的设备临时访问权限的计算机。

3. 单击计算机列表上方的省略号按钮 (**...**) ，然后点击“**授予移动模式设备访问权限**”按钮。

4. 在打开的窗口中选择“**设备控制**”区域。

5. 单击“**浏览**”按钮并下载从用户处收到的请求访问文件。
   您将看到有关用户请求访问的阻止的设备的信息。

6. 如果必要，更改“**访问持续时间 (小时)**”设置的值。
   默认情况下，“**访问持续时间 (小时)**”设置采用用户在创建访问请求文件时指示的值。

7. 指定可以在设备上激活访问密钥的时间段。
   该设置定义用户可使用提供的访问密钥激活被阻止设备访问权限的时间段。

8. 将访问密钥文件保存到计算机内存中。

结果，阻止的设备的访问密钥将下载到计算机内存中。访问密钥文件的扩展名为 *.acode。使用任何可用方法将阻止的设备的访问密钥发送给用户。

用户激活访问密钥，如下所示：

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**安全控制**” → “**设备控制**”。

3. 在“**访问请求**”块中单击“**请求访问设备**”按钮。

4. 在打开的窗口中，单击“**激活访问密钥**”按钮。

5. 在打开的窗口中，选择包含从公司 LAN 管理员处收到的设备访问密钥的文件。
   这将打开一个窗口，其中包含有关访问条款的信息。

6. 单击“**确定**”。

结果，用户在管理员设置的时间段内获得对设备的访问权限。用户获得访问设备的全套权限（读取和写入）。密钥到期后，对设备的访问将被阻止。如果用户需要永久访问设备，请将设备添加到受信任列表中。

编辑设备控制消息模板

当用户尝试访问被阻止的设备时，Kaspersky Endpoint Security 会显示一条消息，表明对该设备的访问被阻止，或对该设备内容的操作被禁止。卡巴斯基专家向用户提供了一条消息模板，描述了阻止访问设备的原因（见下图）。

提供了特殊变量来管理消息模板（例如，`%USER_NAME%`）。变量允许将单个消息模板用于不同的计算机。生成消息时，Kaspersky Endpoint Security 从操作系统设置中检索变量的值，并将其插入到与特定计算机、用户和事件匹配的消息中。

“设备控制”通知

如果用户相信对设备的访问被错误地阻止了，或者对设备内容的操作被错误禁止了，用户可以通过单击被阻止操作显示消息中的链接向公司局域网管理员发送消息。为此，用户必须点击“**请求访问**”或者“**请求临时访问**”按钮并向管理员发送一条消息描述情况。您还可以准备一个发送给管理员的消息模板，并向其中添加数据，这些数据可能会为您允许或阻止访问该设备的决定提供参考。在用户请求提供访问权限后，Kaspersky Endpoint Security 向 Kaspersky Security Center 发送一个事件： **发送给管理员的设备访问阻止消息**。事件描述包含一条给管理员的消息，其中包含替换变量。您可以使用预定义事件分类“**用户请求**”在 Kaspersky Security Center 控制台中查看这些事件。如果您的组织没有部署 Kaspersky Security Center 或者没有连接到管理服务器，应用程序将向管理员发送一条消息到指定的电子邮件地址。

如何在管理控制台 (MMC) 中更改设备控制消息模板

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **安全控制** → **设备控制**。
4. 在“**消息模板设置**”块中单击“**模板**”按钮。
5. 这打开了一个窗口；在该窗口中，配置应用程序控制模板：
   - “**阻止消息**”。当用户尝试访问阻止的设备时所显示的消息的模板。当用户尝试对被阻止使用的设备内容执行操作时，也会显示此消息。
   - “**给管理员的消息**”。当用户确信设备的访问权限或设备内容操作被错误地禁止时，发送给 LAN 管理员的消息的模板。

   要将变量添加到模板文本中，请将光标放在所需的位置，单击“**变量**”，然后从可用选项列表中选择所需的变量。

您也可以恢复默认模板文本。

6. 保存更改。

如何在 Web Console 和云控制台中更改设备控制消息模板

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **安全控制** → **设备控制**。

5. 在“**消息模板**”块，配置应用程序控制消息的模板：

   - “**发送给用户的邮件**”。当用户尝试访问阻止的设备时所显示的消息的模板。当用户尝试对被阻止使用的设备内容执行操作时，也会显示此消息。

   - “**给管理员的消息**”。当用户确信设备的访问权限或设备内容操作被错误地禁止时，发送给 LAN 管理员的消息的模板。

   要将变量添加到模板文本中，请将光标放在所需的位置，单击“**添加变量**”，然后从可用选项列表中选择所需的变量。

   您也可以恢复默认模板文本。

6. 保存更改。

如何在应用程序界面中更改设备控制消息模板

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**安全控制**” → “**应用程序控制**”。

3. 在“**消息模板**”块，配置应用程序控制消息的模板：

   - “**阻止消息**”。当用户尝试访问阻止的设备时所显示的消息的模板。当用户尝试对被阻止使用的设备内容执行操作时，也会显示此消息。

   - “**给管理员的消息**”。当用户确信设备的访问权限或设备内容操作被错误地禁止时，发送给 LAN 管理员的消息的模板。

   要将变量添加到模板文本中，请将光标放在所需的位置，单击“**添加变量**”，然后从可用选项列表中选择所需的变量。

   您也可以恢复默认模板文本。

4. 保存更改。

反桥接

反桥接通过阻止为一台计算机同时建立多个网络连接来禁止创建网桥。这样可以保护公司网络避免未受保护和未经授权的网络上的攻击。

反桥接通过使用*连接规则*管理网络连接的建立。

已针对以下预定义的设备类型创建连接规则：

- 网络适配器；
- Wi-Fi 适配器；
- 调制解调器。

如果启用连接规则，Kaspersky Endpoint Security 将：

- 在建立新连接时阻止活动连接（如果规则中指定的设备类型同时用于这两个连接）；
- 阻止通过使用了较低优先级规则的设备类型建立的连接。

启用反桥接

默认情况下禁用反桥接。

要启用反桥接：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**安全控制**” → “**设备控制**”。
3. 在“**访问设置**”块中单击“**反桥接**”按钮。
4. 使用**启用反桥接**开关启用或禁用该功能。
5. 保存更改。

启用反桥接后，Kaspersky Endpoint Security 会按照连接规则阻止已建立的连接。

更改连接规则的状态

要更改连接规则的状态：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**安全控制**” → “**设备控制**”。
3. 在“**访问设置**”块中单击“**反桥接**”按钮。
4. 在**设备规则**块，选择您希望更改其状态的规则。
5. 使用**控制**栏的开关启用或禁用规则。
6. 保存更改。

更改连接规则的优先级

要更改连接规则的优先级：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**安全控制**” → “**设备控制**”。
3. 在“**访问设置**”块中单击“**反桥接**”按钮。
4. 在**设备规则**块，选择您希望更改其优先级的规则。
5. 使用**上移** / **下移**按钮设置连接规则的优先级。

   规则在规则表中所处位置越高，其优先级就越高。除了通过使用最高级规则的设备类型所建立的连接外，反桥接将阻止所有连接。
6. 保存更改。

自适应异常控制

> 如果 Kaspersky Endpoint Security 安装在运行 Windows for Workstations 的计算机上，则该组件可用。如果 Kaspersky Endpoint Security 安装在运行 Windows for Servers 的计算机上，则该组件不可用。

自适应异常控制组件会监视并阻止不是公司网络内计算机典型操作的相关操作。自适应异常控制使用一组规则来跟踪非典型行为（例如，*从 office 应用程序启动 Microsoft PowerShell* 规则）。规则由 Kaspersky 专家根据恶意活动的典型情景创建。您可以配置“自适应异常控制”处理每条规则的方式，例如，允许执行使某些工作流任务自动化的 PowerShell 脚本。Kaspersky Endpoint Security 会同时更新规则集和应用程序数据库。规则集的更新必须手动确认。

“自适应异常控制”设置

配置“自适应异常控制”包括以下步骤：

1. 训练“自适应异常控制”。

   启用“自适应异常控制”后，其规则在*训练模式*下工作。在训练期间，“自适应异常控制”监控规则触发并将触发事件发送到 Kaspersky Security Center。每条规则都有自己的训练模式持续时间。训练模式持续时间由 Kaspersky 专家设置。通常，训练模式保持活动两周。

   如果在训练期间某条规则完全未触发，“自适应异常控制”会将与此规则关联的操作视为非典型操作。Kaspersky Endpoint Security 将阻止与该规则相关的所有操作。

   如果在训练期间触发了某条规则，Kaspersky Endpoint Security 会将事件记录在规则触发报告和“**智能培训状态下的规则触发器**”存储库中。

2. 分析规则触发报告。

   管理员分析规则触发报告或“**智能培训状态下的规则触发器**”存储库的内容。然后管理员可以选择在触发规则时“自适应异常控制”的行为：阻止或允许。管理员还可以继续监控规则的工作方式并延长训练模式的持续时间。如果管理员未采取任何操作，应用程序也将继续在训练模式下工作。训练模式期限重新开始。

“自适应异常控制”通过以下通道实时配置：

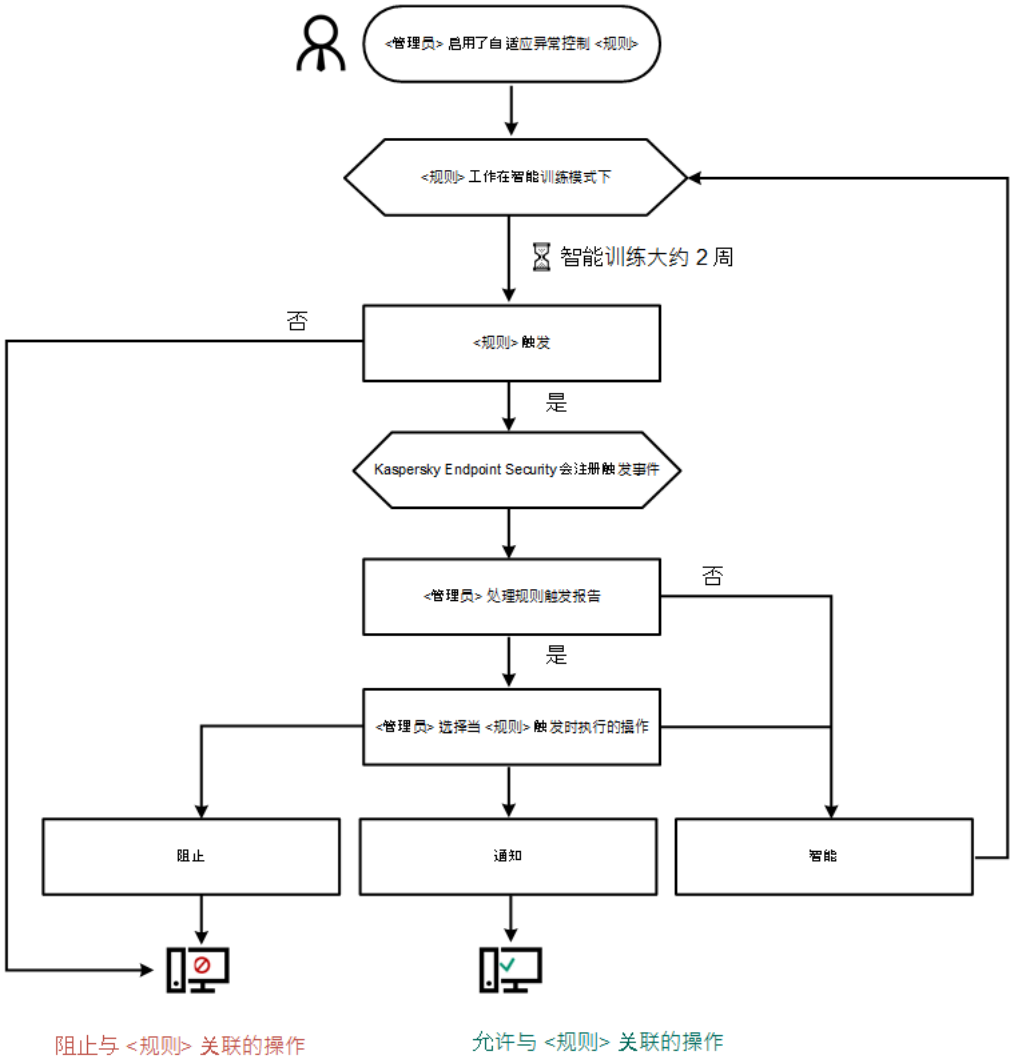
- “自适应异常控制”自动开始阻止与从未在训练模式中触发的规则相关联的操作。
- Kaspersky Endpoint Security 添加新规则或删除过时规则。
- 管理员在查看规则触发报告和“**智能培训状态下的规则触发器**”存储库的内容后配置“自适应异常控制”的操作。我们建议检查有关规则触发的报告以及“**智能培训状态下的规则触发器**”存储的内容。

当恶意应用程序尝试执行操作时，Kaspersky Endpoint Security 将阻止该操作并显示通知（请参见下图）。

“自适应异常控制”通知

“自适应异常控制”操作算法

Kaspersky Endpoint Security 根据以下算法决定是允许还是阻止与某条规则关联的操作（请参见下图）。



“自适应异常控制”操作算法

训练“自适应异常控制”

自适应异常控制包括一组规则（行为模式）。启用“自适应异常控制”后，其规则在*训练模式*下工作。在训练期间，“自适应异常控制”监控规则触发并将触发事件发送到 Kaspersky Security Center。自适应异常控制不会阻止计算机上的应用程序活动，而只会通知管理员。您也可以手动选择触发自适应异常控制规则时执行的操作。

如何在管理控制台 (MMC) 中查看自适应异常控制规则列表

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**策略**”。
3. 选择必要的策略并双击以打开策略属性。
4. 在策略窗口中，选择 **安全控制** → **自适应异常控制**。

5. 选择**自适应异常控制**复选框。

6. 在“**自适应异常控制规则设置**”下，查看规则列表。
   默认情况下，所有规则都工作在“**智能**”模式。

7. 如有必要，确认自适应异常控制规则的更新。

8. 如有必要，选择在自适应异常控制规则触发时执行的操作：

   - “**阻止**”。如果选择此操作，当触发自适应异常控制规则时，Kaspersky Endpoint Security 将阻止规则覆盖的活动，并记录包含活动信息的条目。

   - “**通知**”。如果选择此操作，当触发自适应异常控制规则时，Kaspersky Endpoint Security 将允许规则覆盖的活动，并记录包含活动信息的条目。

9. 如果有必要，请禁用您不想使用的规则。

10. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中查看自适应异常控制规则

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **安全控制** → **自适应异常控制**。

5. 开启 **自适应异常控制已启用**切换开关。

6. 在“**规则**”下，查看规则列表。
   默认情况下，所有规则都工作在“**智能**”模式。

7. 如有必要，确认自适应异常控制规则的更新。

8. 如有必要，选择在自适应异常控制规则触发时执行的操作：

   - “**阻止**”。如果选择此操作，当触发自适应异常控制规则时，Kaspersky Endpoint Security 将阻止规则覆盖的活动，并记录包含活动信息的条目。

   - “**通知**”。如果选择此操作，当触发自适应异常控制规则时，Kaspersky Endpoint Security 将允许规则覆盖的活动，并记录包含活动信息的条目。

9. 如果有必要，请禁用您不想使用的规则。

10. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在应用程序界面中查看自适应异常控制规则列表

1. 打开主应用程序窗口并单击 按钮。

2. 在应用程序设置窗口中，选择“**安全控制**” → “**自适应异常控制**”。

3. 开启 **自适应异常控制**切换开关。

4. 在“**规则**”区域，单击“**编辑规则**”链接。

   “自适应异常控制规则”列表将打开。默认情况下，所有规则都工作在“**智能**”模式。

5. 如有必要，确认自适应异常控制规则的更新。

6. 如有必要，选择在自适应异常控制规则触发时执行的操作：

   - “**阻止**”。如果选择此操作，当触发自适应异常控制规则时，Kaspersky Endpoint Security 将阻止规则覆盖的活动，并记录包含活动信息的条目。

   - “**通知**”。如果选择此操作，当触发自适应异常控制规则时，Kaspersky Endpoint Security 将允许规则覆盖的活动，并记录包含活动信息的条目。

7. 如果有必要，请禁用您不想使用的规则。

8. 保存更改。

每条规则都有自己的训练模式持续时间。训练模式持续时间由 Kaspersky 专家设置。通常，训练模式保持活动两周。

如果在培训过程中，某条规则从未触发，自适应异常控制会认为这种行为不正常，并将规则状态更改为“**智能阻止**”。随后，应用程序会阻止任何符合该规则的活动。

如果在培训期间触发规则，则需要手动配置应用程序对与该规则匹配的检测到的活动所应用的操作。如果您未选择规则触发时的操作，自适应异常控制将继续处于培训模式。

启用和禁用自适应异常控制规则

要禁用或启用自适应异常控制规则：

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**安全控制**” → “**自适应异常控制**”。

3. 在“**规则**”块中单击“**编辑规则**”按钮。

   “自适应异常控制规则”列表将打开。

4. 在表格中，选择规则集（例如，*Office 应用程序的活动*）并扩展该集。

5. 选择规则（例如，*从 office 应用程序启动 Microsoft PowerShell*）。

6. 使用**状态**栏的开关启用或禁用自适应异常控制规则。

7. 保存更改。

在自适应异常控制规则触发时更改执行的操作

要编辑触发自适应异常控制规则时执行的操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**安全控制**” → “**自适应异常控制**”。
3. 在“**规则**”块中单击“**编辑规则**”按钮。

   “自适应异常控制规则”列表将打开。
4. 在表格中选择规则。
5. 单击“**编辑**”。

   “自适应异常控制规则”属性窗口将打开。
6. 在**操作**区块，选择以下选项之一：
   - “**智能**”。果选择此选项，自适应异常控制规则在 Kaspersky 专家定义的时间段内以智能训练状态工作。在此模式下，当触发自适应异常控制规则时，Kaspersky Endpoint Security 允许规则涵盖的活动，并在 Kaspersky Security Center 管理服务器的“**智能培训状态下的规则触发器**”存储中记录条目。当为智能训练状态下的工作设置的时间段结束后， Kaspersky Endpoint Security 将阻止自适应异常控制规则覆盖的活动，并记录包含活动相关信息的条目。
   - “**阻止**”。如果选择此操作，当触发自适应异常控制规则时，Kaspersky Endpoint Security 将阻止规则覆盖的活动，并记录包含活动信息的条目。
   - “**通知**”。如果选择此操作，当触发自适应异常控制规则时，Kaspersky Endpoint Security 将允许规则覆盖的活动，并记录包含活动信息的条目。
7. 保存更改。

为自适应异常控制规则创建排除项

> 您无法为自适应异常控制规则创建超过 1000 个排除项。不建议创建超过 200 个排除项。要减少使用的排除项数量，建议在排除项设置中使用掩码。

自适应异常控制规则的排除项包括源对象和目标对象的说明。*源对象*是执行操作的对象。*目标对象*是被执行操作的对象。例如，您打开了一个名为 `file.xlsx` 的文件。结果，一个带 DLL 扩展名的库文件加载到计算机内存中。该库被浏览器（名为 `browser.exe` 的可执行文件）使用。在此示例中， `file.xlsx` 是源对象，Excel 是源进程， `browser.exe` 是目标对象，Browser 是目标进程。

要为自适应异常控制规则创建排除项：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**安全控制**” → “**自适应异常控制**”。

3. 在“**规则**”块中单击“**编辑规则**”按钮。

   “自适应异常控制规则”列表将打开。

4. 在表格中选择规则。

5. 单击“**编辑**”。

   “自适应异常控制规则”属性窗口将打开。

6. 在“**排除项**”块中单击“**添加**”按钮。

   排除属性窗口将打开。

7. 选择要为其配置排除项的用户。

   您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

   > 自适应异常控制不支持用户组排除项。如果您选择一个用户组，Kaspersky Endpoint Security 不应用排除项。

8. 在“**描述**”字段中输入排除项的说明。

9. 定义源对象的设置或该对象启动的源进程的设置：

   - “**源进程**”。文件或包含文件的文件夹的路径或掩码（例如，`C:\Dir\File.exe` 或 `Dir\*.exe`）。
   - “**源进程哈希**”。文件 SHA256 哈希
   - “**源对象**”。文件或包含文件的文件夹的路径或掩码（例如，`C:\Dir\File.exe` 或 `Dir\*.exe`）。例如，文件路径 `document.docm`，它使用脚本或宏来启动目标进程。

     您还可以指定要排除的其他对象，如 Web 地址、宏、命令行中的命令、注册表路径等等。按照以下模板指定对象：`object://<object>`、其中 `<object>` 指对象的名称，例如 `object://web.site.example.com`、`object://VBA`、`object://ipconfig`、`object://HKEY_USERS`。您也可以使用掩码，例如，`object://*C:\Windows\temp\*`。
   - “**源对象哈希**”。文件 SHA256 哈希

   自适应异常控制规则不适用于该对象执行的操作或该对象启动的进程。

10. 指定目标对象的设置或对该对象启动的目标进程的设置。

    - “**目标进程**”。文件或包含文件的文件夹的路径或掩码（例如，`C:\Dir\File.exe` 或 `Dir\*.exe`）。
    - “**目标进程哈希**”。文件 SHA256 哈希
    - “**目标对象**”。用于启动目标进程的命令。使用模式 `object://<command>` 指定命令， 例如，`object://cmdline:powershell -Command "$result = 'C:\Windows\temp\result_local_users_pwdage.txt'"`。您也可以使用掩码，例如，`object://*C:\Windows\temp\*`。
    - “**目标对象哈希**”。文件 SHA256 哈希

自适应异常控制规则不适用于对该对象执行的操作或对该对象启动的进程。

11. 保存更改。

为自适应异常控制规则导出和导入排除项

要为所选规则导出或导入排除项列表：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**安全控制**” → “**自适应异常控制**”。
3. 在“**规则**”块中单击“**编辑规则**”按钮。
   “自适应异常控制规则”列表将打开。
4. 要导出规则列表：
   a. 选择您要导出其排除的规则。
   b. 单击“**导出**”。
   c. 在打开的窗口中，指定您要将排除项列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。
   d. 确认您仅想导出所选排除项，或导出整个排除项列表。
   e. 保存文件。
5. 要导入排除项列表：
   a. 单击“**导入**”。
   b. 在打开的窗口中，选择要从中导入排除项列表的 XML 文件。
   c. 打开文件。
      如果计算机已经具有排除项的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 XML 文件向其中添加新条目。
6. 保存更改。

更新自适应异常控制规则

可以将新的自适应异常控制规则添加到规则表中，并且可以在更新反病毒数据库时从规则表中删除现有自适应异常控制规则。如果尚未应用这些规则的更新，Kaspersky Endpoint Security 会区分要删除或添加到表中的自适应异常控制规则。

在应用更新之前，Kaspersky Endpoint Security 会显示要由规则表中的更新删除的自适应异常控制规则集，并为其分配“*已禁用*”状态。不能更改这些规则的设置。

要更新自适应异常控制规则：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**安全控制**” → “**自适应异常控制**”。
3. 在“**规则**”块中单击“**编辑规则**”按钮。
   “自适应异常控制规则”列表将打开。
4. 在打开的窗口中，单击“**批准更新**”按钮。
   如果自适应异常控制规则的更新可用，则“**批准更新**”按钮可用。
5. 保存更改。

编辑自适应异常控制消息模板

当用户尝试执行被自适应异常控制规则阻止的操作时，Kaspersky Endpoint Security 会显示一条消息，提示阻止了可能有害的操作。如果用户认为该应用程序被错误地阻止，用户可使用消息文本中的链接向公司局域网管理员发送消息。

特殊模板可用于向管理员发送有关阻止潜在有害操作的消息。提供了特殊变量来管理消息模板（例如，`%USER_NAME%`）。变量允许将单个消息模板用于不同的计算机。生成消息时，Kaspersky Endpoint Security 从操作系统设置中检索变量的值，并将其插入到与特定计算机、用户和事件匹配的消息中。

要编辑消息模板，请执行下列操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**安全控制**” → “**自适应异常控制**”。
3. 在**模板**块，为自适应异常控制消息配置模板：
   - “**阻止消息**”。当阻止非典型操作的自适应异常控制规则触发时，显示给用户的消息的模板。
   - “**给管理员的消息**”。当用户认为阻止是错误的时可以发送给本地公司网络管理员的消息的模板。在用户请求提供访问权限后，Kaspersky Endpoint Security 向 Kaspersky Security Center 发送一个事件：**发送给管理员的应用程序活动阻止消息**。事件描述包含一条给管理员的消息，其中包含替换变量。您可以使用预定义事件分类“**用户请求**”在 Kaspersky Security Center 控制台中查看这些事件。如果您的组织没有部署 Kaspersky Security Center 或者没有连接到管理服务器，应用程序将向管理员发送一条消息到指定的电子邮件地址。

   要将变量添加到模板文本中，请将光标放在所需的位置，单击“**添加变量**”，然后从可用选项列表中选择所需的变量。

   您还可以使用“**重置**”按钮恢复默认模板文本。
4. 保存更改。

监控自适应异常控制操作

自适应异常控制包括几种监控工具。监控自适应异常控制的主要目的是在培训时配置组件。

自适应异常控制报告

自适应异常控制使用以下报告：

- “**有关自适应异常控制规则状态的报告**”。该报告包含有关自适应异常控制规则状态的信息（*关闭*、*智能培训*、*智能阻止*、*通知*、*阻止*）。该报告允许分析自适应异常控制的培训水平，并评估从“*智能培训*”模式切换至正常运行模式（例如，*智能阻止*）的规则数量。
- “**有关触发的自适应异常控制规则的报告**”。该报告包含有关规则触发的信息。报告还展示了规则触发模式：*阻止*（包括“*智能阻止*”）或“*通知*”。该报告可以评估用户计算机上自适应异常控制的活动。

如何在管理控制台 (MMC) 中查看自适应异常控制报告

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **安全控制** → **自适应异常控制**。
4. 执行下列操作之一：
   - 如果您想查看有关自适应异常控制规则状态的报告，请单击“**有关自适应异常控制规则状态的报告**”链接。
   - 如果您想查看有关触发的自适应异常控制规则的报告，请单击“**有关触发的自适应异常控制规则的报告**”链接。
5. 报告生成过程将开始。

   该报告将显示在新窗口中。

如何在 Web Console 中查看自适应异常控制报告

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”选项卡。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **安全控制** → **自适应异常控制**。
5. 在“**规则**”块中执行以下操作之一：
   - 如果您想查看有关自适应异常控制规则状态的报告，请选择“**查看报告** → **规则状态**”。
   - 如果您想查看有关触发的自适应异常控制规则的报告，请单击“**查看报告**”→“**检测**”。
6. 报告生成过程将开始。

   该报告将显示在新窗口中。

要在 Kaspersky Security Center 控制台中生成报告，您必须启用到管理服务器的数据传输。默认情况下启用数据传输。

如何在管理控制台 (MMC) 中启用自适应异常控制的数据传输

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **报告和存储**。
4. 在“**到管理服务器的数据传输**”块中单击“**设置**”按钮。
5. 勾选以下复选框：
   - “**有关自适应异常控制规则状态的报告**”。
   - “**有关触发的自适应异常控制规则的报告**”。
6. 保存更改。

如何在 Web Console 中启用自适应异常控制的数据传输

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **KSC 整合**。
5. 在“**到管理服务器的数据传输**”下，选择以下复选框：
   - “**有关自适应异常控制规则状态的报告**”。
   - “**有关触发的自适应异常控制规则的报告**”。
6. 保存更改。

“智能培训状态下的规则触发器”存储

在培训模式下，自适应异常控制将有关触发规则的信息发送到单独的存储，**智能培训状态下的规则触发器**。有关触发规则的信息在存储中以事件列表的形式表示。要调整自适应异常控制，您可以确认计算机上的异常行为，或者添加规则排除项。

“自适应异常控制”事件

自适应异常控制记录在“*阻止*”（包括“*智能阻止*”）和“*通知*”模式下的规则触发事件。为此目的提供了以下事件：

进程操作已阻止

进程操作已跳过

事件包含有关可疑活动的信息，包括文件校验和、涉及的用户、规则触发时间和计算机名称。分析事件后，如果您发现该活动合法，则可以立即从规则中添加排除项。

应用程序控制

“应用程序控制”管理用户计算机上的应用程序启动。这允许您在使用应用程序时实施公司安全策略。“应用程序控制”还通过限制对应用程序的访问来降低计算机感染的风险。

配置“应用程序控制”包括以下步骤：

1. 创建应用程序类别。

   管理员创建管理员想要管理的应用程序类别。应用程序类别适用于公司网络中的所有计算机，与管理组无关。要创建类别，您可以使用以下条件：KL 类别（例如，*浏览器*或其他类别）、文件哈希、应用程序供应商和其他条件。

2. 创建应用程序控制规则。

   管理员在管理组的策略中创建应用程序控制规则。该规则包括应用程序类别和这些类别中的应用程序的启动状态：已阻止或已允许。管理员可以创建许多规则。一个应用程序可能符合多个规则的条件。阻止规则的优先级高于允许规则的优先级。Kaspersky Endpoint Security 每次启动时都会检查应用程序是否符合规则。Kaspersky Endpoint Security 按顺序将应用程序与所有应用程序控制规则进行匹配。

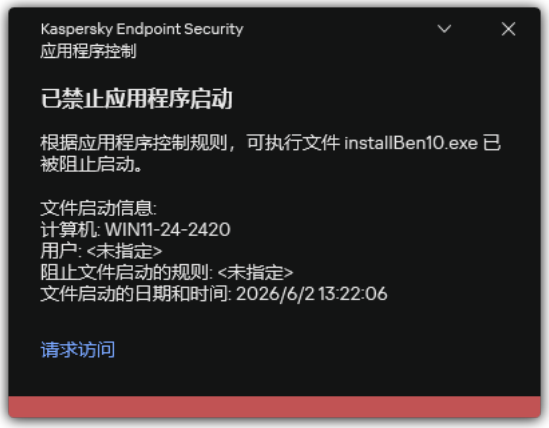
3. 选择应用程序控制模式。

   管理员选择对未包含在以下任何规则中的应用程序的处理模式（应用程序拒绝列表或允许列表）。

当用户尝试启动已禁止的应用程序时，Kaspersky Endpoint Security 将阻止该应用程序启动并显示通知（请参见下图）。

系统提供了一种*测试模式*来检查“应用程序控制”的配置。在此模式下，Kaspersky Endpoint Security 执行以下操作：

- 允许启动应用程序，包括已禁止的应用程序。
- 显示有关已禁止的应用程序启动的通知，并将信息添加到用户计算机上的报告中。
- 将有关已禁止的应用程序启动的数据发送到 Kaspersky Security Center。



“应用程序控制”通知

“应用程序控制”运行模式

“应用程序控制”组件在两种模式下运行：

- “**拒绝列表**”。在此模式下，“应用程序控制”允许用户启动除了应用程序控制规则中禁止的应用程序以外的所有应用程序。

  默认情况下启用“应用程序控制”的这一模式。

- “**允许列表**”。在此模式下，“应用程序控制”阻止用户启动除了应用程序控制规则中允许和未禁止的应用程序以外的任何应用程序。

  如果完整配置了“应用程序控制”的允许规则，则该组件将阻止启动所有未经局域网管理员验证的新应用程序，同时允许运行用户在工作中依赖的操作系统和受信任应用程序。

  您可以阅读有关在允许列表模式下配置应用程序控制规则的建议。

可以使用 Kaspersky Endpoint Security 本地界面和 Kaspersky Security Center 将“应用程序控制”配置为在这些模式下运行。

但是，Kaspersky Security Center 提供了在 Kaspersky Endpoint Security 本地界面中不可用的工具，例如以下任务所需的工具：

- 创建应用程序类别。

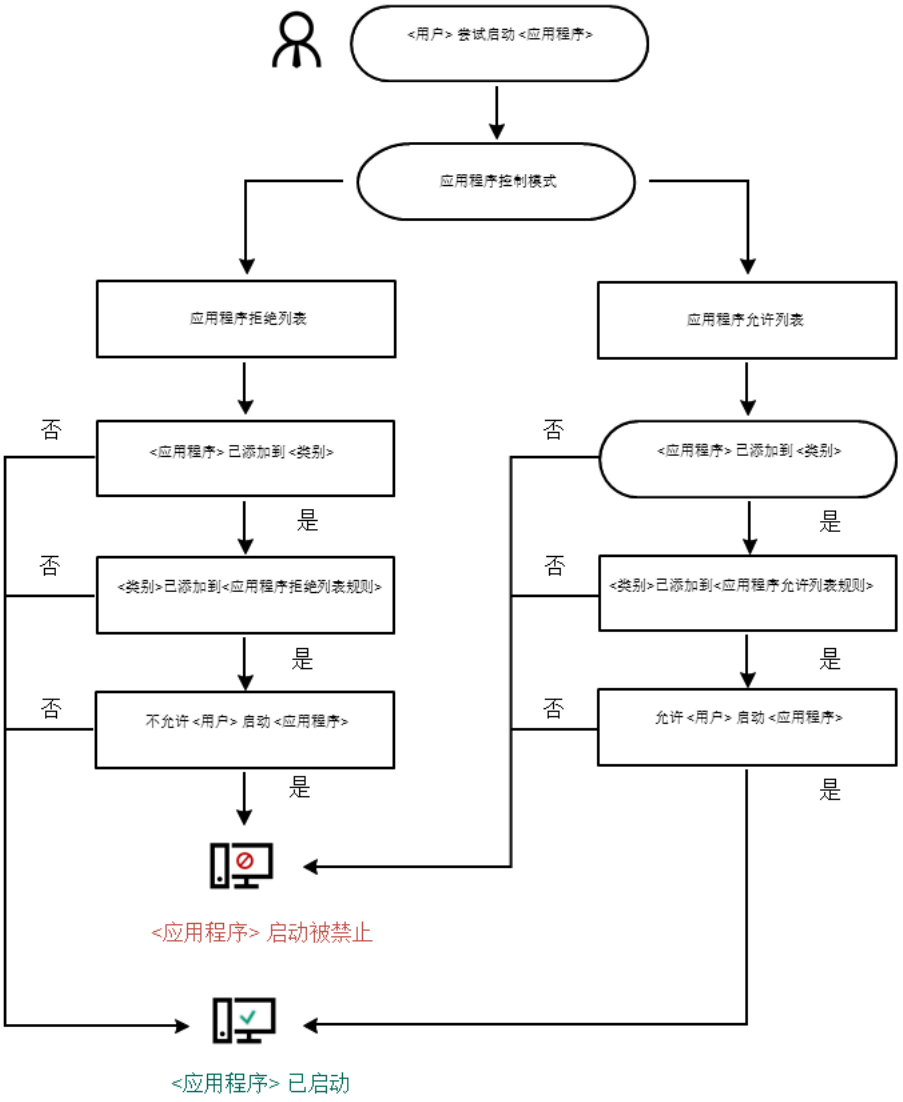
  在 Kaspersky Security Center 管理控制台中创建的应用程序控制规则基于您的自定义应用程序类别，而不是基于像 Kaspersky Endpoint Security 本地界面中的包含和排除条件。

- 接收有关安装在公司局域网计算机上的应用程序的信息。

因此，建议使用 Kaspersky Security Center 配置“应用程序控制”组件的运行。

“应用程序控制”运行算法

Kaspersky Endpoint Security 使用算法来决定是否启动应用程序（请参见下图）。



“应用程序控制”运行算法

应用程序控制功能限制

在以下情况中“应用程序控制”组件的运行受到限制：

- 应用程序版本升级时，不支持导入“应用程序控制”组件设置。
- 如果没有与 KSN 服务器连接，则 Kaspersky Endpoint Security 将仅从本地数据库中接收关于应用程序及其模块信誉的信息。

  Kaspersky Endpoint Security 指定为“**其他软件\根据 KSN 信誉受信任的其他软件**”KL 类别的应用程序的列表可能会有所不同，具体取决于与 KSN 服务器的连接是否可用。

- 在 Kaspersky Security Center 数据库中可以储存 150,000 份已处理文件的信息。一旦达到这一数量的记录，新的文件将不会被处理。要恢复清单操作，您必须从安装了 Kaspersky Endpoint Security 的计算机上删除之前存在 Kaspersky Security Center 数据库中的文件。
- 该组件不会控制脚本的启动，除非通过命令行将脚本发送给解释器。

  如果应用程序控制规则允许解释器的启动，则该组件将不会阻止从该解释器启动脚本。

  如果应用程序控制规则从一开始就阻止解释器命令行中指定的至少一个脚本，该组件将阻止解释器命令行中指定的所有脚本。

- 该组件不会阻止从不受 Kaspersky Endpoint Security 支持的解释器启动脚本。

  Kaspersky Endpoint Security 支持以下解释器：

  - Java
  - PowerShell

  支持以下类型的解释器：

  - %ComSpec%
  - %SystemRoot%\system32\regedit.exe
  - %SystemRoot%\regedit.exe
  - %SystemRoot%\system32\regedt32.exe
  - %SystemRoot%\system32\cscript.exe
  - %SystemRoot%\system32\wscript.exe
  - %SystemRoot%\system32\msiexec.exe
  - %SystemRoot%\system32\mshta.exe

- %SystemRoot%\system32\rundll32.exe
- %SystemRoot%\system32\wwahost.exe
- %SystemRoot%\syswow64\cmd.exe
- %SystemRoot%\syswow64\regedit.exe
- %SystemRoot%\syswow64\regedt32.exe
- %SystemRoot%\syswow64\cscript.exe
- %SystemRoot%\syswow64\wscript.exe
- %SystemRoot%\syswow64\msiexec.exe
- %SystemRoot%\syswow64\mshta.exe
- %SystemRoot%\syswow64\rundll32.exe
- %SystemRoot%\syswow64\wwahost.exe

接收有关安装在用户计算机上的应用程序的信息

要创建优化的应用程序控制规则，建议首先思考一下公司 LAN 中的计算机上使用的应用程序。若要执行操作，您可以获得以下信息：

- 公司局域网络中所用应用程序的供应商、版本和本地化语言。
- 应用程序的更新频率。
- 公司中所使用的应用程序使用策略（这可能是安全策略或管理策略）。
- 应用程序分发包的存储位置。

查看应用程序信息

有关已安装应用程序的信息由 Kaspersky Security Center 网络代理提供。有关已安装应用程序的信息可在 Kaspersky Security Center 控制台中找到（“**应用程序注册表**”文件夹）。网络代理每次与 Kaspersky Security Center 同步时都会更新信息。有关网络代理发送的信息的详细信息，请参阅 Kaspersky Security Center 帮助。

要在“应用程序注册表”文件夹中打开应用程序属性窗口：

1. 打开 Kaspersky Security Center Administration Console。
2. 在管理控制台树中，选择“**高级**” → “**应用程序管理**” → “**应用程序注册表**”。
3. 选择应用程序。
4. 在应用程序的上下文菜单中，选择“**属性**”。

查看有关可执行文件的信息

查询可执行文件信息时可以减少数据库的负载。为了实现这一点，我们建议在安装了标准软件集的几台参考计算机上执行“*清查*”任务。

您可以使用 Kaspersky Endpoint Security 的“*清查*”任务获取可执行文件的列表。您可以在 Kaspersky Security Center 控制台中查看可执行文件的列表，位于“**可执行文件**”文件夹。

在运行“*清查*”任务之前，请确保数据库满足 Kaspersky Security Center 的建议。有关数据库限制的详细信息，请参阅 Kaspersky Security Center 帮助。

如何在管理控制台 (MMC) 中运行“清查”任务

1. 在 Kaspersky Security Center 管理控制台树中，选择“**任务**”。
   任务列表打开。
2. 单击“**新任务**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 选择任务类型

选择“**Kaspersky Endpoint Security for Windows (14.1)**”→ “**清查**”。

步骤2. 清查范围

创建您希望 Kaspersky Endpoint Security 在其中查找可执行文件的文件夹列表。配置清查设置（参见下表）。

步骤 3. 选择任务将分配到的设备

选择将要执行任务的计算机。下列选项可用：

- 将任务分配给管理组。在这种情况下，任务分配给先前创建的管理组中包括的计算机。
- 选择管理服务器在网络中检测到的计算机：*未分配设备*。特定设备可包括管理组中的设备以及未分配设备。
- 手动指定设备地址或从列表中导入地址。您可以指定您要将任务分配给的设备的 NetBIOS 名称、IP 地址和 IP 子网。

步骤 4. 选择要运行任务的账户

选择要运行*清查*任务的账户。默认情况下，Kaspersky Endpoint Security 将使用本地用户账户的权限启动任务。如果清查范围包括网络驱动器或访问受限的其他对象，请选择具有足够访问权限的用户账户。

步骤 5. 配置任务启动计划

配置任务计划，例如，手动。

步骤 6. 定义任务名称

输入任务的名称，例如“*基线清查*”。

步骤 7. 完成任务创建

退出向导。如有必要，选中“**向导完成时运行任务**”复选框。您可以在任务属性中监控任务进度。结果，根据配置的计划在用户的计算机上执行可执行文件的搜索。

如何在 Web Console 和云控制台中运行“清查”任务

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
2. 单击“**添加**”。
   “任务向导”将启动。
3. 配置任务设置：
   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Endpoint Security for Windows 14.2.0**”。
   b. 在“**任务类型**”下拉列表中，选择“**Inventory**”。
   c. 在“**任务名称**”字段中，输入简要说明，例如“*基线清查*”。
   d. 在“**要对其分配任务的设备**”块，选择任务范围。
4. 按照所选任务范围选项选择设备。转到下一步。
5. 选择要运行任务的账户。默认情况下，Kaspersky Endpoint Security 将使用本地用户账户的权限启动任务。
6. 退出向导。
   在任务列表中将显示一个新任务。
7. 要配置任务，请转到任务属性（见下表）。

8. 选中该任务旁边的复选框。

9. 单击“**开始**”。

   您可以监控任务的状态，以及成功完成任务或完成任务时发生错误的设备数量。结果，将按照指定计划在用户计算机上搜索可执行文件。

清查设置

参数	描述
清查范围	构成清单范围的对象列表。
DLL 模块清查	Kaspersky Endpoint Security 在清查范围内查找 DLL 模块并将信息发送到 Kaspersky Security Center。 启用 DLL 模块清查会显著增加完成清查任务所需的时间和数据库的大小。
脚本文件清查	Kaspersky Endpoint Security 在清查范围内查找脚本并将信息发送到 Kaspersky Security Center。 启用脚本文件清查会显著增加完成清查任务所需的时间和数据库的大小。
仅在计算机空闲时运行	计算机资源忙时推迟任务启动。如果计算机被锁定或屏幕保护开启，Kaspersky Endpoint Security 启动扫描任务。如果您中断了任务的执行，例如通过解锁计算机，Kaspersky Endpoint Security 将自动运行该任务，并从中断点继续运行。此计划选项允许您在使用计算机时节省计算机资源。
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。
跳过扫描时间超过以下值的文件(秒) N 秒	限制任务执行时间。超出指定时间后，Kaspersky Endpoint Security 将停止任务。任务未标记为已完成。下次 Kaspersky Endpoint Security 运行该任务时，它将按计划从头开始运行。
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	扫描第三方应用程序的分发包。
复合文件大于指定值时不解压	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。

要打开“可执行文件”文件夹中的可执行文件的属性窗口：

1. 打开 Kaspersky Security Center Administration Console。

2. 在管理控制台树中，选择“**高级**” → “**应用程序管理**” → “**可执行文件**”。

3. 选择可执行文件。

4. 在可执行文件的上下文菜单中，选择“**属性**”。

要查看该应用程序及其可执行文件的常规信息以及安装了该应用程序的计算机的列表，请打开在“**应用程序注册表**”文件夹或“**可执行文件**”文件夹中选择的应用程序的属性窗口。

更新有关已安装的应用程序和可执行文件的信息

从 Kaspersky Endpoint Security 12.3 for Windows 开始，应用程序控制组件与可执行文件数据库的操作得到了优化。从计算机中删除文件后，Kaspersky Endpoint Security 12.3 for Windows 会自动更新数据库。这可以使数据库保持最新并节省 Kaspersky Security Center 资源。

为了使已安装应用程序的数据库保持最新，必须启用向管理服务器发送应用程序信息（默认启用）。

如何在管理控制台（MMC）中启用应用程序信息提交

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **报告和存储**。
4. 在“**到管理服务器的数据传输**”块中单击“**设置**”按钮。
5. 选择**已启动的应用程序**复选框。
6. 保存更改。

如何在 Web Console 和云控制台中启用应用程序信息提交

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **KSC 整合**。
5. 在“**到管理服务器的数据传输**”块中单击“**高级设置**”按钮。
6. 在打开的窗口中，选中“**关于已启动的应用程序**”复选框。
7. 保存更改。

如何启用阻止的应用程序模式

在“*已阻止的应用程序*”模式下，应用程序控制允许用户启动除了应用程序控制规则中禁止的应用程序以外的所有应用程序。也就是说，如果不存在拒绝规则，应用程序控制将允许启动该应用程序。默认情况下启用“应用程序控制”的这一模式。

> 在启用“*已阻止的应用程序*”模式之前，我们建议测试您的应用程序控制规则。为此，您可以启用测试模式。

如何在管理控制台 (MMC) 中启用阻止的应用程序模式

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**策略**”。
3. 选择必要的策略并双击以打开策略属性。
4. 在策略窗口中，选择 **安全控制** → **应用程序控制**。
5. 选择**应用程序控制**复选框。

6. 在“**应用程序控制设置**”块中，使用“**控制模式**”下拉列表选择“**拒绝列表**”。

7. 在“**操作**”下拉列表中，选择应用程序控制的操作：

   - “**测试规则**”。应用程序控制不会阻止规则阻止运行的应用程序，但会生成有关原本会被阻止的应用程序运行的事件。
   - “**应用规则**”。应用程序控制阻止被阻止的应用程序并生成相应的事件。

8. 为应用程序控制规则选择状态：

   - “**启用**”。此状态表示在“应用程序控制”组件运行时使用该规则。
   - “**关闭**”。此状态表示在“应用程序控制”组件运行时忽略该规则。
   - “**测试**”。此状态表示 Kaspersky Endpoint Security 总是允许启动应用了规则的应用程序，但会在报告中记录与启动此类应用程序有关的信息。

   如有需要，添加应用程序控制规则。

9. 配置应用程序控制的高级设置：

   - “**控制 DLL 模块加载(显著增加系统负载)**”。如果选定该复选框，Kaspersky Endpoint Security 将在用户启动应用程序时控制 DLL 模块的加载。有关 DLL 模块和加载该 DLL 模块的应用程序的信息将记录在该报告中。

     当启用对加载 DLL 模块和驱动程序的控制时，请确保在“应用程序控制”设置中已启用以下规则之一：默认“**黄金镜像**”规则或其他包含“**黄金镜像\受信任证书**”KL 类别的规则，并确保在启动 Kaspersky Endpoint Security 之前加载受信任的 DLL 模块和驱动程序。如果在禁用“**黄金镜像**”规则时启用对加载 DLL 模块和驱动程序的控制，可能导致操作系统不稳定。

     Kaspersky Endpoint Security 仅监控自选中该复选框后加载的 DLL 模块和驱动程序。选择复选框后，建议重启计算机以确保应用程序监控所有 DLL 模块和驱动程序，包括那些在 Kaspersky Endpoint Security 启动之前加载的。

   - “**使用严格的数字签名验证**”。您可以选择证书作为应用程序控制规则的触发条件。如果选中此复选框，Kaspersky Endpoint Security 将规则应用于仅使用以下证书签名的应用程序：受信任的系统证书存储。使用此类证书签名的应用程序也被视为受到保护组件（例如“*恶意软件扫描*”任务）的信任。但是，如果您在应用程序控制规则中指定来自不同存储的证书，Kaspersky Endpoint Security 将不会应用此类规则。

     如果清除该复选框，Kaspersky Endpoint Security 会将规则应用于由 Windows Trusted Root Certificate Store中的证书签名的应用程序。此类应用程序不属于受信任区域的一部分。保护组件监控此类应用程序的活动。

   - “**阻止消息**”。当触发了某个阻止应用程序启动的应用程序控制规则时所显示的消息模板。
   - “**给管理员的消息**”。当用户相信某个应用程序被错误地阻止时可以发送给公司局域网管理员的消息模板。

10. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中启用阻止的应用程序模式

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”选项卡。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **安全控制** → **应用程序控制**。
5. 开启 **应用程序控制已启用**切换开关。
6. 在“**操作模式**”块中，选择“**阻止除规则列表外的所有内容**”。
7. 在“**操作**”块中，选择应用程序控制的操作：
   - “**通知**”。应用程序控制不会阻止规则阻止运行的应用程序，但会生成有关原本会被阻止的应用程序运行的事件。
   - “**应用规则**”。应用程序控制阻止被阻止的应用程序并生成相应的事件。
8. 为应用程序控制规则选择状态：
   - “**已启用**”。此状态表示在“应用程序控制”组件运行时使用该规则。
   - “**已禁用**”。此状态表示在“应用程序控制”组件运行时忽略该规则。
   - “**测试模式**”。此状态表示 Kaspersky Endpoint Security 总是允许启动应用了规则的应用程序，但会在报告中记录与启动此类应用程序有关的信息。

   如有需要，添加应用程序控制规则。
9. 配置应用程序控制的高级设置：
   - “**监控 DLL 模块的加载**”。如果选定该复选框，Kaspersky Endpoint Security 将在用户启动应用程序时控制 DLL 模块的加载。有关 DLL 模块和加载该 DLL 模块的应用程序的信息将记录在该报告中。

     当启用对加载 DLL 模块和驱动程序的控制时，请确保在“应用程序控制”设置中已启用以下规则之一：默认“**黄金镜像**”规则或其他包含“**黄金镜像\受信任证书**”KL 类别的规则，并确保在启动 Kaspersky Endpoint Security 之前加载受信任的 DLL 模块和驱动程序。如果在禁用“**黄金镜像**”规则时启用对加载 DLL 模块和驱动程序的控制，可能导致操作系统不稳定。

     Kaspersky Endpoint Security 仅监控自选中该复选框后加载的 DLL 模块和驱动程序。选择复选框后，建议重启计算机以确保应用程序监控所有 DLL 模块和驱动程序，包括那些在 Kaspersky Endpoint Security 启动之前加载的。

- “**使用严格的数字签名验证**”。您可以选择证书作为应用程序控制规则的触发条件。如果选中此复选框，Kaspersky Endpoint Security 将规则应用于仅使用以下证书签名的应用程序：受信任的系统证书存储。使用此类证书签名的应用程序也被视为受到保护组件（例如“*恶意软件扫描*”任务）的信任。但是，如果您在应用程序控制规则中指定来自不同存储的证书，Kaspersky Endpoint Security 将不会应用此类规则。

  如果清除该复选框，Kaspersky Endpoint Security 会将规则应用于由 Windows Trusted Root Certificate Store中的证书签名的应用程序。此类应用程序不属于受信任区域的一部分。保护组件监控此类应用程序的活动。

- “**发送给用户的邮件**”。当触发了某个阻止应用程序启动的应用程序控制规则时所显示的消息模板。

- “**给管理员的消息**”。当用户相信某个应用程序被错误地阻止时可以发送给公司局域网管理员的消息模板。

10. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在应用程序界面中启用阻止的应用程序模式

1. 打开主应用程序窗口并单击 按钮。

2. 在应用程序设置窗口中，选择“**安全控制**” → “**应用程序控制**”。

3. 开启 **应用程序控制**切换开关。

4. 在“**应用程序启动控制模式**”块中，选择“**拒绝列表。规则列表之外的应用程序都被允许**”。

5. 在“**启动被规则阻止的应用程序时的操作**”块中，选择应用程序控制的操作：

   - **通知(测试模式)并记录事件 报告**。应用程序控制不会阻止规则阻止运行的应用程序，但会生成有关原本会被阻止的应用程序运行的事件。

   - “**阻止**”。应用程序控制阻止被阻止的应用程序并生成相应的事件。

6. 为应用程序控制规则选择状态：

   - “**已启用**”。此状态表示在“应用程序控制”组件运行时使用该规则。

   - “**已禁用**”。此状态表示在“应用程序控制”组件运行时忽略该规则。

   - “**测试模式**”。此状态表示 Kaspersky Endpoint Security 总是允许启动应用了规则的应用程序，但会在报告中记录与启动此类应用程序有关的信息。

   如有需要，添加应用程序控制规则。

7. 配置应用程序控制的高级设置：

   - “**监控 DLL 模块的加载**”。如果选定该复选框，Kaspersky Endpoint Security 将在用户启动应用程序时控制 DLL 模块的加载。有关 DLL 模块和加载该 DLL 模块的应用程序的信息将记录在该报告中。

     当启用对加载 DLL 模块和驱动程序的控制时，请确保在“应用程序控制”设置中已启用以下规则之一：默认“**黄金镜像**”规则或其他包含“**黄金镜像\受信任证书**”KL 类别的规则，并确保在启动 Kaspersky Endpoint Security 之前加载受信任的 DLL 模块和驱动程序。如果在禁用“**黄金镜像**”规则时启用对加载 DLL 模块和驱动程序的控制，可能导致操作系统不稳定。

Kaspersky Endpoint Security 仅监控自选中该复选框后加载的 DLL 模块和驱动程序。选择复选框后，建议重启计算机以确保应用程序监控所有 DLL 模块和驱动程序，包括那些在 Kaspersky Endpoint Security 启动之前加载的。

- "**使用严格的数字签名验证**"。您可以选择证书作为应用程序控制规则的触发条件。如果选中此复选框，Kaspersky Endpoint Security 将规则应用于仅使用以下证书签名的应用程序：受信任的系统证书存储。使用此类证书签名的应用程序也被视为受到保护组件（例如"*恶意软件扫描*"任务）的信任。但是，如果您在应用程序控制规则中指定来自不同存储的证书，Kaspersky Endpoint Security 将不会应用此类规则。

  如果清除该复选框，Kaspersky Endpoint Security 会将规则应用于由 Windows Trusted Root Certificate Store中的证书签名的应用程序。此类应用程序不属于受信任区域的一部分。保护组件监控此类应用程序的活动。

- "**关于应用程序阻止的消息模板**"。当触发了某个阻止应用程序启动的应用程序控制规则时所显示的消息模板。

- "**当应用程序被阻止启动时显示的消息文本的模板。**"。当用户相信某个应用程序被错误地阻止时可以发送给公司局域网管理员的消息模板。

8. 保存更改。

因此，应用程序控制会阻止阻止的应用程序。Kaspersky Endpoint Security 还会生成"*已禁止应用程序启动*"事件。您可以使用这些事件在 Kaspersky Security Center 控制台中生成"*禁止的应用程序报告*"报告。在报告摘要中，您可以查看触发应用程序控制规则的应用程序和计算机的列表。

基于基线计算机的应用程序控制

您可以使用基线计算机来创建包含一组所需应用程序的镜像。然后，您可以使用该镜像在其他计算机上部署操作系统和应用程序。保持镜像始终处于最新状态并不总是可行的。应用程序控制允许您根据基线计算机维护允许的应用程序列表。应用程序控制会自动确定基线计算机上安装了哪些应用程序并更新类别。这样，计算机就获得了最新的允许应用程序列表。

根据基线计算机配置应用程序控制涉及以下步骤：

1. 创建自动更新类别。创建新类别时，选择"**包含特定文件夹中的可执行文件的类别**"类别并选择您的基线计算机。

   如何在管理控制台 (MMC) 中创建自动更新类别

   1. 打开 Kaspersky Security Center Administration Console。

   2. 在管理控制台树中，选择"**高级**" → "**应用程序管理**" → "**应用程序类别**"。

   3. 在工作区中单击"**新类别**"按钮。

      这将启动应用程序类别创建向导。

   4. 按照应用程序类别创建向导的说明进行操作。

   步骤 1. 选择类别类型

   选择"**包含来自选定设备的可执行文件的类别**"作为类别类型。

步骤 2. 输入用户类别名称

在此步骤中，为应用程序类别指定一个名称。

步骤 3. 设置

> 如果您选择“**包含所选设备上可执行文件的类别**”类别类型，此步骤可用。

在此步骤中，单击“**添加**”按钮并指定 Kaspersky Security Center 将其可执行文件添加到应用程序类别的计算机。“**可执行文件**”文件夹中指定计算机的所有可执行文件都将由 Kaspersky Security Center 添加到该应用程序类别。

在此步骤还可以配置以下设置：

- 哈希函数计算的算法。要选择算法，您必须选中以下至少一个复选框：
  - “**为该类别中的文件计算 SHA256(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本中支持)**”。
  - “**为该类别中的文件计算 MD5(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 更早版本中支持)**”。
- “**与管理服务器存储库同步数据**”复选框。如果您希望 Kaspersky Security Center 定期清除应用程序类别并将“**可执行文件**”文件夹中指定计算机的所有可执行文件添加到该类别，请选择该复选框。

  如果清除“**与管理服务器存储库同步数据**”复选框，Kaspersky Security Center 在应用程序类别创建后不会对其进行任何修改。

步骤 4. 过滤器

这一步，配置文件的过滤器。

您可以指定要用于创建应用程序类别的文件类型。

- “**所有文件**”。该类别将匹配所有文件。默认情况下已选定该选项。
- “**仅应用程序类别之外的文件**”。该类别将仅匹配应用程序类别之外的文件。

您可以指定选定计算机的文件夹，其中包含要用于创建应用程序类别的文件。

- “**所有文件夹**”。该类别将匹配所有文件夹。默认情况下已选定该选项。
- “**指定文件夹**”。该类别将仅与指定的文件夹匹配。如果选择此选项，则需要指定文件夹路径。

步骤 5. 创建自定义类别

退出向导。

如何在 Web Console 和云控制台中创建自动添加内容的类别

1. 在 Web Console 的主窗口中，选择“**操作**” → “**第三方应用程序**” → “**应用程序类别**”。
   这将打开应用程序类别列表。

2. 单击“**添加**”。
   这将启动应用程序类别创建向导。

3. 配置应用程序类别的常规设置：

   - 类别名称。

   - 类别创建方法。选择“**包含来自选定设备的可执行文件的类别**”作为类别类型。

   转到下一步。

4. 配置应用程序类别的高级设置：

   - 指定 Kaspersky Security Center 将在其中将可执行文件添加到应用程序类别的计算机。“**可执行文件**”文件夹中指定计算机的所有可执行文件都将由 Kaspersky Security Center 添加到该应用程序类别。

   - 选择哈希函数计算的算法。

   - 配置与管理服务器存储同步数据的间隔。

   - 配置文件的过滤器。

5. 退出向导。

创建自动更新的类别时，将文件细分为多个类别可能会很方便。例如，操作系统文件和来自“Program Files”文件夹的文件。为此，您可以在类别设置中使用过滤器并选择单个文件夹。

2. 选择应用程序控制模式。您需要阻止所有未明确允许的应用程序的执行。要执行此操作，请选择“*已阻止的应用程序*”模式。

3. 创建一个应用程序控制规则。在规则设置中，选择基线计算机的可执行文件所属的类别。

   如何在管理控制台 (MMC) 中基于基线计算机配置应用程序控制

   1. 打开 Kaspersky Security Center Administration Console。

   2. 在控制台树中，选择“**策略**”。

   3. 选择必要的策略并双击以打开策略属性。

   4. 在策略窗口中，选择 **安全控制** → **应用程序控制**。

   5. 选择**应用程序控制**复选框。

   6. 在“**应用程序控制设置**”块中，使用“**控制模式**”下拉列表选择“**拒绝列表**”。

7. 在“**操作**”下拉列表中，选择应用程序控制的操作：

   - “**测试规则**”。应用程序控制不会阻止规则阻止运行的应用程序，但会生成有关原本会被阻止的应用程序运行的事件。

   - “**应用规则**”。应用程序控制阻止被阻止的应用程序并生成相应的事件。

8. 在应用程序控制规则列表中，单击“**添加**”按钮。

   这将启动添加应用程序控制规则的向导。

9. 在“**类别**”下拉列表中，选择基于基线计算机的自动更新类别。

10. 选择您要应用应用程序控制规则的用户或用户组。

11. 配置应用程序控制规则的高级设置：

    - “**拒绝其他用户**”。应用程序会阻止所有不在列表中的用户启动属于所选类别的应用程序。

    - “**受信任更新程序**”。Kaspersky Endpoint Security 将选定类别中包括的应用程序视为受信任更新程序，并且允许它们创建将被允许随后运行的其它可执行文件。

12. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中基于基线计算机配置应用程序控制

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **安全控制** → **应用程序控制**。

5. 开启 **应用程序控制已启用**切换开关。

6. 在“**操作模式**”块中，选择“**阻止除规则列表外的所有内容**”。

7. 在“**操作**”块中，选择应用程序控制的操作：

   - “**通知**”。应用程序控制不会阻止规则阻止运行的应用程序，但会生成有关原本会被阻止的应用程序运行的事件。

   - “**应用规则**”。应用程序控制阻止被阻止的应用程序并生成相应的事件。

8. 在应用程序控制规则列表中，单击“**添加**”按钮。

   这将启动添加应用程序控制规则的向导。

9. 在“**类别/应用程序**”下，选择基于基线计算机的自动更新类别。

10. 选择您要应用应用程序控制规则的用户或用户组。

11. 配置应用程序控制规则的高级设置：

    - “**用户**”。应用程序会阻止所有不在列表中的用户启动属于所选类别的应用程序。
    - “**受信任更新程序**”。Kaspersky Endpoint Security 将选定类别中包括的应用程序视为受信任更新程序，并且允许它们创建将被允许随后运行的其它可执行文件。

12. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在应用程序界面中基于基线计算机配置应用程序控制

1. 打开主应用程序窗口并单击 按钮。
2. 在应用程序设置窗口中，选择“**安全控制**” → “**应用程序控制**”。
3. 开启 **应用程序控制**切换开关。
4. 在“**应用程序启动控制模式**”块中，选择“**拒绝列表。规则列表之外的应用程序都被允许**”。
5. 在“**启动被规则阻止的应用程序时的操作**”块中，选择应用程序控制的操作：

    - **通知(测试模式)并记录事件 报告**。应用程序控制不会阻止规则阻止运行的应用程序，但会生成有关原本会被阻止的应用程序运行的事件。
    - “**阻止**”。应用程序控制阻止被阻止的应用程序并生成相应的事件。

6. 在应用程序控制规则列表中，单击“**添加**”按钮。

    这将启动添加应用程序控制规则的向导。

7. 在“**类别**”下，选择基于基线计算机的自动更新类别。
8. 选择您要应用应用程序控制规则的用户或用户组。
9. 配置应用程序控制规则的高级设置：

    - “**拒绝其他用户**”。应用程序会阻止所有不在列表中的用户启动属于所选类别的应用程序。
    - “**受信任更新程序**”。Kaspersky Endpoint Security 将选定类别中包括的应用程序视为受信任更新程序，并且允许它们创建将被允许随后运行的其它可执行文件。

10. 保存更改。

管理应用程序控制规则

Kaspersky Endpoint Security 根据规则按照用户控制应用程序的启动。应用程序控制规则指定触发条件以及规则被触发时（用户允许或阻止应用程序启动）“应用程序控制”执行的操作。

规则触发条件

规则触发条件具有以下关联：“条件类型 - 条件标准 - 条件值”。根据规则触发条件，Kaspersky Endpoint Security 将对应用程序应用（或不应用）规则。

以下条件类型被用于规则：

- *包括条件*。如果应用程序匹配至少一个包括条件，Kaspersky Endpoint Security 会将规则应用至该应用程序。
- *排除条件*。如果应用程序匹配至少一个排除条件并且不匹配任何包括条件，Kaspersky Endpoint Security 不会将规则应用至该应用程序。

规则触发条件使用标准进行创建。Kaspersky Endpoint Security 中使用以下标准创建规则：

- 包含应用程序可执行文件的文件夹的路径或该应用程序的可执行文件的路径。
- 元数据：应用程序可执行文件名称、应用程序可执行文件版本、应用程序名称、应用程序版本、应用程序提供商。
- 应用程序可执行文件的哈希值。
- 证书：发布者、主题、指纹。
- 在 KL 类别 中包括应用程序。
- 可移动驱动器上应用程序可执行文件的位置。

必须为条件中使用的每个标准制定标准值。如果要启动的应用程序参数符合包括条件中指定的标准值，则触发规则。在这种情况下，“应用程序控制”将执行规则中指定的操作。如果应用程序参数匹配排除条件中指定的值，“应用程序控制”不会控制应用程序的启动。

> 如果您已选择证书作为规则触发条件，则需要确保将此证书添加到计算机上的受信任系统存储中，并检查应用程序中的受信任系统存储使用设置。

触发规则后由“应用程序控制”组件做出决定。

触发规则后，“应用程序控制”将根据规则允许用户（或用户组）启动应用程序或阻止启动。您可以选择允许或不允许匹配规则的应用程序启动的用户或用户组。

如果一个规则未指定那些被允许启动匹配该规则的应用程序的用户，则该规则称为“*阻止*”规则。

如果一个规则未指定任何不允许启动匹配该规则的应用程序的用户，则该规则称为“*允许*”规则。

阻止规则的优先级高于允许规则的优先级。例如，如果已经为一个用户组指定了应用程序控制允许规则，但已经为该用户组中的一个用户指定了一个应用程序控制阻止规则，则该用户将被阻止启动应用程序。

规则的运行状态

应用程序控制规则可具有以下运行状态之一：

- “**已启用**”。此状态表示在“应用程序控制”组件运行时使用该规则。
- “**已禁用**”。此状态表示在“应用程序控制”组件运行时忽略该规则。
- “**测试模式**”。此状态表示 Kaspersky Endpoint Security 允许启动应用了规则的应用程序，但会在报告中记录与启动此类应用程序有关的信息。

为应用程序控制规则添加触发条件

您可以创建应用程序类别，以便于创建应用程序控制规则。

建议您创建涵盖公司内所使用的标准应用程序集的“工作应用程序”类别。如果工作中不同的用户组使用不同的应用程序集，则可以为每个用户组创建单独的应用程序类别。

要在管理控制台创建应用程序类别：

1. 打开 Kaspersky Security Center Administration Console。
2. 在管理控制台树中，选择“**高级**” → “**应用程序管理**” → “**应用程序类别**”。
3. 在工作区中单击“**新类别**”按钮。

   用户类别创建向导将启动。
4. 按照用户类别创建向导的说明进行操作。

步骤 1. 选择类别类型

在此步骤中，选择以下应用程序类别之一：

- 含有手动添加内容的类别。可执行文件的数据被手动添加到该类别中 如果您选择此类型的类别，则在“*配置包含应用程序到类别的条件*”步骤和“*配置从类别排除应用程序的条件*”步骤，您将能够定义将可执行文件纳入类别的标准。
- 包含所选设备上可执行文件的类别。这些可执行文件被自动处理，它们的度量数据被添加到类别中 如果您选择此类型的类别，您可以在“*设置*”步骤中指定将自动包括在该类别中的可执行文件所属的计算机。
- 包含指定文件夹内可执行文件的类别。复制到指定文件夹的应用程序可执行文件被自动处理，它们的度量数据被添加到类别中 如果您选择此类型的类别，您可以在“*存储库文件夹*”步骤中指定将自动包括在类别中的可执行文件所来自的文件夹。

创建包含自动添加内容的类别时，Kaspersky Security Center 对以下格式的文件执行清查：EXE, COM, DLL, SYS, BAT, PS1, CMD, JS, VBS, REG, MSI, MSC, CPL, HTML, HTM, DRV, OCX 和 SCR。

步骤 2. 输入用户类别名称

在此步骤中，为应用程序类别指定一个名称。

步骤 3. 配置将应用程序包括在类别中的条件

当向应用程序控制规则添加大量条件（例如文件哈希值）时，计算机资源的消耗会增加。当条件总数达到 50,000 时，可能会出现性能问题。为了优化性能，推荐审查并减少条件数量。

如果您选择“**包含手动添加内容的类别**”类别类型，此步骤可用。

在此步骤中，在“**添加**”下拉列表中选择用于将应用程序包括到类别中的条件：

- “**从可执行文件列表**”。将客户端设备上的可执行文件列表中的应用程序添加到自定义类别。
- “**从文件属性**”。指定可执行文件的详细数据，作为将应用程序添加到自定义类别的条件。
- “**文件夹内文件元数据**”。选择客户端设备上包含可执行文件的文件夹。Kaspersky Security Center 会将这些可执行文件的元数据作为将应用程序添加到自定义类别的条件。
- “**文件夹中文件的校验和**”。选择客户端设备上包含可执行文件的文件夹。Kaspersky Security Center 会将这些可执行文件的哈希值作为将应用程序添加到自定义类别的条件。
- “**文件夹中的文件证书**”。选择客户端设备上包含带证书签名的可执行文件的文件夹。Kaspersky Security Center 会将这些可执行文件的证书作为将应用程序添加到自定义类别的条件。

  不建议使用其属性中未指定“**证书指纹**”参数的条件。

- “**MSI 安装文件元数据**”。选择 MSI 包。Kaspersky Security Center 会将 MSI 包内封装的可执行文件的元数据作为将应用程序添加到自定义类别的条件。
- “**应用程序 MSI 安装程序中文件的校验和**”。选择 MSI 包。Kaspersky Security Center 会将该 MSI 包内封装的可执行文件的哈希值作为将应用程序添加到自定义类别的条件。
- “**从 KL 类别**”。指定 KL 类别作为将应用程序添加到自定义类别的条件。*KL 类别*是具有共享主题属性的应用程序列表。该列表由 Kaspersky 专家维护。例如，“*Office 应用程序*”KL 类别就包含了 Microsoft Office 套装的所有应用程序、Adobe Acrobat 和其他应用程序。

  您可以选择所有 KL 类别来生成受信任应用程序的扩展列表。

- “**指定应用程序路径(支持掩码)**”。选择客户端设备上的文件夹。Kaspersky Security Center 会将该文件夹下的可执行文件添加到自定义类别。
- “**从存储库选择证书**”。选择用来对可执行文件签名的证书作为将应用程序添加到自定义类别的条件。

  不建议使用其属性中未指定“**证书指纹**”参数的条件。

您可以选择证书存储。默认情况下，应用程序控制仅对使用来自受信任的系统证书存储的证书签名的应用程序应用规则。这是通过“**使用严格的数字签名验证**”复选框启用的。

- “**驱动器类型**”。指定存储设备类型（所有硬盘驱动器和可移动驱动器，或者仅限可移动驱动器）作为将应用程序添加到自定义类别的条件。

步骤 4. 配置将应用程序从类别中排除的条件

如果您选择“**包含手动添加内容的类别**”类别类型，此步骤可用。

在此步骤指定的应用程序将从类别中排除，即使在“配置将应用程序包括在类别中的条件”步骤指定了这些应用程序。

在此步骤中，在“**添加**”下拉列表中选择用于将应用程序从类别中排除的条件：

- “**从可执行文件列表**”。将客户端设备上的可执行文件列表中的应用程序添加到自定义类别。
- “**从文件属性**”。指定可执行文件的详细数据，作为将应用程序添加到自定义类别的条件。
- “**文件夹内文件元数据**”。选择客户端设备上包含可执行文件的文件夹。Kaspersky Security Center 会将这些可执行文件的元数据作为将应用程序添加到自定义类别的条件。
- “**文件夹中文件的校验和**”。选择客户端设备上包含可执行文件的文件夹。Kaspersky Security Center 会将这些可执行文件的哈希值作为将应用程序添加到自定义类别的条件。
- “**文件夹中的文件证书**”。选择客户端设备上包含带证书签名的可执行文件的文件夹。Kaspersky Security Center 会将这些可执行文件的证书作为将应用程序添加到自定义类别的条件。
- “**MSI 安装文件元数据**”。选择 MSI 包。Kaspersky Security Center 会将 MSI 包内封装的可执行文件的元数据作为将应用程序添加到自定义类别的条件。
- “**应用程序 MSI 安装程序中文件的校验和**”。选择 MSI 包。Kaspersky Security Center 会将该 MSI 包内封装的可执行文件的哈希值作为将应用程序添加到自定义类别的条件。
- “**从 KL 类别**”。指定 KL 类别作为将应用程序添加到自定义类别的条件。*KL 类别*是具有共享主题属性的应用程序列表。该列表由 Kaspersky 专家维护。例如，“*Office 应用程序*”KL 类别就包含了 Microsoft Office 套装的所有应用程序、Adobe Acrobat 和其他应用程序。

  您可以选择所有 KL 类别来生成受信任应用程序的扩展列表。
- “**指定应用程序路径(支持掩码)**”。选择客户端设备上的文件夹。Kaspersky Security Center 会将该文件夹下的可执行文件添加到自定义类别。
- “**从存储库选择证书**”。选择用来对可执行文件签名的证书作为将应用程序添加到自定义类别的条件。
- “**驱动器类型**”。指定存储设备类型（所有硬盘驱动器和可移动驱动器，或者仅限可移动驱动器）作为将应用程序添加到自定义类别的条件。

步骤 5. 设置

> 如果您选择“**包含所选设备上可执行文件的类别**”类别类型，此步骤可用。

在此步骤中，单击“**添加**”按钮并指定 Kaspersky Security Center 将其可执行文件添加到应用程序类别的计算机。“**可执行文件**”文件夹中指定计算机的所有可执行文件都将由 Kaspersky Security Center 添加到该应用程序类别。

在此步骤还可以配置以下设置：

- 哈希函数计算的算法。要选择算法，您必须选中以下至少一个复选框：
  - “**为该类别中的文件计算 SHA256(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本中支持)**”。
  - “**为该类别中的文件计算 MD5(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 更早版本中支持)**”。
- “**与管理服务器存储库同步数据**”复选框。如果您希望 Kaspersky Security Center 定期清除应用程序类别并将“**可执行文件**”文件夹中指定计算机的所有可执行文件添加到该类别，请选择该复选框。

  如果清除“**与管理服务器存储库同步数据**”复选框，Kaspersky Security Center 在应用程序类别创建后不会对其进行任何修改。

步骤 6. 存储库文件夹

> 如果您选择“**包含指定文件夹内可执行文件的类别**”类别类型，此步骤可用。

在此步骤中，指定 Kaspersky Security Center 将在其中搜索可执行文件的文件夹，以便自动将应用程序添加到该应用程序类别。

在此步骤还可以配置以下设置：

- “**包含动态链接库 (DLL) 到该类别**”复选框。如果您希望将动态链接库（DLL 文件）包含在应用程序类别中，请选中此复选框。

  > 在应用程序类别中包含 DLL 文件可能降低 Kaspersky Security Center的性能。

- “**包含脚本数据到该类别**”复选框。如果您希望将脚本包含在应用程序类别中，请选中此复选框。

  > 在应用程序类别中包含脚本可能降低 Kaspersky Security Center 的性能。

- 哈希函数计算的算法。要选择算法，您必须选中以下至少一个复选框：
  - “**为该类别中的文件计算 SHA256(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 或更新版本中支持)**”。
  - “**为该类别中的文件计算 MD5(在 Kaspersky Endpoint Security 10 Service Pack 2 for Windows 更早版本中支持)**”。
- “**强制扫描文件夹以查找更改**”复选框。如果您希望 Kaspersky Security Center 在用于自动添加到应用程序类别的文件夹中定期搜索可执行文件，请选择该复选框。

  如果清除“**强制扫描文件夹以查找更改**”复选框，Kaspersky Security Center 仅在用于自动添加到应用程序类别的文件夹有变更、该文件夹内添加或删除了文件时才在该文件夹中搜索可执行文件。
- “**扫描间隔 (1–168 小时)**”字段.在此字段中，您可以指定 Kaspersky Security Center 在用于自动添加到应用程序类别的文件夹中搜索可执行文件的时间间隔（以小时为单位）。

  如果选中“**强制扫描文件夹以查找更改**”复选框，则该字段可用。

步骤 7. 创建自定义类别

退出向导。

要在应用程序界面中为应用程序控制规则添加触发条件：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**安全控制**” → “**应用程序控制**”。
3. 单击“**已阻止的应用程序**”或“**允许的应用程序**”按钮。

   这将打开应用程序控制规则列表。
4. 选择要为其配置触发条件的规则。

   “应用程序控制规则”属性将开启。
5. 选择“**条件: N**”选项卡或“**排除项: N**”选项卡并单击“**添加**”按钮。
6. 为应用程序控制规则选择触发条件。
   - “**来自已启动应用程序属性的条件**”。在运行中的应用程序列表中，您可以选择要应用应用程序控制规则的应用程序。Kaspersky Endpoint Security 也列出先前运行在计算机上的应用程序。您需要选择用于创建一个或多个规则触发条件的标准：**文件哈希**、**证书**、**KL 类别**、**元数据**或**文件或文件夹路径**。
   - **条件"KL 类别"**。*KL 类别*是具有共享主题属性的应用程序列表。该列表由 Kaspersky 专家维护。例如，“Office 应用程序”KL 类别就包含了 Microsoft Office 套装的所有应用程序、Adobe® Acrobat® 和其他应用程序。
   - “**自定义条件**”。您可以选择应用程序文件并选择以下规则触发条件之一：**文件哈希**、**证书**、**元数据**或**文件或文件夹路径**。

- “**按文件驱动器归类的条件(可移动驱动器)**”。应用程序控制规则仅应用到在可移动驱动器上运行的文件。
- “**来自指定文件夹中文件属性的条件**”。应用程序控制规则仅应用到指定文件夹中的文件。您也可以从子文件夹包含或排除文件。您需要选择用于创建一个或多个规则触发条件的标准：**文件哈希**、**证书**、**KL 类别**、**元数据**或**文件或文件夹路径**。

7. 保存更改。

当添加条件时，请考虑应用程序控制的以下特殊情况：

- Kaspersky Endpoint Security 支持 `*` 和 `?` 字符以在元数据中输入掩码：**文件名**、**应用程序名称**、**供应商**。
- Kaspersky Endpoint Security 不支持拥有哈希代码的 MD5 文件并且不会基于 MD5 哈希控制应用程序的启动。规则触发条件使用了 SHA256 哈希代码。
- 不建议仅将**发布者**和**证书主题**标准设定为规则触发条件。使用这些标准不可靠。
- 如果您在“**文件或文件夹路径**”字段中使用符号链接，建议您解析符号链接以正确操作应用程序控制规则。要执行此操作，请单击“**解析符号链接**”按钮。

将“可执行文件”文件夹中的可执行文件添加到应用程序类别

在“**可执行文件**”文件夹中，将显示在计算机上的检测到的可执行文件列表。Kaspersky Endpoint Security 在执行清查任务后生成可执行文件列表。

要将“可执行文件”文件夹中的可执行文件添加到应用程序类别：

1. 打开 Kaspersky Security Center Administration Console。
2. 在管理控制台树中，选择“**高级**” → “**应用程序管理**” → “**可执行文件**”。
3. 在工作区中，选择要添加到应用程序类别的可执行文件。
4. 右键单击以打开选定可执行文件的上下文菜单，然后选择“**添加到类别**”。
5. 在打开的窗口中，做以下事项：
   - 在窗口上部，选择下列选项之一：
     - “**添加到新的应用程序类别**”。如果您要创建新的应用程序类别并向其中添加可执行文件，则选择此选项。
     - “**添加到现有应用程序类别**”。如果您要选择现有应用程序类别并向其中添加可执行文件，则选择此选项。
   - 在“**规则类型**”区域中，选择以下选项之一：
     - “**添加到包含的规则**”。如果您要创建将可执行文件添加到应用程序类别的条件，则选择此选项。
     - “**添加到排除的规则**”。如果您要创建将可执行文件从应用程序类别排除的条件，则选择此选项。

- 在**用作条件的参数**区块，选择以下选项之一：
  - “**证书详情(或没有证书的文件的 SHA256 哈希)**”。
  - “**证书详情(没有证书的文件将被跳过)**”。
  - “**仅 SHA256 (没有哈希的文件将被跳过)**”。
  - “**仅 MD5 (停产模式，仅对Kaspersky Endpoint Security 10 Service Pack 1 版本)**”。

6. 保存更改。

将事件相关的可执行文件添加到应用程序类别

要将与应用程序控制事件相关联的可执行文件添加到应用程序类别中：

1. 打开 Kaspersky Security Center Administration Console。
2. 在管理控制台树的“**管理服务器**”中选择“**事件**”选项卡。
3. 在“**事件分类**”下拉列表中选择与“应用程序控制”组件运行相关的事件集合（查看“应用程序控制”组件的运行所产生的事件，查看“应用程序控制”组件的测试运行所产生的事件）。
4. 单击“**运行分类**”按钮。
5. 选择您要将其相关可执行文件添加到应用程序类别的事件。
6. 右键单击以打开选定事件的上下文菜单，然后选择“**添加到类别**”。
7. 在打开的窗口中，配置应用程序类别设置：
   - 在窗口上部，选择下列选项之一：
     - **添加到新的应用程序类别**。如果您要创建新的应用程序类别并向其中添加可执行文件，则选择此选项。
     - **添加到现有应用程序类别**。如果您要选择现有应用程序类别并向其中添加可执行文件，则选择此选项。
   - 在“**规则类型**”区域中，选择以下选项之一：
     - **添加到包含的规则**。如果您要创建将可执行文件添加到应用程序类别的条件，则选择此选项。
     - **添加到排除的规则**。如果您要创建将可执行文件从应用程序类别排除的条件，则选择此选项。
   - 在**用作条件的参数**区块，选择以下选项之一：
     - **证书详情(或没有证书的文件的 SHA-256 哈希)**。
     - **证书详情(没有证书的文件将被跳过)**。
     - **仅 SHA-256 (没有哈希的文件将被跳过)**。
     - **仅 MD5 (停产模式，仅对Kaspersky Endpoint Security 10 Service Pack 1 版本)**。
8. 保存更改。

添加应用程序控制规则

要使用 Kaspersky Security Center 添加应用程序控制规则：

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **安全控制** → **应用程序控制**。
   在窗口右侧，显示了“应用程序控制”组件的设置。
4. 单击“**添加**”。
   “**应用程序控制规则**”窗口将打开。
5. 执行下列操作之一：
   - 如果要创建新类别：
     a. 单击“**创建类别**”。
     用户类别创建向导将启动。
     b. 按照用户类别创建向导的说明进行操作。
     c. 在“**类别**”下拉列表中，选择所创建的应用程序类别。
   - 如果要编辑现有类别：
     a. 在“**类别**”下拉列表中，选择要编辑的已创建的应用程序类别。
     b. 单击“**属性**”。
     c. 修改所选应用程序类别的设置。
     d. 保存更改。
     e. 在“**类别**”下拉列表中，选择您要依据其创建规则的应用程序类别。
6. 在“**用户及其权限**”表中，单击“**添加**”按钮。
   您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。
7. 在“**用户及其权限**”表中，做以下操作：
   - 如果您希望允许用户和/或用户组启动属于选定类别的应用程序，则选择相关行中的“**允许**”复选框。
   - 如果您希望阻止用户和/或用户组启动属于选定类别的应用程序，则选择相关行中的“**阻止**”复选框。
8. 如果您希望“用户或组”栏中没有出现的和不属于“用户或组”栏中指定用户组的所有用户被阻止启动属于所选类别的应用程序，则选择“**拒绝其他用户**”复选框。

9. 如果您希望 Kaspersky Endpoint Security 将选定应用程序类别中包括的应用程序视为受信任更新程序，并且希望允许它们创建将被允许随后运行的其它可执行文件，请选择“**受信任更新程序**”复选框。

> 在转移 Kaspersky Endpoint Security 设置时，也会转移受信任更新程序创建的可执行文件列表。

10. 保存更改。

要添加应用程序控制规则：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**安全控制**” → “**应用程序控制**”。
3. 单击“**已阻止的应用程序**”或“**允许的应用程序**”按钮。

   这将打开应用程序控制规则列表。
4. 单击“**添加**”。

   这将打开“应用程序控制”规则设置窗口。
5. 在**常规设置**选项卡，定义二规则的主要设置：

   a. 在“**规则名称**”字段中输入规则的名称。

   b. 在“**描述**”字段中输入规则的说明。

   c. 在“**用户及其权限**”表中，单击“**添加**”按钮。

   您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。

   该规则默认适用于所有用户。

   > 如果该表中没有指定用户，则无法保存该规则。

   d. 在**用户及其权限**表格，使用开关定义启动应用程序的用户权限。

   e. 如果您希望应用程序阻止满足规则触发条件的应用程序为“**用户及其权限**”表中未列出且不是“**用户及其权限**”表中列出的用户组成员的所有用户运行，请选中“**拒绝其他用户**”复选框。

   > 如果清空了“**拒绝其他用户**”复选框，则 Kaspersky Endpoint Security 不会控制“**用户及其权限**”表中未指定的用户以及不属于“**用户及其权限**”表中指定用户组的用户启动应用程序。

   f. 如果您想让 Kaspersky Endpoint Security 将匹配规则触发条件的应用程序视为受信任更新程序，请选择“**受信任更新程序**”复选框。*受信任更新程序*是允许创建其他可执行文件的应用程序，这些文件随后将被允许运行。

   如果一个应用程序触发多个规则，如果满足以下条件，Kaspersky Endpoint Security 设置“*受信任更新程序*”标志：

   - 所有规则都允许应用程序运行。
   - 至少有一条规则选中了“**受信任更新程序**”复选框。

6. 在“**条件: N**”选项卡，创建或编辑触发规则的包含条件列表。

7. 在“**排除项: N** ”选项卡，创建或编辑触发规则的排除条件列表。
   在转移 Kaspersky Endpoint Security 设置时，也会转移受信任更新程序创建的可执行文件列表。

8. 保存更改。

通过 Kaspersky Security Center 更改应用程序控制规则的状态

要在管理控制台中更改应用程序控制规则的状态：

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **安全控制** → **应用程序控制**。
   在窗口右侧，显示了“应用程序控制”组件的设置。

4. 在“**状态**”列中，单击左键以显示上下文菜单，并选择以下选项之一：

   - “**启用**”。此状态表示在“应用程序控制”组件运行时使用该规则。

   - “**关闭**”。此状态表示在“应用程序控制”组件运行时忽略该规则。

   - “**测试**”。此状态表示 Kaspersky Endpoint Security 总是允许启动应用了规则的应用程序，但会在报告中记录与启动此类应用程序有关的信息。

5. 保存更改。

要在应用程序界面中更改应用程序控制规则的状态：

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**安全控制**” → “**应用程序控制**”。

3. 单击“**已阻止的应用程序**”或“**允许的应用程序**”按钮。
   这将打开应用程序控制规则列表。

4. 在“**状态**”列中，打开上下文菜单并选择以下选项之一：

   - “**已启用**”。此状态表示在“应用程序控制”组件运行时使用该规则。

   - “**已禁用**”。此状态表示在“应用程序控制”组件运行时忽略该规则。

   - “**测试模式**”。此状态表示 Kaspersky Endpoint Security 总是允许启动应用了规则的应用程序，但会在报告中记录与启动此类应用程序有关的信息。

5. 保存更改。

导出和导入应用程序控制规则

可以将应用程序控制规则列表导出到 XML 文件。还可以使用导出/导入功能备份应用程序控制规则列表或将列表迁移到其他服务器。

导出和导入应用程序控制规则时，请牢记以下指定情况：

- Kaspersky Endpoint Security 仅为应用程序控制模式导出规则列表。换言之，如果应用程序控制按拒绝列表模式操作，则 Kaspersky Endpoint Security 将仅导出该模式的规则。若要导出允许列表模式的规则列表，您需要切换模式然后再次运行导出操作。

- Kaspersky Endpoint Security 使用应用程序控制规则的应用程序类别才起作用。当把应用程序控制规则的列表迁移到另一台服务器时，您也需要迁移应用程序类别列表。要了解有关导出或导入应用程序类别的更多详情，请参阅 Kaspersky Security Center 帮助。

如何在管理控制台(MMC)中导出和导入应用程序控制规则列表

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **安全控制** → **应用程序控制**。

4. 要导出应用程序控制规则列表：

   a. 选择您要导出的规则。要选择多个端口，使用 **CTRL** 或 **SHIFT** 键。

      如果您未选择任何规则，Kaspersky Endpoint Security 将导出所有规则。

   b. 单击**导出**链接。

   c. 在打开的窗口中，指定您要将规则列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。

   d. 保存文件。

      Kaspersky Endpoint Security 会将整个规则列表导出到 XML 文件。

5. 要导入应用程序控制规则列表：

   a. 单击**导入**链接。

      在打开的窗口中，选择要从中导入规则列表的 XML 文件。

   b. 打开文件。

      如果计算机已经具有规则的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 XML 文件向其中添加新条目。

6. 保存更改。

如何在 Web Console 和云控制台中导出和导入应用程序控制规则列表

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **安全控制** → **应用程序控制**。

5. 在“**操作模式**”下，选择规则列表：应用程序拒绝列表或允许列表。

6. 要导出规则列表：

   a. 选择您要导出的规则。

   b. 单击“ → **导出**”按钮。
      Kaspersky Endpoint Security 导出规则列表到默认下载文件夹中的 JSON 文件。

7. 要导入规则列表：

   a. 单击“ → **导入**”按钮。
      在打开的窗口中，选择要从中导入规则列表的 JSON 文件。

   b. 打开文件。
      如果计算机已经具有规则的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 JSON 文件向其中添加新条目。

8. 保存更改。

查看“应用程序控制”组件的运行所产生的事件

要查看 Kaspersky Security Center 收到的由“应用程序控制”组件的运行所产生的事件：

1. 打开 Kaspersky Security Center Administration Console。

2. 在管理控制台树的“**管理服务器**”中选择“**事件**”选项卡。

3. 单击“**创建新分类**”按钮。

4. 在打开的窗口中转到“**事件**”区域。

5. 单击“**全部清空**”按钮。

6. 在“**事件**”表中选择“**已禁止应用程序启动**”复选框。

7. 保存更改。

8. 在“**事件分类**”下拉列表中选择创建的分类。

9. 单击“**运行分类**”按钮。

查看有关阻止的应用程序的报告

要查看有关阻止的应用程序的报告：

1. 打开 Kaspersky Security Center Administration Console。
2. 在管理控制台树的“**管理服务器**”中选择“**报告**”选项卡。
3. 单击“**新建报告模板**”。
   “新报告模板向导”将启动。
4. 按照“报告模板向导”的说明进行操作。在“**选择报告模板类型**”步骤，选择“**其他 → 禁止的应用程序报告**”。
   完成新报告模板向导之后，新报告模板将出现在“**报告**”选项卡上。
5. 双击报告将其打开。

报告生成过程将开始。该报告将显示在新窗口中。

测试应用程序控制规则

要确保应用程序控制规则不会阻止工作所需的应用程序，建议启用应用程序控制规则的测试并在创建新规则后分析其运行。启用应用程序控制规则的测试后，Kaspersky Endpoint Security 不会阻止被“应用程序控制”禁止启动的应用程序，但是会将有关它们启动的通知发送给管理服务器。

分析应用程序控制规则的运行需要查看报告给 Kaspersky Security Center 的已发生的应用程序控制事件。如果对于计算机用户工作所需的所有应用程序，测试模式都不会产生阻止启动事件，则说明创建了正确的规则。否则，建议您更新已创建的规则的设置，创建附加规则或删除现有规则。

默认情况下，Kaspersky Endpoint Security 允许启动所有应用程序，但规则禁止的应用程序除外。

启用和禁用应用程序控制规则测试

要在 Kaspersky Security Center 中启用或禁用应用程序控制规则的测试：

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **安全控制 → 应用程序控制**。
   在窗口右侧，显示了“应用程序控制”组件的设置。
4. 在“**控制模式**”下拉列表中选择以下项之一：
   - “**拒绝列表**”。如果选择该选项，应用程序控制将允许所有用户启动所有应用程序，符合应用程序控制阻止规则的应用程序除外。
   - “**允许列表**”。如果选择该选项，应用程序控制将阻止所有用户启动任何应用程序，符合应用程序控制允许规则的应用程序除外。

5. 执行下列操作之一：

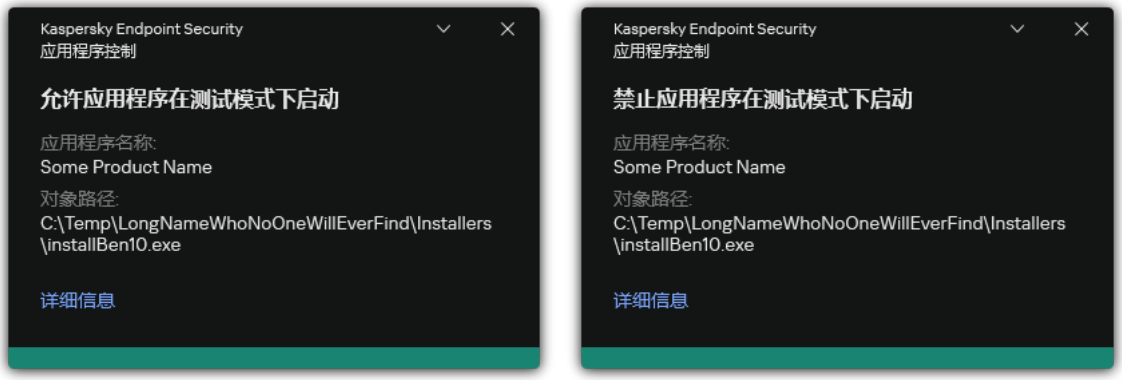
- 如果要启用应用程序控制规则的测试，请在“**操作**”下拉列表中选择“**测试规则**”选项。
- 如果要启用应用程序控制以管理用户计算机上应用程序的启动，请在下拉列表中选择**应用规则**。

6. 保存更改。

要启用应用程序控制规则的测试或为“应用程序控制”选择阻止操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**安全控制**” → “**应用程序控制**”。
3. 单击“**已阻止的应用程序**”或“**允许的应用程序**”按钮。
   这将打开应用程序控制规则列表。
4. 在“**状态**”区域中，选择“**测试模式**”。
   此状态表示 Kaspersky Endpoint Security 总是允许启动应用了规则的应用程序，但会在报告中记录与启动此类应用程序有关的信息。
5. 保存更改。

Kaspersky Endpoint Security 不会阻止被“应用程序控制”组件禁止启动的应用程序，但是会将它们的启动报告给管理服务器。您还可以配置用户计算机上规则测试通知的显示（参见下图）。



测试模式中的应用程序控制通知

查看有关测试模式下阻止的应用程序的报告

要查看有关测试模式下阻止的应用程序的报告：

1. 打开 Kaspersky Security Center Administration Console。
2. 在管理控制台树的“**管理服务器**”中选择“**报告**”选项卡。
3. 单击“**新建报告模板**”。
   “新报告模板向导”将启动。

4. 按照“报告模板向导”的说明进行操作。在“**选择报告模板类型**”步骤，选择“**其他**” → “**测试模式中禁止的应用程序报告**”。

   完成新报告模板向导之后，新报告模板将出现在“**报告**”选项卡上。

5. 双击报告将其打开。

报告生成过程将开始。该报告将显示在新窗口中。

查看“应用程序控制”组件的测试运行所产生的事件

要查看 Kaspersky Security Center 收到的应用程序控制测试事件：

1. 打开 Kaspersky Security Center Administration Console。
2. 在管理控制台树的“**管理服务器**”中选择“**事件**”选项卡。
3. 单击“**创建新分类**”按钮。
4. 在打开的窗口中转到“**事件**”区域。
5. 单击“**全部清空**”按钮。
6. 在“**事件**”表中选择“**禁止应用程序在测试模式下启动**”以及“**允许应用程序在测试模式下启动**”复选框。
7. 保存更改。
8. 在“**事件分类**”下拉列表中选择创建的分类。
9. 单击“**运行分类**”按钮。

应用程序活动监控

如果 Kaspersky Endpoint Security 安装在运行 Windows for Workstations 的计算机上，则该组件可用。如果 Kaspersky Endpoint Security 安装在运行 Windows for Servers 的计算机上，则该组件不可用。

*应用程序活动监控器*是一个用于实时查看用户计算机应用程序活动信息的工具。

使用应用程序活动监控需要安装应用程序控制和主机入侵防御组件。如果未安装这些组件，则会隐藏主应用程序窗口中的应用程序活动监控部分。

若要启动应用程序活动监控器，请：

在应用程序主窗口中，在“**监控**”区域，单击“**应用程序活动监控**”瓦片。

在此窗口中，有关用户计算机上的应用程序活动的信息将呈现在三个选项卡上：

- “**所有应用程序**”选项卡显示计算机上安装的所有应用程序的信息。
- “**正在运行**”选项卡实时显示每个应用程序对计算机资源消耗的信息。您可以从该选项卡去配置单个应用程序的权限。
- “**系统启动时运行**”选项卡显示操作系统启动时所启动的应用程序列表。

果要在用户的计算机上隐藏应用程序活动信息，您可以限制用户对应用程序活动监控工具的访问。

如何使用管理控制台 (MMC) 在应用程序界面中隐藏应用程序活动监控

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **界面**。
4. 使用**隐藏应用程序活动监控区域**复选框授予或取消对工具的访问权限。
5. 保存更改。

如何使用 Web Console 在应用程序界面中隐藏应用程序活动监控

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **用户交互**。
5. 使用**隐藏应用程序活动监控区域**复选框授予或取消对工具的访问权限。
6. 保存更改。

为文件或文件夹创建名称掩码的规则

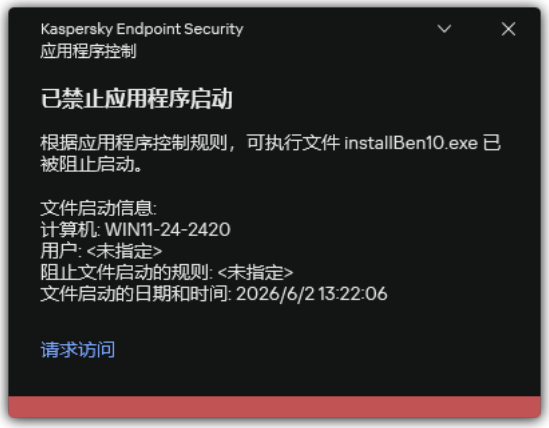
*文件或文件夹名称的掩码*是使用通用字符对文件夹名称或文件名和扩展名的表示。

您可以使用以下通用字符创建文件或文件夹名称掩码：

- `*`（星号）字符，代替任何字符集（包括空集）。例如，`C:\*.txt` 掩码将包括位于（C:）驱动器的文件夹和子文件夹中所有具有 `txt` 扩展名的文件的路径。
- `?`（问号）字符代表任意单个字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\???.txt` 将包括位于 `Folder` 文件夹中所有带 TXT 扩展名且名称由三个字符构成的文件的路径。

编辑应用程序控制消息模板

用户尝试启动被应用程序控制规则阻止的应用程序时，Kaspersky Endpoint Security 会显示消息，指明该应用程序被阻止启动。卡巴斯基专家向用户提供了一个消息模板，描述了应用程序被阻止的原因（见下图）。提供了特殊变量来管理消息模板（例如，`%USER_NAME%`）。变量允许将单个消息模板用于不同的计算机。生成消息时，Kaspersky Endpoint Security 从操作系统设置中检索变量的值，并将其插入到与特定计算机、用户和事件匹配的消息中。



"应用程序控制"通知

如果用户认为该应用程序被错误地阻止启动了，该用户可使用消息文本中的链接向公司局域网管理员发送消息。为此，用户必须点击"**请求访问**"按钮并向管理员发送一条消息描述情况。您还可以准备一个发送给管理员的消息模板，并向其中添加数据，这些数据可能会为您允许或阻止访问该应用程序的决定提供参考。在用户请求提供访问权限后，Kaspersky Endpoint Security 向 Kaspersky Security Center 发送一个事件：**发送给管理员的应用程序启动阻止消息**。事件描述包含一条给管理员的消息，其中包含替换变量。您可以使用预定义事件分类"**用户请求**"在 Kaspersky Security Center 控制台中查看这些事件。如果您的组织没有部署 Kaspersky Security Center 或者没有连接到管理服务器，应用程序将向管理员发送一条消息到指定的电子邮件地址。

如何在管理控制台 (MMC) 中编辑应用程序控制消息模板

1. 在 Kaspersky Security Center 管理控制台树中，选择"**策略**"。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **安全控制** → **应用程序控制**。
4. 在"**消息模板设置**"块中单击"**模板**"按钮。
5. 这打开了一个窗口；在该窗口中，配置应用程序控制模板：
   - "**阻止消息**"。当触发了某个阻止应用程序启动的应用程序控制规则时所显示的消息模板。

     您无法在测试模式下为应用程序控制配置消息模板。测试模式下的应用程序控制显示预设通知。
   - "**给管理员的消息**"。当用户相信某个应用程序被错误地阻止时可以发送给公司局域网管理员的消息模板。

   要将变量添加到模板文本中，请将光标放在所需的位置，单击"**变量**"，然后从可用选项列表中选择所需的变量。

您还可以使用“**默认**”按钮恢复默认模板文本。

6. 保存更改。

如何在 Web Console 和云控制台中编辑应用程序控制消息模板

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **安全控制** → **应用程序控制**。

5. 在“**消息模板**”块，点击“**关于应用程序启动阻止的消息**”链接并配置应用程序控制消息的模板：

   - “**发送给用户的邮件**”。当触发了某个阻止应用程序启动的应用程序控制规则时所显示的消息模板。
     您无法在测试模式下为应用程序控制配置消息模板。测试模式下的应用程序控制显示预设通知。

   - “**给管理员的消息**”。当用户相信某个应用程序被错误地阻止时可以发送给公司局域网管理员的消息模板。

   要将变量添加到模板文本中，请将光标放在所需的位置，单击“**添加变量**”，然后从可用选项列表中选择所需的变量。
   您还可以使用“**重置为默认值**”按钮恢复默认模板文本。

6. 保存更改。

如何在应用程序界面中编辑应用程序控制消息模板

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**安全控制**” → “**应用程序控制**”。

3. 在“**关于应用程序阻止的消息模板**”块，配置应用程序控制消息的模板：

   - “**阻止消息**”。当触发了某个阻止应用程序启动的应用程序控制规则时所显示的消息模板。
     您无法在测试模式下为应用程序控制配置消息模板。测试模式下的应用程序控制显示预设通知。

   - “**给管理员的消息**”。当用户相信某个应用程序被错误地阻止时可以发送给公司局域网管理员的消息模板。

   要将变量添加到模板文本中，请将光标放在所需的位置，单击“**添加变量**”，然后从可用选项列表中选择所需的变量。
   您还可以使用“**重置**”按钮恢复默认模板文本。

4. 保存更改。

应用程序控制消息模板中的变量

您可以在用户消息模板或管理员消息模板中使用以下变量：

- **触发的规则的名称** – %RULE%。
  阻止文件执行的规则名称。
- **当前日期** – %DATE%。
  文件执行被阻止的日期，格式为 DD.MM.YYYY。
- **当前时间** – %TIME%。
  文件执行被阻止的时间，格式为 HH:MM。
- **用户名** – %USER_NAME%。
  文件执行被阻止的计算机上的当前用户账户名称，格式为 <device name>\<user alias>（例如，DESKTOP-123\John.Smith）。
- **计算机名称** – %COMPUTER_NAME%。
  文件执行被阻止的计算机名称。
- **可执行文件名称** – %FILE_NAME%。
  被阻止的应用程序的可执行文件名称。
- **可执行文件的 KL 类别** – %KL_CAT%。
  被阻止的应用程序所属的 KL 类别（例如，*浏览器*或其他类别）。
- **可执行文件的路径** – %FILE_PATH%。
  被阻止的应用程序的可执行文件完整路径。
- **可执行文件版本** – %FILE_VERSION%。
  被阻止的应用程序的可执行文件版本。
- **可执行文件的原始名称** – %ORIGINAL_FILE_NAME%。
  被阻止的应用程序的可执行文件的原始名称。文件名在应用程序可执行文件的属性中指定。
- **供应商** – %FILE_PUBLISHER%。
  被阻止的应用程序的供应商。
- **应用程序名称** – %FILE_PRODUCT_NAME%。
  被阻止的应用程序的名称。
- **应用程序版本** – %PRODUCT_VERSION%。
  被阻止的应用程序的版本。
- **可执行文件哈希** – %FILE_HASH%。
  被阻止的应用程序的可执行文件哈希。

- **证书发布者** – `%CERT_ISSUER%`。
  可执行文件签名所用的证书的颁发者。
- **证书主题** – `%CERT_SUBJECT%`。
  可执行文件签名所用的证书的主题。
- **证书指纹** – `%CERT_THUMBPRINT%`。
  可执行文件签名所用的证书的指纹。

允许的应用程序列表的最佳实践

计划实施允许的应用程序列表时，建议执行以下操作：

1. 形成以下类型的组：
   - 用户组。需要设置为允许使用各种应用程序集的用户组。
   - 管理组。Kaspersky Security Center 将白名单模式应用于的一个或多个计算机组。如果不同的允许列表设置被不同的组使用，则有必要创建多个计算机组。
2. 创建必须允许启动的应用程序列表。
   在创建列表前，建议执行以下操作：
   a. 运行清查任务。
      清查任务的创建、重新配置和启动的相关信息可在“任务管理”区域查看。
   b. 查看可执行文件列表。

为应用程序配置允许列表模式

配置允许列表模式时，建议执行以下操作：

1. 创建包含必须允许启动的应用程序的应用程序类别。
   您可以选择以下用于创建应用程序类别的方法之一：
   - **包含手动添加内容的类别**。您可以通过使用以下条件手动添加到此类别：
     - 文件元数据。Kaspersky Security Center 会将所有附带指定元数据的可执行文件添加到该应用程序类别。
     - 文件哈希代码。Kaspersky Security Center 会将所有具有指定哈希值的可执行文件添加到该应用程序类别。

       使用此条件将排除自动安装更新的功能，因为不同版本的文件哈希值也不同。

     - 文件证书。Kaspersky Security Center 会将所有具有指定证书签名的可执行文件添加到该应用程序类别。

- KL 类别。Kaspersky Security Center 会将所有属于指定 KL 类别的应用程序添加到该应用程序类别。
- 应用程序文件夹。Kaspersky Security Center 会将此文件夹中的所有可执行文件添加到该应用程序类别。

> 使用“**应用程序文件夹**”条件可能不安全，因为指定文件夹中的任何应用程序都将被允许启动。建议只将使用具有“**应用程序文件夹**”条件的应用程序类别的规则应用于那些必须允许为其自动安装更新的用户。

- **包含指定文件夹内可执行文件的类别**。您可以指定将自动分配到已创建的应用程序类别的可执行文件所来自的文件夹。
- **包含所选设备上可执行文件的类别**。您可以指定其所有可执行文件都将自动分配到已创建的应用程序类别的计算机。

> 使用这种方法创建应用程序类别时，Kaspersky Security Center 从“**可执行文件**”文件夹接收计算机上的应用程序的相关信息。

2. 为“应用程序控制”组件选择允许列表模式。
3. 使用已创建的应用程序类别创建应用程序控制规则。

> **黄金镜像**规则和**受信任更新程序**规则最初为允许列表模式定义。这些应用程序控制规则对应于 KL 类别。“*黄金镜像*”KL 类别包含确保操作系统正常运行的程序。“*受信任更新程序*”KL 类别包含最具信誉的软件厂商的更新程序。您无法删除这些规则。这些规则的设置无法编辑。默认情况下，启用“**黄金镜像**”规则，禁用“**受信任更新程序**”规则。所有用户允许启动匹配这些规则的触发条件的应用程序。

4. 确定必须允许为其自动安装更新的应用程序。

   您可以通过以下任意一种方式允许自动安装更新：

   - 通过允许属于任何 KL 类别的所有应用程序启动来指定允许的应用程序的扩展列表。
   - 通过允许有证书签名的所有应用程序启动来指定允许的应用程序的扩展列表。

     要允许有证书签名的所有应用程序启动，您可以创建一个包含基于证书的条件的类别，该条件只使用值为“*”的“**主题**”参数。
   - 对于应用程序控制规则，选择“**受信任更新程序**”参数。如果选中此复选框，Kaspersky Endpoint Security 会将规则中包含的应用程序视为受信任更新程序。Kaspersky Endpoint Security 允许启动已由规则中包含的应用程序安装或更新的应用程序，条件是不会对这些应用程序应用阻止规则。

     > 在转移 Kaspersky Endpoint Security 设置时，也会转移受信任更新程序创建的可执行文件列表。

   - 创建一个文件夹，并在其中放置想要允许自动安装更新的应用程序的可执行文件。然后使用“**应用程序文件夹**”条件创建应用程序类别，并指定该文件夹的路径。随后创建一个允许规则并选择此类型。

     > 使用“**应用程序文件夹**”条件可能不安全，因为指定文件夹中的任何应用程序都将被允许启动。建议只将使用具有“**应用程序文件夹**”条件的应用程序类别的规则应用于那些必须允许为其自动安装更新的用户。

而是允许列表模式

要确保应用程序控制规则不会阻止工作所需的应用程序，建议启用应用程序控制规则的测试并在创建新规则后分析其运行。启用测试后，Kaspersky Endpoint Security 不会阻止被应用程序控制规则禁止启动的应用程序，但是会将有关它们启动的通知发送给管理服务器。

测试允许列表模式时，建议执行以下操作：

1. 确定测试周期（从几天到两个月）。
2. 启用应用程序控制规则的测试。
3. 检查"应用程序控制"的运行测试所产生的事件和有关测试模式下阻止的应用程序的报告来分析测试结果。
4. 根据分析结果，更改允许列表模式设置。
   特别是，根据测试结果，您可以将与事件相关的可执行文件添加到应用程序类别。

支持允许列表模式

为"应用程序控制"选择阻止操作后，建议执行以下操作以继续支持允许列表模式：

- 检查"应用程序控制"的运行所产生的事件和被阻止运行的报告来分析"应用程序控制"的效果。
- 分析用户的应用程序访问请求。
- 通过在卡巴斯基安全网络中检查信誉信息来分析陌生可执行文件。
- 在安装操作系统或软件的更新前，请在计算机测试组中安装这些更新，以检查应用程序控制规则将如何处理它们。
- 将必要的应用程序添加到应用程序控制规则中使用的类别。

网络端口监控

在 Kaspersky Endpoint Security 运行期间，"Web 控制"、"邮件威胁防护"、"Web 威胁防护"、"行为检测"和"漏洞利用防御"组件将监控通过特定协议传输并经过用户计算机上开放的特定 TCP 和 UDP 端口的数据流。例如，"邮件威胁防护"组件分析通过 SMTP 传输的信息，而"Web 威胁防护"组件分析通过 HTTP 和 FTP 传输的信息。

Kaspersky Endpoint Security 将用户计算机的 TCP 和 UDP 端口根据其组成方式分成多个组。某些网络端口保留用于易受攻击的服务。建议您更全面地监控这些端口，因为它们更有可能成为网络攻击的目标。如果使用依赖非标准网络端口的非标准服务，这些网络端口也可能成为攻击计算机的目标。您可以指定网络端口列表和请求网络访问的应用程序列表。这样在网络流量监控期间，这些端口和应用程序会受到"邮件威胁防护"和"Web 威胁防护"组件的特别关注。

为了确保计算机的安全，行为检测和漏洞利用防御组件还监控通过网络端口的数据流。这些组件持续监控网络流量，以发现可能造成威胁的单个进程。

启用对所有网络端口的监控

要启用对所有网络端口的监控，请执行以下操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**网络设置**”。

网络端口监控设置

3. 在“**受监控端口**”块中，选择“**监控所有网络端口**”。
4. 保存更改。

创建受监控网络端口的列表

更改受监控网络端口列表可能会受到父策略属性的阻止。要更改列表，您需要允许更改以下设置：Web Console 中的受信任区域（“挂锁”必须处于解锁状态）。

管理控制台(MMC) 和 Web Console 中受信任区域的分组方式不同。同样，防止受信任区域参数更改的方式也不同（“挂锁”不同）。我们建议仅使用 Web Console 来管理应用程序。如果在不同的控制台中配置受信任区域，管理插件可能会将“挂锁”重置为其默认状态。

创建受监控的网络端口列表

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**网络设置**”。
3. 在“**受监控端口**”块中，选择“**仅监控选定网络端口**”。
4. 单击“**选择**”。
   这将打开一个常用于传送电子邮件和网络流量的网络端口列表。该网络端口列表包含在 Kaspersky Endpoint Security 数据包中。
5. 使用**状态**栏的开关启用或禁用网络端口监控。
6. 如果某网络端口未在网络端口列表中，请按照以下步骤添加：
   a. 单击“**添加**”。
   b. 在打开的窗口中，输入网络端口号和简短描述。
   c. 为网络端口监控设置**活动**或**非活动**状态。
7. 保存更改。

当 FTP 协议以被动模式运行时，可以通过一个未添加在监控网络端口列表中的随机端口建立连接。要保护此类连接，启用对所有网络端口的监控或配置对建立了 FTP 连接的应用程序的网络端口的控制。

创建所有网络端口受监控的应用程序的列表

您可以创建 Kaspersky Endpoint Security 为其监控所有网络端口的应用程序的列表。

建议您在 Kaspersky Endpoint Security 为其监控所有网络端口的应用程序列表中包括通过 FTP 协议接收或发送数据的应用程序。

要创建所有网络端口受监控的应用程序的列表，请执行以下操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**网络设置**”。
3. 在“**受监控端口**”块中，选择“**仅监控选定网络端口**”。
4. 选择**监控卡巴斯基推荐的列表中的应用程序的所有端口**复选框。
   若选中此复选框，则 Kaspersky Endpoint Security 将监控以下应用程序的所有端口：
   - Adobe Acrobat Reader。
   - Apple Application Support。
   - Google Chrome。

- Microsoft Edge。
- Mozilla Firefox。
- Internet Explorer。
- Java。
- mIRC。
- Opera。
- Pidgin。
- Safari。
- Mail.ru Agent。
- Yandex Browser。

5. 选择**监控指定应用程序的所有端口**复选框。
6. 单击“**选择**”。
   这将打开 Kaspersky Endpoint Security 监控其网络端口的应用程序的列表。
7. 使用**状态**栏的开关启用或禁用网络端口监控。
8. 如果列表中未包含某应用程序，请按照以下步骤添加：
   a. 单击“**添加**”。
   b. 在打开的窗口中，输入应用程序可执行文件的路径和简短描述。
   c. 为网络端口监控设置**活动**或**非活动**状态。
9. 保存更改。

导入和导入受监控端口列表

Kaspersky Endpoint Security 使用以下列表监控网络端口：网络端口列表和其端口在 Kaspersky Endpoint Security 中被监控的应用程序列表。您可以将受监控端口列表导出到 XML 文件。然后可以修改文件，例如，添加大量相同描述的端口。还可以使用导出/导入功能备份受监控端口列表或将列表迁移到其他服务器。

如何在管理控制台(MMC)中导出和导入受监控端口列表

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **网络设置**。

5. 要导出网络端口列表：

   a. 在“**受监控端口**”块中，选择“**仅监控选定网络端口**”。

   b. 单击“**已选定 N 端口**”链接。

      “**网络端口**”窗口将打开。“**网络端口**”窗口中将显示一个常用于传送电子邮件和网络流量的网络端口列表。该网络端口列表包含在 Kaspersky Endpoint Security 数据包中。

   c. 在网络端口列表，选择您要导出的端口。

   d. 单击“**导出**”。

   e. 在打开的窗口中，输入您要将网络端口列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。

   f. 保存文件。

      Kaspersky Endpoint Security 会将整个网络端口列表导出到 XML 文件。

6. 要导出其端口在 Kaspersky Endpoint Security 中被监控的应用程序列表：

   a. 在“**受监控端口**”块中，选中“**监控指定应用程序的所有端口**”复选框。

   b. 单击“**已选定 N 应用程序**”链接。

   c. 在应用程序列表，选择您要导出的应用程序。

   d. 单击“**导出**”。

   e. 在打开的窗口中，指定您要将应用程序列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。

   f. 保存文件。

      Kaspersky Endpoint Security 会将整个应用程序列表导出到 XML 文件。

7. 要导入网络端口列表：

   a. 在网络端口列表中，单击“**导入**”按钮。

      在打开的窗口中，选择要从中导入网络端口列表的 XML 文件。

   b. 打开文件。

      如果计算机已经具有网络端口的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 XML 文件向其中添加新条目。

8. 要导入其端口在 Kaspersky Endpoint Security 中被监控的应用程序列表：

   a. 在应用程序列表中，单击“**导入**”按钮。

      在打开的窗口中，选择要从中导入应用程序列表的 XML 文件。

   b. 打开文件。

      如果计算机已经具有应用程序的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 XML 文件向其中添加新条目。

9. 保存更改。

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **常规设置** → **网络设置**。

4. 在“**受监控端口**”块中，选择“**仅监控选定网络端口**”。

5. 单击“**设置**”。

   “**网络端口**”窗口将打开。“**网络端口**”窗口中将显示一个常用于传送电子邮件和网络流量的网络端口列表。该网络端口列表包含在 Kaspersky Endpoint Security 数据包中。

6. 要导出网络端口列表：

   a. 在网络端口列表，选择您要导出的端口。要选择多个端口，使用 **CTRL** 或 **SHIFT** 键。

      如果您未选择任何端口，Kaspersky Endpoint Security 将导出所有端口。

   b. 单击“**导出**”。

   c. 在打开的窗口中，输入您要将网络端口列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。

   d. 保存文件。

      Kaspersky Endpoint Security 会将整个网络端口列表导出到 XML 文件。

7. 要导出其端口在 Kaspersky Endpoint Security 中被监控的应用程序列表：

   a. 选择**监控指定应用程序的所有端口**复选框。

   b. 在应用程序列表，选择您要导出的应用程序。要选择多个端口，使用 **CTRL** 或 **SHIFT** 键。

      如果您未选择任何应用程序，Kaspersky Endpoint Security 将导出所有应用程序。

   c. 单击“**导出**”。

   d. 在打开的窗口中，指定您要将应用程序列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。

   e. 保存文件。

      Kaspersky Endpoint Security 会将整个应用程序列表导出到 XML 文件。

8. 要导入网络端口列表：

   a. 在网络端口列表中，单击“**导入**”按钮。

      在打开的窗口中，选择要从中导入网络端口列表的 XML 文件。

   b. 打开文件。

      如果计算机已经具有网络端口的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 XML 文件向其中添加新条目。

9. 要导入其端口在 Kaspersky Endpoint Security 中被监控的应用程序列表：

   a. 在应用程序列表中，单击“**导入**”按钮。

      在打开的窗口中，选择要从中导入应用程序列表的 XML 文件。

b. 打开文件。

如果计算机已经具有应用程序的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 XML 文件向其中添加新条目。

10. 保存更改。

日志审查

如果 Kaspersky Endpoint Security 安装在运行 Windows for Servers 的计算机上，则该组件可用。如果 Kaspersky Endpoint Security 安装在运行 Windows for Workstations 的计算机上，则该组件不可用。

从版本 11.11.0 开始，Kaspersky Endpoint Security for Windows 包含日志审查组件。日志检查根据 Windows 事件日志分析监控受保护环境的完整性。当应用程序在系统中检测到非典型行为的迹象时，它会通知管理员，因为该行为可能表示试图进行网络攻击。

Kaspersky Endpoint Security 分析 Windows 事件日志，并根据规则检测违规行为。该组件包括预定义规则。预定义规则由启发式分析提供支持。您还可以添加自己的规则（自定义规则）。当规则触发时，应用程序将创建具有“*严重*”状态的事件（参见下图）。

如果您要使用日志审查，请确保已配置审计策略安全设置，并且系统正在记录相关事件（有关详细信息，请参阅 Microsoft 技术支持网站）。

日志审查通知

配置预定义规则

预定义规则包括受保护计算机上异常活动的模板。异常活动可能表示攻击未遂。预定义规则由启发式分析提供支持。有七条预定义规则可用于日志审查。您可以启用或禁用任意这些规则。无法删除预定义规则。

您可以为监视以下操作事件的规则配置触发条件：

- 密码强力检测
- 网络登录检测

如何在管理控制台（MMC）中配置预定义规则

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **安全控制** → **日志审查**。
4. 确保“**日志审查**”复选框被选中。
5. 在“**预定义规则**”块中单击“**设置**”按钮。
6. 选择或清空复选框以配置预定义规则：
   - “**系统中存在可能的暴力攻击模式**”。
   - “**在网络登录会话期间检测到非典型活动**”。
   - “**存在可能的 Windows 事件日志滥用模式**”。
   - “**检测到代表安装了新服务的非典型操作**”。
   - “**检测到使用显式凭证的非典型登录**”。
   - “**系统中存在可能的 Kerberos 伪造的 PAC (MS14-068) 攻击模式**”。
   - “**在特权内置管理员组中检测到可疑更改**”。
7. 如果必要，配置“**系统中存在可能的暴力攻击模式**”规则：
   a. 单击规则下的“**设置**”按钮。
   b. 在打开的窗口中，指定要触发规则必须尝试输入密码的次数和时间段。
   c. 单击“**确定**”。
8. 如果您选择了“**在网络登录会话期间检测到非典型活动**”规则，您需要配置其设置：
   a. 单击规则下的“**设置**”按钮。
   b. 在“**网络登录检测**”块中，指定时间间隔的开始和结束。

      Kaspersky Endpoint Security 将在所定义期间执行的登录尝试视为异常活动。

      默认情况下，不设置间隔，并且应用程序不监控登录尝试。要让应用程序连续监控登录尝试，请将间隔设置为 12:00 AM - 11:59 PM。间隔的开始和结束不能重合。如果它们相同，则应用程序不会监控登录尝试。

   c. 创建受信任用户和受信任 IP 地址（IPv4 和 IPv6）列表。

      您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。Kaspersky Endpoint Security 不监控这些用户和计算机的登录尝试。

   d. 单击“**确定**”。
9. 保存更改。

如何在 Web Console 和云控制台中配置预定义规则

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **安全控制** → **日志审查**。
5. 确保“**日志审查已启用**”开关已开启。
6. 在“**预定义规则**”块，使用开关启用或及你用预定义规则：
   - “**系统中存在可能的暴力攻击模式**”。
   - “**在网络登录会话期间检测到非典型活动**”。
   - “**存在可能的 Windows 事件日志滥用模式**”。
   - “**检测到代表安装了新服务的非典型操作**”。
   - “**检测到使用显式凭证的非典型登录**”。
   - “**系统中存在可能的 Kerberos 伪造的 PAC (MS14-068) 攻击模式**”。

   a. “**在特权内置管理员组中检测到可疑更改**”。
7. 如果必要，配置“**系统中存在可能的暴力攻击模式**”规则：
   a. 单击规则下方的“**设置**”。
   b. 在打开的窗口中，指定要触发规则必须尝试输入密码的次数和时间段。
   c. 单击“**确定**”。
8. 如果您选择了“**在网络登录会话期间检测到非典型活动**”规则，您需要配置其设置：
   a. 单击规则下方的“**设置**”。
   b. 在“**网络登录检测**”块中，指定时间间隔的开始和结束。
      Kaspersky Endpoint Security 将在所定义期间执行的登录尝试视为异常活动。
      默认情况下，不设置间隔，并且应用程序不监控登录尝试。要让应用程序连续监控登录尝试，请将间隔设置为 12:00 AM - 11:59 PM。间隔的开始和结束不能重合。如果它们相同，则应用程序不会监控登录尝试。
   c. 在“**排除项**”块，添加受信任用户和受信任 IP 地址（IPv4 和 IPv6）。
      您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。Kaspersky Endpoint Security 不监控这些用户和计算机的登录尝试。
   d. 单击“**确定**”。
9. 保存更改。

如何在应用程序界面中配置预定义规则

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**安全控制**” → “**日志审查**”。
3. 确保“**日志审查**”开关已开启。
4. 在“**预定义规则**”块中单击“**配置**”按钮。
5. 选择或清空复选框以配置预定义规则：
   - “**系统中存在可能的暴力攻击模式**”。
   - “**在网络登录会话期间检测到非典型活动**”。
   - “**存在可能的 Windows 事件日志滥用模式**”。
   - “**检测到代表安装了新服务的非典型操作**”。
   - “**检测到使用显式凭证的非典型登录**”。
   - “**系统中存在可能的 Kerberos 伪造的 PAC (MS14-068) 攻击模式**”。

   a. “**在特权内置管理员组中检测到可疑更改**”。
6. 如果必要，配置“**系统中存在可能的暴力攻击模式**”规则：
   a. 单击规则下方的“**设置**”。
   b. 在打开的窗口中，指定要触发规则必须尝试输入密码的次数和时间段。
7. 如果您选择了“**在网络登录会话期间检测到非典型活动**”规则，您需要配置其设置：
   a. 单击规则下方的“**设置**”。
   b. 在“**网络登录检测**”块中，指定时间间隔的开始和结束。

      Kaspersky Endpoint Security 将在所定义期间执行的登录尝试视为异常活动。

      默认情况下，不设置间隔，并且应用程序不监控登录尝试。要让应用程序连续监控登录尝试，请将间隔设置为 12:00 AM - 11:59 PM。间隔的开始和结束不能重合。如果它们相同，则应用程序不会监控登录尝试。

   c. 在“**排除项**”块，添加受信任用户和受信任 IP 地址（IPv4 和 IPv6）。

      您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。Kaspersky Endpoint Security 不监控这些用户和计算机的登录尝试。
8. 保存更改。

因此，当触发规则时，Kaspersky Endpoint Security 创建“*关键事件*”。

添加自定义规则

您可以设置自己的日志审查规则和触发条件。为此，您必须输入事件 ID 并选择事件源。您可以在 Microsoft 技术支持网站上查找事件 ID。您可以从标准日志中选择事件源： *Application*、 *Security*或*System*。您还可以指定第三方应用程序的日志。您可以使用事件查看器工具查找第三方应用程序日志的名称。第三方应用程序日志保存在应用程序和服务日志文件夹中（例如， *Windows PowerShell* 日志）。

> 应用程序不检查指定的日志是否实际存在于 Windows 事件日志中。如果日志名称有错误，则应用程序不会监控该日志中的事件。

自定义规则列表已经包括卡巴斯基专家创建的三个规则。

如何在管理控制台 (MMC) 中添加自定义规则

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **安全控制** → **日志审查**。
4. 确保“**日志审查**”复选框被选中。
5. 在“**自定义规则**”块中单击“**设置**”按钮。
6. 在打开的窗口中，选中要启用的自定义规则旁边的复选框。
7. 如有必要，单击“**添加**”创建您自己的自定义规则。
8. 这打开了一个窗口；在该窗口中，配置自定义规则：
   - “**规则名称**”。
   - “**日志名称**”。Windows 事件日志。有以下日志可用： *Application*、 *Security*、 *System*。
   - “**源**”。第三方应用程序日志。您可以使用事件查看器工具查找第三方应用程序日志的名称。第三方应用程序日志保存在应用程序和服务日志文件夹中（例如， *Windows PowerShell* 日志）。
   - “**事件标识符**”。Windows 事件日志中的事件 ID。您可以在 Microsoft 技术文档中查找事件 ID。
9. 保存更改。

如何在 Web Console 和云控制台中添加自定义规则

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **安全控制** → **日志审查**。

5. 确保“**日志审查已启用**”开关已开启。

6. 在**自定义规则**块，选择您要启用的自定义规则。

7. 如有必要，单击“**添加**”创建您自己的自定义规则。

8. 这打开了一个窗口；在该窗口中，配置自定义规则：

   - “**规则名称**”。
   - “**自定义日志名称**”。Windows 事件日志。有以下日志可用： *Application*、*Security*、*System*。
   - “**来源**”。第三方应用程序日志。您可以使用事件查看器工具查找第三方应用程序日志的名称。第三方应用程序日志保存在应用程序和服务日志文件夹中（例如， *Windows PowerShell* 日志）。
   - “**事件标识符**”。Windows 事件日志中的事件 ID。您可以在 Microsoft 技术文档 中查找事件 ID。

9. 保存更改。

如何在应用程序界面中添加自定义规则

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**安全控制**” → “**日志审查**”。

3. 确保“**日志审查**”开关已开启。

4. 在“**自定义规则**”块中单击“**配置**”按钮。

5. 在打开的窗口中，选中要启用的自定义规则旁边的复选框。

6. 如有必要，单击“**添加**”创建您自己的自定义规则。

7. 这打开了一个窗口；在该窗口中，配置自定义规则：

   - “**规则名称**”。
   - “**日志名称**”。Windows 事件日志。有以下日志可用： *Application*、*Security*、*System*。
   - “**源**”。第三方应用程序日志。您可以使用事件查看器工具查找第三方应用程序日志的名称。第三方应用程序日志保存在应用程序和服务日志文件夹中（例如， *Windows PowerShell* 日志）。
   - “**事件标识符**”。Windows 事件日志中的事件 ID。您可以在 Microsoft 技术文档 中查找事件 ID。

8. 保存更改。

因此，当触发规则时，Kaspersky Endpoint Security 创建“*严重*”事件。

系统完整性监控

如果 Kaspersky Endpoint Security 安装在运行 Windows for Servers 的计算机上，则该组件可用。如果 Kaspersky Endpoint Security 安装在运行 Windows for Workstations 的计算机上，则该组件不可用。

从 12.6 版本开始，Kaspersky Endpoint Security for Windows 包含系统完整性监控组件，而不是文件完整性监控组件。系统完整性监控组件包括文件完整性监控的所有功能，另外还允许监控注册表更改和外部设备的连接。

系统完整性监控组件监控操作系统中可能预示计算机安全漏洞的变化。当检测到此类变化时，Kaspersky Endpoint Security 会生成相应的事件并向管理员发出警报。系统完整性监控可以实时运行，也可以根据需要执行系统完整性检查。

实时系统完整性监控

在实时模式下，系统完整性监控跟踪组件范围（*监控范围*）中包含的对象中的更改。系统完整性监控还允许实时阻止对此类对象的未经授权的访问。

按需系统完整性检查

按需系统完整性检查是一项您可以手动或按计划运行的任务。要运行“*系统完整性检查*”任务，您必须配置组件的范围（*监控范围*）并创建基线。*基线*是系统中对象的记录状态，应用程序在与当前状态进行比较时以其作为参考。

迁移文件完整性监控设置

当您将 Kaspersky Endpoint Security 更新至 12.6 版本时，文件完整性监控设置会自动迁移。作为迁移的一部分，应用程序将监控规则移动到系统完整性监控。在以下情况下，文件完整性监控规则也会迁移到系统完整性监控：从 KSWS 迁移到 KES。

> 为了确保系统完整性监控正常运行，Kaspersky Endpoint Security 应用程序和管理插件应更新至 12.6 版本。如果您安装了早期版本的管理插件，则无法配置系统完整性监控，因为管理插件缺少“**系统完整性监控**”部分。

关于系统完整性监控规则

要使系统完整性监控正常工作，您必须添加至少一个规则。*系统完整性监控规则*是一组定义用户对文件和注册表的访问权限的标准。系统完整性监控检测指定*监测范围*内文件和注册表的更改。监控范围是系统完整性监控规则的标准之一。

系统完整性监控允许监控以下对象：

- 文件
- 注册表
- 外部设备

文件监控中涉及的特殊注意事项

系统完整性监控监控文件和文件夹的变化以及添加到监控范围或从监控范围中删除的文件。这些更改可能表明存在计算机安全漏洞。我们建议添加很少修改的对象或只有管理员才能访问的对象。这将帮助减少系统完整性监控事件的数量。

> 系统完整性监控不会监控服务器共享文件夹中文件的更改。系统完整性监控只能在本地使用。

Kaspersky Endpoint Security 仅监控实时系统完整性监控开始运行时连接的磁盘上的文件和文件夹的变化。如果实时系统完整性监控开始运行时未连接磁盘，则即使将文件和文件夹添加到监控范围，应用程序也不会监控该磁盘上文件和文件夹的变化。

注册表监控中涉及的特殊注意事项

系统完整性监控负责监控注册表。这些更改可能表明存在计算机安全漏洞。

系统完整性监控监控注册表的以下根键：

- HKCR
- HKLM
- HKU
- HKCC
- HKEY_CLASSES_ROOT
- HKEY_LOCAL_MACHINE
- HKEY_USERS
- HKEY_CURRENT_CONFIG（仅在实时系统完整性监控中可用）
- HKEY_CURRENT_USER（仅在实时系统完整性监控中可用）

> “*系统完整性检查*”任务不支持 HKEY_CURRENT_USER 键。您可以指定 HKEY_USERS 下的一个键，作为 HKEY_USERS\<user profile ID>\<key>。

外部设备监控涉及的特殊注意事项

系统完整性监控监控外部设备的连接和断开连接。这对于保护计算机免受与此类设备进行文件交换所导致的安全威胁是必要的。系统完整性监控不会监控对外部设备的访问，也不会阻止文件交换。您可以使用不同的应用程序组件配置对设备的访问，例如设备控制。

> 当运行“*基线系统完整性监控*”任务时，如果外部设备在操作系统中具有相同的驱动器号，则应用程序将忽略该设备的重新连接。为了记录，重新连接的设备必须具有不同的驱动器号。

系统完整性监控监视以下类型的外部设备的连接：

- 可移动驱动器 （包括 USB 闪存驱动器）
- 硬盘驱动器
- 外部网络适配器
- CD/DVD/Blu-ray 驱动器
- 扫描仪/摄像头

实时系统完整性监控

系统完整性监控允许实时跟踪操作系统的变化。您可以跟踪可能表明计算机存在安全漏洞的变化。该组件允许阻止这些更改或仅记录更改事件。

要使系统完整性监控正常工作，您必须添加至少一个规则。*系统完整性监控规则*是一组定义用户对文件和注册表的访问权限的标准。系统完整性监控检测指定*监测范围*内文件和注册表的更改。监控范围是系统完整性监控规则的标准之一。

实时系统完整性监控模式

为了确保系统完整性监控规则不会阻止任何对操作系统或其他服务的运行至关重要的资源的操作，我们建议启用测试模式并分析组件如何影响系统。启用测试模式后，Kaspersky Endpoint Security 不会阻止规则禁止的用户活动，而是生成“*警告*” ⚠ 事件。

实时系统完整性监控组件有两种模式：

- 阻止

  在这种模式下，系统完整性监控会跟踪系统中的变化并根据规则执行操作：“**允许**”或者“**阻止**”。系统完整性监控还会生成相应的事件并改变 Kaspersky Security Center 控制台中设备的状态。

- 通知

  在这种模式下，系统完整性监控允许对监控范围内的文件和注册表项执行操作。如果禁止对文件或注册表进行操作，应用程序将生成一个事件：*在测试模式下允许执行禁止的操作*。要分析规则如何影响系统，你可以查看报告。

启用实时系统完整性监控

如何在管理控制台 (MMC) 中启用实时系统完整性监控

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **安全控制** → **系统完整性监控**。
4. 选择**系统完整性监控**复选框。
5. 在“**阻止规则的操作模式**”下，选择实时系统完整性监控的模式：
   - “**阻止**”。在此模式下，系统完整性监控会阻止对监控范围内的文件和注册表项的操作，并生成相应的事件。
   - “**通知**”。在此模式下，系统完整性监控会允许对监控范围内的文件和注册表项的操作，并生成相应的事件。
6. 在“**实时系统完整性监控**”块中，选中“**实时系统完整性监控**”复选框。
7. 配置外部设备监控：
   a. 选择**监控设备**复选框。
   b. 在“**事件严重级别**”下拉列表中，选择外部设备监控事件的重要性级别：*信息*、*警告*、*关键*。

   系统完整性监控记录外部设备的当前连接。在应用程序设置中启用该组件后，应用程序开始监控外部设备的连接和断开连接。随后，当外部设备连接或者断开时，应用程序就会产生相应的事件。
8. 配置文件和注册表监控：
   a. 选择**监控文件和注册表**复选框。
   b. 单击“**设置**”。
   这将打开系统完整性监控规则列表。
   c. 单击“**添加**”。
   您也可以从其他来源导入规则。
   d. 配置系统完整性监控规则（见下表）。
9. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 中启用实时系统完整性监控

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。

4. 选择 **安全控制** → **系统完整性监控**。

5. 开启 **系统完整性监控已启用**切换开关。

6. 选择Windows选项卡。

7. 在“**实时系统完整性监控**”下，选择实时系统完整性监控的模式：

   - “**应用规则**”。在此模式下，系统完整性监控会阻止对监控范围内的文件和注册表项的操作，并生成相应的事件。

   - “**测试规则(通知)**”。在此模式下，系统完整性监控会允许对监控范围内的文件和注册表项的操作，并生成相应的事件。

8. 配置文件和注册表监控：

   a. 选择**监控文件和注册表**复选框。

   b. 单击“**规则**”。

      这将打开系统完整性监控规则列表。

   c. 单击“**添加**”。

      您也可以从其他来源导入规则。

   d. 配置系统完整性监控规则（见下表）。

9. 配置外部设备监控：

   a. 选择**监控设备**复选框。

   b. 在“**事件严重级别**”下拉列表中，选择外部设备监控事件的重要性级别：*信息*、*警告*、*关键*。

   系统完整性监控记录外部设备的当前连接。在应用程序设置中启用该组件后，应用程序开始监控外部设备的连接和断开连接。随后，当外部设备连接或者断开时，应用程序就会产生相应的事件。

10. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在应用程序界面中启用实时系统完整性监控

1. 打开主应用程序窗口并单击 按钮。

2. 在应用程序设置窗口中，选择“**安全控制**” → “**系统完整性监控**”。

3. 打开“**系统完整性监控**”切换开关。

4. 在“**阻止规则的操作模式**”下，选择实时系统完整性监控的模式：

   - “**阻止**”。在此模式下，系统完整性监控会阻止对监控范围内的文件和注册表项的操作，并生成相应的事件。

   - “**通知**”。在此模式下，系统完整性监控会允许对监控范围内的文件和注册表项的操作，并生成相应的事件。

5. 在“**实时系统完整性监控**”块中，选中“**实时系统完整性监控**”复选框。

6. 配置外部设备监控：

   a. 选择**监控设备**复选框。

   b. 在“**事件严重级别**”下拉列表中，选择外部设备监控事件的重要性级别：*信息*、*警告*、*关键*。

   系统完整性监控记录外部设备的当前连接。在应用程序设置中启用该组件后，应用程序开始监控外部设备的连接和断开连接。随后，当外部设备连接或者断开时，应用程序就会产生相应的事件。

7. 配置文件和注册表监控：

   a. 选择**监控文件和注册表**复选框。

   b. 单击“**设置**”。

      这将打开系统完整性监控规则列表。

   c. 单击“**添加**”。

      您也可以从其他来源导入规则。

8. 配置系统完整性监控规则（见下表）。

9. 保存更改。

实时系统完整性监控规则设置

参数	描述
规则名称	实时系统完整性监控规则的名称
对文件和注册表的操作	• “**允许**”。系统完整性监控允许对监控范围内的文件和注册表项执行操作。 • “**阻止**”。系统完整性监控行为取决于所选的模式。如果您选择了“*系统保护模式*”，系统完整性监控阻止对监控范围内的文件和注册表项执行操作，生成相应事件，并在 Kaspersky Security Center 控制台中更改设备的状态。如果您选择了“*测试模式*”，系统完整性监控允许对监控范围内的文件和注册表项执行操作。

参数	描述
事件严重级别	Kaspersky Endpoint Security 在监控范围内的文件或注册表项被修改时记录文件修改事件。以下事件严重性级别可用：*信息*，*警告*，*关键*。
监控范围	• "**文件**"。组件监控的文件和文件夹列表。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。 使用掩码： • `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\*\*.txt` 将包括位于 C: 驱动器的文件夹（但不包括子文件夹）中所有具有 TXT 扩展名的文件的路径。 • 两个连续 `*` 字符在文件或文件夹名称中代表任意一组字符（包括空集），包括 `\` 和 `/` 字符（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\**\*.txt` 将包括位于 `Folder` 嵌套子文件夹（除了 `Folder` 本身）中所有带 TXT 扩展名的文件的路径。掩码必须包含至少一个嵌套级别。掩码 `C:\**\*.txt` 不是有效掩码。 • `?`（问号）字符代表任意单个字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\???.txt` 将包括位于 `Folder` 文件夹中所有带 TXT 扩展名且名称由三个字符构成的文件的路径。 • "**注册表**"。组件监控的注册表项和值的列表。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。
排除项	• "**文件**"。监控范围的排除项列表。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。例如，`C:\Folder\Application\*.log`。排除项的优先级高于监控范围。 使用掩码： • `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\*\*.txt` 将包括位于 C: 驱动器的文件夹（但不包括子文件夹）中所有具有 TXT 扩展名的文件的路径。 • 两个连续 `*` 字符在文件或文件夹名称中代表任意一组字符（包括空集），包括 `\` 和 `/` 字符（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\**\*.txt` 将包括位于 `Folder` 嵌套子文件夹（除了 `Folder` 本身）中所有带 TXT 扩展名的文件的路径。掩码必须包含至少一个嵌套级别。掩码 `C:\**\*.txt` 不是有效掩码。 • `?`（问号）字符代表任意单个字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\???.txt` 将包括位于 `Folder` 文件夹中所有带 TXT 扩展名且名称由三个字符构成的文件的路径。 • "**注册表**"。监控范围的排除项列表。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。排除项的优先级高于监控范围。
受信任的用户和/或用户组	*受信任的用户*是被允许对监控范围内的文件和注册表项执行操作的用户。如果 Kaspersky Endpoint Security 检测到受信任用户执行的操作，系统完整性监控会生成"*信息*"事件。 您可以在 Active Directory 中、在 Kaspersky Security Center 的账户列表中或通过手动输入本地用户名来选择用户。卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。
文件操作标记 / 监控的操作	使用应用程序将监控的文件或注册表项来描述操作的标记。
哈希	在修改时计算文件哈希值。当事件生成时，Kaspersky Endpoint Security 会添加有关文件哈希值的信息。

按需系统完整性检查

按需系统完整性检查是一项您可以手动或按计划运行的任务。运行"*系统完整性检查*"任务时，应用程序将监控范围内的对象的当前状态与其*基线*状态进行比较。与实时系统完整性监控相比，"*系统完整性检查*"任务有助于限制事件的数量，并允许您生成操作系统变化的总体报告。

要使系统完整性监控正常工作，您必须添加至少一个规则。*系统完整性监控规则*是一组定义用户对文件和注册表的访问权限的标准。系统完整性监控检测指定*监测范围*内文件和注册表的更改。监控范围是系统完整性监控规则的标准之一。您可以配置实时系统完整性监控和"*系统完整性检查*"任务共享的规则，或为该任务创建单独的规则。为了创建基线，Kaspersky Endpoint Security 将"*系统完整性检查*"任务的监控范围应用到"*基线更新*"任务。

创建和更新基线

“*系统完整性检查*”任务需要基线才能进行。*基线*是系统中对象的记录状态，应用程序在与当前状态进行比较时以其作为参考。如果系统的当前状态与基线记录的系统状态不同，Kaspersky Endpoint Security 会生成相应的事件。您可以使用“*基线更新*”任务创建或更新基线。

您可以在以下模式中更新基线：

- 完整更新。
  应用程序更新监控范围内的所有对象。
- 增量更新。
  该应用程序仅检测和更新已修改或新的对象。

如何在管理控制台 (MMC) 中创建或更新基线

1. 在 Kaspersky Security Center 管理控制台树中，选择“**任务**”。
   任务列表打开。
2. 单击“**新任务**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 选择任务类型

选择“**Kaspersky Endpoint Security for Windows (14.1)**”→ “**基线更新**”。

步骤2. 选择基线更新模式

选择基线更新模式：

- “**完整更新**”。应用程序更新监控范围内的所有对象。
- “**增量更新**”。该应用程序仅检测和更新已修改或新的对象。

步骤 3. 选择任务将分配到的设备

选择将要执行任务的计算机。下列选项可用：

- 将任务分配给管理组。在这种情况下，任务分配给先前创建的管理组中包括的计算机。
- 选择管理服务器在网络中检测到的计算机：*未分配设备*。特定设备可包括管理组中的设备以及未分配设备。
- 手动指定设备地址或从列表中导入地址。您可以指定您要将任务分配给的设备的 NetBIOS 名称、IP 地址和 IP 子网。

步骤 4. 定义任务名称

输入任务的名称，例如“*基线 2024*”。

步骤 5. 完成任务创建

退出向导。如有必要，选中“**向导完成时运行任务**”复选框。您可以在任务属性中监控任务进度。

如何在 Web Console 中创建或更新基线

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
2. 单击“**添加**”。
   “任务向导”将启动。
3. 配置任务设置：
   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Endpoint Security for Windows 14.2.0**”。
   b. 在“**任务类型**”下拉列表中，选择“**基线更新**”。
   c. 在“**任务名称**”字段中，输入简要说明，例如“*基线 2024*”。
   d. 在“**要对其分配任务的设备**”块，选择任务范围。
4. 按照所选任务范围选项选择设备。转到下一步。
5. 选择要运行任务的账户。默认情况下，Kaspersky Endpoint Security 将使用本地用户账户的权限启动任务。
6. 退出向导。
   在任务列表中将显示一个新任务。
7. 单击新任务。
   任务属性窗口将打开。

8. 选择**应用程序设置**选项卡。

9. 选择基线更新模式：

   - “**完整更新**”。应用程序更新监控范围内的所有对象。

   - “**增量更新**”。该应用程序仅检测和更新已修改或新的对象。

10. 保存更改。

11. 选中该任务旁边的复选框。

12. 单击“**开始**”。

配置“系统完整性检查”任务的监控范围

默认情况下，“*系统完整性检查*”任务的监控范围与实时系统完整性监控的监控范围相同。您可以为任务配置不同的监控范围。

> 系统完整性监控不支持为“*系统完整性检查*”任务导入键 `HKEY_CURRENT_USER` 和 `HKEY_CURRENT_CONFIG`。如果任务的监控范围包含这些键，应用程序将生成“*监控范围包括错误对象*”事件。

如何在管理控制台 (MMC) 中为“系统完整性检查”任务配置不同的监控范围

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **安全控制** → **系统完整性监控**。

4. 选择**系统完整性监控**复选框。

5. 在“**系统完整性检查**”下，选择任务配置模式：**自定义设置**。

6. 配置外部设备监控：

   a. 选择**监控设备**复选框。

   b. 在“**事件严重级别**”下拉列表中，选择外部设备监控事件的重要性级别：*信息*、*警告*、*关键*。

   系统完整性监控记录基线创建时所连接的外部设备的信息。随后，当外部设备连接时，应用程序就会产生相应的事件。运行“*系统完整性检查*”任务时，应用程序不会监控外部设备的断开连接。

7. 配置文件和注册表监控：

   a. 选择**监控文件和注册表**复选框。

   b. 单击“**设置**”。

      这将打开系统完整性监控规则列表。

c. 单击“**添加**”。
   您也可以从其他来源导入规则。

d. 配置系统完整性监控规则（见下表）。

8. 保存更改。

如何在 Web Console 中为“系统完整性检查”任务配置不同的监控范围

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **安全控制** → **系统完整性监控**。

5. 选择**Windows**选项卡。

6. 开启 **系统完整性监控已启用**切换开关。

7. 在“**系统完整性检查**”下，选择任务配置模式：**自定义设置**。

8. 配置外部设备监控：

   a. 选择**监控设备**复选框。

   b. 在“**事件严重级别**”下拉列表中，选择外部设备监控事件的重要性级别：*信息*、*警告*、*关键*。

   系统完整性监控记录基线创建时所连接的外部设备的信息。随后，当外部设备连接时，应用程序就会产生相应的事件。运行“*系统完整性检查*”任务时，应用程序不会监控外部设备的断开连接。

9. 配置文件和注册表监控：

   a. 选择**监控文件和注册表**复选框。

   b. 单击“**规则**”。
      这将打开系统完整性监控规则列表。

   c. 单击“**添加**”。
      您也可以从其他来源导入规则。

   d. 配置系统完整性监控规则（见下表）。

10. 保存更改。

如何在应用程序界面中为“系统完整性检查”任务配置不同的监控范围

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**安全控制**” → “**系统完整性监控**”。

3. 打开“**系统完整性监控**”切换开关。

4. 在“**系统完整性检查**”下，选择任务配置模式：**自定义设置**。

5. 配置外部设备监控：

   a. 选择**监控设备**复选框。

   b. 在“**事件严重级别**”下拉列表中，选择外部设备监控事件的重要性级别：*信息*、*警告*、*关键*。

   系统完整性监控记录基线创建时所连接的外部设备的信息。随后，当外部设备连接时，应用程序就会产生相应的事件。运行“*系统完整性检查*”任务时，应用程序不会监控外部设备的断开连接。

6. 配置文件和注册表监控：

   a. 选择**监控文件和注册表**复选框。

   b. 单击“**设置**”。

      这将打开系统完整性监控规则列表。

   c. 单击“**添加**”。

      您也可以从其他来源导入规则。

   d. 配置系统完整性监控规则（见下表）。

7. 保存更改。

参数	描述
规则名称	“*系统完整性检查*”任务规则名称。
事件严重级别	Kaspersky Endpoint Security 在监控范围内的文件或注册表项被修改时记录文件修改事件。以下事件严重性级别可用：*信息*, *警告*, *关键*。

监控范围	• “**文件**”。组件监控的文件和文件夹列表。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。
	使用掩码：
	  • `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\*\*.txt` 将包括位于 C: 驱动器的文件夹（但不包括子文件夹）中所有具有 TXT 扩展名的文件的路径。
	  • 两个连续 `*` 字符在文件或文件夹名称中代表任意一组字符（包括空集），包括 `\` 和 `/` 字符（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\**\*.txt` 将包括位于 `Folder` 嵌套子文件夹（除了 `Folder` 本身）中所有带 TXT 扩展名的文件的路径。掩码必须包含至少一个嵌套级别。掩码 `C:\**\*.txt` 不是有效掩码。
	  • `?`（问号）字符代表任意单个字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\???.txt` 将包括位于 `Folder` 文件夹中所有带 TXT 扩展名且名称由三个字符构成的文件的路径。
	• “**注册表**”。组件监控的注册表项和值的列表。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。

排除项	• “**文件**”。监控范围的排除项列表。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。例如，`C:\Folder\Application\*.log`。排除项的优先级高于监控范围。
	使用掩码：
	  • `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\*\*.txt` 将包括位于 C: 驱动器的文件夹（但不包括子文件夹）中所有具有 TXT 扩展名的文件的路径。
	  • 两个连续 `*` 字符在文件或文件夹名称中代表任意一组字符（包括空集），包括 `\` 和 `/` 字符（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\**\*.txt` 将包括位于 `Folder` 嵌套子文件夹（除了 `Folder` 本身）中所有带 TXT 扩展名的文件的路径。掩码必须包含至少一个嵌套级别。掩码 `C:\**\*.txt` 不是有效掩码。
	  • `?`（问号）字符代表任意单个字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\???.txt` 将包括位于 `Folder` 文件夹中所有带 TXT 扩展名且名称由三个字符构成的文件的路径。
	• “**注册表**”。监控范围的排除项列表。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。排除项的优先级高于监控范围。

运行“系统完整性检查”任务

“*系统完整性检查*”任务允许检查文件或注册表项是否发生变化，还可以检查外部设备的连接。要检查文件是否有更改，您可以在下列模式中运行“*系统完整性检查*”任务：

- 快速扫描。

  检查文件是否有变化时，应用程序只检查文件属性。应用程序不检查文件的内容。

- 全盘扫描。

  在检查文件是否有更改时，应用程序会检查所有文件属性和文件的内容。

任务运行的模式不会影响注册表或外部设备的检查。

如何在管理控制台 (MMC) 中运行“系统完整性检查”任务

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**任务**”。

   任务列表打开。

3. 单击“**新任务**”。
   “任务向导”将启动。按照向导的说明进行操作。

4. 选择“**Kaspersky Endpoint Security → 基线系统完整性监控**”。选择系统完整性监控模式：

   - “**全盘扫描**”。在这种模式下，应用程序会检查文件的所有属性和哈希值。
   - “**快速扫描**”。在这种模式下，应用程序仅检查文件的属性。

5. 选择将要执行任务的计算机。下列选项可用：

   - 选择管理服务器在网络中检测到的计算机：未分配设备。特定设备可包括管理组中的设备以及未分配设备。
   - 手动指定设备地址或从列表中导入地址。您可以指定您要将任务分配给的设备的 NetBIOS 名称、IP 地址和 IP 子网。
   - 指定要运行任务的设备分类。
   - 将任务分配给管理组。在这种情况下，任务分配给先前创建的管理组中包括的计算机。

6. 选择要运行任务的账户。默认情况下，Kaspersky Endpoint Security 将使用本地用户账户的权限启动任务。

7. 配置任务启动计划，例如，手动或在周中的特定天。

8. 输入任务的名称。

9. 退出向导。如有必要，选中“**向导完成时运行任务**”复选框。您可以在任务属性中监控任务进度。

如何在 Web Console 中运行“系统完整性检查”任务

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。

2. 单击“**添加**”。
   “任务向导”将启动。

3. 配置任务设置：

   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Endpoint Security for Windows 14.2.0**”。

   b. 在“**任务类型**”下拉列表中，选择“**系统完整性检查**”。

   c. 在“**任务名称**”字段中，输入简要说明，例如“*每周系统完整性检查*”。

   d. 在“**要对其分配任务的设备**”块，选择任务范围。

4. 按照所选任务范围选项选择设备。转到下一步。

5. 选择要运行任务的账户。默认情况下，Kaspersky Endpoint Security 将使用本地用户账户的权限启动任务。

6. 退出向导。
   在任务列表中将显示一个新任务。

7. 单击新任务。
   任务属性窗口将打开。

8. 选择**应用程序设置**选项卡。

9. 选择系统完整性检查模式：

   - "**快速扫描**"。应用程序仅检查文件属性。应用程序不检查文件的内容。
   - "**全盘扫描**"。应用程序检查文件的所有属性及其内容。

10. 保存更改。

11. 选中该任务旁边的复选框。

12. 单击"**开始**"。

为了"*系统完整性检查*"任务顺利完成，"*系统完整性检查*"任务的监控范围必须完全匹配基线。如果监控范围不同，任务将以错误结束。要同步监控范围，请运行具有新的监控范围的"*基线更新*"任务。

导出和导入系统完整性监控规则

您可以将系统完整性监控规则列表导出到 XML 文件。然后可以修改文件，例如，添加大量相同类型的记录。您还可以使用导出/导入功能备份系统完整性监控规则列表或将列表迁移到其他服务器。

> 系统完整性监控不支持为"*系统完整性检查*"任务导入键 `HKEY_CURRENT_USER` 和 `HKEY_CURRENT_CONFIG`。如果任务的监控范围包含这些键，应用程序将生成"*监控范围包括错误对象*"事件。

如何在管理控制台 (MMC) 中导出和导入系统完整性监控规则列表

1. 在 Kaspersky Security Center 管理控制台树中，选择"**策略**"。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **安全控制** → **系统完整性监控**。

4. 要导出或导入*实时系统完整性监控*规则：

   a. 在"**实时系统完整性监控**"块中单击"**设置**"按钮。

   b. 要导出实时系统完整性监控规则列表：

      1. 选择您要导出的规则。要选择多个端口，使用 **CTRL** 或 **SHIFT** 键。
         如果您未选择任何规则，Kaspersky Endpoint Security 将导出所有规则。

      2. 单击**导出**链接。

      3. 在打开的窗口中，指定您要将规则列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。

      4. 保存文件。
         Kaspersky Endpoint Security 会将整个规则列表导出到 XML 文件。

c. 要导入实时系统完整性监控规则列表：

1. 单击**导入**链接。

   在打开的窗口中，选择要从中导入规则列表的 XML 文件。

2. 打开文件。

   如果计算机已经具有规则的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 XML 文件向其中添加新条目。

5. 要导出或导入*系统完整性检查*规则：

a. 在“**系统完整性检查**”块中，选择“**自定义设置**”。

b. 单击“**设置**”。

c. 要导出系统完整性检查规则列表：

1. 选择您要导出的规则。要选择多个端口，使用 **CTRL** 或 **SHIFT** 键。

   如果您未选择任何规则，Kaspersky Endpoint Security 将导出所有规则。

2. 单击**导出**链接。

3. 在打开的窗口中，指定您要将规则列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。

4. 保存文件。

Kaspersky Endpoint Security 会将整个规则列表导出到 XML 文件。

d. 要导入系统完整性检查规则列表：

1. 单击**导入**链接。

   在打开的窗口中，选择要从中导入规则列表的 XML 文件。

2. 打开文件。

如果计算机已经具有规则的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 XML 文件向其中添加新条目。

6. 保存更改。

如何在 Web Console 中导出和导入系统完整性监控规则列表

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **安全控制** → **系统完整性监控**。

5. 选择**Windows**选项卡。

6. 要导出或导入*实时系统完整性监控*规则：

   a. 在“**实时系统完整性监控**”区域，单击“**规则**”链接。

   b. 要导出实时系统完整性监控规则列表：

      1. 选择您要导出的规则。

      2. 单击“ → **导出**”按钮。

         Kaspersky Endpoint Security 导出规则列表到默认下载文件夹中的 JSON 文件。

   c. 要导入实时系统完整性监控规则列表：

      1. 单击“ → **导入**”按钮。

         在打开的窗口中，选择要从中导入受信任地址列表的 JSON 文件。

      2. 打开文件。

         如果计算机已经具有规则的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 JSON 文件向其中添加新条目。

7. 要导出或导入*系统完整性检查*规则：

   a. 在“**按需系统完整性检查**”块中，选择“**自定义设置**”。

   b. 单击**规则**链接。

   c. 要导出系统完整性检查规则列表：

      1. 选择您要导出的规则。

      2. 单击“ → **导出**”按钮。

         Kaspersky Endpoint Security 导出规则列表到默认下载文件夹中的 JSON 文件。

   d. 要导入系统完整性检查规则列表：

      1. 单击“ → **导入**”按钮。

         在打开的窗口中，选择要从中导入受信任地址列表的 JSON 文件。

      2. 打开文件。

         如果计算机已经具有规则的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 JSON 文件向其中添加新条目。

8. 保存更改。

查看系统完整性监控报告

要分析系统完整性监控规则的性能，您可以查看应用程序生成的报告和事件。Kaspersky Endpoint Security 生成有关该组件的以下报告：

- 在应用程序界面中：
  - 系统完整性监控报告
  - 系统完整性检查报告
  - 基线更新报告

  报告包含系统完整性监控事件。
- 在 Kaspersky Security Center 控制台中:
  - 监控规则触发次数最多的计算机报告
  - 最常触发的监控规则报告

  默认情况下，将创建前 30 天的报告，包括创建报告的日期。

  如何在管理控制台 (MMC) 中查看系统完整性监控报告

  1. 打开 Kaspersky Security Center Administration Console。
  2. 在管理控制台树的“**管理服务器**”中选择“**报告**”选项卡。
  3. 单击“**新建报告模板**”。

     “新报告模板向导”将启动。
  4. 按照“报告模板向导”的说明进行操作。在“**选择报告模板类型**”步骤，选择系统完整性监控报告（“**其他**”部分）：
     - “**文件完整性监控/系统完整性监控规则触发最频繁的 10 台设备**”。
     - “**在设备上触发次数最频繁的 10 条文件完整性监控/系统完整性监控规则**”。

     完成新报告模板向导之后，新报告模板将出现在“**报告**”选项卡上。
  5. 双击报告将其打开。

  报告生成过程将开始。该报告将显示在新窗口中。

  如何在 Web Console 中查看系统完整性监控报告

  1. 在 Web Console 的主窗口中，选择“**监控**” → “**报告**”。
  2. 单击“**添加**”。

     “新报告模板向导”将启动。

3. 在“**模板类型**”下，在“**其他**”部分中，选择系统完整性监控报告：

   - “**文件完整性监控/系统完整性监控规则触发最频繁的 10 台设备**”。
   - “**在设备上触发次数最频繁的 10 条文件完整性监控/系统完整性监控规则**”。

   完成新报告模板向导之后，新报告模板将出现在表格中。

4. 选择并运行报告。

   报告生成过程将开始。该报告将显示在新窗口中。

要查看应用程序生成的事件，您还可以使用 Kaspersky Security Center 控制台中的事件分类。

系统完整性状态重置

Kaspersky Security Center 控制台中的计算机具有以下状态之一：*确定*、*警告*或者*严重*。如果系统完整性监控检测到监控范围内的文件或注册表项被修改，计算机的状态将变为“*警告*”或者“*严重*”。系统完整性监控指定的状态称为*系统完整性状态*。例如，如果分析结果证明检测到的对象修改不会影响计算机的安全性，您可以重置系统完整性状态。

如何在管理控制台 (MMC) 中重置系统完整性状态

1. 在 Kaspersky Security Center 管理控制台树中，选择“**任务**”。
   任务列表打开。

2. 单击“**新任务**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 选择任务类型

选择“**Kaspersky Endpoint Security for Windows (14.1)**”→ “**系统完整性状态重置**”。

步骤 2. 选择任务将分配到的设备

选择将要执行任务的计算机。下列选项可用：

- 将任务分配给管理组。在这种情况下，任务分配给先前创建的管理组中包括的计算机。
- 选择管理服务器在网络中检测到的计算机：*未分配设备*。特定设备可包括管理组中的设备以及未分配设备。
- 手动指定设备地址或从列表中导入地址。您可以指定您要将任务分配给的设备的 NetBIOS 名称、IP 地址和 IP 子网。

步骤 3. 配置任务启动计划

配置任务计划，例如，手动。

步骤 4. 定义任务名称

输入任务名称，例如，*修改监控范围后重置状态*。

步骤 5. 完成任务创建

退出向导。如有必要，选中“**向导完成时运行任务**”复选框。您可以在任务属性中监控任务进度。

如何在 Web Console 中重置系统完整性状态

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
2. 单击“**添加**”。
   “任务向导”将启动。
3. 配置任务设置：
   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Endpoint Security for Windows 14.2.0**”。
   b. 在“**任务类型**”下拉列表中，选择“**系统完整性状态重置**”。
   c. 在“**任务名称**”字段中输入简短描述，例如，*修改监控范围后重置状态*。
   d. 在“**要对其分配任务的设备**”块，选择任务范围。
4. 按照所选任务范围选项选择设备。转到下一步。
5. 选择要运行任务的账户。默认情况下，Kaspersky Endpoint Security 将使用本地用户账户的权限启动任务。
6. 退出向导。
   在任务列表中将显示一个新任务。
7. 选中该任务旁边的复选框。
8. 单击“**开始**”。

因此，如果计算机的状态更改为“*警告*”或者“*严重*”，由于系统完整性监控事件，计算机的状态被重置为“*确定*”。如果计算机的状态也因为其他事件而改变，则计算机的状态保持不变。

云发现

云发现管理用户对云服务的访问。云服务包括，例如，Microsoft Teams、Salesforce 和 Microsoft Office 365。云服务按类别分组，例如，*文件共享*、*消息软件*、*电子邮件*。卡巴斯基专家定期更新云发现类别和分类的云服务。Kaspersky Endpoint Security 使用应用程序数据库更新类别和云服务集。这意味着云发现不使用卡巴斯基安全网络对云服务进行分类。

云发现提供了以下功能：

- 监控云服务使用情况
- 阻止用户访问云服务

系统要求

如果满足以下条件，则云发现可用：

- 该应用程序安装在运行 Windows 工作站的计算机上。

  该组件对服务器不可用。

- Kaspersky Security Center 版本 15.1 或更高版本。

  该组件在管理控制台(MMC)中不可用。您可以在 Kaspersky Security Center Web Console 和 Kaspersky Security Center 云控制台中配置云发现。

- Kaspersky Next 授权许可。

启用 Cloud Discovery 组件所需的应用程序功能：

1. “**扫描加密连接**”。这对于 HTTPS 流量监控是必要的。您可以在“**网络设置**”部分管理此功能。
2. “**注入脚本到 Web 流量从而与网页交互**”。该脚本确保云发现事件的注册。该脚本还提供了对云服务访问的全功能阻止。如果没有脚本，应用程序将仅阻止云服务域的访问。您可以在“**网络设置**”部分管理此功能。

您还可以启用“**记录允许页面的打开**”功能。该功能包括当用户访问属于同一域的网页时对事件进行分组。这样，当用户使用云服务时，云发现只为每个网页记录一个事件，而不是多个事件。您可以在“**Web 控制**”部分管理此功能。

监控云服务

当用户开始使用云服务时，Kaspersky Endpoint Security 会注册该事件并在报告中创建一个条目。云发现控制浏览器以及相应应用程序中的云服务使用。云发现通过 HTTP 和 HTTPS 控制云服务的使用。

如何在云控制台中启用云服务监控

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **通信和 Web 保护** → **Cloud Discovery**。
5. 开启 **Cloud Discovery 已启用**切换开关。
6. 保存更改。

因此，该应用程序将有关正在使用的云服务的信息转发给 Kaspersky Security Center。您可以在报告中查看云服务使用情况信息。如有必要，您可以阻止访问云服务。

阻止访问云服务

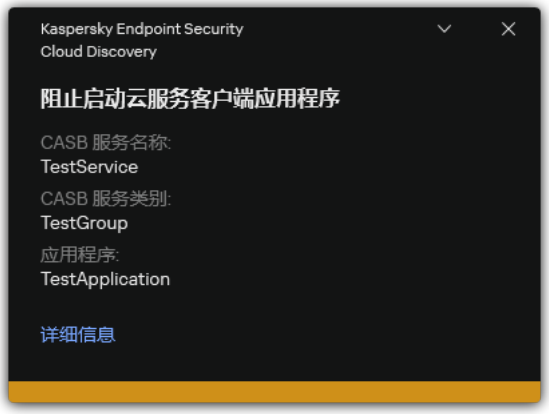
阻止访问云服务仅适用于 Kaspersky Next EDR Optimum 和 XDR Expert 授权许可。此功能不适用于 Kaspersky Next EDR Foundations 授权许可。根据“卡巴斯基新一代安全”授权许可类型比较应用程序功能，请参阅““卡巴斯基新一代安全”帮助”。

管理员可以限制用户访问云发现类别或单个云服务。通过这种方式，管理员可以只允许安全的云服务，并避免数据泄露。云发现中会显示每个云服务的*风险级别信息*。风险级别有助于检测不满足组织安全要求的服务。

风险水平只是一种估计，并不意味着对云服务或其供应商的质量有任何说明。风险等级只是卡巴斯基专家的建议。

云服务的风险级别显示在所有受控云服务列表中的策略的“**Cloud Discovery**”区域。

其他 Kaspersky Endpoint Security 组件在使用云服务时提供保护，防止受到威胁并跟踪可疑用户活动。



云发现通知

云发现不会阻止在 Kaspersky Endpoint Security 之前启动的云应用程序。

如何在云控制台中阻止对云服务的访问

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **通信和 Web 保护** → **Cloud Discovery**。
5. 开启 **Cloud Discovery 已启用**切换开关。
   将显示所有云服务的列表。云服务按类别分组，例如：*文件共享*、*即时通讯软件*、*电子邮件*。卡巴斯基专家定期更新云发现类别和分类的云服务。Kaspersky Endpoint Security 使用应用程序数据库更新类别和云服务集。
6. 使用“**访问**”列中的切换开关来配置对云服务的访问。
7. 保存更改。

因此，应用程序控制浏览器中以及相应应用程序中的云服务使用。

信任区域

受*信任区域*是由系统管理员配置的、Kaspersky Endpoint Security 在活动期间不予监控的对象和应用程序的列表。

考虑到所处理对象的特点和安装在计算机上的应用程序，管理员可以自主创建受信任区域。当 Kaspersky Endpoint Security 阻止访问特定对象或应用程序时，如果您确定此对象或应用程序是无害的，则有必要将其包含在受信任区域中。管理员也可以允许用户为特定计算机创建他们自己的本地受信任域。这样，除了策略中的常规受信任域，用户可以创建他们自己的本地排除项和受信任应用程序列表。

从 Kaspersky Endpoint Security 12.5 for Windows 开始，您可以将 EDR 遥测添加到受信任区域。这允许优化应用程序发送到 Kaspersky Anti Targeted Attack Platform (EDR) 解决方案的遥测采集服务器的数据。

从 Kaspersky Endpoint Security 12.6 for Windows 开始，扫描排除项和受信任的应用程序被添加到信任区域。预定义的扫描排除项和受信任的应用程序有助于在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上快速配置 Kaspersky Endpoint Security。这意味着您不需要在服务器上为应用程序手动设置信任区域。

从 Kaspersky Endpoint Security 12.8 for Windows 开始，您可以在 Light Agent 模式下安装该应用程序来保护虚拟环境。预定义的扫描排除项和受信任的应用程序可以帮助您在 Citrix 和 VMware 虚拟环境中快速配置 Kaspersky Endpoint Security。

创建扫描排除项

"*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。有关可被入侵者用来破坏计算机或个人数据的合法软件的详细信息，请访问 Kaspersky IT 百科全书网站。

这类应用程序可以被 Kaspersky Endpoint Security 阻止。若要防止它们被阻止，您可以为正在使用的应用程序排除扫描排除项。为此，请将 Kaspersky IT 百科全书中列出的名称或名称掩码添加到受信任区域。例如，您经常使用 Radmin 应用程序来远程管理计算机。Kaspersky Endpoint Security 会将这些活动看做可疑活动并进行阻止。若要防止应用程序被阻止，请使用 Kaspersky IT 百科全书中列出的名称或名称掩码创建扫描排除项。

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 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 从扫描中排除该应用程序。

扫描排除项可用于下列特定应用程序组件和系统管理员配置的任务：

- 行为检测
- 漏洞利用防御
- 主机入侵防御
- 文件威胁防护
- Web 威胁防护

- 邮件威胁防护
- "*恶意软件扫描*"任务

如果包含某个对象的驱动器或文件夹在扫描任务启动时包括在扫描范围中，则 Kaspersky Endpoint Security 不会扫描该对象。但是，当启动了针对该特殊对象的自定义扫描任务时，扫描排除项将不应用。

更改扫描排除项列表可能会受到父策略属性的阻止。要更改列表，您需要允许更改以下设置：Web Console 中的受信任区域（"挂锁"必须处于解锁状态）。

管理控制台(MMC) 和 Web Console 中受信任区域的分组方式不同。同样，防止受信任区域参数更改的方式也不同（"挂锁"不同）。我们建议仅使用 Web Console 来管理应用程序。如果在不同的控制台中配置受信任区域，管理插件可能会将"挂锁"重置为其默认状态。

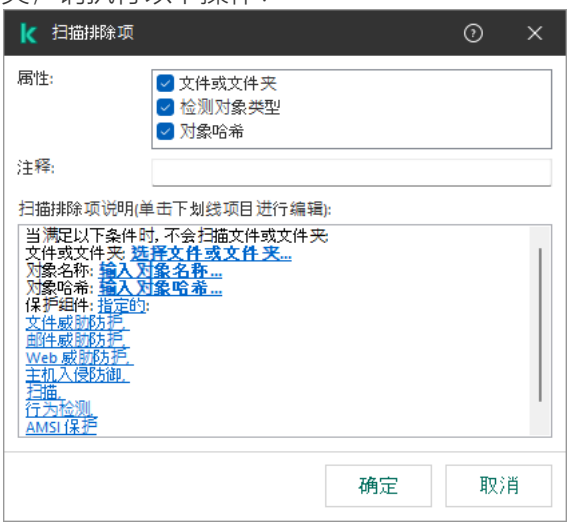
如何在管理控制台 (MMC) 中创建扫描排除项

1. 在 Kaspersky Security Center 管理控制台树中，选择"**策略**"。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **排除项和对象类型**。
4. 在"**扫描排除项和受信任应用程序** → **扫描排除项**"块中单击"**设置**"按钮。

   这将打开包含排除项列表的窗口。
5. 如果要为公司内的所有计算机创建排除项的综合列表，请选中"**继承时合并值**"复选框。将合并父策略和子策略中的排除项列表。如果启用继承时合并值，则将合并列表。父策略中的排除项以只读视图的形式显示在子策略中。无法更改或删除父策略的排除项。
6. 如果您要让用户创建排除项本地列表，选择"**允许使用本地排除项**"复选框。这样，除了策略中生成的排除项常规列表，用户可以创建他们自己的排除项本地列表。管理员可以使用 Kaspersky Security Center 在计算机属性中查看、添加、编辑或删除列表项目。

   如果复选框被清空，用户仅可以访问策略中生成的排除项常规列表。此外，如果清除此复选框，Kaspersky Endpoint Security 会在应用程序的用户界面中隐藏扫描排除项的综合列表。
7. 点击"**添加**"并选择一个操作：
   - "**类别**"。您可以将扫描排除项分组到不同的类别中。要创建新类别，请输入类别名称并向该类别添加至少一个扫描排除项。
   - "**新建排除项**"。Kaspersky Endpoint Security 会将新的扫描排除项添加到列表的根目录中。
   - "**从列表选择排除项**"。为了在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上快速配置 Kaspersky Endpoint Security，应用程序包括*预定义的扫描排除项*。还添加了预定义的扫描排除项，以支持 Citrix 和 VMware 虚拟环境中的应用程序设置。您必须根据受保护服务器的用途选择预定义的扫描排除项。
   - "**将新排除项添加到所选类别**"。要将新的扫描排除项添加到特定类别，请选择一个类别。

8. 要从扫描中排除某个文件或文件夹，请执行以下操作：



排除项设置

a. 在“**属性**”块中，选中“**文件或文件夹**”复选框。

b. 单击以下块中的链接，打开“**文件或文件夹名称**”窗口。

选择文件或文件夹

a. 输入文件或文件夹名称，或者文件或文件夹名称掩码，或者单击“**浏览**”选择文件夹树中的文件或文件夹。

使用掩码：

- `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\*\*.txt` 将包括位于 C: 驱动器的文件夹（但不包括子文件夹）中所有具有 TXT 扩展名的文件的路径。

- 两个连续 `*` 字符在文件或文件夹名称中代表任意一组字符（包括空集），包括 `\` 和 `/` 字符（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\**\*.txt` 将包括位于 `Folder` 嵌套子文件夹（除了 `Folder` 本身）中所有带 TXT 扩展名的文件的路径。掩码必须包含至少一个嵌套级别。掩码 `C:\**\*.txt` 不是有效掩码。

- `?`（问号）字符代表任意单个字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\???.txt` 将包括位于 `Folder` 文件夹中所有带 TXT 扩展名且名称由三个字符构成的文件的路径。

您可以在文件路径的开头、中间或末尾使用掩码。例如，您如果要将所有用户的文件夹添加到排除项，请输入 `?:\Users\*\Folder\` 掩码。

Kaspersky Endpoint Security 支持环境变量

您可以排除网络文件夹。为此，请手动输入网络文件夹的路径（例如，`\\Network Share\*`）。

> 使用 Kaspersky Security Center 控制台生成排除项列表时，Kaspersky Endpoint Security 不支持 `%userprofile%` 环境变量。要应用条目到所有用户账户，您可以使用 `*` 字符（例如，`C:\Users\*\Documents\File.exe`）。无论何时添加新的环境变量，都需要重新启动应用程序。

b. 保存更改。

9. 要从扫描中排除带有特定名称的对象，请执行以下操作：

a. 在“**属性**”块中，选中“**检测对象类型**”复选框。

b. 单击以下块中的链接，打开“**检测对象类型**”窗口。

选择对象

a. 根据 Kaspersky 百科全书 输入对象类型名称（例如，`Email-Worm`、`Rootkit` 或 `RemoteAdmin`）。

您可以使用带有 `?` 字符（取代单个字符）和 `*` 字符（取代任意数量字符）的掩码。例如，如果 `Client*` 掩码被指定，Kaspersky Endpoint Security 从扫描中排除 `Client-IRC`、`Client-P2P` 和 `Client-SMTP` 对象。

b. 保存更改。

10. 如果您要从扫描排除单个文件：

a. 在“**属性**”块中，选中“**对象哈希**”复选框。

b. 单击以下块中的链接，打开“**对象哈希**”窗口。

选择文件

a. 输入文件哈希或通过单击“**浏览**”按钮选择文件。

如果文件被修改，文件哈希也将被修改。如果发生此事，修改的文件将不被添加到排除项。

b. 保存更改。

11. 如有必要，在“**注释**”字段，输入您创建的扫描排除项的简短描述。

12. 指定应该使用扫描排除项的 Kaspersky Endpoint Security 组件：

    a. 单击以下块中的链接，打开“**保护组件**”窗口。

选择保护组件

    a. 选择必须应用扫描排除项的组件旁的复选框。

    如果在扫描排除项设置中指定了组件，则只有在 Kaspersky Endpoint Security 的这些组件扫描期间才会应用该排除项。

    如果在扫描排除项的设置中没有指定组件，则在 Kaspersky Endpoint Security 的所有组件扫描期间都会应用该排除规则。

13. 单击“**确定**”。

    新的排除项将被添加到列表。您可以随时使用对象旁边的复选框禁用排除项。

14. 保存更改。

如何在 Web Console 和云控制台中创建扫描排除项

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 转到**受信任区域**区域。

5. 在打开的窗口中，单击“**恶意软件扫描排除项**”链接。

6. 如果要为公司内的所有计算机创建排除项的综合列表，请选中“**继承时合并值**”复选框。将合并父策略和子策略中的排除项列表。如果启用继承时合并值，则将合并列表。父策略中的排除项以只读视图的形式显示在子策略中。无法更改或删除父策略的排除项。

7. 如果您要让用户创建排除项本地列表，选择“**允许使用本地排除项**”复选框。这样，除了策略中生成的排除项常规列表，用户可以创建他们自己的排除项本地列表。管理员可以使用 Kaspersky Security Center 在计算机属性中查看、添加、编辑或删除列表项目。

   如果复选框被清空，用户仅可以访问策略中生成的排除项常规列表。此外，如果清除此复选框，Kaspersky Endpoint Security 会在应用程序的用户界面中隐藏扫描排除项的综合列表。

8. 点击“**添加**”并选择一个操作：

   - “**类别**”。您可以将扫描排除项分组到不同的类别中。要创建新类别，请输入类别名称并向该类别添加至少一个扫描排除项。

   - “**新建排除项**”。Kaspersky Endpoint Security 会将新的扫描排除项添加到列表的根目录中。

   - “**从列表选择排除项**”。为了在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上快速配置 Kaspersky Endpoint Security，应用程序包括*预定义的扫描排除项*。还添加了预定义的扫描排除项，以支持 Citrix 和 VMware 虚拟环境中的应用程序设置。您必须根据受保护服务器的用途选择预定义的扫描排除项。

   要将新的扫描排除项添加到特定类别中，请选中该类别旁边的复选框，并选择“**新建排除项**”选项。

9. 选择您要添加排除项的方式：**文件或文件夹路径**、**对象类型**或**对象哈希**。

10. 要从扫描中排除某个文件或文件夹，请手动输入路径。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符：

    - `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\*\*.txt` 将包括位于 C: 驱动器的文件夹（但不包括子文件夹）中所有具有 TXT 扩展名的文件的路径。

    - 两个连续 `*` 字符在文件或文件夹名称中代表任意一组字符（包括空集），包括 `\` 和 `/` 字符（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\**\*.txt` 将包括位于 `Folder` 嵌套子文件夹（除了 `Folder` 本身）中所有带 TXT 扩展名的文件的路径。掩码必须包含至少一个嵌套级别。掩码 `C:\**\*.txt` 不是有效掩码。

    - `?`（问号）字符代表任意单个字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\???.txt` 将包括位于 `Folder` 文件夹中所有带 TXT 扩展名且名称由三个字符构成的文件的路径。

      您可以在文件路径的开头、中间或末尾使用掩码。例如，您如果要将所有用户的文件夹添加到排除项，请输入 `?:\Users\*\Folder\` 掩码。

      您可以排除网络文件夹。为此，请手动输入网络文件夹的路径（例如，`\\Network Share\*`）。

11. 如果您要从扫描排除特定类型的对象，在“**对象类型**”字段输入对象类型的名称，根据卡巴斯基百科全书的分类（例如 `Email-Worm`、`Rootkit`或`RemoteAdmin`）。

    您可以使用带有 `?` 字符（取代单个字符）和 `*` 字符（取代任意数量字符）的掩码。例如，如果 `Client*` 掩码被指定，Kaspersky Endpoint Security 从扫描中排除 `Client-IRC`、`Client-P2P` 和 `Client-SMTP` 对象。

12. 如果您要从扫描排除单个文件，在**对象哈希**字段输入文件哈希。

    如果文件被修改，文件哈希也将被修改。如果发生此事，修改的文件将不被添加到排除项。

13. 在**将排除项应用于**块，选择您要应用扫描排除项的组件。

14. 如有必要，在“**注释**”字段，输入您创建的扫描排除项的简短描述。

15. 单击“**确定**”。

    新的排除项将被添加到列表。您可以随时使用开关停止排除项。

16. 保存更改。

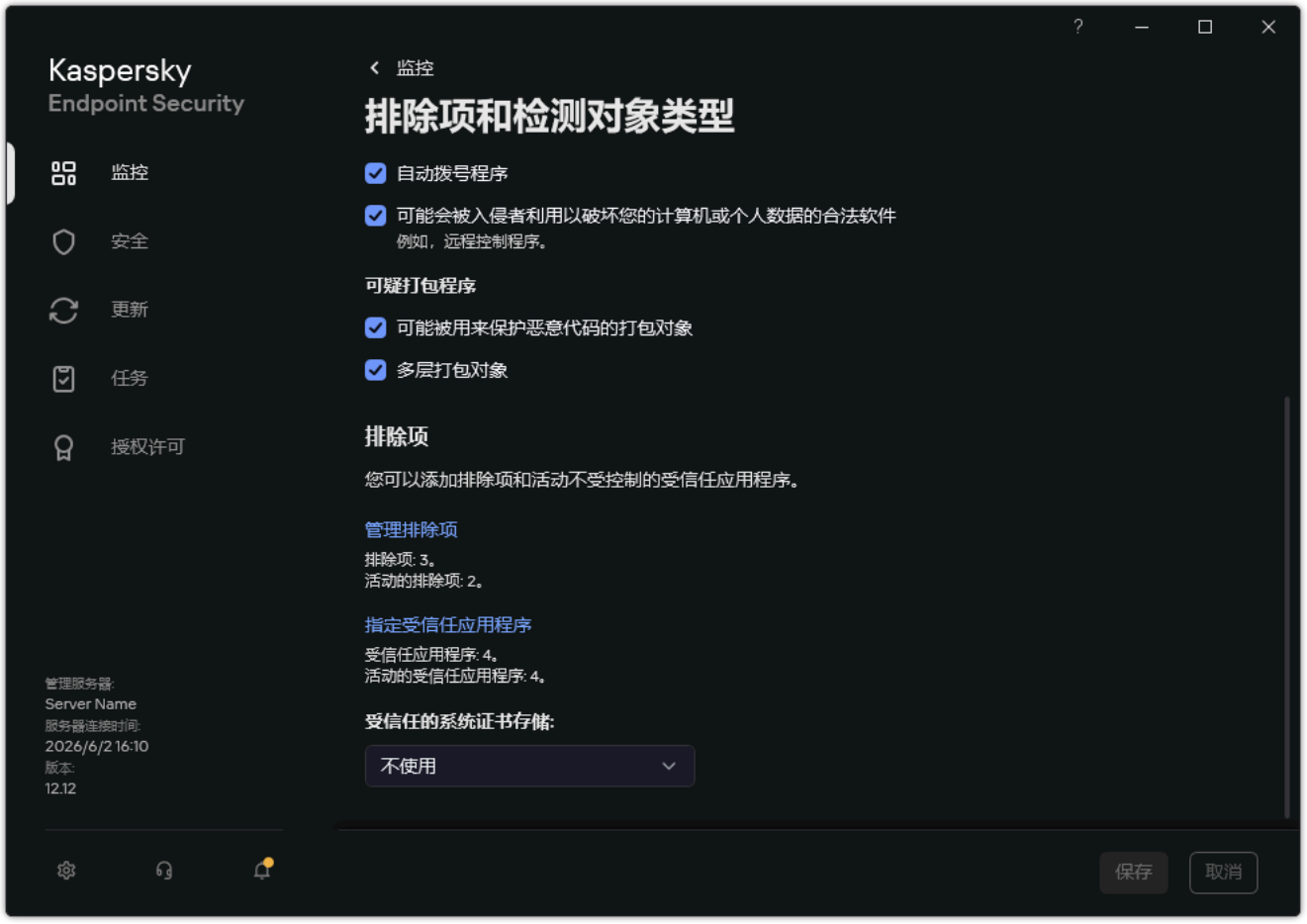
如何在应用程序界面中创建扫描排除项

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**常规设置**” → “**排除项和检测对象类型**”。

3. 在“**排除项**”区域，单击“**管理排除项**”链接。

> 如果管理员在控制台中阻止扫描排除项的配置（“关闭锁”符号）并且本地扫描排除项被禁止（**允许使用本地排除项** 复选框被清除），则 Kaspersky Endpoint Security 会在应用程序的用户界面中隐藏扫描排除项的综合列表。



排除项设置

4. 点击“**添加**”并选择一个操作：

   - “**类别**”。您可以将扫描排除项分组到不同的类别中。要创建新类别，请输入类别名称并向该类别添加至少一个扫描排除项。

   - “**新建排除项**”。Kaspersky Endpoint Security 会将新的扫描排除项添加到列表的根目录中。

   - “**从列表选择排除项**”。为了在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上快速配置 Kaspersky Endpoint Security，应用程序包括*预定义的扫描排除项*。还添加了预定义的扫描排除项，以支持 Citrix 和 VMware 虚拟环境中的应用程序设置。您必须根据受保护服务器的用途选择预定义的扫描排除项。

   要将新的扫描排除项添加到特定类别中，请选中该类别旁边的复选框，并选择“**新建排除项**”选项。

5. 如果您要从扫描排除文件或文件夹，通过单击**浏览**按钮选择文件或文件夹。

您也可以手动输入路径。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符：

- `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\*\*.txt` 将包括位于 C: 驱动器的文件夹（但不包括子文件夹）中所有具有 TXT 扩展名的文件的路径。

- 两个连续 `*` 字符在文件或文件夹名称中代表任意一组字符（包括空集），包括 `\` 和 `/` 字符（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\**\*.txt` 将包括位于 `Folder` 嵌套子文件夹（除了 `Folder` 本身）中所有带 TXT 扩展名的文件的路径。掩码必须包含至少一个嵌套级别。掩码 `C:\**\*.txt` 不是有效掩码。

- `?`（问号）字符代表任意单个字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\???.txt` 将包括位于 `Folder` 文件夹中所有带 TXT 扩展名且名称由三个字符构成的文件的路径。

  您可以在文件路径的开头、中间或末尾使用掩码。例如，您如果要将所有用户的文件夹添加到排除项，请输入 `?:\Users\*\Folder\` 掩码。

  您可以排除网络文件夹。为此，请手动输入网络文件夹的路径（例如，`\\Network Share\*`）。

6. 如果您要从扫描排除特定类型的对象，在“**检测对象类型**”字段输入对象类型的名称，根据卡巴斯基百科全书的分类（例如 `Email-Worm`、`Rootkit`或`RemoteAdmin`）。

   您可以使用带有 `?` 字符（取代单个字符）和 `*` 字符（取代任意数量字符）的掩码。例如，如果 `Client*` 掩码被指定，Kaspersky Endpoint Security 从扫描中排除 `Client-IRC`、`Client-P2P` 和 `Client-SMTP` 对象。

7. 如果您要从扫描排除单个文件，在**对象哈希**字段输入文件哈希。

   如果文件被修改，文件哈希也将被修改。如果发生此事，修改的文件将不被添加到排除项。

8. 在**保护组件**块，选择您要应用扫描排除项的组件。

9. 如有必要，在“**注释**”字段，输入您创建的扫描排除项的简短描述。

10. 为排除项选择**活动**状态。

11. 单击“**添加**”。

    新的排除项将被添加到列表。您可以随时使用“**状态**”列中的复选框禁用排除项。

12. 保存更改。

排除项列表

路径掩码例子：

我们建议指定相对路径而不是绝对路径。这不仅允许排除文件系统对象，还允许排除无文件对象。例如，`*\Program Files (x86)\Folder\Subfolder`。

位于任意文件夹的文件的路径：

- 掩码 `*.exe` 将包括具有 exe 扩展名的文件的所有路径。
- 掩码 `example*` 将包括名为 EXAMPLE 的文件的所有路径。

位于指定文件夹的文件的路径：

- 掩码 `C:\dir\*.*` 将包括位于 `C:\dir\` 的所有文件的路径，但不包括 `C:\dir\` 的子文件夹中的路径。
- 掩码 `C:\dir\*` 将包括位于 `C:\dir\` 文件夹中的所有文件的路径，包括子文件夹。
- 掩码 `C:\dir\` 将包括位于 `C:\dir\` 文件夹中的所有文件的路径，包括子文件夹。
- 掩码 `C:\dir\*.exe` 将包括位于 `C:\dir\` 文件夹中具有 EXE 扩展名的所有文件的路径，但不包括 `C:\dir\` 的子文件夹中的此类文件的路径。
- 掩码 `C:\dir\test` 将包括位于 `C:\dir\` 文件夹中名为“test”的所有文件的路径，但不包括 `C:\dir\` 的子文件夹中的此类文件的路径。
- 掩码 `C:\dir\*\test` 将包括位于 `C:\dir\` 文件夹及 `C:\dir\` 的子文件夹中名为“test”的所有文件的路径。
- 掩码 `C:\dir1\*\dir3\` 将包含指向 `C:\dir1\` 文件夹中一级 dir3 子文件夹中文件的所有路径。
- 掩码 `C:\dir1\**\dirN\` 将包括 `C:\dir1\` 文件夹中 dirN 子文件夹中任何级别的所有文件路径。

位于所有文件夹中具有指定名称的文件的路径：

- 掩码 `dir\*.*` 将包括名为“dir”的文件夹中的所有文件的路径，但不包括这些文件夹的子文件夹中的文件的路径。
- 掩码 `dir\*` 将包括名为“dir”的文件夹中的所有文件的路径，但不包括这些文件夹的子文件夹中的文件的路径。
- 掩码 `dir\` 将包括名为“dir”的文件夹中的所有文件的路径，但不包括这些文件夹的子文件夹中的文件的路径。
- 掩码 `dir\*.exe` 将包括名为“dir”的文件夹中具有 EXE 扩展名的所有文件的路径，但不包括这些文件夹的子文件夹中的此类文件的路径。
- 掩码 `dir\test` 将包括名为“dir”的文件夹中名为“test”的所有文件的路径，但不包括这些文件夹的子文件夹中的此类文件的路径。

按检测到的对象类型创建排除项

Kaspersky Endpoint Security 将检测到的对象按以下方式分类：

- **病毒和蠕虫**

  子类别：病毒和蠕虫 (Viruses_and_Worms)

  危险级别：高

  典型的病毒和蠕虫会执行未经用户授权的操作。它们会创建可自我复制的副本。

  典型病毒

  典型病毒侵入计算机后，会感染文件，激活并执行恶意操作，以及将自身的副本添加到其他文件中。

典型病毒仅在计算机本地资源上复制副本，不会自行侵入其他计算机。仅当该病毒将其副本添加至存储在共享文件夹或放入计算机中的 CD 中的文件时，或者在用户发送附有受感染文件的电子邮件消息时，该病毒才会传染给其他计算机。

典型病毒代码可以入侵计算机、操作系统和应用程序的各种区域。根据具体的环境，病毒可分为*文件病毒*、*引导区病毒*、*脚本病毒*和*宏病毒*。

病毒可以使用多种不同的技术来感染文件。*Overwriting*病毒会使用其代码覆盖受感染文件的代码，从而抹除文件的内容。感染的文件会停止发挥作用，且无法恢复。*Parasitic*病毒会修改文件，从而使之发挥全部或部分功能。*Companion*不会修改文件，而是创建副本。当您打开受感染的文件时会启动该文件的副本（实际上是病毒）。您也会遇到以下类型的病毒：*Link viruses*、*OBJ 病毒*、*LIB 病毒*、*源代码病毒*和许多其他病毒。

蠕虫

与典型病毒一样，蠕虫在侵入计算机后，其代码将激活并执行恶意操作。之所以称为蠕虫，是因为它们能够从一台计算机“爬”到另一台计算机，并不需用户权限即可通过许多数据通道来传播副本。

可用于区分各种类型蠕虫的主要特征是蠕虫的传播方式。下表提供了各种类型蠕虫的概览，这些蠕虫按其传播方式进行了分类。

蠕虫传播方式

类型	名称	描述
电子邮件蠕虫	电子邮件蠕虫	这些蠕虫通过电子邮件传播。 受感染的电子邮件消息包含带有蠕虫副本的附件，或指向上传到可能已被攻击或者专门创建用于传播蠕虫的网站上某文件的链接。打开该附件时，蠕虫将被激活。在您单击该链接，进行下载，然后打开文件时，蠕虫还会开始执行其恶意操作。之后，蠕虫会继续传播其副本，搜索其他电子邮件地址，并向它们发送受感染的邮件。
IM 蠕虫	IM 客户端蠕虫	它们通过 IM 传播。 通常，此类蠕虫会利用用户的联系人列表发送消息，其中包含指向某网站上带有蠕虫副本的文件的链接。用户下载并打开文件时，蠕虫将被激活。
IRC 蠕虫	互联网聊天蠕虫	它们会通过Internet Relay Chats（允许通过互联网与其他人实时通信的服务系统）传播。 这些蠕虫会在互联网聊天中年发布包含自身副本的文件或指向该文件的链接。用户下载并打开文件时，蠕虫将被激活。
网络蠕虫	网络蠕虫	这些蠕虫通过计算机网络传播。 与其他类型的蠕虫不同，典型的网络蠕虫不需用户参与即可传播。它会扫描本地网来寻找安装了有漏洞的程序的计算机。为此，它会发送特殊格式的网络数据包（漏洞），其中包含蠕虫代码或部分蠕虫代码。如果网络上存在“有漏洞”的计算机，该计算机会接收到此种网络数据包。蠕虫完全入侵计算机后，将被激活。
P2P 蠕虫	文件共享网络蠕虫	它们通过点对点文件共享网络传播。 为了渗透到 P2P 网络，蠕虫会将自身复制到通常位于用户计算机上的文件共享文件夹中。P2P 网络会显示有关该文件的信息，以便用户可以在网络中像任何其他文件一样“找到”受感染的文件，然后下载并打开该文件。 更加狡猾的蠕虫会模仿特定 P2P 网络的网络协议：它们会返回对搜索程序的积极响应，并提供自身的副本供下载。
蠕虫	其他类型的蠕虫	其他类型的蠕虫包括： • 通过网络资源传播自身副本的蠕虫。通过使用操作系统的功能，它们扫描可用的网络文件夹，连接到互联网上的计算机，并尝试获取对磁盘驱动器的完全访问。与之前描述的蠕虫类型不同，其他类型的蠕虫不会自行激活，而是在用户打开包含蠕虫副本的文件时激活。 • 不使用上表中所述的任何方法进行传播的蠕虫（例如，通过手机传播的蠕虫）。

- **木马(包含勒索软件)**

子类别：木马

危险级别：高

与蠕虫和病毒不同，木马不能进行自我复制。例如，用户访问受感染的网页时，它们会通过电子邮件或浏览器侵入计算机。木马通过用户参与而启动。木马启动后即会开始执行恶意操作。

在受感染的计算机上，不同的木马会表现出不同的行为。木马的主要功能包括阻止、修改或破坏信息，以及禁用计算机或网络。木马还可以接收或发送文件，在屏幕上显示消息，请求网页，下载和安装程序，以及重启计算机。

黑客通常使用各种不同木马的“集合”。

下表中介绍了木马行为的类型。

受感染计算机上木马行为的类型

类型	名称	描述
木马炸弹	木马 –“压缩文件炸弹”	解压缩时，这些压缩文件的大小会急剧增加，从而影响计算机的操作。 用户尝试解压缩这种压缩文件时，计算机可能会运行缓慢或停止运行；硬盘可能会充满“空白”数据。“压缩文件炸弹”对于文件和邮件服务器尤为危险。如果服务器使用自动系统处理接收信息，则“压缩文件炸弹”可能会中断服务器运行。
后门	用于远程管理的木马	此种木马被视为最危险的木马类型。在功能方面，这些木马与安装在计算机上的远程管理应用程序相似。 这些程序会在不被用户发觉的情况下将自身安装到计算机上，以便入侵者远程管理计算机。
木马	木马	木马包括以下恶意应用程序： • **典型木马**。这些程序仅执行木马的主要功能：阻止、修改或破坏信息，以及禁用计算机或网络。它们没有任何高级功能，与表中描述的其他类型的木马不同。 • **万能木马**。这些程序具有多种典型木马类型的高级功能。
勒索木马	勒索木马	这些木马将用户信息作为“人质”，修改或阻止信息，或者影响计算机的操作，以使用户无法使用信息。入侵者向用户进行勒索，许诺发送应用程序来恢复计算机的性能以及计算机上存储的数据。
木马点击器	木马点击器	这些木马通过自行向浏览器发送命令或更改在操作系统文件中指定的网址的方式，从用户的计算机访问网页。 通过使用这些程序，入侵者进行网络攻击并提高网站访问量，从而增加条幅广告的显示次数。
木马下载器	木马下载器	这些木马会访问入侵者的网页，从中下载其他恶意应用程序，并将它们安装到用户的计算机。这些木马包含要下载的恶意应用程序的文件名，或从访问的网页中接收该文件名。
木马释放器	木马释放器	这些木马包含安装在硬盘驱动器上并随后进行安装的其他木马。 入侵者可能会使用木马释放器类型的程序来达到以下目的： • 未通知用户就安装恶意应用程序：木马释放器类型的程序不会显示消息，或者会显示虚假消息，例如通知压缩文件中存在错误或操作系统的版本不兼容。 • 保护另一个已知恶意应用程序不被检测：并非所有反病毒软件都可检测到木马释放器类型应用程序中的恶意应用程序。
通知型木马	通知型木马	这些木马会通知入侵者受感染的计算机可供访问，并向入侵者发送有关计算机的信息：IP 地址、已开放端口号或电子邮件地址。它们通过电子邮件、FTP、访问入侵者的网页或以其他方式与入侵者联系。 通知型木马类型的程序通常用于包含多种木马的集合中。这些木马会通知入侵者其他木马已成功安装到用户的计算机。
代理型木马	代理型木马	这些木马允许入侵者使用用户的计算机匿名访问网页，它们通常用于发送垃圾邮件。
PSW 木马	密码盗窃软件	密码盗劫软件是盗窃用户账户（如软件注册数据）的一种木马。这些木马会查找系统文件和注册表中的机密数据，并通过电子邮件、FTP、访问入侵者的网页或以其他方式将其发送给“攻击者”。 部分这些木马分类为此表中描述的单独类型。这些木马会盗窃银行账户（网银窃贼木马），窃取 IM 客户端用户的数据（IM 木马），以及盗窃在线游戏用户的信息（游戏窃贼木马）。
间谍木马	间谍木马	这些木马暗中监视用户，收集有关用户使用计算机时所做的操作的信息。它们可能会拦截用户通过键盘输入的数据，截取屏幕，或收集活动应用程序的列表。收到信息后，这些木马会通过电子邮件、FTP、访问入侵者的网页或以其他方式将信息传输给入侵者。
分布式拒绝服务攻击木马	木马网络攻击者	这些木马会从用户计算机将大量请求发送至远程服务器。服务器缺少资源来处理所有请求，因此会停止运行（拒绝服务，或简称为 DoS）。黑客通常会使用这些程序感染许多计算机，以使用这些计算机来同时攻击一个服务器。 DoS 程序在用户知悉的情况下从一台计算机发起攻击。DDoS（分布式 DoS）程序在不被受感染计算机用户发觉的情况下从多台计算机发起分布式攻击。
IM 木马	从 IM 客户端用户那里窃取信息的木马	它们会窃取 IM 客户端用户的帐号和密码。这些木马会通过电子邮件、FTP、访问入侵者的网页或以其他方式将数据传输给入侵者。
Rootkit	Rootkit	这些木马会掩盖其他恶意应用程序及其活动，从而延长这些应用程序在操作系统中持续存在的时间。它们还会隐藏文件、受感染计算机内存中的进程或运行恶意应用程序的注册表键。Rootkit 会掩盖用户计算机上的应用程序与网络上其他计算机之间进行的数据交换。

类型	名称	描述
SMS 木马	SMS格式的木马	这些木马会感染手机，向额外收费的手机号码发送 SMS。
游戏窃贼木马	从在线游戏用户那里窃取信息的木马	这些木马会窃取在线游戏用户的账户凭据，然后将这些凭据通过电子邮件、FTP、访问黑客的网页或以其他方式发送给黑客。
网银窃贼木马	窃取银行账户的木马	这些木马会窃取银行账户数据或电子货币系统数据；将这些数据通过电子邮件、FTP、访问黑客的网页或以其他方式发送给黑客。
邮件侦测木马	收集电子邮件地址的木马	这些木马会收集存储在计算机上的电子邮件地址，然后通过电子邮件、FTP、访问入侵者的网页或以其他方式将它们发送给入侵者。入侵者可能会向收集到的地址发送垃圾邮件。

- **恶意工具**

子类别：恶意工具

危险级别：中

与其他类型的恶意软件不同，恶意工具在启动过后不会执行其操作。恶意工具可以在用户的计算机上安全地存储和启动。入侵者通常使用这些程序的功能来创建病毒、蠕虫和木马，对远程服务器进行网络入侵，攻击计算机或执行其他恶意操作。

恶意工具的各种功能按下表中所述的类型进行分组。

恶意工具的功能

类型	名称	描述
构建器	构建器	通过它们可以创建新的病毒、蠕虫和木马。一些构建器扬言构建了基于窗口的标准界面，用户可在该界面中选择要创建的恶意应用程序的类型，对付调试程序的方式，以及其他功能。
拒绝服务攻击	网络攻击	这些木马会从用户计算机将大量请求发送至远程服务器。服务器缺少资源来处理所有请求，因此会停止运行（拒绝服务，或简称为 DoS）。
漏洞	漏洞	“*漏洞*”是一组数据或程序代码，利用处理它们的应用程序的缺陷对计算机执行恶意操作。例如，漏洞可以写入或读取文件，或请求“受感染”的网页。 不同的漏洞会利用不同应用程序或网络服务的缺陷。漏洞会伪装成网络数据包通过网络传输到许多计算机，然后搜索网络服务存在缺陷的计算机。DOC 文件中的漏洞会利用文本编辑器的缺陷。在用户打开受感染的文件时，它可能会开始执行黑客编程的操作。嵌入在电子邮件消息中的漏洞会搜索电子邮件客户端的缺陷。用户在电子邮件客户端中打开受感染的邮件时，漏洞会立即开始执行恶意操作。 网络蠕虫会使用漏洞通过网络进行传播。Nuker 漏洞是可禁用计算机的网络数据包。
文件加密器	加密器	加密器会加密其他恶意应用程序，以隐藏它们不被反病毒应用程序发现。
洪水攻击器	用于“污染”网络的程序	这些程序会通过网络通道发送大量邮件。例如，该类型的工具包括污染互联网中继聊天的程序。 洪水攻击器工具不包括“污染”电子邮件、IM 客户端以及移动通信系统所使用通道的程序。这些程序可分为表中介绍的各种类型（电子邮件洪水攻击器、IM 洪水攻击器和 SMS 洪水攻击器）。
黑客工具	黑客工具	这些工具可以破坏其所在的计算机，或攻击其他计算机（例如，未经用户许可添加新系统账户，或清除系统日志以隐藏在操作系统中的存在路径）。这种类型的工具包括一些具有恶意功能的嗅探器，例如密码截取。嗅探器是允许查看网络流量的程序。
恶作剧程序	恶作剧程序	这些程序会警告用户类似病毒的消息：它们可能会在未受感染的文件中“检测到病毒”，或通知用户磁盘已被格式化，尽管这些情况实际并未发生。
地址欺骗程序	地址欺骗工具	这些工具使用伪造的发件人地址发送邮件和网络请求。例如，入侵者会使用地址欺骗程序类型的工具来掩盖他们作为邮件实际发件人的事实。
病毒修改工具	修改恶意应用程序的工具	通过这些工具可以修改其他恶意软件，隐藏它们不被反病毒程序发现。
电子邮件洪水攻击器	“污染”电子邮件地址的程序	这些程序会向各种电子邮件地址发送大量邮件，从而“污染”这些地址。大量的接收邮件会妨碍用户查看收件箱中的有用邮件。

类型	名称	描述
IM 洪水攻击器	“污染”IM 流量的程序	它们向 IM 的用户发送大量消息。大量的信息会妨碍用户查看有用的接收信息。
SMS 洪水攻击器	使用 SMS“污染”流量的程序	这些程序向手机发送大量 SMS。

- **广告软件**

  子类别：广告软件；

  危险级别：中

  广告软件向用户显示广告信息。广告软件程序会在其他程序的界面中显示条幅广告，并将搜索查询重定向至广告网页。某些广告软件程序会收集有关用户的营销信息，并将其发送给开发者：该信息可能包括用户访问的网站的名称，或用户搜索查询的内容。与间谍木马类型的程序不同，广告软件程序会在用户许可的情况下将该信息发送给开发者。

- **自动拨号程序**

  子类别：自动拨号器（拨号器）。

  危险级别：中

  自动拨号器可以使用调制解调器秘密建立电话连接。

- **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**

  子类别：可能会被入侵者用来破坏计算机或个人数据的合法软件。

  危险级别：中

  大多数这些应用程序都很有用，因此有许多用户使用它们。这些应用程序包括 IRC 客户端、自动拨号程序、文件下载程序、计算机系统活动监控器、密码实用程序以及用于 FTP、HTTP 和 Telnet 的互联网服务器。

  但是，如果入侵者获得了这些程序的访问权限，或如果他们在用户的计算机上安置这些程序，应用程序的某些功能可能会被用来危害安全。

  这些应用程序具有不同的功能，下表介绍了它们的类型。

类型	名称	描述
客户端 IRC	互联网聊天客户端	用户安装这些程序与他人进行互联网中继聊天。入侵者使用这些程序来传播恶意软件。
下载器	用于下载的程序	这些程序可以在隐藏模式下从网页下载文件。
监控器	用于监控的程序	这些程序可监控其安装到的计算机上的活动（查看哪些应用程序正在活动，以及它们如何与安装在其他计算机上的应用程序交换数据）。
密码工具	密码恢复器	通过它们可以查看和恢复已忘记的密码。入侵者出于相同的目的，秘密地将它们安置在用户的计算机上。
远程管理程序	远程管理程序	系统管理员广泛使用的一些程序。通过这些程序可以获取对远程计算机界面的访问权限，以监控和管理该计算机。入侵者出于同样的目的，秘密地将它们安置在用户的计算机上：用于监控和管理远程计算机。 合法的远程管理程序与实现远程管理的后门类型的木马不同。木马能够独自入侵操作系统并自行安装；合法的程序则无法做到这些。
FTP 服务程序	FTP 服务器	这些程序可起到 FTP 服务器的作用。入侵者将它们安置在用户计算机上，以打开通过 FTP 对该计算机的远程访问。
代理服务程序	代理服务器	这些程序可起到代理服务器的作用。入侵者将它们安置在用户计算机上，以用户名义发送垃圾邮件。

类型	名称	描述
Telnet 服务程序	Telnet 服务器	这些程序可起到 Telnet 服务器的作用。入侵者将它们安置在用户计算机上，以打开通过 Telnet 对该计算机的远程访问。
Web 服务程序	Web 服务器	这些程序可起到 Web 服务器的作用。入侵者将它们安置在用户计算机上，以打开通过 HTTP 对该计算机的远程访问。
风险工具	在本地计算机上工作的工具	在用户自己的计算机上工作时，这些工具会为用户提供其他选项。通过这些工具，用户可以隐藏文件或活动应用程序的窗口，并终止活动的进程。
网络工具	网络工具	与网络上的其他计算机配合工作时，这些工具会为用户提供其他选项。通过这些工具可以进行重启，检测开放的端口，以及启动安装在计算机上的应用程序。
P2P 客户端	P2P 网络客户端	通过它们可以在对等网络中工作。入侵者可能会利用它们传播恶意软件。
客户端 SMTP	SMTP 客户端	它们未经用户的同意便发送电子邮件。入侵者将它们安置在用户计算机上，以用户名义发送垃圾邮件。
Web 工具栏	Web 工具栏	它们会向其他应用程序的界面中添加工具栏，以使用搜索引擎。
欺骗工具	欺骗程序	这些程序将自己伪装为其他程序。例如，一些欺骗反病毒程序会显示有关恶意软件检测的信息。但实际上，它们并未找到任何内容或进行清除。

- **可能被用来保护恶意代码的打包对象**

  子类别：可能造成危害的打包文件。

  危险级别：中。

  该文件使用专门用于打包恶意软件（病毒、蠕虫、特洛伊木马）的特殊打包程序进行打包。Kaspersky Endpoint Security 会扫描 SFX（自解压）存档中的解包工具模块。

  为了隐藏恶意软件以避免被反病毒软件检测到，黑客使用特殊的打包程序对其进行打包。卡巴斯基专家已识别出黑客最常使用的解包工具。

- **多层打包对象**

  子类别：多重打包文件。

  危险级别：中。

  该文件被一个或多个打包程序打包三次或三次以上。

  为了隐藏恶意软件以避免被反病毒软件检测到，黑客可能会多次打包文件。Kaspersky Endpoint Security 将扫描打包文件。

默认情况下，Kaspersky Endpoint Security 检测所有对象类型。为了提高计算机的安全性，我们建议启用所有类型对象的检测功能。如果您使用的内部实用程序被应用程序检测为恶意的，将这些实用程序添加到排除项列表中，但不要禁用对所有类型对象的检测。

如何在管理控制台 (MMC) 中选择可检测对象的类型

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**策略**”。
3. 选择必要的策略并双击以打开策略属性。
4. 在策略窗口中，选择 **常规设置** → **排除项和对象类型**。

5. 在“**检测对象类型**”块中单击“**设置**”按钮。

6. 在打开的窗口中，请选择您想要 Kaspersky Endpoint Security 检测的对象类型旁边的复选框。

7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 和云控制台中选择可检测对象的类型

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **常规设置** → **检测设置**。

5. 在“**检测其他类型的对象**”块，请选择您想要 Kaspersky Endpoint Security 检测的对象类型旁边的复选框。

6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

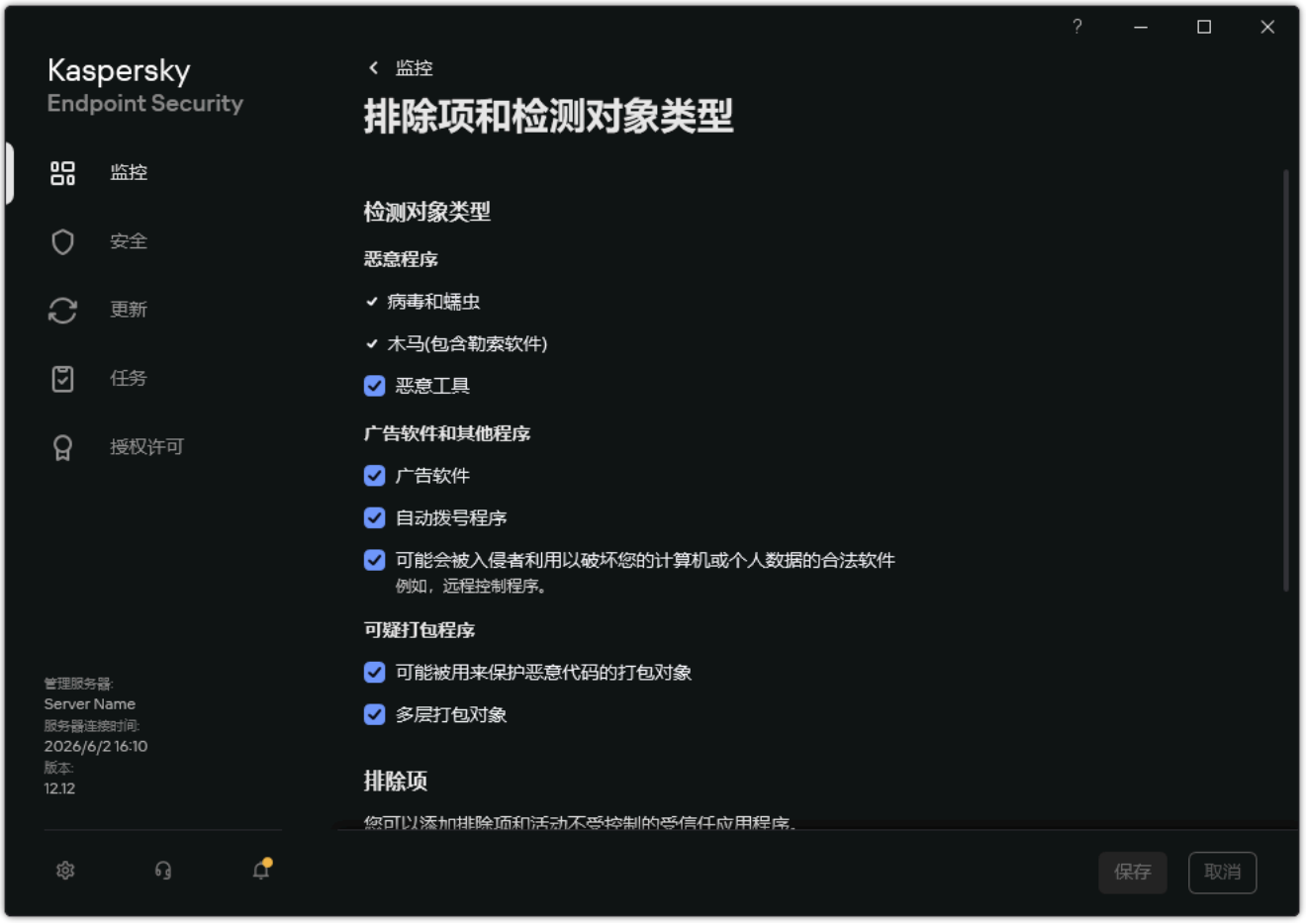
如何在应用程序界面中选择可检测对象的类型

1. 打开主应用程序窗口并单击 按钮。

2. 在应用程序设置窗口中，选择“**常规设置**” → “**排除项和检测对象类型**”。

3. 在“**检测对象类型**”块，请选择您想要 Kaspersky Endpoint Security 检测的对象类型旁边的复选框。

4. 保存更改。



可检测对象的类型

编辑受信任应用程序列表

*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。

扫描排除项和受信任的应用程序之间的区别在于，对于排除项，Kaspersky Endpoint Security 不扫描文件，而对于受信任的应用程序，它不控制启动的进程。如果受信任的应用程序在未包含在扫描排除项中的文件夹中创建恶意文件，Kaspersky Endpoint Security 将检测该文件并消除威胁。如果该文件夹被添加到排除项，Kaspersky Endpoint Security 将跳过该文件。

例如，如果您认为被标准 Microsoft Windows 记事本使用的对象是安全的，也即您信任此应用程序，则可将 Microsoft Windows 记事本添加到受信任的应用程序列表中，从而不监控该应用程序所使用的对象。这将提高计算机性能，这在使用服务器应用程序时尤为重要。

此外，被 Kaspersky Endpoint Security 分类为可疑操作的某些操作，在很多应用程序的功能环境中可能是安全的。例如，拦截键盘键入的文本，是自动键盘布局切换器中的一种例行程序（例如 Punto Switcher）。考虑到此类程序的特点并将其行为从监控中排除，我们建议您可将此类程序添加到受信任应用程序列表中。

受信任的应用程序有助于避免 Kaspersky Endpoint Security 与其他应用程序之间的兼容性问题（例如，Kaspersky Endpoint Security 和另一个反病毒应用程序对第三方计算机的网络流量进行双重扫描的问题）。

同时，受信任应用程序的可执行文件和进程仍然会扫描病毒和其他恶意软件。您可以通过扫描排除项将应用程序从 Kaspersky Endpoint Security 扫描中完全排除。

更改受信任应用程序列表可能会受到父策略属性的阻止。要更改列表，您需要允许更改以下设置：Web Console 中的受信任区域（“挂锁”必须处于解锁状态）。

管理控制台(MMC) 和 Web Console 中受信任区域的分组方式不同。同样，防止受信任区域参数更改的方式也不同（“挂锁”不同）。我们建议仅使用 Web Console 来管理应用程序。如果在不同的控制台中配置受信任区域，管理插件可能会将“挂锁”重置为其默认状态。

如何添加应用程序到管理控制台(MMC)中的受信任列表

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **排除项和对象类型**。
4. 在“**扫描排除项和受信任应用程序** → **受信任应用程序**”块中单击“**设置**”按钮。

   这将打开包含受信任应用程序列表的窗口。
5. 如果要为公司内的所有计算机创建受信任应用程序的综合列表，请选中“**继承时合并值**”复选框。将合并父策略和子策略中的受信任应用程序列表。如果启用继承时合并值，则将合并列表。父策略中的受信任应用程序以只读视图的形式显示在子策略中。无法更改或删除父策略的受信任应用程序。
6. 如果您要让用户创建受信任应用程序本地列表，选择**允许使用本地受信任应用程序**复选框。这样，除了策略中生成的受信任应用程序常规列表，用户可以创建他们自己的受信任应用程序本地列表。管理员可以使用 Kaspersky Security Center 在计算机属性中查看、添加、编辑或删除列表项目。

   如果复选框被清空，用户仅可以访问策略中生成的受信任应用程序常规列表。此外，如果清除此复选框，Kaspersky Endpoint Security 会在应用程序的用户界面中隐藏受信任应用程序的综合列表。
7. 点击“**添加**”并选择一个操作：
   - “**类别**”。您可以将受信任的应用程序分组到不同的类别中。要创建新类别，请输入类别的名称并向该类别添加至少一个受信任的应用程序。
   - “**新建排除项**”。Kaspersky Endpoint Security 会将新的受信任应用程序添加到列表的根目录中。
   - “**从列表选择排除项**”。为了在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上快速配置 Kaspersky Endpoint Security，该应用程序包括*预定义的受信任应用程序*。还添加了预定义的受信任应用程序，以支持 Citrix 和 VMware 虚拟环境中的应用程序设置。您必须根据受保护服务器的用途选择预定义的受信任的应用程序。
   - “**将新排除项添加到所选类别**”。要将新的受信任的应用程序添加到特定类别，请选择一个类别。
8. 选择信任标准：
   - “**使用磁盘上的完整进程路径将其视为受信任**”。输入受信任应用程序的可执行文件的路径。

     当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。

Kaspersky Endpoint Security 将对受信任应用程序的文件名区分大小写。如果您输入的文件名有大小写错误，Kaspersky Endpoint Security 将无法识别受信任应用程序。

- "**使用进程文件哈希将其视为受信任**"。

在 Kaspersky Security Center 控制台上生成受信任应用程序列表时，Kaspersky Endpoint Security 不支持 `%userprofile%` 环境变量。要应用条目到所有用户账户，您可以使用 * 字符（例如，`C:\Users\*\Documents\File.exe`）。无论何时添加新的环境变量，都需要重新启动应用程序。

受信任应用程序设置

9. 为受信任应用程序（参加下表）配置高级设置。

10. 单击"**确定**"。

新的受信任的应用程序将被添加到列表。您可以随时使用对象旁边的复选框将应用程序从信任区域中排除。

11. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

受信任应用程序列表

如何添加应用程序到 Web 控制和云控制台中的受信任列表

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 转到**受信任区域**区域。

5. 在打开的窗口中，单击“**应用程序**”链接。

   这将打开包含受信任应用程序列表的窗口。

6. 如果要为公司内的所有计算机创建受信任应用程序的综合列表，请选中“**继承时合并值**”复选框。将合并父策略和子策略中的受信任应用程序列表。如果启用继承时合并值，则将合并列表。父策略中的受信任应用程序以只读视图的形式显示在子策略中。无法更改或删除父策略的受信任应用程序。

7. 如果您要让用户创建受信任应用程序本地列表，选择**允许使用本地排除项**复选框。这样，除了策略中生成的受信任应用程序常规列表，用户可以创建他们自己的受信任应用程序本地列表。管理员可以使用 Kaspersky Security Center 在计算机属性中查看、添加、编辑或删除列表项目。

   如果复选框被清空，用户仅可以访问策略中生成的受信任应用程序常规列表。此外，如果清除此复选框，Kaspersky Endpoint Security 会在应用程序的用户界面中隐藏受信任应用程序的综合列表。

8. 点击“**添加**”并选择一个操作：

- “**类别**”。您可以将受信任的应用程序分组到不同的类别中。要创建新类别，请输入类别的名称并向该类别添加至少一个受信任的应用程序。
- “**新建排除项**”。Kaspersky Endpoint Security 会将新的受信任应用程序添加到列表的根目录中。
- “**从列表选择排除项**”。为了在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上快速配置 Kaspersky Endpoint Security，该应用程序包括*预定义的受信任应用程序*。还添加了预定义的受信任应用程序，以支持 Citrix 和 VMware 虚拟环境中的应用程序设置。您必须根据受保护服务器的用途选择预定义的受信任的应用程序。

要将新的受信任应用程序添加到特定类别中，请选中该类别旁边的复选框，并选择“**新建排除项**”选项。

9. 选择信任标准：

- “**文件或文件夹路径**”。输入受信任应用程序的可执行文件的路径。

  当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。

  Kaspersky Endpoint Security 将对受信任应用程序的文件名区分大小写。如果您输入的文件名有大小写错误，Kaspersky Endpoint Security 将无法识别受信任应用程序。

- “**应用程序哈希**”。

> 在 Kaspersky Security Center 控制台上生成受信任应用程序列表时，Kaspersky Endpoint Security 不支持 %userprofile% 环境变量。要应用条目到所有用户账户，您可以使用 `*` 字符（例如，`C:\Users\*\Documents\File.exe`）。无论何时添加新的环境变量，都需要重新启动应用程序。

10. 为受信任应用程序（参加下表）配置高级设置。

11. 单击“**确定**”。

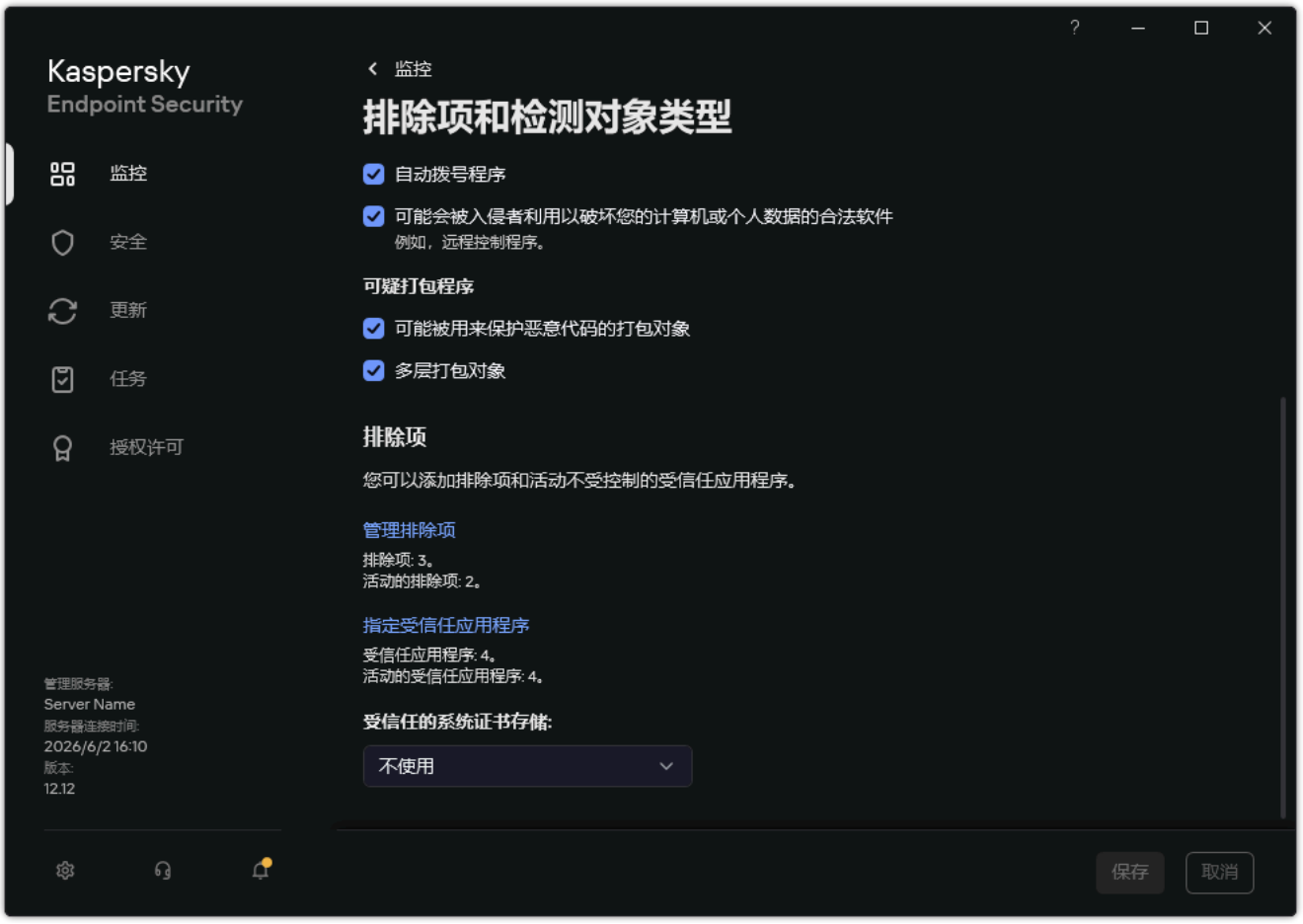
    新的受信任的应用程序将被添加到列表。您可以随时使用“**状态**”列中的复选框将应用程序从信任区域中排除。

12. 保存更改。

如何添加应用程序到应用程序界面中的受信任列表

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**排除项和检测对象类型**”。
3. 在“**排除项**”区域，单击“**指定受信任应用程序**”链接。

如果管理员在控制台中阻止受信任应用程序的配置（“关闭锁”符号）并且本地受信任应用程序被禁止（**允许使用本地受信任应用程序** 复选框被清除），则 Kaspersky Endpoint Security 会在应用程序的用户界面中隐藏受信任应用程序的综合列表。



排除项设置

4. 点击“**添加**”并选择一个操作：

- “**类别**”。您可以将受信任的应用程序分组到不同的类别中。要创建新类别，请输入类别的名称并向该类别添加至少一个受信任的应用程序。
- “**新建排除项**”。Kaspersky Endpoint Security 会将新的受信任应用程序添加到列表的根目录中。
- “**从列表选择排除项**”。为了在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上快速配置 Kaspersky Endpoint Security，该应用程序包括*预定义的受信任应用程序*。还添加了预定义的受信任应用程序，以支持 Citrix 和 VMware 虚拟环境中的应用程序设置。您必须根据受保护服务器的用途选择预定义的受信任的应用程序。

要将新的受信任应用程序添加到特定类别中，请选中该类别旁边的复选框，并选择“**新建排除项**”选项。

5. 选择信任标准：

- “**使用磁盘上的完整进程路径将其视为受信任**”。输入受信任应用程序的可执行文件的路径。

  当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。

  Kaspersky Endpoint Security 将对受信任应用程序的文件名区分大小写。如果您输入的文件名有大小写错误，Kaspersky Endpoint Security 将无法识别受信任应用程序。

- “**使用进程文件哈希将其视为受信任**”。

Kaspersky Endpoint Security 支持环境变量，并在应用程序的本地接口中转换路径。换言之，如果您输入文件路径 `%userprofile%\Documents\File.exe`，`C:\Users\Fred123\Documents\File.exe` 记录被添加到用户 Fred123 的应用程序的本地界面中。相应地，Kaspersky Endpoint Security 对其他用户忽略 `File.exe` 受信任程序。要应用条目到所有用户账户，您可以使用 `*` 字符（例如，`C:\Users\*\Documents\File.exe`）。无论何时添加新的环境变量，都需要重新启动应用程序。

6. 在受信任应用程序属性窗口，配置高级设置。

7. 单击“**确定**”。

   新的受信任的应用程序将被添加到列表。您可以随时使用“**状态**”列中的复选框将应用程序从信任区域中排除。

8. 保存更改。

受信任应用程序列表

受信任应用程序设置

参数	描述
不扫描应用程序打开的文件	应用程序打开的所有文件被从 Kaspersky Endpoint Security 的扫描中排除。例如，如果您正使用应用程序备份文件，该功能帮助降低 Kaspersky Endpoint Security 的资源消耗。
不监控应用程序活动	Kaspersky Endpoint Security 将不监控应用程序文件和其在操作系统中的网络活动。您可以为 Kaspersky Endpoint Security 的不同组件配置应用程序活动监控： • “**不监控保护和控制组件**”。应用程序活动被以下组件监控：行为检测、漏洞利用防御、主机入侵防御、修复引擎和防火墙。 • “**不监控 Managed Detection and Response 和 Endpoint Detection and Response**”。应用程序活动由内置 MDR 代理和内置 EDR (KATA) 代理监控。 • “**不拦截 Endpoint Detection and Response 的控制台交互式输入**”。Kaspersky Endpoint Security 不会发送有关在控制台上管理应用程序的遥测数据。遥测数据由 Kaspersky Anti Targeted Attack Platform (EDR)使用。
不监控子应用程序活动	Kaspersky Endpoint Security 将不监控被该应用程序启动的应用程序的文件活动或网络活动。您可以递归地应用排除。这样应用程序就不会监控整个子应用程序链的活动。
不继承父进程(应用程序)的限制	为父进程配置的限制将不被 Kaspersky Endpoint Security 应用到子进程。父进程由配置了应用程序权限（主机入侵防御）和应用程序网络规则（防火墙）的应用程序启动。

参数	描述
不监控子应用程序活动	Kaspersky Endpoint Security 将不监控被该应用程序启动的应用程序的文件活动或网络活动。您可以递归地应用排除。这样应用程序就不会监控整个子应用程序链的活动。
允许与程序界面交互	Kaspersky Endpoint Security 自我保护阻止所有从远程计算机管理应用程序服务的尝试。如果选择该复选框，则允许远程访问应用程序通过 Kaspersky Endpoint Security 界面管理 Kaspersky Endpoint Security 设置。
不阻止与 AMSI 保护组件的交互	Kaspersky Endpoint Security 将不监控受信任应用程序让AMSI 保护组件扫描对象的请求。
不扫描网络流量	应用程序发起的网络流量将被 Kaspersky Endpoint Security 从扫描排除。您可以从扫描排除所有流量，也可以仅排除加密流量。您也可以从扫描排除单个 IP 地址和端口号。 如果为受信任应用程序指定哈希值而不是路径，则 Kaspersky Endpoint Security 14.0 或更早版本不支持排除网络流量。
不拦截文件修改 *（仅在 Kaspersky Security Center 控制台可用）*	Kaspersky Endpoint Security 不会监控来自系统完整性监控监测范围的文件更改。应用程序排除项应用于所有系统完整性监控模式：实时系统完整性监控和按需系统完整性检查。
不拦截注册表修改 *（仅在 Kaspersky Security Center 控制台可用）*	Kaspersky Endpoint Security 不监控系统完整性监控监测范围内注册表键的更改。应用程序排除项应用于所有系统完整性监控模式：实时系统完整性监控和按需系统完整性检查。
注释	如果必要，您可以提供受信任应用程序的简短注释。注释帮助对受信任应用程序进行简单搜索和排序。
状态	受信任应用程序状态： • **活动**状态表示应用程序已包括在“受信任”域。 • **非活动**状态表示应用程序已从“受信任”域排除。

创建本地受信任区域

用户现在可以为特定计算机创建自己的本地受信任区域。这样，除了策略中的常规受信任域，用户可以创建他们自己的本地排除项和受信任应用程序列表。管理员可以在策略设置中允许或阻止使用本地排除项或本地受信任应用程序。为此，请使用策略“**排除项**”区域中的“**允许使用本地排除项**”和“**允许使用本地受信任应用程序**”复选框。

如果管理员允许创建本地受信任区域，则用户可以在应用程序的用户界面中添加自己的扫描排除项和受信任应用程序。同时，用户无权修改或删除策略中配置的受信任区域中的对象。如果需要为单台计算机添加排除项，管理员还可以在 Kaspersky Security Center 控制台中查看、添加、修改或删除列表项。

如果管理员在控制台中阻止受信任域的配置（“关闭锁”符号）并且本地扫描排除项和受信任应用程序被禁止，则 Kaspersky Endpoint Security 会在应用程序的用户界面中隐藏扫描排除项和受信任应用程序的综合列表。

如何在管理控制台（MMC）中添加对象到本地受信任区域

1. 打开 Kaspersky Security Center Administration Console。
2. 在管理控制台树的“**受管理设备**”文件夹中，打开相关客户端计算机所属的管理组名称的文件夹。
3. 在工作区中选择“**设备**”选项卡。
4. 双击以打开计算机属性窗口。
5. 在计算机属性窗口中，选择“**应用程序**”区域。

6. 在计算机上安装的卡巴斯基应用程序列表中，选择 **Kaspersky Endpoint Security for Windows (14.1)** 并双击以打开应用程序属性。

7. 在应用程序设置窗口中，选择“**常规设置**” → “**排除项和对象类型**”。

8. 在“**扫描排除项和受信任应用程序** → **本地扫描排除项**”块中单击“**设置**”按钮。

   这将打开包含本地排除项列表的窗口。

受信任区域设置

9. 制作本地扫描排除项列表。

   创建本地扫描排除项的规则与常规排除项相同。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 * 以及 ? 字符。

10. 在“**扫描排除项和受信任应用程序** → **本地受信任应用程序**”块中单击“**设置**”按钮。

    这将打开包含本地受信任应用程序列表的窗口。

11. 列出本地受信任的应用程序。

    添加应用程序到本地受信任应用程序列表的规则与将它们添加到常规列表的规则相同。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 * 以及 ? 字符。

12. 保存更改。

如何在 Web Console 和云控制台中添加对象到本地受信任区域

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**资产(设备)**”。

2. 单击要允许用户执行阻止操作的计算机的名称。

3. 选择**应用程序**选项卡。

4. 单击“**Kaspersky Endpoint Security for Windows**”。

   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. 在应用程序设置窗口中，选择“**常规设置**” → “**排除项和检测对象类型**”。

7. 在“**扫描排除项和受信任应用程序**”区域，单击“**本地扫描排除项**”链接。

8. 制作本地扫描排除项列表。

   创建本地排除项的规则与创建常规排除项的规则相同。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 * 以及 ? 字符。

9. 在“**扫描排除项和受信任应用程序**”区域，单击“**本地受信任应用程序**”链接。

10. 列出本地受信任的应用程序。

    添加应用程序到本地受信任应用程序列表的规则与将它们添加到常规列表的规则相同。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 * 以及 ? 字符。

11. 保存更改。

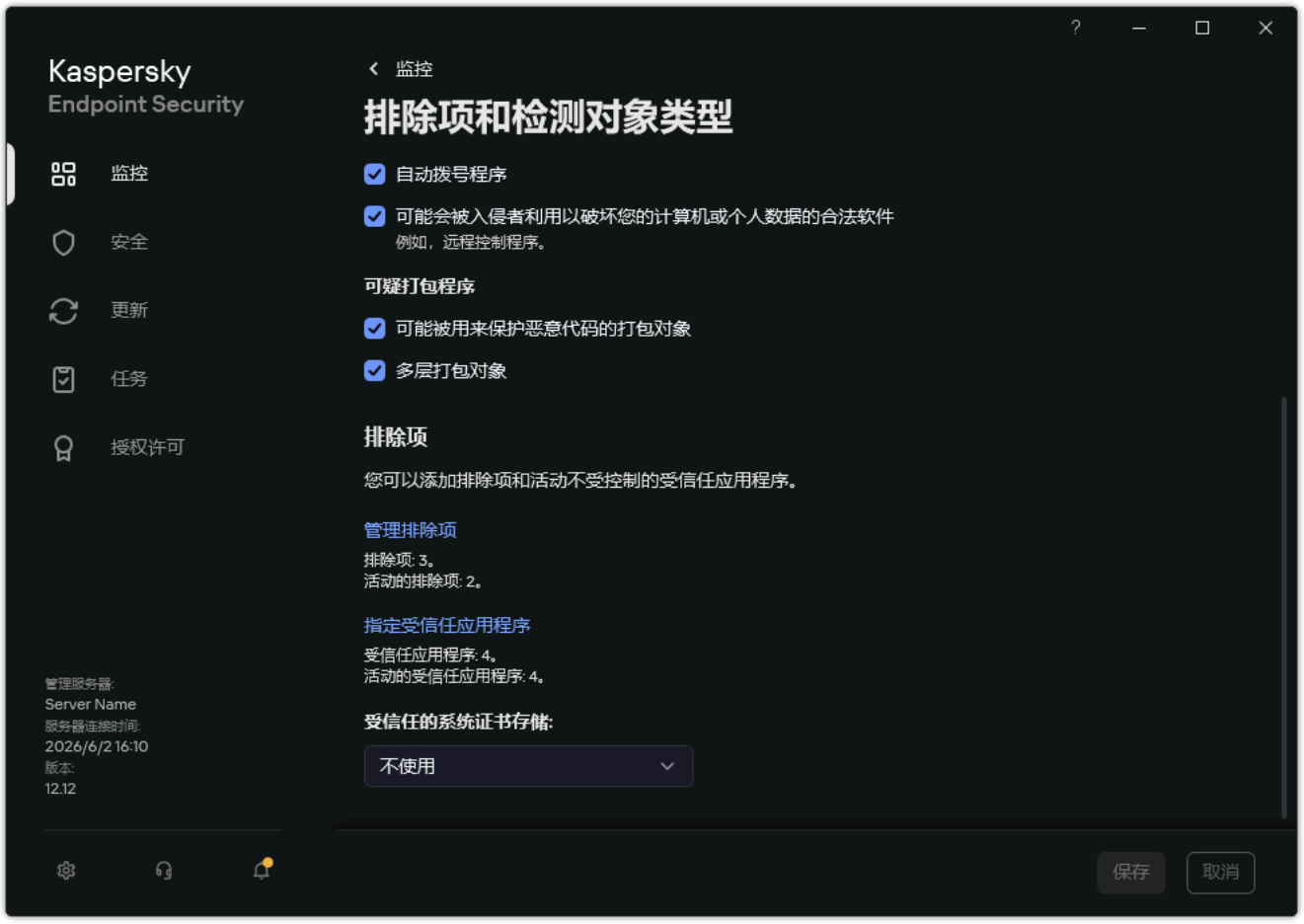
如何在应用程序界面中创建本地扫描排除项

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**常规设置**” → “**排除项和检测对象类型**”。

3. 在“**排除项**”区域，单击“**管理排除项**”链接。

如果管理员在控制台中阻止扫描排除项的配置（“关闭锁”符号）并且本地扫描排除项被禁止（**允许使用本地排除项** 复选框被清除），则 Kaspersky Endpoint Security 会在应用程序的用户界面中隐藏扫描排除项的综合列表。



排除项设置

4. 点击“**添加**”并选择一个操作：

- “**类别**”。您可以将扫描排除项分组到不同的类别中。要创建新类别，请输入类别名称并向该类别添加至少一个扫描排除项。
- “**新建排除项**”。Kaspersky Endpoint Security 会将新的扫描排除项添加到列表的根目录中。
- “**从列表选择排除项**”。为了在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上快速配置 Kaspersky Endpoint Security，应用程序包括*预定义的扫描排除项*。还添加了预定义的扫描排除项，以支持 Citrix 和 VMware 虚拟环境中的应用程序设置。您必须根据受保护服务器的用途选择预定义的扫描排除项。

要将新的扫描排除项添加到特定类别中，请选中该类别旁边的复选框，并选择“**新建排除项**”选项。

5. 如果您要从扫描排除文件或文件夹，通过单击**浏览**按钮选择文件或文件夹。

您也可以手动输入路径。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符：

- `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\*\*.txt` 将包括位于 C: 驱动器的文件夹（但不包括子文件夹）中所有具有 TXT 扩展名的文件的路径。

- 两个连续 `*` 字符在文件或文件夹名称中代表任意一组字符（包括空集），包括 `\` 和 `/` 字符（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\**\*.txt` 将包括位于 `Folder` 嵌套子文件夹（除了 `Folder` 本身）中所有带 TXT 扩展名的文件的路径。掩码必须包含至少一个嵌套级别。掩码 `C:\**\*.txt` 不是有效掩码。

- `?`（问号）字符代表任意单个字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\???.txt` 将包括位于 `Folder` 文件夹中所有带 TXT 扩展名且名称由三个字符构成的文件的路径。

  您可以在文件路径的开头、中间或末尾使用掩码。例如，您如果要将所有用户的文件夹添加到排除项，请输入 `?:\Users\*\Folder\` 掩码。

  您可以排除网络文件夹。为此，请手动输入网络文件夹的路径（例如，`\\Network Share\*`）。

6. 如果您要从扫描排除特定类型的对象，在“**检测对象类型**”字段输入对象类型的名称，根据卡巴斯基百科全书的分类（例如 `Email-Worm`、`Rootkit`或`RemoteAdmin`）。

   您可以使用带有 `?` 字符（取代单个字符）和 `*` 字符（取代任意数量字符）的掩码。例如，如果 `Client*` 掩码被指定，Kaspersky Endpoint Security 从扫描中排除 `Client-IRC`、`Client-P2P` 和 `Client-SMTP` 对象。

7. 如果您要从扫描排除单个文件，在**对象哈希**字段输入文件哈希。

   如果文件被修改，文件哈希也将被修改。如果发生此事，修改的文件将不被添加到排除项。

8. 在**保护组件**块，选择您要应用扫描排除项的组件。

9. 如有必要，在“**注释**”字段，输入您创建的扫描排除项的简短描述。

10. 为排除项选择**活动**状态。

11. 单击“**添加**”。

    新的排除项将被添加到列表。您可以随时使用“**状态**”列中的复选框禁用排除项。

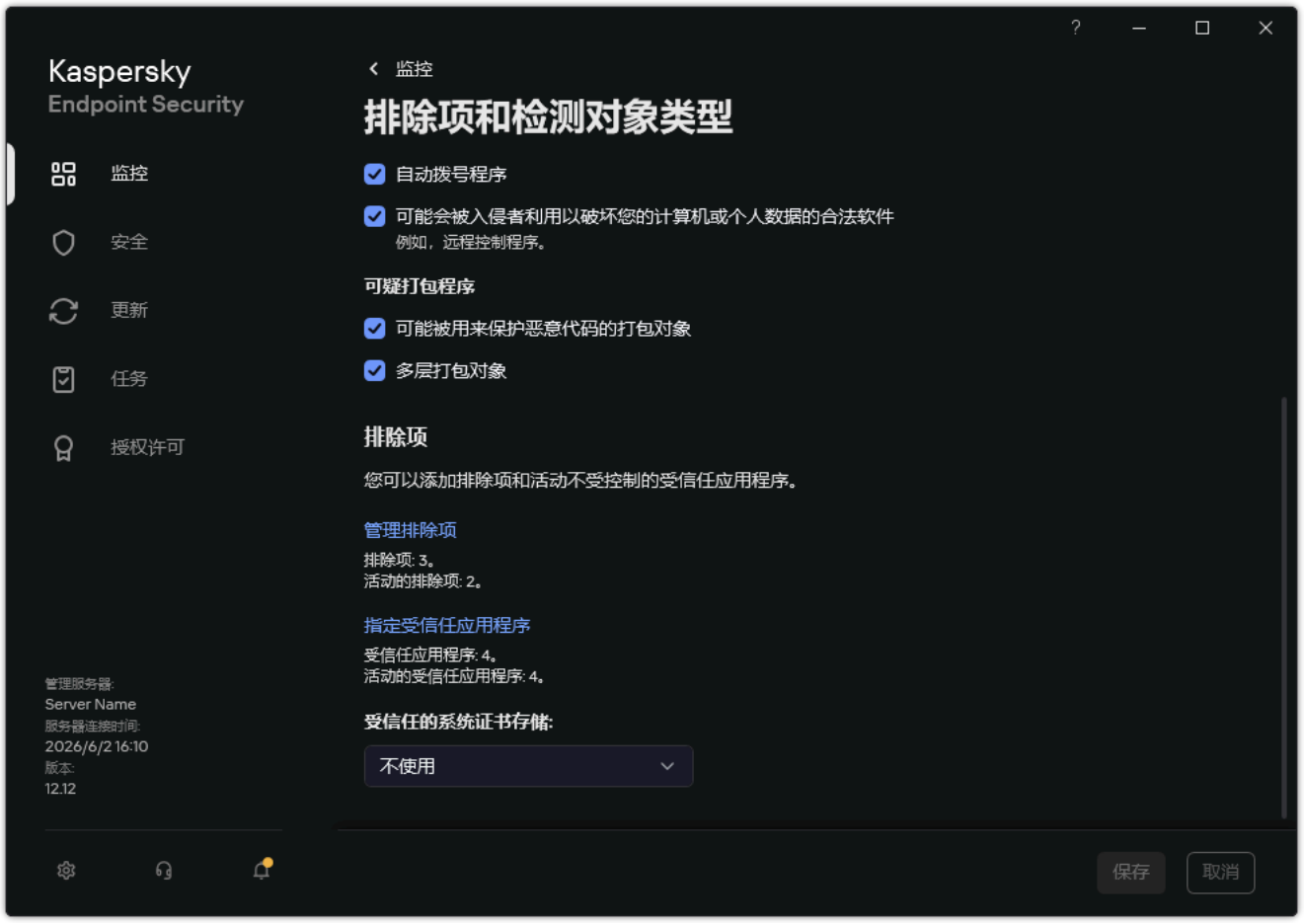
12. 保存更改。

排除项列表

如何在应用程序界面中添加应用程序到本地受信任应用程序列表

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**排除项和检测对象类型**”。
3. 在“**排除项**”区域，单击“**指定受信任应用程序**”链接。

如果管理员在控制台中阻止受信任应用程序的配置（“关闭锁”符号）并且本地受信任应用程序被禁止（**允许使用本地受信任应用程序** 复选框被清除），则 Kaspersky Endpoint Security 会在应用程序的用户界面中隐藏受信任应用程序的综合列表。



排除项设置

4. 点击“**添加**”并选择一个操作：

- “**类别**”。您可以将受信任的应用程序分组到不同的类别中。要创建新类别，请输入类别的名称并向该类别添加至少一个受信任的应用程序。
- “**新建排除项**”。Kaspersky Endpoint Security 会将新的受信任应用程序添加到列表的根目录中。
- “**从列表选择排除项**”。为了在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上快速配置 Kaspersky Endpoint Security，该应用程序包括*预定义的受信任应用程序*。还添加了预定义的受信任应用程序，以支持 Citrix 和 VMware 虚拟环境中的应用程序设置。您必须根据受保护服务器的用途选择预定义的受信任的应用程序。

要将新的受信任应用程序添加到特定类别中，请选中该类别旁边的复选框，并选择“**新建排除项**”选项。

5. 选择信任标准：

- “**使用磁盘上的完整进程路径将其视为受信任**”。输入受信任应用程序的可执行文件的路径。

  当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。

  Kaspersky Endpoint Security 将对受信任应用程序的文件名区分大小写。如果您输入的文件名有大小写错误，Kaspersky Endpoint Security 将无法识别受信任应用程序。

- “**使用进程文件哈希将其视为受信任**”。

Kaspersky Endpoint Security 支持环境变量，并在应用程序的本地接口中转换路径。换言之，如果您输入文件路径 `%userprofile%\Documents\File.exe`，`C:\Users\Fred123\Documents\File.exe` 记录被添加到用户 Fred123 的应用程序的本地界面中。相应地，Kaspersky Endpoint Security 对其他用户忽略 `File.exe` 受信任程序。要应用条目到所有用户账户，您可以使用 `*` 字符（例如，`C:\Users\*\Documents\File.exe`）。无论何时添加新的环境变量，都需要重新启动应用程序。

6. 在受信任应用程序属性窗口，配置高级设置。

7. 单击“**确定**”。

   新的受信任的应用程序将被添加到列表。您可以随时使用“**状态**”列中的复选框将应用程序从信任区域中排除。

8. 保存更改。

受信任应用程序列表

导出和导入受信任域

*受信任区域*是由系统管理员配置的、Kaspersky Endpoint Security 在活动期间不予监控的对象和应用程序的列表。受信任区域由以下列表组成：“*扫描排除项*”和“*受信任应用程序*”。您可以将这些列表导出为 XML 文件和其他格式。然后可以修改文件，例如，添加大量相同类型的排除项。还可以使用导出/导入功能备份排除列表和受信任应用程序列表或将列表迁移到其他服务器。

应用程序使用以下格式导出和导入*排除项列表*：

- XML 在管理控制台（MMC）、Web 控制台和云控制台中可用。
- DAT 仅可在管理控制台（MMC）中导入。此格式的目的是保持与应用程序旧版本的兼容性。您可以在管理控制台（MMC）中将 DAT 文件转换为 XML，以将排除项列表迁移到 Web 控制台。
- CSV 仅在应用程序的本地界面中可用。

Kaspersky Endpoint Security 使用 XML 格式导出和导入*受信任应用程序列表*。

如何在管理控制台（MMC）中导出和导入受信任区域

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **排除项和对象类型**。
4. 在“**扫描排除项和受信任应用程序**”下，选择要导出或导入的受信任区域的组件：**扫描排除项**或者**受信任应用程序**。
5. 单击“**设置**”。
6. 要导出规则列表：
   a. 选择您要导出的排除项。要选择多个端口，使用 **CTRL** 或 **SHIFT** 键。
      如果您未选择任何排除项，Kaspersky Endpoint Security 将导出所有排除项。
   b. 单击“ → **导出**”按钮。
   c. 在打开的窗口中，指定您要将排除项列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。

d. 保存文件。

Kaspersky Endpoint Security 会将整个排除项列表导出到 XML 文件。Kaspersky Endpoint Security 还支持将排除项列表导出到 DAT 文件。

受信任应用程序列表

7. 要导入排除项列表：

   a. 单击“ → **导入**”按钮。

   b. 在打开的窗口中，选择要从中导入排除项列表的 XML 文件。

   c. 打开文件。

   如果计算机已经具有排除项的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 XML 文件向其中添加新条目。Kaspersky Endpoint Security 还支持从 DAT 文件导入排除项列表。

8. 保存更改。

如何在 Web Console 和云控制台中导出和导入受信任区域

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 转到**受信任区域**区域。

5. 要导出规则列表：

   a. 单击**恶意软件扫描排除项**链接。

   b. 选择您要导出的排除项。

   c. 单击“ → **导出**”按钮。

      Kaspersky Endpoint Security 导出排除项列表到默认下载文件夹中的 JSON 文件。

6. 要导出受信任应用程序列表：

   a. 选择您要导出的受信任应用程序。

   b. 单击“ → **导出**”按钮。

      Kaspersky Endpoint Security 导出受信任应用程序列表到默认下载文件夹中的 JSON 文件。

7. 要导入排除项列表：

   a. 单击**恶意软件扫描排除项**链接。

   b. 单击“ → **导入**”按钮。

      在打开的窗口中，选择要从中导入排除项列表的 JSON 文件。

   c. 打开文件。

      如果计算机已经具有排除项的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 JSON 文件向其中添加新条目。

8. 要导入受信任应用程序列表：

   a. 单击**应用程序**链接。

   b. 单击“ → **导入**”按钮。

      在打开的窗口中，选择要从中导入受信任应用程序列表的 JSON 文件。

   c. 打开文件。

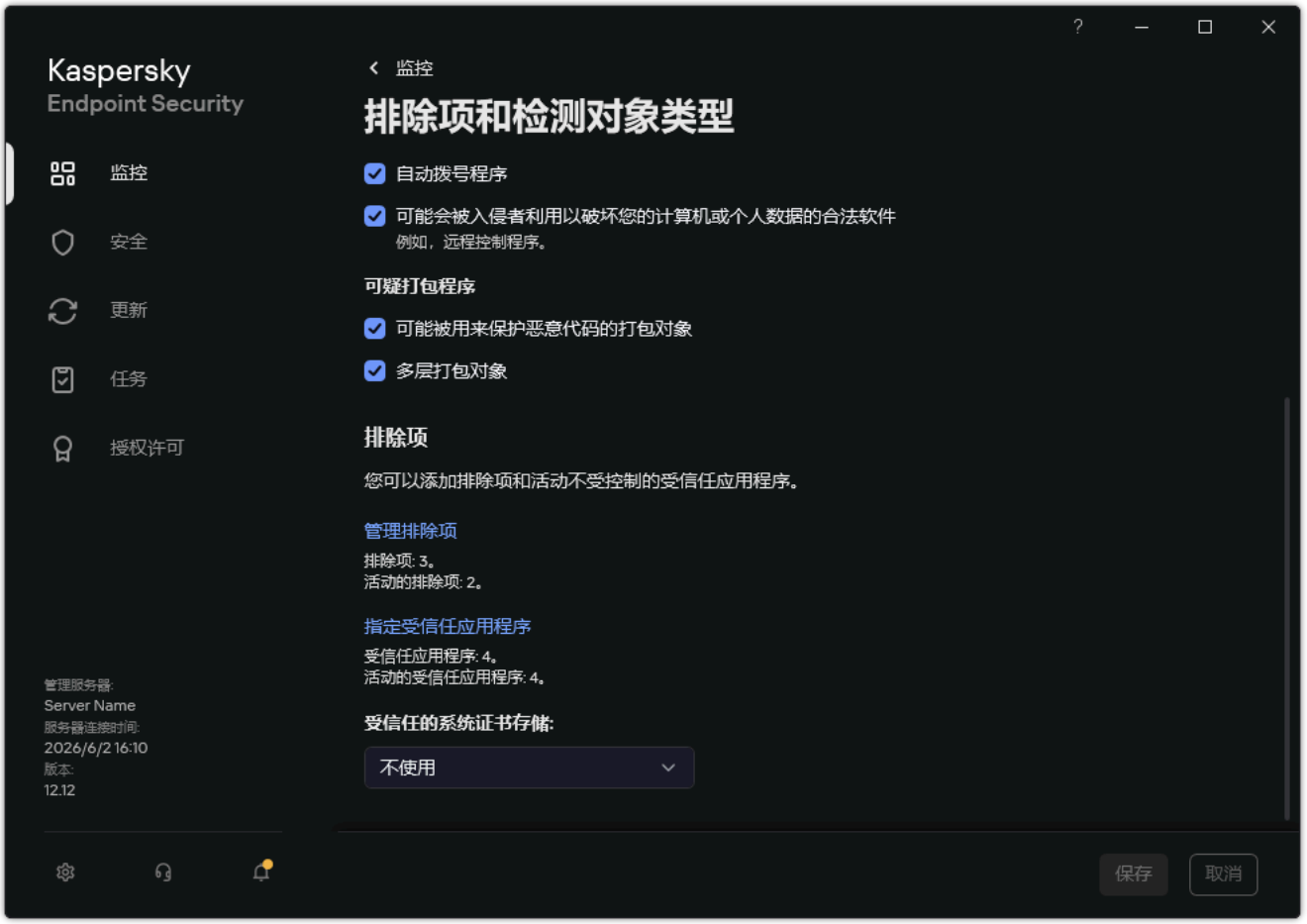
      如果计算机已经具有受信任应用程序的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 JSON 文件向其中添加新条目。

9. 保存更改。

如何在应用程序界面中导出和导入受信任区域

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**常规设置**” → “**排除项和检测对象类型**”。



排除项设置

3. 要导出规则列表：

   a. 在“**排除项**”区域，单击“**管理排除项**”链接。

   b. 选择您要导出的排除项。

   c. 单击“**导出**”。

   d. 确认您仅想导出所选排除项，或导出整个排除项列表。

   e. 在打开的窗口中，指定您要将排除项列表导出到的 CSV 文件的名称，然后选择要保存此文件的文件夹。

f. 保存文件。

Kaspersky Endpoint Security 会将整个排除项列表导出到 CSV 文件。

排除项列表

4. 要导出受信任应用程序列表：

   a. 在“**排除项**”区域，单击“**指定受信任应用程序**”链接。

   b. 选择您要导出的受信任应用程序。

   c. 单击“**导出**”。

   d. 确认您仅想导出所选受信任应用程序，或导出整个列表。

   e. 在打开的窗口中，输入您要将受信任应用程序列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。

f. 保存文件。

Kaspersky Endpoint Security 会将整个受信任应用程序列表导出到 XML 文件。

受信任应用程序列表

5. 要导入排除项列表：

   a. 在“**排除项**”区域，单击“**管理排除项**”链接。

   b. 单击“**导入**”。

   c. 在打开的窗口中，选择要从中导入排除项列表的 CSV 文件。

   d. 打开文件。

   如果计算机已经具有排除项的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 CSV 文件向其中添加新条目。

6. 要导入受信任应用程序列表：

   a. 在“**排除项**”区域，单击“**指定受信任应用程序**”链接。

   b. 单击“**导入**”。

   c. 在打开的窗口中，选择要从中导入受信任应用程序列表的 XML 文件。

d. 打开文件。

如果计算机已经具有受信任应用程序的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 XML 文件向其中添加新条目。

7. 保存更改。

使用受信任数字签名处理应用程序

使用系统证书存储允许您从病毒扫描中排除由受信任数字签名签发的应用程序。Kaspersky Endpoint Security 自动分配此类应用程序到“*受信任*”组。

如何在管理控制台(MMC)中启动受信任系统证书存储的使用

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **排除项和对象类型**。
4. 在“**受信任的系统证书存储**”块中，选中“**使用受信任的系统证书存储**”复选框。
5. 在下拉列表中，选择必须被 Kaspersky Endpoint Security 视为受信任的系统存储。
6. 保存更改。

如何在 Web Console 和云控制台中启动受信任系统证书存储的使用

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”选项卡。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到**受信任区域**区域。
5. 在打开的窗口中，单击“**受信任证书**”链接。
6. 在打开的窗口中，选中“**使用受信任的系统证书存储**”复选框。
7. 选择 Kaspersky Endpoint Security 必须信任的系统存储。
8. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在应用程序界面中启动受信任系统证书存储的使用

1. 打开主应用程序窗口并单击 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**排除项和检测对象类型**”。
3. 在“**受信任的系统证书存储**”下拉列表中，选择必须被 Kaspersky Endpoint Security 视为受信任的系统存储。
4. 保存更改。

附录。预定义的扫描排除项和受信任的应用程序

从 Kaspersky Endpoint Security 12.6 for Windows 开始，扫描排除项和受信任的应用程序被添加到信任区域。预定义的扫描排除项和受信任的应用程序有助于在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上快速配置 Kaspersky Endpoint Security。这意味着您不需要在服务器上为应用程序手动设置信任区域。从 Kaspersky Endpoint Security 12.8 for Windows 开始，您可以在 Light Agent 模式下安装该应用程序来保护虚拟环境。预定义的扫描排除项和受信任的应用程序可以帮助您在 Citrix 和 VMware 虚拟环境中快速配置 Kaspersky Endpoint Security。

您可以通过以下方式选择预定义排除项和受信任的应用程序：

- 安装应用程序。
  - 使用向导在本地安装应用程序
  - 安装包属性
- 设置策略。
  - 新策略向导
  - 策略属性：扫描排除项和受信任的应用程序

SQL 服务器

在 SQL Server 上安装 Kaspersky Endpoint Security 时，您必须从预定义的排除项和受信任的应用程序创建受信任域，以确保服务器的运行不受干扰。

预定义扫描排除项

路径	SQL 版本
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.mdf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL??. MSSQLSERVER\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022
%ProgramFiles(x86)%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012
%ProgramFiles%\Microsoft SQL Server\MSSQL.?*\Data*.ldf	2012

路径	SQL 版本
%ProgramFiles%\Microsoft SQL Server\MSSQL??.*\MSSQL\DATA*.mdf	2012 2014 2016 2017 2019 2022
%ProgramFiles%\Microsoft SQL Server\MSSQL??.**\MSSQL\DATA*.ldf	2012 2014 2016 2017 2019 2022

Microsoft Exchange 服务器

在 Microsoft Exchange 服务器上安装 Kaspersky Endpoint Security 时，您必须从预定义的排除项和受信任的应用程序创建受信任域，以确保服务器的运行不受干扰。

预定义扫描排除项

路径	Microsoft Exchange 版本
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\Mailbox*.jsl	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Chk	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Edb	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Jrs	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.log	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.Que	2013 2016 2019
C:\Program Files\Microsoft\Exchange Server\V15\TransportRoles\Data\Queue*.jsl	2013 2016 2019

预定义的受信任应用程序

路径	Microsoft Exchange 版本
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\EdgeTransport.exe	2013 2016 2019
%ProgramFiles%\Microsoft\Exchange Server\V15\Bin\MSExchangeFrontendTransport.exe	2013 2016 2019

System Center Configuration Manager

预定义扫描排除项

路径	System Center Configuration Manager 版本
%ProgramFiles%\Microsoft Configuration Manager\Inboxes	2012 2012 R2

Citrix

在 Citrix 虚拟环境中安装 Kaspersky Endpoint Security 时，您必须从预定义的排除项和受信任的应用程序创建受信任域，以确保服务器的运行不受干扰。

预定义扫描排除项

路径
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName.mdf
%SystemRoot%\ServiceProfiles\NetworkService\HaDatabaseName_log.ldf
%SystemRoot%\ServiceProfiles\NetworkService\HaImportDatabaseName_log.ldf
%ProgramData%\Citrix\Broker\Cache
%SystemRoot%\System32\drivers\CtxUvi.sys
%ProgramFiles%\Citrix\HDX\bin\CitrixLogonCsp.dll
mcsdif.vhdx
%Temp%\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%Temp%\Citrix\HDXRTConnector**.txt
%SystemDrive%\Users*\AppData\Local\Temp\Citrix\RTMediaEngineSRV\MediaEngineSRVDebugLogs**.txt
%ProgramFiles(x86)%\Citrix\ICA Client\epclient32.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epclient64.dll
%ProgramFiles(x86)%\Citrix\ICA Client\epinject.sys
%ProgramFiles(x86)%\Citrix\ICA Client\EntryProtect.dll

路径
*.vhd
*.avhd
*.vhdx
*.avhdx
*.pvp
*.lok
%SystemRoot%\System32\drivers\CVhdMp.sys (Windows Server 2012 R2)
%SystemRoot%\System32\drivers\CfsDep2.sys
%ProgramData%\Citrix\Provisioning Services\Tftpboot\ARDBP32.BIN
.vdiskcache
vdiskdif.vhdx
%SystemRoot%\ServiceProfiles\NetworkService\AppData\Roaming\Citrix\SubscriptionsStore**\PersistentDictionary.edb

预定义的受信任应用程序

路径	Citrix 解决方案
%ProgramFiles%\Citrix\Broker\Service\BrokerService.exe	虚拟应用和桌面
%ProgramFiles%\Microsoft SQL Server\150\LocalDB\Binn\sqlservr.exe	虚拟应用和桌面
%ProgramFiles%\Citrix\Broker\Service\HighAvailabilityService.exe	虚拟应用和桌面
%ProgramFiles%\Citrix\ConfigSync\ConfigSyncService.exe	虚拟应用和桌面
%ProgramFiles%\Citrix\User Profile Manager\UserProfileManager.exe	虚拟应用和桌面
%ProgramFiles%\Citrix\Virtual Desktop Agent\BrokerAgent.exe	虚拟应用和桌面
%SystemRoot%\System32\drivers\CVhdFilter.sys	虚拟应用和桌面
%ProgramFiles(x86)%\Citrix\ICAService\CtxSvcHost.exe	虚拟应用和桌面
%ProgramFiles%\Citrix\System32\ctxgfx.exe	虚拟应用和桌面
%ProgramFiles%\Citrix\ICAService\picaSvc2.exe	虚拟应用和桌面
%ProgramFiles%\Citrix\ICAService\CpSvc.exe	虚拟应用和桌面
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	虚拟应用和桌面
%ProgramFiles%\Citrix\HDX\bin\CtxSvcHost.exe	虚拟应用和桌面
%ProgramFiles%\Citrix\HDX\bin\ctxgfx.exe	虚拟应用和桌面
%ProgramFiles%\Citrix\HDX\bin\picaSvc2.exe	虚拟应用和桌面
%ProgramFiles%\Citrix\HDX\bin\CpSvc.exe	虚拟应用和桌面

路径	Citrix 解决方案
%ProgramFiles(x86)%\Citrix\System32\WebSocketService.exe	虚拟应用和桌面
%ProgramFiles%\Citrix\ICAService\WebSocketService.exe	虚拟应用和桌面
%ProgramFiles(x86)%\Citrix\HDX\bin\WebSocketService.exe	虚拟应用和桌面
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\AudioTranscoder.exe	虚拟应用和桌面
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngine.Net.Service.exe	虚拟应用和桌面
%ProgramFiles(x86)%\Citrix\HDX RealTime Connector\MediaEngineService.exe	虚拟应用和桌面
%ProgramFiles(x86)%\Citrix\ICA Client\MediaEngineService.exe	工作区应用
%ProgramFiles(x86)%\Citrix\ICA Client\CDViewer.exe	工作区应用
%ProgramFiles(x86)%\Citrix\ICA Client\concentr.exe	工作区应用
%ProgramFiles(x86)%\Citrix\ICA Client\wfica32.exe	工作区应用
%ProgramFiles(x86)%\Citrix\ICA Client\bgblursvc.exe	工作区应用
%ProgramFiles(x86)%\Citrix\ICA Client\AuthManager\AuthManSvr.exe	工作区应用
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfService.exe	工作区应用
%ProgramFiles(x86)%\Citrix\ICA Client\SelfServicePlugin\SelfServicePlugin.exe	工作区应用
%ProgramFiles(x86)%\Citrix\ICA Client\HdxRtcEngine.exe	工作区应用
%ProgramFiles(x86)%\Citrix\ICA Client\HdxTeams.exe	工作区应用
%ProgramFiles%\Citrix\Provisioning Services\BNTFTP.EXE	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\PVSTSB.EXE	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\StreamService.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\StreamProcess.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\soapserver.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\Inventory.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\Notifier.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\MgmtDaemon.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNPXE.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\CdfSvc.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNAbsService.exe	Provisioning
%SystemRoot%\System32\drivers\bnistack6.sys	Provisioning
%SystemRoot%\System32\drivers\CfsDep2.sys	Provisioning
%SystemRoot%\System32\drivers\cnicteam.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\BNDevice.exe	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\BNIstack6.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CNicTeam.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CFsDep2.sys	Provisioning
%ProgramFiles%\Citrix\Provisioning Services\drivers\CVhdMp.sys	Provisioning

路径	Citrix 解决方案
%ProgramFiles%\Citrix\Receiver StoreFront\Services\SubscriptionsStoreService\Citrix.DeliveryServices.SubscriptionsStore.ServiceHost.exe	StoreFront
%ProgramFiles%\Citrix\Receiver StoreFront\Services\CredentialWallet\Citrix.DeliveryServices.CredentialWallet.ServiceHost.exe	StoreFront

VMware

在 Vmware 虚拟环境中安装 Kaspersky Endpoint Security 时，您必须从预定义的受信任的应用程序创建受信任域，以确保服务器的运行不受干扰。

预定义的受信任应用程序

路径	VMware 解决方案
C:\Program Files\VMware\VMware View\Agent\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\wsnm_jms.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\ws_scripthost.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastS.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\VMware Blast\VMBlastW.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\SecurityGateway.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\x64\pcoip_server_win32.exe	Horizon
C:\Program Files\Common Files\VMware\Teradici PCoIP Server\pcoip_server_win32.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\Scanner.exe	Horizon
C:\Program Files\VMware\VMware View\Agent\bin\tsdrvdisvc.dll	Horizon
C:\Program Files\VMware\VMware View\Server\appblastgateway\nssm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\wsnm.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\SecurityGateway.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_TunnelService.exe	Horizon
C:\Program Files\VMware\VMware View\Server\bin\ws_SecurityServer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmUpdateLauncher.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-appstub.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-helper.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-previewer.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-print-redir-client.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-remotemks.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\vmware-view-usbloader.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\ClientService\horizon_client_service.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\DCT\ws_diag.exe	Horizon
C:\Program Files\VMware\VMware Horizon View Client\cef\HTML5VideoPlayer.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vmware-usbarbitrator64.exe	Horizon

路径	VMware 解决方案
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\vnetlib64.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib.exe	Horizon
C:\Program Files (x86)\Common Files\VMware\USB\DriverCache\vnetlib64.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlping.exe	Horizon
C:\Program Files\Common Files\VMware\DeviceRedirectionCommon\ftnlsv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\diagutil.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\ftscanmgrhv.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan.exe	Horizon
C:\Program Files\Common Files\VMware\ScannerRedirection\scan64.exe	Horizon
C:\Program Files\Common Files\VMware\SerialPortRedirection\Client\vmwsprrdpwks.exe	Horizon

管理备份

*备份*存储保存在清除过程中删除或修改的文件的副本。*备份副本*是指对文件进行病毒清除或删除前创建的文件副本。文件的备份副本以特定格式保存并且不会带来威胁。

文件的备份副本存储在 `C:\ProgramData\Kaspersky Lab\KES.14.1\QB` 文件夹中。

管理员组中的用户被授予访问该文件夹的完整权限。其账户用于安装 Kaspersky Endpoint Security 的用户被授予该文件夹的有限访问权限。

Kaspersky Endpoint Security 不提供用于配置文件备份副本的用户访问权限的功能。

有时，在清除过程中无法维护文件的完整性。如果您在杀毒后失去对受感染文件中重要信息的部分或全部访问权限，可以尝试将文件从其备份副本还原到其原文件夹中。

如果 Kaspersky Endpoint Security 在 Kaspersky Security Center 管理下运行，则文件的备份副本可能会发送至 Kaspersky Security Center 管理服务器。有关在 Kaspersky Security Center 管理文件的备份副本的更多详细信息，请参阅《Kaspersky Security Center 帮助》系统。

配置备份区中的文件的最长存储期

备份区中的文件副本的默认最长存储期是 30 天。最长存储期限到期后，Kaspersky Endpoint Security 将删除备份区中最旧的文件。

要配置备份区中的文件的最长存储期：

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口的“**常规设置**”下，点击“**报告和存储**”瓦片。

备份设置

3. 如果您要限制备份中文件副本的存储期限，在“**备份**”块选择“**存储对象时间不超过 N 天**”复选框。输入备份区中的文件副本的最长存储期。

4. 保存更改。

配置备份区的最大大小

您可以指定备份的最大大小。默认情况下，备份区大小无限制。当达到最大大小后，Kaspersky Endpoint Security 将自动删除备份区中最旧的文件。

要配置备份区的最大大小：

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口的“**常规设置**”下，点击“**报告和存储**”瓦片。

备份设置

3. 在“**备份**”块中，选择“**限制备份区大小为 N MB**”复选框。如果选中该复选框，则最大存储大小限制为定义值。默认情况下，最大大小为 1024 MB。为避免超过最大存储大小，当达到最大存储大小时，Kaspersky Endpoint Security 将自动删除存储中的最早文件。

4. 保存更改。

从备份区中还原文件

如果在文件中检测到恶意代码，Kaspersky Endpoint Security 将阻止该文件，为其指定“*未清除*”状态，并将其副本放到“备份区”中并尝试对其清除。文件杀毒成功后，该文件的备份副本的状态将变为“*已清除*”。文件在原始文件夹中将不可用。如果文件无法被杀毒，Kaspersky Endpoint Security 将把它从原始文件夹中删除。您可以将该文件从它的备份副本还原到它的原文件夹。

带有“*将在计算机重启后删除*”状态的文件无法恢复。重新启动计算机，文件状态将更改为“*已清除*”或“*已删除*”。您还可以将该文件从它的备份副本还原到它的原文件夹。

在属于 Windows Store 应用程序的文件中检测到恶意代码以后，Kaspersky Endpoint Security 将立即删除文件，而不会将其备份副本移至备份区。您可以使用操作系统的适当工具恢复 Windows Store 应用程序的完整性（有关恢复 Windows Store 应用程序的详细信息，请参阅 Microsoft Windows 帮助文件）。

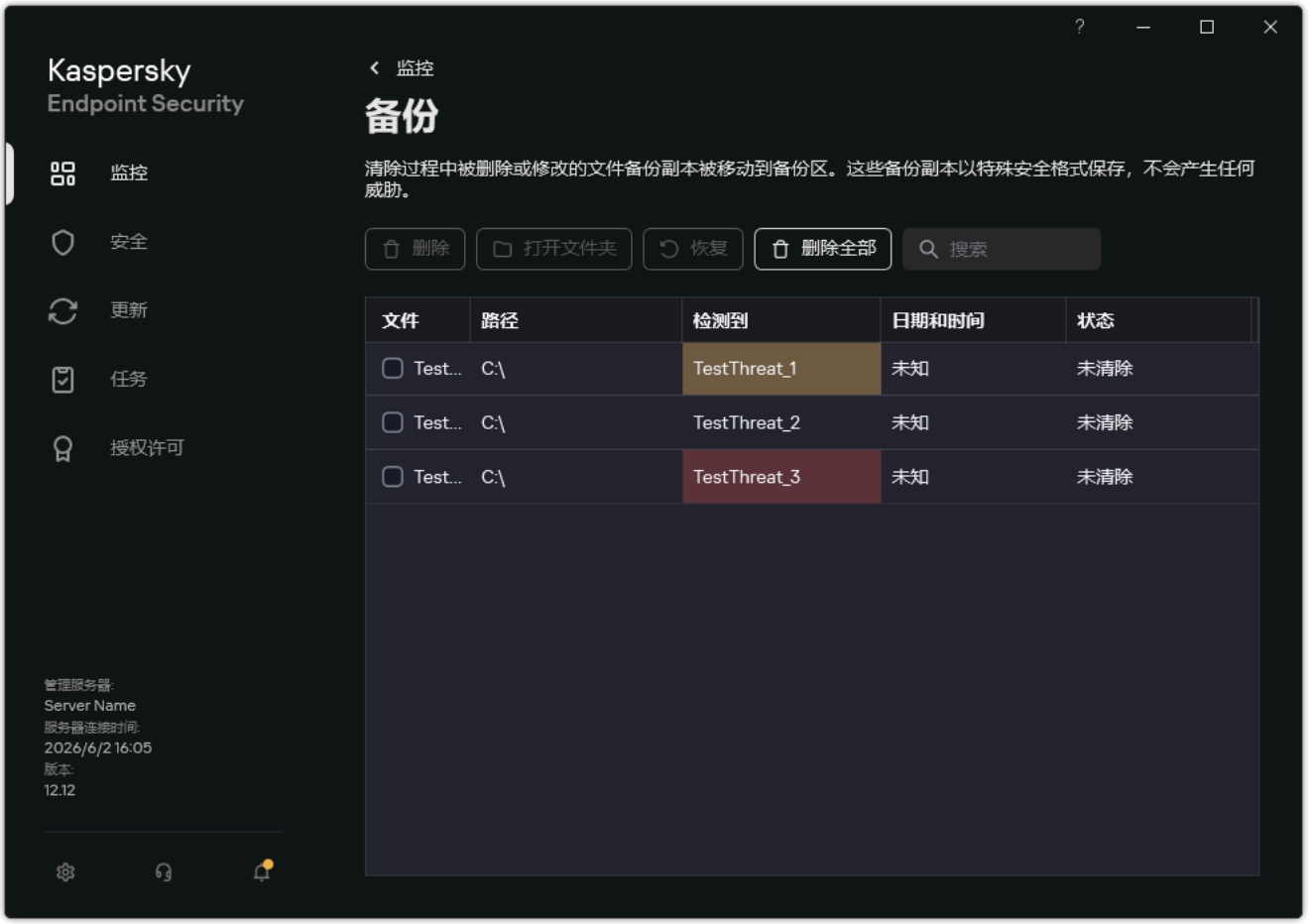
文件备份副本集合以表格显示。对于文件的备份副本，显示文件的原始文件夹路径。文件原始文件夹路径中可能包含个人数据。

> 如果将位于同一文件夹中具有相同名称但内容不同的多个文件移至备份区，则只能恢复最后放入备份区的文件。

要从备份区中还原文件，请执行以下操作：

1. 在应用程序主窗口中，在“**监控**”区域，单击“**备份**”瓦片。
2. 这将打开备份中的文件列表；在该列表中，选择要恢复的文件，然后单击**恢复**。

   Kaspersky Endpoint Security 会将把所选文件的备份副本还原至它们原来所在的文件夹。



备份

从备份区中删除文件备份副本

当应用程序设置中配置的存储期限到期后，Kaspersky Endpoint Security 将自动删除备份区中的所有文件备份副本，而不管它们的状态是什么。您也可以手动从备份区中删除文件的副本。

要从备份区中删除文件备份副本：

1. 在应用程序主窗口中，在“**监控**”区域，单击“**备份**”瓦片。
2. 这将打开备份中的文件列表；在该列表中，选择要从备份删除的文件，然后单击**删除**。

Kaspersky Endpoint Security 从本分区中删除所选文件备份副本。

备份

通知服务

Kaspersky Endpoint Security 执行操作时发生的所有类型的事件。这些事件通知可以是纯粹的信息或包含重要信息。例如，通知可以告知成功更新了数据库和应用程序模块或记录需要纠正的组件错误。

Kaspersky Endpoint Security 支持记录 Microsoft Windows 应用程序日志和 / 或 Kaspersky Endpoint Security 事件日志操作中的事件信息。

Kaspersky Endpoint Security 通过下列方式传送通知：

- 使用 Microsoft Windows 任务栏通知区域中的弹窗通知；
- 通过电子邮件。

您可以配置事件通知的发送方式。您可以为每一类事件配置通知发送方式。

使用事件表配置通知服务时，您可以执行以下操作：

- 按列值或者自定义过滤条件过滤通知服务事件。
- 使用搜索功能搜索通知服务事件。
- 对通知服务事件进行排序。
- 更改通知服务事件列表中的显示顺序和列设置。

配置事件日志设置

要配置事件日志设置，请执行以下操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**界面**”。
3. 在“**通知**”块中单击“**配置通知**”按钮。

   Kaspersky Endpoint Security 组件和任务显示在该窗口的左侧。该窗口的右侧列出了为选定组件或任务生成的事件。

   事件可能包含以下用户数据：

   - Kaspersky Endpoint Security 扫描的文件的路径。
   - 在 Kaspersky Endpoint Security 运行期间修改的注册表项路径。
   - Microsoft Windows 用户名。
   - 用户打开的网页的地址。
4. 在窗口左侧，选择您要为其配置事件日志设置的组件或任务。

5. 选中“**保存在本地报告中**”和“**保存在 Windows 事件日志中**”列中相关事件旁的复选框。

   已在“**保存在本地报告中**”栏中选中复选框的事件将显示在“应用程序日志”中。已在“**保存在 Windows 事件日志中**”栏中选中复选框的事件将显示在“`Application`”区域中的“Windows 日志”中。

6. 保存更改。

配置通知的显示和传送

若要配置通知的显示和传送：

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**常规设置**” → “**界面**”。

3. 在“**通知**”块中单击“**配置通知**”按钮。

   Kaspersky Endpoint Security 组件和任务显示在该窗口的左侧。该窗口的右侧列出了为选定组件或任务生成的事件。

   事件可能包含以下用户数据：

   - Kaspersky Endpoint Security 扫描的文件的路径。
   - 在 Kaspersky Endpoint Security 运行期间修改的注册表项路径。
   - Microsoft Windows 用户名。
   - 用户打开的网页的地址。

4. 在窗口的左侧，选择要为其配置通知传送方式的组件或任务。

5. 在“**在屏幕上通知**”列中，选中相关事件旁的复选框。

   有关选定事件的信息会以 Microsoft Windows 任务栏通知区域中弹出消息的形式显示在屏幕上。

6. 在“**通过电子邮件通知**”列中，选中相关事件旁的复选框。

   如果配置了邮件通知传递设置，则通过电子邮件传送选定事件的信息。

7. 单击“**确定**”。

8. 如果您启用了邮件通知，配置邮件传送设置：

   a. 单击“**配置电子邮件通知**”。

   b. 选择“**通知事件**”复选框以启用传送有关在“**通过电子邮件通知**”列中选定的 Kaspersky Endpoint Security 事件信息的功能。

   c. 指定电子邮件通知传送设置。

   d. 单击“**确定**”。

9. 保存更改。

配置应用程序状态警告在通知区域的显示

若要配置通知区域中应用程序状态警告的显示：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**界面**”。
3. 在“**在通知区域显示应用程序状态**”块中，选择您要在 Microsoft Windows 通知区域中看到通知的事件类型旁的复选框。
4. 保存更改。

发生与选定类别关联的事件时，通知区域的应用程序图标将根据警告的严重性更改为 或 。

用户和管理员之间的消息传递

“应用程序控制”、“设备控制”、“Web 控制”和“自适应异常控制”组件允许其计算机已安装 Kaspersky Endpoint Security 的 LAN 用户向管理员发送消息。

在以下情况下，用户可能需要向本地公司网络管理员发送邮件：

- 设备控制阻止对该设备的访问。

  请求被阻止设备访问权限的邮件模板在“设备控制”区域中 Kaspersky Endpoint Security 界面内。

- “应用程序控制”阻止了某个应用程序的启动。

  请求允许启动被阻止的应用程序的邮件模板在 Kaspersky Endpoint Security 界面的“应用程序控制”区域中提供。

- Web 控制阻止对网页资源的访问。

  请求被阻止网页资源访问权限的邮件模板在“Web 控制”区域中 Kaspersky Endpoint Security 界面内。

用于发送消息的方式和所使用的模板取决于安装 Kaspersky Endpoint Security 的计算机上运行 Kaspersky Security Center 策略，是否连接了 Kaspersky Security Center 管理服务器。有以下情景：

- 如果安装了 Kaspersky Endpoint Security 的计算机上没有运行 Kaspersky Security Center 策略，用户的消息将通过电子邮件发送给本地局域网管理员。

  消息字段的内容将来自 Kaspersky Endpoint Security 本地界面中定义的模板。

- 如果安装了 Kaspersky Endpoint Security 的计算机上运行着 Kaspersky Security Center 策略，标准消息将发送至 Kaspersky Security Center 管理服务器。

  在这种情况下，可以在 Kaspersky Security Center 事件存储中查看用户消息（参见下面的说明）。消息字段的内容将来自 Kaspersky Security Center 策略中定义的模板。

- Kaspersky Security Center 漫游策略运行在安装了 Kaspersky Endpoint Security 的计算机上，用于发送邮件的方法将取决于是否连接了 Kaspersky Security Center。
  - 如果建立了与 Kaspersky Security Center 的连接，Kaspersky Endpoint Security 会将标准邮件发送至 Kaspersky Security Center 管理服务器。
  - 如果没有 Kaspersky Security Center 连接，则用户的消息通过电子邮件发送给本地局域网管理员。

  在这两种情况中，消息字段的内容将来自 Kaspersky Security Center 策略中定义的模板。

要在 Kaspersky Security Center 事件存储中查看用户消息，请执行以下操作：

1. 打开 Kaspersky Security Center Administration Console。
2. 在管理控制台树的“**管理服务器**”中选择“**事件**”选项卡。

   Kaspersky Security Center 工作区将显示 Kaspersky Endpoint Security 运行期间发生的所有事件，包括接收自局域网用户发送给管理员的邮件。
3. 若要配置事件过滤，则在“**事件分类**”下拉列表中选择“**用户请求**”。
4. 选择发送给管理员的消息。
5. 单击管理控制台工作区右侧的“**打开事件属性窗口**”按钮。

管理报告

有关每个 Kaspersky Endpoint Security 组件的操作、数据加密事件、每个扫描任务的性能、更新任务和完整性检查任务以及应用程序的整体操作的信息都记录在报告中。

报告存储在 `C:\ProgramData\Kaspersky Lab\KES.14.1\Report` 文件夹中。

报告可能包含以下用户数据：

- Kaspersky Endpoint Security 扫描的文件的路径。
- 在 Kaspersky Endpoint Security 运行期间修改的注册表项路径。
- Microsoft Windows 用户名。
- 用户打开的网页的地址。

报告中的数据以表格形式显示。每个表格行都含有一个单独事件的相关信息。事件属性位于表格列中。部分列为复合列，包含有带附加属性的嵌套列。要查看附加属性，请单击列名称旁边的 ⊞ 按钮。在各种不同组件或各种任务运行过程中记录下来的事件拥有不同的属性集合。

以下报告可用：

- **系统审计**报告。包含在用户和应用程序进行交互过程中和在应用程序总体操作中发生的事件的相关信息，这些信息与任何特定的 Kaspersky Endpoint Security 组件或任务无关。
- 有关 Kaspersky Endpoint Security 组件操作的报告。
- Kaspersky Endpoint Security 任务报告。
- **数据加密**报告。包含数据加密和解密期间所发生事件的信息。

报告使用以下事件重要性级别：

- **信息性消息**。通常不包含重要信息的参考事件。
- **警告**。反映了 Kaspersky Endpoint Security 操作上的重要情况而需要注意的事件。
- **关键事件**。十分重要的事件以及 Kaspersky Endpoint Security 运行问题或在保护用户计算机时的漏洞。

为便于处理报告，您可以通过以下几种方法修改数据的显示方式：

- 通过各种不同的规则过滤事件列表。
- 使用搜索功能查找特定的事件。
- 在单独的区域中查看所选事件。
- 按照每个报告列的值排列事件列表。

- 使用 ⊞ 按钮显示和隐藏按照事件筛选分组的事件。
- 更改报告中表格列的顺序和排列。

如有需要，您可以将生成的报告保存为文本文件。您还可以删除合并成组的 Kaspersky Endpoint Security 组件和任务的报告信息。

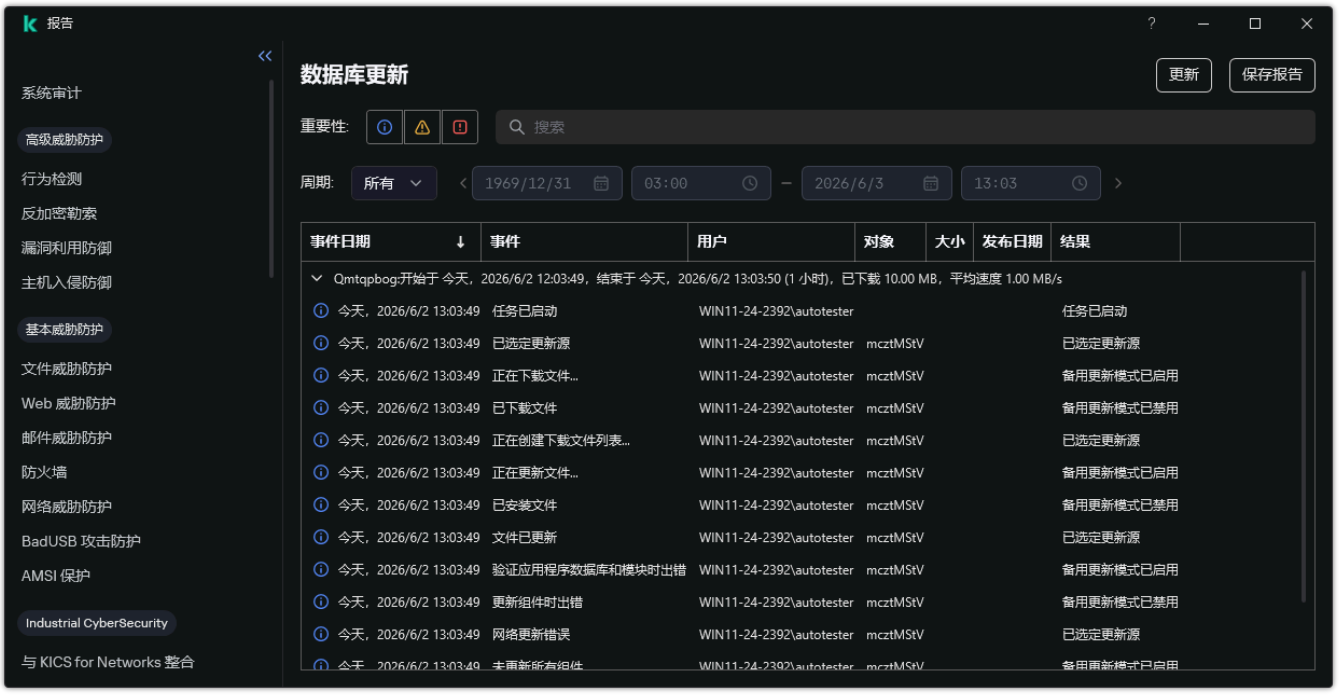
如果 Kaspersky Endpoint Security 在 Kaspersky Security Center 的管理下运行，则有关事件的信息可能会发送到 Kaspersky Security Center 管理服务器（有关更多详细信息，请参阅 Kaspersky Security Center 帮助）。

查看报告

如果用户能查看报告，该用户也能查看报告中反映的所有事件。

若要查看报告：

1. 在应用程序主窗口中，在“**监控**”区域，单击“**报告**”瓦片。



报告

2. 在组件和任务列表中，选择一个组件或任务。

   窗口右侧部分显示的报告中包含 Kaspersky Endpoint Security 的选定组件或选定任务运行所生成的事件列表。您可以根据其中一列的单元格中的值对报告中的事件进行排序。

3. 要查看事件的相关详细信息，请在报告中选择事件。

带有事件概览的块将显示在窗口的底部。

配置最大报告存储时间

Kaspersky Endpoint Security 记录的事件报告的最长存储时间默认为 30 天。在此时间之后，Kaspersky Endpoint Security 将自动删除报告文件中的最早条目。

要修改报告的最大存储期限，请执行下列操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口的“**常规设置**”下，点击“**报告和存储**”瓦片。

报告设置

3. 如果您要限制报告存储期限，在“**报告**”块中选择“**存储报告时间不超过 N 天**”复选框。定义最大报告存储时间。
4. 保存更改。

配置报告文件的最大大小

您可以指定包含报告的文件的最大大小。默认情况下，最大报告文件大小为 1024 MB。要避免超过最大报告文件大小，当达到最大报告文件大小时，Kaspersky Endpoint Security 将自动删除报告文件中的最早条目。

要配置报告文件的最大大小，请执行以下操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口的“**常规设置**”下，点击“**报告和存储**”瓦片。

报告设置

3. 如果您要限制报告文件的大小，在“**报告**”块，选择“**限制报告文件大小为 N MB**”复选框。定义报告文件的最大大小。
4. 保存更改。

将报告保存到文件

用户个人负责确保保存为文件的报告的信息安全，尤其是控制和限制访问该信息。

您可以将所生成的报告保存到文本格式 (TXT) 文件或 CSV 文件中。

Kaspersky Endpoint Security 在报告中记录事件的方式与其在屏幕上的显示方式相同，换言之，两者使用相同的事件属性集和序列。

要将报告保存到文件中，请执行下列操作：

1. 在应用程序主窗口中，在“**监控**”区域，单击“**报告**”瓦片。

报告

2. 这将打开一个窗口，您可以在其中选择组件或任务。
   报告显示在窗口的右侧，其中包含所选 Kaspersky Endpoint Security 组件或任务操作中事件的列表。

3. 如有必要，您可以通过下列方法修改报告中的数据呈现方式：

   - 过滤事件
   - 运行事件搜索
   - 重新排列各列
   - 事件排序

4. 单击窗口右上部的“**保存报告**”按钮。

5. 在打开的窗口中，指定报告文件的目标文件夹。

6. 输入报告文件的名称。

7. 选择必要的报告文件格式：TXT 或 CSV。

8. 保存更改。

清理报告

要删除报告中的信息，请执行下列操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口的“**常规设置**”下，点击“**报告和存储**”瓦片。

报告设置

3. 在“**报告**”块中单击“**清除**”按钮。
4. 如果密码保护被启用，Kaspersky Endpoint Security 可能提示您输入用户账户凭证。如果用户没有所需权限，应用程序提示输入账户凭证。

Kaspersky Endpoint Security 将删除所有应用程序组件和任务报告。

Kaspersky Endpoint Security 自我保护

自我保护可防止其他应用程序执行可能干扰 Kaspersky Endpoint Security 操作的操作，例如，从计算机中卸载 Kaspersky Endpoint Security。对 Kaspersky Endpoint Security 的可用的自我保护技术的设置取决于操作系统是 32 位还是 64 位（参见下表）。自我保护还包括密码保护和管理服务器连接保护。

*密码保护*允许您根据用户被授予的权限（例如，退出应用程序的权限）来限制用户对 Kaspersky Endpoint Security 的访问。

*管理服务器连接保护*防止计算机未经授权重新连接到不受信任的服务器。

Kaspersky Endpoint Security 自我保护技术

技术	描述	x86 计算机	x64 计算机
自我保护机制	该技术阻止对以下应用程序组件的访问： • 位于 Kaspersky Endpoint Security 安装文件夹中的文件和应用程序的其他文件； • 属于应用程序的注册表键； • 应用程序运行的进程。	✓	✓
AM-PPL (Antimalware Protected Process Light)	该技术保护 Kaspersky Endpoint Security 进程免受恶意操作。有关 AM-PPL 技术的详细信息，请访问 Microsoft 网站。 AM-PPL 技术适用于 Windows 10 版本 1703 (RS2) 或更高版本以及 Windows Server 2019 操作系统。	✓	✓
外部管理防御机制	该技术阻止其他应用程序（例如 TeamViewer 或 RemotelyAnywhere）访问 Kaspersky Endpoint Security。	✓	– （除了 Windows 7）

启用和禁用自我防御

Kaspersky Endpoint Security 可防止修改或删除硬盘驱动器中的应用程序文件、内存进程和系统注册表中的条目。

该技术阻止对以下应用程序组件的访问：

- 位于 Kaspersky Endpoint Security 安装文件夹中的文件和应用程序的其他文件；
- 属于应用程序的注册表键；
- 应用程序运行的进程。

默认情况下已启用 Kaspersky Endpoint Security 的自我保护机制。

如何在管理控制台(MMC)中启用或禁用自我保护

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **应用程序设置**。

4. 使用**启用自我保护**复选框启用或禁用自我保护机制。

5. 保存更改。

如何在 Web Console 和云控制台中启用或禁用自我保护

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **常规设置** → **自我保护**。

5. 使用“**自我保护已启用**”切换开关启用或禁用自我保护机制。

6. 保存更改。

如何在应用程序界面中启用或禁用自我保护

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**常规设置**” → “**应用程序设置**”。

Kaspersky Endpoint Security for Windows 设置

3. 使用**启用自我保护**复选框启用或禁用自我保护机制。

4. 保存更改。

启用和禁用 AM-PPL 支持

Kaspersky Endpoint Security 支持 Microsoft 的“Antimalware Protected Process Light”技术（以下简称“AM-PPL”）。AM-PPL 保护 Kaspersky Endpoint Security 进程免受恶意操作（例如，终止应用程序）。AM-PPL 仅允许运行受信任的进程。Kaspersky Endpoint Security 进程根据 Windows 安全要求进行签名，因此它们是受信任的。有关 AM-PPL 技术的详细信息，请访问 Microsoft 网站。默认情况下启用 AM-PPL 技术。

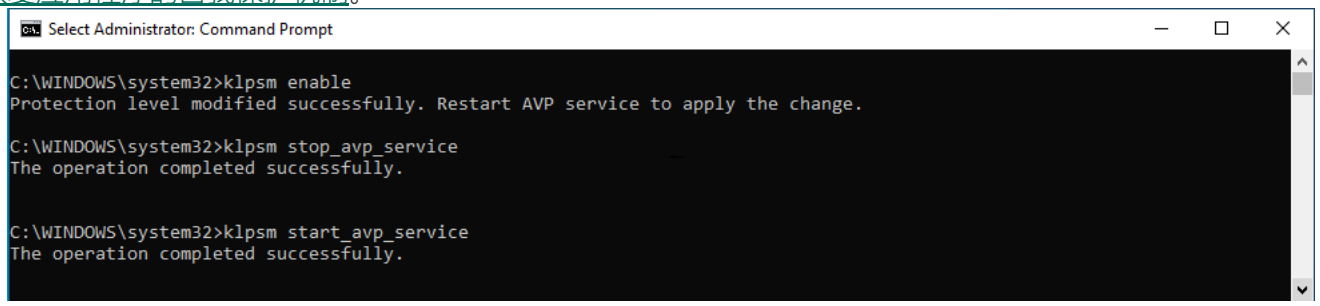
Kaspersky Endpoint Security 还具有用于保护应用程序进程的内置机制。AM-PPL 支持允许您将进程安全功能委派给操作系统。从而可以提高应用程序的速度并减少计算机资源的消耗。

持续使用 AM-PPL 技术。AM-PPL 是操作系统保护的重要组件。禁用 AM-PPL 支持可能会导致某些 Kaspersky Endpoint Security 功能失败（例如，应用程序与 Windows Security Center 的整合）。仅允许在单独的测试环境中出于故障排除目的禁用 AM-PPL 支持。

AM-PPL 技术适用于 Windows 10 版本 1703 (RS2) 或更高版本以及 Windows Server 2019 操作系统。

要启用或禁用 AM-PPL 技术：

1. 关闭应用程序的自我保护机制。
   自我保护机制会阻止修改和删除计算机内存中的应用程序进程，包括更改 AM-PPL 状态。
2. 以管理员身份运行命令行解释器 (cmd.exe)。
3. 转到 Kaspersky Endpoint Security 可执行文件所在文件夹。
   您可以在应用程序安装期间将可执行文件的路径添加到 %PATH% 系统变量中。
4. 在命令行中输入以下命令：
   - `klpsm.exe enable` – 启用对 AM-PPL 技术的支持（请参见下图）。
   - `klpsm.exe disable` – 禁用对 AM-PPL 技术的支持。
5. 重新启动 Kaspersky Endpoint Security。
6. 恢复应用程序的自我保护机制。



启用对 AM-PPL 技术的支持

针对外部管理对应用程序服务的保护

针对外部管理对应用程序服务的保护阻止用户和其他应用程序试图停止 Kaspersky Endpoint Security 服务的尝试。保护可确保以下服务的运行：

- Kaspersky Endpoint Security 服务 (AVP.KES.14.1)
- Kaspersky Seamless Update Service 服务（AVPSUS.KES.14.1）

要从命令行退出应用程序，禁用对 Kaspersky Endpoint Security 服务的外部管理的防御。

您只能在不支持 AM-PPL 技术的计算机或禁用该技术的计算机上允许对应用程序服务进行外部管理。

如何在管理控制台 (MMC) 中启用或禁用应用程序服务免受外部管理的保护

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **应用程序设置**。
4. 使用“**阻止应用程序服务的外部管理**”复选框启用或禁用对 Kaspersky Endpoint Security 服务的外部管理的防御。
5. 保存更改。

如何在 Web Console 和云控制台中启用或禁用应用程序服务免受外部管理的保护

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **自我保护**。
5. 使用“**阻止应用程序服务的外部管理**”复选框启用或禁用对 Kaspersky Endpoint Security 服务的外部管理的防御。
6. 保存更改。

如何在应用程序界面中启用或禁用应用程序服务免受外部管理的保护

1. 打开主应用程序窗口并单击 ⚙ 按钮。

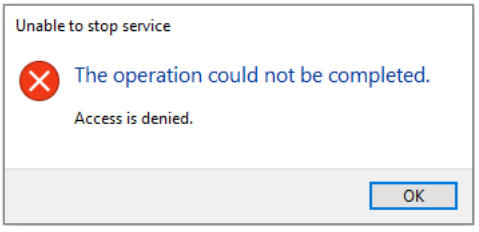
2. 在应用程序设置窗口中，选择“**常规设置**” → “**应用程序设置**”。

Kaspersky Endpoint Security for Windows 设置

3. 使用“**阻止应用程序服务的外部管理**”复选框启用或禁用对 Kaspersky Endpoint Security 服务的外部管理的防御。

4. 保存更改。

因此，当用户尝试停止应用程序服务时，会出现一个带有错误消息的系统窗口。用户只能从 Kaspersky Endpoint Security 界面管理应用程序服务。



应用程序服务访问错误

支持远程管理应用程序

在启用外部管理防御的情况下，您偶尔可能需要使用远程管理应用程序。

若要启用远程管理应用程序的操作，请执行以下操作：

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**排除项和检测对象类型**”。
3. 在“**排除项**”区域，单击“**指定受信任应用程序**”链接。
4. 在打开的窗口中，单击“**添加**”按钮。
5. 选择远程管理应用程序的可执行文件。

   您也可以手动输入路径。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。
6. 选择**允许与 Kaspersky Endpoint Security 的界面进行交互**复选框。
7. 保存更改。

密码保护

多个不同计算机知识水平的用户可以公用一台计算机。如果用户可以无限制访问 Kaspersky Endpoint Security 及其设置，则计算机保护的总体水平可能会下降。密码保护允许您根据用户被授予的权限（例如，退出应用程序的权限）来限制用户对 Kaspersky Endpoint Security 的访问。

如果启动 Windows 会话的用户（*会话用户*）拥有执行操作的权限，则 Kaspersky Endpoint Security 不会请求用户名和密码或临时密码。用户将按照授予的权限获得 Kaspersky Endpoint Security 的访问权限。

如果会话用户没有执行操作的权限，该用户可以通过以下方式获得应用程序的访问权限：

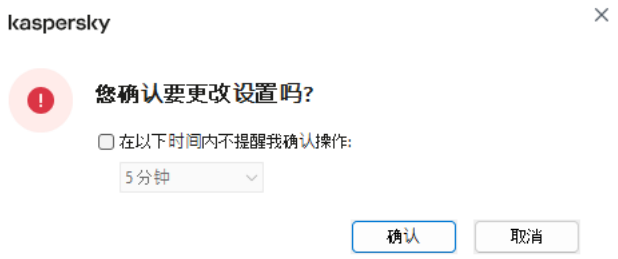
- 输入用户名和密码。

  此方法适合日常操作。要执行受密码保护的操作，必须输入具有所需权限的用户的域账户凭据。在这种情况下，计算机必须位于该域中。如果计算机不在域中，您可以使用 KL Admin 账户或手动添加的账户。
- 输入临时密码。

  此方法适合为公司网络外部的用户授予执行被阻止操作（例如，退出应用程序）的临时权限。当临时密码到期或会话结束后，Kaspersky Endpoint Security 会将其设置恢复为先前状态。

当用户尝试执行受密码保护的操作时，Kaspersky Endpoint Security 会提示用户输入用户名和密码或者临时密码（请参见下图）。

在密码输入窗口中，只能按 **ALT+SHIFT** 切换语言。即使在操作系统中配置了其他快捷方式，使用这些快捷方式也无法切换语言。



Kaspersky Endpoint Security 访问密码提示

用户名和密码

要访问 Kaspersky Endpoint Security，您应该输入账户凭据。密码保护支持以下账户：

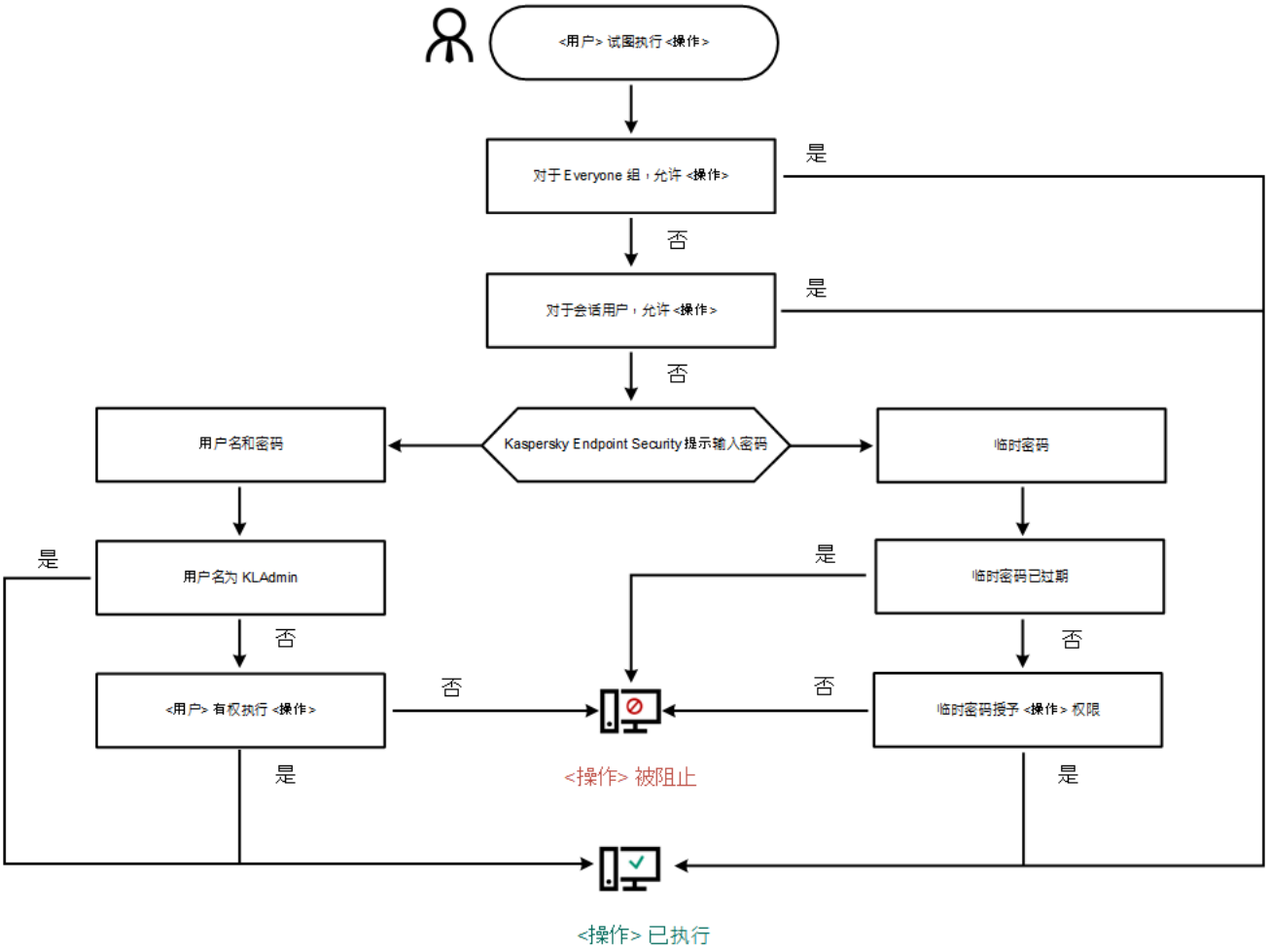
- **KLAdmin**。具有 Kaspersky Endpoint Security 无限制访问权限的管理员账户。KLAdmin 账户有权执行任何受密码保护的操作。KLAdmin 账户的权限无法撤销。当启用密码保护时，Kaspersky Endpoint Security 会提示您设置 KLAdmin 账户的密码。
- **手动添加的账户**。Active Directory 域之外的账户。如果您不想共享管理员密码，可以使用此服务账户而不是 KLAdmin。您可以设置任何用户名和密码，并配置个人权限。
- **Everyone 组**。Windows 内置的组，包括公司网络内的所有用户。Everyone 组中的用户可以根据其被分配的权限访问应用程序。
- **单个用户或组**。可以为其配置单个权限的用户账户。例如，如果针对 Everyone 组阻止某个操作，您可以允许单个用户或组执行该操作。
- **会话用户**。启动了 Windows 会话的用户账户。当系统提示输入密码时，您可以切换到其他会话用户（“**保存当前会话密码**”复选框）。此时，Kaspersky Endpoint Security 会将输入了账户凭据的用户（而不是启动了 Windows 会话的用户）视为会话用户。

临时密码

临时密码可用于授权公司网络外部的单台计算机临时访问 Kaspersky Endpoint Security。管理员在 Kaspersky Security Center 的计算机属性中为单台计算机生成临时密码。管理员选择将以临时密码保护的操作，并指定临时密码的有效期。

密码保护操作算法

Kaspersky Endpoint Security 根据以下算法决定是允许还是阻止受密码保护的操作（请参见下图）。



密码保护操作算法

启用密码保护

密码保护允许您根据用户被授予的权限（例如，退出应用程序的权限）来限制用户对 Kaspersky Endpoint Security 的访问。

如何在管理控制台（MMC）中启用密码保护

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **界面**。
4. 在“**密码保护**”块中单击“**设置**”按钮。
   这将打开一个带有密码保护设置的窗口。
5. 使用“**启用密码保护**”复选框启用或禁用组件。

6. 在“**权限**”下，选择 KLAdmin 账户。

7. 这会打开一个窗口；在该窗口中，单击“**密码**”并为 KLAdmin 账户设置密码。
   KLAdmin 账户有权执行任何受密码保护的操作。

   > 如果您忘记了您的 KLAdmin 账户密码，您可以在策略属性中重置密码。

8. 返回账户列表。

9. 设置公司网络内所有用户的权限：

   a. 在“**权限**”下，选择“所有人”组。
      *Everyone 组*是 Windows 内置的组，包括公司网络内的所有用户。

   b. 在打开的窗口中，选中用户不必输入密码即可执行的操作旁边的复选框。
      如果清除某个复选框，用户将被阻止执行相应操作。例如，如果清除“**退出应用程序**”权限旁边的复选框，则只有您以 KLAdmin 身份登录或者以拥有所需权限的单个用户身份登录或者输入临时密码才能退出应用程序。

      > 密码保护权限有几个需要考虑的重要方面。确保已满足访问 Kaspersky Endpoint Security 的所有条件。

10. 保存更改。

如何在 Web Console 和云控制台中启用密码保护

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **常规设置** → **自我保护**。

5. 在“**密码保护**”下，使用“**密码保护已启用**”开关启用或禁用组件。

6. 指定 KLAdmin 账户的密码并确认。
   KLAdmin 账户有权执行任何受密码保护的操作。

   > 如果您忘记了您的 KLAdmin 账户密码，您可以在策略属性中重置密码。

7. 返回账户列表。

8. 设置公司网络内所有用户的权限：

   a. 在账户表中，选择“所有人”组。
      *Everyone 组*是 Windows 内置的组，包括公司网络内的所有用户。

b. 在打开的窗口中，选中用户不必输入密码即可执行的操作旁边的复选框。

如果清除某个复选框，用户将被阻止执行相应操作。例如，如果清除“**退出应用程序**”权限旁边的复选框，则只有您以 KLAdmin 身份登录或者以拥有所需权限的单个用户身份登录或者输入临时密码才能退出应用程序。

> 密码保护权限有几个需要考虑的重要方面。确保已满足访问 Kaspersky Endpoint Security 的所有条件。

9. 保存更改。

如何在应用程序界面中启用密码保护

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**界面**”。
3. 使用**密码保护**开关启用或禁用组件。
4. 指定 KLAdmin 账户的密码并确认。

   KLAdmin 账户有权执行任何受密码保护的操作。

> 如果计算机在某个策略下运行，管理员可以在策略属性中重置 KLAdmin 账户的密码。如果计算机未连接到 Kaspersky Security Center 并且您忘记了 KLAdmin 账户的密码，则无法恢复密码。

5. 设置公司网络内所有用户的权限：

   a. 在账户表中，单击“**编辑**”以打开 Everyone 组的权限列表。

   *Everyone 组*是 Windows 内置的组，包括公司网络内的所有用户。

   b. 选中用户不必输入密码即可执行的操作旁边的复选框。

   如果清除某个复选框，用户将被阻止执行相应操作。例如，如果清除“**退出应用程序**”权限旁边的复选框，则只有您以 KLAdmin 身份登录或者以拥有所需权限的单个用户身份登录或者输入临时密码才能退出应用程序。

> 密码保护权限有几个需要考虑的重要方面。确保已满足访问 Kaspersky Endpoint Security 的所有条件。

6. 保存更改。

启用密码保护后，应用程序将根据 Everyone 组被授予的权限来限制用户对 Kaspersky Endpoint Security 的访问。只有您使用 KLAdmin 账户，使用被授予所需权限的其他账户或者输入临时密码时，才能执行 Everyone 组被阻止的操作。

> 仅当您以 KLAdmin 身份登录时，才能禁用密码保护。如果您使用任何其他用户账户或临时密码，则无法禁用密码保护。

在密码检查期间，可以选中“**保存当前会话密码**”复选框。在这种情况下，当用户尝试在会话期间执行其他受密码保护的操作时，Kaspersky Endpoint Security 不会提示输入密码。

为单个用户或组授予权限

密码保护允许授予 Kaspersky Endpoint Security 对单个 Active Directory 用户账户和手动添加的用户账户的访问权限。

Active Directory 用户账户

您可以向 Active Directory 域中的单个用户或组授予 Kaspersky Endpoint Security 访问权限。例如，如果 Everyone 组被阻止退出应用程序，您可以将“**退出应用程序**”权限授予给单个用户。这样，只有以该用户或以 KLAdmin 身份登录时才能退出应用程序。

> 仅当计算机位于域中时，才能使用账户凭据访问应用程序。如果计算机不在域中，您可以使用 KLAdmin 账户或临时密码。

手动添加的用户账户

您可以创建 Active Directory 中不存在的用户账户，并为该用户账户分配单独权限。也就是说，您可以创建一个*服务用户账户*并使用它来代替 KLAdmin。这样，您就不需要与其他用户共享您的 KLAdmin 密码或创建新的 Active Directory 用户账户。您可以指定任何用户名和密码。例如，您可以将“**查看报告**”权限授予服务用户账户。因此，如果“全部”组禁止查看报告，您可以使用服务用户账户或 KLAdmin 用户账户打开报告。

为单个用户或组授予权限

如何在管理控制台 (MMC) 中向单个用户或组授予权限

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **界面**。
4. 在“**密码保护**”块中单击“**设置**”按钮。
   这将打开一个带有密码保护设置的窗口。
5. 在账户表格中，单击“**添加**”。
6. 选择要添加的用户账户的类型：
   - **从 Active Directory 中选择用户/组** – Active Directory 用户账户。
     要选择用户帐户，请单击“**选择**”。选择 Active Directory 中的用户或组，然后确认选择。
   - 为手动添加的服务用户账户**手动添加用户/用户组**。

要添加服务用户账户，请输入用户名和密码（例如，SecureAdmin）。

> 您可以在策略设置中重置服务用户账户密码。必须以与 KL Admin 密码相同的方式重置服务用户账户密码。如果允许编辑密码保护设置（“锁”打开）或计算机上未应用任何策略，您可以在应用程序界面中重置服务用户账户的密码。为此，请使用 KL Admin 密码确认服务用户账户信息的更改。

7. 在“**权限**”列表中，选中选定用户或组在不被提示输入密码的情况下即可执行的操作旁边的复选框。

   如果清除某个复选框，用户将被阻止执行相应操作。例如，如果清除“**退出应用程序**”权限旁边的复选框，则只有您以 KL Admin 身份登录或者以拥有所需权限的单个用户身份登录或者输入临时密码才能退出应用程序。

> 密码保护权限有几个需要考虑的重要方面。确保已满足访问 Kaspersky Endpoint Security 的所有条件。

8. 保存更改。

如何在 Web Console 和云控制台中向单个用户或组授予权限

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

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **自我保护**。
5. 在“**密码保护**”区域，单击“**用户权限**”链接。

   这将打开授予启用密码权限的表单。
6. 单击“**添加**”。
7. 选择要添加的用户账户的类型：

   - **从 Active Directory 中选择** – Active Directory 用户账户。

     要选择用户帐户，请单击“**编辑**”。选择 Active Directory 中的用户或组，然后确认选择。
   - 为手动添加的服务用户账户**手动添加**。

     要添加服务用户账户，请输入用户名和密码（例如，SecureAdmin）。

> 您可以在策略设置中重置服务用户账户密码。必须以与 KL Admin 密码相同的方式重置服务用户账户密码。如果允许编辑密码保护设置（“锁”打开）或计算机上未应用任何策略，您可以在应用程序界面中重置服务用户账户的密码。为此，请使用 KL Admin 密码确认服务用户账户信息的更改。

8. 在“**权限**”列表中，选中选定用户或组在不被提示输入密码的情况下即可执行的操作旁边的复选框。

   如果清除某个复选框，用户将被阻止执行相应操作。例如，如果清除“**退出应用程序**”权限旁边的复选框，则只有您以 KL Admin 身份登录或者以拥有所需权限的单个用户身份登录或者输入临时密码才能退出应用程序。

> 密码保护权限有几个需要考虑的重要方面。确保已满足访问 Kaspersky Endpoint Security 的所有条件。

9. 单击“**添加**”。

10. 保存更改。

如何在应用程序的用户界面中向单个用户或组授予权限

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在应用程序设置窗口中，选择“**常规设置**” → “**界面**”。

3. 在账户表格中，单击“**添加**”。

4. 选择要添加的用户账户的类型：

   - **从 Active Directory 中选择用户/组** – Active Directory 用户账户。

     要选择用户帐户，请单击“**选择用户或组**”。选择 Active Directory 中的用户或组，然后确认选择。

   - 为手动添加的服务用户账户**手动添加用户**。

     要添加服务用户账户，请输入用户名和密码（例如，SecureAdmin）。

     > 您可以在策略设置中重置服务用户账户密码。必须以与 KLAdmin 密码相同的方式重置服务用户账户密码。如果允许编辑密码保护设置（“锁”打开）或计算机上未应用任何策略，您可以在应用程序界面中重置服务用户账户的密码。为此，请使用 KLAdmin 密码确认服务用户账户信息的更改。

5. 在“**权限**”列表中，选中选定用户或组在不被提示输入密码的情况下即可执行的操作旁边的复选框。

   如果清除某个复选框，用户将被阻止执行相应操作。例如，如果清除“**退出应用程序**”权限旁边的复选框，则只有您以 KLAdmin 身份登录或者以拥有所需权限的单个用户身份登录或者输入临时密码才能退出应用程序。

   > 密码保护权限有几个需要考虑的重要方面。确保已满足访问 Kaspersky Endpoint Security 的所有条件。

6. 保存更改。

结果，如果限制了 Everyone 组访问应用程序，将根据用户的单个权限授予用户访问 Kaspersky Endpoint Security 的权限。

使用临时密码授予权限

临时密码可用于授权公司网络外部的单台计算机临时访问 Kaspersky Endpoint Security。要允许用户在不获取 KLAdmin 账户凭据的情况下执行被阻止的操作，这是必需的。要使用临时密码，必需将计算机添加到 Kaspersky Security Center 中。

如何允许用户通过管理控制台(MMC)使用临时密码执行阻止的操作

1. 打开 Kaspersky Security Center Administration Console。

2. 在管理控制台树的“**受管理设备**”文件夹中，打开相关客户端计算机所属的管理组名称的文件夹。

3. 在工作区中选择“**设备**”选项卡。

4. 双击以打开计算机属性窗口。

5. 在计算机属性窗口中，选择“**应用程序**”区域。

6. 在计算机上安装的卡巴斯基应用程序列表中，选择 **Kaspersky Endpoint Security for Windows (14.1)** 并双击以打开应用程序属性。

7. 在应用程序设置窗口中，选择“**常规设置**” → “**界面**”。

8. 在“**密码保护**”块中单击“**设置**”按钮。

9. 在打开的窗口中，在“**临时密码**”块，点击“**临时密码列表**”按钮。
   临时密码管理窗口打开。

10. 单击“**添加**”。

11. 在“**到期日期**”字段中，指定临时密码的到期日期。

12. 在“**临时密码范围**”表中，选中用户在输入临时密码后可以执行的操作旁边的复选框。

13. 单击“**生成**”。
    将打开一个包含临时密码的窗口（请参见下图）。

14. 复制密码并将其提供给用户。

如何允许用户通过 Web Console 和云控制台使用临时密码执行阻止的操作

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**资产(设备)**”。

2. 单击要允许用户执行阻止操作的计算机的名称。

3. 选择**应用程序**选项卡。

4. 单击“**Kaspersky Endpoint Security for Windows**”。
   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. 在应用程序设置窗口中，选择“**常规设置**” → “**界面**”。

7. 在“**临时密码**”块中单击“**添加**”按钮。

8. 在“**到期日期**”字段中，指定临时密码的到期日期。

9. 在“**临时密码范围**”表中，选中用户在输入临时密码后可以执行的操作旁边的复选框。

10. 单击“**生成**”。

    将打开一个包含临时密码的窗口。

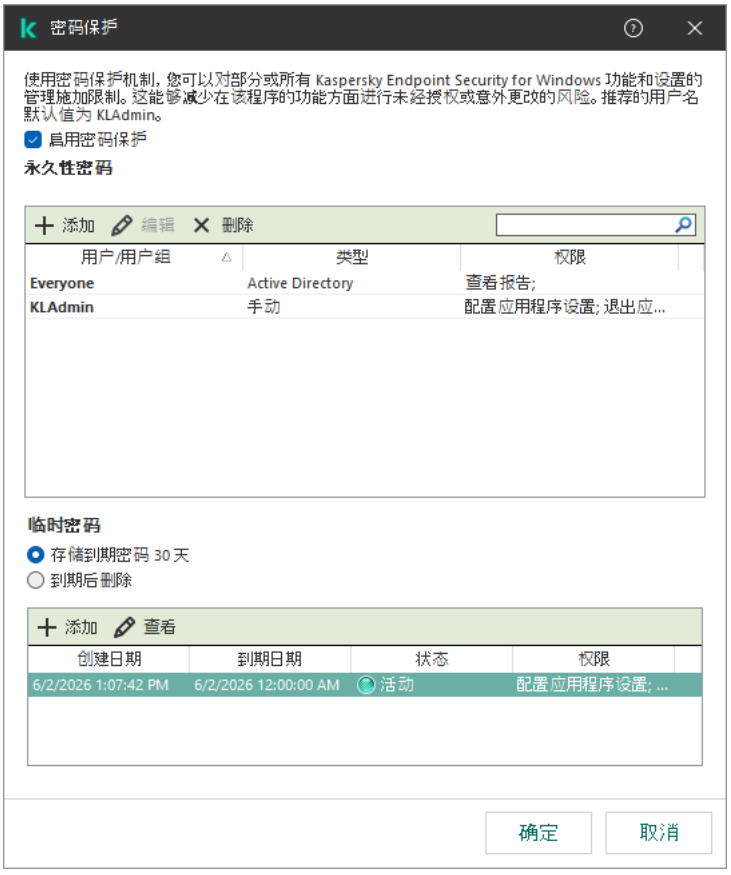
11. 复制密码并将其提供给用户。

临时密码

撤销临时密码

从 12.9 版开始， Kaspersky Endpoint Security for Windows 包含*临时密码管理*功能。管理临时密码可让您执行以下操作：

- 保存密码历史记录（最多 30 天）。
- 监控临时密码状态：*活动*、*已过期*、*已撤销*。
- 撤销临时密码。



临时密码管理

临时密码管理仅在将计算机与 Kaspersky Security Center 同步后才更新密码的状态和撤销密码。

如何使用管理控制台（MMC）撤销临时密码

1. 打开 Kaspersky Security Center Administration Console。
2. 在管理控制台树的“**受管理设备**”文件夹中，打开相关客户端计算机所属的管理组名称的文件夹。
3. 在工作区中选择“**设备**”选项卡。
4. 双击以打开计算机属性窗口。
5. 在计算机属性窗口中，选择“**应用程序**”区域。
6. 在计算机上安装的卡巴斯基应用程序列表中，选择 **Kaspersky Endpoint Security for Windows (14.1)** 并双击以打开应用程序属性。
7. 在应用程序设置窗口中，选择“**常规设置**” → “**界面**”。
8. 在“**密码保护**”块中单击“**设置**”按钮。
9. 这将打开一个窗口；在该窗口中，在“**临时密码**”下，配置过期密码的存储设置。
10. 单击“**临时密码列表**”。
    临时密码管理窗口打开。临时密码管理显示密码的到期日期、密码的状态、权限列表。
11. 选择要撤销的活动临时密码，然后双击该密码以打开其属性。
12. 在打开的窗口中，单击“**撤销**”按钮。
13. 保存更改。要在计算机上应用该策略，请关闭“挂锁”。

如何在 Web Console 和云控制台中撤销临时密码

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**资产(设备)**”。
2. 单击要允许用户执行阻止操作的计算机的名称。
3. 选择**应用程序**选项卡。
4. 单击“**Kaspersky Endpoint Security for Windows**”。
   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. 在应用程序设置窗口中，选择“**常规设置**” → “**界面**”。
7. 在“**临时密码**”下，配置过期密码的存储。
8. 单击**临时密码**链接。
   临时密码管理窗口打开。临时密码管理显示密码的到期日期、密码的状态、权限列表。
9. 选择要撤销的活动临时密码。

10. 在打开的窗口中，单击“**撤销密码**”按钮。

11. 保存更改。要在计算机上应用该策略，请关闭“挂锁”。

因此，临时密码管理将密码的状态设置为“*正在撤销(与主机同步)*”。将计算机与 Kaspersky Security Center 同步后，应用程序会立即撤销临时密码并阻止授予的权限。

密码保护权限的特殊方面

密码保护权限有几个需要考虑的重要方面和限制。

配置应用程序设置

如果用户的计算机在某个策略下运行，请确保策略中的所有必需设置均可编辑（属性是打开的）。

退出应用程序

没有特殊注意事项或限制。

禁用保护组件

- 无法为 Everyone 组授予禁用保护组件的权限。要允许除 KLAdmin 以外的用户禁用控制组件，请在密码保护设置中添加具有“**禁用保护组件**”权限的用户或组。
- 如果用户的计算机在某个策略下运行，请确保策略中的所有必需设置均可编辑（属性是打开的）。
- 要在应用程序设置中禁用保护组件，用户必须具有“**配置应用程序设置**”权限。
- 要从上下文菜单禁用保护组件（使用“**暂停保护**”菜单项），除了“**禁用控制组件**”权限外，用户还必须具有“**禁用保护组件**”权限。

禁用控制组件

- 无法为 Everyone 组授予禁用控制组件的权限。要允许除 KLAdmin 以外的用户禁用控制组件，请在密码保护设置中添加具有“**禁用控制组件**”权限的用户或组。
- 如果用户的计算机在某个策略下运行，请确保策略中的所有必需设置均可编辑（属性是打开的）。
- 要在应用程序设置中禁用控制组件，用户必须具有“**配置应用程序设置**”权限。
- 要从上下文菜单禁用控制组件（使用“**暂停保护**”菜单项），除了“**禁用保护组件**”权限外，用户还必须具有“**禁用控制组件**”权限。

禁用 Kaspersky Security Center 策略

您不能为“Everyone”组授予禁用 Kaspersky Security Center 策略的权限。要允许除 KLAdmin 以外的用户禁用该策略，请在密码保护设置中添加具有“**禁用 Kaspersky Security Center 策略**”权限的用户或组。

删除密钥

没有特殊注意事项或限制。

卸载/修改/恢复应用程序

如果您对“所有”组允许了卸载、修改和恢复应用程序，Kaspersky Endpoint Security 在用户试图做这些操作时不请求密码。因此，包括域外用户的任何用户都可以安装、修改或恢复应用程序。

恢复加密驱动器数据的访问权限

只有以 KLAdmin 身份登录时，才能恢复对加密驱动器数据的访问。执行此操作的权限不能授予给任何其他用户。

查看报告

没有特殊注意事项或限制。

从备份区恢复

没有特殊注意事项或限制。

导出设置

默认情况下，“全部”组均无法导出应用程序设置。您可以使用 KLAdmin 用户账户导出应用程序设置。导出应用程序设置仅包括在应用程序界面中创建带有 Kaspersky Endpoint Security 设置的配置文件。该权限不限制导出扫描排除项列表、受信任的网址、受信任设备或应用程序组件维护的其他列表。

重置 KLAdmin 密码

如果您忘记了您的 KLAdmin 账户密码，您可以在策略属性中重置密码。您无法在应用程序界面中重置密码。

您可以使用临时密码执行密码保护的操作。此种情况下，您不需要输入 KLAdmin 凭证。

如果计算机未连接到 Kaspersky Security Center 并且您忘记了 KLAdmin 账户的密码，则无法恢复密码。

如何使用管理控制台(MMC)重置 KLAdmin 账户密码

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **界面**。
4. 在“**密码保护**”块中单击“**设置**”按钮。
5. 在打开的窗口中，清空“**启用密码保护**”复选框。
6. 保存更改。
7. 再次选择**启用密码保护**复选框。
8. 单击“**确定**”。
   这将打开管理员密码窗口。
9. 指定 KLAdmin 账户的新密码并确认。
10. 保存更改。

如何在 Web 控制台和云控制台重置 KLAdmin 账户密码

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**资产(设备)**”。
2. 选择要为其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 Windows**”。
   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 **常规设置** → **自我保护**。
7. 在“**密码保护**”下，关闭“**密码保护**”开关。
8. 保存更改。

9. 再次开启“**密码保护**”开关。

10. 指定 KLAdmin 账户的新密码并确认。

11. 保存更改。

这样，您的 KLAdmin 账户的密码就在应用策略后被更新。

管理服务器连接保护

使用 Kaspersky Security Center 的*网络代理*组件可以将计算机连接到管理服务器。如果入侵者有足够的权限修改服务器连接设置，则存在将计算机连接到不受信任的服务器的风险。这将允许入侵者应用他们自己的组策略，例如，禁用应用程序的自我保护。Kaspersky Endpoint Security 可以防止未经授权将计算机重新连接到其他服务器。为了保护服务器连接，应用程序建议设置密码并使用Password-Based key Derivation Function(PBKDF2)。因此，在没有密码的情况下访问应用程序是不可能的。

> 为了确保 Kaspersky Endpoint Security 和网络代理免受未经授权的访问的全面保护，我们建议启用额外的保护。对于 Kaspersky Endpoint Security，我们建议启用密码保护。为了保护网络代理，我们建议设置卸载密码。有关保护网络代理不被删除的详细信息，请参阅 Kaspersky Security Center 帮助。

管理计算机与管理服务器的连接是使用“*管理服务器连接保护*”任务实现的。任务允许您执行以下操作：

- 设置密码以保护服务器连接。
- 更改密码。
- 将计算机重新连接到其他服务器。
- 禁用服务器连接保护。

连接到管理服务器时的计算机身份验证

设置密码后，应用程序使用密码的 PBKDF2 转换创建一个数据数组。然后，应用程序使用网络代理密钥对该数据数组进行加密。应用程序使用加密的数据数组来检查管理服务器的后续连接的权限和特权。

随后，每当尝试将计算机重新连接到管理服务器时，应用程序都会使用网络代理密钥解密数据数组，并将其与本地副本进行比较。如果它们不匹配，则会限制对应用程序的访问。

管理服务器连接保护

如何在管理控制台 (MMC) 中为服务器连接保护设置密码

1. 在 Kaspersky Security Center 管理控制台树中，选择“**任务**”。

   任务列表打开。

2. 单击“**新任务**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 选择任务类型

选择“**Kaspersky Endpoint Security for Windows (14.1)**”→ “**管理服务器连接保护**”。

步骤 2. 保护管理服务器连接

设置密码以保护管理服务器连接：

1. 在“**管理服务器连接保护**”下，选择“**使用密码保护**”。
2. 在“**管理服务器**”下拉列表中，选择“**新服务器**”。
3. 在“**管理服务器连接密码**”字段中，设置并确认连接到管理服务器的密码。

   如果您忘记了密码，您可以使用任务更改密码。
4. 如果您已部署 Kaspersky Endpoint Security 12.7 或更早应用程序版本，请选择“**为以前的应用程序版本(12.7 及更低版本)启用密码加密兼容性**”复选框。

   从 Kaspersky Endpoint Security 12.8 for Windows 开始，应用程序使用更强的密码加密。如果您部署了 Kaspersky Endpoint Security 12.8 或更高版本，我们建议清除此复选框并使用更强的密码加密。应用程序的早期版本不支持强密码加密。要运行该任务，您必须选中该复选框。

步骤 3. 选择要运行任务的账户

选择“**默认账户**”。默认下，Kaspersky Endpoint Security 以系统用户账户 (SYSTEM) 启动任务。

步骤 4. 配置任务启动计划

在“**计划开始**”下，选择“**手动**”。

步骤 5. 定义任务名称

输入任务的名称，例如“*主服务器连接密码*”。

步骤 6. 完成任务创建

退出向导。选中“**向导完成时运行任务**”复选框或手动运行任务。您可以在任务属性中监控任务进度。

如何在 Web Console 和云控制台中为服务器连接保护设置密码

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
2. 单击“**添加**”。
   “任务向导”将启动。
3. 配置任务设置：
   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Endpoint Security for Windows 14.2.0**”。
   b. 在“**任务类型**”下拉列表中，选择“**管理服务器连接保护**”。
   c. 在“**任务名称**”字段中，输入简要说明，例如，“*主服务器连接密码*”。
   d. 在“**要对其分配任务的设备**”块，选择任务范围。
4. 按照所选任务范围选项选择设备。转到下一步。
5. 选择默认用户账户。默认下，Kaspersky Endpoint Security 以系统用户账户 (SYSTEM) 启动任务。
6. 退出向导。
   在任务列表中将显示一个新任务。
7. 单击 Kaspersky Endpoint Security 的“**管理服务器连接保护**”任务。
   任务属性窗口将打开。
8. 选择**应用程序设置**选项卡。
9. 在“**管理服务器连接保护**”下，选择“**使用密码保护**”。
10. 在“**与管理服务器的连接**”下拉列表中，选择“**新密码**”。
11. 在“**密码**”字段中，设置并确认连接到管理服务器的密码。
    如果您忘记了密码，您可以使用任务更改密码。
12. 如果您已部署 Kaspersky Endpoint Security 12.7 或更早应用程序版本，请选择“**为以前的应用程序版本(12.7 及更低版本)启用密码加密兼容性**”复选框。
    从 Kaspersky Endpoint Security 12.8 for Windows 开始，应用程序使用更强的密码加密。如果您部署了 Kaspersky Endpoint Security 12.8 或更高版本，我们建议清除此复选框并使用更强的密码加密。应用程序的早期版本不支持强密码加密。要运行该任务，您必须选中该复选框。
13. 保存更改。

14. 选中该任务旁边的复选框。

15. 单击“**开始**”。

您可以监控任务的状态，以及成功完成任务或完成任务时发生错误的设备数量。

将计算机重新连接到其他管理服务器

将计算机重新连接到其他管理服务器涉及以下步骤：

1. 在当前“[KSC1]”服务器的控制台中，运行网络代理的“*更改管理服务器*”任务。

   运行任务后，计算机将重新连接到新的“[KSC2]”服务器。

   计算机将显示在 [KSC1] 服务器控制台，带有“*严重*”状态。使用策略配置应用程序或在计算机上远程运行任务是不可能的。

2. 在新的“[KSC2]”服务器的控制台中，为 Kaspersky Endpoint Security 创建一个新的“*管理服务器连接保护*”任务。在任务属性中，输入上一台服务器的密码，然后为新服务器设置密码。

   如何在管理控制台 (MMC) 中设置用于重新连接到新服务器的新密码

   1. 在 Kaspersky Security Center 管理控制台树中，选择“**任务**”。

      任务列表打开。

   2. 单击“**新任务**”。

   “任务向导”将启动。按照向导的说明进行操作。

步骤 1. 选择任务类型

选择“**Kaspersky Endpoint Security for Windows (14.1)**”→ “**管理服务器连接保护**”。

步骤 2. 保护管理服务器连接

设置密码以保护与新管理服务器的连接：

1. 在“**管理服务器连接保护**”下，选择“**使用密码保护**”。

2. 在“**管理服务器**”下拉列表中，选择“**从另一台服务器重新连接**”。

3. 在“**当前密码**”字段中，输入为连接到先前使用的受信任服务器而设置的密码。

4. 在“**新密码**”字段中，设置连接到新管理服务器的密码并确认密码。

   如果您忘记了密码，您可以使用任务更改密码。

5. 如果您已部署 Kaspersky Endpoint Security 12.7 或更早应用程序版本，请选择“**为以前的应用程序版本(12.7 及更低版本)启用密码加密兼容性**”复选框。

   从 Kaspersky Endpoint Security 12.8 for Windows 开始，应用程序使用更强的密码加密。如果您部署了 Kaspersky Endpoint Security 12.8 或更高版本，我们建议清除此复选框并使用更强的密码加密。应用程序的早期版本不支持强密码加密。要运行该任务，您必须选中该复选框。

步骤 3. 选择要运行任务的账户

选择“**默认账户**”。默认下，Kaspersky Endpoint Security 以系统用户账户 (SYSTEM) 启动任务。

步骤 4. 配置任务启动计划

在“**计划开始**”下，选择“**手动**”。

步骤 5. 定义任务名称

输入任务的名称，例如“*主服务器连接密码*”。

步骤 6. 完成任务创建

退出向导。选中“**向导完成时运行任务**”复选框或手动运行任务。您可以在任务属性中监控任务进度。

如何在 Web Console 和云控制台中设置用于重新连接到新服务器的新密码

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。

2. 单击“**添加**”。
   “任务向导”将启动。

3. 配置任务设置：

   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Endpoint Security for Windows 14.2.0**”。

   b. 在“**任务类型**”下拉列表中，选择“**管理服务器连接保护**”。

   c. 在“**任务名称**”字段中，输入简要说明，例如，“*主服务器连接密码*”。

   d. 在“**要对其分配任务的设备**”块，选择任务范围。

4. 按照所选任务范围选项选择设备。转到下一步。

5. 选择默认用户账户。默认下，Kaspersky Endpoint Security 以系统用户账户 (SYSTEM) 启动任务。

6. 退出向导。

   在任务列表中将显示一个新任务。

7. 单击 Kaspersky Endpoint Security 的“**管理服务器连接保护**”任务。

   任务属性窗口将打开。

8. 选择**应用程序设置**选项卡。

9. 在“**管理服务器连接保护**”下，选择“**使用密码保护**”。

10. 在“**与管理服务器的连接**”下拉列表中，选择“**从另一台服务器重新连接**”。

11. 在“**当前密码**”字段中，输入为连接到先前使用的受信任服务器而设置的密码。

12. 在“**新密码**”字段中，设置连接到新管理服务器的密码并确认密码。

    如果您忘记了密码，您可以使用任务更改密码。

13. 如果您已部署 Kaspersky Endpoint Security 12.7 或更早应用程序版本，请选择“**为以前的应用程序版本(12.7 及更低版本)启用密码加密兼容性**”复选框。

    从 Kaspersky Endpoint Security 12.8 for Windows 开始，应用程序使用更强的密码加密。如果您部署了 Kaspersky Endpoint Security 12.8 或更高版本，我们建议清除此复选框并使用更强的密码加密。应用程序的早期版本不支持强密码加密。要运行该任务，您必须选中该复选框。

14. 保存更改。

15. 选中该任务旁边的复选框。

16. 单击“**开始**”。

    您可以监控任务的状态，以及成功完成任务或完成任务时发生错误的设备数量。

完成任务后，确保在新的“`[KSC2]`”服务器的控制台中，计算机处于“*确定*”状态。测试您是否可以远程运行任务并使用策略配置应用程序。

重置管理服务器连接密码

如果您忘记了管理服务器连接密码或密码被泄露，您可以在任务属性中重置密码。您还可以为一组具有不同管理服务器连接保护状态的计算机重置密码并设置新密码。也就是说，如果某些计算机启用了保护，而某些计算机禁用了保护，则任务会为所有计算机设置密码。

> 您只能在计算机连接到的受信任服务器的控制台中重置管理服务器连接密码。

如何使用管理控制台(MMC)重置管理服务器连接密码

1. 打开 Kaspersky Security Center Administration Console。

2. 在控制台树中，选择“**任务**”。

3. 选择“**管理服务器连接保护**”任务并双击以打开任务属性。

4. 在任务属性窗口中，选择“**设置**”区域。

5. 在“**管理服务器连接保护**”下，选择“**保护并更改密码**”。

6. 在“**管理服务器连接密码**”字段中，设置用于连接到当前受信任服务器的新密码，然后确认密码。

7. 保存更改。

8. 运行任务。

如何在 Web Console 和云控制台中重置管理服务器连接密码

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。

2. 单击 Kaspersky Endpoint Security 的“**管理服务器连接保护**”任务。
   任务属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 在“**管理服务器连接保护**”下，选择“**保护并更改密码**”。

5. 在“**密码**”字段中，设置用于连接到当前受信任服务器的新密码，然后确认密码。

6. 保存更改。

7. 选中该任务旁边的复选框。

8. 单击“**开始**”。

因此，管理服务器连接密码将在任务完成后重置。

禁用管理服务器连接保护

> 您只能在计算机连接到的受信任服务器的控制台中远程禁用管理服务器连接保护。您还可以使用命令行在本地禁用保护。

如何在管理控制台 (MMC) 中禁用服务器连接保护

1. 打开 Kaspersky Security Center Administration Console。

2. 在控制台树中，选择“**任务**”。

3. 选择“**管理服务器连接保护**”任务并双击以打开任务属性。

4. 在任务属性窗口中，选择“**设置**”区域。

5. 在“**管理服务器连接保护**”下，选择“**不保护**”。

6. 保存更改。

7. 运行任务。
   您可以监控任务的状态，以及成功完成任务或完成任务时发生错误的设备数量。

如何在 Web Console 和云控制台中禁用服务器连接保护

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
2. 单击 Kaspersky Endpoint Security 的“**管理服务器连接保护**”任务。
   任务属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 在“**管理服务器连接保护**”下，选择“**不保护**”。
5. 保存更改。
6. 选中该任务旁边的复选框。
7. 单击“**开始**”。
   您可以监控任务的状态，以及成功完成任务或完成任务时发生错误的设备数量。

如何使用命令行禁用服务器连接保护

1. 以管理员身份运行命令行解释器 (cmd.exe)。
2. 转到 Kaspersky Endpoint Security 可执行文件所在文件夹。
3. 运行以下命令：

   ```
   avp.com SERVERBINDINGDISABLE [/password=<password>]
   ```

   其中`<password>`是 KL Admin 用户账户的密码或“*管理服务器连接保护*”任务的密码。如果未指定参数，Kaspersky Endpoint Security 会在下一行提示您输入密码。

   > 要执行此命令，必须启用密码保护。

示例

```
avp.com SERVERBINDINGDISABLE /password=samplePassword
```

数据加密

Kaspersky Endpoint Security 允许您加密存储在本地和可移动驱动器上的文件和文件夹，或者整个可移动驱动器和硬盘驱动器。笔记本电脑、可移动驱动器或硬盘丢失或被盗时，又或者在未经许可的用户或应用程序访问数据时，数据加密功能能够最小化信息泄露的危险。Kaspersky Endpoint Security 使用 Advanced Encryption Standard （AES）加密算法。

如果授权许可已过期，本程序不会加密新数据，旧的已加密数据仍保持加密状态并且可用。在此情况下，加密新数据将要求用允许使用加密的新授权许可来激活程序。

如果 Kaspersky Endpoint Security 安装在基于 Arm 的计算机上，则仅提供 BitLocker 驱动器加密。应用程序不支持其他数据加密组件。

如果授权许可已过期，或违反了最终用户授权许可协议，亦或授权许可密钥、Kaspersky Endpoint Security 或加密组件已删除，则先前加密文件的加密状态将得不到保证。这是因为某些应用程序，例如 Microsoft Office Word，会在编辑期间创建临时文件副本。原始文件保存后，临时文件副本将会替换原始文件，结果是，在没有或无法访问加密功能的计算机上，文件仍保持为不加密。

Kaspersky Endpoint Security 提供了以下方面的数据保护：

- **本地计算机驱动器上的文件级加密**。您可以根据扩展名或扩展名组编制文件列表，和存储在本地计算机驱动器上的文件夹列表，并为特定应用程序创建的文件创建加密规则。应用策略后，Kaspersky Endpoint Security 将加密和解密以下文件：
  - 单独添加到加密和解密列表中的文件；
  - 存储在添加到加密和解密列表中的文件夹内的文件；
  - 单独应用程序创建的文件。
- **可移动驱动器加密**。您可以指定默认加密规则，应用程序将根据该规则对所有可移动驱动器应用相同操作，您也可以为个别可移动驱动器指定加密规则。

  默认加密规则低于为个别可移动驱动器创建的加密规则的优先级。为拥有特定设备型号的可移动驱动器创建的加密规则的优先级低于为拥有特定设备 ID 的可移动驱动器创建的文件加密规则的优先级。

  若要为可移动驱动器上的文件选择加密规则，Kaspersky Endpoint Security 将会检查设备的型号和 ID 是否已知。然后该程序将执行以下操作之一：
  - 如果只有设备型号已知，程序将使用为特定设备型号的可移动驱动器创建的加密规则（如果已创建）。
  - 如果只有设备 ID 已知，程序将使用为特定设备 ID 的可移动驱动器创建的加密规则（如果已创建）。
  - 如果设备型号和 ID 已知，程序将使用为特定设备 ID 的可移动驱动器创建的加密规则（如果已创建）。如果不存在此类规则，但是存在为特定设备型号的可移动驱动器创建的加密规则，则应用程序将应用该规则。如果没有为特定的设备 ID 或特定的设备型号指定加密规则，应用程序将应用默认的加密规则。
  - 如果设备型号和设备 ID 都未知，程序将使用默认的加密规则。

  程序可以让您准备可移动驱动器以便携模式使用驱动器上存储的加密数据。启用便携模式后，您可以访问连接到没有加密功能的计算机上的可移动驱动器上的加密文件。

- **管理应用程序访问加密文件的规则**。对于任何应用程序，您可以创建加密文件访问规则，阻止对加密文件的访问或者允许仅使用加密文字（应用加密时获得的字符串）访问加密文件。

- **创建加密数据包**.您可以创建加密存档，使用密码保护对此类存档的访问。只有输入您保护该存档的密码才能访问加密存档中的内容。此类存档可以安全地通过网络或通过可移动驱动器传输。

- **完整磁盘加密**。您可以选择加密技术：卡巴斯基磁盘加密 或 BitLocker 驱动器加密（以下简称"BitLocker"）。

  BitLocker 技术是 Windows 操作系统的一部分。如果计算机配备了 Trusted Platform Module (TPM)，BitLocker 将用其存储提供加密硬盘驱动器访问的恢复密钥。计算机启动时，BitLocker 将从受信任平台模块请求硬盘驱动器恢复密钥并解锁驱动器。您可以配置访问恢复密钥使用密码和/或 PIN 码。

  您可以指定默认的完整磁盘加密规则，并创建要从加密中排除的硬盘驱动器的列表。应用 Kaspersky Security Center 策略后，Kaspersky Endpoint Security 将按照扇区执行完整磁盘加密。应用程序加密将同时应用至硬盘驱动器的所有逻辑分区上。

  加密系统硬盘驱动器后，在下次计算机启动时，用户能够访问硬盘驱动器并且操作系统加载前，用户必须通过身份验证代理的身份验证。这需要输入连接至计算机的令牌或智能卡的密码，或者本地局域网管理员使用"*管理身份验证代理账户*"任务创建的身份验证代理账户的用户名或密码。这些账户以用户登录操作系统的 Microsoft Windows 账户为基础。这些帐户以用户登录操作系统的 Microsoft Windows 帐户为基础。您还可以使用 Single Sign-On (SSO) 技术，该技术允许您使用身份验证代理账户的用户名和密码自动登录到操作系统。

  > 如果您备份计算机，然后对计算机数据进行加密，之后恢复计算机备份副本并再次加密计算机数据，Kaspersky Endpoint Security 将会创建相同的身份验证代理帐户。要删除重复帐户，您必须使用带有 `dupfix` 密钥的 klmover 实用程序。Klmover 实用程序包含在 Kaspersky Security Center 分发包中。您可以在《Kaspersky Security Center 帮助》中了解有关其操作的更多信息。

  只能在安装了带有完整磁盘加密功能的 Kaspersky Endpoint Security 的计算机上访问已加密的硬盘驱动器。当出现公司的本地局域网之外的连接尝试访问加密数据时，该功能能够最大限度地降低加密硬盘驱动器的数据泄露风险。

若要加密硬盘驱动器和可移动驱动器，您可以使用"仅加密使用的磁盘空间"功能。建议您仅为先前未使用的新设备使用该功能。如果您在已使用的设备上应用加密，建议您加密整个设备。这将确保所有数据受到保护 – 即使删除了可能仍包含可检索信息的数据。

开始加密之前，Kaspersky Endpoint Security 将获得文件系统扇区图。第一波加密包括开始加密时文件占用的扇区。第二波加密包括加密开始后写入的扇区。加密完成后，所有包含数据的扇区都将被加密。

加密完成并且用户删除文件后，存储删除文件的扇区可以在文件系统级别存储新的信息但是仍保持为加密状态。因此，在启用"**仅加密使用的磁盘空间**"功能的情况下，随着文件写入新设备和定期加密该设备，在一段时间后所有扇区都将加密。

解密文件所需的数据由加密时控制计算机的 Kaspersky Security Center 管理服务器提供。如果含有加密对象的计算机由于某种原因由其他管理服务器管理，则可以通过以下方式之一获取对加密数据的访问权限：

- 同一层次结构中的管理服务器：
  - 您无需执行任何其他操作。用户将保留对加密对象的访问权限。加密密钥将分发到所有管理服务器。
- 单独的管理服务器：
  - 向局域网管理员请求对加密对象的访问权限。
  - 使用"恢复实用工具"恢复加密设备上的数据。
  - 从备份副本恢复在加密时控制计算机的 Kaspersky Security Center 管理服务器的配置，并且在现在控制包含加密对象的计算机的管理服务器上使用此配置。

如果没有加密数据的访问权限，请遵循有关处理加密数据的特殊说明（还原对加密文件的访问权限、无法访问加密设备时的设备使用）。

加密功能限制

数据加密具有以下限制：

- 程序将在加密期间创建服务文件。需要硬盘上大约 0.5% 的非碎片磁盘空间来存储这些文件。如果硬盘驱动器上的可用非碎片磁盘空间不足，加密操作不会运行，直至您清理出足够的空间。
- 您可以在 Kaspersky Security Center 管理控制台和 Kaspersky Security Center Web Console 中管理所有数据加密组件。在 Kaspersky Security Center 云控制台，您仅可以管理 Bitlocker。
- 数据加密仅在将 Kaspersky Endpoint Security 与 Kaspersky Security Center 管理系统或 Kaspersky Security Center 云控制台一起使用时可用（仅 BitLocker）。在离线模式下使用 Kaspersky Endpoint Security 时，无法使用数据加密，因为 Kaspersky Endpoint Security 将加密密钥存储在 Kaspersky Security Center 中。
- 如果 Kaspersky Endpoint Security 安装在运行 Microsoft Windows for Servers 的计算机上，则只有使用 BitLocker 驱动器加密技术的完整磁盘加密可用。如果 Kaspersky Endpoint Security 安装在运行 Windows for Workstations 的计算机上，则数据加密功能完全可用。
- 如果 Kaspersky Endpoint Security 安装在基于 Arm 的计算机上，则仅支持使用 BitLocker 驱动器加密技术的完整磁盘加密，不支持其他加密组件。

对于不满足软硬件要求的硬盘驱动器，无法使用 卡巴斯基磁盘加密 技术进行完整磁盘加密。

Kaspersky Endpoint Security 的完整磁盘加密功能与用于 UEFI 的卡巴斯基反病毒软件之间不兼容。用于 UEFI 的卡巴斯基反病毒软件在操作系统加载前启动。使用完整磁盘加密时，应用程序将检测计算机上是否缺少已安装的操作系统。因此，用于 UEFI 的卡巴斯基反病毒软件的运行将以错误结束。文件级加密 (FLE) 不会影响用于 UEFI 的卡巴斯基反病毒软件的操作。

Kaspersky Endpoint Security 支持以下配置：

- HDD、SSD 和 USB 驱动器。

  Kaspersky Disk Encryption (FDE) 技术在保留 SSD 驱动器的性能和服务周期时支持对 SSD 的使用。

- 通过总线连接的设备：SCSI、ATA、IEEE1934、USB、RAID、SAS、SATA、NVME。
- 通过 SD 或 MMC 总线连接的固定驱动器。
- 具有512字节扇区的驱动器。
- 具有模拟512字节的4096字节扇区的驱动器。
- 具有以下类型分区的驱动器：GPT、MBR和VBR（可移动驱动器）。
- UEFI 64 和传统 BIOS 标准的嵌入式软件。
- 支持安全引导的 UEFI 标准嵌入式软件。

*安全引导*是一种旨在验证 UEFI 加载应用程序和驱动程序的数字签名的技术。安全引导阻止启动未签名或由未知发布者签名的 UEFI 应用程序和驱动程序。卡巴斯基磁盘加密（FDE）完全支持安全引导。身份验证代理由 Microsoft Windows UEFI 驱动程序发布者证书签名。

在某些设备（例如，Microsoft Surface Pro 和 Microsoft Surface Pro 2）上，默认情况下可能会安装过期的数字签名验证证书列表。在加密驱动器之前，您需要更新证书列表。

- 支持快速引导的 UEFI 标准嵌入式软件。

  *快速引导*是一种帮助计算机更快启动的技术。启用快速引导技术时，计算机通常只加载启动操作系统所需的最小 UEFI 驱动程序集。启用快速引导技术后，当身份验证代理运行时，USB 键盘、鼠标、USB 令牌、触摸板和触摸屏可能无法工作。

> 要使用卡巴斯基磁盘加密（FDE），建议禁用快速引导技术。您可以使用 FDE 测试工具 来测试卡巴斯基磁盘加密（FDE）的操作。

Kaspersky Endpoint Security 不支持以下配置：

- 引导加载程序位于某个驱动器上而操作系统位于其他驱动器上。
- 系统包含 UEFI 32 标准的嵌入式软件。
- 系统具有 Intel® 快速启动技术和拥有休眠分区的驱动器，即使 Intel® 快速启动技术被禁用。
- MBR 格式的驱动器拥有超过 10 个扩展分区。
- 系统具有位于非系统驱动器的交换文件。
- 同时安装有多个操作系统的多启动系统。
- 动态分区（仅支持主分区）。
- 未经过磁盘整理可用空间少于 0.5% 的驱动器。
- 扇区大小不是 512 字节或模拟 512 字节的 4096 字节的驱动器。
- 混合驱动器。
- 系统具有第三方加载程序。
- 带有压缩 NTFS 目录的驱动器。
- 卡巴斯基磁盘加密（FDE）技术与其他完整磁盘加密技术（如 BitLocker、McAfee Drive Encryption 和 WinMagic SecureDoc）不兼容。
- 卡巴斯基磁盘加密（FDE）技术与快速缓存技术不兼容。
- 不支持在加密驱动器上创建、删除和修改分区。你可能会丢失数据。
- 不支持文件系统格式。你可能会丢失数据。

  如果需要格式化使用卡巴斯基磁盘加密（FDE）技术加密的驱动器，请在未安装 Kaspersky Endpoint Security for Windows 的计算机上格式化驱动器，并仅使用完整磁盘加密。

  使用快速格式化选项格式化的加密驱动器下次连接到安装了 Kaspersky Endpoint Security for Windows 的计算机时，可能会被错误地标识为加密驱动器。用户数据将不可用。

- 身份验证代理支持不超过 100 个帐户。
- 单点登录技术与第三方开发人员的其他技术不兼容。
- 以下型号的设备不支持卡巴斯基磁盘加密（FDE）技术：
  - Dell Latitude E6410（UEFI模式）
  - HP Compaq nc8430（传统 BIOS 模式）
  - Lenovo ThinkCentre 8811（传统 BIOS 模式）
- 启用旧版 USB 支持时，身份验证代理不支持使用 USB 令牌。计算机上只能进行基于密码的身份验证。
- 在旧版 BIOS 模式下加密驱动器时，建议您在以下型号的设备上启用旧版 USB 支持：
  - Acer Aspire 5560G
  - Acer Aspire 6930
  - Acer TravelMate 8572T
  - Dell Inspiron 1420
  - Dell Inspiron 1545
  - Dell Inspiron 1750
  - Dell Inspiron N4110
  - Dell Latitude E4300
  - Dell Studio 1537
  - Dell Studio 1569
  - Dell Vostro 1310
  - Dell Vostro 1320
  - Dell Vostro 1510
  - Dell Vostro 1720
  - Dell Vostro V13
  - Dell XPS L502x
  - Fujitsu Celsius W370
  - Fujitsu LifeBook A555
  - HP Compaq dx2450 Microtower PC
  - Lenovo G550

- Lenovo ThinkPad L530
- Lenovo ThinkPad T510
- Lenovo ThinkPad W540
- Lenovo ThinkPad X121e
- Lenovo ThinkPad X200s (74665YG)
- Samsung R530
- Toshiba Satellite A350
- Toshiba Satellite U400 10O
- MSI 760GM-E51 (motherboard)

更改加密密钥的长度 (AES56 / AES256)

Kaspersky Endpoint Security 使用高级加密标准 (AES) 加密算法。Kaspersky Endpoint Security 支持有效密钥长度为 256 或 56 位的 AES 加密算法。数据加密算法取决于分发包中包含的 AES 加密库：*强加密 (AES256)* 或 *简单加密 (AES56)*。AES 加密库与应用程序一起安装。

只有 Kaspersky Endpoint Security 11.2.0 或更高版本可以更改加密密钥的长度。

更改加密密钥长度包括以下步骤：

1. 开始更改加密密钥长度之前，解密 Kaspersky Endpoint Security 加密的对象：
   a. 解密硬盘驱动器。
   b. 解密本地驱动器上的文件。
   c. 解密可移动驱动器。

   更改加密密钥长度后，先前加密的对象变为不可用。

2. 删除 Kaspersky Endpoint Security。
3. 从包含其他加密库的 Kaspersky Endpoint Security 分发包安装 Kaspersky Endpoint Security。

您也可以通过升级应用程序来更改加密密钥长度。只有满足以下条件，才可以通过应用程序升级来更改密钥长度：

- 计算机上已安装 Kaspersky Endpoint Security 版本 10 Service Pack 2 或更高版本。
- 计算机上未安装数据加密组件（文件级加密、完整磁盘加密）。

  默认情况下，Kaspersky Endpoint Security 不包含数据加密组件。BitLocker 管理组件不会影响加密密钥长度的更改。

要更改加密密钥长度，请运行包含必要加密库的分发包中的 kes_win.msi 或 setup_kes.exe 文件。您还可以使用安装包远程升级应用程序。

无法使用与计算机上安装的应用程序版本相同的分发包更改加密密钥的长度，除非先卸载应用程序。

卡巴斯基磁盘加密

卡巴斯基磁盘加密不支持基于 Arm 的计算机。

卡巴斯基磁盘加密仅适用于运行面向工作站的 Windows 操作系统的计算机。对于运行面向服务器的 Windows 操作系统的计算机，请使用 BitLocker 驱动器加密技术。

Kaspersky Endpoint Security 支持 FAT32、NTFS 和 exFat 文件系统的完整磁盘加密。

开始完整磁盘加密之前，应用程序会执行一系列检查，确定是否能对该设备进行加密，其中包括检查系统硬盘驱动器与身份验证代理或 BitLocker 加密组件的兼容性。若要检查兼容性，计算机必须重启。计算机重新启动后，应用程序会自动执行所有必要的检查。如果兼容性检查成功，则在加载操作系统和启动应用程序后开始完整磁盘加密。如果发现系统硬盘驱动器与身份验证代理或 BitLocker 加密组件不兼容，需要按重启硬件按钮重新启动计算机。Kaspersky Endpoint Security 将记录不兼容的信息。根据此信息，应用程序在操作系统启动时不会启动完整磁盘加密。此事件信息将被记录在 Kaspersky Security Center 报告中。

如果更改了计算机硬件配置，应删除先前检查中所记录的应用程序不兼容信息，以便重新检查系统硬盘驱动器与身份验证代理和 BitLocker 加密组件的兼容性。要执行此操作，请在完整磁盘加密前，在命令行中键入 `avp pbatestreset`。如果操作系统未能在检查系统硬盘驱动器是否与身份验证代理兼容之后加载，您必须在身份验证代理测试运行之后使用恢复实用工具删除剩余对象和数据，然后启动 Kaspersky Endpoint Security 并再次执行 `avp pbatestreset` 命令。

启动完整磁盘加密后，Kaspersky Endpoint Security 将加密硬盘上写入的所有的数据。

如果用户在完整磁盘加密期间关闭了或重新启动了计算机，下次启动操作系统之前系统将载入身份验证代理。成功通过身份验证代理并在操作系统启动后，Kaspersky Endpoint Security 将恢复完整磁盘加密。

如果操作系统在完整磁盘加密期间切换至休眠模式，操作系统退出休眠模式时将加载身份验证代理。成功通过身份验证代理并在操作系统启动后，Kaspersky Endpoint Security 将恢复完整磁盘加密。

如果操作系统在完整磁盘加密期间进入睡眠模式，则当操作系统退出睡眠模式时，Kaspersky Endpoint Security 将恢复完整磁盘加密，而不会加载身份验证代理。

可以通过两种方式在身份验证代理中执行用户身份验证：

- 输入局域网管理员使用 Kaspersky Security Center 工具创建的身份验证代理帐户的用户名和密码。
- 输入连接至计算机的令牌的密码或智能卡的密码。

仅当计算机硬盘驱动器使用 AES256 加密算法进行加密时，才可以使用令牌或智能卡。如果使用 AES56 算法加密了计算机硬盘驱动器，添加电子证书文件到命令将被拒绝。

身份验证代理支持以下语言的键盘布局：

- 英语（英国）
- 英语（美国）
- 阿拉伯语（阿尔及利亚、摩洛哥、突尼斯、AZERTY 布局）
- 西班牙语（拉丁美洲）
- 意大利语
- 德语（德国和奥地利）
- 德语（瑞士）
- 葡萄牙语（巴西、ABNT2 布局）
- 俄语（针对带有 QWERTY 布局的 105 键 IBM / Windows 键盘）
- 土耳其语（QWERTY 布局）
- 法语（法国）
- 法语（瑞士）
- 法语（比利时 AZERTY 布局）
- 日语（针对带有 QWERTY 布局的 106 键键盘）

> 如果操作系统的语言和区域标准设置中添加了该布局，则在身份验证代理中可以使用该键盘布局。

如果身份验证代理账户名包含身份验证代理中无法使用键盘布局输入的符号，则只能使用恢复实用工具恢复后或恢复身份验证代理账户名和密码恢复后访问加密的硬盘驱动器。

SSD 驱动器加密的特殊功能

应用程序支持对 SSD 驱动器、混合 SSHD 驱动器和具有 Intel 智能响应功能的驱动器进行加密。应用程序不支持使用“英特尔快速入门”功能加密驱动器。在加密此类驱动器之前，请禁用“英特尔快速启动”功能。

SSD 驱动器加密具有以下特殊功能：

- 如果 SSD 驱动器是新的并且不包含机密数据，则只对占用的空间启用加密。这样可以覆盖相关的驱动器扇区。
- 如果正在使用 SSD 驱动器，并且它有机密数据，请选择以下选项之一：
  - 完全擦除 SSD 驱动器（安全擦除），安装操作系统并在启用仅加密占用空间选项的情况下运行 SSD 驱动器加密。
  - 运行 SSD 驱动器的加密，并禁用仅加密已占用空间的选项。

加密 SSD 驱动器需要 5-10 GB 的可用空间。下表提供了存储加密管理数据的可用空间要求。

存储加密管理数据的可用空间要求

SSD 驱动器大小（GB）	SSD 驱动器主分区上的可用空间（MB）	SSD 驱动器辅助分区上的可用空间（MB）
128	250	64
256	250	640
512	300	128

启动卡巴斯基磁盘加密

在开始完整磁盘加密之前，建议您确保计算机未受到感染。若要执行操作，应启动全盘扫描或关键区域扫描任务。在已被 rootkit 感染的计算机上执行完整磁盘加密可能导致计算机无法运行。

在您启动磁盘加密之前，您必须检查身份验证代理账户的设置。使用采用卡巴斯基磁盘加密 (FDE) 技术保护的驱动器时，需要身份验证代理。加载操作系统之前，用户需要使用代理完成身份验证。Kaspersky Endpoint Security 允许您在加密驱动器之前自动创建身份验证代理账户。您可以在“完整磁盘加密”策略设置中启用自动创建身份验证代理账户（参加以下说明）。您还可以使用单点登录 (SSO) 技术。

Kaspersky Endpoint Security 允许您为以下用户组自动创建身份验证代理账户：

- “**计算机上的所有账户**”。计算机上曾经处于活动状态的所有账户。
- “**计算机上的所有域账户**”。计算机上属于某个域且曾经处于活动状态的所有账户。
- “**计算机上的所有本地账户**”。计算机上曾经处于活动状态的所有本地账户。
- “**使用一次性密码的服务账户**”。服务账户是访问计算机所必需的，例如，当用户忘记密码时。您还可以将服务账户用作备用账户。您必须输入账户名称（默认是 `ServiceAccount`）。Kaspersky Endpoint Security 自动创建密码。您可以在 Kaspersky Security Center 控制台查找密码。
- “**本地管理员**”。Kaspersky Endpoint Security 为计算机的本地管理员创建身份验证代理用户账户。
- “**计算机管理者**”。Kaspersky Endpoint Security 为计算机的管理者账户创建身份验证代理用户账户。您可以在 Active Directory 的计算机属性中查看哪些账户具有计算机管理者角色。默认情况下，计算机管理者角色未定义，即不对应于任何账户。
- “**活动账户**”。Kaspersky Endpoint Security 为在磁盘加密过程中活动的账户自动创建身份验证代理账户。

“*管理身份验证代理账户*”任务设计用于配置用户身份验证设置。您可以使用此任务添加新账户，修改当前账户的设置，或者在必要时删除账户。对于单台计算机可以使用本地任务，对于单独管理组中的计算机或一组选定计算机，可以使用组任务。

如何通过管理控制台 (MMC) 运行卡巴斯基磁盘加密

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **数据加密** → **完整磁盘加密**。

4. 在“**加密技术**”下拉列表中，选择“**卡巴斯基磁盘加密**”。

> 如果计算机的硬盘驱动器先前使用 BitLocker 加密，则无法使用 卡巴斯基磁盘加密。

5. 在“**加密模式**”下拉列表中，选择“**加密所有硬盘驱动器**”。

> 如果计算机安装了多个操作系统，则在加密所有硬盘后，您将只能加载安装了该应用程序的操作系统。

> 如果您需要从加密中排除某些硬盘驱动器，则创建此类硬盘驱动器的列表。

6. 配置高级卡巴斯基磁盘加密选项（参见下表）。
7. 保存更改。

如何通过 Web Console 和云控制台运行卡巴斯基磁盘加密

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **数据加密** → **完整磁盘加密**。
5. 选择“**卡巴斯基磁盘加密**”技术。

> 如果计算机的硬盘驱动器先前使用 BitLocker 加密，则无法使用 卡巴斯基磁盘加密。

6. 在“**设备上的操作**”块中，选择“**加密所有硬盘驱动器**”。

> 如果计算机安装了多个操作系统，在加密后，您将能够只加载执行了加密的操作系统。

> 如果您需要从加密中排除某些硬盘驱动器，则创建此类硬盘驱动器的列表。

7. 配置高级卡巴斯基磁盘加密选项（参见下表）。
8. 保存更改。

您可以使用加密监控器工具控制用户计算机上的磁盘加密或解密过程。您可以从主应用程序窗口运行加密监控器工具。

加密监控

如果系统硬盘驱动器被加密，则身份验证代理在操作系统启动之前加载。使用身份验证代理完成身份验证以便访问加密的系统硬盘驱动器并加载操作系统。在成功完成身份验证过程后，操作系统将加载。身份验证过程将在每次操作系统重新启动时重新开始。

卡巴斯基磁盘加密组件设置

参数	描述
为以下用户自动创建身份验证代理账户用户加密过程中	如果该复选框被选中，应用程序基于计算机上的 Windows 用户账户创建身份验证代理账户。默认情况下，Kaspersky Endpoint Security 使用在过去 30 天内登录到操作系统的用户所使用的所有本地账户和域账户。
登录时为该计算机的所有用户自动创建身份验证代理账户	如果该复选框被选中，应用程序在启动身份验证代理之前检查计算机上的 Windows 用户账户信息。如果 Kaspersky Endpoint Security 检测到有 Windows 用户账户没有身份验证代理账户，应用程序将创建新账户以访问加密驱动器。新身份验证代理账户将具有以下默认设置：仅密码保护的登录、第一次身份验证时的密码更改。因此，您不需要使用“*管理身份验证代理账户*”任务对存在已加密驱动器的计算机手动添加身份验证代理账户。
保存在身份验证代理中输入的用户名	如果选中该复选框，应用程序将保存身份验证代理账户的名称。下次使用同一账户在身份验证代理中尝试完成认证时不会被提示输入账户名。

参数	描述
仅加密使用的磁盘空间(减少加密时间)	该复选框可启用/禁用将加密区域仅限为已用硬盘驱动器扇区的选项。该限制可减少加密时间。 加密开始后启用或禁用**仅加密使用的磁盘空间(减少加密时间)**功能在硬盘驱动器被加密之前并不修改该设置。开始加密之前您必须选择或清除该复选框。 如果选定该复选框，则仅加密使用的硬盘驱动器部分。Kaspersky Endpoint Security 将自动加密添加的新数据。 如果清空该复选框，整个硬盘驱动器将被加密，包括先前删除和修改文件残留的碎片。 推荐对尚未修改或删除数据的新硬盘驱动器使用该选项。如果对已在使用中的硬盘驱动器应用加密，则推荐加密整个硬盘驱动器。这样可确保保护所有数据，甚至已删除的数据也能够部分恢复。 默认下，复选框被清除。
使用 Legacy USB Support (不推荐)	此复选框启用或禁用"Legacy USB Support"功能。*Legacy USB Support* **是**一种 BIOS/UEFI 功能，允许您在启动操作系统（BIOS 模式）之前，在计算机的引导阶段使用 USB 设备（例如安全令牌）。"Legacy USB Support"不会影响操作系统启动后对 USB 设备的支持。 如果选中该复选框，在计算机初始启动期间对 USB 设备的支持将启用。 启用"Legacy USB Support"功能时，BIOS 模式下的身份验证代理不支持通过 USB 使用令牌。推荐仅当存在硬件兼容性问题时并仅对发生问题的计算机使用此选项。

创建硬盘驱动器加密排除列表

您可以仅为 卡巴斯基磁盘加密 技术创建加密排除项列表。

若要创建从加密范围中排除的硬盘驱动器列表，请执行以下操作：

1. 在 Kaspersky Security Center 管理控制台树中，选择"**策略**"。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **数据加密** → **完整磁盘加密**。
4. 在"**加密技术**"下拉列表中，选择"**卡巴斯基磁盘加密**"。
   从加密项目中排除的硬盘驱动器所对应的条目将显示在"**请勿加密以下硬盘驱动器**"表中。如果您先前并未创建硬盘驱动器加密排除列表，该表将是空表。
5. 若要向从加密范围中排除的硬盘驱动器列表中添加硬盘驱动器，请执行以下操作：
   a. 单击"**添加**"。
   b. 在打开的窗口中，指定"**设备名称**"、"**计算机**"、"**磁盘类型**"、"**卡巴斯基磁盘加密**"的值。
   c. 单击"**刷新**"。
   d. 在"**名称**"列中，在表行中选择与您要添加到硬盘驱动器加密排除列表中的硬盘驱动器对应的复选框。
   e. 单击"**确定**"。

对应于选定硬盘驱动器的条目将显示在“**请勿加密以下硬盘驱动器**”表中。

6. 保存更改。

导出或导入从加密范围中排除的硬盘驱动器列表

您可以将硬盘驱动器加密排除项列表导出到 XML 文件。然后可以修改文件，例如，添加大量相同类型的排除项。还可以使用导出/导入功能备份排除列表或将排除项迁移到其他服务器。

如何在管理控制台(MMC)中导出和导入硬盘驱动器加密排除项列表

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **数据加密** → **完整磁盘加密**。
4. 在“**加密技术**”下拉列表中，选择“**卡巴斯基磁盘加密**”。
   从加密项目中排除的硬盘驱动器所对应的条目将显示在“**请勿加密以下硬盘驱动器**”表中。
5. 要导出排除项列表：
   a. 选择您要导出的排除项。要选择多个端口，使用 **CTRL** 或 **SHIFT** 键。
      如果您未选择任何排除项，Kaspersky Endpoint Security 将导出所有排除项。
   b. 单击“ → **导出**”按钮。
   c. 在打开的窗口中，指定您要将排除项列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。
   d. 保存文件。
      Kaspersky Endpoint Security 会将整个排除项列表导出到 XML 文件。
6. 要导入规则列表：
   a. 单击“ → **导入**”按钮。
   b. 在打开的窗口中，选择要从中导入排除项列表的 XML 文件。
   c. 打开文件。
      如果计算机已经具有排除项的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 XML 文件向其中添加新条目。
7. 保存更改。

如何在 Web Console 中导出和导入硬盘驱动器加密排除项列表

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。

4. 选择 **数据加密** → **完整磁盘加密**。
   选择“**卡巴斯基磁盘加密**”技术。

5. 单击**排除项**链接。
   排除项列表打开。

6. 要导出规则列表：

   a. 选择您要导出的排除项。

   b. 单击“ → **导出**”按钮。
      Kaspersky Endpoint Security 导出排除项列表到默认下载文件夹中的 JSON 文件。

7. 要导入排除项列表：

   a. 单击“ → **导入**”按钮。
      在打开的窗口中，选择要从中导入排除项列表的 JSON 文件。

   b. 打开文件。
      如果计算机已经具有排除项的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 JSON 文件向其中添加新条目。

8. 保存更改。

启用单点登录 (SSO) 技术

Single Sign-On (SSO) 技术允许您使用身份验证代理的凭据自动登录到操作系统。这意味着用户在登录 Windows 时只需输入一次密码（身份验证代理账户密码）。单点登录技术还允许您在更改 Windows 账户密码时自动更新身份验证代理账户的密码。

使用单点登录技术时，身份验证代理将忽略 Kaspersky Security Center 中指定的密码强度要求。您可以在操作系统设置中设置密码强度要求。

启用单点登录技术

如何在管理控制台 (MMC) 中启用单点登录技术

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **数据加密** → **通用加密设置**。

4. 在“**密码设置**”块中单击“**设置**”按钮。

5. 在打开的窗口中的“**身份验证代理**”选项卡上，选中“**使用单点登录 (SSO) 技术**”复选框。

6. 如果您正使用第三方凭证提供程序，请选择“**包装第三方凭证提供者**”复选框。

7. 保存更改。

结果，用户只需与代理完成一次身份验证过程。加载操作系统不需要身份验证过程。操作系统会自动加载。

如何在 Web Console 中启用单点登录

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **数据加密** → **完整磁盘加密**。

5. 选择“**卡巴斯基磁盘加密**”技术。

6. 在“**密码设置**”块中，选中“**使用单点登录 (SSO) 技术**”复选框。

7. 如果您正使用第三方凭证提供程序，请选择“**包装第三方凭证提供者**”复选框。

8. 保存更改。

结果，用户只需与代理完成一次身份验证过程。加载操作系统不需要身份验证过程。操作系统会自动加载。

为使单点登录起作用，Windows 账户密码和身份验证代理账户的密码必须匹配。如果密码不匹配，用户需要执行两次身份验证过程：在身份验证代理的界面中以及在加载操作系统之前。这些操作只需执行一次即可同步密码。之后，Kaspersky Endpoint Security 会使用 Windows 账户的密码替换身份验证代理账户的密码。更改 Windows 账户密码时，应用程序将自动更新身份验证代理账户的密码。

第三方凭证提供程序

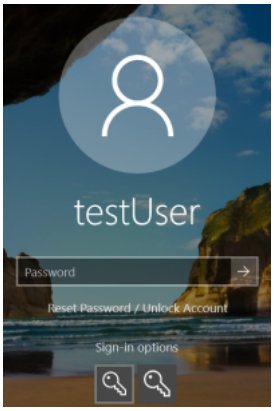
Kaspersky Endpoint Security 支持第三方凭证提供程序 ADSelfService Plus。

使用第三方凭证提供程序时，身份验证代理会在加载操作系统之前拦截密码。这意味着用户在登录 Windows 时只需输入一次密码。例如，在登录到 Windows 之后，用户可以利用第三方凭证提供程序的功能在公司服务中进行身份验证。第三方凭证提供程序还允许用户独立重置自己的密码。在这种情况下，Kaspersky Endpoint Security 将自动更新身份验证代理的密码。

如果您使用的是应用程序不支持的第三方凭证提供程序，则在单点登录技术操作中可能会遇到一些限制。登录 Windows 时，用户将可以使用两个配置文件：系统内凭证提供程序和第三方凭证提供程序。这些配置文件的图标将是相同的（参见下图）。用户将有以下继续选项：

- 如果用户选择*第三方凭证提供程序*，身份验证代理将无法将密码与 Windows 账户同步。因此，如果用户更改了 Windows 账户密码，Kaspersky Endpoint Security 将无法更新身份验证代理账户的密码。因此，用户需要执行两次身份验证过程：在身份验证代理的界面中以及在加载操作系统之前。此种情况下，用户可以利用第三方凭证提供程序的功能在公司服务中进行身份验证。

- 如果用户选择*系统内凭证提供程序*，身份验证代理会将密码与 Windows 账户同步。此种情况下，用户无法利用第三方凭证提供程序的功能在公司服务中进行身份验证。



Windows 登录的系统身份验证配置文件和第三方身份验证配置文件

管理身份验证代理帐户

使用采用卡巴斯基磁盘加密 (FDE) 技术保护的驱动器时，需要身份验证代理。加载操作系统之前，用户需要使用代理完成身份验证。“*管理身份验证代理账户*”任务设计用于配置用户身份验证设置。对于单台计算机可以使用本地任务，对于单独管理组中的计算机或一组选定计算机，可以使用组任务。

> 您无法配置用于启动“*管理身份验证代理账户*”任务的计划。也不能强行停止任务。

如何在管理控制台 (MMC) 中创建“管理身份验证代理账户”任务

1. 在 Kaspersky Security Center 管理控制台树中，选择“**任务**”。
   任务列表打开。

2. 单击“**新任务**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 选择任务类型

选择“**Kaspersky Endpoint Security for Windows (14.1)**”→ “**管理身份验证代理账户**”。

步骤 2. 选择身份验证代理账户管理命令

生成身份验证代理账户管理命令列表。管理命令允许您添加、修改和删除身份验证代理账户（请参见以下说明）。只有拥有身份验证代理账户的用户可以完成身份验证过程、加载操作系统和获得对加密驱动器的访问权限。

步骤 3. 选择任务将分配到的设备

选择将要执行任务的计算机。下列选项可用：

- 将任务分配给管理组。在这种情况下，任务分配给先前创建的管理组中包括的计算机。
- 选择管理服务器在网络中检测到的计算机：*未分配设备*。特定设备可包括管理组中的设备以及未分配设备。
- 手动指定设备地址或从列表中导入地址。您可以指定您要将任务分配给的设备的 NetBIOS 名称、IP 地址和 IP 子网。

步骤 4. 定义任务名称

输入任务的名称，例如“*管理员账户*”。

步骤 5. 完成任务创建

退出向导。如有必要，选中“**向导完成时运行任务**”复选框。您可以在任务属性中监控任务进度。

结果，在下次计算机启动时，当任务完成后，新用户可以完成身份验证过程、加载操作系统和获得对加密驱动器的访问权限。

如何在 Web Console 中创建“管理身份验证代理账户”任务

1. 在 Web Console 的主窗口中，选择“**任务**”。

   任务列表打开。

2. 单击“**添加**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 配置常规任务设置

配置常规任务设置：

1. 在“**应用程序**”下拉列表中，选择“**Kaspersky Endpoint Security for Windows (14.1)**”。
2. 在“**任务类型**”下拉列表中，选择“**管理身份验证代理账户**”。
3. 在“**任务名称**”字段中，输入简要说明，例如“*管理员账户*”。
4. 在“**要对其分配任务的设备**”块，选择任务范围。

步骤 2. 管理身份验证代理账户

生成身份验证代理账户管理命令列表。管理命令允许您添加、修改和删除身份验证代理账户（请参见以下说明）。只有拥有身份验证代理账户的用户可以完成身份验证过程、加载操作系统和获得对加密驱动器的访问权限。

步骤 3. 完成任务创建

退出向导。在任务列表中将显示一个新任务。

要运行任务，请选中与任务对应的复选框，然后单击“**开始**”按钮。

结果，在下次计算机启动时，当任务完成后，新用户可以完成身份验证过程、加载操作系统和获得对加密驱动器的访问权限。

要添加身份验证代理账户，您需要向“*管理身份验证代理账户*”任务添加特殊命令。使用组任务很方便，例如，将管理员账户添加到所有计算机。

Kaspersky Endpoint Security 允许您在加密驱动器之前自动创建身份验证代理账户。您可以在“完整磁盘加密”策略设置中启用自动创建身份验证代理账户。您还可以使用单点登录 (SSO) 技术。

如何通过管理控制台 (MMC) 添加身份验证代理账户

1. 打开“*管理身份验证代理账户*”任务的属性。
2. 在任务属性中，选择“**设置**”区域。
3. 单击**添加** → **账户添加命令**。
4. 在打开的窗口的“**Windows 账户**”字段中，指定将用于创建身份验证代理账户的 Microsoft Windows 账户的名称。
5. 如果您手动输入了 Windows 账户名称，请单击“**允许**”按钮以定义账户安全标识符 (SID)。

   如果您单击“**允许**”按钮时选择不决定安全标识符 SID，SID 将在任务在计算机上执行时确定。

定义 Windows 账户安全标识符对于验证 Windows 账户名称是否正确输入是必需的。如果计算机或受信任域中不存在 Windows 账户，则“*管理身份验证代理账户*”任务将以出错结束。

6. 如果您希望将先前为身份验证代理创建的现有账户替换为正在创建的帐户，请选择“**替换现有账户**”复选框。

当您在管理身份验证代理帐户的组任务中添加身份验证代理创建命令时，该步骤将可用。当您在*管理身份验证代理账户*本地任务中添加身份验证代理创建命令时，该步骤不可用。

7. 在“**用户名**”字段中，输入在身份验证过程中必须输入的身份验证代理帐户名，以便访问加密的硬盘驱动器。

8. 如果您希望在身份验证期间应用程序提示用户输入身份验证代理账户以便访问加密硬盘，请选择“**允许基于密码的身份验证**”。设置身份验证代理账户的密码。如有必要，您可以在首次身份验证后向用户请求新密码。

9. 如果您希望在访问加密硬盘驱动器的身份验证期间应用程序提示用户输入连接至计算机的令牌或智能卡，请选择“**允许基于证书的身份验证**”。选择一个证书文件以使用智能卡或令牌进行身份验证。

10. 如有必要，在“**命令描述**”字段中输入您需要管理命令的身份验证代理帐户的详情。

11. 在“**在身份验证代理中进行身份验证的权限**”块，为使用命令中指定的账户的用户配置在身份验证代理中进行身份验证的权限。

12. 保存更改。

如何通过 Web Console 添加身份验证代理账户

1. 在 Web Console 的主窗口中，选择“**任务**”。

   任务列表打开。

2. 单击 Kaspersky Endpoint Security 的“**管理身份验证代理账户**”任务。

   任务属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 在身份验证代理账户列表中，单击“**添加**”按钮。

   这将启动“身份验证代理账户管理向导”。

5. 选择“**添加**”命令类型。

6. 选择用户账户。您可以从域账户列表中选择账户，也可以手动输入账户名称。转到下一步。

   Kaspersky Endpoint Security 会确定账户安全标识符 (SID)。这是验证账户所必需的。如果输入的用户名不正确，Kaspersky Endpoint Security 将以出错结束任务。

7. 配置身份验证代理账户设置。

   - “**创建新的身份验证代理账户以替换现有账户**”。Kaspersky Endpoint Security 将扫描计算机上的现有账户。如果计算机上和任务中的用户安全 ID 匹配，则 Kaspersky Endpoint Security 将根据任务更改用户账户设置。

   - “**用户名**”。身份验证代理账户的默认用户名与用户的域名相对应。

- “**允许基于密码的身份验证**”。设置身份验证代理账户的密码。如有必要，您可以在首次身份验证后向用户请求新密码。这样，每个用户将拥有自己的唯一密码。您还可以在策略中为身份验证代理账户设置密码强度要求。

- “**允许基于证书的身份验证**”。选择一个证书文件以使用智能卡或令牌进行身份验证。这样，用户将需要输入智能卡或令牌的密码。

- “**账户对加密数据的访问权限**”。配置用户对加密驱动器的访问权限。例如，您可以暂时禁用用户身份验证，而不是删除身份验证代理账户。

- “**注释**”。如有必要，输入账户说明。

8. 保存更改。

9. 选中任务旁边的复选框，然后单击“**开始**”按钮。

结果，在下次计算机启动时，当任务完成后，新用户可以完成身份验证过程、加载操作系统和获得对加密驱动器的访问权限。

要更改身份验证代理账户的密码和其他设置，您需要向“*管理身份验证代理账户*”任务添加特殊命令。使用组任务很方便，例如，替换所有计算机上的管理员令牌证书。

如何通过管理控制台 (MMC) 更改身份验证代理账户

1. 打开“*管理身份验证代理账户*”任务的属性。

2. 在任务属性中，选择“**设置**”区域。

3. 单击**添加** → **账户编辑命令**。

4. 在打开的窗口的“**Windows 账户**”字段中，指定要更改的 Microsoft Windows 用户账户的名称。

5. 如果您手动输入了 Windows 账户名称，请单击“**允许**”按钮以定义账户安全标识符 (SID)。

   如果您单击“**允许**”按钮时选择不决定安全标识符 SID，SID 将在任务在计算机上执行时确定。

   > 定义 Windows 账户安全标识符对于验证 Windows 账户名称是否正确输入是必需的。如果计算机或受信任域中不存在 Windows 账户，则“*管理身份验证代理账户*”任务将以出错结束。

6. 如果您希望 Kaspersky Endpoint Security 为所有基于 Microsoft Windows 的以下字段中输入的“**Windows 账户**”的身份验证代理账户更改用户名，请选择“**更改用户名**”复选框，然后为身份验证代理用户账户输入新名称。

7. 选择“**修改基于密码的身份验证设置**”复选框使基于密码的身份验证设置变为可用。

8. 如果您希望在身份验证期间应用程序提示用户输入身份验证代理账户以便访问加密硬盘，请选择“**允许基于密码的身份验证**”。设置身份验证代理账户的密码。

9. 如果您希望 Kaspersky Endpoint Security 为所有基于 Microsoft Windows 的以下字段中输入的“**Windows 账户**”的身份验证代理账户更改密码，请选择“**在身份验证代理中进行身份验证时编辑密码更改规则**”复选框。

10. 在身份验证代理中验证身份时指定密码更改设置的值。

11. 选择“**修改基于证书的身份验证设置**”复选框以便编辑基于令牌或智能卡电子证书的身份验证设置。

12. 如果您希望在身份验证期间应用程序提示用户输入连接至计算机的令牌或智能卡以便访问加密硬盘，请选择“**允许基于证书的身份验证**”。选择一个证书文件以使用智能卡或令牌进行身份验证。

13. 如果您希望 Kaspersky Endpoint Security 为所有使用 Microsoft Windows 的以下字段中输入的“**Windows 账户**”的身份验证代理帐户更改命令描述，请选择“**编辑命令描述**”复选框。

14. 如果您希望 Kaspersky Endpoint Security 为所有 **Windows 账户**字段中指定的 Microsoft Windows 帐户创建的所有身份验证代理帐户将身份验证代理中身份验证用户访问规则更改为以下指定值，请选择“**编辑身份验证代理中的身份验证访问规则**”复选框。

15. 在身份验证代理中指定访问身份验证对话框的规则。

16. 保存更改。

如何通过 Web Console 更改身份验证代理账户

1. 在 Web Console 的主窗口中，选择“**任务**”。

   任务列表打开。

2. 单击 Kaspersky Endpoint Security 的“**管理身份验证代理账户**”任务。

   任务属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 在身份验证代理账户列表中，单击“**添加**”按钮。

   这将启动“身份验证代理账户管理向导”。

5. 选择“**更改**”命令类型。

6. 选择用户账户。您可以从域账户列表中选择账户，也可以手动输入账户名称。转到下一步。

   Kaspersky Endpoint Security 会确定账户安全标识符 (SID)。这是验证账户所必需的。如果输入的用户名不正确，Kaspersky Endpoint Security 将以出错结束任务。

7. 选中要编辑的设置旁边的复选框。

8. 配置身份验证代理账户设置。

   - “**创建新的身份验证代理账户以替换现有账户**”。Kaspersky Endpoint Security 将扫描计算机上的现有账户。如果计算机上和任务中的用户安全 ID 匹配，则 Kaspersky Endpoint Security 将根据任务更改用户账户设置。

   - “**用户名**”。身份验证代理账户的默认用户名与用户的域名相对应。

   - “**允许基于密码的身份验证**”。设置身份验证代理账户的密码。如有必要，您可以在首次身份验证后向用户请求新密码。这样，每个用户将拥有自己的唯一密码。您还可以在策略中为身份验证代理账户设置密码强度要求。

   - “**允许基于证书的身份验证**”。选择一个证书文件以使用智能卡或令牌进行身份验证。这样，用户将需要输入智能卡或令牌的密码。

   - “**账户对加密数据的访问权限**”。配置用户对加密驱动器的访问权限。例如，您可以暂时禁用用户身份验证，而不是删除身份验证代理账户。

   - “**注释**”。如有必要，输入账户说明。

9. 保存更改。

10. 选中任务旁边的复选框，然后单击“**开始**”按钮。

要删除身份验证代理账户，您需要向“*管理身份验证代理账户*”任务添加特殊命令。使用组任务很方便，例如，删除已解雇的员工的账户。

如何通过管理控制台 (MMC) 删除身份验证代理账户

1. 打开“*管理身份验证代理账户*”任务的属性。

2. 在任务属性中，选择“**设置**”区域。

3. 单击**添加** → **账户删除命令**。

4. 在打开的窗口的“**Windows 账户**”字段中，指定用于创建您要删除的身份验证代理账户的 Windows 用户账户的名称。

5. 如果您手动输入了 Windows 账户名称，请单击“**允许**”按钮以定义账户安全标识符 (SID)。

   如果您单击“**允许**”按钮时选择不决定安全标识符 SID，SID 将在任务在计算机上执行时确定。

   > 定义 Windows 账户安全标识符对于验证 Windows 账户名称是否正确输入是必需的。如果计算机或受信任域中不存在 Windows 账户，则“*管理身份验证代理账户*”任务将以出错结束。

6. 保存更改。

如何通过 Web Console 删除身份验证代理账户

1. 在 Web Console 的主窗口中，选择“**任务**”。

   任务列表打开。

2. 单击 Kaspersky Endpoint Security 的“**管理身份验证代理账户**”任务。

   任务属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 在身份验证代理账户列表中，单击“**添加**”按钮。

   这将启动“身份验证代理账户管理向导”。

5. 选择“**删除**”命令类型。

6. 选择用户账户。您可以从域账户列表中选择账户，也可以手动输入账户名称。

7. 保存更改。

8. 选中任务旁边的复选框，然后单击“**开始**”按钮。

   结果，在下次计算机启动时，当任务完成后，用户将无法完成身份验证过程和加载操作系统。Kaspersky Endpoint Security 将拒绝对加密数据的访问。

要查看可以通过代理完成身份验证并加载操作系统的用户列表，您需要转到受管理计算机的属性。

如何通过管理控制台 (MMC) 查看身份验证代理账户列表

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**设备**”。
3. 双击以打开计算机属性窗口。
4. 在计算机属性窗口中，选择“**任务**”区域。
5. 在任务列表中，选择“**管理身份验证代理账户**”并双击打开任务属性。
6. 在任务属性中，选择“**设置**”区域。

结果，您将能够访问此计算机上的身份验证代理账户列表。只有列表中的用户可以通过代理完成身份验证并加载操作系统。

如何通过 Web Console 查看身份验证代理账户列表

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**资产(设备)**”。
2. 单击要查看其上的身份验证代理账户列表的计算机的名称。
3. 在计算机属性中选择“**任务**”选项卡。
4. 在任务列表中，选择“**管理身份验证代理账户**”。
5. 在任务属性中，选择“**应用程序设置**”选项卡。

结果，您将能够访问此计算机上的身份验证代理账户列表。只有列表中的用户可以通过代理完成身份验证并加载操作系统。

配合身份验证代理使用令牌和智能卡

访问加密硬盘驱动器时可将令牌或智能卡用于身份验证。为此，必须将令牌或智能卡的电子证书文件添加到“*管理身份验证代理账户*”任务中。

> 仅当计算机硬盘驱动器使用 AES256 加密算法进行加密时，才可以使用令牌或智能卡。如果使用 AES56 算法加密了计算机硬盘驱动器，添加电子证书文件到命令将被拒绝。

Kaspersky Endpoint Security 支持以下令牌、智能卡读卡器和智能卡：

- SafeNet eToken PRO 64K (4.2b)；
- SafeNet eToken PRO 72K Java；
- SafeNet eToken 4100-72K Java；
- SafeNet eToken 5100；
- SafeNet eToken 5105；

- SafeNet eToken 7300；
- EMC RSA SID 800；
- Gemalto IDPrime.NET 510；
- Gemalto IDPrime.NET 511；
- Rutoken ECP；
- Rutoken ECP Flash；
- Athena IDProtect Laser；
- SafeNet eToken PRO 72K Java；
- Aladdin-RD JaCarta PKI。

要把令牌文件或智能卡电子证书文件添加到用于创建身份验证代理帐户的命令中，请首先使用用于管理证书的第三方软件保存文件。

令牌或智能卡证书必须具有下列属性：

- 证书必须兼容 X.509 标准，并且证书必须具有 DER 编码。
- 该证书包含至少 1024 位长度的 RSA 密钥。

如果令牌或智能卡的电子证书不满足这些要求，则无法将证书文件加载到用于创建身份验证代理账户的命令中。

证书的 `KeyUsage` 参数的值必须为 `keyEncipherment` 或 `dataEncipherment`。`KeyUsage` 参数确定证书的用途。如果参数的值不同，Kaspersky Security Center 将下载证书文件，但会显示警告。

如果用户丢失了令牌或智能卡，则管理员必须将令牌或智能卡电子证书文件添加到命令以创建身份验证代理账户。然后用户必须完成在加密设备上接受加密设备访问或恢复数据的过程。

硬盘驱动器解密

> 即使没有允许数据加密的当前授权许可，您也可以解密硬盘驱动器。

若要解密硬盘驱动器，请执行以下操作：

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **数据加密** → **完整磁盘加密**。
4. 在“**加密技术**”下拉列表中选择加密硬盘驱动器的技术。

5. 执行下列操作之一：

- 在“**加密模式**”下拉列表中，选择“**解密所有硬盘驱动器**”选项，如果您希望解密所有加密的硬盘驱动器。
- 将您希望解密的加密硬盘驱动器添加至“**请勿加密以下硬盘驱动器**”表。

> 该选项仅对 卡巴斯基磁盘加密 技术有效。

6. 保存更改。

您可以使用加密监控器工具控制用户计算机上的磁盘加密或解密过程。您可以从主应用程序窗口运行加密监控器工具。

加密组件	对象	状态	ID
完整磁盘加密	硬盘	加密程度 53%	4&30559173&0&000000
完整磁盘加密	硬盘	解密程度 92%	4&1557B4B5&0&000300
BitLocker 驱动器加密	卷 C:	加密程度 0%	\\?\Volume{7588d728-3008-47b1-a681-5b5a9d9c9a95}\
BitLocker 驱动器加密	卷 D: (Data)	解密程度 21%	\\?\Volume{dab54211-5eb4-457a-8a8f-efc4194e995d}\
BitLocker 驱动器加密	卷 E: (Storage)	加密程度 47%	\\?\Volume{f0b1506e-9ca8-4998-9a31-ed30c413b542}\
BitLocker 驱动器加密	卷 H:	解密程度 100%	\\?\Volume{e9b2ea99-ce84-4c58-a3bd-d9938a2f22de}\
完整磁盘加密	可移动驱动器	加密程度 0%	USBSTOR\DISK&VEN_JETFLASH&PROD_TRANSCEND_2GB&R...
完整磁盘加密	可移动驱动器	解密程度 100%	USBSTOR\DISK&VEN_KINGSTON&PROD_KINGSTON_128GB&...

加密监控

如果用户在解密使用卡巴斯基磁盘加密技术进行了加密的硬盘驱动器期间关闭了或重新启动了计算机，下次启动操作系统之前系统将载入身份验证代理。成功通过身份验证代理并在操作系统启动后，Kaspersky Endpoint Security 将恢复硬盘驱动器解密。

如果操作系统在在解密使用卡巴斯基磁盘加密技术进行了加密的硬盘驱动器期间切换至休眠模式，操作系统退出休眠模式时将加载身份验证代理。成功通过身份验证代理并在操作系统启动后，Kaspersky Endpoint Security 将恢复硬盘驱动器解密。硬盘驱动器解密之后，休眠模式直至首次重启操作系统才可用。

如果操作系统在硬盘驱动器解密期间进入睡眠模式，则当操作系统退出睡眠模式时，Kaspersky Endpoint Security 将恢复硬盘驱动器加密，且无需加载身份验证代理。

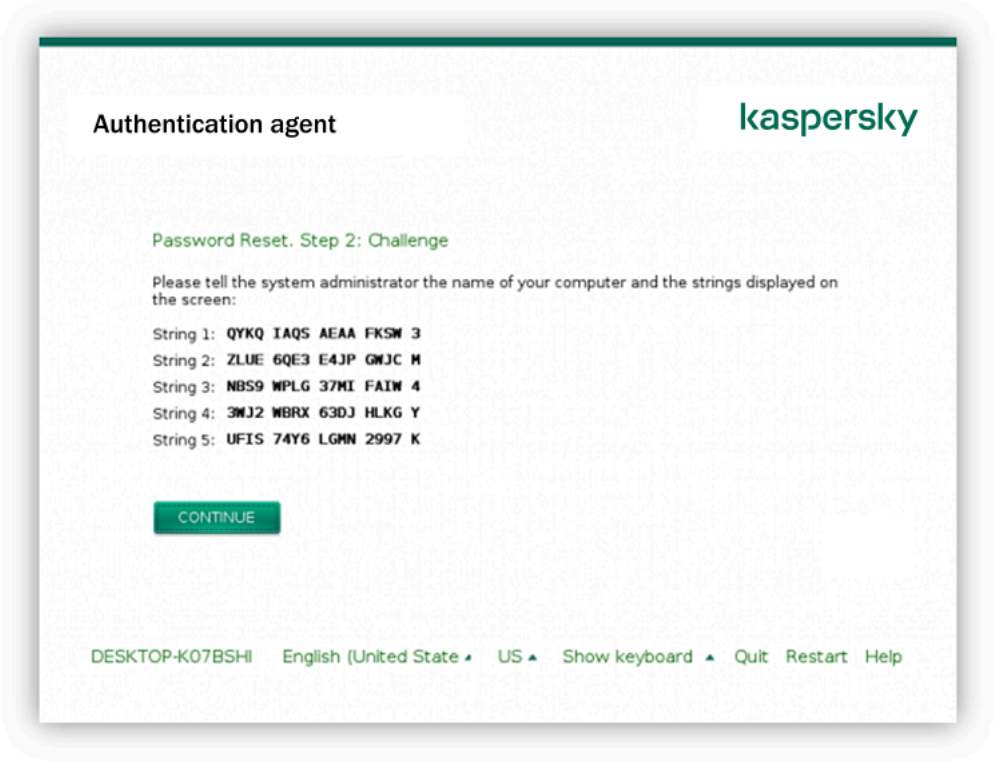
还原对受卡巴斯基磁盘加密技术保护的驱动器的访问权限

如果用户忘记了受卡巴斯基磁盘加密技术保护的硬盘驱动器的访问密码，则需要启动恢复过程（请求-响应）。如果在磁盘加密设置中启用了此功能，您还可以使用服务账户访问硬盘。

还原对系统硬盘驱动器的访问权限

还原对受卡巴斯基磁盘加密技术保护的系统硬盘驱动器的访问权限包括以下步骤：

1. 用户将请求块报告给管理员（请参见下图）。
2. 管理员将请求块输入 Kaspersky Security Center，接收响应块并将响应块报告给用户。
3. 用户在“身份验证代理”界面中输入响应块，并获得对硬盘驱动器的访问权限。



还原对受卡巴斯基磁盘加密技术保护的系统硬盘驱动器的访问权限

要启动恢复过程，用户需要在“身份验证代理”界面中单击“**Forgot your password**”按钮。

如何在管理控制台 (MMC) 中获取受卡巴斯基磁盘加密技术保护的系统硬盘驱动器的响应块

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**设备**”。
3. 在“**设备**”选项卡上，选择用户正在请求加密数据访问权限的计算机，然后单击鼠标右键打开上下文菜单。
4. 在上下文菜单中，选择“**授予离线模式下的访问权限**”。

5. 这将打开一个窗口；在该窗口中，选择“**身份验证代理**”选项卡。

6. 在“**正在使用的加密算法**”块中，选择加密算法：**AES56** 或 **AES256**。

   数据加密算法取决于分发包中包含的 AES 加密库：*强加密(AES256)* 或 *轻度加密(AES56)*。AES 加密库与应用程序一起安装。

7. 在“**账户**”下拉列表中，选择请求恢复驱动器访问权限的用户的身份验证代理账户名称。

8. 在**硬盘驱动器**下拉列表中，选择您要恢复访问的加密硬盘驱动器。

9. 在“**用户请求**”块输入用户填写的请求框。

   结果，对用户的恢复身份验证代理账户的用户名和密码的请求的响应块内容将显示在“**访问密钥**”字段中。将响应块的内容传达给用户。

在移动模式下授予访问权限

如何在 Web Console 中获取受卡巴斯基磁盘加密技术保护的系统硬盘驱动器的响应块

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**资产(设备)**”。

2. 选中要恢复其驱动器访问权限的计算机名称旁边的复选框。

3. 单击“**授予移动模式设备访问权限**”。

4. 在打开的窗口中选择“**身份验证代理**”区域。

5. 在“**账户**”下拉列表中，选择为请求恢复身份验证代理帐户名和密码的用户创建的身份验证代理帐户的名称。

6. 输入用户传达的请求块。

   对用户的恢复身份验证代理账户的用户名和密码的请求的响应块内容将显示在窗口底部。将响应块的内容传达给用户。

完成恢复过程后，身份验证代理将提示用户更改密码。

还原对非系统硬盘驱动器的访问权限

还原对受卡巴斯基磁盘加密技术保护的非系统硬盘驱动器的访问权限包括以下步骤：

1. 用户将请求访问文件发送给管理员。
2. 管理员将请求访问文件添加到 Kaspersky Security Center 中，创建访问密钥文件并将该文件发送给用户。
3. 用户将访问密钥文件添加到 Kaspersky Endpoint Security 并获得对硬盘驱动器的访问权限。

要启动恢复过程，用户需要尝试访问硬盘驱动器。结果，Kaspersky Endpoint Security 将创建一个请求访问文件（扩展名为 KESDC 的文件），用户需要将该文件发送给管理员，例如通过电子邮件发送。

如何在管理控制台 (MMC) 中获取加密的非系统硬盘驱动器的访问密钥文件

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**设备**”。
3. 在“**设备**”选项卡上，选择用户正在请求加密数据访问权限的计算机，然后单击鼠标右键打开上下文菜单。
4. 在上下文菜单中，选择“**授予离线模式下的访问权限**”。
5. 这将打开一个窗口；在该窗口中，选择“**数据加密**”选项卡。
6. 在“**数据加密**”选项卡上单击“**浏览**”按钮。
7. 在用于选择请求访问文件的窗口中，指定从用户处接收的文件的路径。

   您将看到有关用户请求的信息。Kaspersky Security Center 会生成一个密钥文件。通过电子邮件将生成的加密数据访问密钥文件发送给用户。或保存该访问文件并使用任何可用方法来传输该文件。

在移动模式下授予访问权限

如何在 Web Console 中获取非系统硬盘驱动器访问密钥文件

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**资产(设备)**”。
2. 选中要还原其数据访问权限的计算机名称旁边的复选框。
3. 单击“**授予移动模式设备访问权限**”。
4. 选择“**数据加密**”。
5. 单击“**选择文件**”按钮，然后选择从用户处收到的请求访问文件（扩展名为 KESDC 的文件）。
   Web Console 将显示有关请求的信息。这将包括用户请求访问的文件所在的计算机的名称。
6. 单击“**保存密钥**”按钮，然后选择一个文件夹来保存加密数据访问密钥文件（扩展名为 KESDR 的文件）。

结果，您将能够获取加密数据访问密钥，您需要将该密钥传输给用户。

使用身份验证代理服务账户登录

Kaspersky Endpoint Security 允许您在加密驱动器时添加身份验证代理服务账户。服务账户是访问计算机所必需的，例如，当用户忘记密码时。您还可以将服务账户用作备用账户。要添加账户，在磁盘加密设置中选择服务账户，然后输入用户账户的名称（默认是 `ServiceAccount`）。要使用代理进行身份验证，您将需要一次性密码。

如何在管理控制台(MMC)找到一次性密码

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**设备**”。
3. 双击以打开计算机属性窗口。
4. 在计算机属性窗口中，选择“**任务**”区域。
5. 在任务列表中，选择“**管理身份验证代理账户**”并双击打开任务属性。
6. 在任务属性窗口中，选择“**设置**”区域。
7. 在账户列表中，选择身份验证代理服务账户（例如，`WIN10-USER\ServiceAccount`）。
8. 在“**操作**”下拉列表中，选择“**查看账户**”。
9. 在账户属性中，选择“**显示原密码**”复选框。
10. 复制一次性密码用于登录服务账户。

如何在 Web 控制台找到一次性密码

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**资产(设备)**”。
2. 单击要查看其上的身份验证代理账户列表的计算机的名称。
   这将打开计算机属性。
3. 在计算机属性中选择“**任务**”选项卡。

4. 在任务列表中，选择“**管理身份验证代理账户**”。

5. 在任务属性中，选择“**应用程序设置**”选项卡。

6. 在账户列表中，选择身份验证代理服务账户（例如，`WIN10-USER\ServiceAccount`）。

7. 在账户属性中，选择“**显示密码**”复选框。

8. 复制一次性密码用于登录服务账户。

每次用户使用服务账户进行身份验证时，Kaspersky Endpoint Security 会自动更新密码。在使用代理进行身份验证后，您必须输入 Windows 账户密码。当使用服务账户登录时，您无法使用 SSO 技术。

更新操作系统

更新受完整磁盘加密 (FDE) 保护的计算机的操作系统有许多特殊注意事项。按如下方式更新操作系统：先更新一台计算机上的操作系统，然后更新一小部分计算机上的操作系统，再更新网络中所有计算机上的操作系统。

如果正在使用卡巴斯基磁盘加密技术，则在启动操作系统之前会加载身份验证代理。使用身份验证代理，用户可以登录系统并获得对加密驱动器的访问权限。然后，操作系统开始加载。如果在使用卡巴斯基磁盘加密技术保护的计算机上启动操作系统更新，则操作系统更新向导将删除身份验证代理。结果，计算机可被锁定，因为操作系统加载程序将无法访问加密驱动器。

操作系统更新的功能：

- **通过 WSUS 更新操作系统**。您可以按照常规方式更新操作系统。
- **从 ISO 更新操作系统**。要更新操作系统，您必须指定包含卡巴斯基磁盘加密驱动程序的文件夹。应用程序会自动将驱动程序复制到单独的文件夹。执行以下操作：

  1. 挂载 ISO 镜像。

  2. 使用以下密钥开始安装系统更新：

     ```
     setup.exe /ReflectDrivers %ProgramFiles(x86)%\Kaspersky Lab\KES.14.1\reflect_drivers
     ```

> 仅当计算机运行 Windows 10 1607 (RS1) 或更高版本时，才可以使用操作系统自动更新。要升级早期版本的操作系统，推荐您先解密磁盘，执行操作系统升级，然后加密磁盘。

如果正在使用 BitLocker 驱动器加密技术，则无需解密硬盘驱动器即可更新 Windows 10。有关 BitLocker 的详细信息，请访问 Microsoft 网站。

消除加密功能更新的错误

在以前版本的应用程序升级到 Kaspersky Endpoint Security for Windows 14.1 时，将更新“完整磁盘加密”。

开始更新“完整磁盘加密”功能时，可能出现以下错误：

- 无法初始化更新。
- 设备与身份验证代理不兼容。

要消除在开始新应用程序版本中的“完整磁盘加密”功能的更新流程时出现的错误：

1. 解密硬盘驱动器。
2. 再次加密硬盘驱动器。

在更新“完整磁盘加密”功能的过程中，可能出现以下错误：

- 无法完成更新。
- “完整磁盘加密”升级回滚完成但出错。

要消除在“完整磁盘加密”功能更新流程中出现的错误，

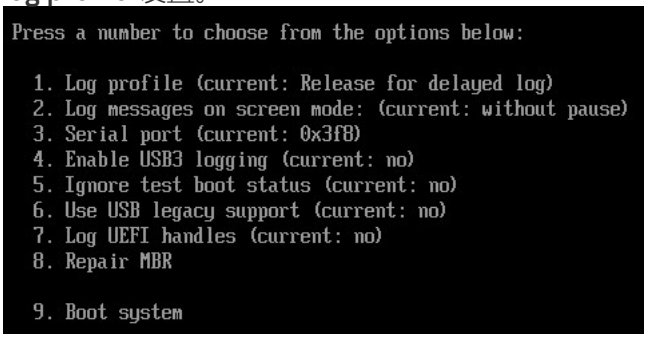
请使用恢复实用程序恢复对加密设备的访问权限。

跟踪身份验证代理

跟踪文件中关于身份验证代理的应用程序日志服务信息和关于身份验证代理用户操作的信息。

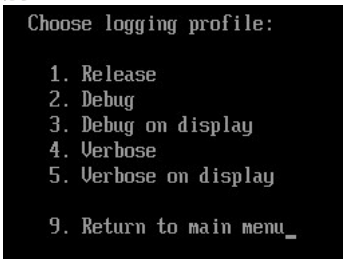
要启用身份验证代理跟踪：

1. 启用 Kaspersky Endpoint Security 追踪。
2. 重新启动计算机。
3. 当带有加密硬盘驱动器的计算机启动后，请按 **F3** 按钮，调出用于配置身份验证代理设置的窗口。
4. FDE 引导加载程序启动后，选择“**KES (FDE <version>)**”启动管理器。
5. 在启动管理器菜单中，转到“**Log profile**”设置。



启动管理器菜单

6. 在日志配置文件设置窗口中，选择跟踪级别：



身份验证代理跟踪级别

- “**Release**”。如果选定该选项，应用程序不会在跟踪文件中记录有关身份验证代理事件的信息。
- “**Debug**”。如果选择此选项，应用程序在跟踪文件中记录身份验证代理的操作和身份验证代理的用户执行操作。
- “**Debug on display**”。如果选择此选项，应用程序将在跟踪文件中记录身份验证代理的操作输入和身份验证代理的用户执行操作，并通过 COM 端口传输该文件。

  如果带有已加密硬盘驱动器的计算机通过 COM 端口连接至另一台计算机时，可以从另一台计算机检查身份验证代理事件。
- “**Verbose**”。如果选择此选项，应用程序将把身份验证代理的操作输入和身份验证代理的用户执行操作纳入跟踪文件。

  > 与“**Debug**”选项的级别相比，在此选项下，输入项的详细信息程度要更高。输入项的详细信息程度更高将会减慢身份验证代理和操作系统的启动。

- “**Verbose on display**”。如果选择此选项，应用程序将在跟踪文件中详细记录身份验证代理的操作输入和身份验证代理的用户操作，并通过 COM 端口传输该文件。

  > 与“**Debug on display**”选项的级别相比，在此选项下，输入项的详细信息程度要更高。输入项的详细信息程度更高将会减慢身份验证代理和操作系统的启动。

选择跟踪级别后，启动管理器会再次显示菜单。

7. 在启动管理器菜单中，选择“**Boot system**”。

   FDE 引导加载程序启动身份验证代理。

   重现问题。

   如果计算机上有已加密的硬盘驱动器或者在完整磁盘加密期间，数据将记录在身份验证代理跟踪文件中。

8. 要停止跟踪进程，返回支持工具窗口并禁用跟踪。

结果，将在文件夹 `%ProgramData%\Kaspersky Lab\KES.14.1\Traces` 中创建身份验证代理 KES.SRV 操作跟踪文件。与其他程序跟踪文件不一样，身份验证代理跟踪文件不会发送至 Kaspersky。如有必要，您可以手动将身份验证代理跟踪文件发送至 Kaspersky 以供分析。

编辑身份验证代理帮助文本

> 在编辑身份验证代理的帮助消息之前，请查看预启动环境中支持的字符列表（请参见下文）。

若要编辑身份验证代理帮助邮件，请执行以下操作：

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **数据加密 → 通用加密设置**。
4. 在“**模板**”块中单击“**帮助**”按钮。
5. 在打开的窗口中，做以下事项：
   - 输入帐户凭证时选择“**身份验证**”选项卡编辑身份验证代理窗口中显示的帮助文本。
   - 选择“**更改密码**”选项卡可编辑在更改身份验证代理帐户密码时显示在“身份验证代理”窗口中的帮助文本。
   - 选择“**恢复密码**”选项卡可编辑在恢复身份验证代理帐户密码时显示在“身份验证代理”窗口中的帮助文本。
6. 编辑帮助消息。
   如果您希望恢复原始文本，则单击“**默认**”按钮。

   > 您可以输入包含 16 或更少行的帮助文本。每行的最大长度为 64 个字符。

7. 保存更改。

身份验证代理帮助邮件中字符串的有限支持

在预启动环境下，支持以下 Unicode 字符：

- 基本拉丁字母 (0000 - 007F)
- 附加 Latin-1 字符 (0080 - 00FF)
- 扩展 Latin-A (0100 - 017F)
- 扩展 Latin-B (0180 - 024F)
- 未组合的扩展 ID 字符 (02B0 - 02FF)
- 组合变音标记 (0300 - 036F)
- 希腊和科普特字母 (0370 - 03FF)
- 西里尔字母 (0400 - 04FF)
- 希伯来语 (0590 - 05FF)
- 阿拉伯语 (0600 - 06FF)
- 附加扩展拉丁语 (1E00 - 1EFF)

- 标点符号 (2000 - 206F)
- 货币符号 (20A0 - 20CF)
- 类似字母的符号 (2100 - 214F)
- 几何符号 (25A0 - 25FF)
- 阿拉伯语 Script-B (FE70 - FEFF)

该列表中未指定的字符在预启动环境中不受支持。不建议在身份验证代理帮助消息中使用此类字符。

测试身份验证代理的操作后，删除剩余的对象和数据

应用程序卸载期间，如果 Kaspersky Endpoint Security 在身份验证代理测试运行后检测到系统硬盘驱动器上遗留对象和数据，则应用程序卸载将被中断且在删除此类对象和数据之前无法继续。

仅在例外情况下，当身份验证代理测试运行后，遗留的对象和数据才能留在系统硬盘驱动器上。例如，如果应用执行加密设置的 Kaspersky Security Center 策略之后计算机尚未启动过，或者如果身份验证代理试运行后应用程序启动失败时，会发生此情况。

您可以使用以下方式删除身份验证代理在测试运行之后遗留在系统硬盘驱动器中的对象和数据：

- 使用 Kaspersky Security Center 策略。
- 使用恢复实用程序。

若要使用 Kaspersky Security Center 策略删除身份验证代理测试运行后遗留的对象和数据：

1. 将带有配置为解密所有计算机硬盘驱动器设置的 Kaspersky Security Center 策略应用至计算机。
2. 启动 Kaspersky Endpoint Security。

若要使用“恢复实用工具”删除身份验证代理测试运行后遗留的对象和数据：

1. 运行名为 fdert.exe 的文件，该文件是恢复实用程序的可执行文件。该文件由 Kaspersky Endpoint Security 创建。
2. 在“恢复实用工具”窗口中，选择所需的设备。
3. 单击“**扫描**”。
4. 如果在诊断系统硬盘后收到一条消息，提示身份验证代理的测试运行后仍有对象和数据残留，请单击 **删除 AA 对象和数据**。

   仅当检测到身份验证代理测试运行后残留的对象和数据时，**删除 AA 对象和数据** 按钮才可用。

若要删除应用程序与身份验证代理的兼容性信息，

请在命令行中输入 `avp pbatestreset`。

BitLocker 管理

BitLocker 是 Windows 操作系统内置的加密技术。Kaspersky Endpoint Security 允许您使用 Kaspersky Next 基础设施控制和管理 Bitlocker。BitLocker 可对逻辑卷进行加密。BitLocker 不能用于可移动驱动器的加密。有关 BitLocker 的详细信息，请参阅 Microsoft 文档。

加密磁盘时，BitLocker 将引导加载程序和其他辅助文件放入 system partition。此分区未加密。操作系统在安装 Windows 时会自动创建系统分区。如果在安装 Windows 之前磁盘已完全分区，则操作系统无法创建系统分区。在这种情况下，当启动 BitLocker 磁盘加密时，操作系统会提示您对磁盘重新分区，并创建系统分区。创建系统分区后，操作系统启动 BitLocker 加密。

BitLocker 加密算法不依赖于分发包（AES256 或 AES56）中包含的 AES 库版本。加密使用操作系统内置的加密库。

默认情况下，应用程序使用有效密钥长度为 256 位的 BitLocker 加密算法来加密从未加密过的设备。对于在安装应用程序之前已加密的设备，加密算法可能有所不同。有关选择加密算法的详细信息，请参阅 Microsoft 技术支持网站。从 12.9 版本开始，Kaspersky Endpoint Security 会将之前由第三方应用程序加密的设备的原始恢复密钥发送到 Kaspersky Security Center。

BitLocker 使用受信任平台模块提供对访问密钥的安全存储。 *Trusted Platform Module*(TPM) 是一个与安全相关的提供基本功能的微芯片（例如用于存储加密密钥）。受信任平台模块通常安装在计算机主板上，并通过硬件总线与其他所有系统组件进行交互。使用 TPM 是存储 BitLocker 访问密钥的最安全方式，因为 TPM 提供了启动前系统完整性验证。您仍然可以在没有 TPM 的计算机上对驱动器进行加密。在这种情况下，将使用密码对访问密钥进行加密。BitLocker 使用以下身份验证方式：

- TPM。
- TPM 和 PIN。
- 密码。

对系统硬盘驱动器进行加密后，用户需要通过 BitLocker 身份验证才能启动操作系统。身份验证完成后，BitLocker 允许用户登录。BitLocker 不支持单点登录技术 (SSO)。

在对驱动器进行加密后，BitLocker 会创建一个恢复密钥。Kaspersky Endpoint Security 会将恢复密钥发送到 Kaspersky Security Center，以便您可以恢复对磁盘的访问，例如，如果用户忘记了密码。

如果用户使用 BitLocker 对磁盘进行加密，Kaspersky Endpoint Security 会将恢复密钥和有关磁盘加密的信息发送到 Kaspersky Security Center。

如果正在使用 Windows 组策略，请在策略设置中关闭 BitLocker 管理。Windows 策略设置可能与 Kaspersky Endpoint Security 策略设置冲突。在对驱动器进行加密时，可能会发生错误。

启动 BitLocker 驱动器加密

在开始完整磁盘加密之前，建议您确保计算机未受到感染。若要执行操作，应启动全盘扫描或关键区域扫描任务。在已被 rootkit 感染的计算机上执行完整磁盘加密可能导致计算机无法运行。

若要在运行适用于服务器的 Windows 操作系统的计算机上使用 BitLocker 驱动器加密，可能需要安装“BitLocker 驱动器加密”组件。可使用操作系统工具（添加角色和组件向导）安装该组件。有关安装“BitLocker 驱动器加密”的更多信息，请参阅 Microsoft 文档。

如何通过管理控制台 (MMC) 运行 BitLocker 驱动器加密

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **数据加密** → **完整磁盘加密**。
4. 在“**加密技术**”下拉列表中，选择“**BitLocker 驱动器加密**”。
5. 在“**加密模式**”下拉列表中，选择“**加密所有硬盘驱动器**”。

   如果计算机安装了多个操作系统，在加密后，您将能够只加载执行了加密的操作系统。

6. 配置高级 BitLocker 驱动器加密选项（参见下表）。
7. 保存更改。

如何通过 Web Console 和云控制台运行 BitLocker 驱动器加密

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **数据加密** → **完整磁盘加密**。
5. 选择“**BitLocker 磁盘加密**”技术。
6. 在“**设备上的操作**”块中，选择“**加密所有硬盘驱动器**”。

   如果计算机安装了多个操作系统，在加密后，您将能够只加载执行了加密的操作系统。

7. 配置高级 BitLocker 驱动器加密选项（参见下表）。

8. 保存更改。

您可以使用加密监控器工具控制用户计算机上的磁盘加密或解密过程。您可以从主应用程序窗口运行加密监控器工具。

加密监控

应用策略后，应用程序将根据身份验证设置显示以下查询：

- 仅 TPM。不需要用户输入。磁盘将在计算机重启时被加密。
- TPM + PIN / 密码。如果 TPM 模块可用，将显示 PIN 码提示窗口。如果 TPM 模块不可用，您将看到一个用于预启动身份验证的密码提示窗口。
- 仅密码。您将看到预启动身份验证的密码提示窗口。

> 如果为计算机操作系统启用联邦信息处理标准兼容模式，则在 Windows 8 及更早版本的操作系统中，将显示存储设备连接请求以保存恢复密钥文件。您可以将多个恢复密钥文件保存在单个存储设备上。

设置密码或 PIN 后，BitLocker 将要求您重新启动计算机以完成加密。接下来，用户需要完成 BitLocker 身份验证过程。完成身份验证过程后，用户必须登录到系统。加载操作系统后，BitLocker 将完成加密。

如果无法访问加密密钥，用户可以请求局域网管理员提供恢复密钥（如果恢复密钥在较早前未保存在存储设备上或已丢失）。

参数	描述
启用需要在平板电脑上预启动键盘输入的 BitLocker 身份验证	使用在预启动环境中需要数据输入的身份验证，即使该平台没有能力进行预启动输入（例如使用平板电脑上的触摸屏键盘）。 平板电脑的触摸屏在预启动环境中不可用。例如，要在平板电脑上完成 BitLocker 身份验证，用户必须连接 USB 键盘。 如果选定该复选框，则允许使用需要预启动输入的身份验证。我们推荐在预启动环境中仅对拥有备用数据输入工具的设备（例如除了触摸屏键盘之外的 USB 键盘）使用该设置。 如果清除此复选框，则无法在平板电脑上使用 BitLocker 驱动器加密。
使用硬件加密(OS Windows 8 和后续版本)	如果选定该复选框，则应用程序将应用硬件加密。这可以提高加密速度并使用较少的计算机资源。
仅加密使用的磁盘空间(Windows 8 和后续版本)	该复选框可启用/禁用将加密区域仅限为已用硬盘驱动器扇区的选项。该限制可减少加密时间。 加密开始后启用或禁用**仅加密使用的磁盘空间(减少加密时间)**功能在硬盘驱动器被加密之前并不修改该设置。开始加密之前您必须选择或清除该复选框。 如果选定该复选框，则仅加密使用的硬盘驱动器部分。Kaspersky Endpoint Security 将自动加密添加的新数据。 如果清空该复选框，整个硬盘驱动器将被加密，包括先前删除和修改文件残留的碎片。 推荐对尚未修改或删除数据的新硬盘驱动器使用该选项。如果对已在使用中的硬盘驱动器应用加密，则推荐加密整个硬盘驱动器。这样可确保保护所有数据，甚至已删除的数据也能够部分恢复。 默认下，复选框被清除。
身份验证方法	**仅密码(Windows 8 和后续版本)** 如果选定该选项，Kaspersky Endpoint Security 将在用户尝试访问加密磁盘时提示用户输入密码。 没有使用受信任平台模块 (TPM) 时可以选择该选项。 **受信任平台模块 (TPM)** 如果选定该复选框，则 BitLocker 使用受信任平台模块 (TPM)。 *Trusted Platform Module*(TPM) 是一个与安全相关的提供基本功能的微芯片（例如用于存储加密密钥）。受信任平台模块通常安装在计算机主板上并且通过硬件总线与其他所有系统组件进行互动。 对于运行 Windows 7 或 Windows Server 2008 R2 的计算机，只能使用 TPM 模块进行加密。如果未安装 TPM 模块，则无法进行 BitLocker 加密。不支持在这些计算机上使用密码。 配有受信任平台模块的设备可以创建只能使用该设备解密的加密密钥。受信任平台模块将使用其自有的根存储密钥加密加密密钥。根存储密钥存储在受信任平台模块中。这提供了防御黑客攻击加密密钥的附加保护。 默认情况下已选择此操作。 您可以为访问加密密钥设置额外的保护层，并使用密码或 PIN 加密密钥： • "**为 TPM 使用 PIN**"。如果选中该复选框，用户可以使用 PIN 码获得对存储在受信任平台模块 (TPM) 中的加密密钥的访问权限。如果清除此复选框，则禁止用户使用 PIN 码。要访问加密密钥，用户必须输入密码。 • "**受信任平台模块 (TPM)，或密码(如果 TMP 不可用)**"。如果选定该选项，当受信任平台模块 (TPM) 不可用时，用户可使用密码访问加密密钥。如果清除该复选框且 TPM 不可用，则将不会启动完整磁盘加密。 必须通过指定密码或 PIN 来配置所选的身份验证方法： • "**最小 PIN 码长度(字符数)**"。 • "**最小密码长度(字符数)**"。 • "**为 TPM 限制密码/PIN 有效期(天)**"。 • **使用增强 PIN (字母和数字)**。*增强 PIN* 允许使用数字字符以外的其他字符：大写和小写拉丁字母、特殊字符和空格。
自动重新创建恢复密钥(天)	自动更新密码以恢复对受 BitLocker 保护的驱动器的访问权限。如果选中该复选框，请指定恢复密钥密码的有效期。这有助于防止重复使用恢复密钥密码。

解密受 BitLocker 保护的硬盘驱动器

用户可以使用操作系统解密磁盘（“*关闭 BitLocker*”功能）。之后，Kaspersky Endpoint Security 将提示用户重新对磁盘进行加密。除非在策略中启用磁盘解密，否则 Kaspersky Endpoint Security 将提示您加密磁盘。

如何通过管理控制台 (MMC) 解密受 BitLocker 保护的硬盘驱动器

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **数据加密** → **完整磁盘加密**。
4. 在“**加密技术**”下拉列表中，选择“**BitLocker 驱动器加密**”。
5. 在“**加密模式**”下拉列表中，选择“**解密所有硬盘驱动器**”。
6. 保存更改。

如何通过 Web Console 和云控制台解密由 BitLocker 加密的硬盘驱动器

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **数据加密** → **完整磁盘加密**。
5. 选择“**BitLocker 磁盘加密**”技术。
6. 在“**设备上的操作**”块中，选择“**解密所有硬盘驱动器**”。
7. 保存更改。

您可以使用加密监控器工具控制用户计算机上的磁盘加密或解密过程。您可以从主应用程序窗口运行加密监控器工具。

加密监控

恢复对 BitLocker 保护的驱动器的访问权限

如果用户忘记了由 BitLocker 加密的硬盘驱动器的访问密码，则需要启动恢复过程（请求-响应）。

> 如果计算机的操作系统启用了联邦信息处理标准 (FIPS) 兼容模式，则在 Windows 8 和更早版本中，恢复密钥文件将在加密之前保存到可移动驱动器中。要恢复对驱动器的访问权限，请插入可移动驱动器，然后按照屏幕上的说明进行操作。

恢复对 BitLocker 加密的硬盘驱动器的访问权限包括以下步骤：

1. 用户告知管理员恢复密钥 ID（请参见下图）。
2. 管理员在 Kaspersky Security Center 中验证计算机属性中的恢复密钥 ID。用户提供的 ID 必须与计算机属性中显示的 ID 匹配。
3. 如果恢复密钥 ID 匹配，管理员将为用户提供恢复密钥或发送恢复密钥文件。

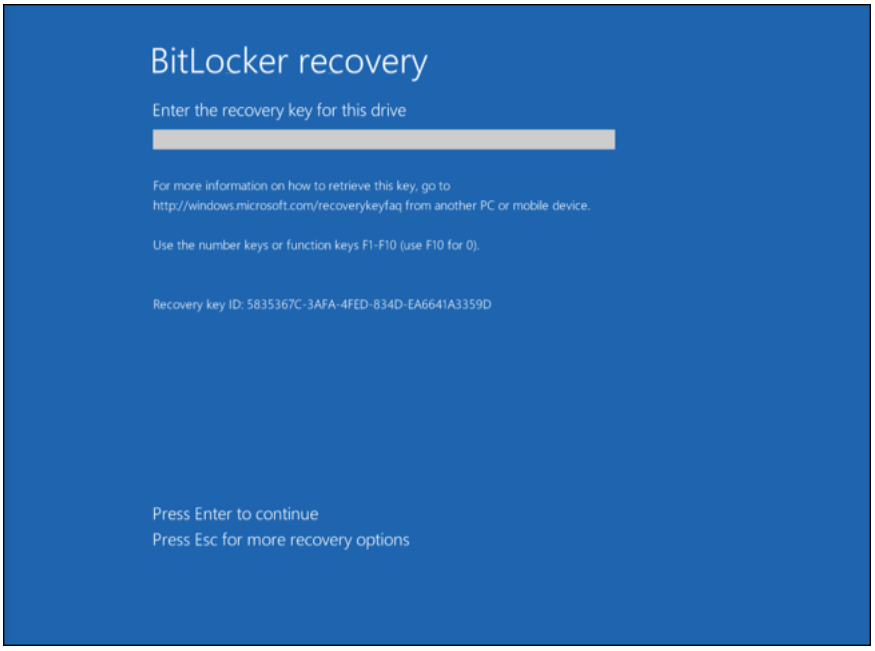
   恢复密钥文件用于运行以下操作系统的计算机：

   - Windows 7
   - Windows 8

- Windows Server 2008；
- Windows Server 2011；
- Windows Server 2012；

对于所有其他操作系统，使用恢复密钥。
为了防止重复使用恢复密钥密码，您可以在策略设置中配置自动密码更新。

4. 用户输入恢复密钥，然后获得对硬盘驱动器的访问权限。



恢复对 BitLocker 加密的硬盘驱动器的访问权限

恢复对系统驱动器的访问权限

要启动恢复过程，用户需要在预引导身份验证阶段按 **Esc** 键。

如何在管理控制台 (MMC) 中查看由 BitLocker 加密的系统驱动器的恢复密钥

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**受管理设备**”。
3. 在“**设备**”选项卡上，选择用户正在请求加密数据访问权限的计算机，然后单击鼠标右键打开上下文菜单。
4. 在上下文菜单中，选择“**授予离线模式下的访问权限**”。
5. 这将打开一个窗口；在该窗口中，选择“**访问受 BitLocker 保护的系统驱动器**”选项卡。
6. 提示用户在 BitLocker 密码输入窗口中输入恢复密钥 ID，然后在“**恢复密钥 ID**”字段中对比该 ID。

> 如果 ID 不匹配，该密钥无法用于恢复指定系统驱动器的访问。请确保选定计算机的名称与用户计算机的名称相符合。

结果，您将有权访问恢复密钥或恢复密钥文件，该密钥或密钥文件将需要传输给用户。

恢复对 BitLocker 加密的驱动器的访问权限

如何在 Web Console 和云控制台中查看 BitLocker 加密的系统驱动器的恢复密钥

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**资产(设备)**”。
2. 选中要恢复其驱动器访问权限的计算机名称旁边的复选框。
3. 单击“**授予移动模式设备访问权限**”。
4. 在打开的窗口中选择“**BitLocker**”区域。
5. 验证恢复密钥 ID。用户提供的 ID 必须与计算机设置中显示的 ID 匹配。

   如果 ID 不匹配，该密钥无法用于恢复指定系统驱动器的访问。请确保选定计算机的名称与用户计算机的名称相符合。

6. 单击“**接收密钥**”。

   结果，您将有权访问恢复密钥或恢复密钥文件，该密钥或密钥文件将需要传输给用户。

在操作系统锁定后，Kaspersky Endpoint Security 提示用户更改密码或 PIN 码。在您设置了新密码或 PIN 码后，BitLocker 将创建一个新的恢复密钥并将其发送到 Kaspersky Security Center。结果，恢复密钥和恢复密钥文件将被更新。如果用户未更改密码，可以在下次操作系统加载时使用旧的恢复密钥。

Windows 7 计算机不允许更改密码或 PIN 码。在输入了恢复密钥且操作系统加载后，Kaspersky Endpoint Security 不提示用户更改密码或 PIN 码。因此，无法设置新密码或 PIN 码。该问题源于操作系统特色。要继续，您需要重新加密硬盘驱动器。

恢复对非系统驱动器的访问权限

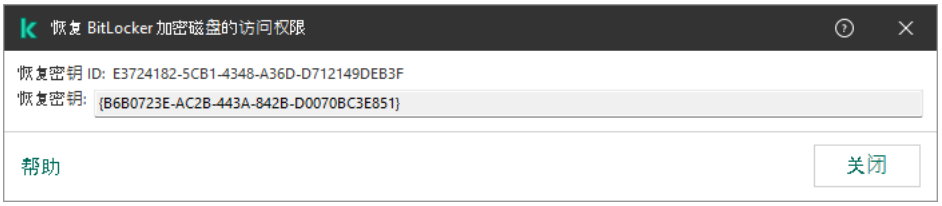
要启动恢复过程，用户需要在提供驱动器访问的窗口中单击“**Forgot your password**”链接。获得对加密驱动器的访问权限后，用户可以在 BitLocker 设置中启用在 Windows 身份验证期间自动解锁驱动器。

如何在管理控制台 (MMC) 中查看由 BitLocker 加密的非系统驱动器的恢复密钥

1. 打开 Kaspersky Security Center Administration Console。
2. 在管理控制台树中，选择“**高级**” → “**数据加密和保护**” → “**加密驱动器**”文件夹。
3. 在工作区中，选择要为其创建访问密钥文件的加密设备，然后在该设备的上下文菜单中，单击“**获取 Kaspersky Endpoint Security中的设备访问权限**”。
4. 提示用户在 BitLocker 密码输入窗口中输入恢复密钥 ID，然后在“**恢复密钥 ID**”字段中对比该 ID。

   如果 ID 不匹配，该密钥无法用于恢复指定驱动器的访问。请确保选定计算机的名称与用户计算机的名称相符合。

5. 向用户发送“**恢复密钥**”字段中指定的密钥。



恢复对 BitLocker 加密的驱动器的访问权限

如何在 Web Console 和云控制台中查看 BitLocker 加密的非系统驱动器的恢复密钥

1. 在 Web Console 的主窗口中，选择“**操作**” → “**数据加密和保护**” → “**加密驱动器**”。
2. 选中要恢复其驱动器访问权限的计算机名称旁边的复选框。
3. 单击“**授予移动模式设备访问权限**”。

   这将启动用于授予设备访问权限的向导。

4. 按照向导的说明授予对设备的访问权限：

   a. 选择“**Kaspersky Endpoint Security for Windows**”插件

   b. 验证恢复密钥 ID。用户提供的 ID 必须与计算机设置中显示的 ID 匹配。

   如果 ID 不匹配，该密钥无法用于恢复指定系统驱动器的访问。请确保选定计算机的名称与用户计算机的名称相符合。

   c. 单击“**接收密钥**”。

结果，您将有权访问恢复密钥或恢复密钥文件，该密钥或密钥文件将需要传输给用户。

暂停 BitLocker 保护以更新软件

在更新操作系统、安装操作系统更新包或在启用 BitLocker 保护的情况下更新其他软件时，有许多特殊注意事项。安装更新可能需要多次重新启动计算机。每次重新启动后，用户必须完成 BitLocker 身份验证。要确保更新安装正确，可以暂时关闭 BitLocker 身份验证。在这种情况下，磁盘保持加密状态，用户在登录系统后可以访问数据。要管理 BitLocker 身份验证，您可以使用 *BitLocker 保护管理*任务。您可以使用此任务指定不需要 BitLocker 身份验证的计算机重启次数。这样，在安装更新且 *BitLocker 保护管理* 任务完成后，BitLocker 身份验证将自动启用。您可以随时启用 BitLocker 身份验证。

如何使用管理控制台 (MMC) 暂停 BitLocker 保护

1. 在 Kaspersky Security Center 管理控制台树中，选择“**任务**”。

   任务列表打开。

2. 单击“**新任务**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 选择任务类型

选择“**Kaspersky Endpoint Security for Windows (14.1)**”→ “**BitLocker 保护管理**”。

步骤2. BitLocker 保护管理

配置 BitLocker 身份验证。要暂停 BitLocker 保护，请选择“**临时允许跳过 BitLocker 身份验证**”，然后输入未经 BitLocker 身份验证的重新启动次数（1 到 15 次）。如有必要，请输入任务的到期日期和时间。在指定的时间，任务将自动关闭，并且用户必须在计算机重新启动时完成 BitLocker 身份验证。

步骤 3. 选择任务将分配到的设备

选择将要执行任务的计算机。下列选项可用：

- 将任务分配给管理组。在这种情况下，任务分配给先前创建的管理组中包括的计算机。
- 选择管理服务器在网络中检测到的计算机：*未分配设备*。特定设备可包括管理组中的设备以及未分配设备。
- 手动指定设备地址或从列表中导入地址。您可以指定您要将任务分配给的设备的 NetBIOS 名称、IP 地址和 IP 子网。

步骤 4. 定义任务名称

输入任务的名称，例如*更新到 Windows 10*。

步骤 5. 完成任务创建

退出向导。如有必要，选中“**向导完成时运行任务**”复选框。您可以在任务属性中监控任务进度。

如何使用 Web Console 暂停 BitLocker 保护

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**任务**”。
   任务列表打开。
2. 单击“**添加**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 配置常规任务设置

配置常规任务设置：

1. 在“**应用程序**”下拉列表中，选择“**Kaspersky Endpoint Security**”。
2. 在“**任务类型**”下拉列表中，选择“**BitLocker 保护管理**”。
3. 在“**任务名称**”字段中，输入简要说明，例如，“*更新到 Windows 10*”。
4. 在“**要对其分配任务的设备**”块，选择任务范围。

步骤2. BitLocker 保护管理

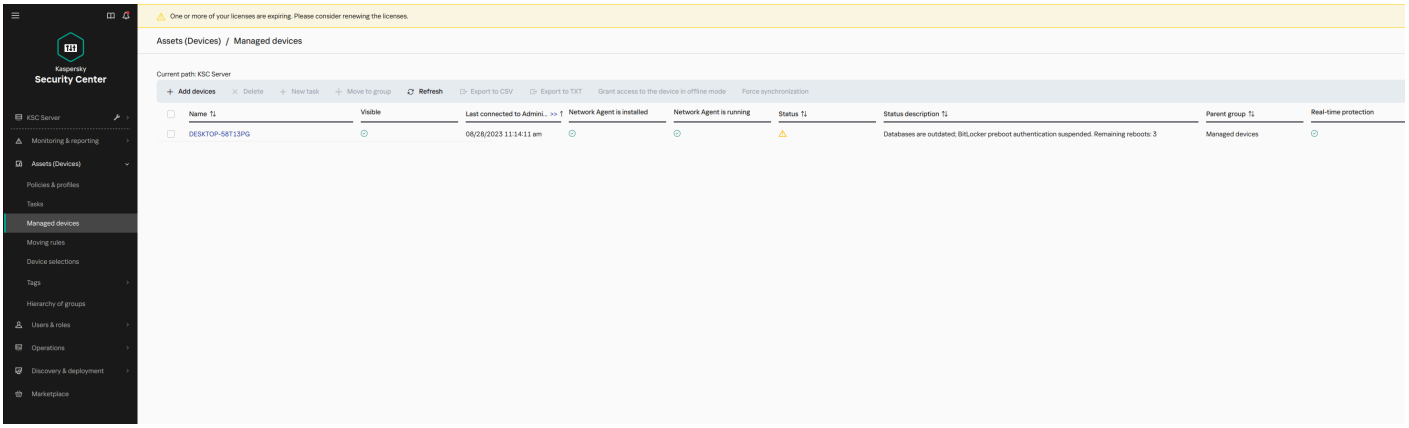
配置 BitLocker 身份验证。要暂停 BitLocker 保护，请选择“**临时允许跳过 BitLocker 身份验证**”，然后输入未经 BitLocker 身份验证的重新启动次数（1 到 15 次）。如有必要，请输入任务的到期日期和时间。在指定的时间，任务将自动关闭，并且用户必须在计算机重新启动时完成 BitLocker 身份验证。

步骤 3. 完成任务创建

退出向导。在任务列表中将显示一个新任务。

要运行任务，请选中与任务对应的复选框，然后单击“**开始**”按钮。

因此，当任务运行时，在下次重新启动计算机后，BitLocker 不会提示用户进行身份验证。每次在没有 BitLocker 身份验证的情况下重新启动计算机后，Kaspersky Endpoint Security 都会生成相应的事件并记录剩余的重新启动次数。Kaspersky Endpoint Security 然后将事件发送到 Kaspersky Security Center，由管理员进行监控。您还可以在 Kaspersky Security Center 控制台的“**受管理设备**”文件夹的设备状态描述中查看剩余的重新启动次数。



受管理设备列表

当达到指定的重新启动次数或任务到期时间时，BitLocker 身份验证将自动打开。要访问数据，用户必须完成 BitLocker 身份验证。

在运行 Windows 7 的计算机上，BitLocker 无法计算计算机重新启动的次数。Windows 7 计算机上的重新启动计数由 Kaspersky Endpoint Security 处理。因此，要在每次重新启动后自动启用 BitLocker 身份验证，必须启动 Kaspersky Endpoint Security。

要提前打开 BitLocker 身份验证，请打开“*BitLocker 保护管理*”任务属性，然后选择“**每次预启动时都请求身份验证**”。

本地计算机驱动器上的文件级加密

基于 Arm 架构的计算机不支持文件加密。

如果 Kaspersky Endpoint Security 安装在运行 Windows for Workstations 的计算机上，则该组件可用。如果 Kaspersky Endpoint Security 安装在运行 Windows for Servers 的计算机上，则该组件不可用。

文件加密具有以下特殊功能：

- Kaspersky Endpoint Security 仅为操作系统的本地用户配置文件加密/解密预定义文件夹内的文件。Kaspersky Endpoint Security 不会加密/解密预定义文件夹内的漫游用户配置文件、强制用户配置文件、临时用户配置文件或重定向的文件夹。
- Kaspersky Endpoint Security 不会加密其修改可能损害操作系统和安装的应用程序的文件。例如，加密排除项列表中包含的以下文件和包含所有嵌套文件夹在内的文件：
  - %WINDIR%；
  - %PROGRAMFILES% 和 %PROGRAMFILES(X86)%；
  - Windows 注册表文件。

  您无法查看或编辑这个加密排除项列表。尽管加密排除项列表中的文件和文件夹可以添加至加密列表，但在文件加密期间，它们不会被加密。

加密本地计算机磁盘驱动器上的文件

Kaspersky Endpoint Security 不会加密位于 OneDrive 云存储中的文件或以 OneDrive 作为名称的其他文件夹中的文件。如果加密文件未添加到解密规则中，Kaspersky Endpoint Security 还会阻止将加密文件复制到 OneDrive 文件夹。

若要在本地驱动器上加密文件，请执行以下操作：

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **数据加密** → **文件级加密**。
4. 在“**加密模式**”下拉列表中，选择“**根据规则**”。
5. 在“**加密**”选项卡下，单击“**添加**”按钮，在下拉列表中选择以下项目之一：
   a. 选择“**预定义文件夹**”项目将 Kaspersky 专家建议的本地用户配置文件文件夹的文件添加至加密规则。
      - “**文档**”。操作系统的“*文档*”文件夹及其子文件夹中的文件。
      - “**收藏夹**”。操作系统的标准“*收藏夹*”文件夹及其子文件夹中的文件。
      - “**桌面**”。操作系统的“*桌面*”文件夹及其子文件夹中的文件。

- “**临时文件**”。与计算机上安装的应用程序的操作有关的临时文件。例如，Microsoft Office 应用程序会创建包含文档备份副本的临时文件。

  > 不建议加密临时文件，因为这可能导致数据丢失。例如，Microsoft Word 在处理文档时创建临时文件。如果临时文件已加密，但原始文件未加密，则用户在尝试保存文档时可能会收到*访问被拒绝*错误。此外，Microsoft Word 可能会保存文件，但下次无法打开文档，即数据将丢失。

- “**Outlook 文件**”。与 Outlook 邮件客户端操作有关的文件：数据文件 (PST)、离线数据文件 (OST)、离线地址簿文件 (OAB) 和个人地址簿文件 (PAB)。

b. 选择“**自定义文件夹**”项目手动将文件夹路径输入至加密规则。

添加文件夹路径时，请遵循以下规则：

- 使用环境变量（例如，`%FOLDER%\UserFolder\`）。您只能在路径的开头使用一次环境变量。
- 不要使用相对路径。
- 不要使用 `*` 和 `?` 字符。
- 不要使用 UNC 路径。
- 使用 `;` 或 `,` 作为分隔符。

c. 选择“**按扩展名选择文件**”项目将单个文件扩展名添加至加密规则。Kaspersky Endpoint Security 将加密计算机的所有本地驱动器中具有指定扩展名的文件。

d. 选择“**按扩展名组选择文件**”项将成组的文件扩展名添加至加密规则（例如，*Microsoft Office 文档*）。Kaspersky Endpoint Security 会加密计算机上所有本地驱动器上扩展名组中列出扩展名的文件。

6. 保存更改。

一旦应用该策略，Kaspersky Endpoint Security 将加密所有加密规则中包括的和解密规则中不包括的文件。

文件加密具有以下特殊功能：

- 如果将同一文件添加到加密规则和解密规则中，则 Kaspersky Endpoint Security 将执行以下操作：
  - 如果文件未加密，则 Kaspersky Endpoint Security 不会对此文件进行加密。
  - 如果文件已加密，则 Kaspersky Endpoint Security 会解密此文件。
- 如果新文件符合加密规则的条件，则 Kaspersky Endpoint Security 会继续对这些文件进行加密。例如，当您更改未加密文件的属性（路径或扩展名）时，该文件将符合加密规则的条件。Kaspersky Endpoint Security 将对该文件进行加密。
- 当用户创建其属性复合加密规则条件的新文件时，Kaspersky Endpoint Security 将在文件打开时加密文件。
- Kaspersky Endpoint Security 将会推迟加密已打开的文件，直至其关闭。
- 如果您在本地驱动器上将加密文件移动至另一个文件夹，该文件仍保持为加密状态，而与该文件夹是否包含在加密规则中无关。
- 如果您解密文件并将其复制到解密规则中未包含的另一个本地文件夹中，则可能会对该文件的副本进行加密。要防止对复制的文件进行加密，请为目标文件夹创建解密规则。

为应用程序创建加密文件访问规则

默认情况下，所有应用程序都以解密状态处理加密文件。如果您经常使用某些应用程序（例如，浏览器或文本编辑器），您可以创建加密文件访问规则来保护信息。

> 我们建议为 Microsoft Internet Explorer 和 Microsoft Edge 浏览器创建加密文件访问规则。由于这些浏览器的工作方式，如果您将加密文件上传到网站（例如，云存储），该文件会自动解密。这可能会导致数据泄露。无法使用这些浏览器上传加密文件。我们建议设置“**仅授权访问采用密文格式加密的文件**”规则。您不需要为其他浏览器（例如 Google Chrome）创建规则。

要为应用程序创建加密文件访问规则：

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **数据加密** → **文件级加密**。
4. 在“**加密模式**”下拉列表中，选择“**根据规则**”。

   > 访问规则仅在“**根据规则**”模式下可以应用。在“**根据规则**”模式下应用访问规则后，如果您切换到“**保留不变**”模式，则 Kaspersky Endpoint Security 将忽略所有访问规则。所有应用程序将能够访问所有加密文件。

5. 在窗口右侧，选择“**应用程序规则**”选项卡。
6. 如果您只希望从 Kaspersky Security Center 列表中选择应用程序，则单击“**添加**”按钮并在下拉列表中选择“**Kaspersky Security Center 应用程序列表**”项目。

   a. 指定过滤条件以缩小表中的应用程序列表。若要执行操作，指定“**应用程序**”、“**提供商**”和“**添加的时间段**”参数的值和“**组**”块中所有复选框。

   b. 单击“**刷新**”。

   c. 列表将列出匹配所应用过滤条件的应用程序。

   d. 在“**应用程序**”列中，选择您要为其创建加密文件访问规则的应用程序旁边的复选框。

   e. 在“**应用程序规则**”下拉列表中，选择确定应用程序对加密文件访问权限的规则。

   f. 在“**先前为应用程序选定的操作**”下拉列表中，选择根据先前为此类应用程序所创建加密文件访问规则 Kaspersky Endpoint Security 所执行的操作。

   应用程序加密文件访问规则的详情将显示在“**应用程序规则**”选项卡中。

7. 如果您希望手动选择应用程序，则单击“**添加**”按钮并在下拉列表中选择“**自定义应用程序**”项目。

   a. 在输入字段中，输入应用程序可执行文件的名称或名称列表，包括其扩展名。

      您也可以从 Kaspersky Security Center 列表中添加应用程序可执行文件的名称，请单击“**从 Kaspersky Security Center 列表添加**”按钮。

b. 如有必要，在“**描述**”字段中输入应用程序列表的说明。

c. 在“**应用程序规则**”下拉列表中，选择确定应用程序对加密文件访问权限的规则。

应用程序加密文件访问规则的详情将显示在“**应用程序规则**”选项卡中。

8. 保存更改。

加密特定应用程序创建或修改的文件

您可以创建规则，Kaspersky Endpoint Security 将加密该规则内指定的应用程序创建或修改的文件。

加密规则应用前指定应用程序创建或修改的文件将不会被加密。

若要加密特定应用程序创建或修改的文件：

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **数据加密** → **文件级加密**。
4. 在“**加密模式**”下拉列表中，选择“**根据规则**”。

   加密规则仅在“**根据规则**”模式下可以应用。在“**根据规则**”模式下应用加密规则后，如果您切换到“**保留不变**”模式。Kaspersky Endpoint Security 将忽略所有加密规则。先前加密的文件将保持为加密。

5. 在窗口右侧，选择“**应用程序规则**”选项卡。
6. 如果您只希望从 Kaspersky Security Center 列表中选择应用程序，则单击“**添加**”按钮并在下拉列表中选择“**Kaspersky Security Center 应用程序列表**”项目。

   a. 指定过滤条件以缩小表中的应用程序列表。若要执行操作，指定“**应用程序**”、“**提供商**”和“**添加的时间段**”参数的值和“**组**”块中所有复选框。

   b. 单击“**刷新**”。

   列表将列出匹配所应用过滤条件的应用程序。

   c. 在“**应用程序**”列中，选中您要加密其创建的文件的应用程序旁边的复选框。

   d. 在“**应用程序规则**”下拉列表中，选择“**加密所有已创建的文件**”。

   e. 在“**先前为应用程序选定的操作**”下拉列表中，选择根据先前为此类应用程序所创建文件加密规则 Kaspersky Endpoint Security 所执行的操作。

选定应用程序创建或修改的文件的加密规则的信息将显示在“**应用程序规则**”选项卡中的表中。

7. 如果您希望手动选择应用程序，则单击“**添加**”按钮并在下拉列表中选择“**自定义应用程序**”项目。

   a. 在输入字段中，输入应用程序可执行文件的名称或名称列表，包括其扩展名。

      您也可以从 Kaspersky Security Center 列表中添加应用程序可执行文件的名称，请单击“**从 Kaspersky Security Center 列表添加**”按钮。

   b. 如有必要，在“**描述**”字段中输入应用程序列表的说明。

   c. 在“**应用程序规则**”下拉列表中，选择“**加密所有已创建的文件**”。

   选定应用程序创建或修改的文件的加密规则的信息将显示在“**应用程序规则**”选项卡中的表中。

8. 保存更改。

生成解密规则

若要生成解密规则：

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **数据加密** → **文件级加密**。

4. 在“**加密模式**”下拉列表中，选择“**根据规则**”。

5. 在“**解密**”选项卡下，单击“**添加**”按钮，在下拉列表中选择以下项目之一：

   a. 选择“**预定义文件夹**”项目将 Kaspersky 专家建议的本地用户配置文件文件夹的文件添加至解密规则。

   b. 选择“**自定义文件夹**”项目手动将文件夹路径输入至解密规则。

   c. 选择“**按扩展名选择文件**”项目将单个文件扩展名添加至解密规则。Kaspersky Endpoint Security 不会加密计算机的所有本地驱动器中具有指定扩展名的文件。

   d. 选择“**按扩展名组选择文件**”项将成组的文件扩展名添加至解密规则（例如，*Microsoft Office 文档*）。Kaspersky Endpoint Security 不会加密计算机的所有本地驱动器上扩展名组中列出扩展名的文件。

6. 保存更改。

如果同一个的文件被添加至加密规则和解密规则中，Kaspersky Endpoint Security 不会加密已加密的文件，但是会解密已经加密的文件。

在本地计算机磁盘驱动器上解密文件

若要在本地驱动器上解密文件，请执行以下操作：

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **数据加密** → **文件级加密**。
4. 在窗口右侧，选择“**加密**”选项卡。
5. 从加密列表中卸载您要解密的文件和文件夹。若要执行操作，请选择文件，然后在“**删除**”按钮的上下文菜单中选择“**删除规则并解密文件**”项。

   从加密列表中删除的文件和文件夹将自动添加至解密列表中。
6. 创建文件解密列表。
7. 保存更改。

应用策略后，Kaspersky Endpoint Security 将会解密被添加至解密列表的已加密文件。

如果未加密文件的参数（文件路径/文件名/文件扩展名）已更改为匹配已添加至解密列表的对象的参数时，Kaspersky Endpoint Security 将会解密这些加密文件。

Kaspersky Endpoint Security 将会推迟解密已打开的文件，直至其关闭。

创建加密数据包

在将文件发送给公司网络外部的用户时，为了保护您的数据，可以使用加密数据包。由于电子邮件客户端具有文件大小限制，因此使用加密数据包可以方便地通过可移动驱动器传输大文件。

在创建加密数据包之前，Kaspersky Endpoint Security 将提示用户输入密码。为了可靠地保护数据，您可以启用密码强度检查并指定密码强度要求。这将防止用户使用短密码和简单密码，例如 1234。

在管理控制台 (MMC) 中创建加密存档时如何启用密码强度检查

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **数据加密** → **通用加密设置**。
4. 在“**密码设置**”块中单击“**设置**”按钮。
5. 这将打开一个窗口；在该窗口中，选择“**加密数据包**”选项卡。
6. 在创建加密数据包时配置密码复杂性设置。

在 Web Console 中创建加密存档时如何启用密码强度检查

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **数据加密** → **文件级加密**。
5. 在“**加密数据包密码设置**”块，配置创建加密包所需的密码强度标准。

您可以在安装了 Kaspersky Endpoint Security 且具有文件级加密功能的计算机上创建加密数据包。

> 向其内容位于 OneDrive 云存储中的加密数据包中添加文件时，Kaspersky Endpoint Security 会下载文件内容并执行加密。

若要创建加密数据包，请执行以下操作：

1. 在任意文件管理器中，选择要添加到加密数据包的文件或文件夹。右键单击以打开其上下文菜单。
2. 在上下文菜单中，选择“**新建加密数据包**”（请参见下图）。

创建加密数据包

3. 在打开的窗口中，指定密码并确认。
   密码必须符合策略中指定的复杂性标准。
4. 单击“**创建**”。

   加密数据包创建过程将启动。Kaspersky Endpoint Security 创建加密数据包时不会执行文件压缩。该过程完成后，将在选定的目标文件夹中创建一个受密码保护的自解压加密数据包（扩展名为 .exe 的可执行文件 – ）。

要访问加密数据包中的文件，请双击它以启动解压缩向导，然后输入密码。如果忘记或丢失密码，将无法恢复密码和访问加密数据包中的文件。您可以重新创建加密数据包。

还原对加密文件的访问权限

加密文件后，Kaspersky Endpoint Security 会收到直接访问加密文件所需的加密密钥。如果用户在文件加密过程中处于活动状态的任何 Windows 帐户下工作，则可以使用该加密密钥直接访问加密文件。如果用户在文件加密过程中处于非活动状态的 Windows 帐户下工作，则必须连接至 Kaspersky Security Center 才能访问加密文件。

在以下情况下可能无法访问加密文件：

- 用户计算机上存储了加密密钥，但是未连接 Kaspersky Security Center 以管理这些加密密钥。在这种情况下，用户必须从局域网管理员处请求加密文件访问权限。

  如果不存在对 Kaspersky Security Center 的访问权限，您必须：

  - 请求访问密钥以访问计算机硬盘驱动器上的加密文件；
  - 若要访问可移动驱动器上所存储的加密文件，请为每个可移动驱动器上加密的文件请求单独的访问密钥。

- 加密组件被从用户计算机上删除。在此情况下，用户可以打开本地和移动磁盘上的加密文件，但是文件内容将显示为加密。

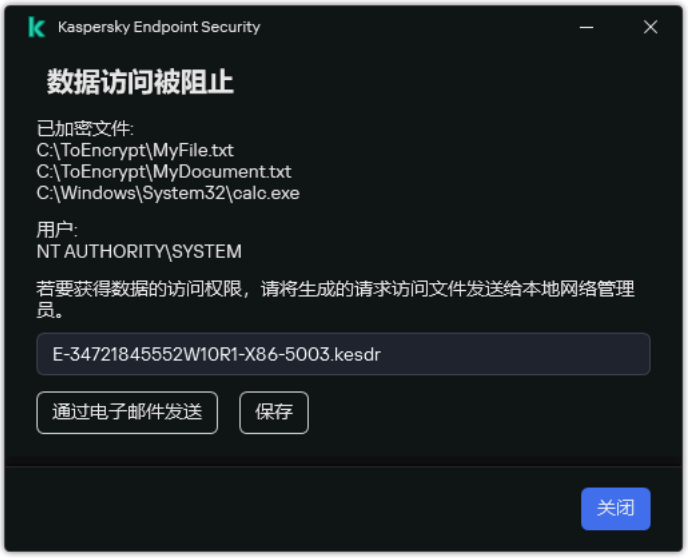
  在以下情况下，用户可以使用加密文件：

  - 文件放置在创建于安装了 Kaspersky Endpoint Security 的计算机上的 加密数据包 里。
  - 文件储存在允许 便携模式 的可移动驱动器上。

要获得对加密文件的访问权限，用户需要启动恢复过程（请求-响应）。

恢复对加密文件的访问权限包括以下步骤：

1. 用户将请求访问文件发送给管理员（请参见下图）。
2. 管理员将请求访问文件添加到 Kaspersky Security Center 中，创建访问密钥文件并将该文件发送给用户。
3. 用户将访问密钥文件添加到 Kaspersky Endpoint Security 并获得对文件的访问权限。



还原对加密文件的访问权限

要启动恢复过程，用户需要尝试访问文件。结果，Kaspersky Endpoint Security 将创建一个请求访问文件（扩展名为 KESDC 的文件），用户需要将该文件发送给管理员，例如通过电子邮件发送。

Kaspersky Endpoint Security 生成请求访问文件，该文件用于访问存储在计算机驱动器（本地驱动器或可移动驱动器）上的所有加密文件。

如何在管理控制台 (MMC) 中获取加密数据访问密钥文件

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**设备**”。
3. 在“**设备**”选项卡上，选择用户正在请求加密数据访问权限的计算机，然后单击鼠标右键打开上下文菜单。
4. 在上下文菜单中，选择“**授予离线模式下的访问权限**”。
5. 这将打开一个窗口；在该窗口中，选择“**数据加密**”选项卡。
6. 在“**数据加密**”选项卡上单击“**浏览**”按钮。
7. 在用于选择请求访问文件的窗口中，指定从用户处接收的文件的路径。

您将看到有关用户请求的信息。Kaspersky Security Center 会生成一个密钥文件。通过电子邮件将生成的加密数据访问密钥文件发送给用户。或保存该访问文件并使用任何可用方法来传输该文件。

在移动模式下授予访问权限

如何在 Web Console 中获取加密数据访问密钥文件

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**资产(设备)**”。
2. 选中要还原其数据访问权限的计算机名称旁边的复选框。
3. 单击“**授予移动模式设备访问权限**”。
4. 选择“**数据加密**”。
5. 单击“**选择文件**”按钮，然后选择从用户处收到的请求访问文件（扩展名为 KESDC 的文件）。
   Web Console 将显示有关请求的信息。这将包括用户请求访问的文件所在的计算机的名称。
6. 单击“**保存密钥**”按钮，然后选择一个文件夹来保存加密数据访问密钥文件（扩展名为 KESDR 的文件）。

结果，您将能够获取加密数据访问密钥，您需要将该密钥传输给用户。

收到加密数据访问密钥文件后，用户需要双击来运行该文件。结果，Kaspersky Endpoint Security 将授予对驱动器上存储的所有加密文件的访问权限。要访问其他驱动器上存储的加密文件，您必须为每个驱动器获取单独的访问密钥文件。

操作系统故障后恢复对加密数据的访问

只有使用了文件级加密 (FLE) 时，才能在操作系统故障后恢复对数据的访问。如果使用了完整磁盘加密 (FDE)，则无法恢复对数据的访问。

要在操作系统故障后恢复对加密数据的访问：

1. 不格式化硬盘驱动器的情况下重新安装操作系统。
2. 安装 Kaspersky Endpoint Security。
3. 在计算机与数据被加密时控制计算机的 Kaspersky Security Center 管理服务器之间建立连接。

   授予加密数据访问权限的条件与操作系统发生故障之前适用的条件相同。

编辑加密文件访问消息模板

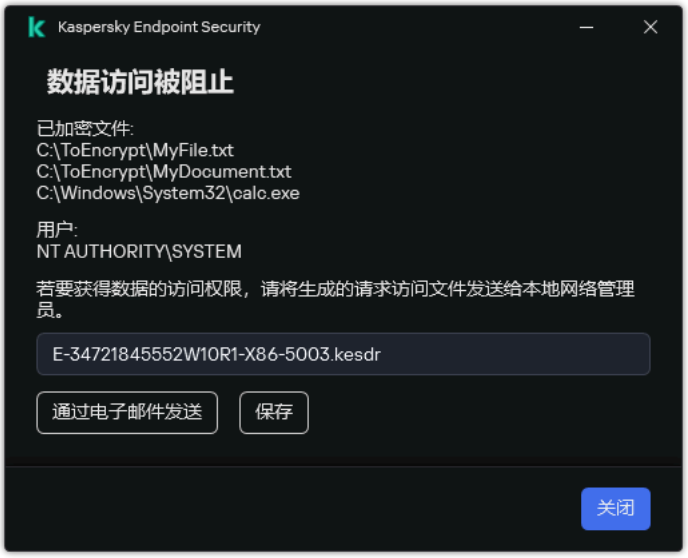
若要编辑加密文件访问消息模板，请执行以下操作：

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **数据加密** → **通用加密设置**。
4. 在“**模板**”块中单击“**模板**”按钮。
5. 在打开的窗口中，做以下事项：
   - 如果您希望编辑用户邮件模板，则选择“**用户消息**”选项卡。当用户计算机上没有用于访问加密文件的可用密钥时，如果用户试图访问加密文件，以下窗口将开启。点击“**通过电子邮件发送**”按钮自动创建一条用户消息。该邮件会将请求访问加密文件访问权限的文件一起发送给公司局域网管理员。
   - 如果您希望编辑管理员邮件模板，则选择“**管理员消息**”选项卡。授予对加密文件的访问权限后，用户会收到此消息。
6. 编辑消息模板。

   要将变量添加到模板文本中，请将光标放在所需的位置，单击“**变量**”，然后从可用选项列表中选择所需的变量。

   您还可以使用“**默认**”按钮恢复默认模板文本。

7. 保存更改。



还原对加密文件的访问权限

可移动驱动器加密

基于 Arm 架构的计算机不支持对可移动驱动器加密。

如果 Kaspersky Endpoint Security 安装在运行 Windows for Workstations 的计算机上，则该组件可用。如果 Kaspersky Endpoint Security 安装在运行 Windows for Servers 的计算机上，则该组件不可用。

Kaspersky Endpoint Security 支持加密 FAT32 和 NTFS 文件系统中的文件。如果将具有不支持的文件系统的可移动驱动器连接到计算机，对该可移动驱动器的加密任务将以出错结束，Kaspersky Endpoint Security 会为该可移动驱动器分配只读状态。

要保护可移动驱动器上的数据，可以使用以下类型的加密：

- Full Disk Encryption (FDE)。

  加密整个可移动驱动器，包括文件系统。

  无法在公司网络外部访问加密数据。如果计算机未连接到 Kaspersky Security Center（例如，“来宾”计算机），也无法访问公司网络内部的加密数据。

- File Level Encryption (FLE)。

  仅加密可移动驱动器上的文件。文件系统保持不变。

  可移动驱动器上的文件加密使用一种称为*便携模式*的特殊模式提供了访问公司网络外部数据的功能。

在加密期间，Kaspersky Endpoint Security 会创建一个主密钥。Kaspersky Endpoint Security 将主密钥保存在以下存储库中：

- Kaspersky Security Center。
- 用户的计算机。
  主密钥使用用户的密钥加密。
- 可移动驱动器。
  主密钥使用 Kaspersky Security Center 的公钥加密。

加密完成后，可在公司网络内访问可移动驱动器上的数据，就像数据在普通的未加密可移动驱动器上一样。

访问加密数据

连接带有加密数据的可移动驱动器后，Kaspersky Endpoint Security 执行以下操作：

1. 检查用户计算机的本地存储中的主密钥。
   如果找到主密钥，用户将获得可移动驱动器上的数据的访问权限。
   如果找不到主密钥，Kaspersky Endpoint Security 会执行以下操作：
   a. 向 Kaspersky Security Center 发送请求。
      收到请求后，Kaspersky Security Center 将发送一个包含主密钥的响应。
   b. Kaspersky Endpoint Security 将主密钥保存在用户计算机的本地存储中，以供以后对加密的可移动驱动器进行操作。
2. 解密数据。

可移动驱动器加密的特殊功能

可移动驱动器加密具有以下特殊功能：

- 已经为指定受管理计算机组形成了针对可移动驱动器加密的带有预设设置的策略。因此，应用为加密/解密可移动驱动器配置的 Kaspersky Security Center 策略的结果取决于可移动驱动器连接到的计算机。
- Kaspersky Endpoint Security 不会加密/解密可移动驱动器上存储的只读文件。
- 支持以下设备类型的可移动驱动器：
  - 通过 USB 总线连接的数据媒体
  - 通过 USB 和 FireWire 总线连接的硬盘磁盘驱动器
  - 通过 USB 和 FireWire 总线连接的 SSD 磁盘驱动器

启动可移动驱动器加密

您可以使用策略来解密可移动驱动器。将为特定管理组生成具有已定义的可移动驱动器加密设置的策略。因此，可移动驱动器上的数据解密结果取决于其所连接的计算机。

Kaspersky Endpoint Security 支持加密 FAT32 和 NTFS 文件系统中的文件。如果将具有不支持的文件系统的可移动驱动器连接到计算机，对该可移动驱动器的加密任务将以出错结束，Kaspersky Endpoint Security 会为该可移动驱动器分配只读状态。

在加密可移动驱动器上的文件之前，请确保它已格式化并且没有隐藏分区（例如 EFI 系统分区）。如果驱动器包含未格式化或隐藏的分区，文件加密可能会失败并出现错误。

若要加密可移动驱动器，请执行以下操作：

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **数据加密** → **可移动驱动器加密**。
4. 在“**加密模式**”下拉列表中，选择您希望 Kaspersky Endpoint Security 对可移动驱动器执行的默认操作：
   - **加密整个可移动驱动器** (FDE)。Kaspersky Endpoint Security 逐个扇区加密可移动驱动器的内容。因此，应用程序不仅会加密可移动驱动器中存储的文件，还会加密其文件系统，包括可移动驱动器上的文件名和文件夹结构。
   - **加密所有文件** (FLE)。Kaspersky Endpoint Security 会加密可移动驱动器中存储的所有文件。应用程序不会加密可移动驱动器的文件系统，包括文件名和文件夹结构。
   - **仅加密新文件** (FLE)。Kaspersky Endpoint Security 只加密已添加到可移动驱动器的文件或者存储在可移动驱动器中并且在上次应用 Kaspersky Security Center 策略后已修改的文件。

   Kaspersky Endpoint Security 不会对已经加密的可移动驱动器进行加密。

5. 如果要使用便携模式对可移动驱动器进行加密，请选中“**便携模式**”复选框。

   *便携模式*是可移动驱动器上的文件加密 (FLE) 模式，它提供了访问公司网络外部数据的能力。便携模式还允许您在未安装 Kaspersky Endpoint Security 的计算机上使用加密数据。

6. 如果要加密新的可移动驱动器，建议选中“**仅加密使用的磁盘空间**”复选框。如果清除该复选框，Kaspersky Endpoint Security 将加密所有文件，包括已删除或已修改文件的残留片段。
7. 如果要配置对单个可移动驱动器的加密，请定义加密规则。
8. 如果要在离线模式下使用可移动驱动器的完整磁盘加密，请选择中“**允许在离线模式下加密可移动驱动器**”复选框。

   *离线加密模式*是指未连接 Kaspersky Security Center 时加密可移动驱动器 (FDE)。在加密过程中，Kaspersky Endpoint Security 只将主密钥保存在用户的计算机上。Kaspersky Endpoint Security 将在下次同步期间将主密钥发送到 Kaspersky Security Center。

如果保存主密钥的计算机损坏，并且数据未发送到 Kaspersky Security Center，则无法访问可移动驱动器。

如果清除“**允许在离线模式下加密可移动驱动器**”复选框，并且未连接到 Kaspersky Security Center，则无法进行可移动驱动器加密。

9. 保存更改。

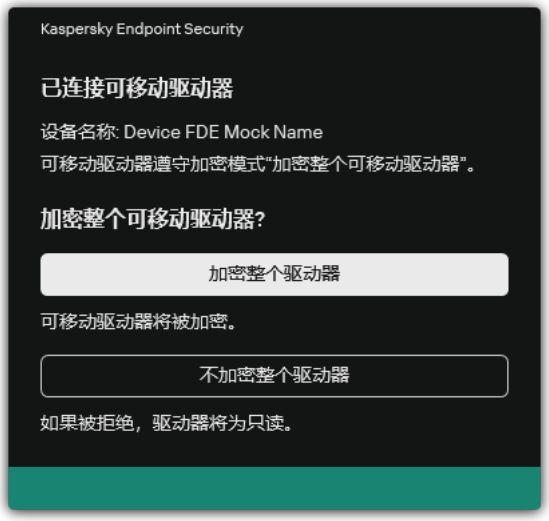
应用策略后，当用户连接可移动驱动器或可移动驱动器已连接时，Kaspersky Endpoint Security 会提示用户确认执行加密操作（请参见下图）。

应用程序允许您执行以下操作：

- 如果用户确认加密请求，Kaspersky Endpoint Security 将加密数据。
- 如果用户拒绝加密请求，Kaspersky Endpoint Security 将保留数据不变，并为该可移动驱动器分配只读访问权限。
- 如果用户未响应加密请求，Kaspersky Endpoint Security 将保留数据不变，并为该可移动驱动器分配只读访问权限。随后应用策略或下次连接该可移动驱动器时，应用程序将再次提示确认。

如果在数据加密期间，用户安全移除可移动驱动器，Kaspersky Endpoint Security 将会在加密过程完成前中断数据加密过程，允许移除可移动驱动器。下次将可移动驱动器连接到此计算机时，将继续数据加密。

如果对可移动驱动器的加密失败，请在 Kaspersky Endpoint Security 界面中查看“**数据加密**”报告。对文件的访问可能被其他应用程序阻止。在这种情况下，请尝试从计算机上拔下可移动驱动器，然后重新连接。



可移动驱动器加密请求

为可移动驱动器添加加密规则

若要为可移动驱动器添加加密规则，请执行以下操作：

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **数据加密** → **可移动驱动器加密**。
4. 单击“**添加**”按钮并在下拉列表中选择以下项目之一：
   - 如果您希望为设备控制组件的受信任设备列表中的可移动磁盘添加加密规则，则选择“**从此策略的受信任设备列表**”。
   - 如果您希望为 Kaspersky Security Center 列表中的可移动磁盘添加加密规则，则选择“**从 Kaspersky Security Center 设备列表**”。
5. 在“**选定设备的加密模式**”下拉列表中，选择 Kaspersky Endpoint Security 对选定可移动驱动器上文件执行的操作。
6. 如果您希望 Kaspersky Endpoint Security 在加密前准备可移动驱动器，请选择“**便携模式**”复选框，这将能够在便携模式中使用上面存储的加密文件。

   便携模式使您可以在存有加密文件的可移动驱动器连接至没有加密功能的计算机时能够访问可移动驱动器中的加密文件。
7. 如果您希望 Kaspersky Endpoint Security 只加密包含有文件的磁盘扇区，则选择“**仅加密使用的磁盘空间**”复选框。

   如果您在已使用的磁盘上应用加密，建议加密整个磁盘。这将确保所有数据受到保护 – 即使删除了可能仍包含可检索信息的数据。建议为先前未使用的新磁盘使用“**仅加密使用的磁盘空间**”功能。

   > 如果先前使用“**仅加密使用的磁盘空间**”功能加密了设备，则在“**加密整个可移动驱动器**”模式中应用策略，未包含文件的扇区将不会被加密。
8. 在“**先前为该设备选定的操作**”下拉列表中，选择根据先前为可移动驱动器所创建加密文件访问规则 Kaspersky Endpoint Security 所执行的操作：
   - 如果您希望先前为可移动磁盘创建的加密规则不变，则选择“**跳过**”。
   - 如果您希望先前为可移动驱动器创建的加密规则由新规则代替，则选择“**刷新**”。
9. 保存更改。

所添加的可移动驱动器加密规则将应用于连接到组织中任何计算机的可移动驱动器。

为可移动驱动器导出和导入加密规则列表

您可以将可移动应用程序加密规则列表导出到 XML 文件。然后可以修改文件，例如，添加大量相同类型可移动驱动器的规则。还可以使用导出/导入功能备份规则列表或将规则迁移到其他服务器。

如何在管理控制台(MMC)中导出和导入可移动驱动器加密规则列表

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **数据加密** → **可移动驱动器加密**。

5. 在“**选定设备的加密规则**”区域，单击“**<N> 个规则**”链接。
   这将打开可移动驱动器加密规则列表。

6. 要导出可移动驱动器加密规则列表：

   a. 选择您要导出的规则。

   b. 单击“**导出**”。

   c. 确认您仅想导出所选规则，或导出整个列表。

   d. 保存文件。
      Kaspersky Endpoint Security 导出规则列表到默认下载文件夹中的 XML 文件。

7. 要导入规则列表：

   a. 单击**导入**链接。
      在打开的窗口中，选择要从中导入规则列表的 XML 文件。

   b. 打开文件。
      如果计算机已经具有规则的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 XML 文件向其中添加新条目。

8. 保存更改。

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **数据加密** → **可移动驱动器加密**。

4. 要导出可移动驱动器加密规则列表：

   a. 选择您要导出的规则。要选择多个端口，使用 **CTRL** 或 **SHIFT** 键。
      如果您未选择任何规则，Kaspersky Endpoint Security 将导出所有规则。

   b. 单击**导出**链接。

   c. 在打开的窗口中，指定您要将规则列表导出到的 XML 文件的名称，然后选择要保存此文件的文件夹。

   d. 保存文件。
      Kaspersky Endpoint Security 会将整个规则列表导出到 XML 文件。

5. 要导入可移动驱动器加密规则列表：

   a. 单击**导入**链接。

      在打开的窗口中，选择要从中导入规则列表的 XML 文件。

   b. 打开文件。

      如果计算机已经具有规则的列表，则 Kaspersky Endpoint Security 将提示您删除现有列表或从 XML 文件向其中添加新条目。

6. 保存更改。

用于访问可移动驱动器上的加密文件的便携模式

*便携模式*是可移动驱动器上的文件加密 (FLE) 模式，它提供了访问公司网络外部数据的能力。便携模式还允许您在未安装 Kaspersky Endpoint Security 的计算机上使用加密数据。

便携模式在以下情况下便于使用：

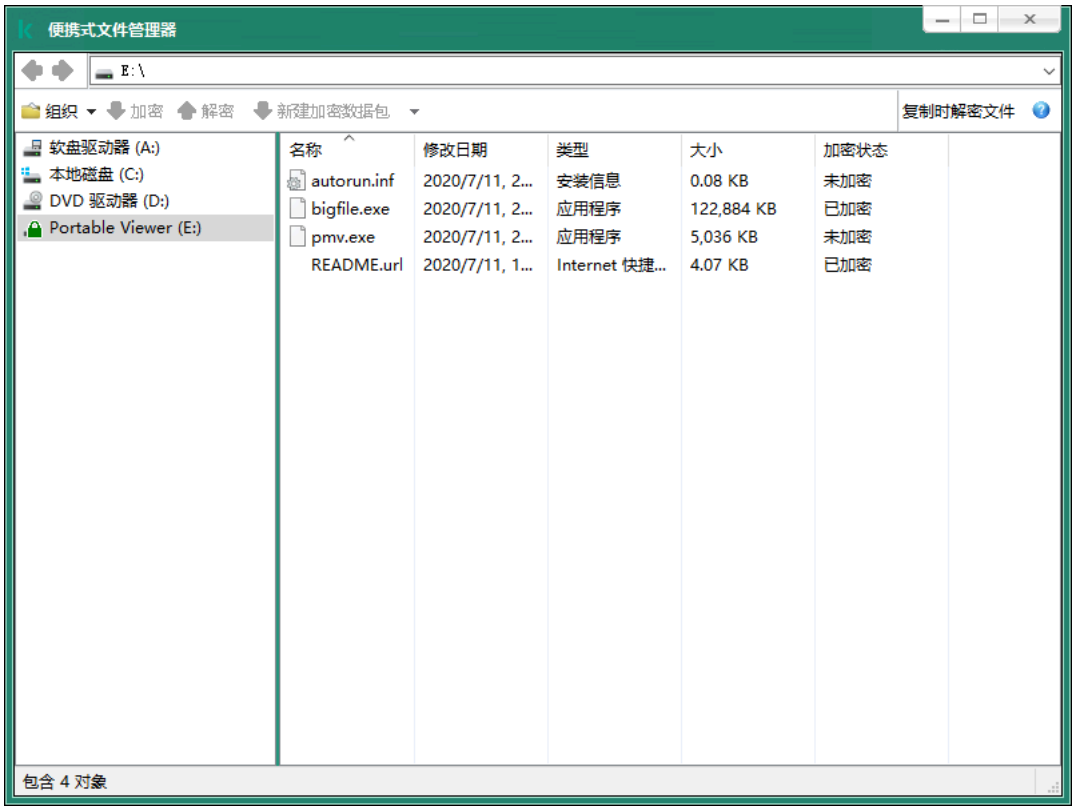
- 计算机和 Kaspersky Security Center 管理服务器之间没有连接。
- 基础结构已随着 Kaspersky Security Center 管理服务器的更改而发生变化。
- 计算机上未安装 Kaspersky Endpoint Security。

便携式文件管理器

为了在便携模式下工作，Kaspersky Endpoint Security 会在可移动驱动器上安装一个名为“*便携式文件管理器*”的特殊加密模块。如果计算机上未安装 Kaspersky Endpoint Security，便携式文件管理器提供了一个处理加密数据的界面（请参见下图）。如果计算机上安装了 Kaspersky Endpoint Security，则可以使用通常的文件管理器（例如资源管理器）使用加密的可移动驱动器。

便携式文件管理器会存储用于加密可移动驱动器上的文件的密钥。该密钥使用用户密码加密。用户在加密可移动驱动器上的文件之前先设置密码。

当可移动驱动器连接到未安装 Kaspersky Endpoint Security 的计算机时，便携式文件管理器会自动启动。如果计算机上已禁用自动启动应用程序，请手动启动便携式文件管理器。要执行此操作，请运行可移动驱动器上存储的名为 pmv.exe 的文件。



便携式文件管理器

支持便携模式以处理加密文件

如何在管理控制台 (MMC) 中启用便携模式支持以处理可移动驱动器上的加密文件

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **数据加密** → **可移动驱动器加密**。
4. 在**选定设备的加密模式**下拉列表中，选择**加密所有文件**或**仅加密新文件**。

   便携模式仅适用于文件级加密 (FLE)。无法为完整磁盘加密 (FDE) 启用便携模式支持。

5. 选择**便携模式**复选框。
6. 如有必要，为单个可移动驱动器添加加密规则。
7. 保存更改。

8. 应用策略后，将可移动驱动器连接到计算机。

9. 确认可移动驱动器加密操作。
   这会打开一个窗口，您可以在其中为便携式文件管理器创建密码。

便携式模式密码请求

10. 指定满足强度要求的密码并确认。

11. 保存更改。

如何在 Web Console 中启用便携模式支持以处理可移动驱动器上的加密文件

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **数据加密** → **可移动驱动器加密**。

5. 在“**默认操作**”块中，选择“**加密所有文件**”或“**仅加密新文件**”。

   > 便携模式仅适用于文件级加密 (FLE)。无法为完整磁盘加密 (FDE) 启用便携模式支持。

6. 选择**便携模式**复选框。

7. 如有必要，为单个可移动驱动器添加加密规则。

8. 保存更改。

9. 应用策略后，将可移动驱动器连接到计算机。

10. 确认可移动驱动器加密操作。

这会打开一个窗口，您可以在其中为便携式文件管理器创建密码。

便携式模式密码请求

11. 指定满足强度要求的密码并确认。

12. 保存更改。

Kaspersky Endpoint Security 将加密可移动驱动器上的文件。用来操作加密文件的便携式文件管理器也将被添加到可移动驱动器。如果可移动驱动器上已经有加密文件，Kaspersky Endpoint Security 将使用自己的密钥再次对其进行加密。这允许用户在便携模式下访问可移动驱动器上的所有文件。

访问可移动驱动器上的加密文件

在便携模式支持下加密可移动驱动器上的文件后，可以使用以下文件访问方法：

- 如果计算机上未安装 Kaspersky Endpoint Security，则便携式文件管理器将提示您输入密码。每次重新启动计算机或重新连接可移动驱动器时，都需要输入密码。
- 如果计算机位于公司网络外部，并且计算机上已安装 Kaspersky Endpoint Security，则应用程序将提示您输入密码或向管理员发送访问文件的请求。获得对可移动驱动器上文件的访问权限后，Kaspersky Endpoint Security 会将密钥保存在计算机的密钥存储中。这样在将来无需输入密码或询问管理员即可访问文件（参见下图）。
- 如果计算机位于公司网络内部，并且计算机上已安装 Kaspersky Endpoint Security，则无需输入密码即可访问设备。Kaspersky Endpoint Security 将从与计算机连接的 Kaspersky Security Center 管理服务器接收密钥。

访问可移动驱动器上的加密文件

恢复在便携模式下工作的密码

如果您忘记了在便携模式下工作的密码，则需要将可移动驱动器与公司网络内安装了 Kaspersky Endpoint Security 的计算机连接。您将获得文件访问权限，因为密钥存储在计算机的密钥存储或管理服务器中。使用新密码解密和重新加密文件。

将可移动驱动器连接到其他网络中的计算机时，便携模式的功能

如果计算机位于公司网络外部，并且计算机上已安装 Kaspersky Endpoint Security，您可以通过以下方式访问文件：

- **基于密码进行访问**

  输入密码后，您将能够查看、修改并将文件保存在可移动驱动器上（*透明访问*）。如果在可移动驱动器的加密策略设置中配置以下参数，Kaspersky Endpoint Security 可以为可移动驱动器设置只读访问权限：

  - 便携模式支持已禁用。
  - 选择了“**加密所有文件**”或“**仅加密新文件**”模式。

  在所有其他情况下，您将获得对可移动驱动器的完全访问权限（读/写权限）。您将能够添加和删除文件。

  即使可移动驱动器连接到计算机时，您也可以更改可移动驱动器访问权限。如果更改可移动驱动器访问权限，Kaspersky Endpoint Security 将阻止对文件的访问，并再次提示您输入密码。

  输入密码后，您无法对可移动驱动器应用加密策略设置。在这种情况下，无法对可移动驱动器上的文件进行解密或重新加密。

- **请管理员提供文件访问权限**

  如果您忘记了在便携模式下工作的密码，则请管理员提供文件访问权限。要访问文件，用户需要向管理员发送请求访问文件（扩展名为 KESDC 的文件）。例如，用户可以通过电子邮件发送请求访问文件。管理员将发送加密数据访问文件（扩展名为 KESDR 的文件）。

  完成请求-响应密码恢复过程之后，您将获得对可移动驱动器上的文件的透明访问权限，以及对可移动驱动器的完全访问权限（读/写权限）。

  例如，您可以应用可移动驱动器加密策略并解密文件。在恢复密码后或在更新策略后，Kaspersky Endpoint Security 将提示您确认更改。

  如何在管理控制台 (MMC) 中获取加密数据访问文件

  1. 打开 Kaspersky Security Center Administration Console。
  2. 在控制台树中，选择“**设备**”。
  3. 在“**设备**”选项卡上，选择用户正在请求加密数据访问权限的计算机，然后单击鼠标右键打开上下文菜单。
  4. 在上下文菜单中，选择“**授予离线模式下的访问权限**”。
  5. 这将打开一个窗口；在该窗口中，选择“**数据加密**”选项卡。
  6. 在“**数据加密**”选项卡上单击“**浏览**”按钮。
  7. 在用于选择请求访问文件的窗口中，指定从用户处接收的文件的路径。

您将看到有关用户请求的信息。Kaspersky Security Center 会生成一个密钥文件。通过电子邮件将生成的加密数据访问密钥文件发送给用户。或保存该访问文件并使用任何可用方法来传输该文件。

在移动模式下授予访问权限

如何在 Web Console 中获取加密数据访问文件

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**资产(设备)**”。
2. 选中要还原其数据访问权限的计算机名称旁边的复选框。
3. 单击“**授予移动模式设备访问权限**”。
4. 选择“**数据加密**”。
5. 单击“**选择文件**”按钮，然后选择从用户处收到的请求访问文件（扩展名为 KESDC 的文件）。
   Web Console 将显示有关请求的信息。这将包括用户请求访问的文件所在的计算机的名称。
6. 单击“**保存密钥**”按钮，然后选择一个文件夹来保存加密数据访问密钥文件（扩展名为 KESDR 的文件）。

结果，您将能够获取加密数据访问密钥，您需要将该密钥传输给用户。

可移动驱动器解密

您可以使用策略来解密可移动驱动器。将为特定管理组生成具有已定义的可移动驱动器加密设置的策略。因此，可移动驱动器上的数据解密结果取决于其所连接的计算机。

若要解密可移动驱动器，请执行以下操作：

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **数据加密** → **可移动驱动器加密**。

4. 如果您希望解密所有存储在可移动驱动器上的加密文件，请在“**加密模式**”下拉列表中选择“**解密整个可移动驱动器**”。

5. 若要解密存储在个人可移动驱动器上的数据，请为您要解密其数据的可移动驱动器编辑加密规则。为此，请执行下列操作：

   a. 在已配置加密规则的可移动驱动器列表中，选择对应您所需可移动驱动器的条目。

   b. 单击“**设置规则**”按钮为所选可移动驱动器编辑加密规则。

   c. 在“**设置规则**”按钮的上下文菜单中，选择“**解密整个可移动驱动器**”条目。

6. 保存更改。

结果是，如果用户连接可移动驱动器或该驱动器已经连接，Kaspersky Endpoint Security 将解密该可移动驱动器。程序将警告用户解密过程可能会花费些时间。如果在数据解密期间，用户安全移除可移动驱动器，Kaspersky Endpoint Security 将会在解密过程完成前中断数据解密过程，并且允许移除可移动驱动器。下次将可移动驱动器连接到此计算机时，将继续数据解密。

如果对可移动驱动器的解密失败，请在 Kaspersky Endpoint Security 界面中查看“**数据加密**”报告。对文件的访问可能被其他应用程序阻止。在这种情况下，请尝试从计算机上拔下可移动驱动器，然后重新连接。

查看数据加密详细信息

当正在执行加密或解密任务时，Kaspersky Security Center 会将应用于客户端计算机的加密参数状态的相关信息转发给 Kaspersky Security Center。

查看加密状态

您可以查看状态以监控数据加密。Kaspersky Endpoint Security 分配以下加密状态：

- **不符合策略；已被用户取消**。用户已取消数据加密。
- “**由于错误而未遵从策略**”。数据加密错误，例如缺少授权许可。
- “**正在应用策略；需要重新启动**”。正在这台计算机上进行数据加密。重新启动计算机以完成数据加密。
- “**未指定加密策略**”。策略设置中的数据加密已关闭。
- **不支持**。计算机上未安装数据加密组件。
- “**正在应用策略**”。正在这台计算机上进行数据加密和/或解密。

若要查看计算机数据的加密状态，请执行以下操作：

1. 打开 Kaspersky Security Center Administration Console。

2. 在控制台树中，选择“**受管理设备**”。

3. 在工作区的“**设备**”选项卡中，将滚动条滑向右侧。如果“**加密状态**”列未显示，请在 Kaspersky Security Center 控制台设置中添加此列。

   “**加密状态**”列将显示选定管理组中计算机上数据的加密状态。该状态是基于计算机本地驱动器上的文件加密信息和完整磁盘加密的信息形成的。

4. 如果计算机的数据加密状态为“**正在应用策略**”，您可以监控加密进度面板：

   a. 双击打开带有“**正在应用策略**”状态的计算机的属性。

   b. 在计算机属性窗口中，选择“**应用程序**”区域。

   c. 在计算机上安装的卡巴斯基应用程序列表中，选择“**Kaspersky Endpoint Security for Windows**”。

   d. 单击“**统计**”。

   e. 在“**设备加密**”下，您可以以百分比形式查看数据加密的当前进度。

在 Kaspersky Security Center 信息显示板上查看加密统计信息

要在 Kaspersky Security Center 信息显示板上查看加密状态：

1. 打开 Kaspersky Security Center Administration Console。

2. 在控制台树中，选择“**管理服务器**”节点。

3. 在管理控制台树的右侧工作区中选择“**统计**”选项卡。

4. 使用包含数据加密统计信息的详细面板创建新页面。为此，请执行下列操作：

   a. 在“**统计**”选项卡上单击“**自定义视图**”按钮。

   b. 在打开的窗口中，单击“**添加**”按钮。

   c. 这将打开一个窗口；在该窗口中，在“**常规**”区域中，输入页面的名称。

   d. 在“**信息窗格**”区域中单击“**添加**”按钮。

   e. 在打开的窗口的“**保护状态**”组中选择“**设备加密**”项。

   f. 单击“**确定**”。

   g. 如果必要，编辑详细窗格的设置。为此，使用“**查看**”和“**设备**”区域。

   h. 单击“**确定**”。

   i. 重复执行说明中的步骤 d – h，在“**保护状态**”区域中，选择“**可移动驱动器加密**”项。
      添加的详细窗格出现在“**信息窗格**”列。

j. 单击“**确定**”。
在先前步骤中创建的带有详情面板的页面名称将显示在“**页面**”列表中。

k. 单击“**关闭**”按钮。

5. 在“**统计**”选项卡上，打开在该说明的先前步骤中创建的页面。

详情页面将出现，其中显示了计算机和可移动驱动器的加密状态。

查看本地计算机驱动器上文件加密错误

若要查看本地计算机驱动器上文件加密错误：

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**受管理设备**”。
3. 在“**设备**”选项卡，选择列表中计算机的名称，单击右键打开上下文菜单。
4. 在计算机的上下文菜单中选择“**属性**”项。在打开的窗口中选择“**保护**”区域。
5. 单击“**查看数据加密错误**”链接打开“**数据加密错误**”窗口。

该窗口将显示本地计算机磁盘驱动器上文件加密错误的详情。错误被纠正后，Kaspersky Security Center 会将该错误详情从“**数据加密错误**”窗口中删除。

查看数据加密报告

Kaspersky Security Center 允许您创建数据加密报告：

- “**受管理设备加密状态报告**”。该报告包括有关计算机的加密状态是否符合加密策略的信息。
- “**大容量存储设备加密状态报告**”。该报告包括有关外部设备和存储设备的加密状态的信息。
- “**加密驱动器访问权限报告**”。该报告包括有关有权访问加密驱动器的账户状态的信息。
- “**文件加密错误报告**”。该报告包含有关在计算机上执行数据加密或解密任务期间发生的错误的信息。
- “**加密文件访问被阻止报告**”。该报告包括有关被阻止访问加密文件的应用程序的信息。

若要查看数据加密报告，请执行以下操作：

1. 打开 Kaspersky Security Center Administration Console。
2. 在管理控制台树的“**管理服务器**”中选择“**报告**”选项卡。
3. 单击“**新建报告模板**”按钮。
“新报告模板向导”将启动。
4. 按照“报告模板向导”的说明进行操作。在“**选择报告模板类型**”窗口中的“**其他**”部分，选择一份数据加密报告。
完成新报告模板向导之后，新报告模板将出现在“**报告**”选项卡上。

5. 选择在说明的上个步骤中创建的报告模板。

6. 在模板的上下文菜单中选择“**显示报告**”。

   报告生成过程将开始。该报告将显示在新窗口中。

无法访问加密设备时的设备使用

获取访问加密设备的权限

在以下情况下用户可能被要求请求访问加密设备：

- 硬盘驱动器在其它计算机上进行的加密。
- 设备的加密密钥不在计算机上（例如，首次尝试访问计算机上的加密可移动驱动器时），计算机未连接到 Kaspersky Security Center。

  用户应用访问密钥到加密设备后，Kaspersky Endpoint Security 将把加密密钥保存在用户的计算机上，允许在随后的访问尝试时访问该设备（即使未连接到 Kaspersky Security Center）。

可用以下方式获得加密设备的访问权限：

1. 用户使用 Kaspersky Endpoint Security 应用程序界面创建带有 kesdc 扩展名的请求访问文件并将其发送给公司局域网管理员。
2. 管理员使用 Kaspersky Security Center 管理控制台创建带有 kesdr 扩展名的访问密钥文件并将其发送给用户。
3. 用户应用访问密钥。

恢复加密设备上的数据

用户可用使用 加密设备恢复实用程序 （以下简称“恢复实用程序”）使用加密设备。在下列情况中可能要求这样做：

- 使用访问密钥获取访问权限的过程不成功。
- 带有加密设备的计算机上尚未安装加密组件。

需要使用“恢复实用工具”恢复对加密设备访问的数据有一段时间以未加密形式在用户计算机的内存里。要降低有人未经授权访问此类数据的风险，建议您在受信任的计算机上恢复访问加密设备。

可用以下方式恢复加密设备上的数据：

1. 用户使用“恢复实用工具”创建带有 fdertc 扩展名的请求访问文件并将其发送给公司局域网管理员。
2. 管理员使用 Kaspersky Security Center 管理控制台创建带有 fdertr 扩展名的访问密钥文件并将其发送给用户。
3. 用户应用访问密钥。

若要恢复加密系统硬盘驱动器上的数据，用户也可以在“恢复实用工具”中指定身份验证代理账户凭证。如果身份验证代理账户的元数据已损坏，用户必须使用请求访问文件完成恢复过程。

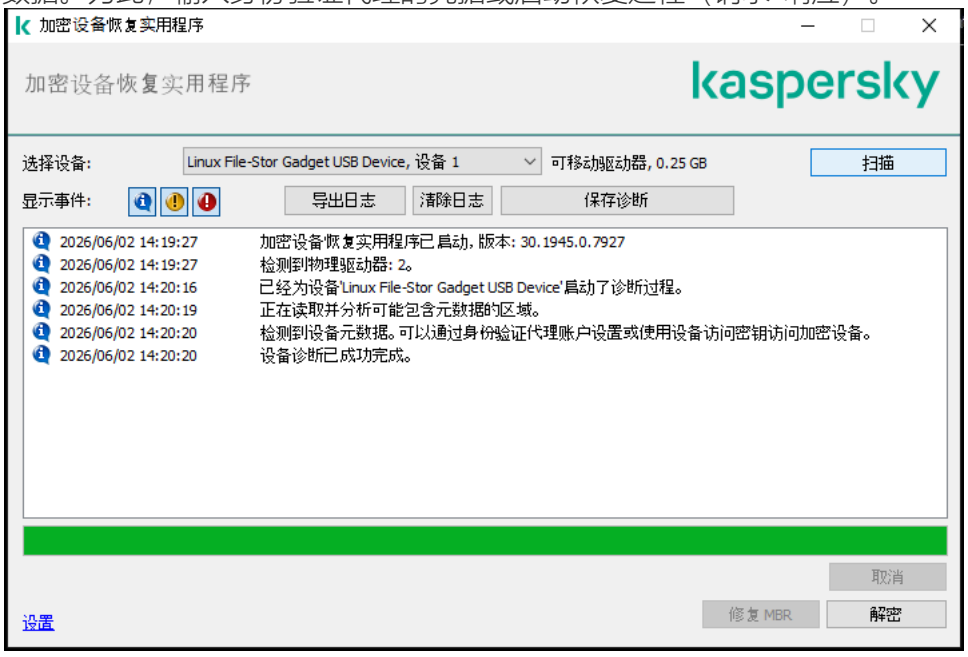
在恢复加密设备上的数据前，建议在将执行过程的计算机上取消 Kaspersky Security Center 策略或禁用 Kaspersky Security Center 策略设置中的加密。这可以防止重新加密设备。

使用 FDERT 恢复实用程序恢复数据

如果硬盘驱动器发生故障，文件系统可能已损坏。如果是这种情况，由卡巴斯基磁盘加密技术保护的数据将不可用。您可以解密数据并将数据复制到新驱动器。

对由卡巴斯基磁盘加密技术保护的驱动器的数据恢复包括以下步骤：

1. 创建一个独立恢复实用程序（请参见下图）。
2. 将驱动器连接到未安装 Kaspersky Endpoint Security 加密组件的计算机。
3. 运行还原实用程序并诊断硬盘驱动器。
4. 访问驱动器上的数据。为此，输入身份验证代理的凭据或启动恢复过程（请求-响应）。



FDERT 恢复实用程序

创建独立恢复实用程序

若要创建恢复实用工具的可执行文件，请执行以下操作：

1. 打开主应用程序窗口并单击 按钮。
2. 在打开的窗口中，单击“**恢复已加密设备**”按钮。

   加密设备恢复实用程序启动。
3. 在恢复实用程序窗口中，单击“**创建独立恢复实用程序**”按钮。
4. 将独立恢复实用程序保存到计算机内存中。

结果，该恢复实用程序的可执行文件 (fdert.exe) 将保存在指定的文件夹中。将该恢复实用程序复制到未安装 Kaspersky Endpoint Security 加密组件的计算机。这可以防止重新加密驱动器。

需要使用“恢复实用工具”恢复对加密设备访问的数据有一段时间以未加密形式在用户计算机的内存里。要降低有人未经授权访问此类数据的风险，建议您在受信任的计算机上恢复访问加密设备。

恢复硬盘驱动器上的数据

若要使用恢复实用工具恢复对加密设备的访问权限。

1. 运行名为 fdert.exe 的文件，该文件是恢复实用程序的可执行文件。该文件由 Kaspersky Endpoint Security 创建。
2. 在“恢复实用程序”窗口中，选择要恢复访问权限的加密设备。
3. 单击“**扫描**”按钮允许该实用工具定义应在设备上执行何种操作：是否应解锁或者解密。

   如果计算机可以访问 Kaspersky Endpoint Security 加密功能，“恢复实用工具”将提示您解锁设备。解锁设备并不进行解密，解锁的设备将可以直接访问。如果计算机不可以访问 Kaspersky Endpoint Security 加密功能，“恢复实用工具”将提示您解密设备。
4. 如果要导入诊断信息，请单击“**保存诊断**”按钮。

   该实用程序将保存一个压缩文件，其中的文件包含诊断信息。
5. 如果加密系统硬盘驱动器的诊断提示设备主引导记录 (MBR) 出现问题，请单击“**修复 MBR**”按钮。

   修复设备的主引导记录可以使获取解锁或解密设备时所需信息的过程加快。
6. 根据诊断结果单击**解锁**或**解密**按钮。
7. 如果您想要使用身份验证代理账户恢复数据，请选择“**使用身份验证代理账户设置**”选项，然后输入身份验证代理的凭据。

   这种方法仅当恢复系统硬盘驱动器上的数据时可用。如果系统硬盘驱动器损坏且身份验证代理账户数据已丢失，您必须从公司局域网管理员获得访问密钥才能恢复加密设备上的数据。

8. 如果要启动恢复过程，请执行以下操作：

   a. 请选择**手动指定设备访问密钥**选项。

   b. 单击“**接收访问密钥**”按钮，然后将请求访问文件（扩展名为 FDERTC 的文件）保存到计算机内存。

   c. 将该请求访问文件发送给公司局域网管理员。

   > 在接收到访问密钥前不要关闭“**接收设备访问密钥**”窗口。当该窗口再次打开时，您将无法应用之前由管理员创建的访问密钥。

   d. 接收并保存由公司局域网管理员创建并发送给您的访问文件（扩展名为 FDERTR 的文件）（请参见以下说明）。

   e. 在“**接收设备访问密钥**”窗口中下载访问文件。

9. 如果要解密设备，则必须配置其他解密设置：

   - 指定解密区域：
     - 如果您想要解密整个设备，请选择**解密整个设备**选项。
     - 如果您想要解密设备上的部分数据，请选择**解密个别设备区域**选项，然后指定解密区域边界。
   - 选择写入解密数据的位置：
     - 如果您想要用解密数据复写原始设备上的数据，请清除“**解密至磁盘镜像文件**”复选框。
     - 如果您想要将解密数据与原始加密数据分开保存，请选中“**解密至磁盘镜像文件**”复选框，然后使用“**浏览**”按钮指定保存 VHD 文件的路径。

10. 单击“**确定**”。

    设备解锁/解密过程将启动。

如何在管理控制台 (MMC) 中创建加密数据访问文件

1. 打开 Kaspersky Security Center Administration Console。

2. 在管理控制台树中，选择“**高级**” → “**数据加密和保护**” → “**加密驱动器**”文件夹。

3. 在工作区中，选择要为其创建访问密钥文件的加密设备，然后在该设备的上下文菜单中，单击“**获取 Kaspersky Endpoint Security中的设备访问权限**”。

   > 如果您不确定访问请求文件是为哪台计算机生成的，请在管理控制台树中选择“**高级** ” → “**数据加密和保护**”文件夹，然后在工作区中，单击“**获取Kaspersky Endpoint Security中的设备加密密钥**”。

4. 在打开的窗口中，选择要使用的加密算法：AES256 或 AES56。

   数据加密算法取决于分发包中包含的 AES 加密库：*强加密(AES256)* 或 *轻度加密(AES56)*。AES 加密库与应用程序一起安装。

5. 单击“**浏览**”打开窗口。在此窗口中，指定从用户接收的具有 fdertc 扩展名的请求文件的路径。

6. 单击“**解锁**”。

您将看到有关用户请求的信息。Kaspersky Security Center 会生成一个密钥文件。通过电子邮件将生成的加密数据访问密钥文件发送给用户。或保存该访问文件并使用任何可用方法来传输该文件。

如何在 Web Console 中创建加密数据访问文件

1. 在 Web Console 的主窗口中，选择“**操作**” → “**数据加密和保护**” → “**加密驱动器**”。

2. 选中要恢复其数据的计算机名称旁边的复选框。

3. 单击“**授予移动模式设备访问权限**”。

   这将启动用于授予设备访问权限的向导。

4. 按照向导的说明授予对设备的访问权限：

   a. 选择 Kaspersky Endpoint Security for Windows 插件。

   b. 选择要使用的加密算法：AES256 或 AES56。

      数据加密算法取决于分发包中包含的 AES 加密库：*强加密(AES256)* 或 *轻度加密(AES56)*。AES 加密库与应用程序一起安装。

   c. 选择从用户处收到的请求访问文件（扩展名为 FDERTC 的文件）。

   d. 选择一个文件夹来保存加密数据访问密钥文件（扩展名为 FDERTR 的文件）。

结果，您将能够获取加密数据访问密钥，您需要将该密钥传输给用户。

创建操作系统紧急修复磁盘

当加密硬盘驱动器由于某种原因而无法访问，因而操作系统无法加载时，操作系统救援盘可能很有用。

您可以使用救援盘加载 Windows 操作系统的镜像，并且使用操作系统镜像中包括的恢复实用工具恢复对加密硬盘驱动器的访问。

若要创建操作系统救援盘：

1. 创建加密设备恢复实用程序的可执行文件。

2. 创建 Windows 预启动环境的自定义镜像。在创建 Windows 预启动环境的自定义镜像的同时，将恢复实用工具的可执行文件添加至镜像。

3. 将 Windows 预安装环境的自定义镜像保存至启动驱动器，如 CD 或可移动驱动器。

   有关创建 Windows 预启动环境的自定义镜像的说明，请参阅 Microsoft 帮助文件（例如，Microsoft TechNet 资源）。

Detection and Response 解决方案

Kaspersky Detection and Response 解决方案是用于检测组织基础设施不同级别的高级威胁和攻击指标的安全系统。Detection and Response 解决方案提供有关检测到的威胁的信息，并允许管理威胁响应操作。

因此，Detection and Response 解决方案执行以下操作：

- 接收有关计算机、服务器或其他设备（遥测）操作的信息。
- 自动分析信息以检测威胁。
- 生成警报详细信息作为威胁发展链的列，以供分析和选择威胁响应操作。
- 执行威胁响应操作（例如，计算机的网络隔离）。

Kaspersky Endpoint Security 使用内置代理支持 Detection and Response 解决方案。内置代理将遥测数据发送到解决方案的服务器并执行威胁响应操作。内置代理支持：

- Kaspersky Managed Detection and Response (MDR)
- Kaspersky Endpoint Detection and Response Optimum 2.0（EDR Optimum）
- Kaspersky Endpoint Detection and Response Expert（EDR Expert）
- Kaspersky Anti Targeted Attack Platform：
  - Endpoint Detection and Response (EDR) 版本 7.1 或更早版本
  - Network Detection and Response（NDR）
  - KATA Sandbox
- Kaspersky Endpoint Detection and Response Expert（本地部署）
- Kaspersky Sandbox 2.0

您可以在各种配置中使用 Kaspersky Endpoint Security 和 Detection and Response 解决方案，例如，[EDR Optimum+MDR]。

MDR 和 EDR Optimum 授权许可

Kaspersky Endpoint Security 支持 Kaspersky Managed Detection and Response (MDR) 和 Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) 解决方案的功能。您可以在各种配置中将 Kaspersky Endpoint Security 与这些解决方案结合使用，并构建满足您特定要求的自定义保护系统。为此，您必须为每个解决方案购买一个授权许可。授权许可可能涵盖使用单一解决方案（例如，仅 MDR 插件）或多个解决方案（[EDR Optimum+MDR] 插件）的权利。

MDR 和 EDR Optimum 支持以下授权许可方法：

- MDR 或 EDR Optimum 功能被包含在 Kaspersky Endpoint Security for Windows 授权许可中。

  该功能将在激活 Kaspersky Endpoint Security for Windows 后立即可用。您只需添加一个密钥。

- MDR 或 EDR Optimum 的单独授权许可（MDR Add-on、EDR Optimum Add-on、[EDR Optimum+MDR] Add-on）。

  为 MDR Add-on、EDR Optimum Add-on 或 [EDR Optimum+MDR] Add-on 添加单独的密钥后，该功能可用。因此，计算机上将添加两个密钥：Kaspersky Endpoint Security 密钥和 MDR 或 EDR Optimum 密钥。必须第一个添加 Kaspersky Endpoint Security 密钥。

Kaspersky Endpoint Security 仅允许添加一个*活动密钥*用于 MDR 和 EDR Optimum 授权许可。因此，如果您需要激活这两种解决方案，则必须添加一个 [EDR Optimum+MDR] Add-on 密钥，而不是为每个解决方案添加单独的密钥。您还可以添加一个*备用密钥*。

如果您在部署 MDR 时使用了 BLOB 文件，则不需要单独的密钥来激活 MDR。BLOB 文件已包含授权许可信息。

解决方案的初始授权许可

首次部署 MDR 和 EDR Optimum 时，解决方案的激活方式与 Kaspersky Endpoint Security 应用程序的激活方式相同。您可以使用 *添加密钥* 任务或使用自动密钥分发功能来添加密钥。如果选中相关复选框，授权许可密钥将作为第二个活动密钥或备用密钥添加到应用程序中。

从一个授权许可切换到另一个授权许可

如果您的组织已经部署了其中一种解决方案，并且相应的密钥已添加到应用程序中，那么新配置的授权许可需要考虑一些特殊事项。切换到不同的授权许可时，应用程序不会将新密钥添加到应用程序中，而是用新密钥替换当前密钥。其原因在于限制仅允许应用程序添加一个密钥来激活 MDR 和 EDR Optimum。

例如，假设您的组织已经部署了 [EDR Optimum+MDR] 解决方案，并且您决定切换到 MDR 加载项配置。要切换到新配置，必须用 MDR 加载项密钥替换 [EDR Optimum+MDR] Add-on 密钥。

EDR Optimum 和 MDR ([EDR Optimum+MDR] Add-on) 的单独授权许可不再可用。如果您想同时使用这两种解决方案，则必须使用 BLOB 文件激活 MDR，并使用授权许可密钥激活 EDR Optimum。

通过自动密钥分发功能，应用程序会拒绝覆盖相同数量解决方案的授权许可密钥。也就是说，如果您添加了 EDR Optimum Add-on 密钥，则不能用 MDR Add-on 密钥替换此密钥。但是，您可以用 [EDR Optimum+MDR] Add-on 密钥替换 EDR Optimum Add-on 密钥。如果您尝试用 EDR Add-on 密钥替换 MDR Add-on 密钥，应用程序也会拒绝密钥。要替换密钥，您可以运行“*添加密钥*”任务。“*添加密钥*”任务替换任意数量解决方案的授权许可密钥。

如果您添加了 [EDR Optimum+MDR] Add-on 备用密钥，为了正确添加 EDR Optimum 加载项或 MDR 加载项的活动密钥，您必须先将备用密钥替换为 EDR Optimum 加载项或 MDR 加载项密钥，或者，删除备用密钥，然后替换活动密钥。

与第三方 EDR 解决方案的兼容性

您可以将 Kaspersky Endpoint Security 与第三方 EDR 解决方案结合使用，以保护工作站和服务器。为了消除误报，我们建议将 Kaspersky Endpoint Security 和 Network Agent 的可执行文件添加到第三方 EDR 解决方案的受信任区域。

可与第三方 EDR 解决方案兼容的受信任区域

	Kaspersky Endpoint Security for Windows	Kaspersky Security Center 网络代理
工作文件夹	C:\Program Files (x86)\Kaspersky Lab\KES.14.1.0	C:\Program Files (x86)\Kaspersky Lab\NetworkAgent
可执行文件	avp.exe avp.com avpsus.exe avpui.exe dump_writer_agent.exe kescli.exe kesdr.exe kldw.exe klpsm.exe kvdb_upgrader.exe modify_watcher.exe pmv.exe remediation.exe service_stub.exe	AVPDTAgt.exe fix_gflags.exe getsysteminfo.exe integrity_checker.exe klcpuld.exe klcsldcl.exe klcsngtgui.exe klcspxy.exe kldumper.exe klmover.exe klnagchk.exe klnagent.exe klnagntf.exe klnagwds.exe klosprep.exe klrbtagt.exe klscflag.exe klscmodchk.exe klshwmsg.exe klwd.exe ksnproxy.exe Patch.exe tslauncher.exe Up2Date.exe vapm.exe

Kaspersky Endpoint Agent

Kaspersky Endpoint Agent 支持在应用程序与其他卡巴斯基解决方案之间进行交互以检测高级威胁（例如，Kaspersky Sandbox）。卡巴斯基解决方案与特定版本的 Kaspersky Endpoint Agent 兼容。

要使用 Kaspersky Endpoint Agent 作为卡巴斯基解决方案的一部分，您必须使用对应的授权许可密钥激活这些解决方案。

对于包含在您正使用的软件解决方案中的 Kaspersky Endpoint Agent 的完整信息，以及独立解决方案的完整信息，请参考相关产品的帮助指南：

- Kaspersky Anti Targeted Attack Platform 帮助
- Kaspersky Sandbox 帮助
- Kaspersky Endpoint Detection and Response Optimum 帮助
- Kaspersky Managed Detection and Response 帮助

Kaspersky Endpoint Security 版本 11.2.0 – 11.8.0 的分发包包括 Kaspersky Endpoint Agent。您可以在安装 Kaspersky Endpoint Security for Windows 时选择 Kaspersky Endpoint Agent。因此，您的计算机上将安装两个应用程序：KEA 和 KES。在 Kaspersky Endpoint Security 11.9.0 中，Kaspersky Endpoint Agent 分发包不再是 Kaspersky Endpoint Security 分发包的一部分。

KEA 版本（作为 KES 的一部分）与 KES 版本的对应关系

Kaspersky Endpoint Security for Windows	Kaspersky Endpoint Agent
11.8.0	3.11.0.216.mr1
11.7.0	3.11
11.6.0	3.10
11.5.0	3.9
11.4.0	3.9
11.3.0	3.9
11.2.0	3.9

卡巴斯基正在将所有 Detection and Response 切换为使用 Kaspersky Endpoint Security 内置代理，而不是 Kaspersky Endpoint Agent。卡巴斯基正在逐步增加对这些解决方案的支持并逐步淘汰 Kaspersky Endpoint Agent（见下表）。从版本 12.1 开始，该应用程序支持所有 Detection and Response 解决方案。此外，从 12.1 版开始，该应用程序不再与 Kaspersky Endpoint Agent 兼容，并且不再可能在同一台计算机上同时安装这两个应用程序。

部署内置代理来管理检测和响应解决方案

Kaspersky Endpoint Security 的版本	Kaspersky Managed Detection and Response	Kaspersky Sandbox	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Endpoint Detection and Response Expert	Kaspersky Anti Targeted Attack Platform（Endpoint Detection and Response 组件）	Kaspersky Anti Targeted Attack Platform（Network Detection and Response 组件）
11.5.0	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.6.0	**内置代理**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.7.0	**内置代理**	**内置代理**	**内置代理**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.8.0	**内置代理**	**内置代理**	**内置代理**	**内置代理**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.9.0	**内置代理**	**内置代理**	**内置代理**	**内置代理**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.10.0	**内置代理**	**内置代理**	**内置代理**	**内置代理**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
11.11.0	**内置代理**	**内置代理**	**内置代理**	**内置代理**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent
12	**内置代理**	**内置代理**	**内置代理**	**内置代理**	Kaspersky Endpoint Agent	Kaspersky Endpoint Agent

Kaspersky Endpoint Security 的版本	Kaspersky Managed Detection and Response	Kaspersky Sandbox	Kaspersky Endpoint Detection and Response Optimum	Kaspersky Endpoint Detection and Response Expert	Kaspersky Anti Targeted Attack Platform（Endpoint Detection and Response 组件）	Kaspersky Anti Targeted Attack Platform（Network Detection and Response 组件）
12.1	**内置代理**	**内置代理**	**内置代理**	**内置代理**	**内置代理**	Kaspersky Endpoint Agent
12.6	**内置代理**	**内置代理**	**内置代理**	**内置代理**	**内置代理**	**内置代理**

迁移 [KES+KEA] 配置到 [KES+内置代理] 配置

Kaspersky Endpoint Security 为 Detection and Response 解决方案引入了内置代理。使用这些解决方案您不再需要单独的 Kaspersky Endpoint Agent 应用程序。当您在安装了 Kaspersky Endpoint Agent 的计算机上部署 Kaspersky Endpoint Security 时，Detection and Response 解决方案将继续与 Kaspersky Endpoint Security 一起工作。此外，Kaspersky Endpoint Agent 将被从计算机卸载。

Kaspersky Endpoint Security 版本 11.2.0 – 11.8.0 的分发包包括 Kaspersky Endpoint Agent。您可以在安装 Kaspersky Endpoint Security for Windows 时选择 Kaspersky Endpoint Agent。因此，您的计算机上将安装两个应用程序：KEA 和 KES。在 Kaspersky Endpoint Security 11.9.0 中，Kaspersky Endpoint Agent 分发包不再是 Kaspersky Endpoint Security 分发包的一部分。

迁移 [KES+KEA] 配置到 [KES+内置代理] 需要以下步骤：

1. **升级 Kaspersky Security Center**

   将所有 Kaspersky Security Center 组件升级到版本 13.2 或更高版本，包括用户计算机上的网络代理和 Web Console。

2. **升级 Kaspersky Endpoint Security Web 插件**

   在 Kaspersky Security Center Web Console，将 Kaspersky Endpoint Security Web 插件升级到版本 11.7.0 或更高版本。要管理 EDR Optimum 和 Kaspersky Sandbox 组件，您必须使用 Web Console。

   要使用 Kaspersky Anti Targeted Attack Platform (EDR)，您需要一个适用于 Kaspersky Endpoint Security 版本 12.1 或更高版本的 Web 插件。

   要使用 Kaspersky Anti Targeted Attack Platform (NDR)，您需要一个适用于 Kaspersky Endpoint Security 版本 12.7 或更高版本的 Web 插件。

3. **迁移策略和任务**

   使用 Kaspersky Endpoint Agent 策略和任务迁移向导将 Kaspersky Endpoint Agent 设置迁移到 Kaspersky Endpoint Security for Windows。

   这将创建一个新的 Kaspersky Endpoint Security 策略。新策略具有*不活动*状态。要应用该策略，打开策略属性，接受卡巴斯基安全网络声明并设置其状态到*活动*。

4. **授权许可功能**

   如果您使用通用 Kaspersky Endpoint Detection and Response Optimum 或 Kaspersky Optimum Security 授权许可激活 Kaspersky Endpoint Security for Windows 和 Kaspersky Endpoint Agent，EDR Optimum 功能将在升级应用程序到版本 11.7.0 后被自动激活。您不需要做任务其他事情。

   如果您使用独立 Kaspersky Endpoint Detection and Response Optimum 加载项授权许可激活 EDR Optimum 功能，您必须确保 EDR Optimum 加载项密钥已添加到 Kaspersky Security Center 存储库且授权许可密钥自动分发功能已启用。在您升级应用程序到版本 11.7.0 后，EDR Optimum 功能被自动激活。

如果您使用 Kaspersky Endpoint Detection and Response Optimum 或 Kaspersky Optimum Security 授权许可激活 Kaspersky Endpoint Agent，并使用其他授权许可激活 Kaspersky Endpoint Security for Windows，您必须使用通用 Kaspersky Endpoint Detection and Response Optimum 或 Kaspersky Optimum Security 密钥替换 Kaspersky Endpoint Security for Windows 密钥。您可以使用"*添加密钥*"任务替换密钥。

您不需要激活 Kaspersky Sandbox 功能。Kaspersky Sandbox 功能将在升级和激活 Kaspersky Endpoint Security for Windows 后立即可用。

只有 Kaspersky Anti Targeted Attack Platform 授权许可可用于激活 Kaspersky Endpoint Security 作为 Kaspersky Anti Targeted Attack Platform 解决方案的一部分。在您升级应用程序到版本 12.1 后，EDR（KATA）功能被自动激活。您不需要做任务其他事情。

5 升级 Kaspersky Endpoint Security 应用程序

要升级应用程序并迁移 EDR Optimum 和 Kaspersky Sandbox 功能，建议使用远程安装任务。

要使用远程安装任务升级应用程序，您必须编辑以下设置：

- 在安装包的设置中选择 Detection and Response 解决方案的组件。
- 在安装包的设置中排除 Kaspersky Endpoint Agent 组件（适用于 Kaspersky Endpoint Security for Windows 版本 11.2.0 – 11.8.0）。
- 如果启用密码保护来限制对 Kaspersky Endpoint Agent 的访问，请在"*远程安装应用程序*"任务的设置中输入应用程序卸载密码。从 Kaspersky Security Center Linux 15.1 开始您可以输入卸载密码。

您还可以使用以下方法升级应用程序：

- 使用 Kaspersky 更新服务（无缝更新 - SMU）。
- 本地使用安装向导。

Kaspersky Endpoint Security 支持在安装了 Kaspersky Endpoint Agent 应用程序的计算机上升级应用程序时自动选择组件。组件的自动选择取决于升级应用程序的用户账户的权限。

如果您在系统账户（SYSTEM）下使用 EXE 或 MSI 文件升级 Kaspersky Endpoint Security，Kaspersky Endpoint Security 获得对卡巴斯基解决方案的当前授权许可的访问权。因此，如果计算机安装了 Kaspersky Endpoint Agent，并且激活了 EDR Optimum 解决方案，则 Kaspersky Endpoint Security 安装程序将自动配置组件集并选择 EDR Optimum 组件。这将使 Kaspersky Endpoint Security 切换到使用内置代理并卸载 Kaspersky Endpoint Agent。在系统账户(SYSTEM)下运行 MSI 安装程序通常在通过 Kaspersky 更新服务(SMU)升级时执行，或者当通过 Kaspersky Security Center 部署安装包时。

如果您在非特权用户账户下使用 MSI 文件升级 Kaspersky Endpoint Security，Kaspersky Endpoint Security 缺少对卡巴斯基解决方案的当前授权许可的访问权。这种情况下，Kaspersky Endpoint Security 基于 Kaspersky Endpoint Agent 配置自动选择组件。此后，Kaspersky Endpoint Security 将切换到使用内置代理并卸载 Kaspersky Endpoint Agent。

6 计算机重新启动

重新启动计算机以使用内置代理完成应用程序的升级。升级应用程序时，安装程序会在计算机重新启动之前卸载 Kaspersky Endpoint Agent。计算机重新启动后，安装程序将添加内置代理。这意味着在计算机重新启动之前，Kaspersky Endpoint Security 不会执行 EDR 和 Kaspersky Sandbox 的功能。

7 检查 Kaspersky Endpoint Detection and Response Optimum 和 Kaspersky Sandbox 的健康

升级之后，计算机在 Kaspersky Security Center 控制台显示*严重*状态：

- 确保计算机安装了网络代理版本 13.2 或更高版本。
- 通过查看“*应用程序组件状态报告*”检查内置代理的操作状态。如果组件具有*未安装*状态，使用“*更改应用程序组件*”任务安装组件。
- 确保您在 Kaspersky Endpoint Security for Windows 的新策略中接受了卡巴斯基安全网络声明。

- 确保使用以下方式激活 EDR Optimum 功能：*应用程序组件状态报告*。如果组件具有“*授权许可不支持*”状态，确保 EDR Optimum 的授权许可密钥自动分发功能已关闭。

Kaspersky Endpoint Agent 的策略和任务迁移

Kaspersky Endpoint Security for Windows 包括一个用于从 Kaspersky Endpoint Agent 迁移到 Kaspersky Endpoint Security 的向导。您可以迁移以下解决方案的策略和任务设置：

- Kaspersky Sandbox
- Kaspersky Endpoint Detection and Response Optimum (EDR Optimum)
- Kaspersky Anti Targeted Attack Platform

从 Kaspersky Endpoint Agent 迁移到 Kaspersky Endpoint Security 的向导仅适用于 Web Console 和云控制台。在管理控制台 (MMC) 中，您只能使用标准的 Kaspersky Security Center 策略和任务迁移向导迁移 Kaspersky Anti Targeted Attack Platform (EDR) 解决方案的设置。

建议首先在一台计算机上将 Kaspersky Endpoint Agent 迁移到 Kaspersky Endpoint Security，然后在一组计算机上进行迁移，然后在组织的所有计算机上完成迁移。

要将策略和任务设置从 Kaspersky Endpoint Agent 迁移到 Kaspersky Endpoint Security，请执行以下操作：

在 Web Console 的主窗口中，选择“**操作**” → “**从 Kaspersky Endpoint Agent 迁移**”。

这将运行策略和任务迁移向导。按照向导的说明进行操作。

步骤 1. 策略迁移

迁移向导将创建一个新策略，该策略将合并 Kaspersky Endpoint Security 和 Kaspersky Endpoint Agent 策略的设置。在策略列表中，选择要将其设置与 Kaspersky Endpoint Security 策略合并的 Kaspersky Endpoint Agent 策略。单击 Kaspersky Endpoint Agent 策略以选择您要与之合并设置的 Kaspersky Endpoint Security 策略。确保选择了正确的策略，然后转到下一步。

步骤 2. 任务迁移

迁移向导为 Kaspersky Endpoint Security 创建新任务。在任务列表中，选择要为 Kaspersky Endpoint Security 策略创建的 Kaspersky Endpoint Agent 任务。该向导支持 Kaspersky Endpoint Detection and Response 和 Kaspersky Sandbox 的任务。转到下一步。

步骤 3. 向导完成

退出向导。因此，向导会执行以下操作：

- 创建一个新的 Kaspersky Endpoint Security 策略。

  策略从 Kaspersky Endpoint Security 和 Kaspersky Endpoint Agent 合并设置。策略被叫做 *<Kaspersky Endpoint Security 策略名称> 和 <Kaspersky Endpoint Agent 策略名称>*。新策略具有*不活动*状态。要继续，将 Kaspersky Endpoint Agent 和 Kaspersky Endpoint Security 策略的状态更改为*不活动*并激活新合并的策略。

  从 Kaspersky Endpoint Agent 迁移到 Kaspersky Endpoint Security for Windows 后，请确保新策略具有将数据传输到设置的管理服务器（隔离文件数据和威胁发展链数据）的功能。数据传输参数值不会从 Kaspersky Endpoint Agent 策略迁移。

  对于 Kaspersky Anti Targeted Attack Platform (EDR) 解决方案，当从 Kaspersky Endpoint Agent 迁移到 Kaspersky Endpoint Security 时，您将计算机连接到 Central Node 服务器时可能会遇到错误。原因是 Web Console 中的迁移向导跳过了以下策略设置并且不迁移它们：

  - 设置修改禁止 **连接到 KATA 服务器** （“锁”）。

    默认情况下，可以修改设置（“锁”是打开的）。因此，这些设置不会应用到计算机上。您必须禁止设置修改并关闭“锁”。

  - 加密容器。

    如果您使用双向身份验证连接到 Central Node 服务器，则必须重新添加加密容器。迁移向导正确迁移了服务器的 TLS 证书。

  管理控制台（MMC）中的策略和任务迁移向导会迁移 Kaspersky Anti Targeted Attack Platform (EDR) 解决方案的所有设置。

- 创建新的 Kaspersky Endpoint Security 任务。

  新任务是 Kaspersky Endpoint Detection and Response 和 Kaspersky Sandbox 的 Kaspersky Endpoint Agent 任务的副本。同时，向导使 Kaspersky Endpoint Agent 任务保持不变。

如何在管理控制台 (MMC)（仅对 KATA (EDR)）中将策略和任务设置从 Kaspersky Endpoint Agent 迁移到 Kaspersky Endpoint Security

1. 在管理控制台中，选择管理服务器并右键单击以打开上下文菜单。

2. 选择“**所有任务**” → “**策略和任务批量转换向导**”。

策略和任务批量转换向导将启动。按照向导的说明进行操作。

步骤 1. 选择您要转换其策略和任务的应用程序

在此步骤，您需要选择“Kaspersky Endpoint Security for Windows”。转到下一步。

步骤 2. 策略转换

迁移向导创建一个新的 Kaspersky Endpoint Security 策略，Kaspersky Endpoint Agent 策略设置将迁移到该策略中。在策略列表中，选择要将其设置传输到 Kaspersky Endpoint Security 策略的 Kaspersky Endpoint Agent 策略。转到下一步。

然后，迁移向导将开始转换策略。在策略转换过程中，迁移向导会提示您接受卡巴斯基安全网络声明。新策略将被命名为 *<策略名称> (已转换)*。

步骤 3. 任务转换

跳过此步骤。该向导仅支持 Kaspersky Endpoint Detection and Response Optimum 和 Kaspersky Sandbox 的任务。这些组件的管理仅在 Web Console 中可用。转到下一步。

步骤 4. 向导完成

退出向导。作为向导的结果，将创建一个新的 Kaspersky Endpoint Security 策略。

Endpoint Detection and Response Agent (EDR Agent)

从 Kaspersky Endpoint Security 12.3 for Windows 开始，应用程序包含 Endpoint Detection and Response Agent（EDR Agent）配置。*Endpoint Detection and Response Agent* 是安装在组织 IT 基础设施中的各个工作站和服务器上的应用程序，用于支持卡巴斯基的如下 Detection and Response 解决方案：

- Kaspersky Managed Detection and Response
- Kaspersky Anti Targeted Attack Platform (EDR)
- Kaspersky Unified Monitoring and Analysis Platform (KUMA)（从 12.6 版开始）
- Kaspersky Anti Targeted Attack Platform (NDR)（从 12.7 版开始）
- Kaspersky Endpoint Detection and Response Expert (on-premises)（自 12.11 版本起）

EDR Agent 不支持与 Kaspersky Endpoint Detection and Response Expert (cloud) 解决方案集成。

EDR Agent 持续监控这些计算机上运行的进程、打开的网络连接以及正在修改的文件。应用程序的保护和控制组件不可用于 EDR Agent。

EDR Agent 与第三方 EPP 应用程序兼容。这使您可以将第三方基础设施安全工具与卡巴斯基的 Detection and Response 一起使用。

要部署 EDR Agent，计算机必须安装网络代理，并且必须将计算机添加到 Kaspersky Security Center 控制台中。要启用 EDR Agent 与 Kaspersky Security Center 的交互，您必须安装 Kaspersky Endpoint Security for Windows 管理插件。您可以使用组策略指定 EDR Agent 设置。要集成 EDR Agent，您必须在适当的策略部分中配置集成。

必须在基础设施上安装以下卡巴斯基应用程序以支持 Kaspersky Detection and Response 解决方案：

	• 网络代理 • EDR Agent
Endpoint	
	Kaspersky Endpoint Security for Windows 管理插件
Kaspersky Security Center	
Detection and Response 解决方案：MDR、KATA（EDR）、KATA（NDR）、KUMA、EDR Expert (on-premises)	

安装 EDR Agent

Endpoint Detection and Response Agent（EDR Agent）配置下的 Kaspersky Endpoint Security 对于 Kaspersky Detection and Response 解决方案的安装方式相同。

可以通过以下方式之一将 EDR Agent 安装在计算机上：

- 使用 Kaspersky Security Center 远程。
- 在本地使用安装向导。
- 在本地通过命令行（仅适用于 KATA (EDR) 和 EDR Expert (on-premises)）。

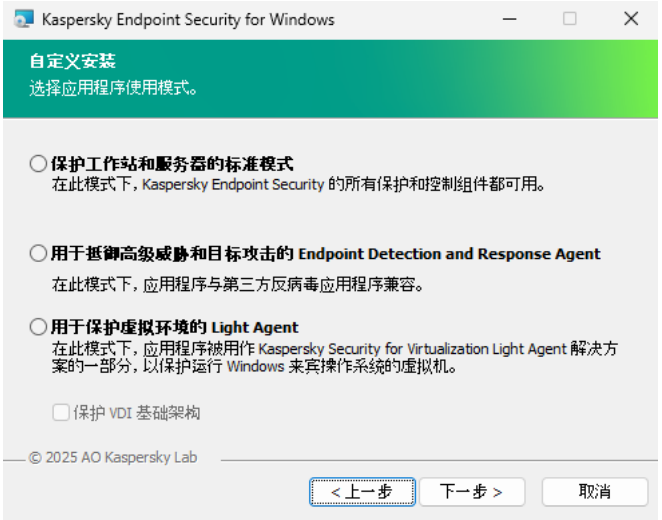
要安装 EDR Agent，您必须在安装包设置或在设置向导中选择适当的配置。

如何使用安装向导安装 EDR Agent

1. 复制分发包文件夹到用户计算机。
2. 运行 setup_kes.exe。

   “安装向导”将启动。

Kaspersky Endpoint Security 的配置



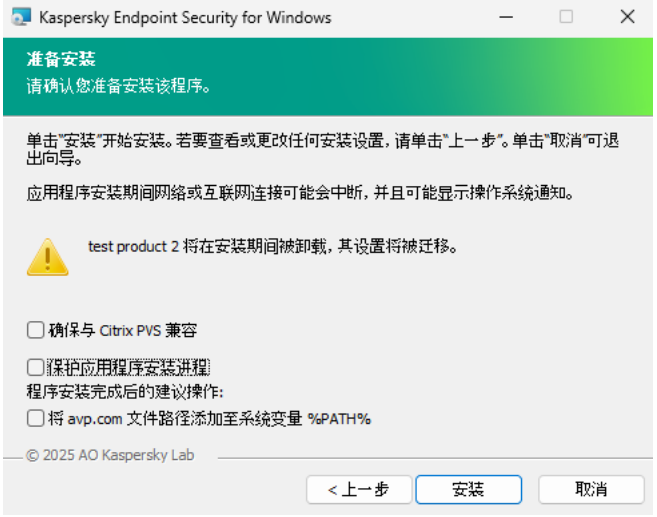
选择应用程序的配置

选择“**Endpoint Detection and Response Agent**”配置。在此配置下，您只能安装为 Detection and Response 解决方案提供支持的组件： MDR、EDR (KATA)、NDR (KATA)、EDR Expert (on-premises) 和 KUMA。如果您的组织中与 Kaspersky Detection and Response 解决方案一起部署了第三方Endpoint Protection Platform (EPP)，则需要此配置。这使得在 Endpoint Detection and Response Agent 配置下的 Kaspersky Endpoint Security 与第三方 EPP 应用程序兼容。

Kaspersky Endpoint Security 组件

选择您要安装的组件。安装应用程序后，您可以更改可用的应用程序组件。为此，您需要再次运行安装向导，然后选择更改可用组件。

高级设置



高级应用程序安装设置

“**保护应用程序安装进程**”。安装保护包括防止分发包被替换为恶意应用程序、阻止对 Kaspersky Endpoint Security 安装文件夹的访问，以及阻止对包含应用程序密钥的系统注册表部分的访问。但是，如果无法安装应用程序（例如，当使用Windows Remote Desktop执行远程安装时），我们建议您禁用安装过程的保护。

“**确保与 Citrix PVS 兼容**”。您可以启用 Citrix Provisioning Services 支持以将 Kaspersky Endpoint Security 安装到虚拟机。

“**将 avp.com 文件路径添加至系统变量 %PATH%**”。您可以将安装路径添加到 %PATH% 变量中，以方便使用命令行界面。

如何通过命令行安装 EDR Agent（仅适用于 KATA (EDR) 和 EDR Expert (on-premises)）

1. 以管理员身份运行命令行解释器 (cmd.exe)。
2. 转到 Kaspersky Endpoint Security 分发包所在文件夹。
3. 运行以下命令：

   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pSTANDALONEMODE=1 [/s]
   ```

   或

   ```
   msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 STANDALONEMODE=1 [/qn]
   ```

因此，用于与 Kaspersky Anti Targeted Attack Platform (EDR) 或 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成的 EDR Agent 应用程序将安装在计算机上。您可以通过发出 `status` 命令确认应用程序已安装并检查应用程序设置。

如何使用管理控制台（MMC）安装 EDR Agent

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**高级**” → “**远程安装**” → “**安装包**”文件夹。

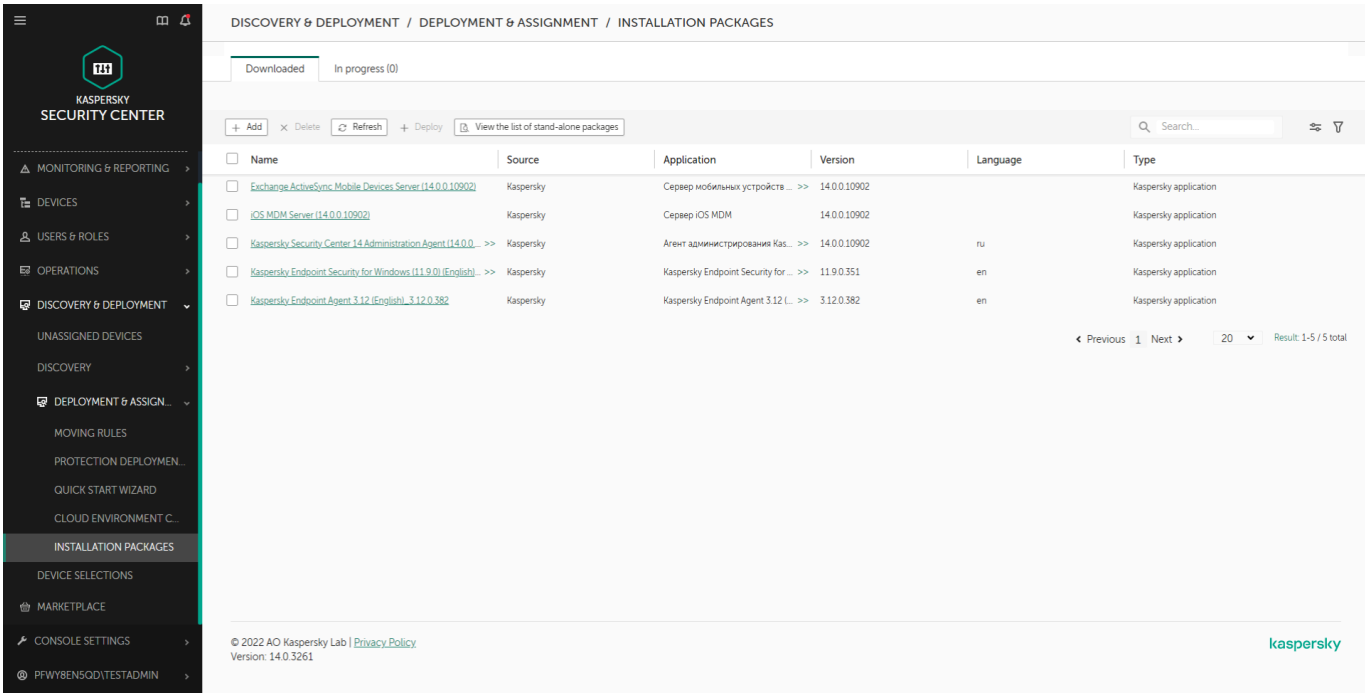
   这将打开已下载到 Kaspersky Security Center 的安装包列表。
3. 打开安装包的属性。

   如果有需要的话， 创建新的安装包。
4. 转到**保护组件**区域。
5. 选择“**用于抵御高级威胁和目标攻击的 Endpoint Detection and Response Agent**”配置。在此配置下，您只能安装为 Detection and Response 解决方案提供支持的组件： MDR、EDR (KATA)、NDR (KATA)、EDR Expert (on-premises) 和 KUMA。如果您的组织中与 Kaspersky Detection and Response 解决方案一起部署了第三方 Endpoint Protection Platform (EPP)，则需要此配置。这使得在 Endpoint Detection and Response Agent 配置下的 Kaspersky Endpoint Security 与第三方 EPP 应用程序兼容。
6. 选择您要安装的组件。

   安装应用程序后，您可以更改可用的应用程序组件。
7. 保存更改。
8. 创建远程安装任务。在任务属性中，选择您创建的安装包。

如何使用 Web Console 安装 EDR Agent

1. 在 Web Console 的主窗口中，选择“**发现和部署**” → “**部署和分配**” → “**安装包**”。
   这将打开已下载到 Kaspersky Security Center 的安装包列表。

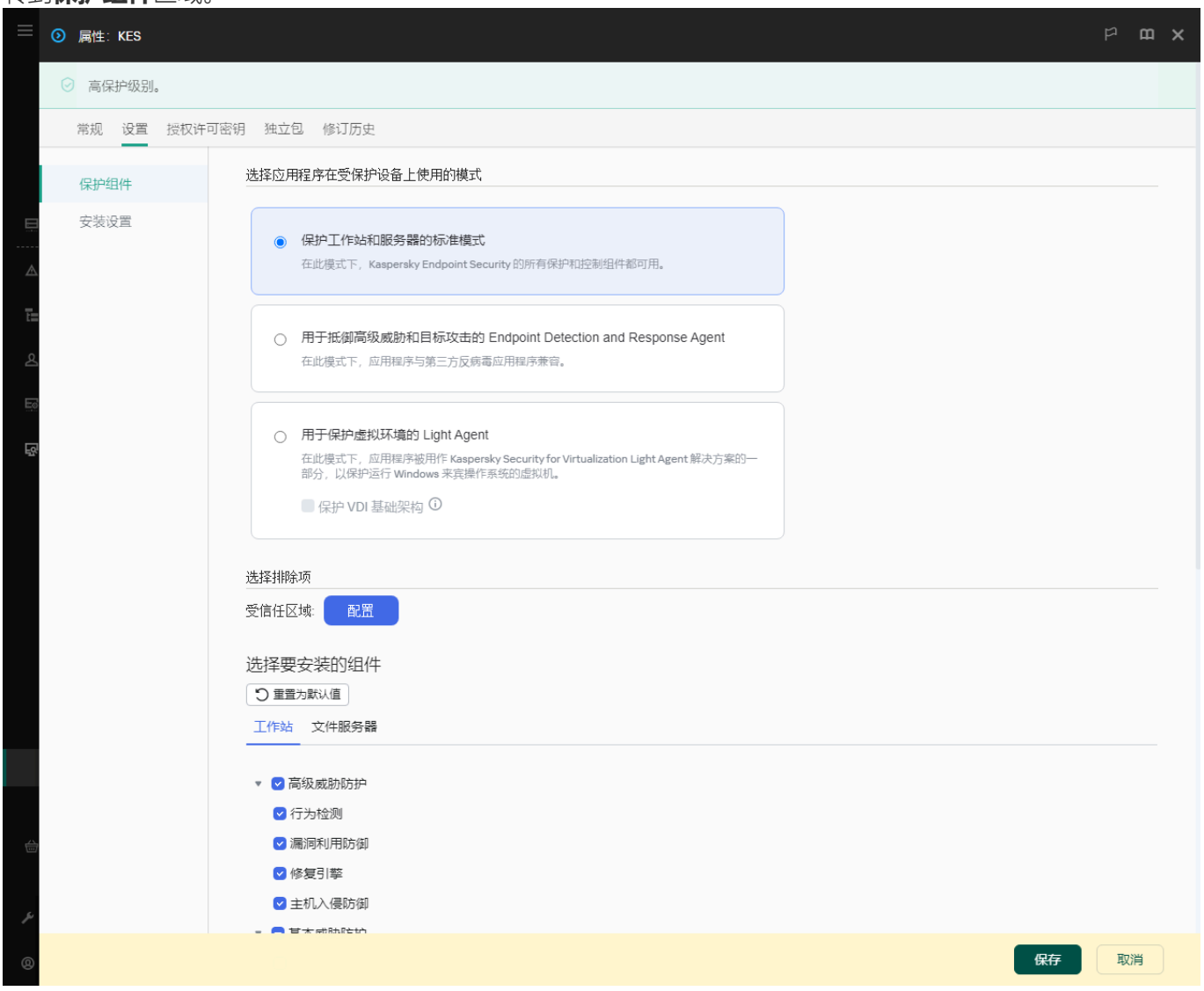


安装包列表

2. 打开安装包的属性。
   如果有需要的话， 创建新的安装包。

3. 选择**设置**选项卡。

4. 转到**保护组件**区域。



安装包中包含的组件

5. 选择“**用于抵御高级威胁和目标攻击的 Endpoint Detection and Response Agent**”配置。在此配置下，您只能安装为 Detection and Response 解决方案提供支持的组件： MDR、EDR (KATA)、NDR (KATA)、EDR Expert (on-premises) 和 KUMA。如果您的组织中与 Kaspersky Detection and Response 解决方案一起部署了第三方 Endpoint Protection Platform (EPP)，则需要此配置。这使得在 Endpoint Detection and Response Agent 配置下的 Kaspersky Endpoint Security 与第三方 EPP 应用程序兼容。

6. 选择您要安装的组件。

   安装应用程序后，您可以更改可用的应用程序组件。

7. 保存更改。

8. 创建远程安装任务。在任务属性中，选择您创建的安装包。

至此，EDR Agent 被安装在用户计算机上。您可以使用应用程序的界面，并且通知区域中会显示应用程序的图标 k。

在 Kaspersky Security Center 中，在 EDR Agent 配置中安装了应用程序的计算机具有“*严重*”状态 - 。计算机出现此状态是因为缺少文件威胁防护组件。您无需执行任何操作。

如果由于安装程序在计算机上发现不兼容的软件而无法在具有第三方 EPP 应用程序的计算机上安装 EDR Agent，您可以跳过不兼容软件检查。

EDR Agent 的主窗口

现在您必须配置与 Kaspersky Managed Detection and Response, Kaspersky Anti Targeted Attack (EDR) 或 Kaspersky Anti Targeted Attack (NDR) 解决方案的整合。您还可以指定应用程序的高级设置，例如， 创建受信任区域或者隐藏应用程序的界面。以下区域中的设置可用：

- 卡巴斯基安全网络
- 应用程序设置
- 网络设置
- 排除项
- 报告

- 界面
- 管理设置

将 EDR Agent 与 MDR 集成

EDR Agent 安装在组织 IT 基础设施中的工作站和服务器上。EDR Agent 处理数据并通过卡巴斯基安全网络流将其发送到 Kaspersky Managed Detection and Response。

为了 Kaspersky Managed Detection and Response 通过 Kaspersky Security Center Web Console 与管理服务器协作，您必须建立新的安全连接，一个*后台连接*。Kaspersky Managed Detection and Response 在您部署解决方案时提示您建立后台连接。确保后台连接已建立。

在 Web Console 中建立后台连接

1. 在 Web Console 的主窗口中，选择“**设置**” → “**整合**”。
2. 转到**整合**区域。
3. 开启 **用于整合的后台连接 已启用**切换开关。
4. 保存更改。

与 Kaspersky Managed Detection and Response 的整合包括以下步骤：

1. **安装“Managed Detection and Response”组件**

   您可以在安装或升级过程中选择 MDR 组件，也可以使用“*更改应用程序组件*”任务。

   > 要使用 *更改应用程序组件* 任务安装 Managed Detection and Response 组件且不重启计算机，您需要在任务设置中禁用 **检查不兼容的第三方应用程序** 选项。

2. **配置卡巴斯基私有安全网络**

   > 如果您正在使用 Kaspersky Security Center 云控制台则跳过此步骤。Kaspersky Security Center 云控制台在安装 MDR 插件时自动配置卡巴斯基私有安全网络。

   *卡巴斯基私有安全网络*是让运行 Kaspersky Endpoint Security 或其他卡巴斯基应用程序的计算机的用户获得卡巴斯基信誉数据库以及其他统计数据的访问权限的解决方案，无需从他们自己的计算机向卡巴斯基发送数据。

   在管理服务器属性中上传卡巴斯基安全网络配置文件。卡巴斯基安全网络配置文件存在于 MDR 配置文件的 ZIP 存档中。您可以在 Kaspersky Managed Detection and Response 控制台获取 ZIP 存档。对于配置卡巴斯基私有安全网络的详情，请参考 Kaspersky Security Center 帮助。您也可以从命令行上传卡巴斯基安全网络配置文件到计算机（参见以下说明）。

   如何从命令行配置卡巴斯基私有安全网络

   1. 以管理员身份运行命令行解释器 (cmd.exe)。
   2. 转到 Kaspersky Endpoint Security 可执行文件所在文件夹。

3. 运行以下命令：

```
avp.com KSN /private <file name>
```

`<file name>`是包含卡巴斯基私有安全网络设置的配置文件名称 (PKCS7 或 PEM 文件格式)。

例如：
```
avp.com KSN /private C:\kpsn_config.pkcs7
```

结果，Kaspersky Endpoint Security 将使用卡巴斯基私有安全网络决定文件、应用程序和网站的信誉。策略设置的"**卡巴斯基安全网络**"区域将显示以下运行状态： *基础设施: 卡巴斯基私人安全网络*。

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

3 激活 Kaspersky Managed Detection and Response

> 从 Kaspersky Endpoint Security for Windows 12.10 开始，要激活 Managed Detection and Response 功能，作为激活码的替代方案，您还可以使用密钥文件。

您需要为 MDR（Kaspersky Managed Detection and Response 加载项）购买单独的授权许可。

该功能将在为 Kaspersky Managed Detection and Response 加载项添加单独密钥后可用。独立 Managed Detection and Response 功能的授权许可与 Kaspersky Endpoint Security 授权许可相同。

确保 MDR 功能包含在授权许可中，并在应用程序的本地界面中工作。

4 启用 Managed Detection and Response 组件

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 文件存在于 MDR 配置文件的 ZIP 存档中。您可以在 Kaspersky Managed Detection and Response 控制台获取 ZIP 存档。对于 BLOB 文件的详情，请参考 Kaspersky Managed Detection and Response 帮助。

从 Kaspersky Endpoint Security 12.6 for Windows 开始，如果您拥有当前授权许可，则可以选择为无租户的 Kaspersky Managed Detection and Response 添加 BLOB 文件。

如何在管理控制台 (MMC) 中启用 Managed Detection and Response 组件

1. 在 Kaspersky Security Center 管理控制台树中，选择"**策略**"。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)**。
4. 选择**Managed Detection and Response (Industrial CyberSecurity)**复选框。
5. 在**设置**块，单击**上传**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。

   > 默认情况下，用户可以管理应用程序设置（"挂锁"处于打开状态 🔓）。要在计算机上应用该策略，请关闭"挂锁"🔒。

6. 保存更改。

如何在 Web Console 和云控制台中启用 Managed Detection and Response 组件

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置** → **Managed Detection and Response**。
5. 开启 **Managed Detection and Response 已启用**切换开关。
6. 单击**上传**并选择在 Kaspersky Managed Detection and Response 控制台获取的 BLOB 文件。该文件具有 P7 扩展名。

   > 默认情况下，用户可以管理策略设置（“挂锁”处于打开状态 🔓）。要在计算机上应用该策略，请关闭“挂锁”🔒。

7. 保存更改。

如何从命令行启用 Managed Detection and Response 组件

1. 以管理员身份运行命令行解释器 (cmd.exe)。
2. 转到 Kaspersky Endpoint Security 可执行文件所在文件夹。
3. 运行以下命令：

   ```
   avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
   ```

   > 要执行此命令，必须启用密码保护。用户必须具有“**配置应用程序设置**”权限。

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 文件被成功验证，Kaspersky Endpoint Security 将下载文件并在与 Kaspersky Security Center 的下次同步过程中发送该文件到计算机。通过查看*应用程序组件状态报告*检查组件的操作状态。您也可以利用 Kaspersky Endpoint Security 的本地界面在报告中查看组件的操作状态。**Managed Detection and Response** 组件将被添加到 Kaspersky Endpoint Security 组件列表。

5 配置应用程序的其他组件以接收遥测数据

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

- 卡巴斯基安全网络（扩展模式）。
- 行为检测。
- 漏洞利用防御。
- Web 威胁防护。
- 邮件威胁防护。

- 文件威胁防护。
- 网络威胁防护。
- 防火墙。
- AMSI 保护。
- 后台扫描。

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置** → **Managed Detection and Response**。
5. 开启 **Managed Detection and Response** **已启用**切换开关。
6. 保存更改。

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**。
4. 选择**Managed Detection and Response (Industrial CyberSecurity)**复选框。
5. 保存更改。

将 EDR Agent 与 EDR（KATA）集成

EDR Agent 安装在组织 IT 基础设施中的工作站和服务器上。在这些计算机上，EDR Agent 持续监控进程、打开的网络连接和正在修改的文件，并将监控数据发送到具有 Central Node 组件的服务器。

要与 EDR（KATA）集成，您必须启用 Endpoint Detection and Response（KATA）组件并配置 EDR Agent。

Endpoint Detection and Response（KATA）必须满足以下条件才能工作：

- Kaspersky Anti Targeted Attack Platform 版本 5.0–7.1。
- Kaspersky Security Center 版本 14.2 或更高版本。在 Kaspersky Security Center 的早期版本中，无法激活 Endpoint Detection and Response（KATA）功能。

https://www.youtube.com/watch?v=cZzgtBoeC7k

与 Kaspersky Endpoint Detection and Response（KATA）的整合包括以下步骤：

1. **激活 Endpoint Detection and Response （KATA）**

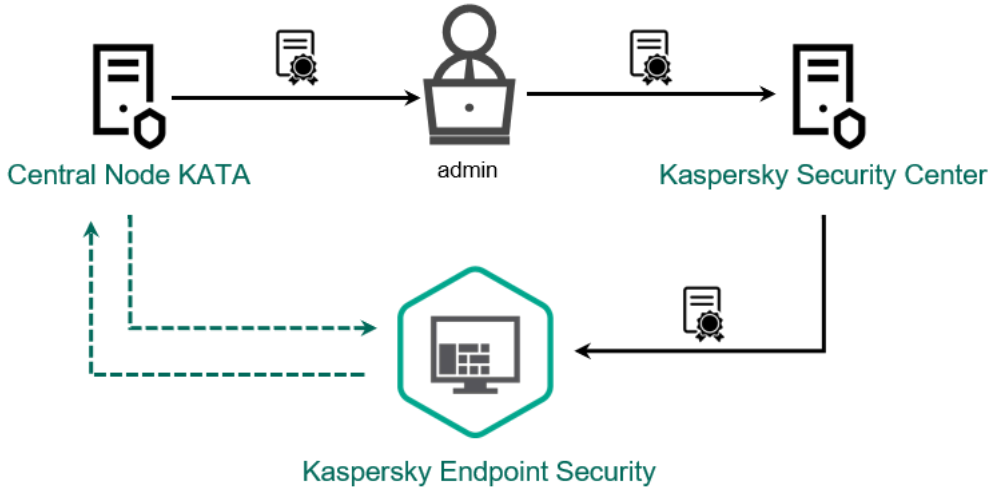
   您需要为 EDR（KATA）（Kaspersky Endpoint Detection and Response （KATA）加载项）购买单独的授权许可。

   该功能将在为 Kaspersky Endpoint Detection and Response (KATA) 添加单独密钥后可用。独立 Endpoint Detection and Response（KATA）功能的授权与 Kaspersky Endpoint Security 的授权相同。

   确保授权许可中包含 EDR （KATA）功能，并且该功能正在应用程序的本地界面中运行。

2. **连接到 Central Node**

   Kaspersky Anti Targeted Attack Platform 需要在 Kaspersky Endpoint Security 和 Central Node 组件之间建立可信连接。要配置可信连接，您必须使用 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）。然后您必须将 TLS 证书添加到 Kaspersky Endpoint Security（参见下面的说明）。



将 TLS 证书添加到 Kaspersky Endpoint Security

默认情况下，Kaspersky Endpoint Security 仅检查 Central Node 的 TLS 证书。为了使连接更安全，您可以额外启用 Central Node 上的计算机验证（双向身份验证）。要启用此验证，您必须在 Central Node 和 Kaspersky Endpoint Security 设置中打开双向身份验证。要使用双向身份验证，您还需要一个加密容器。*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）。

如何使用管理控制台 (MMC) 将 Kaspersky Endpoint Security 计算机连接到 Central Node

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**策略**”。
3. 选择必要的策略并双击以打开策略属性。
4. 在策略窗口中，选择 **Detection and Response → Endpoint Detection and Response Expert (on-premises)**。
5. 选择**Endpoint Detection and Response Expert (on-premises)**复选框。
6. 单击“**服务器连接设置**”。
7. 配置服务器连接：
   - “**超时(秒)**”。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 TLS 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）。
   - “**使用双向认证**”。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。
8. 单击“**确定**”。
9. 添加 Central Node 服务器。为此，请指定服务器地址（IPv4、IPv6）和连接到服务器的端口。

   您可以添加多个 Central Node 服务器地址。Kaspersky Endpoint Security 尝试使用第一个 IP 地址连接到服务器。如果连接建立失败，Kaspersky Endpoint Security 将尝试使用列表中的第二个 IP 地址进行连接，依此类推。
10. 如果有必要，配置遥测。
11. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何使用 Web Console 将 Kaspersky Endpoint Security 计算机连接到 Central Node

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”选项卡。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置** → **Endpoint Detection and Response Expert (on-premise)**。
5. 开启 **Endpoint Detection and Response Expert (on-premise) 已启用**切换开关。
6. 要配置 EDR (KATA)，请从解决方案列表中选择“**Endpoint Detection and Response Expert (版本 7.1 或更早版本)**”。
7. 单击“**连接设置**”。
8. 配置服务器连接：
   - “**超时(秒)**”。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。
9. 单击“**确定**”。
10. 添加 Central Node 服务器。为此，请指定服务器地址（IPv4、IPv6）和连接到服务器的端口。

    您可以添加多个 Central Node 服务器地址。Kaspersky Endpoint Security 尝试使用第一个 IP 地址连接到服务器。如果连接建立失败，Kaspersky Endpoint Security 将尝试使用列表中的第二个 IP 地址进行连接，依此类推。
11. 如果有必要，配置遥测。
12. 要将此策略应用到计算机，请关闭 🔒 挂锁图标并保存更改。

结果，计算机被添加到 Kaspersky Anti Targeted Attack Platform 控制台上。通过查看*应用程序组件状态报告*检查组件的操作状态。您也可以利用 Kaspersky Endpoint Security 的本地界面在报告中查看组件的操作状态。**Endpoint Detection and Response Expert (on-premises)** 组件将被添加到 Kaspersky Endpoint Security 组件列表。

将 EDR Agent 与 NDR（KATA）集成

EDR Agent 安装在组织 IT 基础设施中的工作站和服务器上。在这些计算机上，EDR Agent 持续监控进程、打开的网络连接和正在修改的文件，并将监控数据发送到具有 Central Node 组件的服务器。

要与 NDR（KATA）集成，您必须启用 Network Detection and Response（KATA）组件并配置 EDR Agent。

Network Detection and Response（KATA）必须满足以下条件才能工作：

- Kaspersky Anti Targeted Attack Platform 版本 7.0 或更高版本。
- Kaspersky Security Center 版本 14.2 或更高版本。在 Kaspersky Security Center 的早期版本中，无法激活 Network Detection and Response（KATA）功能。

https://www.youtube.com/watch?v=gd-rySv0ThQ

与 Network Detection and Response（KATA）的整合包括以下步骤：

1. **激活 Network Detection and Response （KATA）**

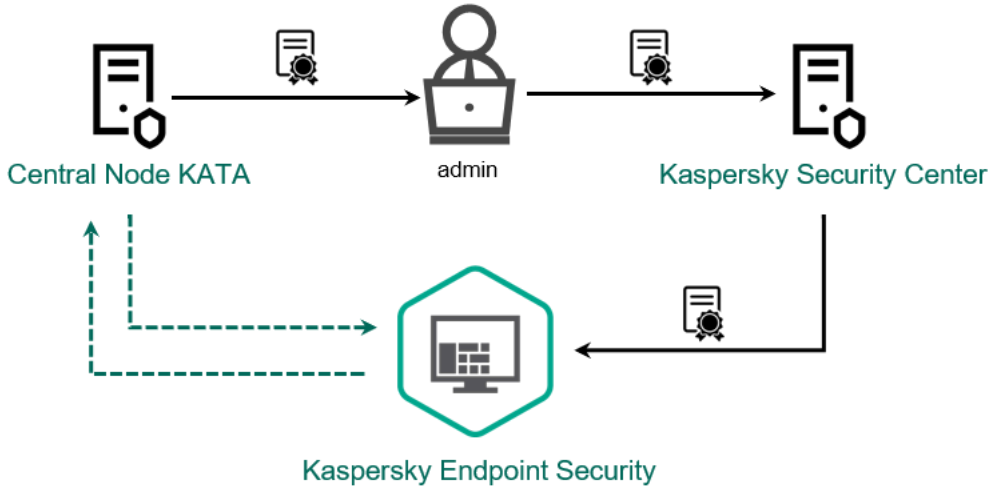
   您需要为 NDR（KATA）（Kaspersky Network Detection and Response （KATA）加载项）购买单独的授权许可。

   该功能将在为 Kaspersky Network Detection and Response (KATA) 添加单独密钥后可用。独立 Network Detection and Response（KATA）功能的授权与 Kaspersky Endpoint Security 的授权相同。

   确保授权许可中包含 NDR （KATA）功能，并且该功能正在应用程序的本地界面中运行。

2. **连接到 Central Node**

Kaspersky Anti Targeted Attack Platform 需要在 Kaspersky Endpoint Security 和 Central Node 组件之间建立可信连接。要配置可信连接，您必须使用 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）。然后您必须将 TLS 证书添加到 Kaspersky Endpoint Security（参见下面的说明）。



将 TLS 证书添加到 Kaspersky Endpoint Security

默认情况下，Kaspersky Endpoint Security 仅检查 Central Node 的 TLS 证书。为了使连接更安全，您可以额外启用 Central Node 上的计算机验证（双向身份验证）。要启用此验证，您必须在 Central Node 和 Kaspersky Endpoint Security 设置中打开双向身份验证。要使用双向身份验证，您还需要一个加密容器。*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）。

如何使用管理控制台 (MMC) 将 Kaspersky Endpoint Security 计算机连接到 Central Node

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **Detection and Response** → **Network Detection and Response (KATA)**。
4. 选择**Network Detection and Response (KATA)**复选框。
5. 单击“**连接设置**”。
6. 配置服务器连接：
   - “**超时(秒)**”。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。

7. 单击“**确定**”。

8. 添加 Central Node 服务器。为此，请指定服务器地址（IPv4、IPv6）和连接到服务器的端口。

9. 您可以添加多个 Central Node 服务器地址。Kaspersky Endpoint Security 尝试使用第一个 IP 地址连接到服务器。如果连接建立失败，Kaspersky Endpoint Security 将尝试使用列表中的第二个 IP 地址进行连接，依此类推。

10. 如果有必要，配置遥测。

11. 保存更改。

如何使用 Web Console 将 Kaspersky Endpoint Security 计算机连接到 Central Node

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **内置代理配置** → **Network Detection and Response (KATA)**。

5. 开启 **Network Detection and Response (KATA) 已启用**切换开关。

6. 单击“**连接设置**”。

7. 配置服务器连接：

   - “**超时(秒)**”。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。

8. 单击“**确定**”。

9. 添加 Central Node 服务器。为此，请指定服务器地址（IPv4、IPv6）和连接到服务器的端口。

10. 您可以添加多个 Central Node 服务器地址。Kaspersky Endpoint Security 尝试使用第一个 IP 地址连接到服务器。如果连接建立失败，Kaspersky Endpoint Security 将尝试使用列表中的第二个 IP 地址进行连接，依此类推。

11. 如果有必要，配置遥测。

12. 保存更改。

结果，计算机被添加到 Kaspersky Anti Targeted Attack Platform 控制台上。通过查看*应用程序组件状态报告*检查组件的操作状态。您也可以利用 Kaspersky Endpoint Security 的本地界面在报告中查看组件的操作状态。**Network Detection and Response (KATA)** 组件将被添加到 Kaspersky Endpoint Security 组件列表。

将 EDR Agent 与 EDR Expert (on-premises) 集成

EDR Agent 安装在组织 IT 基础设施中的工作站和服务器上。在这些计算机上，EDR Agent 持续监控进程、打开的网络连接和正在修改的文件，并将监控数据发送到 EDR Expert (on-premises) 服务器。

要与 EDR Expert (on-premises) 集成，您必须启用 Endpoint Detection and Response Expert (on-premises) 组件并配置 EDR Agent。

与 Kaspersky Endpoint Detection and Response Expert (on-premises) 集成包括以下步骤：

1. **激活 Kaspersky Endpoint Detection and Response Expert (on-premises)**

   您需要为 EDR Expert (on-premises)（Kaspersky Endpoint Detection and Response Expert (on-premises) 加载项）购买单独的授权许可。

   该功能将在为 Kaspersky Endpoint Detection and Response Expert (on-premises) 添加单独密钥后可用。独立 Endpoint Detection and Response Expert (on-premises) 功能的授权许可与 Kaspersky Endpoint Security 的授权许可相同。

   确保授权许可中包含 EDR Expert (on-premises) 功能，并且该功能正在应用程序的本地界面中运行。

2. **连接到遥测采集服务器和响应服务器**

   Kaspersky Endpoint Detection and Response Expert (on-premises) 需要 Kaspersky Endpoint Security 与两台服务器之间建立受信任连接：

   - *遥测采集服务器* 是 SIEM 解决方案的一部分，用于收集、规范化、关联、分析和存储有关计算机上发生的事件的信息。
   - *响应服务器* 是一个用于接收和扫描数据、研究对象行为和发布此类研究结果的服务器。

   要配置可信连接，您必须使用 TLS 证书。您可以在 Open Single Management Platform 上获取 TLS 证书（请参阅 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助中的说明）。然后您必须将 TLS 证书添加到 Kaspersky Endpoint Security（参见下面的说明）。

   默认情况下，Kaspersky Endpoint Security 仅检查服务器的 TLS 证书。为了使连接更安全，您可以额外启用服务器上的计算机验证（双向身份验证）。要启用此验证，您必须在服务器和 Kaspersky Endpoint Security 设置中打开双向身份验证。要使用双向身份验证，您还需要一个加密容器。*加密容器*是带有证书和私钥的 PFX 存档。您可以在 Open Single Management Platform 上获取加密容器（请参阅 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助中的说明）。

   如何使用 Web Console 将 Kaspersky Endpoint Security 计算机连接到 EDR Expert (on-premises)

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

   2. 单击 Kaspersky Endpoint Security 策略的名称。

      策略属性窗口将打开。

   3. 选择**应用程序设置**选项卡。

4. 选择 **内置代理配置** → **Endpoint Detection and Response Expert (on-premise)**。

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

6. 要配置 EDR Expert (on-premises)，请从解决方案列表中选择“**Endpoint Detection and Response Expert (版本 8.0 或更高版本)**”。

7. 配置*遥测采集服务器*连接：

   a. 在“**连接到遥测采集服务器**”区域，单击“**连接设置**”链接。

   b. 配置遥测采集服务器连接：

      - “**超时(秒)**”。最大服务器响应超时。当超时用完时，Kaspersky Endpoint Security 会尝试连接到不同的服务器。

      - “**服务器证书**”。用于与服务器建立受信任连接的 TLS 证书。您可以在 Open Single Management Platform 上获取 TLS 证书（请参阅 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助中的说明）。

      - “**使用双向身份验证**”。在 Kaspersky Endpoint Security 和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 Open Single Management Platform 上获取加密容器（请参阅 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助中的说明）。配置服务器设置后，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。

   c. 单击“**确定**”。

   d. 添加遥测采集服务器。为此，请指定服务器地址（IPv4、IPv6）和连接到服务器的端口。

      您可以添加多个遥测采集服务器地址。Kaspersky Endpoint Security 尝试使用第一个 IP 地址连接到服务器。如果连接建立失败，Kaspersky Endpoint Security 将尝试使用列表中的第二个 IP 地址进行连接，依此类推。

   e. 如果有必要，配置遥测。

8. 配置*响应服务器*连接：

   a. 在“**连接到响应服务器**”块中，配置“**发送同步请求到服务器的间隔(分钟)**”设置。发送到服务器的同步请求的频率。在同步过程中，Kaspersky Endpoint Security 接收威胁响应任务并发送任务结果。

   b. 单击**连接设置**链接。

   c. 配置响应服务器连接：

      - “**超时(秒)**”。最大服务器响应超时。当超时用完时，Kaspersky Endpoint Security 会尝试连接到不同的服务器。

      - “**服务器证书**”。用于与服务器建立受信任连接的 TLS 证书。您可以在 Open Single Management Platform 上获取 TLS 证书（请参阅 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助中的说明）。

- "**使用双向身份验证**"。在 Kaspersky Endpoint Security 和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 Open Single Management Platform 上获取加密容器（请参阅 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助中的说明）。配置服务器设置后，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。

d. 单击"**确定**"。

e. 添加响应服务器。为此，请指定服务器地址（IPv4、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 尝试使用第一个 IP 地址连接到服务器。如果连接建立失败，Kaspersky Endpoint Security 将尝试使用列表中的第二个 IP 地址进行连接，依此类推。

9. 要将此策略应用到计算机，请关闭 🔒 挂锁图标并保存更改。

因此，该计算机被添加到 Open Single Management Platform (OSMP) 中。通过查看*应用程序组件状态报告*检查组件的操作状态。您也可以利用 Kaspersky Endpoint Security 的本地界面在报告中查看组件的操作状态。**Endpoint Detection and Response Expert (on-premises)** 组件将被添加到 Kaspersky Endpoint Security 组件列表。

与第三方 EPP 应用程序的兼容性

EDR Agent 支持 Kaspersky Detection and Response 解决方案的功能。保护和控制组件不可用于 EDR Agent。此配置允许安装第三方 EPP 应用程序并在组织的基础设施中部署 Kaspersky Detection and Response 解决方案。EDR Agent 支持 Kaspersky Managed Detection and Response、Kaspersky Anti Targeted Attack Platform (EDR) 和 Kaspersky Anti Targeted Attack Platform (NDR)。

EDR Agent 与以下供应商的 EPP 应用程序兼容：

- **Dr.Web**

  EDR Agent 与 Windows 13.0.1 或更高版本的 Dr.Web 代理和 Dr.Web 服务器 (x64) 13.0.0.10200 兼容。

- **Dallas Lock**

  EDR Agent 与 Dallas Lock 8.0-C 版本 11.4.2.843 或更高版本兼容。

  > 为了使 EDR Agent 在安装了 Dallas Lock 软件的计算机上运行，您必须在防火墙模块的设置中允许连接到卡巴斯基外部服务。

- **Secret Net Studio**

  EDR Agent 与 Secret Net Studio 版本 8.11 或更高版本兼容。

  > 应用程序无法安装在部署了带有反病毒组件的 Secret Net Studio 的计算机上。要实现互操作性，您必须从 Secret Net Studio 中删除反病毒组件。

- **Trend Micro**

EDR Agent 与 Trend Micro Apex One 版本 14.0.12994 或更高版本兼容（包括 Security Agent）。

EDR Agent 与 Trend Micro Deep Security 版本 20.0.2-4960 或更高版本兼容（包括 Security Agent）。

- **Windows Defender**
- **Sophos**

  EDR Agent 与 Sophos Intercept X 版本 2024.1.2 或更高版本（包括 Endpoint Agent）以及 Sophos Core Agent 版本 2024.3.2.3 兼容。

- **Bitdefender**

  EDR Agent 与 Bitdefender Endpoint Security Tools 版本 7.9.21.523 或更高版本兼容。

- **ESET**

  EDR Agent 与 ESET Endpoint Security 版本 12.0.2049.0 或更高版本以及 ESET Management Agent 版本 12.0 或更高版本兼容。

在运行 Windows 11 for Arm64 的计算机上，EDR Agent 与以下系统不兼容：Bitdefender Endpoint Security Tools。

必须按以下顺序安装应用程序：首先安装 EPP 应用程序，然后安装 Kaspersky Security Center 网络代理，最后安装 EDR Agent。这是必要的，因为 EPP 应用程序的安装程序可能会将 EDR Agent 和网络代理检测为不兼容的软件并将其删除。更新第三方 EPP 应用程序后，还应检查 EDR Agent 和网络代理的运行情况，因为其安装程序可能会重新扫描计算机中是否有不兼容的软件并删除这些应用程序。

如果由于安装程序在计算机上发现不兼容的软件而无法在具有第三方 EPP 应用程序的计算机上安装 EDR Agent，您可以跳过不兼容软件检查。

Managed Detection and Response

Kaspersky Endpoint Security for Windows 支持与 Managed Detection and Response 解决方案集成。*Kaspersky Managed Detection and Response (MDR)* 解决方案自动检测和分析您基础架构中的安全事故。为此，MDR 使用从端点和机器学习接收的遥测数据。MDR 发送事故数据到 Kaspersky 专家。然后专家便可以处理事故，例如，添加新条目到反病毒数据库。或者，专家可以发布处理事件的建议，例如，建议将计算机从网络隔离。对于该解决方案如何工作的详情，请参考 Kaspersky Managed Detection and Response 帮助。

Kaspersky Endpoint Security 与 MDR 集成的配置

以下配置可用于与 MDR 配合使用：

- **[KES+内置代理]**。在此配置中，Kaspersky Endpoint Security 既充当确保计算机安全的应用程序，又充当使用 MDR 的应用程序。Kaspersky Endpoint Security 11.6.0 for Windows 或更高版本中提供了内置代理。
- **[第三方 EPP+EDR Agent]**。在此配置中，IT 基础设施的安全性由第三方端点保护平台（EPP）提供。与 MDR 的交互由 Kaspersky Endpoint Security 在“Endpoint Detection and Response Agent（EDR Agent）”配置下提供。在此配置中，EDR Agent 兼容第三方 EPP 应用程序。EDR Agent 在 Kaspersky Endpoint Security 12.3 for Windows 或更高版本中可用。

对以前版本的 Kaspersky Endpoint Security 的支持

Kaspersky Endpoint Security 版本 11 和后续版本支持 MDR 解决方案。Kaspersky Endpoint Security 版本 11 – 11.5.0 仅发送遥测数据到 Kaspersky Managed Detection and Response 以启用威胁检测。Kaspersky Endpoint Security 版本 11.6.0 具有内置代理（Kaspersky Endpoint Agent）的所有功能。

如果您正在使用 Kaspersky Endpoint Security 11 – 11.5.0，您必须更新数据库到最新版本以整合 MDR 解决方案。您还必须安装 Kaspersky Endpoint Agent。

如果您正在使用 Kaspersky Endpoint Security 11.6.0 或更高版本，您不需要安装 Kaspersky Endpoint Agent 就可以使用 MDR 解决方案。

> 如果 Kaspersky Endpoint Security 策略还应用到未安装 Kaspersky Endpoint Security 11 – 11.5.0 的计算机，您必须先为这些计算机创建单独的 Kaspersky Endpoint Agent 策略。在新策略中，配置与 Kaspersky Managed Detection and Response 的整合。

内置代理与 MDR 的集成

要设置与 Kaspersky Managed Detection and Response 的整合，您必须启用 Managed Detection and Response 组件并配置 Kaspersky Endpoint Security。

为了 Kaspersky Managed Detection and Response 通过 Kaspersky Security Center Web Console 与管理服务器协作，您必须建立新的安全连接，一个*后台连接*。Kaspersky Managed Detection and Response 在您部署解决方案时提示您建立后台连接。确保后台连接已建立。

在 Web Console 中建立后台连接

1. 在 Web Console 的主窗口中，选择“**设置**” → “**整合**”。
2. 转到**整合**区域。
3. 开启 **用于整合的后台连接 已启用**切换开关。
4. 保存更改。

与 Kaspersky Managed Detection and Response 的整合包括以下步骤：

1. **安装“Managed Detection and Response”组件**

   您可以在安装或升级过程中选择 MDR 组件，也可以使用“*更改应用程序组件*”任务。

   > 要使用 *更改应用程序组件* 任务安装 Managed Detection and Response 组件且不重启计算机，您需要在任务设置中禁用 **检查不兼容的第三方应用程序** 选项。

2. **配置卡巴斯基私有安全网络**

   > 如果您正在使用 Kaspersky Security Center 云控制台则跳过此步骤。Kaspersky Security Center 云控制台在安装 MDR 插件时自动配置卡巴斯基私有安全网络。

*卡巴斯基私有安全网络*是让运行 Kaspersky Endpoint Security 或其他卡巴斯基应用程序的计算机的用户获得卡巴斯基信誉数据库以及其他统计数据的访问权限的解决方案，无需从他们自己的计算机向卡巴斯基发送数据。

在管理服务器属性中上传卡巴斯基安全网络配置文件。卡巴斯基安全网络配置文件存在于 MDR 配置文件的 ZIP 存档中。您可以在 Kaspersky Managed Detection and Response 控制台获取 ZIP 存档。对于配置卡巴斯基私有安全网络的详情，请参考 Kaspersky Security Center 帮助。您也可以从命令行上传卡巴斯基安全网络配置文件到计算机（参见以下说明）。

如何从命令行配置卡巴斯基私有安全网络

1. 以管理员身份运行命令行解释器 (cmd.exe)。
2. 转到 Kaspersky Endpoint Security 可执行文件所在文件夹。
3. 运行以下命令：

```
avp.com KSN /private <file name>
```

`<file name>`是包含卡巴斯基私有安全网络设置的配置文件名称 (PKCS7 或 PEM 文件格式)。

例如：
```
avp.com KSN /private C:\kpsn_config.pkcs7
```

结果，Kaspersky Endpoint Security 将使用卡巴斯基私有安全网络决定文件、应用程序和网站的信誉。策略设置的"**卡巴斯基安全网络**"区域将显示以下运行状态： *基础设施: 卡巴斯基私人安全网络*。

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

3 激活 Kaspersky Managed Detection and Response

从 Kaspersky Endpoint Security for Windows 12.10 开始，要激活 Managed Detection and Response 功能，作为激活码的替代方案，您还可以使用密钥文件。

Kaspersky Managed Detection and Response 支持以下授权许可方式：

- Managed Endpoint Detection and Response 功能被包含在 Kaspersky Endpoint Security for Windows 授权许可中。

  该功能将在激活 Kaspersky Endpoint Security for Windows 后立即可用。

- MDR 使用单独的许可证（Kaspersky Managed Detection and Response 插件）。

  该功能将在为 Kaspersky Managed Detection and Response 加载项添加单独密钥后可用。因此，计算机上将添加两个密钥：Kaspersky Endpoint Security 密钥和 Kaspersky Managed Detection and Response 密钥。

  独立 Managed Detection and Response 功能的授权许可与 Kaspersky Endpoint Security 授权许可相同。

确保 MDR 功能包含在授权许可中，并在应用程序的本地界面中工作。

4 启用 Managed Detection and Response 组件

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 文件存在于 MDR 配置文件的 ZIP 存档中。您可以在 Kaspersky Managed Detection and Response 控制台获取 ZIP 存档。对于 BLOB 文件的详情，请参考 Kaspersky Managed Detection and Response 帮助。

从 Kaspersky Endpoint Security 12.6 for Windows 开始，如果您拥有当前授权许可，则可以选择为无租户的 Kaspersky Managed Detection and Response 添加 BLOB 文件。

如何在管理控制台 (MMC) 中启用 Managed Detection and Response 组件

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **Detection and Response → Managed Detection and Response (Industrial CyberSecurity)**。
4. 选择**Managed Detection and Response (Industrial CyberSecurity)**复选框。
5. 在**设置**块，单击**上传**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。

   > 默认情况下，用户可以管理应用程序设置（“挂锁”处于打开状态 ）。要在计算机上应用该策略，请关闭“挂锁”。

6. 保存更改。

如何在 Web Console 和云控制台中启用 Managed Detection and Response 组件

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

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置 → Managed Detection and Response**。
5. 开启 **Managed Detection and Response 已启用**切换开关。
6. 单击**上传**并选择在 Kaspersky Managed Detection and Response 控制台获取的 BLOB 文件。该文件具有 P7 扩展名。

   > 默认情况下，用户可以管理策略设置（“挂锁”处于打开状态 ）。要在计算机上应用该策略，请关闭“挂锁”。

7. 保存更改。

如何从命令行启用 Managed Detection and Response 组件

1. 以管理员身份运行命令行解释器 (cmd.exe)。
2. 转到 Kaspersky Endpoint Security 可执行文件所在文件夹。

3. 运行以下命令：

```
avp.com MDRLICENSE /ADD <file name> /login=<user name> /password=<password>
```

> 要执行此命令，必须启用密码保护。用户必须具有“**配置应用程序设置**”权限。

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 文件被成功验证，Kaspersky Endpoint Security 将下载文件并在与 Kaspersky Security Center 的下次同步过程中发送该文件到计算机。通过查看*应用程序组件状态报告*检查组件的操作状态。您也可以利用 Kaspersky Endpoint Security 的本地界面在报告中查看组件的操作状态。**Managed Detection and Response** 组件将被添加到 Kaspersky Endpoint Security 组件列表。

5. **配置应用程序的其他组件以接收遥测数据**

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

- 卡巴斯基安全网络（扩展模式）。
- 行为检测。
- 漏洞利用防御。
- Web 威胁防护。
- 邮件威胁防护。
- 文件威胁防护。
- 网络威胁防护。
- 防火墙。
- AMSI 保护。
- 后台扫描。

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置** → **Managed Detection and Response**。
5. 开启 **Managed Detection and Response** **已启用**切换开关。
6. 保存更改。

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **Detection and Response** → **Managed Detection and Response (Industrial CyberSecurity)**。

4. 选择**Managed Detection and Response (Industrial CyberSecurity)**复选框。

5. 保存更改。

MDR 的 KEA 到 KES 迁移指南

Kaspersky Endpoint Security for Windows 包括用于 Managed Detection and Response 解决方案的内置代理。您不再需要单独的 Kaspersky Endpoint Agent 应用程序与 MDR 一起使用。Kaspersky Endpoint Agent 的所有功能将由 Kaspersky Endpoint Security 执行。

当您在安装了 Kaspersky Endpoint Agent 的计算机上部署 Kaspersky Endpoint Security 时，Kaspersky Managed Detection and Response 解决方案将继续与 Kaspersky Endpoint Security 一起工作。此外，Kaspersky Endpoint Agent 将被从计算机卸载。当您将 Kaspersky Endpoint Security 更新到版本 11.6.0 或更高版本时，系统中会发生相同的行为。

Kaspersky Endpoint Security 与 Kaspersky Endpoint Agent 不兼容。您不能在同一台计算机上安装这两个应用程序。

Kaspersky Endpoint Security 必须满足以下条件才能作为 Kaspersky Managed Detection and Response 的一部分工作：

- Kaspersky Security Center 版本 13.2 或更高版本（包括网络代理）。在 Kaspersky Security Center 的早期版本中，无法激活 Managed Detection and Response 功能。
- 建立了 Kaspersky Security Center Web Console 和管理服务器之间的后台连接。为了 MDR 通过 Kaspersky Security Center Web Console 与管理服务器协作，您必须建立新的安全连接，一个“*后台连接*”。

MDR 的迁移 [KES+KEA] 配置到 [KES+内置代理] 的步骤

1. **升级 Kaspersky Endpoint Security 管理插件**

   MDR 组件可以使用 Kaspersky Endpoint Security 管理插件版本 11.6 或更高版本进行管理。根据您使用的 Kaspersky Security Center 控制台类型，更新管理控制台（MMC）中的管理插件或 Web Console 中的 Web 插件。

2. **迁移策略和任务**

   将 Kaspersky Endpoint Agent 设置传输到 Kaspersky Endpoint Security for Windows。下列选项可用：

   - 从 Kaspersky Endpoint Agent 迁移到 Kaspersky Endpoint Security 的向导。从 Kaspersky Endpoint Agent 迁移到 Kaspersky Endpoint Security 的向导仅适用于 Web Console

     如何在 Web Console 中将策略和任务设置从 Kaspersky Endpoint Agent 迁移到 Kaspersky Endpoint Security

     在 Web Console 的主窗口中，选择“**操作**” → “**从 Kaspersky Endpoint Agent 迁移**”。

     这将运行策略和任务迁移向导。按照向导的说明进行操作。

步骤 1. 策略迁移

迁移向导将创建一个新策略，该策略将合并 Kaspersky Endpoint Security 和 Kaspersky Endpoint Agent 策略的设置。在策略列表中，选择要将其设置与 Kaspersky Endpoint Security 策略合并的 Kaspersky Endpoint Agent 策略。单击 Kaspersky Endpoint Agent 策略以选择您要与之合并设置的 Kaspersky Endpoint Security 策略。确保选择了正确的策略，然后转到下一步。

步骤 2. 任务迁移

迁移向导不支持 MDR 任务。跳过此步骤。

步骤 3. 向导完成

退出向导。作为向导的结果，将创建一个新的 Kaspersky Endpoint Security 策略。策略从 Kaspersky Endpoint Security 和 Kaspersky Endpoint Agent 合并设置。策略被叫做 *<Kaspersky Endpoint Security 策略名称> 和 <Kaspersky Endpoint Agent 策略名称>*。新策略具有*不活动*状态。要继续，将 Kaspersky Endpoint Agent 和 Kaspersky Endpoint Security 策略的状态更改为*不活动*并激活新合并的策略。

- 标准的策略和任务批量转换向导。策略和任务批量转换向导仅在管理控制台（MMC）中可用。有关策略和任务批量转换向导的详细信息，请参阅 Kaspersky Security Center 帮助。

3. **授权 MDR 功能**

要将 Kaspersky Endpoint Security 作为 Kaspersky Managed Detection and Response 解决方案的一部分激活，您需要单独的 Kaspersky Managed Detection and Response 加载项授权许可。您可以使用"*添加密钥*"任务添加密钥。结果，两个密钥将被添加到应用程序中：*Kaspersky Endpoint Security* 和 *Kaspersky Managed Detection and Response*。

4. **安装/升级 Kaspersky Endpoint Security 应用程序**

要在应用程序安装或升级期间迁移 MDR 功能，建议使用远程安装任务。创建远程安装任务时，您需要在安装包设置中选择 MDR 组件。

您还可以使用以下方法升级应用程序：

- 使用卡巴斯基更新服务。
- 本地使用安装向导。

Kaspersky Endpoint Security 支持在安装了 Kaspersky Endpoint Agent 应用程序的计算机上升级应用程序时自动选择组件。组件的自动选择取决于升级应用程序的用户账户的权限。

如果您在系统账户（SYSTEM）下使用 EXE 或 MSI 文件升级 Kaspersky Endpoint Security，Kaspersky Endpoint Security 获得对卡巴斯基解决方案的当前授权许可的访问权。因此，如果计算机安装了 Kaspersky Endpoint Agent，并且激活了 MDR 解决方案，则 Kaspersky Endpoint Security 安装程序将自动配置组件集并选择 MDR 组件。这将使 Kaspersky Endpoint Security 切换到使用内置代理并卸载 Kaspersky Endpoint Agent。在系统账户（SYSTEM）下运行 MSI 安装程序通常在通过卡巴斯基更新服务升级时执行，或者当通过 Kaspersky Security Center 部署安装包时。

如果您在非特权用户账户下使用 MSI 文件升级 Kaspersky Endpoint Security，Kaspersky Endpoint Security 缺少对卡巴斯基解决方案的当前授权许可的访问权。在这种情况下，Kaspersky Endpoint Security 会根据 Kaspersky Endpoint Agent 的一组组件自动选择组件。此后，Kaspersky Endpoint Security 将切换到使用内置代理并卸载 Kaspersky Endpoint Agent。

> Kaspersky Endpoint Security 支持在不重启计算机的情况下升级。您可以选择策略属性中的应用程序升级模式。

5. **检查应用程序运行情况**

   如果在应用程序安装或升级之后，计算机在 Kaspersky Security Center 控制台显示"*严重*"状态：

   - 确保计算机安装了网络代理版本 13.2 或更高版本。
   - 通过查看"*应用程序组件状态报告*"检查内置代理的操作状态。如果组件具有*未安装*状态，使用"*更改应用程序组件*"任务安装组件。如果一个组件有"*授权许可不支持*"状态，确保您已激活内置代理功能。
   - 确保您在 Kaspersky Endpoint Security for Windows 的新策略中接受了卡巴斯基安全网络声明。

Endpoint Detection and Response

	Kaspersky Endpoint Security for Windows 包含 Kaspersky Endpoint Detection and Response Optimum 解决方案（也叫"EDR Optimum"）的内置代理。从 11.8.0 开始，Kaspersky Endpoint Security for Windows 包含 Kaspersky Endpoint Detection and Response Expert 解决方案（也叫"EDR Expert"）的内置代理。*Kaspersky Endpoint Detection and Response* 是一种保护企业 IT 基础架构免受高级网络威胁的一系列解决方案。该解决方案的功能将自动检测威胁与应对这些威胁的能力结合起来，以抵御高级攻击，包括新的漏洞利用、勒索软件、无文件攻击以及使用合法系统工具的方法。EDR Expert 比 EDR Optimum 提供更多的威胁监控和响应功能。有关解决方案的更多信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助 和 Kaspersky Endpoint Detection and Response Expert 帮助 。

威胁情报工具

Kaspersky Endpoint Detection and Response 使用以下 Threat Intelligence 工具：

- 与卡巴斯基威胁情报门户 集成，该系统包含并显示有关文件和网址信誉的信息。
- 卡巴斯基威胁 数据库。
- 卡巴斯基安全网络（以下也称为"KSN"）云服务基础设施，提供对 Kaspersky 知识库中实时文件、网站和软件信誉信息的访问。使用卡巴斯基安全网络的数据可确保 Kaspersky 应用程序能够更快地对新威胁作出响应，提高一些保护组件的性能，并减少误报风险。
- 允许您在隔离环境中运行检测到的文件并检查其信誉的 Cloud Sandbox 技术。

解决方案的工作原理

Kaspersky Endpoint Detection and Response 查看和分析威胁发展，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 在单独的窗口显示警报详情。*警报*是企业 IT 基础设施中发生的事件，应用程序将其识别为异常或可疑，并可能对企业 IT 基础设施构成安全威胁。*警报详情*是一种工具，用于查看所收集的有关检测到的威胁的全部信息。警报详情包括，例如，出现在计算机的文件历史。有关管理警报详情的更多信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助 和 Kaspersky Endpoint Detection and Response Expert 帮助 。

对以前版本的 Kaspersky Endpoint Security 的支持

如果您正在使用 Kaspersky Endpoint Security 11.2.0–11.6.0 与 Kaspersky Endpoint Detection and Response Optimum 进行互操作，则应用程序包含 Kaspersky Endpoint Agent。您可以将 Kaspersky Endpoint Agent 与 Kaspersky Endpoint Security 一起安装。在 Kaspersky Endpoint Security 11.9.0 中，Kaspersky Endpoint Agent 分发包不再是 Kaspersky Endpoint Security 分发包的一部分。

> Kaspersky Endpoint Detection and Response Expert 解决方案不支持与 Kaspersky Endpoint Agent 协同工作。Kaspersky Endpoint Detection and Response Expert 解决方案使用带有内置代理（版本 11.8.0 或更新版本）的 Kaspersky Endpoint Security。

内置代理与 EDR Optimum / EDR Expert 的集成

要设置与 Kaspersky Managed Detection and Response 的整合，您必须添加 Endpoint Detection and Response Optimum 组件或 Endpoint Detection and Response Expert (cloud) 组件并配置 Kaspersky Endpoint Security。

> “Endpoint Detection and Response Optimum”、“Endpoint Detection and Response Expert (cloud)”和 “Endpoint Detection and Response Expert (on-premises)”组件彼此不兼容。

Endpoint Detection and Response 必须满足以下条件才能工作：

- Kaspersky Security Center 版本 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。

  从 Kaspersky Endpoint Security 12.6 版开始，警报详细信息的显示已从 Kaspersky Endpoint Security 管理插件移至 EDR 管理插件。EDR 管理插件是一个用于与 Windows、Mac 和 Linux 操作系统上的代理协同工作的单一插件。现在，当使用 EDR Optimum 时，您将需要 Kaspersky Endpoint Security 管理插件来创建威胁响应任务，以及 EDR 管理插件来查看警报详细信息。
- 作为 Kaspersky Endpoint Security 一部分的 Endpoint Detection and Response Optimum 组件支持与 Kaspersky Endpoint Detection and Response Optimum 2.0 解决方案的交互。与 Kaspersky Endpoint Detection and Response Optimum 版本 1.0 的交互不被支持。

- EDR Optimum 可以在 Kaspersky Security Center Web Console 和 Kaspersky Security Center 云控制台中被管理。

  EDR Expert 功能只能使用 Kaspersky Security Center 云控制台进行管理。您无法使用管理控制台(MMC)管理此功能。

- 应用程序已激活，授权许可涵盖了该功能。

- Endpoint Detection and Response 组件被开启。

- Endpoint Detection and Response 所依赖的应用程序组件被启用并可以操作。Endpoint Detection and Response 依赖以下组件：

  - 文件威胁防护。
  - Web 威胁防护。
  - 邮件威胁防护。
  - 漏洞利用防御。
  - 行为检测。
  - 主机入侵防御。
  - 修复引擎。
  - 自适应异常控制。

与 Kaspersky Endpoint Detection and Response 的整合包括以下步骤：

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

   您可以在安装或升级过程中选择 Endpoint Detection and Response Optimum 组件或 Endpoint Detection and Response Expert (cloud) 组件，也可以使用"*更改应用程序组件*"任务。

   > 您必须重新启动计算机才能使用新组件完成应用程序的升级。

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

   您可以通过以下方式获得使用 Kaspersky Endpoint Detection and Response 的授权许可：

   - Endpoint Detection and Response 功能被包含在 Kaspersky Endpoint Security for Windows 授权许可中。

     该功能将在激活 Kaspersky Endpoint Security for Windows 后立即可用。

   - 为 EDR Optimum 或 EDR Expert（Kaspersky Endpoint Detection and Response 加载项）购买单独的授权许可。

     该功能将在为 Kaspersky Endpoint Detection and Response 添加单独密钥后可用。因此，计算机上将添加两个密钥：Kaspersky Endpoint Security 密钥和 Kaspersky Endpoint Detection and Response 密钥。

     独立 Endpoint Detection and Response 功能的授权许可与 Kaspersky Endpoint Security 的相同。

   确保授权许可中包含 EDR Optimium 或 EDR Expert 功能，并且该功能正在应用程序的本地界面中运行。

   有关 EDR Optimum 的最终用户授权许可协议的更多信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助。

3 启用 Endpoint Detection and Response 组件

您可以在 Kaspersky Endpoint Security for Windows 策略设置中启用或禁用组件。

如何在 Web Console 和云控制台中启用或禁用 Endpoint Detection and Response 组件

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

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置** → **Endpoint Detection and Response**。
5. 开启 **Endpoint Detection and Response 已启用**切换开关。
6. 保存更改。

Kaspersky Endpoint Detection and Response 组件被启用。通过查看*应用程序组件状态报告*检查组件的操作状态。您也可以利用 Kaspersky Endpoint Security 的本地界面在报告中查看组件的操作状态。**Endpoint Detection and Response Optimum** 或 **Endpoint Detection and Response Expert (cloud)** 组件被添加到 Kaspersky Endpoint Security 组件列表。

4 启用到管理服务器的数据传输

要启用所有 Endpoint Detection and Response 功能，需要对以下数据类型启用传输：

- 隔离文件数据。

  这些数据是通过 Web 控制台和云控制台获取计算机上隔离的文件信息所必需的。例如，您可以从隔离区下载一个文件，以便在 Web 控制台和云控制台中进行分析。
- 威胁发展链数据。

  这些数据是在 Web 控制台和云控制台中获取计算机上检测到的威胁的信息所必需的。您可以在 Web 控制台和云控制台中查看警报详细信息并采取响应操作。

如何在 Web 控制台和云控制台中启用到管理服务器的数据传输

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

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **KSC 整合**。
5. 在“**到管理服务器的数据传输**”区域，单击“**高级设置**”链接。
6. 在打开的窗口中，选择以下复选框：
   - “**关于隔离区文件**”。
   - “**关于威胁发展链**”。
7. 要将此策略应用到计算机，请关闭 🔒 挂锁图标并保存更改。

妥协的指标扫描（标准任务）

妥协的指标 (IOC) 是一组关于对象或活动的数据，表示未经授权访问计算机（数据泄露）。例如，许多登录系统的尝试都不成功，这可能构成妥协的指标。*IOC 扫描*任务允许在计算机上查找妥协的指标，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数检测的指标集的文件。IOC 文件必须符合 OpenIOC 标准。

IOC 扫描任务运行模式

Kaspersky Endpoint Detection and Response 允许您创建标准 IOC 扫描任务以检测受损数据。*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。任务使用用户准备的 IOC 文件运行。如果您要手动添加入侵指标，请阅读 IOC 文件需求。

您可以通过单击下面的链接下载该文件，该文件包含一个表，其中包含 OpenIOC 标准的 IOC 术语的完整列表。

下载 IOC_TERMS.XLSX 文件

当 Kaspersky Endpoint Security 作为“Kaspersky Sandbox”解决方案的一部分使用时，它也支持独立 IOC 扫描任务。

创建 IOC 文件

从 Kaspersky Endpoint Security 12.10 for Windows 开始，您可以直接在任务设置中创建 IOC 文件。要创建 IOC 文件，您必须准备一个包含入侵指标列表的 TXT 文件。您可以添加以下对象的列表作为入侵指标：

- 文件哈希（MD5/SHA256）。

  应用程序准备一个 IOC 文件，其中包含 FileItem/Md5sum 或者 FileItem/Sha256sum 扫描范围。

- IP 地址（IPv4、IPv6）。

  应用程序准备一个 IOC 文件，其中包含 PortItem/RemoteIP 扫描范围。

- DNS 名称。

  应用程序准备一个 IOC 文件，其中包含 DnsEntryItem/RecordName 扫描范围。

如何在 Web Console 中创建 IOC 文件

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

   任务列表打开。

2. 选择“**IOC 扫描**”任务。

   任务属性窗口将打开。如果必要，创建“**IOC 扫描**”任务。

3. 选择**应用程序设置**选项卡。

4. 转到**威胁扫描**区域。

5. 单击“**重定义 IOC 文件**”。

6. 这将打开用于创建 IOC 文件的表单：

   a. 在“**IOC 文件源**”下，选择“**从文件生成**”。

   b. 输入 IOC 文件的名称。

   c. 选择一个包含入侵指标列表的 TXT 文件。

   d. 选择 IOC 文件的类型：**DNS 名称**、**文件哈希**、**IP 地址**。

   e. 单击“**生成**”。

   Kaspersky Endpoint Security 将 IOC 文件添加到 IOC 收集中。如有必要，您可以暂时将 IOC 文件排除在任务范围之外。

7. 保存更改。

创建一个“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）。

  *警报详情*是一种工具，用于查看所收集的有关检测到的威胁的全部信息。警报详情包括，例如，出现在计算机的文件历史。有关管理警报详情的更多信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助和 Kaspersky Endpoint Detection and Response Expert 帮助。

- 使用任务向导。

> 您可以在 Web 控制台和云控制台中为 EDR Optimum 配置任务。EDR Expert 的任务设置仅在云控制台中可用。

创建一个“IOC 扫描”任务：

1. 在 Web Console 的主窗口中，选择“**任务**”。

   任务列表打开。

2. 单击“**添加**”。

   “任务向导”将启动。

3. 配置任务设置：

   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Endpoint Security for Windows 14.2.0**”。

   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，输入简要说明。

d. 在“**要对其分配任务的设备**”块，选择任务范围。

4. 按照所选任务范围选项选择设备。转到下一步。

5. 输入要使用其权限运行任务的用户的账户凭证。转到下一步。

> 默认下，Kaspersky Endpoint Security 以系统用户账户 (SYSTEM) 启动任务。

系统账户（SYSTEM）没有权限在网络驱动器上执行 *IOC 扫描*任务。如果您要为网络驱动器运行任务，选择对该驱动器具有访问权限的用户账户。

> 对于网络驱动器上的独立 IOC 扫描任务，您需要在任务属性中手动选择具有该驱动器访问权限的用户账户。

6. 结束向导。

   在任务列表中将显示一个新任务。

7. 单击新任务。

   任务属性窗口将打开。

8. 选择**应用程序设置**选项卡。

9. 转到**威胁扫描**区域。

10. 上传 IOC 文件以搜索入侵指标。

    上传 IOC 文件后，应用程序会显示有关该文件的摘要信息，包括未通过检查的指标列表。上传 IOC 文件后，您可以直接在任务属性中手动在内置编辑器中编辑文件。Kaspersky Endpoint Security 支持编辑符合 OpenIOC 1.1 标准的 IOC 文件。无法修改符合 OpenIOC 1.0 版本的 IOC 文件的内容。

    Kaspersky Endpoint Security 将 IOC 文件添加到 IOC 收集中。如有必要，您可以暂时将 IOC 文件排除在任务范围之外。

    > 不建议在运行任务后添加或删除 IOC 文件。这可能会导致 IOC 扫描结果在任务之前的运行中显示不正确。要通过新的 IOC 文件搜索妥协的指标，建议添加新任务。

11. 如有必要，选中“**IOC 追溯扫描**”复选框。*回顾性 IOC 扫描*是 *IOC 扫描* 任务的一种模式，在该模式下，Kaspersky Endpoint Security 使用特定时间段的数据扫描入侵指标。此模式旨在通过受保护计算机的遥测数据（例如网络活动、进程、文件和其他遥测数据）来搜索入侵指标。Kaspersky Endpoint Security 分析计算机上的操作系统日志和浏览器日志中的数据。回顾性 IOC 扫描分析以下浏览器的日志：Google Chrome、Mozilla Firefox、Microsoft Edge（版本 79 或更高版本）。

12. 配置 IOC 检测操作：

    - “**将设备与网络隔离**”。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。

      如果清除此复选框，您可以在手动运行任务后将计算机与网络隔离。如果“*IOC 扫描*”任务检测到 IOC，您可以直接从 IOC 将计算机与网络隔离（*IOC 扫描* → **应用程序设置** → **IOC 扫描结果**）。Kaspersky Endpoint Security 还允许立即管理其他设置：网络隔离禁用期和网络隔离排除项。

- “**将副本移动到隔离区，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。

  如果清除此复选框，您可以在手动运行任务后手动隔离该文件。如果“*IOC 扫描*”任务检测到可能危及数据的文件，您可以直接从 IOC 扫描结果中隔离此文件（**应用程序设置** → **IOC 扫描结果**）。因此，Kaspersky Endpoint Security 将使用检测到的文件的预设数据启动任务创建向导。您只需要管理额外的任务设置，例如设置任务计划。

- “**运行关键区域扫描**”。如果选择此选项，Kaspersky Endpoint Security 运行*关键区域扫描*任务。默认情况下，Kaspersky Endpoint Security 会扫描内核内存、运行进程和磁盘的引导扇区。

13. 转到**高级**区域。

14. 选择作为任务的一部分必须被分析的数据类型 (IOC 文档)。

> Kaspersky Endpoint Security 根据加载的 IOC 文件的内容自动选择“*IOC 扫描*”任务的数据类型（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：

- “**文件 – FileItem**”。使用预设范围在计算机上设置 IOC 扫描范围。

  默认下，Kaspersky Endpoint Security 仅在计算机的重要区域扫描 IOC，例如“下载”文件夹、桌面、临时操作系统文件文件夹等等。您也可以手动添加扫描范围。

- “**Windows 事件日志 - EventLogItem**”。输入记录事件的时间段。您还可以选择必须使用哪些 Windows 事件日志进行 IOC 扫描。默认情况下，会选择以下事件日志：应用程序事件日志、系统事件日志和安全事件日志。

- “**Windows 注册表 - RegistryItem**”。在注册表中配置 IOC 扫描范围。

  默认情况下，Kaspersky Endpoint Security 扫描一组注册表项。

15. 在任务属性窗口中，选择“**计划**”选项卡。

16. 配置任务计划。

> “Wake-on-LAN”不可用于此任务。确保计算机已打开以运行任务。

17. 保存更改。

18. 选中该任务旁边的复选框。

19. 单击“**开始**”。

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“**结果**”部分的“任务属性”中查看任务结果。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**。在 IOC 扫描结果中，您还可以手动隔离检测到的文件或者将计算机与网络隔离。

Kaspersky Endpoint Security 会在为同一 IOC 文件创建的记录中查找重复项，并仅在任务结果中保留唯一记录。重复项是同一类型的记录，所有比较字段的值都相同。如果应用程序在一个或多个字段中缺少值，也可能不会创建记录（见下表）。

类型	比较字段	不创建记录的条件
FileItem	• FullPath • Md5sum • Sha256sum • PID • UPID • ImagePath	• 缺失 FullPath、Md5sum、Sha256sum字段的值。 • FullPath 字段的值缺失，且 Md5sum、Sha256sum 字段的值相同。
RegistryItem	• Hive • KeyPath • ValueName • Text • Type	以下字段中至少一个缺少值：Hive、KeyPath、ValueName。
ProcessItem	• startTime • PID	缺失 startTime 或者 PID 字段的值。

"**警报详情**"窗口可能会显示具有相同字段值的 RegistryItem 记录。此类记录不属于重复，因为它们的文本字段值不同，不会显示在界面中。

IOC 扫描结果被保存 30 天。在此时间之后，Kaspersky Endpoint Security 将自动删除最早条目。

IOC 扫描的扩展遥测

我们建议在计算机上启用扩展遥测以进行回顾性 IOC 扫描。扩展遥测提高了 IOC 检测的准确性，但会占用更多的计算机资源。

扩展遥测包括对以下附加术语的支持：

- FileItem/Md5sum
- FileItem/Sha256sum
- FileItem/SizeInBytes
- FileItem/Created
- FileItem/Modified
- FileItem/Changed
- FileItem/Accessed
- FileItem/FileAttributes

如果禁用扩展遥测，Kaspersky Endpoint Security 可能会轮换有关检测到的入侵指标的信息。

要启用扩展遥测：

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

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置** → **Endpoint Detection and Response**。
5. 选择**启用高级系统活动日志记录**复选框。
6. 保存更改。

移动文件到隔离区

在应对威胁时，Kaspersky Endpoint Detection and Response 可以创建*移动文件到隔离区*任务。这对于将威胁的后果降至最低是必要的。*隔离区*是计算机上的一个特别的本地存储区。用户可以隔离用户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 仅在与 Kaspersky Detection and Response 解决方案集成时使用隔离。在其他情况下，Kaspersky Endpoint Security 将相关文件置于备份中。有关将隔离管理作为解决方案的一部分的详细信息，请参阅 Kaspersky Sandbox 帮助、Kaspersky Endpoint Detection and Response Optimum 帮助、Kaspersky Endpoint Detection and Response Expert 帮助、Kaspersky Anti Targeted Attack Platform 帮助 和 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助。

您可以用以下方式创建*移动文件到隔离区*任务：

- 在警报详细信息中（仅适用于 EDR Optimum）。

  *警报详情*是一种工具，用于查看所收集的有关检测到的威胁的全部信息。警报详情包括，例如，出现在计算机的文件历史。有关管理警报详情的更多信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助和 Kaspersky Endpoint Detection and Response Expert 帮助。
- 使用任务向导。

  必须输入文件路径或哈希（SHA256 或 MD5），或者同时输入文件路径和文件哈希。
- 在“*IOC 扫描*”任务设置中。

  如果“*IOC 扫描*”任务检测到可能危及数据的文件，您可以直接从 IOC 扫描结果中隔离此文件（**应用程序设置** → **IOC 扫描结果**）。因此，Kaspersky Endpoint Security 将使用检测到的文件的预设数据启动任务创建向导。您只需要管理额外的任务设置，例如设置任务计划。

“*移动文件到隔离区*”任务具有以下限制：

1. 文件大小不得超过 100 MB。
2. 系统关键对象(SCO)无法被隔离。SCO 是操作系统和 Kaspersky Endpoint Security for Windows 应用程序运行所需的文件。
3. 您可以在 Web 控制台和云控制台中为 EDR Optimum 配置任务。EDR Expert 的任务设置仅在云控制台中可用。
4. 您无法扫描被“*移动文件到隔离区*”任务隔离的对象。

创建一个“移动文件到隔离区”任务：

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。

2. 单击“**添加**”。
   “任务向导”将启动。

3. 配置任务设置：

   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Endpoint Security for Windows 14.2.0**”。

   b. 在“**任务类型**”下拉列表中，选择“**移动文件到隔离区**”。

   c. 在“**任务名称**”字段中，输入简要说明。

   d. 在“**要对其分配任务的设备**”块，选择任务范围。

4. 按照所选任务范围选项选择设备。单击“**下一步**”。

5. 输入要使用其权限运行任务的用户的账户凭证。单击“**下一步**”。

   > 默认下，Kaspersky Endpoint Security 以系统用户账户 (SYSTEM) 启动任务。

6. 单击“**完成**”按钮完成向导。
   在任务列表中将显示一个新任务。

7. 单击新任务。
   任务属性窗口将打开。

8. 选择**应用程序设置**选项卡。

9. 在文件列表中，单击“**添加**”。
   文件添加向导将启动。

10. 要添加文件，您必须输入文件的完整路径或哈希值和路径两者。

    > 如果文件位于网络驱动器上，请输入以“`\\`”开头的文件路径，而不是驱动器盘符。例如，`\\server\shared_folder\file.exe`。如果文件路径包含网络驱动器盘符，则可能会出现“*未找到文件*”错误。

11. 在任务属性窗口中，选择“**计划**”选项卡。

12. 配置任务计划。

    > “Wake-on-LAN”不可用于此任务。确保计算机已打开以运行任务。

13. 保存更改。

14. 选中该任务旁边的复选框。

15. 单击“**开始**”。

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

如果文件被其他进程锁定，则任务显示为*已完成*，但文件本身只有在计算机重新启动后才会被隔离。重新启动计算机后，确认文件已删除。

如果试图隔离当前正在运行的可执行文件，则“*移动文件到隔离区*”任务可能会以“*访问被拒绝*”错误结束。为文件创建终止进程任务，然后重试。

如果试图隔离太大的文件，则“*移动文件到隔离区*”任务可能会以“*隔离区存储空间不足*”错误结束。清空隔离区或扩大隔离区。然后再次尝试。

您可以使用 Web Console 从隔离区恢复文件或清空隔离区。您可以使用命令行在计算机上本地恢复对象。

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。执行任务后，文件将保存在隔离区中。*隔离区*是计算机上的一个特别的本地存储区。您可以使用 Web Console 将此文件从隔离区下载到您的计算机（**操作** → **存储** → **隔离区**）。在用户的计算机上，文件保留在其原始文件夹中。

文件大小不得超过 100 MB。

您可以在 Web 控制台和云控制台中为 EDR Optimum 配置任务。EDR Expert 的任务设置仅在云控制台中可用。

创建一个“获取文件”任务：

1. 在 Web Console 的主窗口中，选择“**任务**”。

   任务列表打开。

2. 单击“**添加**”。

   “任务向导”将启动。

3. 配置任务设置：

   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Endpoint Security for Windows 14.2.0**”。

   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，输入简要说明。

   d. 在“**要对其分配任务的设备**”块，选择任务范围。

4. 按照所选任务范围选项选择设备。单击“**下一步**”。

5. 输入要使用其权限运行任务的用户的账户凭证。单击“**下一步**”。

> 默认下，Kaspersky Endpoint Security 以系统用户账户 (SYSTEM) 启动任务。

6. 单击“**完成**”按钮完成向导。
   在任务列表中将显示一个新任务。

7. 单击新任务。
   任务属性窗口将打开。

8. 选择**应用程序设置**选项卡。

9. 在文件列表中，单击“**添加**”。
   文件添加向导将启动。

10. 要添加文件，您必须输入文件的完整路径或哈希值和路径两者。

> 如果文件位于网络驱动器上，请输入以“`\\`”开头的文件路径，而不是驱动器盘符。例如，`\\server\shared_folder\file.exe`。如果文件路径包含网络驱动器盘符，则可能会出现“*未找到文件*”错误。

11. 在任务属性窗口中，选择“**计划**”选项卡。

12. 配置任务计划。

> “Wake-on-LAN”不可用于此任务。确保计算机已打开以运行任务。

13. 保存更改。

14. 选中该任务旁边的复选框。

15. 单击“**开始**”。

结果，Kaspersky Endpoint Security 创建文件的副本并将其移动到隔离区。您可以在 Web Console 中从隔离区下载文件。

删除文件

您可以使用“*删除文件*”任务远程删除文件。例如，您可以在响应威胁时远程删除文件。

“*删除文件*”任务具有以下限制：

- System Critical Object (SCO) 无法删除。SCO 是操作系统和 Kaspersky Endpoint Security 应用程序运行所需的文件。

- 您可以在 Web 控制台和云控制台中为 EDR Optimum 配置任务。EDR Expert 的任务设置仅在云控制台中可用。

创建一个“删除文件”任务：

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
2. 单击“**添加**”。
   “任务向导”将启动。
3. 配置任务设置：
   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Endpoint Security for Windows 14.2.0**”。
   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，输入简要说明。
   d. 在“**要对其分配任务的设备**”块，选择任务范围。
4. 按照所选任务范围选项选择设备。单击“**下一步**”。
5. 输入要使用其权限运行任务的用户的账户凭证。单击“**下一步**”。

   > 默认下，Kaspersky Endpoint Security 以系统用户账户 (SYSTEM) 启动任务。

6. 单击“**完成**”按钮完成向导。
   在任务列表中将显示一个新任务。
7. 单击新任务。
   任务属性窗口将打开。
8. 选择**应用程序设置**选项卡。
9. 在文件列表中，单击“**添加**”。
   文件添加向导将启动。
10. 要添加文件，您必须输入文件的完整路径或哈希值和路径两者。

    > 如果文件位于网络驱动器上，请输入以“`\\`”开头的文件路径，而不是驱动器盘符。例如，`\\server\shared_folder\file.exe`。如果文件路径包含网络驱动器盘符，则可能会出现“*未找到文件*”错误。

11. 在任务属性窗口中，选择“**计划**”选项卡。
12. 配置任务计划。

    > “Wake-on-LAN”不可用于此任务。确保计算机已打开以运行任务。

13. 保存更改。

14. 选中该任务旁边的复选框。

15. 单击“**开始**”。

    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*，但文件本身只有在计算机重新启动后才会被删除。重新启动计算机后，确认文件已删除。

如果试图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“*访问被拒绝或未找到文件*”错误结束。为文件创建终止进程任务，然后重试。

进程启动

您可以使用“*进程启动*”任务远程运行文件。例如，您可以远程运行创建计算机配置文件的实用程序。下一步，您可以使用*从设备接收文件*任务接收在 Kaspersky Security Center Web Console 中创建的文件。

> 您可以在 Web 控制台和云控制台中为 EDR Optimum 配置任务。EDR Expert 的任务设置仅在云控制台中可用。

创建一个“进程启动”任务：

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。

2. 单击“**添加**”。
   “任务向导”将启动。

3. 配置任务设置：

   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Endpoint Security for Windows 14.2.0**”。

   b. 在“**任务类型**”下拉列表中，选择“**进程启动**”。

   c. 在“**任务名称**”字段中，输入简要说明。

   d. 在“**要对其分配任务的设备**”块，选择任务范围。

4. 按照所选任务范围选项选择设备。单击“**下一步**”。

5. 输入要使用其权限运行任务的用户的账户凭证。单击“**下一步**”。

   > 默认下，Kaspersky Endpoint Security 以系统用户账户 (SYSTEM) 启动任务。

6. 单击“**完成**”按钮完成向导。
   在任务列表中将显示一个新任务。

7. 单击新任务。

8. 任务属性窗口将打开。

9. 选择**应用程序设置**选项卡。

10. 输入进程启动命令。

    假设您想运行一个实用程序(`utility.exe`)，该实用程序将有关计算机配置的信息保存到当前文件夹中名为 `conf.txt` 的文件中（默认情况下）。该实用程序位于 `C:\Users\admin\Diagnostic\` 文件夹。您必须将配置文件保存在 `C:\Users\admin\Documents\Configuration` 文件夹。输入以下值：

    - **可执行命令** – `C:\Users\admin\Diagnostic\utility.exe`
    - **命令行参数(可选)** – `/R conf.txt`
    - **工作文件夹路径(可选)** – `C:\Users\admin\Documents\Configuration`

11. 在任务属性窗口中，选择“**计划**”选项卡。

12. 配置任务计划。

    “Wake-on-LAN”不可用于此任务。确保计算机已打开以运行任务。

13. 保存更改。

14. 选中该任务旁边的复选框。

15. 单击“**开始**”。

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

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“*运行进程*”任务启动的互联网速度测试实用程序。

如果您要禁止运行一个文件，您可以配置执行防护组件。您可以禁止执行可执行文件、脚本、Office 格式文件。

“*终止进程*”任务具有以下限制：

- 系统关键对象(SCO)的进程无法被终止。SCO 是操作系统和 Kaspersky Endpoint Security 应用程序运行所需的文件。
- 您可以在 Web 控制台和云控制台中为 EDR Optimum 配置任务。EDR Expert 的任务设置仅在云控制台中可用。

创建一个“终止进程”任务：

1. 在 Web Console 的主窗口中，选择“**任务**”。

   任务列表打开。

2. 单击“**添加**”。

   “任务向导”将启动。

3. 配置任务设置：

   a. 在“**应用程序**”下拉列表中，选择“**Kaspersky Endpoint Security for Windows 14.2.0**”。

   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，输入简要说明。

   d. 在“**要对其分配任务的设备**”块，选择任务范围。

4. 按照所选任务范围选项选择设备。单击“**下一步**”。

5. 输入要使用其权限运行任务的用户的账户凭证。单击“**下一步**”。

   > 默认下，Kaspersky Endpoint Security 以系统用户账户 (SYSTEM) 启动任务。

6. 单击“**完成**”按钮完成向导。
   在任务列表中将显示一个新任务。

7. 单击新任务。
   任务属性窗口将打开。

8. 选择**应用程序设置**选项卡。

9. 要完成此过程，必须选择要终止的文件。您可以采用以下方式之一选择文件：

   - 输入文件的全名。
   - 输入文件的哈希值和文件的路径。
   - 输入进程的 PID（仅适用于本地任务）。

   > 如果文件位于网络驱动器上，请输入以“`\\`”开头的文件路径，而不是驱动器盘符。例如，`\\server\shared_folder\file.exe`。如果文件路径包含网络驱动器盘符，则可能会出现“*未找到文件*”错误。

10. 在任务属性窗口中，选择“**计划**”选项卡。

11. 配置任务计划。

    > “Wake-on-LAN”不可用于此任务。确保计算机已打开以运行任务。

12. 单击“**保存**”。

13. 选中该任务旁边的复选框。

14. 单击“**开始**”。

结果，Kaspersky Endpoint Security 将在计算机上终止该进程。例如，如果某个“GAME”应用程序正在运行，而您终止了 game.exe 进程，则应用程序将在不保存数据的情况下关闭。您可以在“**结果**”部分的“任务属性”中查看任务结果。

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 格式文件。这样，例如，您可以防止执行您认为不安全的应用程序。结果，威胁传播可以被停止。执行防护支持一组 Office 文件扩展名和一组脚本解释器。

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（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。

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）。

  *警报详情*是一种工具，用于查看所收集的有关检测到的威胁的全部信息。警报详情包括，例如，出现在计算机的文件历史。有关管理警报详情的更多信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助和 Kaspersky Endpoint Detection and Response Expert 帮助。

- 使用组策略或本地应用程序设置。

  必须输入文件路径或哈希（SHA256 或 MD5），或者同时输入文件路径和文件哈希。

您还可以使用命令行在本地管理执行防护。

执行防护具有以下限制：

1. 预防规则不包括 CD 或 ISO 映像中的文件。应用程序不会阻止这些文件的执行或打开。
2. 无法阻止系统关键对象（SCO）的启动。SCO 是操作系统和 Kaspersky Endpoint Security 应用程序运行所需的文件。
3. 不建议创建超过 5000 个运行防护规则，因为这可能会导致系统不稳定。

执行防护规则模式

执行防护组件可以在两种模式下工作：

- **仅统计**

  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对象或打开这样的文档的事件到 Windows 事件日志和 Kaspersky Security Center，但不会阻止尝试运行对象或打开文档。默认情况下已选择此模式。

- **活动**

  在此模式下，应用程序将阻止执行符合防护规则标准的对象或打开这样的文档。应用程序还将尝试执行对象或打开文档的事件发布到 Windows 事件日志和 Kaspersky Security Center 事件日志。

管理执行防护

您仅可以在 Web Console 中配置组件设置。

要防护执行：

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置** → **Endpoint Detection and Response**。
5. 选择**执行防护**选项卡。
6. 开启 **执行防护已启用**切换开关。
7. 在**执行或打开禁止的对象时的操作**块，选择组件操作模式：
   - “**阻止并添加到事件日志**”。在此模式下，应用程序将阻止执行符合防护规则标准的对象或打开这样的文档。应用程序还将尝试执行对象或打开文档的事件发布到 Windows 事件日志和 Kaspersky Security Center 事件日志。
   - “**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对象或打开这样的文档的事件到 Windows 事件日志和 Kaspersky Security Center，但不会阻止尝试运行对象或打开文档。默认情况下已选择此模式。
8. 创建执行防护规则列表：
   a. 单击“**添加**”。
   b. 这将打开一个窗口，在此窗口中，输入执行防护规则名称（例如，*Application A*）。
   c. 在**类型**下拉列表，选择您要阻止的对象：**可执行文件**、**脚本**、**Microsoft Office 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两者。

      如果文件位于网络驱动器上，请输入以“`\\`”开头的文件路径，而不是驱动器盘符。例如，`\\server\shared_folder\file.exe`。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。

      执行防护支持一组 Office 文件扩展名和一组脚本解释器。
9. 保存更改。

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。您也可以在文本编辑器中打开脚本文件，即便执行脚本被阻止。当阻止对象的执行时，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（参见下图）。

执行防护通知

计算机网络隔离

计算机网络隔离允许自动将计算机与网络隔离，以响应检测到的妥协的指标（IOC） – 这是*自动模式*。当您调查检测到的威胁时，您可以手动打开网络隔离 – 这是*手动模式*。

打开网络隔离后，应用程序将断开所有活动连接并阻止计算机上的所有新 TCP/IP 网络连接，除了以下连接：

- 网络隔离排除中列出的连接。
- 由 Kaspersky Endpoint Security 服务启动的连接。
- 由 Kaspersky Security Center 网络代理发起的连接。
- 如果应用程序在 Light Agent 模式下使用，则连接到 SVM 和 Integration Server。
- 将应用程序与 Kaspersky Managed Detection and Response 集成时与 KSN 的连接。

您仅可以在 Web Console 中配置组件设置。

自动网络隔离模式

您可以将网络隔离配置为自动打开以响应 IOC 检测。您可以使用组策略配置自动网络隔离模式。

如何将网络隔离配置为自动打开以响应 IOC 检测

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**任务**”。
   任务列表打开。
2. 单击 Kaspersky Endpoint Security 的“**IOC 扫描**”任务。
   任务属性窗口将打开。
   如果必要，请创建“*IOC 扫描*”任务。

3. 选择**应用程序设置**选项卡。

4. 在“**检测到 IOC 后的操作**”块，选择“**在发现 IOC 后采取响应操作**”和“**从网络隔离计算机**”复选框。

5. 保存更改。

结果，当检测到 IOC 时，应用程序从网络隔离计算机以防止威胁扩散。

您可以配置自动网络隔离，使其在一定时间后禁用。默认情况下，应用程序在打开时已过 8 小时后关闭网络隔离。您还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 的主窗口中，选择“**资产管理**” → “**策略**”。

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **内置代理配置** → **Endpoint Detection and Response**。

5. 选择**网络隔离**选项卡。

6. 选择关闭网络隔离的延迟时间。

7. 保存更改。

手动网络隔离模式

您可以手动打开和关闭网络隔离。您可以使用 Kaspersky Security Center 控制台中的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）。

  *警报详情*是一种工具，用于查看所收集的有关检测到的威胁的全部信息。警报详情包括，例如，出现在计算机的文件历史。有关管理警报详情的更多信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助和 Kaspersky Endpoint Detection and Response Expert 帮助。

- 使用本地应用程序设置。

- 在“*IOC 扫描*”任务设置中。

  如果“*IOC 扫描*”任务检测到 IOC，您可以直接从 IOC 将计算机与网络隔离（*IOC 扫描* → **应用程序设置** → **IOC 扫描结果**）。Kaspersky Endpoint Security 还允许立即管理其他设置：网络隔离禁用期和网络隔离排除项。

如何手动开启计算机网络隔离

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**资产(设备)**”。

2. 选择要为其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 Windows”。
   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，单击**从网络隔离计算机**。

您可以配置自动网络隔离，使其在一定时间后禁用。默认情况下，应用程序在打开时已过 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。

如何配置在手动模式下关闭计算机网络隔离的延迟

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**资产(设备)**”。

2. 选择要为其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. 这将打开一个窗口；在此窗口中，选择关闭网络隔离的延迟。

7. 保存更改。

如何手动关闭计算机网络隔离

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**资产(设备)**”。

2. 选择要为其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 Windows”。
   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，单击**解除阻止从网络隔离的计算机**。

您还可以使用命令行在本地禁用网络隔离。

从 Kaspersky Endpoint Security 12.10 for Windows 开始，您可以在警报详细信息中管理网络隔离。此外，您可以在警报详细信息中指定计算机网络隔离时间段。有关管理警报详情的更多信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助和 Kaspersky Endpoint Detection and Response Expert 帮助。

网络隔离排除项

您可以配置网络隔离排除项。当网络隔离打开时，符合规则的网络连接不会在计算机上被阻止。

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，排除项包括网络配置文件，其中包含确保具有 DNS/DHCP 服务器和 DNS/DHCP 客户端角色的设备不间断运行的规则。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（参见以下说明）。

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 控制台的"计算机属性"中或警报详情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。

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 的主窗口中，选择"**资产管理**" → "**策略**"。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置** → **Endpoint Detection and Response**。
5. 选择**网络隔离**选项卡。
6. 在**网络隔离排除项**块，单击**排除项**。
7. 这将打开一个窗户，在此窗口中，单击**添加** → **从配置文件添加**，然后选择用于配置排除项的标准网络配置文件。

   配置文件中的网络隔离排除项将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。
8. 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** → **添加**并手动编辑网络连接设置。
9. 保存更改。

如何在手动模式下添加网络隔离排除项

1. 在 Web Console 的主窗口中，选择"**资产管理**" → "**资产(设备)**"。
2. 选择要为其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. 这将打开一个窗口；在此窗口中，单击“**排除项**”。

7. 这将打开一个窗户，在此窗口中，单击**从配置文件添加**，然后选择用于配置排除项的标准网络配置文件。

   配置文件中的网络隔离排除项将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。

8. 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。

9. 保存更改。

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，计算机必须被隔离。

从 Kaspersky Endpoint Security 12.10 for Windows 开始，您可以在警报详细信息中添加网络隔离排除项。有关管理警报详情的更多信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助 和 Kaspersky Endpoint Detection and Response Expert 帮助 。

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，以识别恶意活动并决定其信誉。这些文件上的数据随后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。

要运行 Cloud Sandbox，您必须启用卡巴斯基安全网络。

如果您使用的是 卡巴斯基私有安全网络 ，则 Cloud Sandbox 技术不可用。

Cloud Sandbox 技术是永久启用的，可供所有卡巴斯基安全网络用户使用，无论他们使用的授权许可类型如何。如果您已经部署了 Endpoint Detection and Response Optimum 解决方案，您可以为 Cloud Sandbox 检测到的威胁启用单独的计数器。您可以使用此计数器在分析检测到的威胁时汇总统计信息。Kaspersky Endpoint Security 会在 Kaspersky Security Center 控制台的 *威胁报告* 中指示 Cloud Sandbox 威胁检测技术。

威胁计数器

要启用 Cloud Sandbox 计数器，请执行以下操作：

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置** → **Endpoint Detection and Response**。
5. 选择**Cloud Sandbox**选项卡。
6. 开启 **Cloud Sandbox 已启用**切换开关。
7. 要将此策略应用到计算机，请关闭 🔒 挂锁图标并保存更改。

一旦发现威胁，Kaspersky Endpoint Security 将在主应用程序窗口的“**威胁检测技术**”下激活使用 Cloud Sandbox 检测到的威胁的计数器。Kaspersky Endpoint Security 还将在 Kaspersky Security Center 控制台的*威胁报告*中指示 Cloud Sandbox 威胁检测技术。

Endpoint Detection and Response 策略部分

EDR Optimum 的 KEA 到 KES 迁移指南

Kaspersky Endpoint Security for Windows 包括用于 Kaspersky Endpoint Detection and Response Optimum 解决方案的内置代理。您不再需要单独的 Kaspersky Endpoint Agent 应用程序与 EDR Optimum 一起使用。Kaspersky Endpoint Agent 的所有功能将由 Kaspersky Endpoint Security 执行。

当您在安装了 Kaspersky Endpoint Agent 的计算机上部署 Kaspersky Endpoint Security 时，Kaspersky Endpoint Detection and Response Optimum 解决方案将继续与 Kaspersky Endpoint Security 一起工作。此外，Kaspersky Endpoint Agent 将被从计算机卸载。当您将 Kaspersky Endpoint Security 更新到版本 11.7.0 或更高版本时，系统中会发生相同的行为。

Kaspersky Endpoint Security 与 Kaspersky Endpoint Agent 不兼容。您不能在同一台计算机上安装这两个应用程序。

Kaspersky Endpoint Security 必须满足以下条件才能作为 Kaspersky Endpoint Detection and Response Optimum 的一部分工作：

- Kaspersky Endpoint Detection and Response Optimum 版本 2.0 或更高版本。
- Kaspersky Security Center 版本 13.2 或更高版本（包括网络代理）。在 Kaspersky Security Center 的早期版本中，无法激活 EDR Optimum 功能。
- EDR Optimum 功能只能使用 Kaspersky Security Center Web Console 进行管理。
- 启用了到管理服务器的数据传输。这些数据是通过 Web 控制台获取计算机上隔离的文件信息所必需的。
- 建立了 Kaspersky Security Center Web Console 和管理服务器之间的后台连接。为了 EDR Optimum 通过 Kaspersky Security Center Web Console 与管理服务器协作，您必须建立新的安全连接，一个“*后台连接*”。

EDR Optimum 的迁移 [KES+KEA] 配置到 [KES+内置代理] 的步骤

1. **升级 Kaspersky Endpoint Security Web 插件**

   EDR Optimum 组件可以使用 Kaspersky Endpoint Security Web 插件版本 11.7.0 或更高版本进行管理。

2. **迁移策略和任务**

   将 Kaspersky Endpoint Agent 设置传输到 Kaspersky Endpoint Security for Windows。为此，请使用 Web Console 中的 Kaspersky Endpoint Agent 迁移向导。

   如何在 Web Console 中将策略和任务设置从 Kaspersky Endpoint Agent 迁移到 Kaspersky Endpoint Security

   在 Web Console 的主窗口中，选择“**操作**” → “**从 Kaspersky Endpoint Agent 迁移**”。

   这将运行策略和任务迁移向导。按照向导的说明进行操作。

步骤 1. 策略迁移

迁移向导将创建一个新策略，该策略将合并 Kaspersky Endpoint Security 和 Kaspersky Endpoint Agent 策略的设置。在策略列表中，选择要将其设置与 Kaspersky Endpoint Security 策略合并的 Kaspersky Endpoint Agent 策略。单击 Kaspersky Endpoint Agent 策略以选择您要与之合并设置的 Kaspersky Endpoint Security 策略。确保选择了正确的策略，然后转到下一步。

步骤 2. 任务迁移

迁移向导为 Kaspersky Endpoint Security 创建新任务。在任务列表中，选择要为 Kaspersky Endpoint Security 策略创建的 Kaspersky Endpoint Agent 任务。转到下一步。

步骤 3. 向导完成

退出向导。因此，向导会执行以下操作：

- 创建一个新的 Kaspersky Endpoint Security 策略。

  策略从 Kaspersky Endpoint Security 和 Kaspersky Endpoint Agent 合并设置。策略被叫做 *<Kaspersky Endpoint Security 策略名称> 和 <Kaspersky Endpoint Agent 策略名称>*。新策略具有*不活动*状态。要继续，将 Kaspersky Endpoint Agent 和 Kaspersky Endpoint Security 策略的状态更改为*不活动*并激活新合并的策略。

  > 从 Kaspersky Endpoint Agent 迁移到 Kaspersky Endpoint Security for Windows 后，请确保新策略具有将数据传输到设置的管理服务器（隔离文件数据和威胁发展链数据）的功能。数据传输参数值不会从 Kaspersky Endpoint Agent 策略迁移。

- 创建新的 Kaspersky Endpoint Security 任务。

  新任务是 Kaspersky Endpoint Agent 任务的副本。同时，向导使 Kaspersky Endpoint Agent 任务保持不变。

3. **授权 EDR Optimum 功能**

   如果您使用通用 Kaspersky Endpoint Detection and Response Optimum 或 Kaspersky Optimum Security 授权许可激活 Kaspersky Endpoint Security for Windows 和 Kaspersky Endpoint Agent，EDR Optimum 功能将在升级应用程序到版本 11.7.0 或更高版本后被自动激活。您不需要做任务其他事情。

   如果您使用独立 Kaspersky Endpoint Detection and Response Optimum 附加授权许可激活 EDR Optimum 功能，您必须确保 EDR Optimum 密钥已添加到 Kaspersky Security Center 存储库且授权许可密钥自动分发功能已启用。在您升级应用程序到版本 11.7.0 或更高版本后，EDR Optimum 功能被自动激活。

   如果您使用 Kaspersky Endpoint Detection and Response Optimum 或 Kaspersky Optimum Security 授权许可激活 Kaspersky Endpoint Agent，并使用其他授权许可激活 Kaspersky Endpoint Security for Windows，您必须使用通用 Kaspersky Endpoint Detection and Response Optimum 或 Kaspersky Optimum Security 密钥替换 Kaspersky Endpoint Security for Windows 密钥。您可以使用“*添加密钥*”任务替换密钥。

4. **安装/升级 Kaspersky Endpoint Security 应用程序**

   要在应用程序安装或升级期间迁移 EDR Optimum 功能，建议使用远程安装任务。创建远程安装任务时，您需要在安装包设置中选择 EDR Optimum 组件。

您还可以使用以下方法升级应用程序：

- 使用卡巴斯基更新服务。
- 本地使用安装向导。

Kaspersky Endpoint Security 支持在安装了 Kaspersky Endpoint Agent 应用程序的计算机上升级应用程序时自动选择组件。组件的自动选择取决于升级应用程序的用户账户的权限。

如果您在系统账户（SYSTEM）下使用 EXE 或 MSI 文件升级 Kaspersky Endpoint Security，Kaspersky Endpoint Security 获得对卡巴斯基解决方案的当前授权许可的访问权。因此，如果计算机安装了 Kaspersky Endpoint Agent，并且激活了 EDR Optimum 解决方案，则 Kaspersky Endpoint Security 安装程序将自动配置组件集并选择 EDR Optimum 组件。这将使 Kaspersky Endpoint Security 切换到使用内置代理并卸载 Kaspersky Endpoint Agent。在系统账户（SYSTEM）下运行 MSI 安装程序通常在通过卡巴斯基更新服务升级时执行，或者当通过 Kaspersky Security Center 部署安装包时。

如果您在非特权用户账户下使用 MSI 文件升级 Kaspersky Endpoint Security，Kaspersky Endpoint Security 缺少对卡巴斯基解决方案的当前授权许可的访问权。这种情况下，Kaspersky Endpoint Security 基于 Kaspersky Endpoint Agent 配置自动选择组件。此后，Kaspersky Endpoint Security 将切换到使用内置代理并卸载 Kaspersky Endpoint Agent。

Kaspersky Endpoint Security 支持在不重启计算机的情况下升级。您可以选择策略属性中的应用程序升级模式。

5 **检查应用程序运行情况**

如果在应用程序安装或升级之后，计算机在 Kaspersky Security Center 控制台显示“*严重*”状态：

- 确保计算机安装了网络代理版本 13.2 或更高版本。
- 通过查看“*应用程序组件状态报告*”检查内置代理的操作状态。如果组件具有*未安装*状态，使用“*更改应用程序组件*”任务安装组件。如果一个组件有“*授权许可不支持*”状态，确保您已激活内置代理功能。
- 确保您在 Kaspersky Endpoint Security for Windows 的新策略中接受了卡巴斯基安全网络声明。

Kaspersky Sandbox

Kaspersky Endpoint Security for Windows 包含一个用于与 Kaspersky Sandbox 解决方案集成的内置代理。*Sandbox* 组件检测并自动阻止计算机上的高级威胁。Sandbox 分析对象行为，以检测恶意活动和针对组织 IT 基础设施的攻击的活动特征。Sandbox 使用部署的 Microsoft Windows 操作系统虚拟映像（Sandbox 服务器）分析和扫描特殊服务器上的对象。有关解决方案的详细信息，请参阅 Kaspersky Sandbox 帮助 和 Kaspersky Anti Targeted Attack Platform 帮助 。

内置代理与 Kaspersky Sandbox 的集成

与 Kaspersky Sandbox 组件集成需要添加 Sandbox 组件。您可以在安装或升级过程中选择 Sandbox 组件，也可以使用“*更改应用程序组件*”任务。

要使用该组件，必须满足以下条件：

- Kaspersky Security Center 13.2。Kaspersky Security Center 的早期版本不允许为威胁响应创建独立 IOC 扫描任务。
- 该组件只能使用 Web Console 进行管理。您无法使用管理控制台（MMC）管理此组件。
- 应用程序已激活，授权许可涵盖了该功能。
- 启用了到管理服务器的数据传输。

  要使用 Kaspersky Sandbox 的所有功能，请确保启用了隔离文件数据阐述。这些数据是通过 Web 控制台获取计算机上隔离的文件信息所必需的。例如，您可以从隔离区下载一个文件，以便在 Web 控制台中进行分析。

  如何在 Web 控制台中启用到管理服务器的数据传输

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

     策略属性窗口将打开。
  3. 选择**应用程序设置**选项卡。
  4. 选择 **常规设置** → **KSC 整合**。
  5. 在“**到管理服务器的数据传输**”块中，选中“**关于隔离区文件**”复选框。
  6. 保存更改。

- 建立了 Kaspersky Security Center Web Console 和管理服务器之间的后台连接

  为了 Kaspersky Sandbox 通过 Kaspersky Security Center Web Console 与管理服务器协作，您必须建立新的安全连接，一个“*后台连接*”。对于 Kaspersky Security Center 与其他 Kaspersky 解决方案整合的详情，请参阅 Kaspersky Security Center 帮助。

  在 Web Console 中建立后台连接

  1. 在 Web Console 的主窗口中，选择“**设置**” → “**整合**”。
  2. 转到**整合**区域。
  3. 开启 **用于整合的后台连接 已启用**切换开关。
  4. 保存更改。

  如果未建立 Kaspersky Security Center Web Console 与管理服务器之间的后台连接，独立 IOC 扫描任务无法作为威胁响应的一部分被创建。

- 要配置与 Sandbox 服务器的可信连接，必须准备 TLS 证书。您必须使用策略将证书添加到计算机。您还需要将证书添加到 Sandbox 服务器。

  > Kaspersky Sandbox 不提供使用加密容器的双向身份验证。

  您也可以使用命令行在 Web Console 或本地添加 TLS 证书。

- Kaspersky Sandbox 组件已启用。

- 确保 Sandbox 运行的应用程序组件已启用并可运行。以下组件确保 Sandbox 的运行：
  - 文件威胁防护。
  - 主机入侵防御。
  - 防火墙。
  - AMSI 保护。
  - 后台扫描。

要启用或禁用与 Kaspersky Sandbox 的集成：

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

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置** → **Sandbox**。
5. 使用**与 Sandbox 的整合已启用**开关启用或禁用组件。
6. 在**整合模式**块，选择组件操作模式： **Kaspersky Sandbox**.
7. 单击**连接设置**链接。

   这将打开 Sandbox 服务器连接设置窗口。
8. 在**服务器 TLS 证书**块，单击**上传**并选择 TLS 证书文件。

   Kaspersky Endpoint Security 对于 Sandbox 服务器只能有一个 TLS 证书。如果之前添加了 TLS 证书，则该证书将被撤回。仅使用最后添加的证书。
9. 为 Sandbox 服务器配置高级连接设置：
   - “**超时(豪秒)**”。Sandbox 服务器连接超时。配置的超时时间过后，Kaspersky Endpoint Security 将向下一台服务器发送请求。如果连接速度低或连接不稳定，您可以增加服务器的连接超时。建议的请求超时是 0.5 秒或更少。
   - “**请求队列**”。请求队列文件夹的大小。在发送多个对象以在 Sandbox 中进行扫描时，Kaspersky Endpoint Security 会创建一个请求队列。默认情况下，请求队列文件夹的大小限制为 100 MB。达到最大大小后，Sandbox 停止向队列添加新请求，并将相应的事件发送到 Kaspersky Security Center。您可以根据您的服务器配置来配置请求队列文件夹的大小。
10. 在“**连接到 Sandbox 服务器**”块中单击“**添加**”按钮。

11. 这将打开一个窗口，您可以在其中输入 Sandbox 服务器地址 (IPv4、IPv6、DNS) 和端口。

    有关部署虚拟映像和配置 Sandbox 服务器的详细信息，请参阅 Kaspersky Sandbox 帮助。

12. 保存更改。

    结果，Kaspersky Endpoint Security 将验证 TLS 证书。如果证书被成功验证，Kaspersky Endpoint Security 将在与 Kaspersky Security Center 的下次同步过程中上传该证书文件到计算机。如果您添加了两个 TLS 证书，Kaspersky Sandbox 将使用最新的证书建立受信任连接。通过查看*应用程序组件状态报告*检查组件的操作状态。您也可以利用 Kaspersky Endpoint Security 的本地界面在报告中查看组件的操作状态。**Sandbox** 组件将被添加到 Kaspersky Endpoint Security 组件列表。

    您可以使用命令行在 Web Console 或本地启用或禁用与 Kaspersky Sandbox 的集成。

Kaspersky Endpoint Security 将 Kaspersky Sandbox 组件的操作信息保存到一个报告。该报告也包含错误信息。如果您收到具有“`Error code: XXX`”格式描述的错误（例如，`0xa67b01f4`），请联系技术支持。

妥协的指标扫描（独立任务）

妥协的指标 (IOC) 是一组关于对象或活动的数据，表示未经授权访问计算机（数据泄露）。例如，许多登录系统的尝试都不成功，这可能构成妥协的指标。*IOC 扫描*任务允许在计算机上查找妥协的指标，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数检测的指标集的文件。IOC 文件必须符合 OpenIOC 标准。Kaspersky Endpoint Security 自动为 Kaspersky Sandbox 生成 IOC 文件。

IOC 扫描任务运行模式

应用程序为 Kaspersky Sandbox 创建独立 IOC 扫描任务。*独立 IOC 扫描任务*是在对 Kaspersky Sandbox 检测到的威胁作出反应时自动创建的组任务。Kaspersky Endpoint Security 自动生成 IOC 文件。不支持自定义 IOC 文件。任务在创建时间 30 天后被自动删除。有关独立 IOC 扫描任务的更多详细信息，请参阅 Kaspersky Sandbox 帮助。

IOC 扫描 任务设置

Kaspersky Sandbox 在响应威胁时可能自动创建并运行“*IOC 扫描*”任务。

您仅可以在 Web Console 中配置设置。

您需要 Kaspersky Security Center 13.2 以便 Kaspersky Sandbox 的独立 IOC 扫描任务可以正常运行。

要更改“IOC 扫描”任务设置：

1. 在 Web Console 的主窗口中，选择“**任务**”。
   任务列表打开。
2. 单击 Kaspersky Endpoint Security 的“**IOC 扫描**”任务。
   任务属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 转到**IOC 扫描设置**区域。
5. 配置 IOC 检测操作：
   - “**将副本移动到隔离区，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 运行*关键区域扫描*任务。默认情况下，Kaspersky Endpoint Security 会扫描内核内存、运行进程和磁盘的引导扇区。
   - “**仅在计算机空闲时运行**”。计算机资源忙时推迟任务启动。如果计算机被锁定或屏幕保护开启，Kaspersky Endpoint Security 启动扫描任务。如果您中断了任务的执行，例如通过解锁计算机，Kaspersky Endpoint Security 将自动运行该任务，并从中断点继续运行。此计划选项允许您在使用计算机时节省计算机资源。
6. 保存更改。

您可以在“**结果**”部分的“任务属性”中查看任务结果。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**。

IOC 扫描结果被保存 30 天。在此时间之后，Kaspersky Endpoint Security 将自动删除最早条目。

Kaspersky Sandbox 的 KEA 到 KES 迁移指南

Kaspersky Endpoint Security for Windows 包含一个用于 Kaspersky Sandbox 解决方案的内置代理。您不再需要单独的 Kaspersky Endpoint Agent 应用程序与 Kaspersky Sandbox 一起使用。Kaspersky Endpoint Agent 的所有功能将由 Kaspersky Endpoint Security 执行。

当您在安装了 Kaspersky Endpoint Agent 的计算机上部署 Kaspersky Endpoint Security 时，Kaspersky Sandbox 解决方案将继续与 Kaspersky Endpoint Security 一起工作。此外，Kaspersky Endpoint Agent 将被从计算机卸载。当您将 Kaspersky Endpoint Security 更新到版本 11.7.0 或更高版本时，系统中会发生相同的行为。

Kaspersky Endpoint Security 与 Kaspersky Endpoint Agent 不兼容。您不能在同一台计算机上安装这两个应用程序。

Kaspersky Endpoint Security 必须满足以下条件才能作为 Kaspersky Sandbox 的一部分工作：

- Kaspersky Sandbox 版本 2.0 或更高版本。
- Kaspersky Security Center 版本 13.2 或更高版本（包括网络代理）。在 Kaspersky Security Center 的早期版本中，无法激活 Kaspersky Sandbox 功能。
- Kaspersky Sandbox 只能使用 Kaspersky Security Center Web Console 进行管理。
- 启用了到管理服务器的数据传输。这些数据是通过 Web 控制台获取计算机上隔离的文件信息所必需的。
- 建立了 Kaspersky Security Center Web Console 和管理服务器之间的后台连接。为了 Kaspersky Sandbox 通过 Kaspersky Security Center Web Console 与管理服务器协作，您必须建立新的安全连接，一个"*后台连接*"。

Kaspersky Sandbox 的迁移 [KES+KEA] 配置到 [KES+内置代理] 的步骤

1. **升级 Kaspersky Endpoint Security Web 插件**

   Kaspersky Sandbox 组件可以使用 Kaspersky Endpoint Security Web 插件版本 11.7.0 或更高版本进行管理。

2. **迁移策略和任务**

   将 Kaspersky Endpoint Agent 设置传输到 Kaspersky Endpoint Security for Windows。为此，请使用 Web Console 中的 Kaspersky Endpoint Agent 迁移向导。

   如何在 Web Console 中将策略和任务设置从 Kaspersky Endpoint Agent 迁移到 Kaspersky Endpoint Security

   在 Web Console 的主窗口中，选择"**操作**" → "**从 Kaspersky Endpoint Agent 迁移**"。

   这将运行策略和任务迁移向导。按照向导的说明进行操作。

   步骤 1. 策略迁移

   迁移向导将创建一个新策略，该策略将合并 Kaspersky Endpoint Security 和 Kaspersky Endpoint Agent 策略的设置。在策略列表中，选择要将其设置与 Kaspersky Endpoint Security 策略合并的 Kaspersky Endpoint Agent 策略。单击 Kaspersky Endpoint Agent 策略以选择您要与之合并设置的 Kaspersky Endpoint Security 策略。确保选择了正确的策略，然后转到下一步。

   步骤 2. 任务迁移

   迁移向导为 Kaspersky Endpoint Security 创建新任务。在任务列表中，选择要为 Kaspersky Endpoint Security 策略创建的 Kaspersky Endpoint Agent 任务。转到下一步。

步骤 3. 向导完成

退出向导。因此，向导会执行以下操作：

- 创建一个新的 Kaspersky Endpoint Security 策略。

  策略从 Kaspersky Endpoint Security 和 Kaspersky Endpoint Agent 合并设置。策略被叫做 *<Kaspersky Endpoint Security 策略名称> 和 <Kaspersky Endpoint Agent 策略名称>*。新策略具有*不活动*状态。要继续，将 Kaspersky Endpoint Agent 和 Kaspersky Endpoint Security 策略的状态更改为*不活动*并激活新合并的策略。

  > 从 Kaspersky Endpoint Agent 迁移到 Kaspersky Endpoint Security for Windows 后，请确保新策略具有将数据传输到设置的管理服务器（隔离文件数据和威胁发展链数据）的功能。数据传输参数值不会从 Kaspersky Endpoint Agent 策略迁移。

- 创建新的 Kaspersky Endpoint Security 任务。

  新任务是 Kaspersky Endpoint Agent 任务的副本。同时，向导使 Kaspersky Endpoint Agent 任务保持不变。

3 授权 Kaspersky Sandbox 功能

要将 Kaspersky Endpoint Security 作为 Kaspersky Sandbox 解决方案的一部分激活，您需要单独的 Kaspersky Sandbox 加载项授权许可。您可以使用"*添加密钥*"任务添加密钥。结果，两个密钥将被添加到应用程序中：*Kaspersky Endpoint Security* 和 *Kaspersky Sandbox*。

4 安装/升级 Kaspersky Endpoint Security 应用程序

要在应用程序安装或升级期间迁移 Kaspersky Sandbox 功能，建议使用远程安装任务。创建远程安装任务时，您需要在安装包设置中选择 Kaspersky Sandbox 组件。

您还可以使用以下方法升级应用程序：

- 使用卡巴斯基更新服务。
- 本地使用安装向导。

Kaspersky Endpoint Security 支持在安装了 Kaspersky Endpoint Agent 应用程序的计算机上升级应用程序时自动选择组件。组件的自动选择取决于升级应用程序的用户账户的权限。

如果您在系统账户（SYSTEM）下使用 EXE 或 MSI 文件升级 Kaspersky Endpoint Security，Kaspersky Endpoint Security 获得对卡巴斯基解决方案的当前授权许可的访问权。因此，如果计算机安装了 Kaspersky Endpoint Agent，并且激活了 Kaspersky Sandbox 解决方案，则 Kaspersky Endpoint Security 安装程序将自动配置组件集并选择 Kaspersky Sandbox 组件。这将使 Kaspersky Endpoint Security 切换到使用内置代理并卸载 Kaspersky Endpoint Agent。在系统账户（SYSTEM）下运行 MSI 安装程序通常在通过卡巴斯基更新服务升级时执行，或者当通过 Kaspersky Security Center 部署安装包时。

如果您在非特权用户账户下使用 MSI 文件升级 Kaspersky Endpoint Security，Kaspersky Endpoint Security 缺少对卡巴斯基解决方案的当前授权许可的访问权。这种情况下，Kaspersky Endpoint Security 基于 Kaspersky Endpoint Agent 配置自动选择组件。此后，Kaspersky Endpoint Security 将切换到使用内置代理并卸载 Kaspersky Endpoint Agent。

> Kaspersky Endpoint Security 支持在不重启计算机的情况下升级。您可以选择策略属性中的应用程序升级模式。

5 检查应用程序运行情况

如果在应用程序安装或升级之后，计算机在 Kaspersky Security Center 控制台显示“*严重*”状态：

- 确保计算机安装了网络代理版本 13.2 或更高版本。
- 通过查看“*应用程序组件状态报告*”检查内置代理的操作状态。如果组件具有*未安装*状态，使用“*更改应用程序组件*”任务安装组件。如果一个组件有“*授权许可不支持*”状态，确保您已激活内置代理功能。
- 确保您在 Kaspersky Endpoint Security for Windows 的新策略中接受了卡巴斯基安全网络声明。

Kaspersky Anti Targeted Attack Platform

Kaspersky Endpoint Security for Windows 支持与 Kaspersky Anti Targeted Attack Platform (EDR (KATA)) 解决方案配合使用。*Kaspersky Anti Targeted Attack Platform* 是旨在及时检测复杂威胁（如针对性攻击、高级持久性威胁 (APT)、零日攻击等）的解决方案。Kaspersky Anti Targeted Attack Platform 包括三个功能单元：

- Kaspersky Anti Targeted Attack Platform（*KATA*）
- Kaspersky Endpoint Detection and Response（*EDR（KATA）*）
- Network Detection and Response（*NDR（KATA）*）

您可以购买所有功能单元，也可以单独购买单个功能单元。有关解决方案的详细信息，请参阅 Kaspersky Anti Targeted Attack Platform 帮助。应用程序包括 EDR、NDR 组件的内置代理。应用程序还支持与作为 KATA 一部分的 Sandbox 组件配合使用。

威胁情报工具

Kaspersky Endpoint Detection and Response 使用以下 Threat Intelligence 工具：

- 与卡巴斯基威胁情报门户集成，该系统包含并显示有关文件和网址信誉的信息。
- 卡巴斯基威胁数据库。
- 卡巴斯基安全网络（以下也称为“KSN”）云服务基础设施，提供对 Kaspersky 知识库中实时文件、网站和软件信誉信息的访问。使用卡巴斯基安全网络的数据可确保 Kaspersky 应用程序能够更快地对新威胁作出响应，提高一些保护组件的性能，并减少误报风险。

解决方案的工作原理

Kaspersky Endpoint Security 安装在公司 IT 基础设施的各个计算机上，并持续监视流程、开放式网络连接和正在修改的文件。有关计算机上事件的信息（遥测数据）被发送到 Kaspersky Anti Targeted Attack Platform 服务器。此种情况下，Kaspersky Endpoint Security 也将应用程序发现的威胁信息和威胁处理结果信息发送到 Kaspersky Anti Targeted Attack Platform 服务器。

EDR (KATA) 和 NDR (KATA) 集成在 Kaspersky Security Center 控制台上配置。然后使用 Kaspersky Anti Targeted Attack Platform 控制台管理内置代理，包括运行任务、管理隔离对象、查看报告和其他操作。

用于使用 EDR / NDR（KATA）的 Kaspersky Endpoint Security 配置

以下配置可用于使用 EDR / NDR（KATA）：

- **[KES+内置代理]**。在此配置中，Kaspersky Endpoint Security 既充当确保计算机安全的应用程序，又充当使用 EDR / NDR（KATA）的应用程序。Kaspersky Endpoint Security 12.1 for Windows 或更高版本中提供了 EDR (KATA) 内置代理。Kaspersky Endpoint Security 12.7 for Windows 或更高版本中提供了 NDR (KATA) 内置代理。

- **[第三方 EPP+EDR Agent]**。在此配置中，IT 基础设施的安全性由第三方端点保护平台（EPP）提供。与 EDR / NDR（KATA）的交互由 Kaspersky Endpoint Security 在"Endpoint Detection and Response Agent（EDR Agent）"配置下提供。在此配置中，EDR Agent 兼容第三方 EPP 应用程序。EDR (KATA) 的 EDR Agent 在 Kaspersky Endpoint Security 12.3 for Windows 或更高版本中可用。NDR (KATA) 的 EDR Agent 在 Kaspersky Endpoint Security 12.7 for Windows 或更高版本中可用。

对以前版本的 Kaspersky Endpoint Security 的支持

如果您正在使用 Kaspersky Endpoint Security 11.2.0–11.8.0 与 Kaspersky Anti Targeted Attack Platform（EDR）进行互操作，则应用程序包含 Kaspersky Endpoint Agent。您可以将 Kaspersky Endpoint Agent 与 Kaspersky Endpoint Security 一起安装。

如果您使用的是 Kaspersky Endpoint Security 11.9.0 – 12.0，您需要单独安装 Kaspersky Endpoint Agent，因为从 Kaspersky Endpoint Security 11.9.0 开始，Kaspersky Endpoint Agent 分发包不再是 Kaspersky Endpoint Security 分发包的一部分。

内置代理与 EDR / NDR（KATA）的集成

为了与 EDR/NDR（KATA）集成，您必须添加相关组件：Endpoint Detection and Response（KATA）或 Network Detection and Response（KATA）。您可以在安装或升级应用程序时选择与 EDR / NDR (KATA) 集成的组件，也可以使用"*更改应用程序组件*"任务。

从 Kaspersky Endpoint Security for Windows 12.11 版本开始，EDR (KATA) 组件已重命名为 **Endpoint Detection and Response Expert (版本 8.0 或更高版本)**。在此版本的应用程序中，该组件与 Kaspersky Anti Targeted Attack Platform 7.1 及更早版本以及 Kaspersky Endpoint Detection and Response Expert（本地部署）兼容。

"Endpoint Detection and Response Optimum"、"Endpoint Detection and Response Expert (cloud)"和"Endpoint Detection and Response Expert (on-premises)"组件彼此不兼容。

要使用 EDR / NDR（KATA），必须满足以下条件：

- EDR (KATA)：Kaspersky Anti Targeted Attack Platform 版本 5.0–7.1。

- NDR (KATA)：Kaspersky Anti Targeted Attack Platform 版本 7.0 或更高版本。

- EDR (KATA)：Kaspersky Endpoint Security for Windows 12.1 或更高版本。有关 KATA 与不同版本 Kaspersky Endpoint Security 的兼容性的更多详细信息，请参阅 Kaspersky Anti Targeted Attack Platform 帮助。

- NDR (KATA)：Kaspersky Endpoint Security for Windows 12.7 或更高版本。
- Kaspersky Security Center 版本 14.2 或更高版本。在 Kaspersky Security Center 的早期版本中，无法激活 EDR / NDR（KATA）集成功能。
- 应用程序已激活，授权许可涵盖了该功能。
- Endpoint Detection and Response(KATA) 和 Network Detection and Response (KATA) 组件已启用。
- 确保 EDR/NDR（KATA）运行的应用程序组件已启用并可运行。以下组件确保 EDR / NDR（KATA）的运行：
  - 文件威胁防护。
  - Web 威胁防护。
  - 邮件威胁防护。
  - 漏洞利用防御。
  - 行为检测。
  - 主机入侵防御。
  - AMSI 保护。
  - 后台扫描。
  - 卡巴斯基安全网络。

https://www.youtube.com/watch?v=cZzgtBoeC7k

https://www.youtube.com/watch?v=gd-rySv0ThQ

与 Kaspersky Endpoint Detection and Response（KATA）的整合包括以下步骤：

1. **安装 Endpoint Detection and Response (KATA) 和 Detection and Response (KATA) 组件**

   您可以在安装或升级过程中选择 EDR (KATA) 和 NDR (KATA) 组件，也可以使用"*更改应用程序组件*"任务。

   > 您必须重新启动计算机才能使用新组件完成应用程序的升级。

2. **激活 Endpoint Detection and Response (KATA) 和 Network Detection and Response (KATA)**

   您需要为 EDR (KATA) 和 NDR (KATA)（例如，Kaspersky Endpoint Detection and Response （KATA）加载项）购买单独的授权许可。

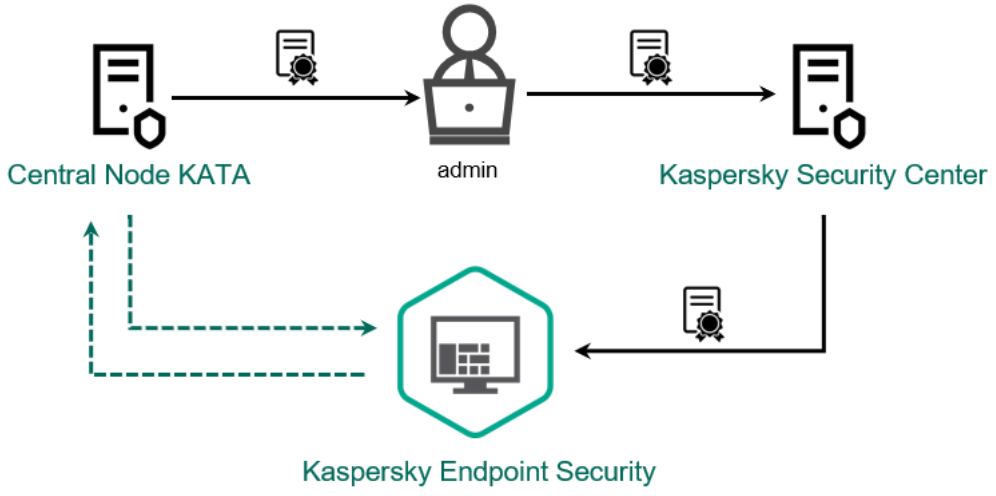
   添加涵盖 EDR（KATA）和 NDR（KATA）功能的单独密钥后，该功能可用。因此，计算机上将添加多个密钥：Kaspersky Endpoint Security 密钥以及 Kaspersky Endpoint Detection and Response (KATA) 和 Network Detection and Response (KATA) 的密钥。

   独立 EDR (KATA) 和 NDR (KATA) 功能的授权与 Kaspersky Endpoint Security 的授权相同。

   确保授权许可中包含 EDR (KATA) 和 NDR (KATA) 功能，并且这些功能正在应用程序的本地界面中运行。

3. **连接到 Central Node**

   Kaspersky Anti Targeted Attack Platform 需要在 Kaspersky Endpoint Security 和 Central Node 组件之间建立可信连接。要配置可信连接，您必须使用 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）。然后您必须将 TLS 证书添加到 Kaspersky Endpoint Security（参见下面的说明）。



将 TLS 证书添加到 Kaspersky Endpoint Security

   默认情况下，Kaspersky Endpoint Security 仅检查 Central Node 的 TLS 证书。为了使连接更安全，您可以额外启用 Central Node 上的计算机验证（双向身份验证）。要启用此验证，您必须在 Central Node 和 Kaspersky Endpoint Security 设置中打开双向身份验证。要使用双向身份验证，您还需要一个加密容器。*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）。

   如何使用管理控制台 (MMC) 将 Kaspersky Endpoint Security 计算机连接到 Central Node

   1. 打开 Kaspersky Security Center Administration Console。
   2. 在控制台树中，选择"**策略**"。
   3. 选择必要的策略并双击以打开策略属性。

4. 在策略窗口中，选择“**Detection and Response**”并选择要配置的组件：**Endpoint Detection and Response Expert (on-premises)** 或者 **Network Detection and Response (KATA)**。

5. 选中相应的复选框：**Endpoint Detection and Response Expert (版本 7.1 或更早版本)** 或者 **Network Detection and Response (KATA)**。

6. 单击“**服务器连接设置**”。

7. 配置服务器连接：

   - “**超时(秒)**”。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 TLS 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）。

   - “**使用双向认证**”。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。

8. 单击“**确定**”。

9. 添加 Central Node 服务器。为此，请指定服务器地址（IPv4、IPv6）和连接到服务器的端口。

   您可以添加多个 Central Node 服务器地址。Kaspersky Endpoint Security 尝试使用第一个 IP 地址连接到服务器。如果连接建立失败，Kaspersky Endpoint Security 将尝试使用列表中的第二个 IP 地址进行连接，依此类推。

10. 如果有必要，配置遥测。

11. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何使用 Web Console 将 Kaspersky Endpoint Security 计算机连接到 Central Node

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 前往“**内置代理配置**”部分并选择要配置的组件：**Endpoint Detection and Response Expert (on-premise)** 或者 **Network Detection and Response (KATA)**。

5. 打开相应的拨动开关：**Endpoint Detection and Response Expert (on-premise) 已启用** 或者 **Network Detection and Response (KATA) 已启用**。

6. 要配置 EDR (KATA)，请从解决方案列表中选择“**Endpoint Detection and Response Expert (版本 7.1 或更早版本)**”。

7. 单击“**连接设置**”。

8. 配置服务器连接：

   - “**超时(秒)**”。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。

9. 单击“**确定**”。

10. 添加 Central Node 服务器。为此，请指定服务器地址（IPv4、IPv6）和连接到服务器的端口。

    您可以添加多个 Central Node 服务器地址。Kaspersky Endpoint Security 尝试使用第一个 IP 地址连接到服务器。如果连接建立失败，Kaspersky Endpoint Security 将尝试使用列表中的第二个 IP 地址进行连接，依此类推。

11. 如果有必要，配置遥测。

12. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

您也可以使用命令行在本地添加 TLS 证书。

结果，计算机被添加到 Kaspersky Anti Targeted Attack Platform 控制台上。通过查看*应用程序组件状态报告*检查组件的操作状态。您也可以利用 Kaspersky Endpoint Security 的本地界面在报告中查看组件的操作状态。“**Endpoint Detection and Response Expert (版本 8.0 或更高版本)**”和“**Network Detection and Response (KATA)**”组件将被添加到 Kaspersky Endpoint Security 组件列表。

您可以在 Kaspersky Security Center 控制台中的计算机属性中的“**组件**”部分检查组件的状态。在控制台中检查组件的状态时，请考虑以下事项。如果未安装该组件且授权许可不涵盖该功能，则控制台会显示“**不被授权许可支持**”状态而不是“**未安装**”。

从 Kaspersky Endpoint Security 12.6 for Windows 开始，您可以在 Kaspersky Security Center 管理控制台 (MMC) 中监控 EDR (KATA) 组件的状态。组件的当前状态显示在计算机属性中，在“**端点传感器状态**”列（*运行中*、*正在启动*、*已停止*、*已暂停*、*失败*、*未知*）。Web Console 不显示 Endpoint Sensor 的状态。

配置 EDR (KATA)遥测

*遥测*是受保护计算机上发生的事件的列表。Kaspersky Endpoint Security 分析遥测数据并在同步期间将其发送到 Kaspersky Anti Targeted Attack Platform。遥测事件几乎连续不断地到达服务器。当满足以下任一条件时，Kaspersky Endpoint Security 启动与服务器的同步：

- 同步间隔已用完。
- 缓冲区中的事件数超过上限。

因此，默认情况下，应用程序每 30 秒或每当缓冲区包含 1024 个事件时同步一次。您可以在 Kaspersky Endpoint Security 策略中配置同步行为并选择最佳值以匹配您的网络负载（请参阅下面的说明）。

如果 Kaspersky Endpoint Security 与服务器之间没有连接，应用程序将对新事件进行排队。当连接恢复时，Kaspersky Endpoint Security 以正确的顺序将排队的事件发送到服务器。为避免服务器过载，Kaspersky Endpoint Security 可能会跳过一些事件。要启用此功能，您可以优化事件传输设置，例如，设置每小时最大事件数值（请参阅下面的说明）。

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（参见下面的说明）。这使您可以优化这些解决方案的服务器负载。例如，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。

如何在管理控制台 (MMC) 中配置遥测

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**策略**”。
3. 选择必要的策略并双击以打开策略属性。
4. 在策略窗口中，选择“**Detection and Response**”并选择要配置的组件：**Endpoint Detection and Response Expert (on-premises)** 或者 **Network Detection and Response (KATA)**。
5. 配置“**发送同步请求到 KATA 服务器的间隔(分钟)**”设置。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。
6. 确保“**发送遥测数据到 KATA**”复选框被选中。
7. 如果需要，请在“**数据传输设置**”块配置与服务器设置的同步：
   - “**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。默认设置是 30 秒。
   - “**事件包的最大数量**”。当缓冲区充满事件时，应用程序会与服务器同步。默认设置是 1024 个事件。
8. 如有必要，在“**请求限制**”块选择“**启用请求限制**”复选框。

   该功能有助于优化服务器上的负载。如果启用此功能，应用程序将限制事件传输。如果事件数量超过配置的限制，Kaspersky Endpoint Security 将停止发送事件。

9. 配置用于将事件发送到服务器的优化设置：

   - “**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。默认设置是每小时 3000 个事件。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。默认设置为 15%。

10. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 中配置遥测

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **内置代理配置** → **Endpoint Detection and Response Expert (on-premise)**。

5. 要配置 EDR (KATA)，请从解决方案列表中选择“**Endpoint Detection and Response Expert (版本 7.1 或更早版本)**”。

6. 确保在“**数据传输设置**”块中，“**将遥测发送到 KATA 服务器**”复选框被选中。

7. 配置“**发送同步请求到服务器的间隔(分钟)**”设置。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。

8. 确保“**将遥测发送到 KATA 服务器**”复选框被选中。

9. 如果需要，请在“**数据传输设置**”块配置与服务器设置的同步：

   - “**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。默认设置是 30 秒。

   - “**事件包的最大数量**”。当缓冲区充满事件时，应用程序会与服务器同步。默认设置是 1024 个事件。

10. 如有必要，在“**请求限制**”块选择“**启用请求限制**”复选框。

    该功能有助于优化服务器上的负载。如果启用此功能，应用程序将限制事件传输。如果事件数量超过配置的限制，Kaspersky Endpoint Security 将停止发送事件。

11. 配置用于将事件发送到服务器的优化设置：

    - “**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。默认设置是每小时 3000 个事件。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。默认设置为 15%。

12. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

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

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

3. 选择**应用程序设置**选项卡。

4. 转到 **KATA 整合** → **遥测排除项**区域。

5. 在“**数据传输设置**”下，选择“**使用排除项**”复选框。

6. 点击“**添加**”并配置排除项：

   > 标准与逻辑 *AND* 相结合。

   - **路径**。文件的完整路径，包括其名称和扩展名。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。要使排除生效，必须指定文件的路径。
   - **命令行**。用于运行对象的命令。
   - **描述**。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。
     有关VersionInfo 资源的更多详细信息，请访问 Microsoft 网站。
   - **原始文件名**。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。
   - **版本**。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。
   - **MD5**文件 MD5 哈希
   - **SHA256**文件 SHA256 哈希
   - **事件类型**。要使排除生效，您必须至少选择一种事件类型。

7. 保存更改。

1. 在 Kaspersky Security Center 管理控制台树中，选择“**任务**”。
   任务列表打开。

2. 单击“**新任务**”。

“任务向导”将启动。按照向导的说明进行操作。

步骤 1. 选择任务类型

1. 选择“**Kaspersky Endpoint Security for Windows (14.1)**”→ “**更新回滚**”。

步骤 2. 选择任务将分配到的设备

选择将要执行任务的计算机。下列选项可用：

- 将任务分配给管理组。在这种情况下，任务分配给先前创建的管理组中包括的计算机。
- 选择管理服务器在网络中检测到的计算机：*未分配设备*。特定设备可包括管理组中的设备以及未分配设备。
- 手动指定设备地址或从列表中导入地址。您可以指定您要将任务分配给的设备的 NetBIOS 名称、IP 地址和 IP 子网。

步骤 3. 配置任务启动计划

配置任务计划，例如，手动。

步骤 4. 定义任务名称

输入任务的名称。

步骤 7. 完成任务创建

退出向导。如有必要，选中“**向导完成时运行任务**”复选框。您可以在任务属性中监控任务进度。

EDR (KATA) 遥测排除项

要提高性能并优化到遥测服务器的数据传输，您可以配置遥测排除项。例如，您可以选择不发送单个应用程序的网络通信数据。

如何在管理控制台 (MMC) 中创建遥测排除项

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **排除项和对象类型**。
4. 在“**遥测设置** → **EDR (KATA) / NDR (KATA) 遥测**”块中单击“**设置**”按钮。

5. 在打开的窗口中，配置遥测排除项（见下表）。

   该应用程序将排除项条件与逻辑“AND”结合起来。要创建规则，您必须在“**完整路径**”字段中指定值，并在“**用于以下事件类型**”列表中选择至少一个事件类型。

6. 保存更改。

如何在 Web Console 和云控制台中创建遥测排除项

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **常规设置** → **遥测设置**。

5. 选择**EDR (KATA) / NDR (KATA) 遥测**选项卡。

6. 在打开的窗口中，配置遥测排除项（见下表）。

   该应用程序将排除项条件与逻辑“AND”结合起来。要创建规则，您必须在“**完整路径**”字段中指定值，并选择至少一个事件类型。

7. 保存更改。

参数	描述
排除的进程	"**优化要发送的遥测大小**"。Kaspersky Endpoint Security 允许优化传输的数据量并从遥测中排除具有某些代码的事件：Microsoft SMB 协议、WinRM 服务和网络代理 klnagent.exe 进程的代码 102（基本通信）和 8（进程的网络活动），以及有关所有类型网络协议的网络数据包类型的扩展信息。 Kaspersky Endpoint Security 将规则触发条件与逻辑 AND 相结合。 **进程** 和 **父进程**： • "**完整路径**"。文件的完整路径，包括其名称和扩展名。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 * 以及 ? 字符。 • "**命令行文本**"。用于运行文件的命令。 • "**描述**"。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。 • "**原始文件名称**"。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。 • "**版本**"。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。 • "**文件校验和**"。MD5 和 SHA256。 您也可以手动选择文件，应用程序将自动填写所选文件中的字段。 在 64 位操作系统中，您必须手动输入进程的 64 位版本可执行文件（`C:\windows\system32` 文件夹中）的参数，因为应用程序使用 32 位版本的相同可执行文件（`C:\windows\syswow64`）的属性中的数据填充可执行文件参数字段。例如，如果您选择 `C:\windows\system32\cmd.exe`，则插件将显示 `C:\windows\syswow64\cmd.exe` 的参数。这种行为是由操作系统的特性决定的。 **用于以下事件类型**： • "**文件修改**"。 • "**网络事件**"。 • "**进程: 控制台交互式输入**"。 • "**模块已加载**"。 • "**注册表已修改**"。 • "DNS **日志**"。 • "**进程访问**"。 • "**代码注入**"。 • "WMI **查询**"。 • "**管道**"。 • "LDAP"。 • "AMSI"。
排除的网络通信	"**规则名称**"。 "**方向**"。 "**协议**"。 "**原始套接字**"。 "**协议号**"。 "TLS **证书**"。 "**本地端口或范围**"。 "**远程端口或范围**"。 "**本地地址**"。Kaspersky Endpoint Security 从网络流量中排除遥测的计算机的网络地址。 "**远程地址**"。Kaspersky Endpoint Security 从网络流量中排除遥测的计算机的网络地址。 IP 地址仅支持 IPv4 格式。 "**应用程序**"。Kaspersky Endpoint Security 从网络流量中排除 EDR 遥测的应用程序的可执行文件列表。

参数	描述
排除的文件操作	"**规则名称**"。 "**文件名或掩码**"。文件或文件夹的名称或掩码；当访问此文件或文件夹时，Kaspersky Endpoint Security 将应用排除规则。输入掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。 "**操作类型**"。 "**先前路径**"。 Kaspersky Endpoint Security 将规则触发条件与逻辑 AND 相结合。 **进程** 和 **父进程**： • "**完整路径**"。文件的完整路径，包括其名称和扩展名。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 * 以及 ? 字符。 • "**命令行文本**"。用于运行文件的命令。 • "**描述**"。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。 • "**原始文件名称**"。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。 • "**版本**"。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。 • "**文件校验和**"。MD5 和 SHA256。 您也可以手动选择文件，应用程序将自动填写所选文件中的字段。 在 64 位操作系统中，您必须手动输入进程的 64 位版本可执行文件（`C:\windows\system32` 文件夹中）的参数，因为应用程序使用 32 位版本的相同可执行文件（`C:\windows\syswow64`）的属性中的数据填充可执行文件参数字段。例如，如果您选择 `C:\windows\system32\cmd.exe`，则插件将显示 `C:\windows\syswow64\cmd.exe` 的参数。这种行为是由操作系统的特性决定的。
排除的 DNS 操作	"**规则名称**"。 Kaspersky Endpoint Security 将规则触发条件与逻辑 AND 相结合。 **进程** 和 **父进程**： • "**完整路径**"。文件的完整路径，包括其名称和扩展名。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 * 以及 ? 字符。 • "**命令行文本**"。用于运行文件的命令。 • "**描述**"。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。 • "**原始文件名称**"。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。 • "**版本**"。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。 • "**文件校验和**"。MD5 和 SHA256。 您也可以手动选择文件，应用程序将自动填写所选文件中的字段。 在 64 位操作系统中，您必须手动输入进程的 64 位版本可执行文件（`C:\windows\system32` 文件夹中）的参数，因为应用程序使用 32 位版本的相同可执行文件（`C:\windows\syswow64`）的属性中的数据填充可执行文件参数字段。例如，如果您选择 `C:\windows\system32\cmd.exe`，则插件将显示 `C:\windows\syswow64\cmd.exe` 的参数。这种行为是由操作系统的特性决定的。 DNS： • "**DNS 服务器 IP 地址**"。 • "**查询选项**"。 • "**状态**"。 • "**域名**"。 • "**设置类型 ID**"。 • "**相应数据**"。

参数	描述
排除的 LDAP 操作	"**规则名称**"。 "**LDAP 搜索范围**"。 "**过滤器**"。 "**LDAP 对象搜索的可分辨名称**"。 "**对象属性**"。 Kaspersky Endpoint Security 将规则触发条件与逻辑 AND 相结合。 **进程** 和 **父进程**: • "**完整路径**"。文件的完整路径，包括其名称和扩展名。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 * 以及 ? 字符。 • "**命令行文本**"。用于运行文件的命令。 • "**描述**"。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。 • "**原始文件名称**"。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。 • "**版本**"。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。 • "**文件校验和**"。MD5 和 SHA256。 您也可以手动选择文件，应用程序将自动填写所选文件中的字段。 在 64 位操作系统中，您必须手动输入进程的 64 位版本可执行文件（`C:\windows\system32` 文件夹中）的参数，因为应用程序使用 32 位版本的相同可执行文件（`C:\windows\syswow64`）的属性中的数据填充可执行文件参数字段。例如，如果您选择 `C:\windows\system32\cmd.exe`，则插件将显示 `C:\windows\syswow64\cmd.exe` 的参数。这种行为是由操作系统的特性决定的。
排除的进程访问查询	"**规则名称**"。 "**操作类型**"。 "**进程访问请求**"。 "**调用堆栈跟踪**"。 Kaspersky Endpoint Security 将规则触发条件与逻辑 AND 相结合。 **进程**、**父进程**、**目标进程文件**、**源进程句柄** 和 **目标进程的句柄**。 • "**完整路径**"。文件的完整路径，包括其名称和扩展名。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 * 以及 ? 字符。 • "**命令行文本**"。用于运行文件的命令。 • "**指定规则触发条件和使用此规则的事件类型。**"。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。 • "**原始文件名称**"。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。 • "**版本**"。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。 • "**文件校验和**"。MD5 和 SHA256。 您也可以手动选择文件，应用程序将自动填写所选文件中的字段。 在 64 位操作系统中，您必须手动输入进程的 64 位版本可执行文件（`C:\windows\system32` 文件夹中）的参数，因为应用程序使用 32 位版本的相同可执行文件（`C:\windows\syswow64`）的属性中的数据填充可执行文件参数字段。例如，如果您选择 `C:\windows\system32\cmd.exe`，则插件将显示 `C:\windows\syswow64\cmd.exe` 的参数。这种行为是由操作系统的特性决定的。

参数	描述
排除的代码注入	"**规则名称**"。 "**访问方法**"。 "**调用堆栈**"。 "**修改的命令行**"。 "**注入地址**"。 "**注入的 DLL 名称**"。 Kaspersky Endpoint Security 将规则触发条件与逻辑 AND 相结合。 **进程** 和 **父进程**: • "**完整路径**"。文件的完整路径，包括其名称和扩展名。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 * 以及 ? 字符。 • "**命令行文本**"。用于运行文件的命令。 • "**描述**"。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。 • "**原始文件名称**"。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。 • "**版本**"。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。 • "**文件校验和**"。MD5 和 SHA256。 您也可以手动选择文件，应用程序将自动填写所选文件中的字段。 在 64 位操作系统中，您必须手动输入进程的 64 位版本可执行文件（`C:\windows\system32` 文件夹中）的参数，因为应用程序使用 32 位版本的相同可执行文件（`C:\windows\syswow64`）的属性中的数据填充可执行文件参数字段。例如，如果您选择 `C:\windows\system32\cmd.exe`，则插件将显示 `C:\windows\syswow64\cmd.exe` 的参数。这种行为是由操作系统的特性决定的。
排除的 WMI 查询	"**规则名称**"。 "**WMI 操作类型**"。 "**远程查询**"。 "**执行 WMI 命令的计算机的名称**"。 "**WMI 用户账户**"。 "**执行的 WMI 命令**"。 "**WMI 名字空间**"。 "**WMI 事件使用者过滤器**"。 "**创建的 WMI 事件使用者的名称**"。 "**WMI 事件使用者源代码**"。 Kaspersky Endpoint Security 将规则触发条件与逻辑 AND 相结合。 **进程** 和 **父进程**: • "**完整路径**"。文件的完整路径，包括其名称和扩展名。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 * 以及 ? 字符。 • "**命令行文本**"。用于运行文件的命令。 • "**描述**"。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。 • "**原始文件名称**"。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。 • "**版本**"。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。 • "**文件校验和**"。MD5 和 SHA256。 您也可以手动选择文件，应用程序将自动填写所选文件中的字段。 在 64 位操作系统中，您必须手动输入进程的 64 位版本可执行文件（`C:\windows\system32` 文件夹中）的参数，因为应用程序使用 32 位版本的相同可执行文件（`C:\windows\syswow64`）的属性中的数据填充可执行文件参数字段。例如，如果您选择 `C:\windows\system32\cmd.exe`，则插件将显示 `C:\windows\syswow64\cmd.exe` 的参数。这种行为是由操作系统的特性决定的。

参数	描述
排除的管道操作	"**规则名称**"。 "**管道名称**"。 "**操作类型**"。 Kaspersky Endpoint Security 将规则触发条件与逻辑 AND 相结合。 **进程** 和 **父进程**: • "**完整路径**"。文件的完整路径，包括其名称和扩展名。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 * 以及 ? 字符。 • "**命令行文本**"。用于运行文件的命令。 • "**描述**"。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。 • "**原始文件名称**"。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。 • "**版本**"。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。 • "**文件校验和**"。MD5 和 SHA256。 您也可以手动选择文件，应用程序将自动填写所选文件中的字段。 在 64 位操作系统中，您必须手动输入进程的 64 位版本可执行文件（`C:\windows\system32` 文件夹中）的参数，因为应用程序使用 32 位版本的相同可执行文件（`C:\windows\syswow64`）的属性中的数据填充可执行文件参数字段。例如，如果您选择 `C:\windows\system32\cmd.exe`，则插件将显示 `C:\windows\syswow64\cmd.exe` 的参数。这种行为是由操作系统的特性决定的。
被排除的注册表更改	"**规则名称**"。 "**操作类型**"。 "**路径**"。 "**值名称**"。 "**值**"。 "**注册表文件全称**"。 Kaspersky Endpoint Security 将规则触发条件与逻辑 AND 相结合。 **进程** 和 **父进程**: • "**完整路径**"。文件的完整路径，包括其名称和扩展名。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 * 以及 ? 字符。 • "**命令行文本**"。用于运行文件的命令。 • "**描述**"。来自 RT_VERSION (VersionInfo) 资源的 FileDescription 参数的值。 • "**原始文件名称**"。来自 RT_VERSION (VersionInfo) 资源的 OriginalFilename 参数的值。 • "**版本**"。来自 RT_VERSION (VersionInfo) 资源的 FileVersion 参数的值。 • "**文件校验和**"。MD5 和 SHA256。 您也可以手动选择文件，应用程序将自动填写所选文件中的字段。 在 64 位操作系统中，您必须手动输入进程的 64 位版本可执行文件（`C:\windows\system32` 文件夹中）的参数，因为应用程序使用 32 位版本的相同可执行文件（`C:\windows\syswow64`）的属性中的数据填充可执行文件参数字段。例如，如果您选择 `C:\windows\system32\cmd.exe`，则插件将显示 `C:\windows\syswow64\cmd.exe` 的参数。这种行为是由操作系统的特性决定的。
排除的设备操作	"**规则名称**"。 "**设备类型**"。 "**设备 ID**"。 "**设备名称**"。

例 1。排除的进程

要从遥测中排除第三方应用程序（进程）事件，在“**排除的进程**”选项卡上打开 EDR 遥测排除项窗口并添加应用程序的可执行文件。

Kaspersky Endpoint Security 将规则触发条件与逻辑 AND 相结合。

当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。例如：

- `C:\Program Files\*\notepad++.exe`
- `%ProgramFiles(x86)%\Notepad++\notepad++.exe`

排除进程

例 1。文件修改

如果您经常在 Notepad++ 应用程序中编辑脚本，并且想要排除相应脚本的修改事件，请添加 Notepad++ 可执行文件到遥测排除项。

指定如下设置：

- **完整路径**：`C:\Program Files\Notepad++\notepad++.exe`。
- **SHA256**：64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34。
- **用于以下事件类型**：文件修改。

例 2。网络事件

如果您使用 WinSCP 应用程序管理远程服务器上的文件，并且想要排除网络事件，请添加 WinSCP 可执行文件到遥测排除项。

指定如下设置：

- **完整路径**：`C:\Program Files (x86)\WinSCP\WinSCP.exe`。
- **SHA256**：47204338f0e092057024c9186f228c02417e917777f3e841d52b58251a956a74 (optional)。
- **用于以下事件类型**：网络事件。

例 2。排除的网络通信

要从遥测中排除远程服务连接事件，在“**排除的网络通信**”选项卡上打开 EDR 遥测排除项窗口并添加连接设置：协议、端口、方向、IP 地址、TLS 证书等。

Kaspersky Endpoint Security 将规则触发条件与逻辑 AND 相结合。

> 您不能指定子网地址（例如，10.28.0.0/24）。应用程序仅允许指定一个 IP 地址（例如，10.28.0.105）。

网络通讯排除项

如果您使用公司 Web 服务器，并且想要在连接到该 Web 服务器时排除浏览器事件，请将服务器的 IP 地址和浏览器的可执行文件添加到遥测排除项中。

指定如下设置：

- **协议**：TCP。
- **远程端口或范围**：443。
- **远程地址**：10.28.0.105。
- **应用程序**：`C:\Program Files (x86)\Google\Chrome\Application\chrome.exe`；`C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe`。

例 3。排除的文件操作

要从遥测中排除涉及受信任文件操作的事件，在“**排除的文件操作**”选项卡上打开 EDR 遥测排除项窗口并添加受信任的文件。

Kaspersky Endpoint Security 将规则触发条件与逻辑 AND 相结合。

排除文件操作

如果应用程序写入日志并且您想要排除日志文件修改事件，请从遥测中添加日志文件和应用程序的可执行文件。

指定如下设置：

- **文件名或掩码**：`C:\Apache24\logs\error.log`。
- **操作类型**：文件修改。
- **完整路径**：`C:\Apache24\bin\httpd.exe`。
- **SHA256**：64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34。

例 4。排除的注册表修改

要从遥测中排除注册表修改事件，在“**被排除的注册表更改**”选项卡上打开 EDR 遥测排除项窗口并添加注册表键。

Kaspersky Endpoint Security 将规则触发条件与逻辑 AND 相结合。

如果应用程序频繁修改其注册表值，并且您想要从遥测中排除这些注册表修改事件，请将注册表键和应用程序的可执行文件添加到遥测排除项中。

指定如下设置：

- **操作类型**：修改。
- **路径**：HKEY_LOCAL_MACHINE\SOFTWARE\SimonTatham\PuTTY64。
- **完整路径**：`C:\Program Files\PuTTY\putty.exe`。
- **SHA256**：64F7A36C01E79CD4B041E8A8607DFF06D5B606D36E3DFF9CFB5FFFA22D14D34。

KATA Sandbox

Kaspersky Anti Targeted Attack Platform 包含 Sandbox（KATA Sandbox）组件。*Sandbox* 是一种可以检测计算机上高级威胁的技术。Sandbox 分析对象行为，以检测恶意活动和针对组织 IT 基础设施的攻击的活动特征。Sandbox 使用部署的 Microsoft Windows 操作系统虚拟映像（Sandbox 服务器）分析和扫描特殊服务器上的对象。有关解决方案的详细信息，请参阅 Kaspersky Anti Targeted Attack Platform 帮助。

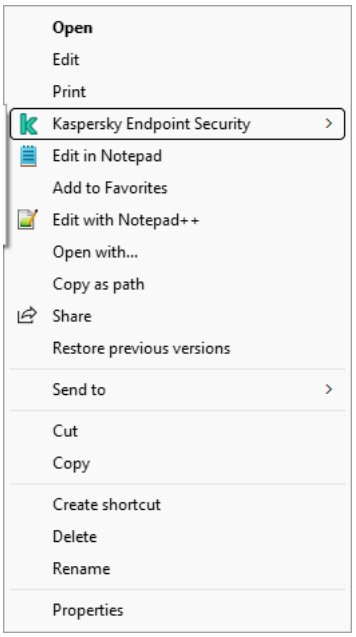
> 要激活 KATA Sandbox，您需要一个包含 KATA 或 KEDR 功能的授权许可密钥。有关可用功能的详细信息，请参阅 Kaspersky Anti Targeted Attack Platform 帮助。

KATA Sandbox 允许以以下模式扫描文件：

- *手动*。用户从上下文菜单手动提交文件进行扫描（**发送到 Sandbox**）。在将文件发送到 Sandbox 时，应用程序还会使用反病毒数据库扫描该文件。
- *自动*。应用程序自动检测对象并将其提交到 Sandbox 进行扫描。

文件发送到 Sandbox 后，用户仍然可以访问该文件。Kaspersky Endpoint Security 记录相应事件并将事件发送至 Kaspersky Security Center 和 Kaspersky Anti Targeted Attack Platform 控制台。如果 Sandbox 检测到恶意活动，Kaspersky Endpoint Security 会自动执行威胁响应操作（例如，它删除对象并启动关键区域扫描）。

为了使 KATA Sandbox 以手动模式运行，必须部署 Kaspersky Anti Targeted Attack Platform 7.0 或更高版本。为了使 KATA Sandbox 以自动模式运行，必须部署 Kaspersky Anti Targeted Attack Platform 8.0 或更高版本。



从上下文菜单在 KATA Sandbox 中扫描

内置代理与 KATA Sandbox 的集成

与 KATA Sandbox 组件集成需要添加 Sandbox 组件。您可以在安装或升级过程中选择 Sandbox 组件，也可以使用“*更改应用程序组件*”任务。

要发送文件进行扫描，您必须启用与 KATA Sandbox 的集成并添加部署在解决方案内部的 Central Node 服务器。该组件只能使用 Kaspersky Security Center Web Console 进行管理。您无法使用管理控制台（MMC）管理此组件。

要启用或禁用与 KATA Sandbox 的集成：

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置** → **Sandbox**。
5. 使用**与 Sandbox 的整合已启用**开关启用或禁用组件。

6. 选择 KATA Sandbox 运行模式：

- “**手动**”。用户从上下文菜单手动提交文件进行扫描（**发送到 Sandbox**）。
- “**自动**”。应用程序自动检测对象并将其提交到 Sandbox 进行扫描。
- “**组合的**”。

7. 单击**连接设置**链接。

8. 配置 Central Node 服务器连接设置：

- “**超时(豪秒)**”。Central Node 服务器连接超时。配置的超时时间过后，Kaspersky Endpoint Security 将向下一台服务器发送请求。如果连接速度低或连接不稳定，您可以增加服务器的连接超时。建议的请求超时是 0.5 秒或更少。
- “**请求队列**”。请求队列文件夹的大小。在发送多个对象以在 Sandbox 中进行扫描时，Kaspersky Endpoint Security 会创建一个请求队列。默认情况下，请求队列文件夹的大小限制为 100 MB。达到最大大小后，Sandbox 停止向队列添加新请求，并将相应的事件发送到 Kaspersky Security Center。您可以根据您的服务器配置来配置请求队列文件夹的大小。
- “**服务器 TLS 证书**”。要配置与 Central Node 服务器的受信任连接，您必须准备 TLS 证书。您必须使用策略将证书添加到计算机。您还需要将证书添加到 Central Node 服务器。
- “**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。

9. 在“**连接到 Sandbox 服务器**”块中单击“**添加**”按钮。

10. 这将打开一个窗口，您可以在其中输入 Central Node 服务器地址 (IPv4、IPv6、DNS) 和端口。

    有关部署虚拟镜像和配置 Central Node 服务器的详细信息，请参阅 Kaspersky Anti Targeted Attack Platform 帮助。

11. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

结果，Sandbox 组件被启用。通过查看*应用程序组件状态报告*检查组件的操作状态。您也可以利用 Kaspersky Endpoint Security 的本地界面在报告中查看组件的操作状态。**Sandbox** 组件将被添加到 Kaspersky Endpoint Security 组件列表。

配置威胁响应操作

如果 Sandbox 检测到恶意活动，Kaspersky Endpoint Security 会自动执行威胁响应操作（例如，删除对象并启动关键区域扫描）。

要配置威胁响应操作：

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **内置代理配置** → **Sandbox**。

5. 在"**检测到威胁后的操作**"块中选择相关操作：

   - "**将副本移动到隔离区，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 运行*关键区域扫描*任务。默认情况下，Kaspersky Endpoint Security 会扫描内核内存、运行进程和磁盘的引导扇区。

   - "**创建 IOC 扫描任务**"。如果选择此选项，Kaspersky Endpoint Security 将自动创建 *IOC 扫描(自主 IOC 扫描任务)*。对于此任务，您可以配置运行模式、扫描范围以及检测到 IOC 时执行的操作（*将副本移动到隔离区，删除对象* 或 *运行关键区域扫描*）。要修改 *IOC 扫描*任务的其他设置，请转到任务设置。

6. 如有必要，在"**IOC 扫描范围**"块配置"*IOC 扫描*"任务设置。

   - "**关键文件区域**"。如果选择此选项，Kaspersky Endpoint Security 仅在计算机的关键文件区域（内核内存和引导扇区）执行 IOC 扫描。

   - "**计算机系统驱动器上的文件区域**"。如果选择此选项，Kaspersky Endpoint Security 在计算机的系统驱动器上执行 IOC 扫描。

7. 如有必要，在"**运行 IOC 扫描任务**"块配置"*IOC 扫描*"任务设置。

   - "**手动**"。您可以在方便时手动启动"*IOC 扫描*"任务的运行模式。

   - "**自动**"。在此运行模式下，Kaspersky Endpoint Security 会在检测到威胁后自动运行 *IOC 扫描* 任务。

   - "**仅在计算机空闲时运行**"。Kaspersky Endpoint Security 在屏幕保护程序处于活动状态或屏幕被锁定时运行 *IOC 扫描*任务。如果用户解锁计算机，Kaspersky Endpoint Security 将暂停任务。这意味着任务可能需要几天才能完成。

8. 配置"*IOC 扫描*"的高级任务设置。

9. 要将此策略应用到计算机，请关闭 🔒 挂锁图标并保存更改。

EDR (KATA) 的 KEA 到 KES 迁移指南

从 12.1 开始，Kaspersky Endpoint Security for Windows 包含一个内置代理，用于管理 Kaspersky Endpoint Detection and Response 组件，作为 Kaspersky Anti Targeted Attack Platform 解决方案的一部分。您不再需要单独的 Kaspersky Endpoint Agent 应用程序与 EDR（KATA）一起使用。Kaspersky Endpoint Agent 的所有功能将由 Kaspersky Endpoint Security 执行。Kaspersky Anti Targeted Attack Platform 服务器上的负载将保持不变。

当您在安装了 Kaspersky Endpoint Agent 的计算机上部署 Kaspersky Endpoint Security 时，Kaspersky Anti Targeted Attack Platform（EDR）解决方案将继续与 Kaspersky Endpoint Security 一起工作。此外，Kaspersky Endpoint Agent 将被从计算机卸载。当您将 Kaspersky Endpoint Security 更新到版本 12.1 或更高版本时，系统中会发生相同的行为。

> Kaspersky Endpoint Security 与 Kaspersky Endpoint Agent 不兼容。您不能在同一台计算机上安装这两个应用程序。

Kaspersky Endpoint Security 必须满足以下条件才能作为 Endpoint Detection and Response（KATA）的一部分工作：

- Kaspersky Anti Targeted Attack Platform 版本 5.0 或更高版本。
- Kaspersky Security Center 版本 14.2 或更高版本（包括网络代理）。在 Kaspersky Security Center 的早期版本中，无法激活 Endpoint Detection and Response（KATA）功能。

EDR（KATA）的迁移 [KES+KEA] 配置到 [KES+内置代理] 的步骤

1. **升级 Kaspersky Endpoint Security 管理插件**

   EDR（KATA）组件可以使用 Kaspersky Endpoint Security 管理插件版本 12.1 或更高版本进行管理。根据您使用的 Kaspersky Security Center 控制台类型，更新管理控制台（MMC）中的管理插件或 Web Console 中的 Web 插件。

2. **迁移策略和任务**

   将 Kaspersky Endpoint Agent 设置传输到 Kaspersky Endpoint Security for Windows。下列选项可用：

   - 从 Kaspersky Endpoint Agent 迁移到 Kaspersky Endpoint Security 的向导。从 Kaspersky Endpoint Agent 迁移到 Kaspersky Endpoint Security 的向导仅适用于 Web Console

     如何在 Web Console 中将策略和任务设置从 Kaspersky Endpoint Agent 迁移到 Kaspersky Endpoint Security

     在 Web Console 的主窗口中，选择“**操作**” → “**从 Kaspersky Endpoint Agent 迁移**”。

     这将运行策略和任务迁移向导。按照向导的说明进行操作。

     步骤 1. 策略迁移

     迁移向导将创建一个新策略，该策略将合并 Kaspersky Endpoint Security 和 Kaspersky Endpoint Agent 策略的设置。在策略列表中，选择要将其设置与 Kaspersky Endpoint Security 策略合并的 Kaspersky Endpoint Agent 策略。单击 Kaspersky Endpoint Agent 策略以选择您要与之合并设置的 Kaspersky Endpoint Security 策略。确保选择了正确的策略，然后转到下一步。

     步骤 2. 任务迁移

     迁移向导不支持 EDR（KATA）任务。跳过此步骤。

     步骤 3. 向导完成

     退出向导。作为向导的结果，将创建一个新的 Kaspersky Endpoint Security 策略。策略从 Kaspersky Endpoint Security 和 Kaspersky Endpoint Agent 合并设置。策略被叫做 *<Kaspersky Endpoint Security 策略名称> 和 <Kaspersky Endpoint Agent 策略名称>*。新策略具有*不活动*状态。要继续，将 Kaspersky Endpoint Agent 和 Kaspersky Endpoint Security 策略的状态更改为*不活动*并激活新合并的策略。

Web Console 中的迁移向导跳过了以下策略设置并且不迁移它们：

- 设置修改禁止 **连接设置** （“锁”）。

  默认情况下，可以修改设置（“锁”是打开的）。因此，这些设置不会应用到计算机上。您必须禁止设置修改并关闭“锁”。

- 加密容器。

  如果您使用双向身份验证连接到 Central Node 服务器，则必须重新添加加密容器。

由于迁移向导不会迁移这些设置，您在将计算机连接到 Central Node 服务器时可能会遇到错误。要修复错误，您需要转到策略属性并配置连接设置。

- 标准的策略和任务批量转换向导。策略和任务批量转换向导仅在管理控制台（MMC）中可用。有关策略和任务批量转换向导的详细信息，请参阅 Kaspersky Security Center 帮助。

为确保 Kaspersky Endpoint Security 在服务器上正常工作，建议将对服务器功能重要的文件添加到受信任区域。对于 SQL 服务器，您必须添加 MDF 和 LDF 数据库文件。对于 Microsoft Exchange 服务器，您必须添加 CHK、EDB、JRS、LOG 和 JSL 文件。你可以使用掩码，例如，`C:\Program Files (x86)\Microsoft SQL Server\*.mdf`。

从 Kaspersky Endpoint Security 12.6 for Windows 开始，扫描排除项和受信任的应用程序被添加到信任区域。预定义的扫描排除项和受信任的应用程序有助于在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上快速配置 Kaspersky Endpoint Security。这意味着您不需要在服务器上为应用程序手动设置信任区域。

EDR 遥测排除项不会从 Kaspersky Endpoint Agent 策略迁移到 Kaspersky Endpoint Security 策略。Kaspersky Endpoint Security 有自己的排除工具 - 受信任应用程序。Kaspersky Endpoint Security 的操作经过优化，与 Kaspersky Endpoint Agent 相比，缺少单个的 EDR 遥测排除项不会对您的计算机造成任何额外负载。Kaspersky Endpoint Security 不仅将遥测用于 EDR（KATA），还用于应用程序保护组件的运行。因此，无需传输单个的 EDR 遥测排除项。如果您的计算机性能下降，请检查应用程序的运行情况（请参阅步骤 7 检查性能）。

3 许可 EDR（KATA）功能

要将 Kaspersky Endpoint Security 作为 Kaspersky Anti Targeted Attack Platform 解决方案的一部分激活，您需要单独的 Kaspersky Endpoint Detection and Response（KATA）加载项授权许可。您可以使用“*添加密钥*”任务添加密钥。结果，两个密钥将被添加到应用程序中：*Kaspersky Endpoint Security* 和 *Kaspersky Endpoint Detection and Response（KATA）*。

在之前激活了 EDR Optimum 或 EDR Expert 功能的计算机上授权 Kaspersky Endpoint Detection and Response（KATA）加载项涉及以下特殊注意事项：

- 如果您正在使用*密钥文件*授权带有 EDR Optimum 或 EDR Expert 功能的 Kaspersky Endpoint Security，您无法为 Kaspersky Endpoint Detection and Response（KATA）加载项添加单独的密钥。您可以切换到使用激活码进行授权，或者联系您的服务提供商以获取新的密钥文件来激活 Kaspersky Endpoint Security 和 EDR 功能。服务提供商将提供一个或多个用于授权的密钥文件。

- 如果您正在使用*密钥文件*授权没有 EDR Optimum 或 EDR Expert 功能的 Kaspersky Endpoint Security，您可以为 Kaspersky Endpoint Detection and Response（KATA）加载项添加单独的密钥，而无需重新发布密钥文件。

- 如果您正在使用*激活码*进行授权，卡巴斯基激活服务器将自动重新发布密钥，并且 EDR（KATA）功能将自动可用。在这种情况下，EDR Optimum 和 EDR Expert 将被禁用。

- Kaspersky Endpoint Security 允许您添加最多两个活动密钥：Kaspersky Endpoint Security 密钥和加载项类型密钥。您还可以添加最多两个备用密钥。一个 Kaspersky Endpoint Security 备用密钥和一个加载项类型备用密钥。

4 **安装/升级 Kaspersky Endpoint Security 应用程序**

要在应用程序安装或升级期间迁移 EDR（KATA）功能，建议使用远程安装任务。创建远程安装任务时，您需要在安装包设置中选择 EDR（KATA）组件。

您还可以使用以下方法升级应用程序：

- 使用卡巴斯基更新服务。

- 本地使用安装向导。

Kaspersky Endpoint Security 支持在安装了 Kaspersky Endpoint Agent 应用程序的计算机上升级应用程序时自动选择组件。组件的自动选择取决于升级应用程序的用户账户的权限。

如果您在系统账户（SYSTEM）下使用 EXE 或 MSI 文件升级 Kaspersky Endpoint Security，Kaspersky Endpoint Security 获得对卡巴斯基解决方案的当前授权许可的访问权。因此，如果计算机安装了 Kaspersky Endpoint Agent，并且激活了 EDR（KATA）解决方案，则 Kaspersky Endpoint Security 安装程序将自动配置组件集并选择 EDR（KATA）组件。这将使 Kaspersky Endpoint Security 切换到使用内置代理并卸载 Kaspersky Endpoint Agent。在系统账户（SYSTEM）下运行 MSI 安装程序通常在通过卡巴斯基更新服务升级时执行，或者当通过 Kaspersky Security Center 部署安装包时。

如果您在非特权用户账户下使用 MSI 文件升级 Kaspersky Endpoint Security，Kaspersky Endpoint Security 缺少对卡巴斯基解决方案的当前授权许可的访问权。在这种情况下，Kaspersky Endpoint Security 会根据 Kaspersky Endpoint Agent 的一组组件自动选择组件。此后，Kaspersky Endpoint Security 将切换到使用内置代理并卸载 Kaspersky Endpoint Agent。

> Kaspersky Endpoint Security 支持在不重启计算机的情况下升级。您可以选择策略属性中的应用程序升级模式。

5 **检查应用程序运行情况**

如果在应用程序安装或升级之后，计算机在 Kaspersky Security Center 控制台显示"*严重*"状态：

- 确保计算机安装了网络代理版本 13.2 或更高版本。

- 通过查看"*应用程序组件状态报告*"检查内置代理的操作状态。如果组件具有*未安装*状态，使用"*更改应用程序组件*"任务安装组件。如果一个组件有"*授权许可不支持*"状态，确保您已激活内置代理功能。

- 确保您在 Kaspersky Endpoint Security for Windows 的新策略中接受了卡巴斯基安全网络声明。

6 **检查与 Kaspersky Anti Targeted Attack Platform 服务器的连接**

检查与 Kaspersky Anti Targeted Attack Platform 服务器的连接。为此，请执行下列操作：

1. 检查您是否拥有有效的证书。

2. 检查服务器连接设置。

3. 检查事件日志。

   如果建立了与服务器的连接，应用程序将发送事件"*成功连接到 EDR Expert 服务器*"。如果没有成功连接事件并且没有连接错误事件，检查事件日志设置并启用 Endpoint Detection and Response（KATA）的事件发送。

服务器连接状态不会影响 Kaspersky Security Center 控制台中的计算机状态。因此，如果没有连接到服务器，计算机仍然可以拥有“*确定*”状态。检查事件日志以验证与服务器的连接。

7 **检查性能**

如果您的计算机在安装或更新应用程序后性能下降，您可以优化数据传输。为此，请执行下列操作：

1. 禁用 EDR（KATA）组件并检查性能下降是由于 EDR（KATA）。
2. 对于受信任的应用程序，关闭控制台输入操作的遥测收集（默认启用）。
3. 将降低计算机性能的应用程序添加到受信任的应用程序列表。
4. 联系卡巴斯基技术支持。支持专家将帮助您在 Kaspersky Anti Targeted Attack Platform 中配置遥测过滤。这将减少流量。如果您的计算机性能受到某个应用程序的影响，请在请求中附上该应用程序的分发包。

Endpoint Detection and Response Expert（本地部署）

Kaspersky Endpoint Security for Windows 支持与 Kaspersky Endpoint Detection and Response Expert (on-premises) 解决方案集成。*Kaspersky Endpoint Detection and Response Expert (on-premises)* 是一款企业网络安全解决方案，其中包括卡巴斯基应用程序，可帮助组织防御大多数类型的网络风险并涵盖最重要的威胁传播场景。EDR Expert (on-premises) 组件部署在 Open Single Management Platform (OSMP) 上。该平台可在单一界面中运行跨平台方案，并允许将卡巴斯基应用程序与第三方应用程序集成到全面的安全系统中。

解决方案的核心要素之一是 *SIEM*。SIEM 跟踪来自所有组件的事件，并使用供应商和用户定义的规则将这些事件相互关联起来。EDR Expert (on-premises) 会查看从企业基础设施接收的日志和遥测数据，以自动检测攻击，并允许使用统一的调查图来调查事件，该调查图结合了 EDR Expert (on-premises) 中采集的所有事件，包括来自卡巴斯基应用程序和第三方信息安全产品的事件。

对于高级事件的响应，EDR Expert (on-premises) 使用预设方案和用户自定义方案。您还可以使用来自第三方应用程序的响应操作以及涉及多个应用程序的响应方案。

威胁情报工具

Kaspersky Endpoint Detection and Response 使用以下 Threat Intelligence 工具：

- 与卡巴斯基威胁情报门户集成，该系统包含并显示有关文件和网址信誉的信息。
- 卡巴斯基威胁数据库。
- 卡巴斯基安全网络（以下也称为“KSN”）云服务基础设施，提供对 Kaspersky 知识库中实时文件、网站和软件信誉信息的访问。使用卡巴斯基安全网络的数据可确保 Kaspersky 应用程序能够更快地对新威胁作出响应，提高一些保护组件的性能，并减少误报风险。

解决方案的工作原理

Kaspersky Endpoint Security 安装在公司 IT 基础设施的各个计算机上，并持续监视流程、开放式网络连接和正在修改的文件。

> 在 VDI 基础架构中以标准模式安装时，Kaspersky Endpoint Security 支持与 EDR Expert (on-premises) 集成。但是，应用程序其他功能的可操作性无法保证。为了保护 VDI 基础架构中的虚拟机，我们建议再 Light Agent 模式下使用 Kaspersky Endpoint Security。

计算机事件信息（遥测数据）被发送到 EDR Expert (on-premises) 服务器。在这种情况下，Kaspersky Endpoint Security 还会将应用程序发现的威胁信息以及这些威胁的处理结果信息发送到遥测采集服务器。

EDR Expert (on-premises) 集成在 Kaspersky Security Center 控制台中配置。然后使用 Open Single Management Platform (OSMP) 管理内置代理，包括运行任务、管理隔离对象、查看报告和其他操作。

用于使用 EDR Expert (on-premises) 的 Kaspersky Endpoint Security 配置

以下配置可用于使用 EDR Expert (on-premises)：

- **[KES+内置代理]**。在此配置中，Kaspersky Endpoint Security 既充当确保计算机安全的应用程序，又充当使用 EDR Expert (on-premises) 的应用程序。Kaspersky Endpoint Security 12.11 for Windows 或更高版本中提供了 EDR Expert (on-premises) 内置代理。
- **[第三方 EPP+EDR Agent]**。在此配置中，IT 基础设施的安全性由第三方 Endpoint Protection Platform（EPP）提供。与 EDR Expert (on-premises) 的交互由 Kaspersky Endpoint Security 在“Endpoint Detection and Response Agent（EDR Agent）”配置中提供。在此配置中，EDR Agent 兼容第三方 EPP 应用程序。EDR Expert (on-premises) 的 EDR Agent 在 Kaspersky Endpoint Security 12.11 for Windows 或更高版本中可用。

内置代理与 EDR Expert (on-premises) 的集成

要与 Kaspersky Endpoint Detection and Response Expert (on-premises) 解决方案集成，您必须添加 Endpoint Detection and Response Expert (on-premises) 组件，并配置 Kaspersky Endpoint Security。

> “Endpoint Detection and Response Optimum”、“Endpoint Detection and Response Expert (cloud)”和“Endpoint Detection and Response Expert (on-premises)”组件彼此不兼容。

要使 Endpoint Detection and Response Expert (on-premises) 正常运行，必须满足以下条件：

- OSMP（Open Single Management Platform 已安装。
- 应用程序已激活，授权许可涵盖了该功能。
- Endpoint Detection and Response Expert (on-premises) 组件已开启。

- 确保 EDR Expert (on-premises) 运行的应用程序组件已启用并正常运行。以下组件确保 EDR Expert (on-premises) 的运行：
  - 文件威胁防护。
  - Web 威胁防护。
  - 邮件威胁防护。
  - 漏洞利用防御。
  - 行为检测。
  - 主机入侵防御。
  - 修复引擎。
  - 自适应异常控制。

设置 EDR Expert (on-premises) 集成涉及以下步骤：

1. **安装 EDR Expert (on-premises) 组件**

   您可以在安装或升级过程中选择 EDR Expert (on-premises) 组件，也可以使用"*更改应用程序组件*"任务。

   > 您必须重新启动计算机才能使用新组件完成应用程序的升级。

2. **激活 Kaspersky Endpoint Detection and Response Expert (on-premises)**

   您需要为 EDR Expert (on-premises)（Kaspersky Endpoint Detection and Response Expert (on-premises) 加载项）购买单独的授权许可。

   该功能将在为 Kaspersky Endpoint Detection and Response Expert (on-premises) 添加单独密钥后可用。因此，计算机上将添加两个密钥：Kaspersky Endpoint Security 密钥和 Kaspersky Endpoint Detection and Response Expert (on-premises) 密钥。

   独立 Endpoint Detection and Response Expert (on-premises) 功能的授权许可与 Kaspersky Endpoint Security 的授权许可相同。

   确保授权许可中包含 EDR Expert (on-premises) 功能，并且该功能正在应用程序的本地界面中运行。

3. **连接到遥测采集服务器和响应服务器**

   Kaspersky Endpoint Detection and Response Expert (on-premises) 需要 Kaspersky Endpoint Security 与两台服务器之间建立受信任连接：

   - *遥测采集服务器* 是 SIEM 解决方案的一部分，用于收集、规范化、关联、分析和存储有关计算机上发生的事件的信息。
   - *响应服务器* 是一个用于接收和扫描数据、研究对象行为和发布此类研究结果的服务器。

   要配置可信连接，您必须使用 TLS 证书。您可以在 Open Single Management Platform 上获取 TLS 证书（请参阅 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助中的说明）。然后您必须将 TLS 证书添加到 Kaspersky Endpoint Security（参见下面的说明）。

默认情况下，Kaspersky Endpoint Security 仅检查服务器的 TLS 证书。为了使连接更安全，您可以额外启用服务器上的计算机验证（双向身份验证）。要启用此验证，您必须在服务器和 Kaspersky Endpoint Security 设置中打开双向身份验证。要使用双向身份验证，您还需要一个加密容器。*加密容器*是带有证书和私钥的 PFX 存档。您可以在 Open Single Management Platform 上获取加密容器（请参阅 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助中的说明）。

如何使用 Web Console 将 Kaspersky Endpoint Security 计算机连接到 EDR Expert (on-premises)

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”选项卡。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置** → **Endpoint Detection and Response Expert (on-premise)**。
5. 开启 **Endpoint Detection and Response Expert (on-premise) 已启用**切换开关。
6. 要配置 EDR Expert (on-premises)，请从解决方案列表中选择“**Endpoint Detection and Response Expert (版本 8.0 或更高版本)**”。
7. 配置*遥测采集服务器*连接：

   a. 在“**连接到遥测采集服务器**”区域，单击“**连接设置**”链接。

   b. 配置遥测采集服务器连接：

   - “**超时(秒)**”。最大服务器响应超时。当超时用完时，Kaspersky Endpoint Security 会尝试连接到不同的服务器。
   - “**服务器证书**”。用于与服务器建立受信任连接的 TLS 证书。您可以在 Open Single Management Platform 上获取 TLS 证书（请参阅 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助中的说明）。
   - “**使用双向身份验证**”。在 Kaspersky Endpoint Security 和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 Open Single Management Platform 上获取加密容器（请参阅 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助中的说明）。配置服务器设置后，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。

   c. 单击“**确定**”。

   d. 添加遥测采集服务器。为此，请指定服务器地址（IPv4、IPv6）和连接到服务器的端口。

   您可以添加多个遥测采集服务器地址。Kaspersky Endpoint Security 尝试使用第一个 IP 地址连接到服务器。如果连接建立失败，Kaspersky Endpoint Security 将尝试使用列表中的第二个 IP 地址进行连接，依此类推。

   e. 如果有必要，配置遥测。

8. 配置*响应服务器*连接：

   a. 在“**连接到响应服务器**”块中，配置“**发送同步请求到服务器的间隔(分钟)**”设置。发送到服务器的同步请求的频率。在同步过程中，Kaspersky Endpoint Security 接收威胁响应任务并发送任务结果。

   b. 单击**连接设置**链接。

   c. 配置响应服务器连接：

      - “**超时(秒)**”。最大服务器响应超时。当超时用完时，Kaspersky Endpoint Security 会尝试连接到不同的服务器。

      - “**服务器证书**”。用于与服务器建立受信任连接的 TLS 证书。您可以在 Open Single Management Platform 上获取 TLS 证书（请参阅 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助中的说明）。

      - “**使用双向身份验证**”。在 Kaspersky Endpoint Security 和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 Open Single Management Platform 上获取加密容器（请参阅 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助中的说明）。配置服务器设置后，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。

   d. 单击“**确定**”。

   e. 添加响应服务器。为此，请指定服务器地址（IPv4、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 尝试使用第一个 IP 地址连接到服务器。如果连接建立失败，Kaspersky Endpoint Security 将尝试使用列表中的第二个 IP 地址进行连接，依此类推。

9. 要将此策略应用到计算机，请关闭 🔒 挂锁图标并保存更改。

因此，计算机被添加到 Open Single Management Platform (OSMP) 上的受管理设备列表中。通过查看*应用程序组件状态报告*检查组件的操作状态。您也可以利用 Kaspersky Endpoint Security 的本地界面在报告中查看组件的操作状态。**Endpoint Detection and Response Expert (on-premises)** 组件将被添加到 Kaspersky Endpoint Security 组件列表。

配置 EDR Expert (on-premises) 遥测设置

*遥测*是受保护计算机上发生的事件的列表。Kaspersky Endpoint Security 在同步期间分析遥测数据并将其发送到遥测采集服务器。遥测事件几乎连续不断地到达服务器。当满足以下任一条件时，Kaspersky Endpoint Security 启动与服务器的同步：

- 同步间隔已用完。

- 缓冲区中的事件数超过上限。

因此，默认情况下，应用程序每 30 秒或每当缓冲区包含 1024 个事件时同步一次。您可以在 Kaspersky Endpoint Security 策略中配置同步行为并选择最佳值以匹配您的网络负载（请参阅下面的说明）。

如果 Kaspersky Endpoint Security 与服务器之间没有连接，应用程序将对新事件进行排队。当连接恢复时，Kaspersky Endpoint Security 以正确的顺序将排队的事件发送到服务器。为避免服务器过载，Kaspersky Endpoint Security 可能会跳过一些事件。要启用此功能，您可以优化事件传输设置，例如，设置每小时最大事件数值（请参阅下面的说明）。

要配置遥测设置，请执行下列步骤：

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”选项卡。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置** → **Endpoint Detection and Response Expert (on-premise)**。
5. 要配置 EDR Expert (on-premises)，请从解决方案列表中选择“**Endpoint Detection and Response Expert (版本 8.0 或更高版本)**”。
6. 确保在“**数据传输设置**”块中，“**将遥测发送到遥测采集服务器**”复选框被选中。
7. 如有必要，选中“**仅发送带有 IOA 的遥测**”复选框。*攻击指标 (IOA)* 是一条包含系统中可能表明有针对性攻击的可疑行为描述的规则。应用程序将系统中正在进行的行为与这些规则进行比较，并记录表明有针对性攻击的事件。应用程序使用*流式扫描*技术，可以实时跟踪此类事件。
8. 如果需要，请在“**数据传输设置**”块配置与服务器设置的同步：
   - “**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。默认设置是 30 秒。
   - “**事件包的最大数量**”。当缓冲区充满事件时，应用程序会与服务器同步。默认设置是 1024 个事件。
9. 如有必要，请清除 **请求限制** 块中的 **启用请求限制** 复选框。

   该功能有助于优化服务器上的负载。如果启用此功能，应用程序将限制事件传输。如果事件数量超过配置的限制，Kaspersky Endpoint Security 将停止发送事件。默认情况下已启用此选项。
10. 配置用于将事件发送到服务器的优化设置：
    - “**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。默认设置是每小时 3000 个事件。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。默认设置为 15%。
11. 在“**连接到响应服务器**”块中，为“**发送同步请求到服务器的间隔(分钟)**”参数输入一个值。
12. 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。
13. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

EDR Expert (on-premises) 遥测排除项

要提高性能并优化到遥测采集服务器的数据传输，您可以配置遥测排除项。例如，您可以选择不发送单个应用程序的网络通信数据。

> 使用过多的规则会增加遥测采集服务器的负载并降低计算机性能。我们建议只添加必要的规则。

要在 Web Console 和云控制台中创建遥测排除项：

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”选项卡。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **遥测设置**。
5. 选择**EDR Expert (on-premise) 遥测**选项卡。
6. 在“**常规排除项**”块中单击“**添加**”按钮。
   “**添加排除规则**”窗口将打开。
7. 如有必要，可更改规则状态。默认情况下，规则已启用。
8. 输入规则的名称。
9. 选择触发规则时要执行的操作：
   - “**不采集**”。被过滤的事件将从发送的遥测数据中排除。
   - “**排除 IOA**”。IOA 规则触发器事件将从发送的遥测数据中排除。
10. 如果选中“**排除 IOA**”选项，请指定要添加到排除项中的 IOA 规则：
    - “**全部排除**”。当满足指定条件时，应用程序将从遥测数据中排除基于所有 IOA 规则生成的事件。
    - “**按 GUID 排除**”。指定 IOA 规则的 GUID。您可以使用“`,`”指定多个 GUID。有关 IOA 规则的更多详细信息，请参阅 EDR Expert（本地部署）帮助。
11. 指定过滤条件：
    a. 选择用于过滤的字段名称。
    b. 选择一个运算符（见下表），并指定要与事件中的字段值进行比较的值。

条件运算符列表

运算符	描述
<	如果字段值小于条件中指定的值，则该事件将被过滤出来。
≤	如果字段值小于或等于条件中指定的值，则该事件将被过滤出来。
=	如果字段值等于条件中指定的值，则该事件将被过滤出来。
≥	如果字段值大于或等于条件中指定的值，则该事件将被过滤出来。
>	如果字段值大于条件中指定的值，则该事件将被过滤出来。
≠	如果字段值与条件中指定的值不相等，则该事件将被过滤出来。
类似	如果字段值与条件中指定的掩码匹配，则该事件将被过滤出来。输入掩码时，应用程序支持“*”字符和“?”字符：
不类似	如果字段值与条件中指定的掩码不匹配，则该事件将被过滤出来。输入掩码时，应用程序支持“*”字符和“?”字符：
之一	如果字段值与条件中指定的列表中的某个值匹配，则该事件被视为已过滤。
没有一个	如果字段值与条件中指定的列表中的任何值都不匹配，则该事件被视为已过滤。
类似其中之一	如果字段值与条件中指定的某个掩码匹配，则该事件将被过滤出来。输入掩码时，Kaspersky Endpoint Security 支持 * 字符和 ? 字符。
不类似其中之一	如果字段值与条件中指定的任何掩码都不匹配，则该事件将被过滤出来。输入掩码时，Kaspersky Endpoint Security 支持 * 字符和 ? 字符。
存在	如果条件中指定的字段出现在事件中，则该事件将被过滤出来。
不存在	如果条件中指定的字段不出现在事件中，则该事件将被过滤出来。
包含	如果条件中指定的值出现在字段值中，则该事件将被过滤出来。
等于	如果字段值等于条件中指定的值，则该事件将被过滤出来。扫描不区分大小写。
按位和	如果字段值与条件中指定的值之间的 Bitwise AND (&) 运算结果为 1，则该事件将被过滤出来。

12. 如有必要，您可以通过添加多个过滤条件和条件组来创建复杂的过滤条件。您还可以向条件组中添加嵌套条件和条件组。您可以使用以下运算符：

    - **且** 表示过滤器会选择符合所有指定条件的事件。
    - **或** 表示过滤器会选择符合指定条件之一的事件。
    - **非**（要使用此运算符，请选择“**在此之前加非**”选项）表示该过滤器选择不符合任何指定条件的事件。

    条件和一级条件组使用 **且** 运算符结合。

13. 如果您的计算机运行的是 Open Single Management Platform (OSMP)，您可以扫描您创建的过滤规则。要运行扫描，请单击“**检查规则**”按钮。

    在打开的窗口中，将显示使用创建的规则过滤的事件表。有关更多详细信息，请参阅 EDR Expert（本地部署）帮助。

14. 如有必要，在“**所有事件类型**”下，按事件类型添加遥测排除项。

    a. 点击事件类型名称。

    b. 在打开的窗口中，单击“**手动设置**”按钮。

    c. 如有必要，请使用“**发送事件**”切换开关配置所选事件类型的遥测发送。默认情况下，所有事件类型均启用遥测数据传输。

d. 在“**排除规则**”块中单击“**添加**”按钮。
“**添加排除规则**”窗口将打开。

e. 对添加的每条规则执行步骤 7-13 中描述的操作。

15. 对于某些事件类型，您还可以添加包含规则来扩展收集到的遥测数据：

a. 在“**包含规则**”块中单击“**添加**”按钮。
“**添加包含规则**”窗口将打开。

b. 输入规则的名称。

c. 在“**条件**”下，输入所显示字段的值。可用字段类型取决于所选事件。

> 排除规则优先于包含规则。

16. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

导出和导入 EDR Expert (on-premises) 事件过滤器

可以将排除列表导出到 JSON 文件。然后可以修改文件，例如，添加大量事件 ID。还可以使用导出/导入功能备份事件过滤器或将列表迁移到其他服务器。

> 使用过多的规则会增加遥测采集服务器的负载并降低计算机性能。我们建议只添加必要的规则。

如何在管理控制台 (MMC) 中导出和导入事件过滤器

1. 打开 Kaspersky Security Center Administration Console。

2. 在控制台树中，选择“**策略**”。

3. 选择必要的策略并双击以打开策略属性。

4. 在策略窗口中，选择 **常规设置** → **排除项和对象类型**。

5. 在“**遥测设置** → **EDR Expert (on-premises) 遥测**”块中单击“**设置**”按钮。

6. 要导出事件过滤器：

a. 单击“**导出**”。
在打开的窗口中，指定您要将事件过滤器导出到的 JSON 文件的名称，然后选择要保存此文件的文件夹。

b. 保存文件。
Kaspersky Endpoint Security 会将事件过滤器导出到 JSON 文件。

7. 要导入事件过滤器：

   a. 单击“**导入**”。

   b. 在打开的窗口中，选择要从中导入事件过滤器的 JSON 文件。

   c. 打开文件。
      如果计算机上已经存在事件过滤规则，Kaspersky Endpoint Security 会在导入时替换这些规则。

8. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 中导出和导入事件过滤器

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **常规设置** → **遥测设置**。

5. 选择**EDR Expert (on-premise) 遥测**选项卡。

6. 要导出事件过滤器：

   a. 单击“**导出**”。

   b. 在打开的窗口中，指定您要将事件过滤器导出到的 JSON 文件的名称，然后选择要保存此文件的文件夹。

   c. 保存文件。
      Kaspersky Endpoint Security 会将事件过滤器导出到 JSON 文件。

7. 要导入事件过滤器：

   a. 单击“**导入**”。

   b. 在打开的窗口中，选择要从中导入事件过滤器的 JSON 文件。

   c. 选择您希望如何导入事件过滤规则：添加到现有规则或丢弃现有规则并用新规则替换。

   d. 打开文件。

8. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

您还可以在命令行上导出或导入事件过滤器。

使用策略配置文件配置与 EDR Expert（(on-premises)和 EDR (KATA) 集成时的特殊注意事项

要在单个策略中为某些管理组配置与 EDR (KATA) 的集成，并为其他管理组配置与 EDR Expert(on-premises)的集成，您需要使用策略配置文件。您必须在策略属性中配置 EDR (KATA) 集成设置，并且应在策略配置文件属性中为选定的管理组配置 EDR Expert(on-premises)集成。

使用策略配置文件配置与 EDR Expert(on-premises)的集成存在以下限制：

- 如果在策略属性中配置与 EDR Expert(on-premises)的集成，则这些设置将应用于所有管理组；策略配置文件中的集成设置将不会应用。
- 使用策略配置文件配置与 EDR Expert(on-premises)的集成时，不能使用管理控制台 (MMC) 来管理策略。在管理控制台中打开策略属性时，策略配置文件中的 EDR Expert(on-premises)集成设置将被策略中的设置覆盖，导致组件无法正常运行。您需要按照以下说明重置 Endpoint Detection and Response Expert (on-premises) 组件设置。
- 使用策略配置文件配置与 EDR Expert(on-premises)的集成时，不能使用子策略。

如果您已有在先前版本的 Web 插件中配置的策略，则必须重置 Endpoint Detection and Response Expert (on-premises) 组件设置，以便将策略配置文件中的 EDR Expert(on-premises)集成设置应用到受管理设备。

要重置组件设置：

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”选项卡。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置** → **Endpoint Detection and Response Expert (on-premise)**。
5. 将运行模式从 **Endpoint Detection and Response Expert (版本 7.1 或更早版本)** 更改为 **Endpoint Detection and Response Expert (版本 8.0 或后续版本)模式**。
6. 切换回 **Endpoint Detection and Response Expert (版本 7.1 或更早版本)**。
7. 保存更改。

Endpoint Detection and Response Expert (cloud)

Kaspersky Endpoint Security for Windows 与 Kaspersky Endpoint Detection and Response Expert (cloud) 的集成暂时不可用。计划在 2026 年底之前支持此功能。请关注我们的发行说明，以了解应用程序升级和新功能。

Kaspersky Endpoint Security for Windows 支持与 Kaspersky Endpoint Detection and Response Expert (cloud) 解决方案集成。*Kaspersky Endpoint Detection and Response Expert (cloud)* 是一款基于云的企业网络安全解决方案，其中包括卡巴斯基应用程序，可帮助组织防御大多数类型的网络风险并涵盖最重要的威胁传播场景。EDR Expert (cloud) 组件部署在 Open Single Management Platform (OSMP) 上。该平台可在单一界面中运行跨平台方案，并允许将卡巴斯基应用程序与第三方应用程序集成到全面的安全系统中。

在基于 Arm 的计算机上不支持与 Kaspersky Endpoint Detection and Response Expert (cloud) 集成。

解决方案的核心要素之一是 *SIEM*。SIEM 跟踪来自所有组件的事件，并使用供应商和用户定义的规则将这些事件相互关联起来。EDR Expert (cloud) 会查看从企业基础设施接收的日志和遥测数据，以自动检测攻击，并允许使用统一的调查图来调查事件，该调查图结合了 EDR Expert (cloud) 中采集的所有事件，包括来自卡巴斯基应用程序和第三方信息安全产品的事件。

对于高级事件的响应，EDR Expert (cloud) 使用预设方案和用户自定义方案。您还可以使用来自第三方应用程序的响应操作以及涉及多个应用程序的响应方案。

威胁情报工具

Kaspersky Endpoint Detection and Response 使用以下 Threat Intelligence 工具：

- 与卡巴斯基威胁情报门户集成，该系统包含并显示有关文件和网址信誉的信息。
- 卡巴斯基威胁数据库。
- 卡巴斯基安全网络（以下也称为“KSN”）云服务基础设施，提供对 Kaspersky 知识库中实时文件、网站和软件信誉信息的访问。使用卡巴斯基安全网络的数据可确保 Kaspersky 应用程序能够更快地对新威胁作出响应，提高一些保护组件的性能，并减少误报风险。

解决方案的工作原理

Kaspersky Endpoint Security 安装在公司 IT 基础设施的各个计算机上，并持续监视流程、开放式网络连接和正在修改的文件。

计算机事件信息（遥测数据）被发送到 EDR Expert (cloud) 服务器。在这种情况下，Kaspersky Endpoint Security 还会将应用程序发现的威胁信息以及这些威胁的处理结果信息发送到遥测采集服务器。

EDR Expert (cloud) 集成在 Kaspersky Security Center 控制台中配置。然后使用 Open Single Management Platform (OSMP) 管理内置代理，包括运行任务、管理隔离对象、查看报告和其他操作。

内置代理与 EDR Expert (cloud) 的集成

要设置与 Kaspersky Endpoint Detection and Response (cloud) 解决方案的集成，您必须安装“Endpoint Detection and Response Expert (cloud)”组件并配置 Kaspersky Endpoint Security。

“Endpoint Detection and Response Optimum”、“Endpoint Detection and Response Expert (cloud)”和“Endpoint Detection and Response Expert (on-premises)”组件彼此不兼容。

EDR Expert（云）运行条件

要使 EDR Expert (cloud) 正常工作，必须满足以下条件：

- Kaspersky Endpoint Detection and Response Expert (cloud) 基础设施已在您所在的地区推出。如需了解您所在地区 EDR Expert (cloud) 基础设施的可用性信息，请联系技术支持。
- OSMP（Open Single Management Platform 已安装。
- Kaspersky Endpoint Security 以标准模式安装。
- Kaspersky Endpoint Security 应用程序已激活，授权许可涵盖了该功能。
- 您已接受 Kaspersky Endpoint Detection and Response Expert (cloud) 数据处理协议的条款。
- “Endpoint Detection and Response Expert (cloud)”组件已启用。
- 确保 EDR Expert (cloud) 运行的应用程序组件已启用并可运行。
  - 文件威胁防护。
  - Web 威胁防护。
  - 邮件威胁防护。
  - 漏洞利用防御。
  - 行为检测。
  - 主机入侵防御。
  - 修复引擎。
  - 自适应异常控制。

与 EDR Expert（云）集成的步骤

设置 EDR Expert (cloud) 集成涉及以下步骤：

1. **安装“Endpoint Detection and Response Expert (cloud)”组件**

   您可以在安装或升级过程中选择 Endpoint Detection and Response Expert (cloud) 组件，也可以使用“*更改应用程序组件*”任务。

   > 您必须重新启动计算机才能使用新组件完成应用程序的升级。

2. **激活 Kaspersky Endpoint Detection and Response Expert (cloud)**

   您需要为 Kaspersky Endpoint Detection and Response Expert (cloud) 购买单独的授权许可。

该功能将在为 Kaspersky Endpoint Detection and Response Expert (cloud) 添加单独密钥后可用。因此，计算机上将添加两个密钥：Kaspersky Endpoint Security 密钥和 Kaspersky Endpoint Detection and Response Expert (cloud) 密钥。

独立 Endpoint Detection and Response Expert (cloud) 功能的授权许可与 Kaspersky Endpoint Security 的相同。

确保授权许可中包含 EDR Expert (cloud) 功能，并且该功能正在应用程序的本地界面中运行。

3 连接到遥测采集服务器和响应服务器

Kaspersky Endpoint Detection and Response Expert (cloud) 需要 Kaspersky Endpoint Security 与两台服务器之间受信任连接：

- *遥测采集服务器* 是 SIEM 解决方案的一部分，用于收集、规范化、关联、分析和存储有关计算机上发生的事件的信息。
- *响应服务器* 是一个用于接收和扫描数据、研究对象行为和发布此类研究结果的服务器。

如何使用 Web Console 将 Kaspersky Endpoint Security 计算机连接到 EDR Expert (cloud)

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”选项卡。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置** → **Endpoint Detection and Response Expert (cloud)**。
5. 使用“**Endpoint Detection and Response Expert (cloud) 已禁用**”拨动开关启用该组件。
6. 如果当前策略是子策略，且父策略禁止更改 EDR Expert (cloud) 集成设置（闭合的“锁”图标），则可以在“**继承**”部分中配置设置继承：
   - **从策略继承连接设置**（默认值）。连接设置将继承自父策略。您将无法编辑这些设置。
   - “**使用自定义连接设置**”。您可以手动配置连接设置。
7. “**响应服务器**”选项卡显示响应服务器的完全限定域名和端口，这些信息会自动检索。如果您的基础架构中的安全策略不允许您直接连接到 EDR Expert (cloud) 服务器，您可以通过 TCP 隧道建立连接：
   a. 选择**使用 TCP 隧道进行响应**复选框。
   b. 指定服务器地址（IPv4、IPv6）和连接到隧道的端口。
8. 如有必要，请在“**发送同步请求到服务器的间隔(分钟)**”字段设置向服务器发送同步请求的频率。在同步过程中，Kaspersky Endpoint Security 接收威胁响应任务并发送任务结果。
9. 转到“**遥测采集服务器**”选项卡。

10. 配置遥测采集服务器连接设置：

    a. 单击**编辑**链接。

    b. 在打开的窗口中，从列表中选择遥测数据收集服务器。KUMA 收集器在 EDR Expert (cloud) 中用作遥测采集服务器。有关更多详细信息，请参阅 Kaspersky Unified Monitoring and Analysis Platform 帮助。

    如果在连接到遥测采集服务器时发生错误，请选择其他服务器。如果您无法连接到遥测数据采集服务器，请联系技术支持。

    c. 如有必要，您可以像为响应服务器配置连接一样，通过 TCP 隧道配置与遥测采集服务器的连接。

11. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

因此，计算机被添加到 Open Single Management Platform (OSMP) 上的受管理设备列表中。通过查看*应用程序组件状态报告*检查组件的操作状态。您也可以利用 Kaspersky Endpoint Security 的本地界面在报告中查看组件的操作状态。**Endpoint Detection and Response Expert (cloud)** 组件将被添加到 Kaspersky Endpoint Security 组件列表。

配置 EDR Expert (cloud) 遥测设置

*遥测*是受保护计算机上发生的事件的列表。Kaspersky Endpoint Security 在同步期间分析遥测数据并将其发送到遥测采集服务器。遥测事件几乎连续不断地到达服务器。当满足以下任一条件时，Kaspersky Endpoint Security 启动与服务器的同步：

- 同步间隔已用完。
- 缓冲区中的事件数超过上限。

因此，默认情况下，应用程序每 30 秒或每当缓冲区包含 1024 个事件时同步一次。您可以在 Kaspersky Endpoint Security 策略中配置同步行为并选择最佳值以匹配您的网络负载（请参阅下面的说明）。

如果 Kaspersky Endpoint Security 与服务器之间没有连接，应用程序将对新事件进行排队。当连接恢复时，Kaspersky Endpoint Security 以正确的顺序将排队的事件发送到服务器。为避免服务器过载，Kaspersky Endpoint Security 可能会跳过一些事件。要启用此功能，您可以优化事件传输设置，例如，设置每小时最大事件数值（请参阅下面的说明）。

要配置遥测设置，请执行下列步骤：

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”选项卡。
2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **内置代理配置** → **Endpoint Detection and Response Expert (cloud)**。
5. 在打开的窗口中，选择“**数据传输设置**”选项卡。
6. 确保“**发送遥测已启用**”复选框被选中。

7. 如有必要，选中“**仅发送带有 IOA 的遥测**”复选框。*攻击指标 (IOA)* 是一条包含系统中可能表明有针对性攻击的可疑行为描述的规则。应用程序将系统中正在进行的行为与这些规则进行比较，并记录表明有针对性攻击的事件。应用程序使用*流式扫描*技术，可以实时跟踪此类事件。

8. 如有必要，请配置服务器同步设置：

   - “**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。默认设置是 30 秒。

   - “**事件包的最大数量**”。当缓冲区充满事件时，应用程序会与服务器同步。默认设置是 1024 个事件。

9. 转到“**请求限制**”选项卡。

10. 如有必要，请使用 **请求限制已启用** 切换开关禁用请求限制。

    该功能有助于优化服务器上的负载。如果启用此功能，应用程序将限制事件传输。如果事件数量超过配置的限制，Kaspersky Endpoint Security 将停止发送事件。默认情况下已启用此选项。

11. 配置用于将事件发送到服务器的优化设置：

    - “**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。默认设置是每小时 3000 个事件。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。默认设置为 15%。

12. 要将此策略应用到计算机，请关闭 🔒 挂锁图标并保存更改。

EDR Expert (cloud) 遥测排除项

要提高性能并优化到遥测采集服务器的数据传输，您可以配置遥测排除项。例如，您可以选择不发送单个应用程序的网络通信数据。

> 使用过多的规则会增加遥测采集服务器的负载并降低计算机性能。我们建议只添加必要的规则。

要在 Web Console 和云控制台中创建遥测排除项：

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **常规设置** → **遥测设置**。

5. 选择**EDR Expert (cloud) 遥测**选项卡。

6. 在“**常规排除项**”块中单击“**添加**”按钮。

   “**添加排除规则**”窗口将打开。

7. 如有必要，可更改规则状态。默认情况下，规则已启用。

8. 输入规则的名称。

9. 选择触发规则时要执行的操作：

- “**不采集**”。被过滤的事件将从发送的遥测数据中排除。
- “**排除 IOA**”。IOA 规则触发器事件将从发送的遥测数据中排除。

10. 如果选中“**排除 IOA**”选项，请指定要添加到排除项中的 IOA 规则：

- “**全部排除**”。当满足指定条件时，应用程序将从遥测数据中排除基于所有 IOA 规则生成的事件。
- “**按 GUID 排除**”。指定 IOA 规则的 GUID。您可以使用“`,`”指定多个 GUID。有关 IOA 规则的详细信息，请参阅 EDR Expert (cloud) 帮助。

11. 指定过滤条件：

    a. 选择用于过滤的字段名称。

    b. 选择一个运算符（见下表），并指定要与事件中的字段值进行比较的值。

条件运算符列表

运算符	描述
<	如果字段值小于条件中指定的值，则该事件将被过滤出来。
≤	如果字段值小于或等于条件中指定的值，则该事件将被过滤出来。
=	如果字段值等于条件中指定的值，则该事件将被过滤出来。
≥	如果字段值大于或等于条件中指定的值，则该事件将被过滤出来。
>	如果字段值大于条件中指定的值，则该事件将被过滤出来。
≠	如果字段值与条件中指定的值不相等，则该事件将被过滤出来。
类似	如果字段值与条件中指定的掩码匹配，则该事件将被过滤出来。输入掩码时，应用程序支持“`*`”字符和“`?`”字符：
不类似	如果字段值与条件中指定的掩码不匹配，则该事件将被过滤出来。输入掩码时，应用程序支持“`*`”字符和“`?`”字符：
之一	如果字段值与条件中指定的列表中的某个值匹配，则该事件被视为已过滤。
没有一个	如果字段值与条件中指定的列表中的任何值都不匹配，则该事件被视为已过滤。
类似其中之一	如果字段值与条件中指定的某个掩码匹配，则该事件将被过滤出来。输入掩码时，Kaspersky Endpoint Security 支持 * 字符和 ? 字符。
不类似其中之一	如果字段值与条件中指定的任何掩码都不匹配，则该事件将被过滤出来。输入掩码时，Kaspersky Endpoint Security 支持 * 字符和 ? 字符。
存在	如果条件中指定的字段出现在事件中，则该事件将被过滤出来。
不存在	如果条件中指定的字段不出现在事件中，则该事件将被过滤出来。
包含	如果条件中指定的值出现在字段值中，则该事件将被过滤出来。
等于	如果字段值等于条件中指定的值，则该事件将被过滤出来。扫描不区分大小写。
按位和	如果字段值与条件中指定的值之间的 Bitwise AND (&) 运算结果为 1，则该事件将被过滤出来。

12. 如有必要，您可以通过添加多个过滤条件和条件组来创建复杂的过滤条件。您还可以向条件组中添加嵌套条件和条件组。您可以使用以下运算符：

    - **且** 表示过滤器会选择符合所有指定条件的事件。
    - **或** 表示过滤器会选择符合指定条件之一的事件。
    - **非**（要使用此运算符，请选择“**在此之前加非**”选项）表示该过滤器选择不符合任何指定条件的事件。

    条件和一级条件组使用 **且** 运算符结合。

13. 要扫描您创建的过滤规则，请单击“**检查规则**”按钮。

    在打开的窗口中，将显示使用创建的规则过滤的事件表。有关更多详细信息，请参阅 EDR Expert (cloud) 帮助。

14. 如有必要，在“**所有事件类型**”下，按事件类型添加遥测排除项。

    a. 点击事件类型名称。

    b. 在打开的窗口中，单击“**手动设置**”按钮。

    c. 如有必要，请使用“**发送事件**”切换开关配置所选事件类型的遥测发送。默认情况下，所有事件类型均启用遥测数据传输。

    d. 在“**排除规则**”块中单击“**添加**”按钮。

    “**添加排除规则**”窗口将打开。

    e. 对添加的每条规则执行步骤 7-13 中描述的操作。

15. 对于某些事件类型，您还可以添加包含规则来扩展收集到的遥测数据：

    a. 在“**包含规则**”块中单击“**添加**”按钮。

    “**添加包含规则**”窗口将打开。

    b. 输入规则的名称。

    c. 在“**条件**”下，输入所显示字段的值。可用字段类型取决于所选事件。

    > 排除规则优先于包含规则。

16. 要将该策略应用于计算机，请确保锁形图标已关闭 (🔒)，然后保存更改。

导出和导入 EDR Expert (cloud) 事件过滤器

可以将排除列表导出到 JSON 文件。然后可以修改文件，例如，添加大量事件 ID。还可以使用导出/导入功能备份事件过滤器或将列表迁移到其他服务器。

> 使用过多的规则会增加遥测采集服务器的负载并降低计算机性能。我们建议只添加必要的规则。

要在 Web Console 中导出和导入事件过滤器：

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”选项卡。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **遥测设置**。
5. 选择**EDR Expert (cloud) 遥测**选项卡。
6. 要导出事件过滤器：
   a. 单击“**导出**”。
   b. 在打开的窗口中，指定您要将事件过滤器导出到的 JSON 文件的名称，然后选择要保存此文件的文件夹。
   c. 保存文件。
      Kaspersky Endpoint Security 会将事件过滤器导出到 JSON 文件。
7. 要导入事件过滤器：
   a. 单击“**导入**”。
   b. 在打开的窗口中，选择要从中导入事件过滤器的 JSON 文件。
   c. 选择您希望如何导入事件过滤规则：添加到现有规则或丢弃现有规则并用新规则替换。
   d. 打开文件。
8. 要将该策略应用到计算机，请确保挂锁已关闭 (🔒)，然后保存更改。
   1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”选项卡。
   2. 单击 Kaspersky Endpoint Security 策略的名称。
      策略属性窗口将打开。
   3. 选择**应用程序设置**选项卡。
   4. 选择 **常规设置** → **遥测设置**。
   5. 选择**EDR Expert (cloud) 遥测**选项卡。
   6. 要导出事件过滤器：
      a. 单击“**导出**”。
      b. 在打开的窗口中，指定您要将事件过滤器导出到的 JSON 文件的名称，然后选择要保存此文件的文件夹。
      c. 保存文件。
         Kaspersky Endpoint Security 会将事件过滤器导出到 JSON 文件。

7. 要导入事件过滤器：

   a. 单击“**导入**”。

   b. 在打开的窗口中，选择要从中导入事件过滤器的 JSON 文件。

   c. 选择您希望如何导入事件过滤规则：添加到现有规则或丢弃现有规则并用新规则替换。

   d. 打开文件。

8. 要将该策略应用到计算机，请确保挂锁已关闭 (🔒)，然后保存更改。

管理隔离

*隔离区*是计算机上的一个特别的本地存储区。用户可以隔离用户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 仅在与 Kaspersky Detection and Response 解决方案集成时使用隔离。在其他情况下，Kaspersky Endpoint Security 将相关文件置于备份中。有关将隔离管理作为解决方案的一部分的详细信息，请参阅 Kaspersky Sandbox 帮助、Kaspersky Endpoint Detection and Response Optimum 帮助、Kaspersky Endpoint Detection and Response Expert 帮助、Kaspersky Anti Targeted Attack Platform 帮助 和 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助。

Kaspersky Endpoint Security 使用系统帐户 (SYSTEM) 隔离文件。

您仅可以在 Kaspersky Security Center 控制台配置隔离设置。您还可以使用 Kaspersky Security Center 控制台管理隔离对象（恢复、删除、添加等）。在本地计算机上，您只能使用命令行恢复对象。

配置最大隔离区大小

默认情况下，隔离区的大小限制为 1024 MB。当隔离区达到最大大小时，Kaspersky Endpoint Security 会停止发送文件并生成“*隔离区存储空间不足*”事件。为了防止隔离区耗尽磁盘空间，您可以设置 Kaspersky Endpoint Security 生成“*隔离区存储空间几乎用完*”事件的阈值。您无法配置隔离文件的保留期限以自动删除它们。

> 如果您的组织中部署了 Kaspersky Anti Targeted Attack Platform（EDR）解决方案，我们建议增加隔离区的大小。进行 YARA 扫描时，应用程序可能会遇到大内存转储。如果内存转储的大小超过隔离区的大小，则 YARA 扫描将以错误结束，并且内存转储不会被隔离。我们建议将隔离区的大小设置为等于计算机上 RAM 的总大小（例如，8 GB），或禁用隔离区的大小限制。

如何在管理控制台 (MMC) 中配置最大隔离区大小

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **常规设置** → **报告和存储**。

4. 在**隔离区**块配置隔离区大小：

- **限制隔离区大小为 N MB**。如果选中该复选框，则最大隔离区大小限制为定义值。默认情况下，最大大小为 1024 MB。当隔离区达到最大大小时，Kaspersky Endpoint Security 将"*隔离区存储空间不足*"事件发送到 Kaspersky Security Center，并在 Windows 事件日志中发布该事件。同时，应用程序停止隔离新对象。您必须手动清空隔离区。

  如果清除该复选框，隔离区大小将受到可用磁盘空间的限制。

- **当隔离区存储达到此限制时通知 N %**。隔离的阈值。例如，您可以将隔离阈值设置为 50%。当隔离区达到阈值时，Kaspersky Endpoint Security 将相应的事件发送到 Kaspersky Security Center，并在 Windows 事件日志中发布该事件。同时，应用程序继续隔离新对象。

  如果清除此复选框，则当达到隔离阈值时，应用程序不会生成事件。

5. 保存更改。

何在 Web Console 和云控制台中配置最大隔离区大小

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **常规设置** → **报告和存储**。

5. 在**隔离**块配置隔离区大小：

- "**限制隔离区大小**"。如果选中该复选框，则隔离区大小限制为指定值。如果清除该复选框，隔离区大小将受到可用磁盘空间的限制。这对于 YARA 扫描来说可能是必要的，因为应用程序可能会保存一个大的内存转储文件。

- "**隔离区最大大小(MB)**"。如果选中该复选框，则最大隔离区大小限制为定义值。默认情况下，最大大小为 1024 MB。当隔离区达到最大大小时，Kaspersky Endpoint Security 将"*隔离区存储空间不足*"事件发送到 Kaspersky Security Center，并在 Windows 事件日志中发布该事件。同时，应用程序停止隔离新对象。您必须手动清空隔离区。

  如果清除该复选框，隔离区大小将受到可用磁盘空间的限制。

- "**当隔离区存储达到此值时通知(%)**"。隔离的阈值。例如，您可以将隔离阈值设置为 50%。当隔离区达到阈值时，Kaspersky Endpoint Security 将相应的事件发送到 Kaspersky Security Center，并在 Windows 事件日志中发布该事件。同时，应用程序继续隔离新对象。

6. 保存更改。

发送有关隔离文件的数据到 Kaspersky Security Center

要在 Web 控制台中对隔离的对象执行操作，您必须启用发送隔离文件数据到管理服务器。例如，您可以从隔离区下载一个文件，以便在 Web 控制台中进行分析。发送隔离文件数据必须启用 Kaspersky Sandbox 和 Kaspersky Endpoint Detection and Response 的所有功能。

如何在管理控制台中启用隔离文件数据传输

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **报告和存储**。
4. 在“**到管理服务器的数据传输**”块中单击“**设置**”按钮。
5. 在打开的窗口中，选中“**隔离文件**”复选框。
6. 保存更改。

如何在 Web 控制台中启用隔离文件数据传输

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **KSC 整合**。
5. 在“**到管理服务器的数据传输**”块中，选中“**关于隔离区文件**”复选框。
6. 保存更改。

因此，您可以在 Kaspersky Security Center 控制台中查看计算机上隔离的文件列表。您可以使用 Web 控制台管理隔离对象（恢复、删除、添加等）。有关使用隔离的详细信息，请参阅 Kaspersky Security Center 帮助。

从隔离区中恢复文件

默认下，Kaspersky Endpoint Security 恢复文件到其原始文件夹。如果目标文件夹已被删除或用户没有该文件夹的访问权限，则应用程序会将该文件放在 `%DataRoot%\QB\Restored` 文件夹中。然后必须手动将文件移动到目标文件夹。

要从隔离区中恢复文件：

1. 在 Web Console 的主窗口中，选择“**操作**” → “**存储库**” → “**隔离**”。
2. 这将打开隔离区中的文件列表；在该列表中，选择要恢复的文件，然后单击“**恢复**”。

   Kaspersky Endpoint Security 将恢复该文件。如果目标文件夹中已有同名文件，则应用程序将取消恢复该文件。对于 EDR Optimum 和 EDR Expert 解决方案，应用程序在恢复后删除文件。对于其他解决方案，应用程序在隔离区中保留文件的副本。

监控 EDR 操作

Kaspersky Endpoint Security for Windows 12.9 引入了 EDR 操作监控中心。*EDR 操作监控中心*是一个控制台，您可以在其中查看所有 Kaspersky Detection and Response 解决方案的威胁响应历史记录。如果您的组织部署了多个 Detection and Response（例如，EDR Optimum 和 MDR），Kaspersky Endpoint Security 将显示所有解决方案的威胁响应历史记录。这使您可以在单独的计算机上分析 Detection and Response 解决方案的性能并优化这些解决方案的设置。

监控中心提供以下信息：

- 有关威胁响应任务（例如"*终止进程*"任务）的信息
- 网络隔离和执行防护规则的变化

如果威胁响应遇到与访问网络共享相关的错误，则会从显示的威胁响应历史记录中省略此类错误。

要导航到 EDR 操作监控中心：

1. 在 Web Console 的主窗口中，选择"**资产管理**" → "**资产(设备)**"。
2. 选择要为其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 Windows**"。
   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** → **响应历史**。

这将打开 EDR 操作监控中心控制台。您可以使用控制台查看威胁响应任务状态、任务持续时间、规则更改和发起者详细信息。

Kaspersky Unified Monitoring and Analysis Platform (KUMA)

Kaspersky Endpoint Security for Windows 支持 Kaspersky Unified Monitoring and Analysis Platform 解决方案。*Kaspersky Unified Monitoring and Analysis Platform (KUMA)* 是针对组织 IT 基础设施的安全信息和事件管理 (SIEM) 解决方案。KUMA 可以在安全威胁造成危害之前检测、分析和减轻它们。

Kaspersky Endpoint Security 安装在公司 IT 基础设施的各个计算机上，并持续监视流程、开放式网络连接和正在修改的文件。有关计算机上事件的信息（遥测数据）被发送到 Kaspersky Unified Monitoring and Analysis Platform (KUMA) 服务器。在其控制台中，KUMA 将事件显示为没有标记的列表，类似于 Windows 事件日志。

Kaspersky Endpoint Security 不提供 KUMA 代理的所有功能。应用程序仅向 KUMA 发送不带标记的事件。要访问所有 KUMA 功能，您需要购买授权许可并按照以下说明部署解决方案：KUMA 管理员指南。

Kaspersky Endpoint Security 与 KUMA 的集成

要使用 KUMA，必须满足以下条件：

- Kaspersky Security Center 版本 14.2 或更高版本。在 Kaspersky Security Center 的早期版本中，无法激活 KUMA 集成功能。
- 应用程序已激活，授权许可涵盖了该功能。
- KUMA 整合集成组件已启用。

设置 KUMA 集成涉及以下步骤：

1. **安装 KUMA 集成组件**

   您可以在安装或升级应用程序时选择 KUMA 集成组件，也可以使用“*更改应用程序组件*”任务。

   > 您必须重新启动计算机才能使用新组件完成应用程序的升级。

2. **KUMA 激活**

   > 除了 Kaspersky Endpoint Security 应用程序授权许可（例如，Kaspersky Endpoint Security for Business Standard）之外，您还需要单独的授权许可才能将 Kaspersky Endpoint Security 与 KUMA 集成（Kaspersky Endpoint Security for Windows KUMA 集成插件）。

   > 如果您以 EDR Agent 模式安装应用程序，您需要用于将 Kaspersky Endpoint Security 与 KUMA 集成的授权许可以及 Kaspersky Anti Targeted Attack Platform (KATA) 授权许可或 Kaspersky Managed Detection and Response (MDR) 授权许可。您不能仅为 KUMA 部署 EDR Agent。

添加单独的 KUMA 键后该功能可用。因此，计算机上将有另一个活动密钥用于 Kaspersky Endpoint Security 与 KUMA 的集成。

独立 KUMA 功能的授权与 Kaspersky Endpoint Security 的授权相同。

确保 KUMA 功能包含在授权许可中，并在应用程序的本地界面中工作。

3 连接到 KUMA

要将安装有 Kaspersky Endpoint Security 应用程序的计算机连接到 KUMA 解决方案：

1. 在 Kaspersky Endpoint Security 策略中，添加 KUMA 服务器地址并指定连接的网络设置。
2. 在 KUMA 控制台中，添加一个具有 tcp 或 udp 类型连接器的收集器，并指定连接的基本网络设置。有关管理收集器的详细信息，请参阅 Kaspersky Unified Monitoring and Analysis Platform 帮助。

您可以在 Kaspersky Endpoint Security 和 KUMA 服务器之间建立信任连接。要配置可信连接，您必须使用 TLS 证书。您可以在 KUMA Core 服务器上获取 TLS 证书（请参阅 Kaspersky Unified Monitoring and Analysis Platform 帮助中的 tcp 类型连接器的设置）。然后您必须将 TLS 证书添加到 Kaspersky Endpoint Security（参见下面的说明）。

为了使连接更安全，您可以额外启用 KUMA 上的计算机验证（双向身份验证）。要启用此验证，您必须在 KUMA 和 Kaspersky Endpoint Security 设置中打开双向身份验证。要使用双向身份验证，您还需要一个加密容器。*加密容器*是带有证书和私钥的 PFX 存档。您必须在外部证书颁发机构处生成具有 PKCS#12 容器格式的私钥的证书。然后，您必须在 KUMA 控制台和 Kaspersky Endpoint Security 中添加 PFX 存档（请参阅 Kaspersky Unified Monitoring and Analysis Platform 帮助中的 tcp 类型连接器的设置）。

如何使用管理控制台 (MMC) 将 Kaspersky Endpoint Security 计算机连接到 KUMA

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择“**KUMA 整合**”。
4. 选择**KUMA 整合**复选框。
5. 在“**整合设置**”块中，选中“**启用向 KUMA 服务器传输 Windows 事件**”复选框。
6. 如有必要，在“**KUMA 服务器连接设置**”块选择“**使用 TLS 加密**”复选框。
7. 配置受信任连接：
   a. 单击“**KUMA 服务器连接设置**”。
   b. 配置服务器连接：
      - “**超时(秒)**”。最大 KUMA 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 KUMA 服务器。
      - “**服务器 TLS 证书**”。用于与 KUMA 服务器建立受信任连接的 TLS 证书。您可以在 Kaspersky Unified Monitoring and Analysis Platform 控制台中获取 TLS 证书（请参阅 Kaspersky Unified Monitoring and Analysis Platform 中的说明）。

        要建立受信任连接，在 KUMA 控制台的 TCP 连接器设置中，必须选择“**With verification**”TLS 模式（请参阅 Kaspersky Unified Monitoring and Analysis Platform 帮助中的 tcp 类型连接器设置）。

- “**使用双向认证**”。在 Kaspersky Endpoint Security 和 KUMA 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，在 KUMA 控制台的 TCP 连接器设置中，必须选择“**Custom PFX**”TLS 模式（请参阅 Kaspersky Unified Monitoring and Analysis Platform 帮助 中的 tcp 类型连接器设置）。然后您必须获取一个加密容器并设置一个密码来保护该加密容器。*加密容器*是带有证书和私钥的 PFX 存档。配置 KUMA 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。

c. 单击“**确定**”。

8. 添加 KUMA 服务器：

   a. 单击“**添加**”。

   这将打开一个表单，您可以在其中添加 KUMA 服务器。

   b. 选择连接到 KUMA 服务器的协议：**HTTP / HTTPS**、**TCP**、**UDP**。

   如果您选择 **HTTP/HTTPS** 协议，默认情况下，应用程序使用 HTTPS 协议连接到 KUMA 服务器。要使用 HTTP，您需要在服务器地址中手动指定此协议（例如，`http://server.com`）。

   c. 请输入服务器地址（IPv4、IPv6）和连接到服务器的端口。

   d. 单击“**确定**”。

   Kaspersky Endpoint Security 连接到列表中第一个 KUMA 服务器。如果连接失败，Kaspersky Endpoint Security 将连接到列表中的第二个 KUMA 服务器，依此类推。

9. 如有必要，在“**数据传输设置**”块配置“**最大事件传输延迟(秒)**”设置。当指定的时间用完时，Kaspersky Endpoint Security 将尝试连接到同一台服务器，或者如果有多个服务器，则连接到列表中的下一个服务器。默认设置是 30 秒。

10. 保存更改。

如何使用 Web Console 将 Kaspersky Endpoint Security 计算机连接到 KUMA

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

2. 单击 Kaspersky Endpoint Security 策略的名称。

   策略属性窗口将打开。

3. 选择**应用程序设置**选项卡。

4. 选择 **内置代理配置** → **KUMA 整合**。

5. 开启 **KUMA 整合已启用**切换开关。

6. 如有必要，在“**服务器连接设置**”块打开“**使用 TLS 加密**”切换开关。

7. 配置受信任连接：

   a. 单击“**连接设置**”。

   b. 配置服务器连接：

   - “**超时(秒)**”。最大 KUMA 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 KUMA 服务器。

   - “**服务器 TLS 证书**”。用于与 KUMA 服务器建立受信任连接的 TLS 证书。您可以在 Kaspersky Unified Monitoring and Analysis Platform 控制台中获取 TLS 证书（请参阅 Kaspersky Unified Monitoring and Analysis Platform 中的说明）。

     要建立受信任连接，在 KUMA 控制台的 TCP 连接器设置中，必须选择“**With verification**”TLS 模式（请参阅 Kaspersky Unified Monitoring and Analysis Platform 帮助中的 tcp 类型连接器设置）。

   - “**使用双向身份验证**”。在 Kaspersky Endpoint Security 和 KUMA 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，在 KUMA 控制台的 TCP 连接器设置中，必须选择“**Custom PFX**” TLS 模式（请参阅 Kaspersky Unified Monitoring and Analysis Platform 帮助中的 tcp 类型连接器设置）。然后您必须获取一个加密容器并设置一个密码来保护该加密容器。*加密容器*是带有证书和私钥的 PFX 存档。配置 KUMA 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。

   c. 单击“**确定**”。

8. 添加 KUMA 服务器：

   a. 单击“**添加**”。

      这将打开一个表单，您可以在其中添加 KUMA 服务器。

   b. 选择连接到 KUMA 服务器的协议：**HTTP/HTTPS**、**TCP**、**UDP**。

      如果您选择 **HTTP/HTTPS** 协议，默认情况下，应用程序使用 HTTPS 连接到 KUMA 服务器。要使用 HTTP，您需要在服务器地址中手动指定此协议（例如，`http://server.com`）。

   c. 请输入服务器地址（IPv4、IPv6）和连接到服务器的端口。

   d. 单击“**确定**”。

   Kaspersky Endpoint Security 连接到列表中第一个 KUMA 服务器。如果连接失败，Kaspersky Endpoint Security 将连接到列表中的第二个 KUMA 服务器，依此类推。

9. 如有必要，在“**服务器连接设置**”块配置“**发送事件时的最大延时（秒）**”设置。当指定的时间用完时，Kaspersky Endpoint Security 将尝试连接到同一台服务器，或者如果有多个服务器，则连接到列表中的下一个服务器。默认设置是 30 秒。

10. 保存更改。

您可以在 KUMA 控制台中验证 KUMA 集成是否配置正确（有关详细信息，请参阅“Kaspersky Unified Monitoring and Analysis Platform 帮助”）。通过查看 Kaspersky Security Center 控制台中的“*应用程序组件状态报告*”来检查组件的运行状态。您也可以利用 Kaspersky Endpoint Security 的本地界面在报告中查看组件的操作状态。**KUMA 整合** 组件将被添加到 Kaspersky Endpoint Security 组件列表。

4 **启用向 KUMA 服务器发送遥测数据**

默认情况下，向 KUMA 服务器发送事件是禁用的。为确保 KUMA 正常工作，您必须启用遥测发送功能。您可以从标准日志中选择事件源：*Application*、*Security*或*System*。

如何在管理控制台(MMC)中启用向 KUMA 服务器发送遥测数据

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**策略**”。
3. 选择必要的策略并双击以打开策略属性。
4. 在策略窗口中，选择 **常规设置** → **排除项和对象类型**。
5. 在“**遥测设置** → **KUMA 遥测**”块中单击“**设置**”按钮。
6. 选择要用作事件源的事件日志：*Application*、*Security* 或者 *System*。
   除了标准日志外，您还可以指定一个第三方应用程序日志。
7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 中启用向 KUMA 服务器发送遥测数据

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”选项卡。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **遥测设置**。
5. 选择**KUMA 遥测**选项卡。
6. 选择要用作事件源的事件日志：*Application*、*Security* 或者 *System*。
   除了标准日志外，您还可以指定一个第三方应用程序日志。
7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

过滤要发送到 KUMA 的事件

默认情况下，向 KUMA 服务器发送事件是禁用的。为确保 KUMA 正常工作，您必须启用遥测发送功能。您可以从标准日志中选择事件源：*Application*、*Security*或*System*。为了提高性能并优化向 KUMA 服务器的数据传输，您可以手动从遥测中添加或排除单个事件。例如，您可以排除 Sysmon 事件。

如何在管理控制台 (MMC) 中创建要发送到 KUMA 的事件列表

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**策略**”。
3. 选择必要的策略并双击以打开策略属性。

4. 在策略窗口中，选择 **常规设置** → **排除项和对象类型**。

5. 在“**遥测设置** → **KUMA 遥测**”块中单击“**设置**”按钮。

6. 在显示的窗口中，配置要发送给 KUMA 的事件过滤器。
   您可以为标准*Application*、*Security*、*System* 日志配置事件过滤或手动添加另一个日志：

   a. 打开日志属性或单击“**添加**”按钮并输入日志名称。

   b. 选择事件发送模式：

      - “**发送所有事件**”。在此模式下，应用程序会发送 Windows 日志中的所有事件（添加到排除规则的事件除外）。

      - “**仅发送选定的事件**”。在此模式下，应用程序仅发送包含规则中添加的事件。

   c. 为相关事件发送模式创建排除规则或包含规则列表。
      要添加规则，您需要指定 Windows 事件日志中事件的 ID。您可以在一个规则中列出多个事件 ID。要指定多个事件 ID，请使用逗号（`,`）。

   d. 如有必要，请使用日志名称旁边的复选框启用事件日志记录。

7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 中创建要发送到 KUMA 的事件列表

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

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

3. 选择**应用程序设置**选项卡。

4. 选择 **常规设置** → **遥测设置**。

5. 选择**KUMA 遥测**选项卡。

6. 在显示的窗口中，配置要发送给 KUMA 的事件过滤器。
   您可以为标准*Application*、*Security*、*System* 日志配置事件过滤或手动添加另一个日志：

   a. 打开日志属性或单击“**添加**”按钮并输入日志名称。

   b. 选择事件发送模式：

      - “**发送所有事件**”。在此模式下，应用程序会发送 Windows 日志中的所有事件（添加到排除规则的事件除外）。

      - “**仅发送选定的事件**”。在此模式下，应用程序仅发送包含规则中添加的事件。

c. 为相关事件发送模式创建排除规则或包含规则列表。

要添加规则，您需要指定 Windows 事件日志中事件的 ID。您可以在一个规则中列出多个事件 ID。要指定多个事件 ID，请使用逗号 (`,`) 。

d. 如有必要，请使用日志名称旁边的切换开关启用事件日志记录。

7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

导出和导入 KUMA 事件过滤器

可以将排除列表导出到 JSON 文件。然后可以修改文件，例如，添加大量事件 ID。还可以使用导出/导入功能备份事件过滤器或将列表迁移到其他服务器。

> 使用过多的规则会增加 KUMA 服务器的负载并降低计算机性能。我们建议只添加必要的规则。

如何在管理控制台 (MMC) 中导出和导入事件过滤器

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择“**策略**”。
3. 选择必要的策略并双击以打开策略属性。
4. 在策略窗口中，选择 **常规设置** → **排除项和对象类型**。
5. 在“**遥测设置** → **KUMA 遥测**”块中单击“**设置**”按钮。
6. 要导出事件过滤器：

   a. 选择您想要导出的带有过滤器的事件日志。

   b. 单击“ → **导出**”按钮。

   c. 在打开的窗口中，指定您要将事件过滤器导出到的 JSON 文件的名称，然后选择要保存此文件的文件夹。

   d. 保存文件。

   Kaspersky Endpoint Security 会将事件过滤器导出到 JSON 文件。

7. 要导入事件过滤器：

   a. 单击“ → **导入**”按钮。

   b. 在打开的窗口中，选择要从中导入事件过滤器的 JSON 文件。

   c. 打开文件。

   如果计算机上已经存在事件过滤规则，Kaspersky Endpoint Security 会在导入时替换这些规则。

8. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在 Web Console 中导出和导入事件过滤器

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”选项卡。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **遥测设置**。
5. 选择**KUMA 遥测**选项卡。
6. 要导出事件过滤器：
   a. 选择您想要导出的带有过滤器的事件日志。
   b. 单击“ → **导出**”按钮。
   c. 在打开的窗口中，指定您要将事件过滤器导出到的 JSON 文件的名称，然后选择要保存此文件的文件夹。
   d. 保存文件。
      Kaspersky Endpoint Security 会将事件过滤器导出到 JSON 文件。
7. 要导入事件过滤器：
   a. 单击“ → **导入**”按钮。
   b. 在打开的窗口中，选择要从中导入事件过滤器的 JSON 文件。
   c. 打开文件。
      如果计算机上已经存在事件过滤规则，Kaspersky Endpoint Security 会在导入时替换这些规则。
8. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

您还可以在命令行上导出或导入事件过滤器。

KSWS 到 KES 的迁移指南

从 11.8.0 开始，Kaspersky Endpoint Security for Windows 支持 Kaspersky Security for Windows Server（KSWS）解决方案的基本功能。*Kaspersky Security for Windows Server* 可保护运行 Microsoft Windows 操作系统的服务器和网络附加存储，防止服务器和网络附加存储在交换文件时受到病毒和其他计算机安全威胁。对于该解决方案如何工作的详情，请参考 Kaspersky Security for Windows Server 帮助。从 Kaspersky Endpoint Security 11.8.0 开始，您可以从 Kaspersky Security for Windows Server 迁移到 Kaspersky Endpoint Security for Windows，并使用相同解决方案来保护工作站和服务器。

软件要求

在开始从 KSWS 迁移到 KES 之前，请确保您的服务器满足 Kaspersky Endpoint Security for Windows 的硬件和软件要求。KES 和 KSWS 支持的操作系统版本列表不同。例如，KES 不支持运行 Windows Server 2003 的服务器。

从 KSWS 迁移到 KES 的最低软件要求：

- Kaspersky Endpoint Security for Windows 12.0。
- Kaspersky Security 11.0.1 for Windows Server。

  如果您安装了早期版本的 Kaspersky Security for Windows Server，我们建议将应用程序升级到最新版本。策略和任务转换向导不支持早期版本的 Kaspersky Security for Windows Server。
- Kaspersky Security Center 14.2。

  如果您安装了早期版本的 Kaspersky Security Center，请将其更新到 14.2 或更高版本。在此版本的 Kaspersky Security Center 中，策略和任务批量转换向导可让您将策略迁移到配置文件中，而不是迁移到策略中。在此版本的 Kaspersky Security Center 中，策略和任务批量转换向导还允许您迁移范围更广的策略设置。
- Kaspersky Endpoint Agent 3.10。

  如果您安装了早期版本的 Kaspersky Endpoint Agent，我们建议将应用程序升级到最新版本。从 Kaspersky Endpoint Agent 3.10 开始，Kaspersky Endpoint Security 支持将 [KSWS+KEA] 配置迁移到 [KES+内置代理]。

迁移建议

从 KSWS 迁移到 KES 时，请遵循以下建议：

- 提前规划好 KSWS 到 KES 的迁移时间。选择服务器在最轻负载下运行的时间，例如周末。
- 迁移后，逐步开启应用程序组件。即，例如，首先单独启用文件威胁防护组件，然后启用其他防护组件，再启用控制组件，依此类推。在每一步，您都必须确保应用程序正常工作，并监控服务器的性能。KES 的体系结构与 KSWS 不同，因此操作系统的行为也可能不同。
- 逐步进行迁移。首先迁移单台服务器，然后迁移多台服务器，然后在组织的所有服务器上进行迁移。

- 分别迁移不同类型的服务器。也就是说，例如，首先迁移数据库服务器，然后迁移邮件服务器，等等。
- 在高负载服务器上迁移涉及一些特殊注意事项。

迁移步骤

从 KSWS 到 KES 的迁移是半自动执行的。这是必要的，因为应用程序的体系结构不同。要迁移策略设置，您必须运行策略和任务批量转换向导（迁移向导）。迁移策略设置后，您必须手动配置迁移向导无法自动迁移的设置（例如，密码保护设置）。迁移后，还建议检查迁移向导是否正确迁移了所有设置。

按以下顺序从 KSWS 迁移到 KES：

1. **迁移 KSWS 任务和策略**

   迁移策略和任务后，您必须执行额外的配置步骤。我们还建议确保 Kaspersky Endpoint Security 在从 KSWS 迁移后提供必要的安全级别。

   > Kaspersky Security for Windows Server 的策略和任务批量转换向导仅在管理控制台 (MMC) 中可用。无法在 Web 控制台和 Kaspersky Security Center 云控制台中迁移策略和任务设置。

2. **安装 Kaspersky Endpoint Security**

   您可以通过以下方式安装 Kaspersky Endpoint Security：

   - 卸载 KSWS 后安装 KES（推荐）。

     > kavremover 实用程序不支持管理 KSWS。

   - 在 KSWS 之上安装 KES。

3. **使用 KSWS 密钥激活 KES**

4. **确认应用程序在迁移后处于工作状态**

   从 KSWS 迁移到 KES 后，确保应用程序正常运行。在控制台查看服务器状态（应该是*正常*）。确保应用程序没有报告任何错误，还要检查最后一次连接到管理服务器的时间、最后一次更新数据库的时间和服务器保护状态。

   > 特别注意排除列表、受信任应用程序、受信任网址、应用程序控制规则的迁移。

KSWS 和 KES 组件的对应关系

从 KSWS 迁移到 KES 时，仅当应用程序在本地安装时才迁移组件集。

Kaspersky Security for Windows Server 与 Kaspersky Endpoint Security for Windows 组件的对应关系

Kaspersky Security for Windows Server 组件	Kaspersky Endpoint Security for Windows 组件
基本功能	应用程序核心
日志审查	日志审查
设备控制	设备控制
防火墙管理	*（不支持）* KSWS 防火墙功能由系统级防火墙执行。在 KES 中，一个单独的组件负责防火墙功能。迁移后，您可以配置 Kaspersky Endpoint Security 防火墙。
文件完整性监控	系统完整性监控
漏洞利用防御	漏洞利用防御
系统托盘图标	*（不支持）* 您可以在应用程序界面设置中配置用户交互。
与 Kaspersky Security Center 集成	网络代理连接器
Endpoint Agent	*（不支持）* 在 Kaspersky Endpoint Security 11.9.0 中，Kaspersky Endpoint Agent 分发包不再是 Kaspersky Endpoint Security 分发包的一部分。您必须另外下载 Kaspersky Endpoint Agent 分发包。
网络威胁防护	网络威胁防护
反加密	行为检测
用于 NetApp 的反加密勒索	*（不支持）*
流量安全	Web 威胁防护 邮件威胁防护 Web 控制
按需扫描	应用程序核心
ICAP 网络存储保护	*（不支持）* Kaspersky Endpoint Security 不支持网络附加存储保护组件。如果您需要这些组件，您可以继续使用 Kaspersky Security for Windows Server。
RPC 网络存储保护	*（不支持）* Kaspersky Endpoint Security 不支持网络附加存储保护组件。如果您需要这些组件，您可以继续使用 Kaspersky Security for Windows Server。
实时文件保护	文件威胁防护
脚本监控	*（不支持）* 脚本监控由其他组件处理，例如，AMSI 保护。
KSN 使用	卡巴斯基安全网络
应用程序启动控制	应用程序控制
性能计数器	*（不支持）*

KSWS 和 KES 设置的对应关系

迁移策略和任务时，KES 根据 KSWS 设置进行配置。KSWS 没有的应用程序组件的设置被设置为默认值。

应用程序设置

可扩展性、界面和扫描设置

Kaspersky Endpoint Security for Windows 不支持应用程序设置。

应用程序设置

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
扩展性设置	*（不迁移）* Kaspersky Endpoint Security 管理所有工作进程。
显示系统托盘图标	*（不迁移）* 在客户端计算机上，Kaspersky Endpoint Security 的主窗口和 Windows 通知区域中的图标均默认可用。在该图标的上下文菜单中，用户可以使用 Kaspersky Endpoint Security 执行操作。Kaspersky Endpoint Security 还会在应用程序图标上方显示通知。您可以在应用程序界面设置中配置用户交互。
扫描后还原文件属性	*（不迁移）* Kaspersky Endpoint Security 在扫描文件后自动恢复文件属性。
限制线程扫描的 CPU 使用率	*（不迁移）* Kaspersky Endpoint Security 不限制扫描时的 CPU 使用。您可以将任务配置为在计算机以最小负载运行时运行。
用于存储在扫描期间创建的临时文件的文件夹	*（不迁移）* Kaspersky Endpoint Security 将临时文件放在 `C:\Windows\Temp` 文件夹中。
HSM 系统设置	*（不迁移）* Kaspersky Endpoint Security 不支持 HSM 系统。

安全性和可靠性

KSWS 安全设置被迁移到“**常规设置**”区域、“**应用程序设置**”和“**界面**”子区域。

应用程序安全设置

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
保护应用程序进程免受外部威胁	**启用自我保护**（**应用程序设置**子区域）
应用密码保护	*（不迁移）* Kaspersky Endpoint Security 具有内置密码保护功能（请参阅**界面**子区域）。
执行任务恢复	*（不迁移）* Kaspersky Endpoint Security 仅自动恢复“*恶意软件扫描*”任务。Kaspersky Endpoint Security 按计划运行其他任务。
不启动已计划扫描任务	**使用电池供电时推迟计划任务**（**应用程序设置**子区域）
停止当前扫描任务	*（不迁移）* 当计算机由 UPS 供电时，Kaspersky Endpoint Security 不会停止正在运行的扫描任务。

连接设置

管理服务器交互设置被迁移到“**常规设置**”区域、“**网络设置**”和“**应用程序设置**”子区域。

管理服务器交互设置

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
代理服务器设置	**代理服务器设置**（**网络设置**子区域）
对于本地地址不使用代理服务器	**对本地地址不使用代理服务器**（**网络设置**子区域）
代理服务器身份验证设置	**使用代理服务器身份验证**（**网络设置**子区域） 代理服务器身份验证密码未迁移。迁移策略后，必须手动输入密码。
激活应用程序时使用 Kaspersky Security Center 作为代理服务器	**将 Kaspersky Security Center 用作代理服务器以进行激活**（**应用程序设置**子区域）

运行本地系统任务

Kaspersky Endpoint Security 忽略运行 Kaspersky Security for Windows Server 的本地系统任务的设置。您可以在“**本地任务**”、“**任务管理**”下配置本地 KES 任务的使用。您还可以在这些任务的属性中配置运行“*恶意软件扫描*”和“*数据库和应用程序模块更新*”任务的计划。

补充

信任区域

KSWS 受信任区域设置被迁移到“**常规设置**”区域，“**排除项**”子区域。

受信任区域设置

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
要扫描的对象（排除）	**扫描排除项** (扫描排除项) KSWS 和 KES 用于选择对象的方法不同。当迁移时，KES 支持定义为单个文件或文件/文件夹路径的排除项。如果 KSWS 将排除项配置为预定义区域或脚本 URL，则不会迁移此类排除项。迁移后，您必须手动添加此类排除项。必须在“*恶意软件扫描*”任务设置中配置作为预定义区域的排除项。必须将作为脚本网址的排除项添加到“Web 威胁保护”的受信任网址中。
同时应用于子文件夹（排除）	**包括子文件夹** (扫描排除项)
检测对象（排除）	**检测对象类型** (扫描排除项)
排除使用范围（排除）	**保护组件** (扫描排除项) 如果在 KSWS 中至少选择了一个组件，KES 会将排除应用于所有应用程序组件。
备注（排除）	**注释** (扫描排除项)
受信任进程（受信任进程）	**受信任应用程序** 受信任进程/应用程序分类方法在 KSWS 和 KES 中有所不同。迁移时，KES 支持配置为可执行文件或掩码路径的受信任应用程序。如果 KSWS 具有配置为文件哈希的受信任进程，则不会迁移此类受信任进程。迁移后，您必须手动添加此类受信任进程。
不检查文件备份操作（受信任进程）	**不监控应用程序活动** (受信任应用程序)

可移动驱动器扫描

可移动驱动器扫描设置被迁移到“**本地任务**”区域，“**可移动驱动器扫描**”子区域。

“可移动驱动器扫描”设置

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
扫描通过 USB 连接的可移动驱动器	**连接可移动驱动器时的操作**
扫描可移动驱动器，如果其存储的数据量未超过(MB)	**可移动驱动器最大大小**
扫描时使用的安全级别： • **最佳保护** • **推荐** • **最优性能**	**连接可移动驱动器时的操作**： • **最大保护** • **建议** KSWS 安全级别对应于 KES 扫描模式，如下所示： • 最佳保护 – 最大保护 • 推荐 – 建议 • 最优性能 – 建议

应用程序管理的用户权限

Kaspersky Endpoint Security 不支持为应用程序管理和应用程序服务管理分配用户访问权限。您可以为用户和用户组配置访问设置，以便在 Kaspersky Security Center 管理应用程序。

Kaspersky Security Service 管理的用户访问权限

Kaspersky Endpoint Security 不支持为应用程序管理和应用程序服务管理分配用户访问权限。您可以为用户和用户组配置访问设置，以便在 Kaspersky Security Center 管理应用程序。

存储

KSWS 存储设置被迁移到“**常规设置**”区域，“**报告和存储**”子区域，以及“**基本威胁防护**”区域，“**网络威胁防护**”子区域。

存储设置

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
备份文件夹	*（不迁移）* Kaspersky Endpoint Security 保存文件的备份副本到 `C:\ProgramData\Kaspersky Lab\KES.14.1\QB` 文件夹。
最大备份容量(MB)	**限制备份区大小为 N MB**（**常规设置** → **报告和存储**区域）
可用空间阈值(MB)	*（不迁移）* 当达到 50% 阈值时，Kaspersky Endpoint Security 记录“*隔离区存储空间几乎用完*”事件。
用于还原对象的目标文件夹	*（不迁移）* Kaspersky Endpoint Security 恢复文件到其原始文件夹。
隔离区文件夹	*（不迁移）* Kaspersky Endpoint Security 保存文件的备份副本到 `C:\ProgramData\Kaspersky Lab\KES.14.1\QB` 文件夹。
隔离区最大容量(MB)	*（不迁移）* Kaspersky Endpoint Security 使用备份区存储疑似感染的对象。在迁移过程中，Kaspersky Endpoint Security 忽略隔离设置。
可用空间阈值(MB)	*（不迁移）* Kaspersky Endpoint Security 使用备份区存储疑似感染的对象。在迁移过程中，Kaspersky Endpoint Security 忽略隔离设置。
用于还原对象的目标文件夹	*（不迁移）* Kaspersky Endpoint Security 恢复文件到其原始文件夹。
在该时间后自动解除阻止 N	**阻止攻击设备 N 分钟**（**基本威胁防护** → **网络威胁防护**区域）

实时服务器保护

实时文件保护

KSWS 实时文件保护设置被迁移到“**基本威胁防护**”区域，“**文件威胁防护**”子区域。

实时文件保护设置

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
对象保护模式: • **智能模式** • **运行时** • **访问时** • **访问和修改时**	**扫描模式**: • **智能模式** • **执行时** • **在访问时** • **在访问和修改时**

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
对启动进程的更深度分析	*（不迁移）* Kaspersky Endpoint Security 仅支持一种分析模式，最优模式。
启发式分析： • **轻度** • **中度** • **深度**	**启发式分析**： • **轻度扫描** • **中度扫描** • **深度扫描**
应用信任区域	*（不迁移）* Kaspersky Endpoint Security 应用受信任区域到所有组件。您可以在受信任区域设置中配置排除项。
在保护中使用 KSN	*（不迁移）* Kaspersky Endpoint Security 对所有应用程序组件使用 KSN。
阻止对显示恶意活动的主机的网络共享资源的访问	*（不迁移）* 默认情况下，Kaspersky Endpoint Security 会阻止显示恶意活动的主机访问网络共享资源。
检测到活动感染时启动关键区域扫描	*（不迁移）* 当检测到活动感染时，Kaspersky Endpoint Security 不会启动关键区域扫描任务。
使用 Kaspersky Sandbox 进行保护	*（不迁移）* 默认情况下，Kaspersky Endpoint Security 将要扫描的对象发送到 Kaspersky Sandbox。
保护范围	**保护范围**
计划设置	*（不迁移）* Kaspersky Endpoint Security 使用其自己的计划暂停文件威胁防护。

KSN 使用

KSWS 的卡巴斯基安全网络设置被迁移到“**高级威胁防护**”区域，“**卡巴斯基安全网络**”子区域。

卡巴斯基安全网络设置

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
我确认我已完全阅读、理解并接受参加卡巴斯基安全网络的条款	**卡巴斯基安全网络声明** 安装应用程序、创建新策略或启用卡巴斯基安全网络使用时，Kaspersky Endpoint Security 请求同意卡巴斯基安全网络声明。
发送关于已扫描文件的数据	*（不迁移）* 如果启用 KSN，Kaspersky Endpoint Security 将自动发送有关扫描文件的数据。
发送关于请求的 URL 的数据	*（不迁移）* 如果启用 KSN，Kaspersky Endpoint Security 将自动发送有关请求的 URL 的数据。
发送卡巴斯基安全网络统计信息	**启用扩展 KSN 模式**
接受 Kaspersky Managed Protection 声明的条款	*（不迁移）* Kaspersky Endpoint Security 不包括 KMP 服务。
对 KSN 不信任的对象执行的操作	*（不迁移）* 您可以在保护组件设置和扫描任务设置中配置威胁检测操作。
如果文件大小超过 N MB，则如果文件大小超过以下大小，则在发送到 KSN 之前不计算校验和	*（不迁移）* 您可以在“保护组件设置”和“扫描任务设置”中配置大文件扫描限制。
使用 Kaspersky Security Center 作为 KSN 代理	**使用管理服务器作为 KSN 代理服务器**
计划设置	*（不迁移）* 无法为组件配置单独的计划。当 Kaspersky Endpoint Security 运行时，该组件始终处于打开状态。

流量安全

KSWS 流量安全设置被迁移到“**基本威胁防护**”区域，“**Web 威胁防护**”和“**邮件威胁防护**”子区域，“**安全控制**”区域，“**Web 控制**”子区域，“**常规设置**”区域，“**网络设置**”子区域。

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
应用基于 URL 的规则	**Web 控制**（**Web 控制**子区域） 基于 URL 的规则被迁移到 Kaspersky Endpoint Security 中的单独规则。
应用基于证书的规则	*（不迁移）* Kaspersky Endpoint Security 不支持基于证书的规则。
应用 Web 流量类别控制规则	**Web 控制**（**Web 控制**子区域） Web 流量类别控制的阻止规则被迁移到 Kaspersky Endpoint Security 中的单独阻止规则。Kaspersky Endpoint Security 忽略类别控制的允许规则。 KSWS 和 KES 类别的对应关系如下所示。
如果无法分类网页，则允许访问	*（不迁移）* 如果网页无法分类，Kaspersky Endpoint Security 允许访问。
允许访问可用来破坏受保护设备的合法 Web 资源	*（不迁移）* Kaspersky Endpoint Security 允许访问可用于损坏受保护设备的合法 Web 资源。
允许访问合法广告	*（不迁移）* 您可以使用"Web 控制"设置中的"*广告栏*"Web 资源类别管理对合法广告的访问。
运行模式： • **驱动程序拦截器** • **重定向器** • **外部代理**	*（不迁移）* Kaspersky Endpoint Security 仅支持"驱动程序侦听器"模式。
ICAP 服务连接设置	*（不迁移）* Kaspersky Endpoint Security 不支持 ICAP 网络存储保护。
检查通过 HTTPS 协议建立的安全连接	**扫描加密连接 / 始终扫描加密连接** 模式（**网络设置** 子区域）
使用 TLS 协议版本	*（不迁移）* Kaspersky Endpoint Security 将扫描通过以下协议传输的加密网络流量： • SSL 3.0。 • TLS 1.0、TLS 1.1、TLS 1.2、TLS 1.3。 您还可以在加密连接扫描设置中阻止 SSL 2.0 连接。
不信任具有无效证书的 Web 服务器	**地址**（**网络设置**子区域）
拦截端口（拦截区域）	**受监控端口**（**网络设置**子区域） 在迁移过程中，KES 清空"**监控卡巴斯基推荐的列表中的应用程序的所有端口**"和"**监控指定应用程序的所有端口**"复选框。
排除端口（拦截区域）	*（不迁移）*
排除 IP 地址（拦截区域）	**配置受信任地址**（**网络设置**子区域）
排除进程（拦截区域）	**配置受信任应用程序**（**网络设置**子区域） 迁移期间，KES 为受信任的应用程序配置以下设置： • 选择"**不扫描网络流量**"复选框。KES 不会扫描任何远程 IP 地址和端口的网络流量。 • 清除受信任应用程序设置中的其他复选框。
安全端口	*（不迁移）*
使用恶意 URL 数据库扫描 Web 链接	**检查网址是否在恶意网址数据库中**（**Web 威胁防护**子区域）
使用反钓鱼数据库扫描网页	**检查网址是否在钓鱼网址数据库中**（**Web 威胁防护**子区域）
在保护中使用 KSN	*（不迁移）* Kaspersky Endpoint Security 对所有应用程序组件使用 KSN。
使用信任区域	*（不迁移）* Kaspersky Endpoint Security 应用受信任区域到所有组件。您可以在受信任区域设置中配置排除项。
使用启发式分析	**使用启发式分析** (**Web 威胁防护** and **邮件威胁防护** 子区域)
安全级别	*（不迁移）* Kaspersky Endpoint Security 对 Web 威胁防护和邮件威胁防护组件有其自己的安全级别。默认下，Kaspersky Endpoint Security 设置推荐的安全级别。

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
启用邮件威胁防护	**邮件威胁防护**（**邮件威胁防护**子区域） **连接 Microsoft Outlook 扩展程序** **仅传入的邮件** (保护范围) **接收时扫描** (电子邮件保护)
计划设置	*（不迁移）* 无法为组件配置单独的计划。当 Kaspersky Endpoint Security 运行时，该组件始终处于打开状态。

漏洞利用防御

KSWS 漏洞利用防御设置被迁移到“**高级威胁防护**”区域，“**漏洞利用防御**”子区域。

漏洞利用防御设置

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
防止易受感染的进程被漏洞利用： • **发现漏洞利用时终止** • **仅通知**	**检测到漏洞时**： • **阻止** • **通知**
通过“终端服务”通知被利用的进程	*（不迁移）* Kaspersky Endpoint Security 不支持终端服务。
即使 Kaspersky Security 服务已禁用，也会防止易受感染的进程被漏洞利用	*（不迁移）* Kaspersky Endpoint Security 持续防止漏洞进程被利用。
受保护进程	**启用系统进程内存保护** Kaspersky Endpoint Security 不支持选择受保护进程。您可以仅启用系统进程内存保护。
漏洞利用防御技术： • **应用所有可用的漏洞利用防御技术** • **应用所选的漏洞利用防御技术**	*（不迁移）* Kaspersky Endpoint Security 应用所有可用的漏洞利用防御技术。

网络威胁防护

KSWS 网络威胁防护设置被迁移到“**基本威胁防护**”区域，“**网络威胁防护**”子区域。

网络威胁防护设置

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
运行模式： • **直通** • **仅通知网络攻击** • **检测到攻击时阻止连接**	**网络威胁防护** 如果选择了“**直通**”模式，网络威胁防护被禁用。 如果选择了“**仅通知网络攻击**”模式或“**检测到攻击时阻止连接**”模式，网络威胁防护被启用。Kaspersky Endpoint Security 总是工作在“**检测到攻击时阻止连接**”模式。
任务未运行时不停止流量分析	*（不迁移）* 如果启用该组件，Kaspersky Endpoint Security 持续分析流量。
不控制排除的 IP 地址	**排除项**
计划设置	*（不迁移）* 无法为组件配置单独的计划。当 Kaspersky Endpoint Security 运行时，该组件始终处于打开状态。

脚本监控

Kaspersky Endpoint Security 不支持脚本监控组件。脚本监控由其他组件处理，例如，AMSI 保护。

网站类别

Kaspersky Endpoint Security 不支持 Kaspersky Security for Windows Server 的所有类别。Kaspersky Endpoint Security 不存在的类别不被迁移。因此， Therefore, 类别不受支持的 Web 资源分类规则不被迁移。

Kaspersky Security for Windows Server 类别	Kaspersky Endpoint Security for Windows 类别
战争游戏	视频游戏
堕胎	*（不迁移）*
彩票（扩展）	赌博、彩票、抽奖
酒精	酒、烟草、毒品
匿名代理服务器	匿名站点
厌食症	*（不迁移）*
房地产租金	*（不迁移）*
音频、视频和软件	软件、音频、视频
银行业	银行
博客	博客
军事	武器、爆炸物、军事
儿童	*（不迁移）*
歧视	暴力、偏执
家庭和家人	*（不迁移）*
托管和域服务	互联网通信
宠物和动物	*（不迁移）*
法律和政治	被区域法律禁止
受 Roskomnadzor 限制(RF)	被俄罗斯联邦法律禁止
受联邦法律 436 限制(RF)	被俄罗斯联邦法律禁止
受 RF 法律限制	被俄罗斯联邦法律禁止
受全球法律限制	被区域法律禁止
成人约会	成人内容
互联网服务	*（不迁移）*
性用品商店	成人内容
信息技术	*（不迁移）*
赌场，纸牌游戏	赌博、彩票、抽奖
读书和写作	*（不迁移）*
计算机游戏	视频游戏
健康和美容	*（不迁移）*
文化和社会	*（不迁移）*
LGBT	成人内容
彩票	赌博、彩票、抽奖
药物	*（不迁移）*
时尚	*（不迁移）*
音乐	*（不迁移）*
毒品	酒、烟草、毒品
暴力	暴力、偏执
不满	*（不迁移）*
非法毒品	酒、烟草、毒品
仇恨和歧视	暴力、偏执

Kaspersky Security for Windows Server 类别	Kaspersky Endpoint Security for Windows 类别
淫秽词汇	污言秽语
妇女贴身内衣	成人内容
新闻	新闻媒体
裸体主义	成人内容
教育	*（不迁移）*
在线购物	在线商店
所有通信介质	互联网通信
信用卡支付	支付系统
在线购物（自有支付系统）	在线商店
在线百科	*（不迁移）*
网上银行	银行
武器	武器、爆炸物、军事
钓鱼和打猎	*（不迁移）*
支付系统	支付系统
求职	求职
搜索引擎	*（不迁移）*
策略决定（JP）	被日本警察禁止
受 KPSN 信任	*（不迁移）*
不受 KPSN 信任	*（不迁移）*
色情	成人内容
媒体托管和流	新闻媒体
Web 邮件	基于 Web 的邮件
旅行	*（不迁移）*
电视和广播	新闻媒体
广告传单和广告服务	广告栏
宗教	宗教、宗教协会
餐厅、咖啡馆和食物	*（不迁移）*
交友网站	约会网站
性教育	成人内容
社交网络	社交网络
运动	*（不迁移）*
赌博	赌博、彩票、抽奖
自杀	暴力、偏执
烟草	酒、烟草、毒品
种子	种子
联邦极端分子名单中提及(RF)	被俄罗斯联邦法律禁止
文件共享	文件共享
药房	*（不迁移）*
爱好和娱乐	*（不迁移）*
聊天和论坛	聊天、论坛、即时通讯
学校和大学页面	*（不迁移）*

Kaspersky Security for Windows Server 类别	Kaspersky Endpoint Security for Windows 类别
占星术和密教	*（不迁移）*
极端主义和种族主义	暴力、偏执
电子商务	在线商店
色情	成人内容
幽默	*（不迁移）*

本地活动控制

应用程序启动控制

KSWS 应用程序控制设置被迁移到“**安全控制**”区域，“**应用程序控制**”子区域。

应用程序启动控制设置

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
运行模式： • **仅统计** • **活动**	**操作**（应用程序控制）： • “**测试规则**”。 • “**应用规则**”。
在此文件的所有后续启动中重复针对首次文件启动执行的操作	*（不迁移）* Kaspersky Endpoint Security 在应用程序每次尝试运行时都对其进行扫描。
在没有可执行的命令时拒绝命令解释器启动	*（不迁移）* Kaspersky Endpoint Security 允许运行不被应用程序控制禁止的命令解释器。
规则	**应用程序控制规则** *（支持但有限制）* Kaspersky Endpoint Security 11.11.0 引入了对迁移应用程序启动控制规则的支持。 应用程序启动控制规则迁移功能有一些限制。默认情况下，KSWS 应用程序启动控制包括两个规则： • **操作系统可信任证书允许执行脚本和 MSI** • **操作系统可信任证书允许执行可执行文件** 如果至少有一个源 KSWS 规则具有**允许**类型，那么在迁移过程中，KES 将创建一个新的允许规则，即**具有受信任根证书的应用程序**。也就是说，KES 应用程序控制使用单个规则来允许运行受信任的脚本、MSI 包和可执行文件。如果两个源 KSWS 规则都具有**拒绝**类型，则 KES 不会添加用于管理具有受信任根证书的应用程序的规则。
将规则应用于可执行文件	*（不迁移）* 无法在 KES 应用程序控制设置中配置规则应用程序范围。KES 应用程序控制将规则应用于所有类型的文件：可执行文件、脚本和 MSI 包。如果所有文件类型都包含在 KSWS 的规则应用范围中，则在迁移过程中，KES 将继承 KSWS 规则。如果某个文件类型被排除在 KSWS 中的规则应用范围之外，则在迁移过程中，KES 也会继承 KSWS 规则，但选择“**测试规则**”作为应用程序控制操作。
监控 DLL 模块的加载	**控制 DLL 模块加载(显著增加系统负载)**
将规则应用于脚本和 MSI 数据包	*（不迁移）* 无法在 KES 应用程序控制设置中配置规则应用程序范围。KES 应用程序控制将规则应用于所有类型的文件：可执行文件、脚本和 MSI 包。如果所有文件类型都包含在 KSWS 的规则应用范围中，则在迁移过程中，KES 将继承 KSWS 规则。如果某个文件类型被排除在 KSWS 中的规则应用范围之外，则在迁移过程中，KES 会继承 KSWS 规则，但选择“**测试规则**”作为应用程序控制操作。
拒绝 KSN 不信任的应用程序	*（不迁移）* Kaspersky Endpoint Security 不考虑应用程序的信誉，根据规则允许或拒绝应用程序运行。
允许 KSN 信任的应用程序	在迁移过程中，KES 添加了一个新的允许规则。“**其他软件\根据 KSN 信誉受信任的其他软件**”KL 类别被指定为规则触发条件。
允许运行 KSN 信任的应用程序的用户和/或用户组	应用程序控制允许规则中的“**用户及其权限**”，其包含“**其他软件\根据 KSN 信誉受信任的其他软件**”KL 类别。
自动允许通过所列应用程序和软件包分发软件	KSWS 和 KES 中的软件分发控制工作方式不同。在迁移过程中，KES 为允许自动软件分发的应用程序添加了新的允许规则。文件哈希被指定为规则触发条件。

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
始终允许通过 Windows Installer 进行软件分发	KSWS 和 KES 中的软件分发控制工作方式不同。在迁移过程中，KES 为允许自动软件分发的应用程序添加了新的允许规则（**允许软件分发应用程序和软件包**）。文件哈希被指定为规则触发条件。在账户属性中，“**受信任更新程序**”复选框被选中。
始终允许使用后台智能传输服务通过 SCCM 进行软件分发	*（不迁移）*
允许的软件分发应用程序和数据包	KSWS 和 KES 中的软件分发控制工作方式不同。在迁移过程中，KES 为允许自动软件分发的应用程序添加了新的允许规则。文件哈希被指定为规则触发条件。在账户属性中，“**受信任更新程序**”复选框被选中。
计划设置	*（不迁移）* 如果在 KSWS 设置中为组件配置了计划，则在迁移时将启用应用程序控制组件。如果未在 KSWS 设置中为组件配置计划，则在迁移时禁用应用程序控制。 无法为组件配置单独的计划。当 Kaspersky Endpoint Security 运行时，该组件始终处于打开状态。

设备控制

KSWS 设备控制设置被迁移到“**安全控制**”区域，“**设备控制**”子区域。

设备控制设置

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
运行模式： • **活动** • **仅统计**	*（不迁移）* 应用程序控制在*活动*模式下运行。设备连接统计数据由审计持续提供。
当未运行设备控制任务时允许使用所有外部设备	*（不迁移）* 当 Kaspersky Endpoint Security 运行时，设备控制始终处于打开状态。
设备控制规则	**受信任设备** 在迁移过程中，Kaspersky Endpoint Security 忽略禁用的 KSWS 规则。
计划设置	*（不迁移）* Kaspersky Endpoint Security 使用自己的计划获取到特定设备类型的访问权限。

网络附加存储保护

RPC 网络存储保护

Kaspersky Endpoint Security 不支持网络附加存储保护组件。如果您需要这些组件，您可以继续使用 Kaspersky Security for Windows Server。

ICAP 网络存储保护

Kaspersky Endpoint Security 不支持网络附加存储保护组件。如果您需要这些组件，您可以继续使用 Kaspersky Security for Windows Server。

用于 NetApp 的反加密勒索

Kaspersky Endpoint Security 不支持 NetApp 的反加密。反加密功能由其他应用程序组件提供，例如行为检测。

网络活动控制

防火墙管理

Kaspersky Endpoint Security 不支持 KSWS 防火墙管理。KSWS 防火墙功能由系统级防火墙执行。迁移后，您可以配置 Kaspersky Endpoint Security 防火墙。

反加密

反网络加密设置被迁移到“**高级威胁防护**”区域，“**行为检测**”子区域。

反加密设置

KSWS 设置	KES 设置
运行模式： • **仅统计** • **活动**	**检测到共享文件夹的外部加密时**： • **通知** • **阻止**
启发式分析器	*（不迁移）* Kaspersky Endpoint Security 不对行为检测使用启发式分析。
保护范围的配置： • **受保护设备上的所有共享网络文件夹** • **仅指定的共享文件夹**	*（不迁移）* Kaspersky Endpoint Security 阻止加密受保护计算机的所有共享网络文件夹。
排除	*（不迁移）* Kaspersky Endpoint Security 对于行为检测组件有自己的排除项。您可以在迁移后手动添加排除项。
计划设置	*（不迁移）* 无法为组件配置单独的计划。当 Kaspersky Endpoint Security 运行时，该组件始终处于打开状态。

系统审查

文件完整性监控

来自 KSWS 的文件完整性监控设置被迁移到**安全控制** 区域，**系统完整性监控**子区域。

文件完整性监控设置

KSWS 设置	KES 设置
记录监控中断期间发生的文件操作信息	*（不迁移）* Kaspersky Endpoint Security 不会记录监控中断期间执行的文件操作的事件。
阻止对 USN 日志的入侵尝试	*（不迁移）* Kaspersky Endpoint Security 不阻止破坏 USN 日志的尝试。
监控范围	**监控范围 → 文件** *（支持但有限制）* 禁用的监视范围记录不会迁移到 KES。Kaspersky Endpoint Security 仅将启用的记录添加到监控范围。
受信任用户	**受信任的用户和/或用户组**
文件操作标记	**文件操作标记**
如果可能，计算文件的校验和	**哈希**
排除	**排除项 → 文件**

日志审查

KSWS 日志审查设置被迁移到“**安全控制**”区域，“**日志审查**”子区域。

日志审查设置

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
应用日志审查的自定义规则	*（不迁移）* Kaspersky Endpoint Security 适用于所有启用的自定义规则。
自定义规则	**自定义规则** **系统中已安装服务(用于 Server 2003 OS)**预定义规则不会迁移到 KES。
针对日志审查应用预定义规则	*（不迁移）* Kaspersky Endpoint Security 适用于所有启用的预定义规则。
预定义规则	**预定义规则**
密码强力检测	**暴力攻击检测**
网络登录检测	**网络登录检测**
排除（IP 地址）	**排除项** (IP 地址)
排除（用户）	**排除项** (用户)
计划设置	*（不迁移）* 无法为组件配置单独的计划。当 Kaspersky Endpoint Security 运行时，该组件始终处于打开状态。

日志和通知

任务日志

KSWS 日志设置被迁移到“**常规设置**”区域、“**界面**”和“**报告和存储**”子区域。

日志设置

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
事件记录	**通知**（**界面**子区域）
日志文件夹	*（不迁移）* Kaspersky Endpoint Security 保存报告到 `C:\ProgramData\Kaspersky Lab\KES.14.1\Report`。
删除早于 N 天的任务日志	*（不迁移）* 您可以在“**常规设置**”，“**报告和存储**”下配置 KES 报告的存储期限。
从审核日志事件中删除 N 天	*（不迁移）* Kaspersky Endpoint Security 应用报告存储限制到所有报告，包括系统审计报告。
与 SIEM 的整合	*（不迁移）* 您可以在 Kaspersky Security Center 中配置与 SIEM 的整合。

事件通知

KSWS 通知设置被迁移到“**常规设置**”区域，“**界面**”子区域。

通知设置

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
通知	**通知**
通知用户: • **使用终端服务** • **使用 Windows Messenger 服务命令**	*（不迁移）* Kaspersky Endpoint Security 不支持修改通知文本。Kaspersky Endpoint Security 显示标准通知。

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
通知管理员: • **使用 Windows Messenger 服务命令** • **通过运行可执行文件** • **通过发送电子邮件**	仅电子邮件通知设置被迁移到 Kaspersky Endpoint Security – **电子邮件通知设置**（**通知**块）。其他通知管理员的方法不被支持。
应用程序数据库已过期	**如果数据库超过以下天数未更新则发送"数据库已过期"通知**
应用程序数据库已严重过期	**如果数据库超过以下天数未更新则发送"数据库严重过期"通知**
已很长时间未执行关键区域扫描	*（不迁移）* Kaspersky Endpoint Security 在三天后生成错过的关键区域扫描事件。

与管理服务器交互

KSWS 管理服务器交互设置被迁移到"**常规设置**"区域，"**报告和存储**"子区域。

管理服务器交互设置

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
已隔离的文件	**隔离文件**
已备份的文件	**备份文件**
已阻止的主机	*（不迁移）* Kaspersky Endpoint Security 自动发送关于已阻止的主机的数据。

任务

激活应用程序

Kaspersky Endpoint Security 不支持*应用程序激活*任务（KSWS）。您可以创建一个*添加密钥*任务（KES），将授权许可密钥添加到安装包，或启用自动授权许可密钥分发。

复制更新

*复制更新*任务设置（KSWS）已被迁移到*数据库和应用程序模块更新*任务（KES）。

复制更新任务设置

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
更新源: • Kaspersky Security Center **管理服务器** • **卡巴斯基更新服务器** • **自定义 HTTP 或 FTP 服务器或网络文件夹**	**更新源**: • Kaspersky Security Center • **卡巴斯基更新服务器** • **由用户指定**
如果指定的服务器不可用，则使用卡巴斯基更新服务器	*（不迁移）* Kaspersky Endpoint Security 允许选择多个更新源，包括卡巴斯基更新服务器。如果第一个更新源不可用，Kaspersky Endpoint Security 将从列表中的其他源获取更新。
使用代理服务器设置连接至卡巴斯基更新服务器	*（不迁移）* Kaspersky Endpoint Security 对所有组件使用代理服务器。您可以在应用程序的网络选项中配置代理服务器连接。
使用代理服务器设置连接至其他服务器	*（不迁移）* Kaspersky Endpoint Security 对所有组件使用代理服务器。您可以在应用程序的网络选项中配置代理服务器连接。

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
复制更新设置: • **复制数据库更新** • **复制关键软件模块更新** • **复制数据库更新和关键应用程序模块的更新**	*（不迁移）* Kaspersky Endpoint Security 复制数据库更新和关键应用程序模块的更新作为一个单独的包。
用于本地存储已复制更新的文件夹	**将更新复制到文件夹**

基线文件完整性监控

"*基线文件完整性监控*"任务设置 (KSWS) 被迁移到"*系统完整性检查*"任务和策略区域"**安全控制**"、子区域"**系统完整性监控**"。

"基线文件完整性监控"任务设置

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
哈希计算算法: • MD5 • SHA256	*（不迁移）* Kaspersky Endpoint Security 使用 SHA256 算法进行校验和计算。
扫描范围	**监控范围**（**系统完整性监控**子区域）

数据库更新

*数据库更新*任务设置（KSWS）已被迁移到*数据库和应用程序模块更新*任务（KES）。

数据库更新任务设置

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
更新源: • Kaspersky Security Center **管理服务器** • **卡巴斯基更新服务器** • **自定义** HTTP **或** FTP **服务器或网络文件夹**	**更新源**: • Kaspersky Security Center • **卡巴斯基更新服务器** • **由用户指定**
如果指定的服务器不可用，则使用卡巴斯基更新服务器	*（不迁移）* Kaspersky Endpoint Security 允许选择多个更新源，包括卡巴斯基更新服务器。如果第一个更新源不可用，Kaspersky Endpoint Security 将从列表中的其他源获取更新。
使用代理服务器设置连接至卡巴斯基更新服务器	*（不迁移）* Kaspersky Endpoint Security 对所有组件使用代理服务器。您可以在应用程序的网络选项中配置代理服务器连接。
使用代理服务器设置连接至其他服务器	*（不迁移）* Kaspersky Endpoint Security 对所有组件使用代理服务器。您可以在应用程序的网络选项中配置代理服务器连接。
降低磁盘 I/O 上的负载	*（不迁移）*

软件模块更新

*软件模块更新*任务设置（KSWS）已被迁移到*数据库和应用程序模块更新*任务（KES）。

软件模块更新任务设置

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
更新源: • Kaspersky Security Center **管理服务器** • **卡巴斯基更新服务器** • **自定义** HTTP **或** FTP **服务器或网络文件夹**	**更新源**: • Kaspersky Security Center • **卡巴斯基更新服务器** • **由用户指定**

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
如果指定的服务器不可用，则使用卡巴斯基更新服务器	*（不迁移）* Kaspersky Endpoint Security 允许选择多个更新源，包括卡巴斯基更新服务器。如果第一个更新源不可用，Kaspersky Endpoint Security 将从列表中的其他源获取更新。
使用代理服务器设置连接至卡巴斯基更新服务器	*（不迁移）* Kaspersky Endpoint Security 对所有组件使用代理服务器。您可以在应用程序的网络选项中配置代理服务器连接。
使用代理服务器设置连接至其他服务器	*（不迁移）* Kaspersky Endpoint Security 对所有组件使用代理服务器。您可以在应用程序的网络选项中配置代理服务器连接。
复制并安装关键软件模块更新	**安装关键和批准的更新**
仅检查关键软件更新是否可用	*（不迁移）* Kaspersky Endpoint Security 持续检查应用程序模块关键更新的可用性。
允许操作系统重启	*（不迁移）* Kaspersky Endpoint Security 提示用户重新启动计算机的权限。
接收有关可用的计划软件模块更新的信息	*（不迁移）* Kaspersky Endpoint Security 显示软件模块更新的通知。

回滚应用程序数据库更新

*回滚应用程序数据库更新*任务设置（KSWS）已被迁移到*更新回滚*任务（KES）。新的"*更新回滚*"任务（KES）有一个任务启动计划 – *手动*。

按需扫描

*按需扫描*任务设置（KSWS）被迁移到"*恶意软件扫描*"任务（KES）。

病毒扫描任务设置

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
扫描范围	**扫描范围**
保护级别： • **最佳保护** • **推荐** • **最优性能**	**安全级别**： • **高** • **建议** • **低** 安全级别设置在 KSWS 和 KES 中有所不同。
要扫描的对象： • **所有对象** • **按格式扫描对象** • **按反病毒数据库中指定的扩展名列表扫描对象** • **按指定的扩展名列表扫描对象**	**文件类型**： • **所有文件** • **按格式扫描文件** • **按扩展名扫描文件** Kaspersky Endpoint Security 不允许创建自定义扩展程序列表。Kaspersky Endpoint Security 使用"**按扩展名扫描文件**"值替换"**按指定的扩展名列表扫描对象**"值。
子文件夹	**包括子文件夹**
子文件	*（不迁移）*
扫描磁盘引导扇区和 MBR	*（不迁移）*
扫描 NTFS 交换数据流	*（不迁移）*
仅扫描新文件和已修改的文件	**仅扫描新建和已修改的文件**
扫描复合对象： • **全部压缩文件** • **所有 SFX 压缩文件** • **全部电子邮件数据库** • **全部打包的对象** • **全部纯文本电子邮件** • **全部嵌入的 OLE 对象**	**扫描复合文件**： • "**扫描压缩包**"。 • "**扫描受密码保护的存档**"。 • "**扫描分发包**"。 • "**扫描电子邮件格式文件**"。 • "**扫描 Microsoft Office 格式文件**"。

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
对受感染对象和其他对象执行的操作： • **清除** • **清除。清除失败时则删除** • **删除** • **执行推荐的操作** • **仅通知**	**检测到威胁后的操作**： • "**清除；如果清除失败则删除**"。 • "**清除；如果清除失败则通知**"。 • "**通知**"。
对疑似感染对象执行的操作： • **隔离** • **删除** • **执行推荐的操作** • **仅通知**	*（不迁移）* Kaspersky Endpoint Security 在检测到威胁是应用操作。
根据检测到的对象的类型执行操作	*（不迁移）*
在检测到嵌入对象时完全删除应用程序无法修改的复合文件	*（不迁移）*
排除文件	*（不迁移）* Kaspersky Endpoint Security 应用受信任区域到所有组件。您可以在受信任区域设置中配置排除项。
不检测	*（不迁移）*
超过 N 秒则停止扫描	**跳过扫描时间超过以下值的文件 N 秒**
不扫描大小大于 N MB 的复合对象	**复合文件大于指定值时不解压**
使用 iSwift 技术	**iSwift 技术**
使用 iChecker 技术	**iChecker 技术**
脱机文件处理： • **不扫描** • **仅扫描文件驻留部分** • **扫描整个文件** • **仅当在指定的时间段(天)内访问了文件时** • **如果可以，不复制文件到本地硬盘驱动器**	*（不迁移）* Kaspersky Endpoint Security scans 扫描整个离线文件。

应用程序完整性检查

"*应用程序完整性控制*"任务设置（KSWS）被迁移到"*应用程序完整性检查*"任务（KES）。

应用程序启动控制规则生成器

Kaspersky Endpoint Security 不支持"*应用程序启动控制生成器*"任务。您可以在"应用程序控制设置"中生成规则。

设备控制规则生成器

Kaspersky Endpoint Security 不支持"*设备控制规则生成器*"任务。您可以在"设备控制设置"中生成访问规则。

迁移 KSWS 组件

在安装前，Kaspersky Endpoint Security 会检查计算机中是否存在卡巴斯基应用程序。如果计算机上安装了 Kaspersky Security for Windows Server，KES 将检测已安装的 KSWS 组件集，并选择相同的组件进行安装。

KSWS 没有的 KES 组件安装如下：

- AMSI 保护、主机入侵预防和修复引擎都是使用默认设置安装的。
- BadUSB 攻击防御、自适应异常控制、数据加密、Detection and Response 组件被忽略。

远程安装时，KES 应用程序会忽略已安装的 KSWS 组件集。安装程序会安装您在安装包的属性中选择的组件。安装 Kaspersky Endpoint Security 和 迁移策略和任务后，KES 设置根据 KSWS 设置进行配置。

迁移 KSWS 任务和策略

您可以通过以下方式迁移 KSWS 策略和任务设置：

- 使用策略和任务批量转换向导（以下简称“迁移向导”）。

  KSWS 迁移向导仅在管理控制台（MMC）中可用。无法在 Web 控制台和云控制台中迁移策略和任务设置。

  对于不同版本的 Kaspersky Security Center，批量转换向导的工作方式不同。我们建议将解决方案升级到版本 14.2 或更高版本。在此版本的 Kaspersky Security Center 中，策略和任务批量转换向导可让您将策略迁移到配置文件中，而不是迁移到策略中。在此版本的 Kaspersky Security Center 中，策略和任务批量转换向导还允许您迁移范围更广的策略设置。

- 使用 Kaspersky Endpoint Security for Windows 的新策略向导。

  新策略向导允许您基于 KSWS 策略创建 KES 策略。

使用迁移向导和新策略向导时，KSWS 策略迁移过程不同。

策略和任务批量转换向导

迁移向导将 KSWS 策略设置而不是 KES 策略设置转移到策略配置文件中。*策略配置文件*是一组策略设置，如果计算机满足配置的激活规则，就会在计算机上激活这些设置。`UpgradedFromKSWS` 设备标签被选为策略配置文件的触发标准。Kaspersky Security Center 自动添加`UpgradedFromKSWS` 标记到您使用远程安装任务在 KSWS 之上安装 KES 的所有计算机。如果您选择了不同的安装方法，您可以手动将标签分配给设备。

向设备添加标签：

1. 为服务器创建一个新标签—— `UpgradedFromKSWS`。

   有关为设备创建标签的详细信息，请参阅 Kaspersky Security Center 帮助。

2. 在 Kaspersky Security Center 控制台中创建一个新的管理组，并添加您要为其分配标签的服务器。

   您可以使用选择工具对服务器进行分组。有关使用选择的详细信息，请参阅 Kaspersky Security Center 帮助。

3. 在 Kaspersky Security Center 控制台中选择管理组的所有服务器，打开所选服务器的属性并分配标签。

如果您正在迁移多个 KSWS 策略，则每个策略都将转换为一个总体策略中的配置文件。如果 KSWS 策略已包含配置文件，这些配置文件也将作为配置文件迁移。因此，您将获得一个单一的策略，其中包括与所有 KSWS 策略相对应的配置文件。

如何使用策略和任务批量转换向导迁移 KSWS 策略设置

1. 在管理控制台中，选择管理服务器并右键单击以打开上下文菜单。
2. 选择“**所有任务**” → “**策略和任务批量转换向导**”。

   策略和任务批量转换向导将启动。按照向导的说明进行操作。

步骤 1. 选择您要转换其策略和任务的应用程序

在此步骤，您需要选择“Kaspersky Endpoint Security for Windows”。转到下一步。

步骤 2. 策略转换

迁移向导在 KES 策略中创建 KSWS 策略配置文件。选择您要转换到策略配置文件的 Kaspersky Security for Windows Server 策略。转到下一步。

然后，迁移向导将开始转换策略。新策略配置文件的名称将与原始 KSWS 策略相对应。

步骤 3. 策略迁移报告

迁移向导创建一个策略迁移报告。策略迁移报告包含策略转换的日期和时间、原始 KSWS 策略的名称、目标 KES 策略的名称以及新策略配置文件的名称。

步骤 4. 任务转换

迁移向导为 Kaspersky Endpoint Security for Windows 创建新任务。在任务列表中，选择要为 Kaspersky Endpoint Security 策略创建的 KSWS 任务。新任务将被命名为 *<KSWS 任务名称> (转换)*。转到下一步。

步骤 5. 向导完成

退出向导。因此，向导会执行以下操作：

- 新策略配置文件已添加到 Kaspersky Endpoint Security 策略中。

  该策略包含带有 Kaspersky Security for Windows Server 设置的配置文件。新策略具有*活动*状态。向导不更改 KSWS 策略。

- 创建新的 Kaspersky Endpoint Security 任务。

  新任务是 KSWS 任务的副本。向导不更改 KSWS 任务。

带有 KSWS 设置的新策略配置文件将被命名为 *UpgradedFromKSWS <Kaspersky Security for Windows Server 策略名称>*。在配置文件属性中，迁移向导会自动选择`UpgradedFromKSWS` 设备标签作为触发标准。因此，策略配置文件中的设置会自动应用于服务器。

基于 KSWS 策略创建策略的向导

当基于 KSWS 策略创建 KES 策略时，向导会相应地将设置传输到新策略。即一个 KES 策略对应一个 KSWS 策略。该向导不会将策略转换为配置文件。

如何使用新建策略向导迁移 KSWS 策略设置

1. 打开 Kaspersky Security Center Administration Console。
2. 在管理控制台树的“**受管理设备**”文件夹中，选择相关客户端计算机所属的管理组名称的文件夹。
3. 在工作区中选择“**策略**”选项卡。
4. 单击“**新策略**”。
   “策略向导”将启动。
5. 按照“策略向导”的说明进行操作。

步骤 1.

选择 **Kaspersky Endpoint Security for Windows (14.1)** 安装包。

步骤 2.

输入组策略的名称，例如，*办公室政策*。

选择**使用早期版本应用程序的策略设置**复选框。单击“**浏览**”并选择一个 KSWS 策略。

步骤 3 加入卡巴斯基安全网络

请阅读并接受卡巴斯基安全网络 (KSN) 声明的条款。

步骤 4.

选择“**保护主机的标准模式**”。Kaspersky Endpoint Security 为所有应用程序模式和操作系统类型提供了通用策略。

> 我们建议针对不同的模式和操作系统类型使用不同的策略。

步骤 5. 导入设置

> 如果您在步骤 4 中选择手动策略配置，则可以执行此步骤。

您可以基于 CFG 配置文件中的 Kaspersky Endpoint Security 设置创建策略。导入应用程序配置文件时，向导无法访问所有策略设置。例如，应用程序设置中缺少策略配置文件。如果您想将所有设置和配置文件转移到该策略，您可以从 KLP 文件导入其他策略。

> 导入配置文件时，Kaspersky Endpoint Security 不会传输加密容器密码。如果在连接服务器时使用双向身份验证，则需要从头开始指定加密容器密码。

步骤 6 - 10.配置策略设置

> 如果您在步骤 4 中选择手动策略配置，则可以执行此步骤。

按照以下步骤管理策略设置。

步骤 11.配置受信任区域

配置受信任区域。您可以添加预定义扫描排除项和受信任的应用程序。预定义的扫描排除项和受信任的应用程序有助于在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上快速配置 Kaspersky Endpoint Security。这意味着您不需要在服务器上为应用程序手动设置信任区域。预定义的扫描排除项和受信任的应用程序还可以帮助您在 Light Agent 模式下快速配置 Citrix 和 VMware 虚拟环境中的 Kaspersky Endpoint Security。

步骤 12.选择策略状态

- “**活动**”。下次同步后，该策略将用作计算机上的活动策略。

  活动策略的设置在同步期间保存到客户端计算机上。您无法同时将多个策略应用到一台计算机，因此每个组只能有一个策略处于活动状态。

- “**不活动**”。备份策略。如有必要，不活动策略可切换为活动状态。

  您可以创建无限数量的不活动策略。不活动策略不影响网络中计算机的应用程序设置。不活动策略用作紧急情况（如病毒攻击）的后备。如果存在通过闪存驱动器进行的攻击，您可以激活用于阻止访问闪存驱动器的策略。在这种情况下，活动策略会自动变为不活动。

- “**漫游**”。当计算机离开组织网络周界时，将激活该策略。

退出向导。

迁移后策略和任务的额外配置

KSWS 和 KES 具有不同的组件和策略设置集，因此迁移后您必须验证策略设置是否满足您的公司安全要求。

检查以下基本策略设置：

- 密码保护。KSWS 密码保护设置未迁移。Kaspersky Endpoint Security 具有内置的密码保护功能。如有需要，开启密码保护并设置密码。

- 受信任区域。KSWS 和 KES 用于选择对象的方法不同。当迁移时，KES 支持定义为单个文件或文件/文件夹路径的排除项。如果 KSWS 将排除项配置为预定义区域或脚本 URL，则不会迁移此类排除项。迁移后，您必须手动添加此类排除项。

  > 为确保 Kaspersky Endpoint Security 在服务器上正常工作，建议将对服务器功能重要的文件添加到受信任区域。对于 SQL 服务器，您必须添加 MDF 和 LDF 数据库文件。对于 Microsoft Exchange 服务器，您必须添加 CHK、EDB、JRS、LOG 和 JSL 文件。你可以使用掩码，例如，`C:\Program Files (x86)\Microsoft SQL Server\*.mdf`。

  > 从 Kaspersky Endpoint Security 12.6 for Windows 开始，扫描排除项和受信任的应用程序被添加到信任区域。预定义的扫描排除项和受信任的应用程序有助于在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上快速配置 Kaspersky Endpoint Security。这意味着您不需要在服务器上为应用程序手动设置信任区域。

- 防火墙。KSWS 防火墙功能由系统级防火墙执行。在 KES 中，一个单独的组件负责防火墙功能。迁移后，您可以配置 Kaspersky Endpoint Security 防火墙。

- 卡巴斯基安全网络。Kaspersky Endpoint Security 不支持为单个组件配置 KSN。Kaspersky Endpoint Security 对所有应用程序组件使用 KSN。要使用 KSN，您必须接受卡巴斯基安全网络声明的新条款和条件。

- Web 控制。Web 流量类别控制的阻止规则被迁移到 Kaspersky Endpoint Security 中的单独阻止规则。Kaspersky Endpoint Security 忽略类别控制的允许规则。Kaspersky Endpoint Security 不支持 Kaspersky Security for Windows Server 的所有类别。Kaspersky Endpoint Security 不存在的类别不被迁移。因此，Therefore, 类别不受支持的 Web 资源分类规则不被迁移。如有需要，添加 Web 控制规则。

- 代理服务器。代理服务器连接密码未迁移。手动输入用于连接代理服务器的密码。

- 各个组件的时间表。Kaspersky Endpoint Security 不支持为单个组件配置计划。当 Kaspersky Endpoint Security 运行时，组件始终处于打开状态。

- 组件集。可用的 Kaspersky Endpoint Security 功能集取决于操作系统的类型：工作站或服务器。例如，在加密工具之外，服务器上只有 BitLocker 驱动器加密可用。

- 属性。属性的状态未迁移。属性将具有默认值。默认情况下，新策略中的几乎所有设置都禁止修改子策略和本地应用程序界面中的设置。该属性具有**Managed Detection and Response (Industrial CyberSecurity)** 区域和**用户支持**设置组（**界面**部分）中策略设置的 值。如果必要，配置从父策略继承设置。

- 处理活动威胁。高级清除针对工作站和服务器具有不同功能。您可以在"*恶意软件扫描*"任务设置和应用程序设置中配置高级清除。

- 升级应用程序。要在不重新启动的情况下安装主要更新和补丁，您必须更改应用程序升级模式。默认情况下，安装应用程序更新而不重新启动功能处于禁用状态。

- Kaspersky Endpoint Agent。Kaspersky Endpoint Security 为 Detection and Response 解决方案引入了内置代理。如有需要，将 Kaspersky Endpoint Agent 策略设置传输到 Kaspersky Endpoint Security 策略。

- "*数据库和应用程序模块更新*"任务。确保*数据库和应用程序模块更新*任务的设置已正确迁移。KES 使用单个 KES 任务而不是 KSWS 的三个任务。你可以优化*数据库和应用程序模块更新*任务并删除多余的任务。

- 其他任务。应用程序控制、设备控制和文件完整性监控组件在 KSWS 和 KES 中的工作方式不同。KES 不使用*基线文件完整性监控*、*应用程序启动控制*、*设备控制规则生成器*任务。因此，不会迁移这些任务。迁移后，您可以配置文件完整性监控、应用程序控制、设备控制组件。

迁移 KSWS 受信任区域

受*信任区域*是由系统管理员配置的、Kaspersky Endpoint Security 在活动期间不予监控的对象和应用程序的列表。您可以使用*策略和任务批量转换向导*或*基于 KSWS 策略创建新 KES 策略的向导*将受信任区域对象从 KSWS 迁移到 KES。KSWS 和 KES 具有不同的组件和功能集，因此迁移后您必须验证排除项是否满足您的公司安全要求。向受信任区域添加排除项的方法对于 KES 和 KSWS 也有所不同。迁移向导没有迁移所有 KSWS 排除项的工具。这意味着在迁移之后，您必须手动添加一些 KSWS 排除项。

为确保 Kaspersky Endpoint Security 在服务器上正常工作，建议将对服务器功能重要的文件添加到受信任区域。对于 SQL 服务器，您必须添加 MDF 和 LDF 数据库文件。对于 Microsoft Exchange 服务器，您必须添加 CHK、EDB、JRS、LOG 和 JSL 文件。你可以使用掩码，例如，`C:\Program Files (x86)\Microsoft SQL Server\*.mdf`。

从 Kaspersky Endpoint Security 12.6 for Windows 开始，扫描排除项和受信任的应用程序被添加到信任区域。预定义的扫描排除项和受信任的应用程序有助于在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上快速配置 Kaspersky Endpoint Security。这意味着您不需要在服务器上为应用程序手动设置信任区域。

KES 和 KSWS 受信任区域创建方法。

KSWS		KES
要扫描的对象		
• 预定义范围	*（不迁移）*	
• 磁盘、文件夹或网络位置	→	**文件或文件夹**
• 文件	→	**文件或文件夹**
• 脚本文件或网址	*（不迁移）*	
检测到的对象	→	**检测对象类型**
受信任进程	→	**受信任应用程序**

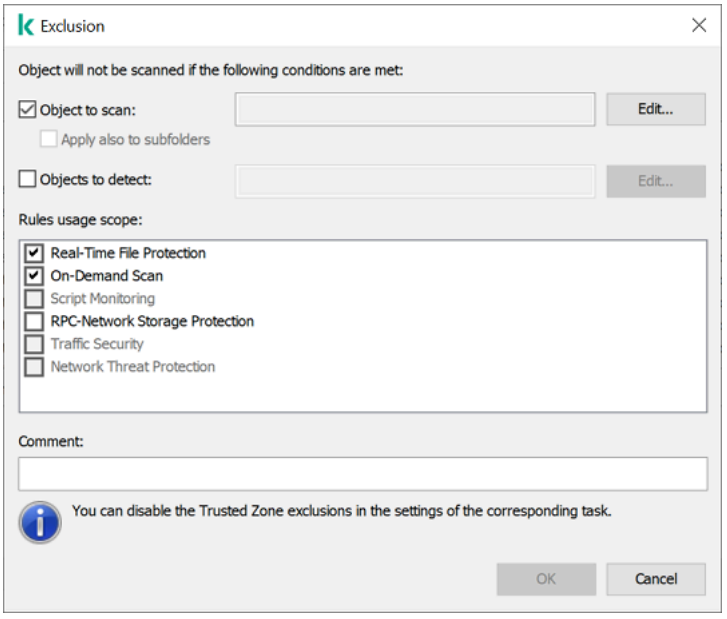
扫描对象的迁移

在属性中选择了“**要扫描的对象**”方法的 KSWS 排除项会迁移到在属性中选择了“**文件或文件夹**”方法的 KES 排除项，但有一些限制。排除项的迁移取决于对象选择方法：

- 预定义范围 – *不迁移*。
  迁移后，您必须手动添加此类排除项。必须在“*恶意软件扫描*”任务设置中配置作为预定义区域的排除项。
- 磁盘、文件夹或网络位置 – 迁移到在属性中选择了“文件或文件夹”方法的 KES 排除项。
- 文件 – 迁移到在属性中选择了“文件或文件夹”方法的 KES 排除项。
- 脚本文件或网址 – *不迁移*。
  迁移后，您必须手动添加此类排除项。必须将作为脚本网址的排除项添加到“Web 威胁保护”的受信任网址中。

如果扫描对象选中了“**也应用到子文件夹**”复选框，则此设置将迁移到 KES 排除项（“**包括子文件夹**”复选框）。

KES 排除项设置



KSWS 排除项设置

迁移检测到的对象

在属性中选择了“**检测到的对象**”方法的 KSWS 排除项会迁移到在属性中选择了“**检测对象类型**”方法的 KES 排除项。对应于 Kaspersky 百科全书的分类的检测到的对象的名称（例如，`Email-Worm`、`Rootkit` 或 `RemoteAdmin`）。Kaspersky Endpoint Security 支持带“`?`”（匹配任何单个字符）和星号“`*`”（匹配任何字符序列）的掩码。

迁移排除项使用范围

排除项的使用范围是应用排除项的组件集。KES 和 KSWS 具有不同的组件集，因此迁移向导无法迁移排除项使用范围。因此，如果在 KSWS 使用范围中至少选择了一个组件，KES 会将排除项应用于所有应用程序组件。

> 您可以在受信任区域设置以及 KSWS 保护组件的设置中配置 KSWS 使用范围。为此，您可以选择或清除策略相应区域中的“**应用受信任区域**”复选框。KES 保护组件的设置不包括这样的复选框。这意味着单个组件设置中的受信任区域状态在迁移时丢失。完成迁移后，在 KES 策略的受信任区域设置中选择应用排除项的组件。

迁移注释

来自 KSWS 受信任区域的注释被迁移到 KES 排除项注释，而不进行修改。

迁移受信任进程

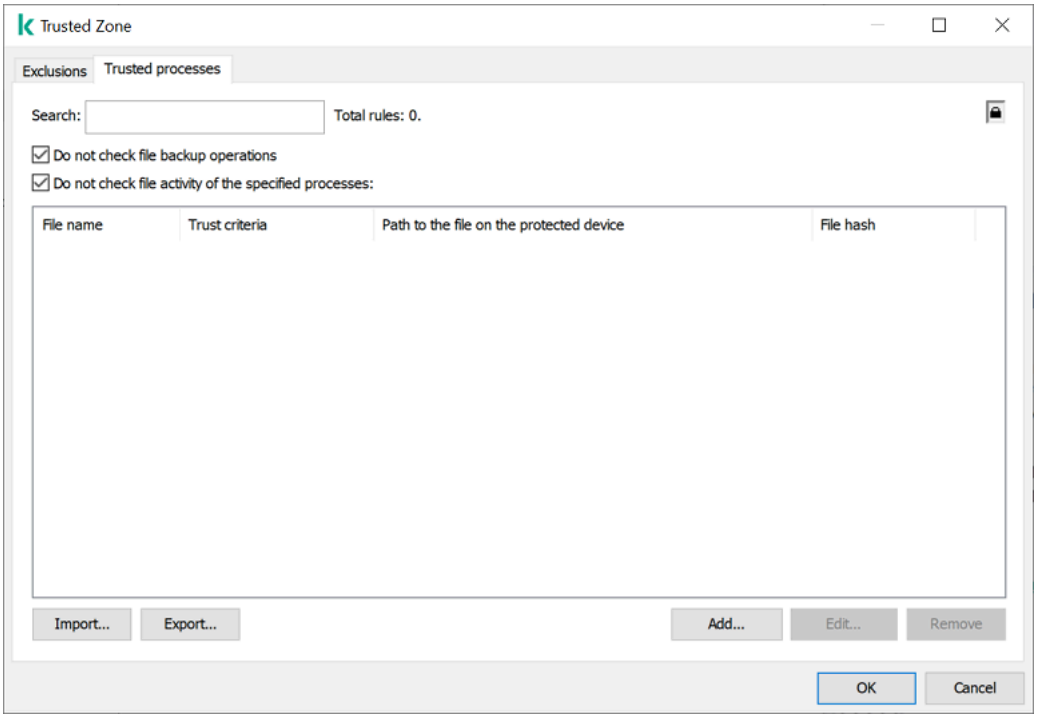
KSWS 受信任进程迁移到 KES 受信任进程，但有一些限制。迁移受信任进程取决于对象选择方法：

- 受保护设备上文件的路径 – 迁移到 KES 受信任的应用程序。
- 文件哈希 – *不迁移*。

如果 KSWS 具有配置为文件哈希的受信任进程，则不会迁移此类受信任进程。迁移后，您必须手动添加此类受信任进程。

如果在受信任的进程设置中选中了“**不检查文件备份操作**”复选框，则此设置将迁移到 KES 受信任的应用程序（“**不监控应用程序活动**”复选框）。

KES 受信任的应用程序设置



KSWS 受信任的进程设置

迁移 KSWS 应用程序启动控制规则

KSWS 应用程序启动控制默认被阻止。也就是说，应用程序启动控制会自动阻止所有未在规则中指定为允许的应用程序的应用程序。因此，KES 应用程序控制的迁移向导会自动设置“**允许列表**”控制模式，对应于默认阻止原则。

您可以使用*策略和任务批量转换向导*或*基于 KSWS 策略创建新 KES 策略的向导*将规则从 KSWS 迁移到 KES。

迁移应用程序启动控制模式

KSWS 应用程序启动控制模式被迁移到 KES 应用程序控制，如下所示：

- **仅统计 → 测试规则**；
- **活动 → 应用规则**。

迁移 KSWS 应用程序启动控制预定义规则

默认情况下，KSWS 应用程序启动控制包括两个规则：

- **操作系统可信任证书允许执行脚本和 MSI**
- **操作系统可信任证书允许执行可执行文件**

预定义规则允许运行由受信任的根证书签名的*脚本*、*MSI 程序包*和*可执行文件*。如果至少有一个预定义 KSWS 规则具有“**允许**”类型，迁移向导将创建一个新的允许规则，即“**具有受信任根证书的应用程序**”。也就是说，KES 应用程序控制使用单个规则来允许运行受信任的脚本、MSI 包和可执行文件。

如果两个 KSWS 预定义规则都具有“**拒绝**”类型，KES 忽略预定义的规则。

迁移 KSWS 应用程序启动控制自定义规则

KSWS 应用程序启动控制规则根据以下标准规范文件的执行：

- 使用数字证书签名；
- SHA256 哈希；
- 文件路径。

KSWS 和 KES 中的规则创建方式不同，因此迁移向导会创建*应用程序类别*，其中包括 KSWS 规则的条件和排除项，并将这些应用程序类别添加到 KES 规则中。向导使用应用程序类别中的“**证书**”、“**文件夹路径**”和“**文件哈希**”条件。Kaspersky Security Center 管理控制台中提供了新的应用程序类别，位于“**应用程序管理 → 应用程序类别**”部分。

迁移向导按类型和用户对 KSWS 规则进行分组。接下来，向导会创建包含 KSWS 规则的条件和排除项的应用程序类别，并将应用程序类别添加到新的 KES 规则中。向导在 KES 规则 的“**描述**”字段指定 KSWS 规则的名称。

迁移 KSWS 应用程序启动控制高级设置

KSWS 应用程序启动控制和 KES 应用程序控制的运行原理不同，因此迁移向导可能会迁移设置子集。

应用程序启动控制设置

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
在此文件的所有后续启动中重复针对首次文件启动执行的操作	*（不迁移）* Kaspersky Endpoint Security 在应用程序每次尝试运行时都对其进行扫描。
在没有可执行的命令时拒绝命令解释器启动	*（不迁移）* Kaspersky Endpoint Security 允许运行不被应用程序控制禁止的命令解释器。
将规则应用于可执行文件	*（不迁移）* 无法在 KES 应用程序控制设置中配置规则应用程序范围。KES 应用程序控制将规则应用于所有类型的文件：可执行文件、脚本和 MSI 包。如果所有文件类型都包含在 KSWS 的规则应用范围中，则在迁移过程中，KES 将继承 KSWS 规则。如果某个文件类型被排除在 KSWS 中的规则应用范围之外，则在迁移过程中，KES 也会继承 KSWS 规则，但选择“**测试规则**”作为应用程序控制操作。
监控 DLL 模块的加载	**控制 DLL 模块加载(显著增加系统负载)**
将规则应用于脚本和 MSI 数据包	*（不迁移）* 无法在 KES 应用程序控制设置中配置规则应用程序范围。KES 应用程序控制将规则应用于所有类型的文件：可执行文件、脚本和 MSI 包。如果所有文件类型都包含在 KSWS 的规则应用范围中，则在迁移过程中，KES 将继承 KSWS 规则。如果某个文件类型被排除在 KSWS 中的规则应用范围之外，则在迁移过程中，KES 会继承 KSWS 规则，但选择“**测试规则**”作为应用程序控制操作。
拒绝 KSN 不信任的应用程序	*（不迁移）* Kaspersky Endpoint Security 不考虑应用程序的信誉，根据规则允许或拒绝应用程序运行。
允许 KSN 信任的应用程序	在迁移过程中，KES 添加了一个新的允许规则。“**其他软件\根据 KSN 信誉受信任的其他软件**”KL 类别被指定为规则触发条件。
允许运行 KSN 信任的应用程序的用户和/或用户组	应用程序控制允许规则中的“**用户及其权限**”，其包含“**其他软件\根据 KSN 信誉受信任的其他软件**”KL 类别。
自动允许通过所列应用程序和软件包分发软件	KSWS 和 KES 中的软件分发控制工作方式不同。在迁移过程中，KES 为允许自动软件分发的应用程序添加了新的允许规则。文件哈希被指定为规则触发条件。
始终允许通过 Windows Installer 进行软件分发	KSWS 和 KES 中的软件分发控制工作方式不同。在迁移过程中，KES 为允许自动软件分发的应用程序添加了新的允许规则（**允许软件分发应用程序和软件包**）。文件哈希被指定为规则触发条件。在账户属性中，“**受信任更新程序**”复选框被选中。
始终允许使用后台智能传输服务通过 SCCM 进行软件分发	*（不迁移）*
允许的软件分发应用程序和数据包	KSWS 和 KES 中的软件分发控制工作方式不同。在迁移过程中，KES 为允许自动软件分发的应用程序添加了新的允许规则。文件哈希被指定为规则触发条件。在账户属性中，“**受信任更新程序**”复选框被选中。

Kaspersky Security for Windows Server 设置	Kaspersky Endpoint Security for Windows 设置
计划设置	*（不迁移）* 如果在 KSWS 设置中为组件配置了计划，则在迁移时将启用应用程序控制组件。如果未在 KSWS 设置中为组件配置计划，则在迁移时禁用应用程序控制。 无法为组件配置单独的计划。当 Kaspersky Endpoint Security 运行时，该组件始终处于打开状态。

安装 KSWS 而不是 KES

您可以通过以下方式安装 Kaspersky Endpoint Security：

- 卸载 KSWS 后安装 KES（推荐）。
- 在 KSWS 之上安装 KES。

卸载 Kaspersky Security for Windows Server

您可以使用*远程卸载应用程序*任务或在服务器本地远程卸载应用程序。卸载 KSWS 后，您可能需要重新启动服务器。如果您想在不重启的情况下安装 Kaspersky Endpoint Security，请确保 Kaspersky Security for Windows Server 已完全卸载。如果应用程序未完全卸载，安装 Kaspersky Endpoint Security 可能会导致服务器运行错误。如果您使用了 kavremover 实用程序，还建议确保应用程序已完全卸载。kavremover 实用程序不支持管理 KSWS。

> 如果启用密码保护来限制对 KSWS 的访问，请在 KES 安装包的设置中输入卸载密码。

卸载 KSWS 后，使用任何可用的方法安装 Kaspersky Endpoint Security for Windows。

安装 Kaspersky Endpoint Security

当您远程安装 KES 时，您在安装包属性中选择的组件都安装在服务器上。我们建议在安装包属性中选择默认组件。在 KSWS 上安装 KES 时不需要重新启动。

在安装前，Kaspersky Endpoint Security 会检查计算机中是否存在卡巴斯基应用程序。如果计算机上安装了 Kaspersky Security for Windows Server，KES 将检测已安装的 KSWS 组件集，并选择相同的组件进行安装。在 KSWS 上安装 KES 时不需要重新启动。

> 如果在 KSWS 之上安装 KES 失败，您可以回滚安装。回滚安装后，建议重启服务器再试。

安装 Kaspersky Endpoint Security for Windows 时，不会迁移 KSWS 设置和任务。要迁移设置和任务，请运行策略和任务批量转换向导。

您可以使用 `status` 命令在应用程序界面的“**安全**”区域或在“计算机属性”中的 Kaspersky Security Center 控制台中检查已安装组件的列表。您可以在安装后更改组件集，方法是使用*更改应用程序组件*。

迁移 [KSWS+KEA] 配置到 [KES+内置代理] 配置

要支持使用 Kaspersky Endpoint Security for Windows 作为 EDR（KATA）、EDR Optimum、EDR Expert、Kaspersky Sandbox、KUMA 和 MDR 的一部分，内置代理已添加到应用程序中。使用这些解决方案您不再需要单独的 Kaspersky Endpoint Agent 应用程序。

从 KSWS 迁移到 KES 时，EDR（KATA）、EDR Optimum、EDR Expert、Kaspersky Sandbox、KUMA 和 MDR 解决方案继续与 Kaspersky Endpoint Security 内置代理协同工作。此外，Kaspersky Endpoint Agent 将被从计算机卸载。

迁移 [KSWS+KEA] 配置到 [KES+内置代理] 需要以下步骤：

1. **从 KSWS 迁移到 KES**

   从 KSWS 迁移到 KES 涉及安装 Kaspersky Endpoint Security 而不是 Kaspersky Security for Windows Server。

   管理员通常启用密码保护以限制对 KSWS 和 KEA 的访问。从 Kaspersky Security Center Linux 15.1 开始，您可以在“*远程安装应用程序*”任务设置中输入应用程序卸载密码。该任务仅允许输入一个卸载密码。也就是说，如果为 KSWS 和 KEA 设置相同的密码，则可以成功删除 KSWS 和 KEA 应用程序。如果密码不同，则删除其中一个应用程序会失败，并出现访问错误。要完成迁移，您必须为无法在“*远程安装应用程序*”任务的设置中输入其密码的应用程序禁用密码保护。

   要执行迁移，您必须选择支持 Detection and Response 解决方案所需的组件作为 Kaspersky Endpoint Security 的一部分。安装应用程序后，Kaspersky Endpoint Security 切换到使用内置代理并卸载 Kaspersky Endpoint Agent。

2. **迁移策略和任务**

   迁移 [KSWS+KEA] 策略和任务到 [KES+内置代理] 需要以下步骤：

   1. 使用策略和任务批量转换向导将策略和任务从 KSWS 迁移到 KES（仅在管理控制台 (MMC) 上可用）。

      因此，带有 *UpgradedFromKSWS <Kaspersky Security for Windows Server 策略名称>*名称的策略配置文件被添加到 KES 策略中。还创建了新的带有 *<KSWS 任务名称>（转换）*名称的 KES 任务。

   2. 使用用于从 Kaspersky Endpoint Agent 迁移的向导将策略和任务从 KEA 迁移到 KES（仅在 Web Console 和云控制台上可用）。

      结果，创建了一个名为 *<Kaspersky Endpoint Security 策略名称>&<Kaspersky Endpoint Agent 策略名称>*的新策略。还创建了新任务和 KES 任务。

3. **授权许可功能**

   如果您使用通用 Kaspersky Endpoint Detection and Response Optimum 或 Kaspersky Optimum Security 授权许可激活 Kaspersky Endpoint Security for Windows 和 Kaspersky Endpoint Agent，EDR Optimum 功能将在升级应用程序到版本 11.7.0 后被自动激活。您不需要做任务其他事情。

   如果您使用独立 Kaspersky Endpoint Detection and Response Optimum 加载项授权许可激活 EDR Optimum 功能，您必须确保 EDR Optimum 加载项密钥已添加到 Kaspersky Security Center 存储库且授权许可密钥自动分发功能已启用。在您升级应用程序到版本 11.7.0 后，EDR Optimum 功能被自动激活。

如果您使用 Kaspersky Endpoint Detection and Response Optimum 或 Kaspersky Optimum Security 授权许可激活 Kaspersky Endpoint Agent，并使用其他授权许可激活 Kaspersky Endpoint Security for Windows，您必须使用通用 Kaspersky Endpoint Detection and Response Optimum 或 Kaspersky Optimum Security 密钥替换 Kaspersky Endpoint Security for Windows 密钥。您可以使用"*添加密钥*"任务替换密钥。

您不需要激活 Kaspersky Sandbox 功能。Kaspersky Sandbox 功能将在升级和激活 Kaspersky Endpoint Security for Windows 后立即可用。

只有 Kaspersky Anti Targeted Attack Platform 授权许可可用于激活 Kaspersky Endpoint Security 作为 Kaspersky Anti Targeted Attack Platform 解决方案的一部分。在您升级应用程序到版本 12.1 后，EDR（KATA）功能被自动激活。您不需要做任务其他事情。

4 **检查 Kaspersky Endpoint Detection and Response Optimum 和 Kaspersky Sandbox 的健康**

升级之后，计算机在 Kaspersky Security Center 控制台显示*严重*状态：

- 确保计算机安装了网络代理版本 13.2 或更高版本。
- 通过查看"*应用程序组件状态报告*"检查内置代理的操作状态。如果组件具有*未安装*状态，使用"*更改应用程序组件*"任务安装组件。
- 确保您在 Kaspersky Endpoint Security for Windows 的新策略中接受了卡巴斯基安全网络声明。

确保使用以下方式激活 EDR Optimum 功能：*应用程序组件状态报告*。如果组件具有"*授权许可不支持*"状态，确保 EDR Optimum 的授权许可密钥自动分发功能已关闭。

确保已成功卸载 Kaspersky Security for Windows Server

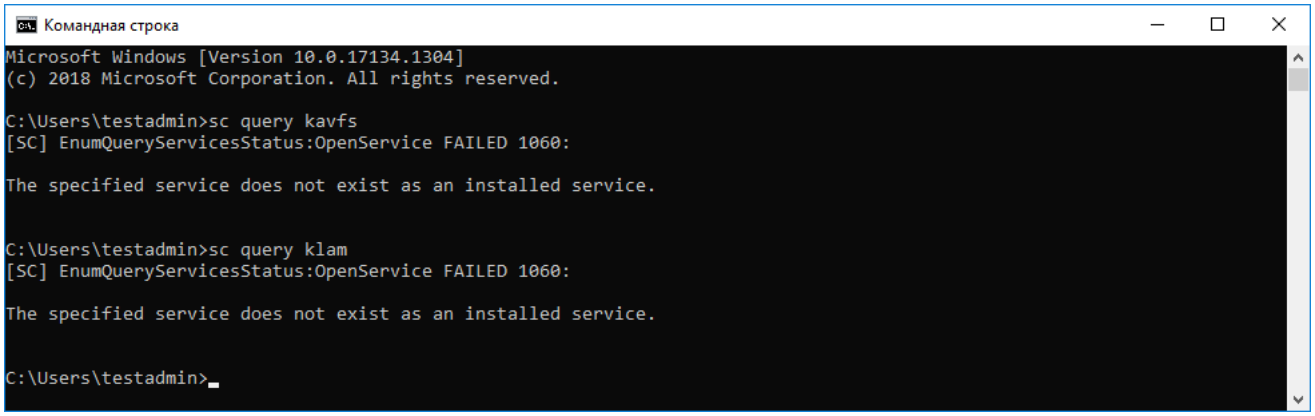
确保 Kaspersky Security for Windows Server 已完全卸载：

- `%ProgramFiles%\Kaspersky Lab\Kaspersky Security for Windows Server\` 文件夹不存在。
- 不存在以下服务：
  - Kaspersky Security Service （KAVFS）
  - Kaspersky Security Management 服务（KAVFSGT）
  - Kaspersky Security Exploit Prevention 服务（KAVFSSLP）
  - Kaspersky Security Script Checker 服务（KAVFSSCS）

  您可以在任务管理器中检查正在运行的服务或通过发出 `sc query` 命令（见下图）。
- 以下驱动程序不存在：
  - klam.sys
  - klflt.sys
  - klramdisk.sys
  - klelaml.sys
  - klfltdev.sys

- klips.sys
- klids.sys
- klwtpee

您可以在 `C:\Windows\System32\drivers` 文件夹检查已安装的驱动程序或发出 `sc query` 命令。如果缺少服务或驱动程序，您将收到以下响应：



确保已成功卸载 Kaspersky Security for Windows Server 服务和驱动程序

如果应用程序或驱动程序文件保留在服务器上，请手动删除相关文件。如果 Kaspersky Security for Windows Server 服务仍在服务器上运行，请手动停止（`sc stop`）和删除（`sc delete`）服务。要停止 klam.sys 驱动程序，请使用 `fltmc unload klam` 命令。

使用 KSWS 密钥激活 KES

安装应用程序后，可以使用 Kaspersky Security for Windows Server（KSWS）授权许可密钥激活 Kaspersky Endpoint Security for Windows（KES）。迁移后的激活过程取决于 KSWS 激活方法（见下表）。

Kaspersky Endpoint Security 不支持 *Kaspersky Security for Storage 授权许可*。要使用此授权许可，您需要使用 Kaspersky Security for Windows Server。

要使用 KSWS 密钥激活 KES，您只能使用激活码。如果您正使用密钥文件激活应用程序，您需要联系技术支持以获得 Kaspersky Endpoint Security 密钥文件。

使用 Kaspersky Security for Windows Server 密钥激活 Kaspersky Endpoint Security for Windows

Kaspersky Security for Windows Server 激活方法	迁移密钥到 Kaspersky Endpoint Security for Windows。
自动向计算机分发 KSWS 授权许可密钥。	如果在 KSWS 授权许可密钥属性中启用了自动密钥分发，则会使用 KSWS 密钥自动激活 KES。
KSWS 密钥由任务添加。	如果您使用任务激活了 KSWS，则在从 KSWS 迁移期间会删除 KSWS 授权许可密钥。您必须再次激活该应用程序。例如，您可以将授权许可密钥添加到 Kaspersky Endpoint Security For Windows 安装包中。
KSWS 密钥在应用程序接口中本地添加。	如果您使用应用程序激活向导在本地激活了 KSWS，则在从 KSWS 迁移期间会删除 KSWS 授权许可密钥。您必须再次激活该应用程序。例如，您可以将授权许可密钥添加到 Kaspersky Endpoint Security For Windows 安装包中。
KSWS 密钥将添加到安装包中。	如果您使用安装包中的密钥激活了 KSWS，则在从 KSWS 迁移期间将删除 KSWS 授权许可密钥。您必须再次激活该应用程序。例如，您可以将授权许可密钥添加到 Kaspersky Endpoint Security For Windows 安装包中。

Kaspersky Security for Windows Server 激活方法	迁移密钥到 Kaspersky Endpoint Security for Windows。
Amazon Web Services (AWS) 中的付费虚拟机映像 (Amazon Machine Image – AMI)。	如果您购买了 Kaspersky Security Center 作为 Amazon Web Services (AWS) 中的付费虚拟机映像（Amazon Machine Image – AMI），则不需要激活 KES。在这种情况下，Kaspersky Security Center 使用已添加到应用程序的 AWS 订阅。
带有您自己的授权许可的现成免费 Kaspersky Security Center 映像（自带许可证 – BYOL 模型）。	如果您在云环境中使用带有您自己的授权许可的开箱即用的免费 Kaspersky Security Center 映像（自带许可证 – BYOL 模型），您必须使用任何可用的方法激活该应用程序。您将需要 Kaspersky Hybrid Cloud Security 授权许可。

迁移高负载服务器的特殊注意事项

在高负载服务器上，监控性能和避免故障很重要。迁移到 Kaspersky Endpoint Security for Windows 后，我们建议暂时禁用相对于其他组件使用大量服务器资源的应用程序组件。确保服务器正常运行后，您可以重新开启应用程序组件。

我们建议按如下方式迁移高负载服务器：

1. 使用默认设置创建 Kaspersky Endpoint Security 策略。

   默认设置被认为是最佳的。此设置由 Kaspersky 专家推荐。默认设置提供建议的保护级别和最佳资源使用。

2. 在策略设置中，关闭以下组件： 网络威胁防护、行为检测、漏洞利用防御、修复引擎、应用程序控制。

   如果您的组织部署了 Kaspersky Managed Detection and Response (MDR) 解决方案， 将 BLOB 配置文件上传到 Kaspersky Endpoint Security 策略。

3. 从服务器中卸载 Kaspersky Security for Windows Server。

4. 使用默认组件集安装 Kaspersky Endpoint Security for Windows。

   如果您的组织部署了 Detection and Response 解决方案，请在安装包的属性中选择相关组件。

5. 检查应用程序的设置：

   - 该应用程序使用 KSWS 授权许可密钥激活。
   - 新策略已应用。先前选择的组件被禁用。

6. 确保服务器正常工作。确保 Kaspersky Endpoint Security for Windows 未使用超过 1% 的服务器资源。

7. 如有需要，创建扫描排除项，添加受信任的应用程序，创建受信任网址列表。

8. 开启行为检测、漏洞利用防御、修复引擎组件。确保 Kaspersky Endpoint Security for Windows 未使用超过 1% 的服务器资源。

9. 开启网络威胁防护组件。确保 Kaspersky Endpoint Security for Windows 未使用超过 2% 的服务器资源。

10. 以规则测试模式开启应用程序控制组件。

11. 确保应用程序控制正在运行。如有需要，添加新的应用程序控制规则并在确认应用程序控制正常工作后，关闭规则测试模式。

从 KSWS 迁移到 KES 后，确保应用程序正常运行。在控制台查看服务器状态（应该是*正常*）。确保应用程序没有报告任何错误，还要检查最后一次连接到管理服务器的时间、最后一次更新数据库的时间和服务器保护状态。

在 Server Core 模式下管理服务器上的应用程序

Server Core 模式的服务器不具有 GUI。因此，您只能使用 Kaspersky Security Center 控制台或在命令行上本地远程管理应用程序。

使用 Kaspersky Security Center 控制台管理应用程序

使用 Kaspersky Security Center 控制台安装应用程序与正常安装没有区别。当创建安装包时，您可以添加授权许可密钥以激活应用程序。您可以使用 Kaspersky Endpoint Security for Windows 密钥或 Kaspersky Security for Windows Server 密钥。

> 在 Server Core 模式的服务器上，以下应用程序组件不可用：Web 威胁防护、邮件威胁防护、Web 控制、BadUSB 攻击防护、文件级加密 (FLE)、卡巴斯基磁盘加密 (FDE)。

安装 Kaspersky Endpoint Security 时，不需要重新启动。仅当在安装前必须删除不兼容的应用程序时，才需要重新启动。更新应用程序版本时也可能需要重新启动。应用程序无法显示提示用户重新启动服务器的窗口。您可以从 Kaspersky Security Center 控制台的报告中了解重新启动服务器的必要性。

在 Server Core 模式的服务器上管理应用程序与管理计算机没有什么不同。您可以使用策略和任务来配置应用程序。

在 Server Core 模式的服务器上管理应用程序涉及以下特殊注意事项：

- Server Core 模式的服务器没有 GUI，因此 Kaspersky Endpoint Security 不会显示警告，告诉用户需要进行高级清除。要清除威胁，您需要在应用程序设置中启用高级清除技术以及在“*恶意软件扫描*”任务设置中立即启动高级清除。然后您需要启动“*恶意软件扫描*”任务。
- BitLocker 驱动器加密仅适用于受信任的平台模块（TPM）。PIN/密码不能用于加密，因为应用程序无法显示预引导身份验证的密码提示窗口。如果操作系统已启用联邦信息处理标准（FIPS）兼容模式，请在开始加密驱动器之前连接可移动驱动器以保存加密密钥。

从命令行管理应用程序

当您无法使用 GUI 时，您可以从命令行管理 Kaspersky Endpoint Security。

要安装应用程序到 Server Core 模式的服务器，运行以下命令：

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /s
```

要激活应用程序，运行以下命令：

```
avp.com license /add <activation code or key file>
```

要检查应用程序配置文件状态，运行以下命令：

```
avp.com status
```

要查看应用程序管理命令列表，运行以下命令：

```
avp.com help
```

迁移 [KSWS+KEA] 到 [KES+内置代理]

从 Kaspersky Security for Windows Server (KSWS) 迁移到 Kaspersky Endpoint Security (KES) 时，您可以使用以下建议来配置服务器保护和优化性能。在这里，我们将查看单个组织的迁移示例。

组织的基础设施

公司安装了以下设备：

- Kaspersky Security Center 14.2。

  管理员使用管理控制台 (MMC) 管理卡巴斯基解决方案。Kaspersky Endpoint Detection and Response Optimum (EDR Optimum) 也被部署

  在 Kaspersky Security Center 中，创建了三个管理组，包含组织的服务器：两个用于 SQL 服务器的管理组和一个用于 Microsoft Exchange 服务器的管理组。每个管理组都由自己的策略管理。*数据库更新*和*按需扫描*任务为组织中的所有服务器所创建。

  KSWS 激活密钥已添加到 Kaspersky Security Center。自动密钥分发已启用。

- 安装了 Kaspersky Security for Windows Server 11.0.1 和 Kaspersky Endpoint Agent 3.11 的 SQL 服务器。SQL 服务器组合成两个集群。

  KSWS 由 *SQL_Policy(1)* 和 *SQL_Policy(2)* 策略管理。*数据库更新*、*按需扫描*任务也被创建。

- 安装了 Kaspersky Security for Windows Server 11.0.1 和 Kaspersky Endpoint Agent 3.11 的 Microsoft Exchange 服务器。

  KSWS 由 *Exchange_Policy* 策略管理。*数据库更新*、*按需扫描*任务也被创建。

规划迁移

迁移涉及以下步骤：

1. 使用策略和任务批量转换向导迁移 KSWS 任务和策略。
2. 使用策略和任务批量转换向导迁移 Kaspersky Endpoint Agent 策略。
3. 使用标签激活新策略属性中的策略配置文件。

4. 安装 KES 而不是 KSWS。

5. 激活 EDR Optimum。

6. 确认 KES 正在运行。

迁移方案最初是在 SQL 服务器集群之一上执行的。然后在另一个 SQL 服务器集群上执行迁移场景。然后在 Microsoft Exchange 上执行迁移方案。

使用策略和任务批量转换向导迁移 KSWS 任务和策略

要迁移 KSWS 任务，您可以使用策略和任务批量转换向导（迁移向导）。结果，不是 *SQL_Policy(1)*、*SQL_Policy(2)* 和 *Exchange_Policy* 策略，您将获得一个其中包含分别用于 SQL 和 Microsoft Exchange 服务器的三个配置文件的单一策略。带有 KSWS 设置的新策略配置文件将被命名为 *UpgradedFromKSWS <Kaspersky Security for Windows Server 策略名称>*。在配置文件属性中，迁移向导会自动选择`UpgradedFromKSWS` 设备标签作为触发标准。因此，策略配置文件中的设置会自动应用于服务器。

使用策略和任务批量转换向导迁移 Kaspersky Endpoint Agent 策略

要迁移 Kaspersky Endpoint Agent 策略，您可以使用策略和任务批量转换向导。Kaspersky Endpoint Agent 的策略和任务迁移向导仅在 Web 控制台中可用。

使用标签激活新策略属性中的策略配置文件

选择您之前分配的设备标签作为配置文件激活条件。打开策略属性并选择*策略配置文件激活常规规则*作为配置文件激活条件。

安装 KSWS 而不是 KES

在安装 KES 之前，您必须在 KSWS 策略属性中禁用密码保护。

安装 KES 涉及以下步骤：

1. 准备安装包。在安装包属性中，选择 Kaspersky Endpoint Security for Windows 12.0 分发包并选择默认组件集。

2. 为 SQL 服务器管理组之一创建一个“*远程安装应用程序*”任务。

3. 在任务属性中，选择安装包和授权许可密钥文件。

4. 等待任务成功完成。

5. 为剩余的管理组重复 KES 安装。

KES 安装完成后，Kaspersky Security Center 自动添加 `UpgradedFromKSWS` 标签到控制台上的计算机名称。

要检查 KES 安装，您可以使用*保护部署报告*。您还可以检查设备状态。要确认应用程序激活，您可以使用*授权许可密钥使用报告*。

激活 EDR Optimum

您可以使用独立的 Kaspersky Endpoint Detection and Response Optimum 附加授权许可激活 EDR Optimum 功能。您必须确认 EDR Optimum 密钥已添加到 Kaspersky Security Center 存储库并且启用了自动授权许可密钥分发功能。

要检查 EDR Optimum 激活情况，您可以使用“*应用程序组件状态报告*”。

确认 KES 正在工作

要确认 KES 正常工作，您可以检查并查看没有报错。设备状态必须是*正常*。更新和恶意软件扫描任务成功完成。

用于保护虚拟机的 Light Agent 模式

从 12.8 版本开始，您可以将 Kaspersky Endpoint Security for Windows 用作 Kaspersky Security for Virtualization Light Agent 的一部分。*Kaspersky Security for Virtualization Light Agent* 解决方案是一款集成解决方案，可为虚拟机提供全面保护，使其免受各种类型的信息安全威胁、网络攻击和网络钓鱼攻击。要使用此解决方案，您必须以 Light Agent 模式安装该应用程序。

不支持在基于 Arm 的虚拟机上以 Light Agent 模式安装 Kaspersky Endpoint Security。

从 6.2 版开始，您可以在 Light Agent 模式下使用 Kaspersky Endpoint Security，作为 Kaspersky Security for Virtualization Light Agent 的一部分。

启动 Light Agent 时，它会建立并维护与虚拟机 SVM 的连接 (Secure Virtual Machine）。Protection Server 部署在 SVM 上。*Protection Server* 是 Kaspersky Security for Virtualization Light Agent 解决方案组件，可扫描文件以查找病毒和其他恶意软件、更新反病毒数据库和管理授权许可密钥。Light Agent 将需要扫描的文件或其片段发送到 SVM。扫描结果适用于所有安装了 Light Agent 的虚拟机（SharedCache 技术）。此技术提高了解决方案效率，并能更快地应对威胁。

组织的基础架构可能包含许多安装了 Light Agent 的虚拟机和许多 SVM。集成服务器处理虚拟机和 SVM 之间的交互。*集成服务器*是 Kaspersky Security for Virtualization Light Agent 解决方案的一个组件，它生成可用 SVM 列表并将此数据传输到 Light Agent，参与 Light Agent 对 SVM 的发现，保护 Light Agent 和 SVM 之间的连接，并执行其他功能。

Light Agent 模式的特殊注意事项

您可以使用 Kaspersky Endpoint Security 策略和任务在标准模式和 Light Agent 模式下管理 Kaspersky Endpoint Security。在 Light Agent 模式下，应用程序的某些组件和功能不可用。

更新数据库和程序软件模块

Light Agent 模式下的 Kaspersky Endpoint Security 使用特殊恶意软件数据库，应用程序需要此数据库才能作为 Kaspersky Security for Virtualization Light Agent 的一部分来运行。Kaspersky Endpoint Security 从 Protection Server 获取数据库和应用程序模块更新。

受保护虚拟机上的数据库和模块使用特殊的“*数据库和应用程序模块更新*”任务进行更新，在该任务中，将 SVM 上的某个文件夹指定为更新源。Light Agent 自动运行“*数据库和应用程序模块更新*”任务。您不能选择不同的更新源、配置任务计划或删除任务。

Protection Server 端还处理最新恶意软件数据库更新的回滚。在 SVM 上回滚数据库和应用程序模块更新后，会有一个特殊的本地“*数据库和应用程序模块更新*”任务在受保护的虚拟机上启动。该任务使得 Light Agent 恢复为使用先前的一组恶意软件数据库。

Light Agent 模式下的 Kaspersky Endpoint Security 不支持“*更新回滚*”任务。

激活 Light Agent

要激活该应用程序，您必须将授权许可密钥添加到 Light Agent 所连接的 SVM。您不需要单独激活应用程序。

Light Agent 模式的其他特殊注意事项

- 为应用程序创建策略时，我们建议选择 Light Agent 模式。在此模式下，新策略向导会提示您配置 SVM 连接。这些设置是应用程序在 Light Agent 模式下工作所必需的。
- 您无法在 Light Agent 模式下安装数据加密组件和自适应异常控制。组件集还取决于访客操作系统的类型：工作站或服务器。
- Light Agent 不支持与 Kaspersky Endpoint Detection and Response Expert 和 Kaspersky Endpoint Detection and Response Expert (cloud) 解决方案集成。
- 您可以在管理控制台 (MMC) 和 Kaspersky Security Center Web Console 中管理 Light Agent。无法在 Kaspersky Security Center 云控制台中管理 Light Agent。
- 不支持更改 VDI 虚拟机上的应用程序组件集。
- Kaspersky Endpoint Security 通过 KSN 代理服务器与 KSN 服务器通信。不支持与 KSN 直接通信。
- 不支持卡巴斯基安全网络的云模式。
- 不支持在连接到 Integration Server(VIIS)、Protection Server (SVM) 和 KSN 服务器时使用应用程序代理服务器。

虚拟机的初步配置

您可以在使用虚拟平台技术的虚拟机上安装 Kaspersky Endpoint Security。Kaspersky Endpoint Security 支持 VMware、Microsoft Hyper-V、Citrix 虚拟平台。在安装之前，您必须对虚拟机进行初步配置。

与 Citrix App Layering 技术的兼容性

如果您打算使用“Full User Layer”来保存临时虚拟机的状态，您必须在虚拟机模板上安装之前执行以下操作：

1. 创建 C:\Program Files\Unidesk\Uniservice\UserExclusions\KESLA.txt 文件并向其中添加以下排除项：
   - `C:\ProgramData\KasperskyLab\`
   - `C:\ProgramData\Kaspersky Lab\`
   - `C:\Program Files (x86)\Kaspersky Lab\`

2. 在操作系统的注册表中，在 HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Unifltr 键，创建一个名为 MiniFilterBypass 的新 DWORD 值并将其设置为 1。

3. 在操作系统的注册表中，在 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Unirsd 键，创建一个名为 ExcludeKey 的新 MULTI_SZ 值并将其设置为 \Registry\Machine\SOFTWARE\WOW6432Node\KasperskyLab。

4. 重新启动虚拟机。

要在使用 Citrix App Layering 的基础架构中的虚拟机上进行安装，必须执行以下操作：

1. 在应用层的虚拟机模板上安装 Kaspersky Security Center 管理代理和 Kaspersky Endpoint Security for Windows。

2. 创建由多层组成的虚拟机镜像。

3. 在支持 Citrix App Layering 解决方案的虚拟机管理程序上部署创建的镜像。

4. 配置从创建的镜像创建临时虚拟机。

有关如何与 Citrix App Layering 一起安装反病毒软件的详细信息，请参阅 Citrix App Layering 文档。

与 Citrix Provisioning（Citrix Provisioning Services）技术的兼容性

要确保应用程序与 Citrix Provisioning 技术 (Citrix Provisioning Services) 兼容：

- 如果虚拟机上安装了 Citrix Provisioning Target Device 软件，则必须先将其卸载，然后再安装 Kaspersky Endpoint Security 应用程序（详情请访问 Citrix 技术支持网站）。安装应用程序后，您必须重新安装 Citrix Provisioning Target Device。

- 使用安装向导或者使用 Kaspersky Security Center 远程安装应用程序时，您必须选择“**确保与 Citrix PVS 兼容**”复选框。

与 Omnissa App Volumes 技术的兼容性

在虚拟机模板上安装之前，您必须创建“%SVAgent%\Config\Custom\snapvol.cfg”文件并向其中添加以下排除项：

- `exclude_path=\ProgramData\Kaspersky Lab`

- `exclude_path=\ProgramData\KasperskyLab`

- `exclude_path=\Program Files\Kaspersky Lab`

- `exclude_path=\Program Files\Common Files\Kaspersky Lab`

- `exclude_path=\Program Files\Kaspersky Lab`

- `exclude_path=\Program Files (x86)\Kaspersky Lab`

- `exclude_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Kaspersky Lab`
- `exclude_process_path=\Program Files (x86)\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Common Files\Kaspersky Lab`
- `exclude_process_path=\Program Files\Kaspersky Lab`
- `exclude_process_name=avp.exe`
- `exclude_process_name=klnagent.exe`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\Wow6432Node\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SOFTWARE\KasperskyLab`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_arkmon`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klark`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_klbg`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_mark`
- `exclude_registry=\REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Services\klupd_klif_swmon`

有关详细信息，请参阅 Omnissa 文档。

安装 Light Agent

不支持在基于 Arm 的虚拟机上以 Light Agent 模式安装 Kaspersky Endpoint Security。

在 Light Agent 模式下安装应用程序与在标准模式下安装相同。在虚拟机上安装 Light Agent 之前，您必须确保已安装 Kaspersky Security Center 网络代理。*网络代理*可促进管理服务器与客户端计算机之间的交互。

Light Agent 组件可以通过以下方式之一安装在虚拟机上：

- 使用 Kaspersky Security Center 远程。
- 在本地使用安装向导。
- 使用命令行本地进行。

要安装 Light Agent，您必须在安装包设置或在设置向导中选择适当的配置。

在服务器上安装 Light Agent 时，高级保护组件（行为检测、漏洞预防、修复引擎）将从应用程序的默认配置中排除。默认应用程序设置提供推荐的保护级别和服务器资源的最佳使用。在工作站上安装 Light Agent 时，高级保护组件包含在应用程序的默认配置中。

安装 Light Agent 时，我们建议为相关虚拟环境选择预定义的排除项和受信任的应用程序。预定义的扫描排除和受信任的应用程序可帮助您快速设置应用程序并避免虚拟环境兼容性问题。您还可以在策略中配置安装后的预定义扫描排除项和受信任的应用程序。

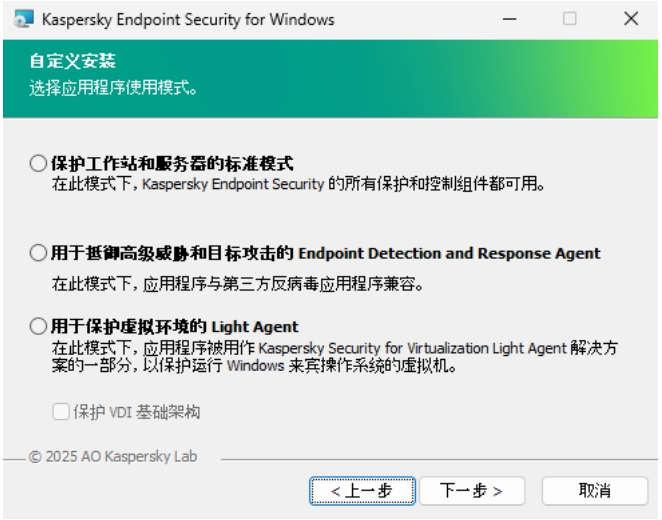
在持久虚拟机上安装 Light Agent 时，您可能需要更改"Sensor ID"生成算法。Sensor ID 在 Kaspersky Anti Targeted Attack Platform 解决方案中用于识别向服务器发送遥测数据的计算机。要创建一个唯一的 Sensor ID，在命令行上安装应用程序时设置 `EnableUniqueSensorID=1`。

如何使用安装向导安装 Light Agent

1. 复制分发包文件夹到虚拟机。
2. 运行 setup_kes.exe。

   "安装向导"将启动。

Kaspersky Endpoint Security 的配置



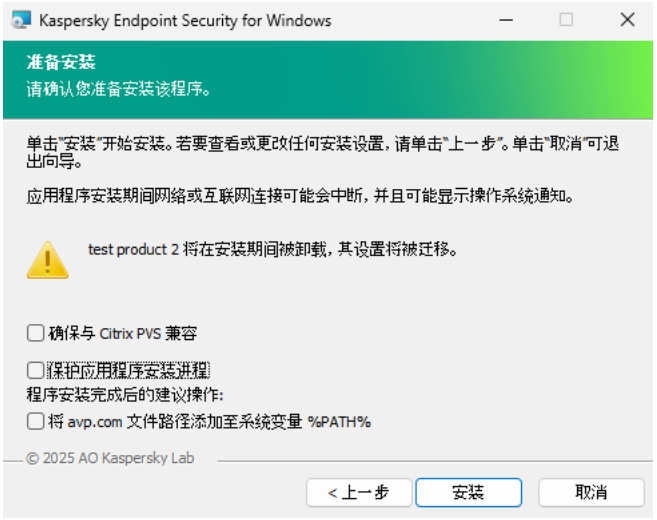
选择应用程序的配置

选择"**用于保护虚拟环境的 Light Agent**"配置。此配置适用于作为 Kaspersky Security for Virtualization Light Agent 解决方案的一部分使用的应用程序。Light Agent 必须安装在需要使用解决方案保护的每个虚拟机上。在此配置中，您不能使用数据加密组件或自适应异常控制。如果您正在虚拟机模板上安装 Light Agent，该模板将用于创建*非持久虚拟机*，选择"**保护 VDI 基础架构**"复选框（VDI 代表 Virtual Desktop Infrastructure）。VDI 保护模式能够在临时虚拟机上优化 Kaspersky Endpoint Security 的性能。在此模式下，Light Agent 会拒绝需要重新启动虚拟机的应用程序更新。当接收到需要重新启动的应用程序更新时，Light Agent 会生成需要更新受保护虚拟机模板的事件。

Kaspersky Endpoint Security 组件

选择您要安装的组件（见下图）。安装应用程序后，您可以更改可用的应用程序组件。为此，您需要再次运行安装向导，然后选择更改可用组件。

高级设置



高级应用程序安装设置

"**保护应用程序安装进程**"。安装保护包括防止分发包被替换为恶意应用程序、阻止对 Kaspersky Endpoint Security 安装文件夹的访问，以及阻止对包含应用程序密钥的系统注册表部分的访问。但是，如果无法安装应用程序（例如，当使用Windows Remote Desktop执行远程安装时），我们建议您禁用安装过程的保护。

"**确保与 Citrix PVS 兼容**"。您可以启用 Citrix Provisioning Services 支持以将 Kaspersky Endpoint Security 安装到虚拟机。

"**将 avp.com 文件路径添加至系统变量 %PATH%**"。您可以将安装路径添加到 %PATH% 变量中，以方便使用命令行界面。

如何使用命令行安装 Light Agent

1. 以管理员身份运行命令行解释器 (cmd.exe)。

2. 转到 Kaspersky Endpoint Security 分发包所在文件夹。

3. 运行以下命令：

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pLIGHTAGENTMODE=1 [/pVDI=1] [/s]
```

或

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 KSN=1 LIGHTAGENTMODE=1 [VDI=1] [/qn]
```

"`VDI`"选项启用 VDI (Virtual Desktop Infrastructure)保护模式。VDI 保护模式能够在临时虚拟机上优化 Kaspersky Endpoint Security 的性能。在此模式下，Light Agent 会拒绝需要重新启动虚拟机的应用程序更新。当接收到需要重新启动的应用程序更新时，Light Agent 会生成需要更新受保护虚拟机模板的事件。默认禁用 VDI 保护模式。

因此，Light Agent 会使用默认的组件集安装在虚拟机上。您可以使用 setup.ini 文件编辑组件集并指定高级设置。您还可以在命令行上指定安装设置。

如何使用管理控制台（MMC）安装 Light Agent

1. 打开 Kaspersky Security Center Administration Console。
2. 在控制台树中，选择"**高级**" → "**远程安装**" → "**安装包**"文件夹。

   这将打开已下载到 Kaspersky Security Center 的安装包列表。
3. 打开 Kaspersky Endpoint Security for Windows 安装包的属性。

   如果有需要的话， 创建新的安装包。
4. 转到"**设置**"区域。
5. 选择"**用于保护虚拟环境的 Light Agent**"配置。此配置适用于作为 Kaspersky Security for Virtualization Light Agent 解决方案的一部分使用的应用程序。Light Agent 必须安装在需要使用解决方案保护的每个虚拟机上。在此配置中，您不能使用数据加密组件或自适应异常控制。如果您正在虚拟机模板上安装 Light Agent，该模板将用于创建*非持久虚拟机*，选择"**保护 VDI 基础架构**"复选框（VDI 代表 Virtual Desktop Infrastructure）。VDI 保护模式能够在临时虚拟机上优化 Kaspersky Endpoint Security 的性能。在此模式下，Light Agent 会拒绝需要重新启动虚拟机的应用程序更新。当接收到需要重新启动的应用程序更新时，Light Agent 会生成需要更新受保护虚拟机模板的事件。
6. 选择您要安装的组件。

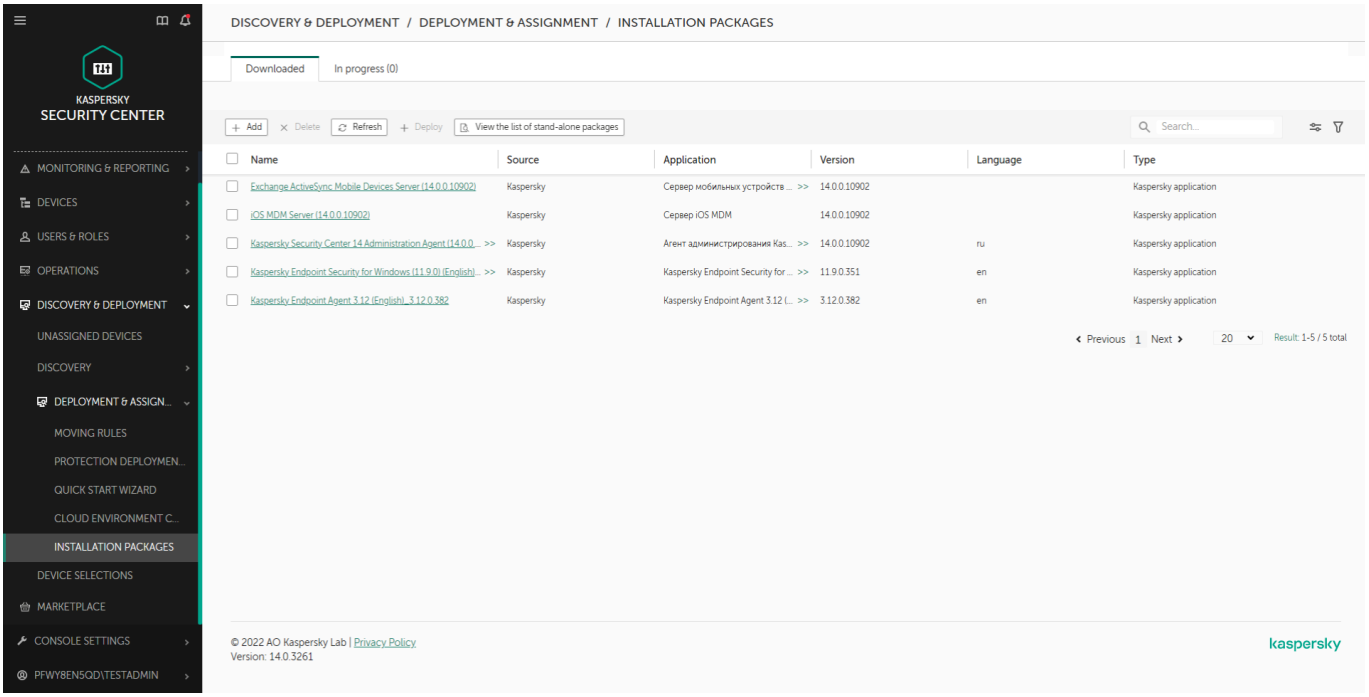
   安装应用程序后，您可以更改可用的应用程序组件。
7. 配置受信任区域。为您要安装应用程序的虚拟环境选择预定义的扫描排除项和受信任的应用程序。

   预定义的扫描排除和受信任的应用程序可帮助您快速设置应用程序并避免虚拟环境兼容性问题。
8. 保存更改。
9. 创建远程安装任务。在任务属性中，选择您创建的安装包。

如何使用 Web Console 安装 Light Agent

1. 在 Web Console 的主窗口中，选择"**发现和部署**" → "**部署和分配**" → "**安装包**"。

这将打开已下载到 Kaspersky Security Center 的安装包列表。



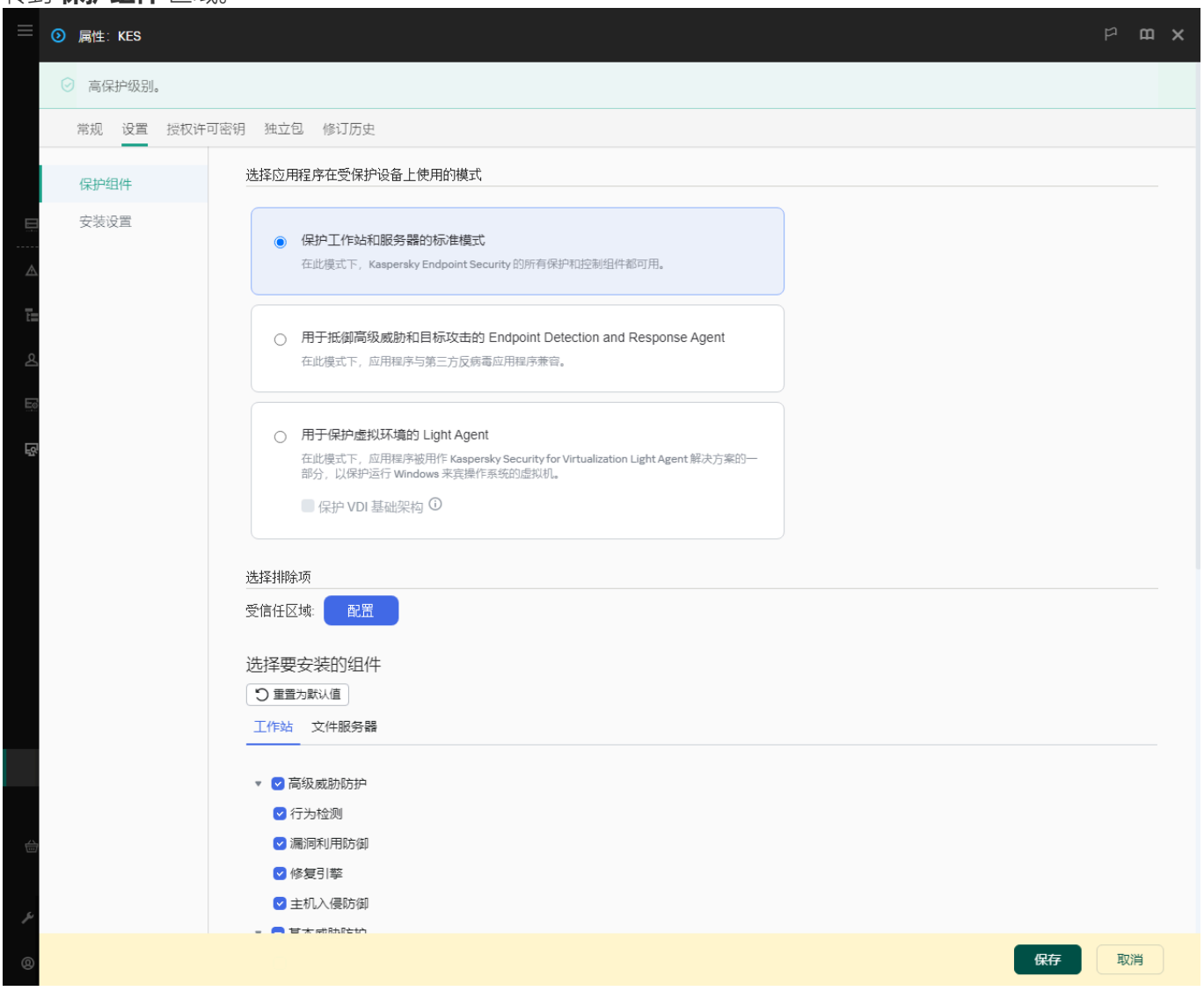
安装包列表

2. 打开 Kaspersky Endpoint Security for Windows 安装包的属性。

   如果有需要的话， 创建新的安装包。

3. 选择“**设置**”选项卡。

4. 转到“**保护组件**”区域。



安装包中包含的组件

5. 选择“**用于保护虚拟环境的 Light Agent**”配置。此配置适用于作为 Kaspersky Security for Virtualization Light Agent 解决方案的一部分使用的应用程序。Light Agent 必须安装在需要使用解决方案保护的每个虚拟机上。在此配置中，您不能使用数据加密组件或自适应异常控制。如果您正在虚拟机模板上安装 Light Agent，该模板将用于创建*非持久虚拟机*，选择“**保护 VDI 基础架构**”复选框（VDI 代表 Virtual Desktop Infrastructure）。VDI 保护模式能够在临时虚拟机上优化 Kaspersky Endpoint Security 的性能。在此模式下，Light Agent 会拒绝需要重新启动虚拟机的应用程序更新。当接收到需要重新启动的应用程序更新时，Light Agent 会生成需要更新受保护虚拟机模板的事件。

6. 选择您要安装的组件。

   安装应用程序后，您可以更改可用的应用程序组件。

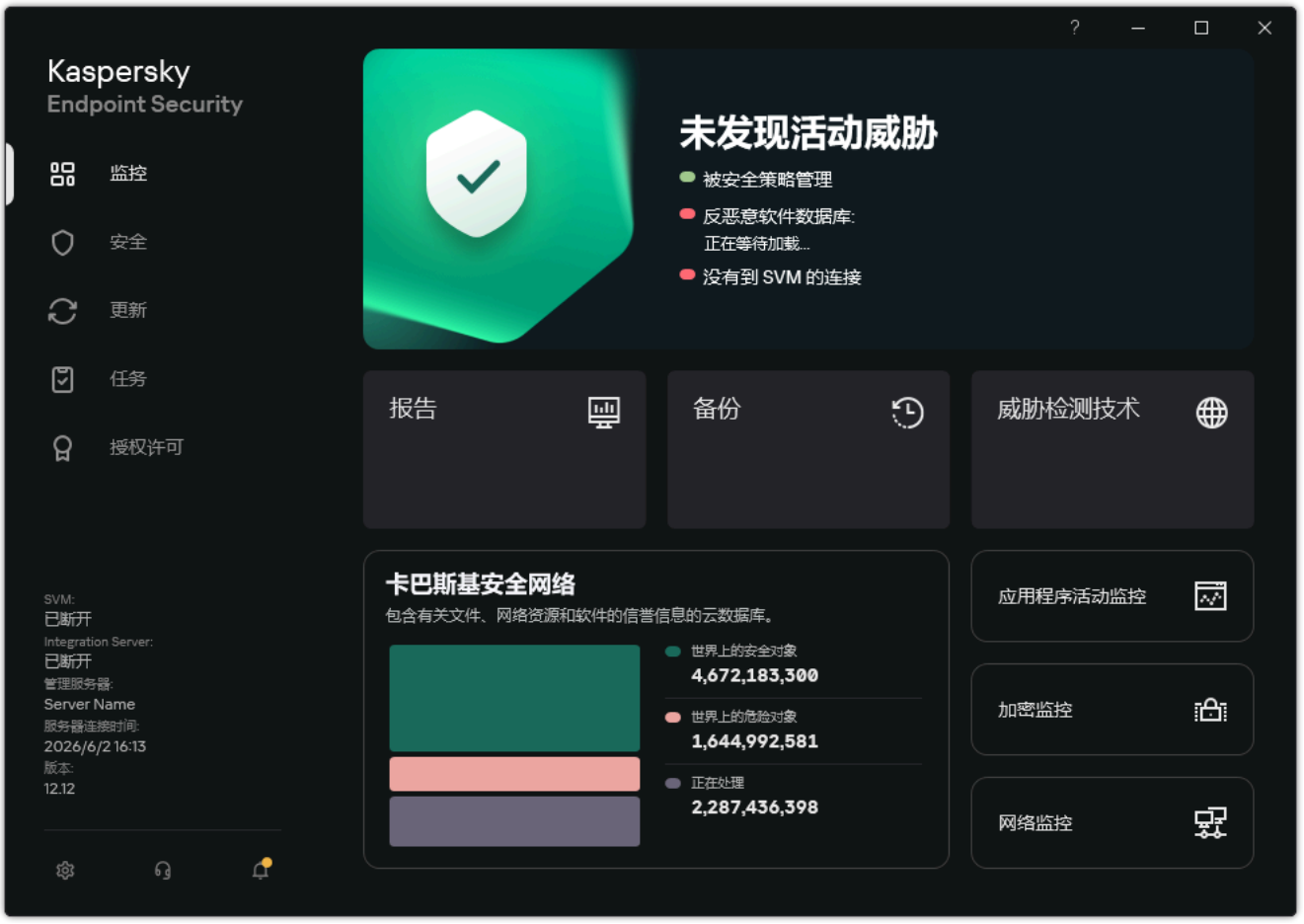
7. 配置受信任区域。为您要安装应用程序的虚拟环境选择预定义的扫描排除项和受信任的应用程序。

   预定义的扫描排除和受信任的应用程序可帮助您快速设置应用程序并避免虚拟环境兼容性问题。

8. 保存更改。

9. 创建远程安装任务。在任务属性中，选择您创建的安装包。

这样，Light Agent 就安装在虚拟机上了。您可以使用应用程序的界面，并且通知区域中会显示应用程序的图标 。现在您需要配置 Light Agent 与 SVM 的连接。



Light Agent 的主窗口

将 Light Agent 连接至 SVM

Kaspersky Security for Virtualization Light Agent 解决方案需要 Light Agent 和 SVM 持续通信。这对于扫描 Light Agent 发送的文件中是否存在病毒和其他恶意软件是必要的。如果没有 SVM 连接，Light Agent 就无法发送文件进行扫描。如果超过五分钟都无法建立连接，扫描将以错误结束。

将 Light Agent 连接到 SVM 涉及以下步骤：

1. Light Agent 获取可用 SVM 列表。
2. Light Agent 根据 SVM 选择算法决定一个对连接最优的可用 Protection Server (SVM)。
3. Light Agent 检查其他 SVM 连接设置： 标签、连接保护状态、授权许可涵盖的应用程序功能。
4. 将 Light Agent 连接至 SVM。

您可以在 Kaspersky Endpoint Security 中获取有关 Light Agent 与 SVM 的连接状态的信息，也可以使用应用程序命令。每当 Light Agent 的 SVM 连接丢失或建立时，应用程序都会生成一个事件，并将这些事件发送到 Kaspersky Security Center。如果您使用 Integration Server 进行 SVM 发现，则可以在 Integration Server 控制台中获取有关 SVM 状态和已连接 Light Agent 数量的信息。有关 SVM 状态监控的详细信息，请参阅 Kaspersky Security for Virtualization Light Agent 帮助。

SVM 发现

您可以为 Light Agent 选择 SVM 检测方法之一：

- 使用 Integration Server (VIIS)。

  集成服务器 是一种解决方案组件，可支持 Kaspersky Security for Virtualization Light Agent 与虚拟基础架构交互，并生成可供连接的 SVM 列表。Light Agent 与Integration Server 建立连接并获取 SVM 地址列表。

  集成服务器尤其适用于大型虚拟基础架构，因为它会自动平衡 SVM 之间的负载，获取有关可用 SVM 的信息，分析这些信息，并向 Light Agent 提供最适合连接的保护服务器 (SVM) 列表。

  为了使 Light Agent 能够获取 SVM 列表，您只需输入 Integration Server 的地址。

- 使用 SVM 地址的列表。

  如果需要指定 Light Agent 想要连接的各个 SVM，您可以手动准备一个列表。

  您需要列出 Light Agent 可以连接的可用 SVM 的地址。

如何在管理控制台 (MMC) 中配置 Light Agent 的 SVM 发现

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **Light Agent 模式** → **SVM 检测设置**。
4. 选择 SVM 发现方法。
   - “**使用 Integration Server**”。输入 Integration Server 连接设置。输入安装了 Integration Server 的设备的 IP 地址（IPv4 格式）或完全限定域名 (FQDN)。
   - “**使用 SVM 地址的自定义列表**”。创建 Light Agent 可连接到的 SVM 的列表。指定 SVM 的 IP 地址（IPv4 格式）或完全限定域名 (FQDN)。每个列表项必须另起一行，或者用分号 (`;`) 与前一项分隔开。

     > 在 SVM 地址列表中，仅指定与单个 IP 地址匹配的完全限定域名（FQDN）。使用与多个 IP 地址对应的完全限定域名可能会导致解决方案出错。

5. 保存更改。

如何在 Web Console 中配置 Light Agent 的 SVM 发现

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

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **Light Agent 模式** → **SVM 发现设置**。

5. 选择 SVM 发现方法。

- "**使用 Integration Server**"。输入 Integration Server 连接设置。输入安装了 Integration Server 的设备的 IP 地址（IPv4 格式）或完全限定域名 (FQDN)。
- "**使用 SVM 地址的自定义列表**"。创建 Light Agent 可连接到的 SVM 的列表。指定 SVM 的 IP 地址（IPv4 格式）或完全限定域名 (FQDN)。每个列表项必须另起一行，或者用分号 (`;`) 与前一项分隔开。

> 在 SVM 地址列表中，仅指定与单个 IP 地址匹配的完全限定域名（FQDN）。使用与多个 IP 地址对应的完全限定域名可能会导致解决方案出错。

6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在应用程序界面中配置 Light Agent 的 SVM 发现

1. 打开主应用程序窗口并单击 按钮。
2. 在应用程序设置窗口的"**Light Agent 模式**"下，点击"**SVM 检测设置**"瓦片。
3. 选择 SVM 发现方法。

- "**使用 Integration Server**"。输入 Integration Server 连接设置。输入安装了 Integration Server 的设备的 IP 地址（IPv4 格式）或完全限定域名 (FQDN)。
- "**使用 SVM 地址的自定义列表**"。创建 Light Agent 可连接到的 SVM 的列表。指定 SVM 的 IP 地址（IPv4 格式）或完全限定域名 (FQDN)。每个列表项必须另起一行，或者用分号 (`;`) 与前一项分隔开。

> 在 SVM 地址列表中，仅指定与单个 IP 地址匹配的完全限定域名（FQDN）。使用与多个 IP 地址对应的完全限定域名可能会导致解决方案出错。

4. 保存更改。

为 Light Agent 配置 SVM 选择算法

组织的基础架构可能已部署多个 SVM，Light Agent 可以连接到这些 SVM。为了平衡网络和虚拟基础架构资源的负载，需要在 SVM 之间分发 Light Agent。

在连接时，Light Agent 可应用以下 SVM 选择算法：

标准算法（默认情况下）

如果应用此算法，则在安装和启动后，虚拟机上的 Light Agent 选择连接到相对于 Light Agent 是*本地*的 SVM。

SVM 是否为 Light Agent 的本地 SVM，取决于虚拟基础架构的类型：

- 在基于 Basis Dynamix Enterprise 的虚拟基础架构中，部署在与安装了 Light Agent 的虚拟机相同节点上的 SVM 会被视为 Light Agent 的本地 SVM。
- 在基于 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、华为 FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 的虚拟基础架构中，部署在与安装了 Light Agent 的虚拟机相同 Hypervisor 上的 SVM 会被视为 Light Agent 的本地 SVM。
- 在 OpenStack 或 VK Private Cloud 平台上运行的虚拟基础架构中，您可以使用 Integration Server 配置文件 appsettings.json 中 `HypervisorSpecificSettings:Openstack` 部分的 `StandardAlgorithmSvmLocality` 参数，指定如何确定 SVM 相对于 Light Agent 的本地性。根据 Integration Server 的版本，文件位于以下路径之一：
  - /var/opt/kaspersky/viis/common/ - 对于基于 Linux 的 Integration Server
  - %ProgramFiles(x86)%\Kaspersky Lab\Kaspersky VIISLA\ - 对于基于 Windows 的 Integration Server

  `StandardAlgorithmSvmLocality` 参数可以采用以下值：

  - `ServerGroup` – 如果选择此值，只要 SVM 与安装了 Light Agent 的虚拟机位于同一服务器组内，则该 SVM 被视为 Light Agent 的本地 SVM。默认情况下使用此值。
  - `Project` – 如果选择此值，只要 SVM 与安装了 Light Agent 的虚拟机部署在同一个 OpenStack 项目中，则该 SVM 被视为 Light Agent 的本地 SVM。
  - `AvailabilityZone` – 如果选择此值，只要 SVM 与安装了 Light Agent 的虚拟机位于同一可用域内，则该 SVM 被视为 Light Agent 的本地 SVM。

如果没有可连接的本地 SVM，Light Agent 会选择连接的 Light Agent 数量最少的 SVM，无论该 SVM 在虚拟基础架构中的路径如何。

> 如果在 SVM 上为 Protection Server 启用了大型基础架构保护模式，则应用程序无法确定 SVM 相对于 Light Agent 是否为本地。在这种情况下，建议使用扩展 SVM 选择算法并选择 Integration Server 作为 SVM 发现方法。

扩展算法

如果应用此算法，您可以定义以下 SVM 选择设置：

- 在选择用于连接的 SVM 时是否考虑或忽略基础架构中的 SVM 位置
- 如果考虑 SVM 的位置，则确定 SVM 相对于 Light Agent 的本地性的方法

如果 Light Agent 忽略基础架构中 SVM 的位置，则 Light Agent 将能够连接到任何可供连接的 SVM。

如果 Light Agent 必须考虑基础架构中 SVM 的位置，则需要选择在确定相对于 Light Agent 的 SVM 位置时要考虑的 SVM 路径类型。SVM 是否为 Light Agent 的本地 SVM，取决于虚拟基础架构的类型。

在基于 Basis Dynamix Enterprise 的虚拟基础架构中，在以下情况之一，SVM 可被视为 Light Agent 的本地 SVM：

- SVM 与安装了 Light Agent 的虚拟机部署在同一节点上。
- SVM 与安装了 Light Agent 的虚拟机部署在同一区域中。
- SVM 与安装了 Light Agent 的虚拟机部署在同一数据中心中。

在基于 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、华为 FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 的虚拟基础架构中，在以下任何一种情况下，SVM 可被视为 Light Agent 的本地 SVM：

- SVM 与安装了 Light Agent 的虚拟机部署在同一 Hypervisor 上。
- SVM 与安装了 Light Agent 的虚拟机部署在同一 Hypervisor 集群上。
- SVM 与安装了 Light Agent 的虚拟机部署在同一数据中心中。

在 OpenStack 或 VK Private Cloud 平台上运行的虚拟基础架构中，在以下情况之一，SVM 可被视为 Light Agent 的本地 SVM：

- SVM 与安装了 Light Agent 的虚拟机位于同一服务器组中。
- SVM 与安装了 Light Agent 的虚拟机部署在同一 OpenStack 项目中。
- SVM 与安装了 Light Agent 的虚拟机位于同一可用域中。

如果 Light Agent 在选择连接哪个 SVM 时考虑 SVM 在基础架构中的位置，则 Light Agent 只能连接到本地的 SVM。

例如，如果您将 Hypervisor 集群指定为 SVM 路径类型，则部署在该 Hypervisor 集群上的所有 SVM 都将被视为对 Light Agent 而言是本地的，而 Light Agent 只能连接到其中一个 SVM。如果运行 Light Agent 的同一集群中没有 SVM 可供连接，则 Light Agent 将不连接到 SVM。

在选择 SVM 时，Light Agent 将考虑已连接的 Light Agent 数量，以确保在可供连接的 SVM 之间平均分布 Light Agent。

> 如果 Light Agent 使用扩展 SVM 选择算法，选择 SVM 地址列表作为 SVM 发现方法，并且 SVM 上启用了大型基础架构保护模式，则只有在忽略 SVM 路径的情况下才可以将 Light Agent 连接到该 SVM。

除了 SVM 连接算法之外，您还可以使用标签来管理 Light Agent 与 SVM 的连接。

如何在管理控制台(MMC)中配置 Light Agent 的 SVM 选择算法

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **Light Agent 模式** → **SVM 选择算法**。

4. 选择算法：

- “**使用标准 SVM 选择算法**”。Light Agent 选择部署在同一个 Hypervisor 中的 SVM。
- “**使用扩展 SVM 选择算法**”。Light Agent 选择部署在选定 SVM 路径类型的 SVM（默认情况下，**Hypervisor**）。

5. 如果需要，为扩展的 SVM 选择算法选择 SVM 路径：

- “**Hypervisor**”。Light Agent 选择与符合特定标准的 SVM 进行连接（取决于虚拟基础架构的类型）：
  - SVM 与安装了 Light Agent 的虚拟机部署在同一 Hypervisor 上（在基于 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、华为 FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 的虚拟基础架构中）。
  - SVM 与安装了 Light Agent 的虚拟机位于同一服务器组中（在 OpenStack 或 VK Private Cloud 平台上运行的虚拟基础架构中）。
  - SVM 与安装了 Light Agent 的虚拟机托管在同一计算节点上（在 Basis Dynamix Enterprise 的虚拟基础架构中）。

  如果安装了 Light Agent 的虚拟机所在的同一 Hypervisor 或同一服务器组中没有可连接的 SVM，则 Light Agent 不会连接到 SVM。

- “**集群**”。Light Agent 选择符合以下标准的 SVM 进行连接（取决于虚拟基础架构的类型）：
  - SVM 与安装了 Light Agent 的虚拟机部署在同一 Hypervisor 集群中（在基于 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、华为 FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 的虚拟基础架构中）。
  - SVM 与安装了 Light Agent 的虚拟机部署在同一 OpenStack 项目中（在 OpenStack 或 VK Private Cloud 平台上运行的虚拟基础架构中）。
  - SVM 与安装了 Light Agent 的虚拟机位于同一区域中（在 Bais Dynamix Enterprise 的虚拟基础架构中）。

  如果安装了 Light Agent 的虚拟机所在的同一 Hypervisor 集群或同一 OpenStack 项目中没有可连接的 SVM，则 Light Agent 不会连接到 SVM。

- “**数据中心**”。Light Agent 选择符合以下标准的 SVM 进行连接（取决于虚拟基础架构的类型）：
  - SVM 与安装了 Light Agent 的虚拟机部署在同一数据中心中（在基于 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、华为 FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 的虚拟基础架构中）。
  - SVM 与安装了 Light Agent 的虚拟机位于同一可用区中（在 OpenStack 或 VK Private Cloud 平台上运行的虚拟基础架构中）。
  - SVM 与安装了 Light Agent 的虚拟机位于同一数据中心中（在 Dynamix Enterprise Basis 的虚拟基础架构中）。

如果带有 Light Agent 的虚拟机所在的同一数据中心或可用区中没有可连接的 SVM，则 Light Agent 不会连接到 SVM。

- “**忽略**”。Light Agent 会忽略用于连接 Protection Server 的 SVM 路径。Light Agents 考虑了其他标准：标签、连接到 SVM 的 Light Agents 数量等等。

6. 保存更改。

如何在 Web Console 中为 Light Agent 配置 SVM 选择算法

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

   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **Light Agent 模式** → **SVM 选择算法**。
5. 选择算法：
   - “**使用标准 SVM 选择算法**”。Light Agent 选择部署在同一个 Hypervisor 中的 SVM。
   - “**使用扩展 SVM 选择算法**”。Light Agent 选择部署在选定 SVM 路径类型的 SVM（默认情况下，**Hypervisor**）。
6. 如果需要，为扩展的 SVM 选择算法选择 SVM 路径：
   - “**Hypervisor**”。Light Agent 选择符合以下标准的 SVM 进行连接（取决于虚拟基础架构的类型）：
     - SVM 与安装了 Light Agent 的虚拟机部署在同一 Hypervisor 上（在基于 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、华为 FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 的虚拟基础架构中）。
     - SVM 与安装了 Light Agent 的虚拟机位于同一服务器组中（在 OpenStack 或 VK Private Cloud 平台上运行的虚拟基础架构中）。
     - SVM 与安装了 Light Agent 的虚拟机托管在同一计算节点上（在 Basis Dynamix Enterprise 的虚拟基础架构中）。

     如果安装了 Light Agent 的虚拟机所在的同一 Hypervisor 或同一服务器组中没有可连接的 SVM，则 Light Agent 不会连接到 SVM。
   - “**集群**”。Light Agent 选择符合以下标准的 SVM 进行连接（取决于虚拟基础架构的类型）：
     - SVM 与安装了 Light Agent 的虚拟机部署在同一 Hypervisor 集群中（在基于 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、华为 FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 的虚拟基础架构中）。
     - SVM 与安装了 Light Agent 的虚拟机部署在同一 OpenStack 项目中（在 OpenStack 或 VK Private Cloud 平台上运行的虚拟基础架构中）。
     - SVM 与安装了 Light Agent 的虚拟机位于同一区域中（在 Bais Dynamix Enterprise 的虚拟基础架构中）。

如果安装了 Light Agent 的虚拟机所在的同一 Hypervisor 集群或同一 OpenStack 项目中没有可连接的 SVM，则 Light Agent 不会连接到 SVM。

- "**数据中心**"。Light Agent 选择符合以下标准的 SVM 进行连接（取决于虚拟基础架构的类型）：

  - SVM 与安装了 Light Agent 的虚拟机部署在同一数据中心中（在基于 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、华为 FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 的虚拟基础架构中）。

  - SVM 与安装了 Light Agent 的虚拟机位于同一可用区中（在 OpenStack 或 VK Private Cloud 平台上运行的虚拟基础架构中）。

  - SVM 与安装了 Light Agent 的虚拟机位于同一数据中心中（在 Dynamix Enterprise Basis 的虚拟基础架构中）。

  如果带有 Light Agent 的虚拟机所在的同一数据中心或可用区中没有可连接的 SVM，则 Light Agent 不会连接到 SVM。

- "**忽略**"。Light Agent 会忽略用于连接 Protection Server 的 SVM 路径。Light Agents 考虑了其他标准：标签、连接到 SVM 的 Light Agents 数量等等。

7. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在应用程序界面中配置 Light Agent 的 SVM 选择算法

1. 打开主应用程序窗口并单击 按钮。

2. 在应用程序设置窗口的"**Light Agent 模式**"下，点击"**SVM 检测设置**"瓦片。

3. 选择算法：

   - "**使用标准 SVM 选择算法**"。Light Agent 选择部署在同一个 Hypervisor 中的 SVM。

   - "**使用扩展 SVM 选择算法**"。Light Agent 选择部署在选定 SVM 路径类型的 SVM（默认情况下，**Hypervisor**）。

4. 如果需要，为扩展的 SVM 选择算法选择 SVM 路径：

   - "**Hypervisor**"。Light Agent 选择符合以下标准的 SVM 进行连接（取决于虚拟基础架构的类型）：

     - SVM 与安装了 Light Agent 的虚拟机部署在同一 Hypervisor 上（在基于 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、华为 FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 的虚拟基础架构中）。

     - SVM 与安装了 Light Agent 的虚拟机位于同一服务器组中（在 OpenStack 或 VK Private Cloud 平台上运行的虚拟基础架构中）。

     - SVM 与安装了 Light Agent 的虚拟机托管在同一计算节点上（在 Basis Dynamix Enterprise 的虚拟基础架构中）。

     如果安装了 Light Agent 的虚拟机所在的同一 Hypervisor 或同一服务器组中没有可连接的 SVM，则 Light Agent 不会连接到 SVM。

- “**集群**”。Light Agent 选择符合以下标准的 SVM 进行连接（取决于虚拟基础架构的类型）：

  - SVM 与安装了 Light Agent 的虚拟机部署在同一 Hypervisor 集群中（在基于 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、华为 FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 的虚拟基础架构中）。

  - SVM 与安装了 Light Agent 的虚拟机部署在同一 OpenStack 项目中（在 OpenStack 或 VK Private Cloud 平台上运行的虚拟基础架构中）。

  - SVM 与安装了 Light Agent 的虚拟机位于同一区域中（在 Bais Dynamix Enterprise 的虚拟基础架构中）。

  如果安装了 Light Agent 的虚拟机所在的同一 Hypervisor 集群或同一 OpenStack 项目中没有可连接的 SVM，则 Light Agent 不会连接到 SVM。

- “**数据中心**”。Light Agent 选择符合以下标准的 SVM 进行连接（取决于虚拟基础架构的类型）：

  - SVM 与安装了 Light Agent 的虚拟机部署在同一数据中心中（在基于 Microsoft Hyper-V、XenServer、VMware vSphere、KVM、Proxmox VE、Basis、华为 FusionSphere、Nutanix Acropolis、ALT Virtualization Server、Astra Linux、Numa vServer 或 Basis Dynamix Standard 的虚拟基础架构中）。

  - SVM 与安装了 Light Agent 的虚拟机位于同一可用区中（在 OpenStack 或 VK Private Cloud 平台上运行的虚拟基础架构中）。

  - SVM 与安装了 Light Agent 的虚拟机位于同一数据中心中（在 Dynamix Enterprise Basis 的虚拟基础架构中）。

  如果带有 Light Agent 的虚拟机所在的同一数据中心或可用区中没有可连接的 SVM，则 Light Agent 不会连接到 SVM。

- “**忽略**”。Light Agent 会忽略用于连接 Protection Server 的 SVM 路径。Light Agents 考虑了其他标准：标签、连接到 SVM 的 Light Agents 数量等等。

5. 保存更改。

将 Light Agent 的连接分发到 SVM（标签）

多个 Light Agent 可以连接到一个 SVM。要平衡 Light Agent 连接，您可以指定单独的 SVM 列表。如果您使用 Integration Server 进行 SVM 发现，则可以使用“*标签*”平衡 Light Agent 与 SVM 的连接。也就是说，对于 Light Agent，您可以分配一个 SVM 列表，以便使用标签进行连接。为此，您必须为 Light Agent 分配一个标签，并在 SVM 设置中指定此标签。有关在 SVM 设置中指定标签的详细信息，请参阅 Kaspersky Security for Virtualization Light Agent 帮助。

示例：Kaspersky Endpoint Detection and Response Optimum 解决方案部署在您的基础设施中，用于指定的虚拟机主机。在这种情况下，您可以分配“`[EDROptimum]`”标签到 Light Agent，使其连接到已添加 EDR Optimum（EDR Optimum 插件）授权许可密钥的 SVM。因此，您可以在带有 Light Agent 的虚拟机上使用 EDR Optimum 功能。当将 Light Agent 连接到没有 EDR Optimum 授权许可密钥的 SVM 时， Kaspersky Endpoint Detection and Response Optimum 功能不可用。

如何在管理控制台(MMC)中将 SVM 连接标签分配给 Light Agent

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **Light Agent 模式** → **SVM 连接标签**。
4. 选择“**使用连接标签**”复选框并输入 SVM 连接标签。
   对于标签，可以输入最长 255 个字符的文本字符串。可以使用除 `;` 字符外的任何字符。
5. 保存更改。

如何在 Web Console 中将 SVM 连接标签分配给 Light Agent

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **Light Agent 模式** → **SVM 连接标签**。
5. 选择“**使用连接标签**”复选框并输入 SVM 连接标签。
   对于标签，可以输入最长 255 个字符的文本字符串。可以使用除 `;` 字符外的任何字符。
6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在应用程序界面中将 SVM 连接标签分配给 Light Agent

1. 打开主应用程序窗口并单击 按钮。
2. 在应用程序设置窗口的“**Light Agent 模式**”下，点击“**SVM 连接标签**”瓦片。
3. 选择“**使用连接标签**”复选框并输入 SVM 连接标签。
   对于标签，可以输入最长 255 个字符的文本字符串。可以使用除 `;` 字符外的任何字符。
4. 保存更改。

保护 Light Agent 和 SVM 之间的连接

您可以配置 Light Agent 和 Protection Server 之间的连接加密。为此，您需要在 SVM 上的 Protection Server 设置和 Light Agent 设置中启用 Light Agent 和 Protection Server 之间的数据通道加密。

启用了连接保护的 Light Agent 只能连接到在 Light Agent 与 Protection Server 之间启用了数据通道加密的 SVM。禁用了连接保护的 Light Agent 只能连接到禁用了通道加密或允许 Protection Server 与 Light Agent 之间建立不安全连接的 SVM。

有关在 Protection Server 上配置连接保护的详细信息，请参阅 Kaspersky Security for Virtualization Light Agent 帮助。

使用加密保护连接可能会降低 Kaspersky Security for Virtualization Light Agent 的性能。

如何在管理控制台(MMC) 中配置 Light Agent 中的连接保护

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **Light Agent 模式** → **连接保护**。
4. 选择**加密 Light Agent 与 Protection Server 之间的数据通道**复选框。
5. 保存更改。

如何在 Web Console 中配置 Light Agent 中的连接保护

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **Light Agent 模式** → **连接保护**。
5. 选择**加密 Light Agent 与 Protection Server 之间的数据通道**复选框。
6. 要将此策略应用到计算机，请关闭 挂锁图标并保存更改。

如何在应用程序界面中配置 Light Agent 中的连接保护

1. 打开主应用程序窗口并单击 按钮。
2. 在应用程序设置窗口的“**Light Agent 模式**”下，点击“**连接保护**”瓦片。
3. 选择**加密 Light Agent 与 Protection Server 之间的数据通道**复选框。
4. 保存更改。

激活 Light Agent

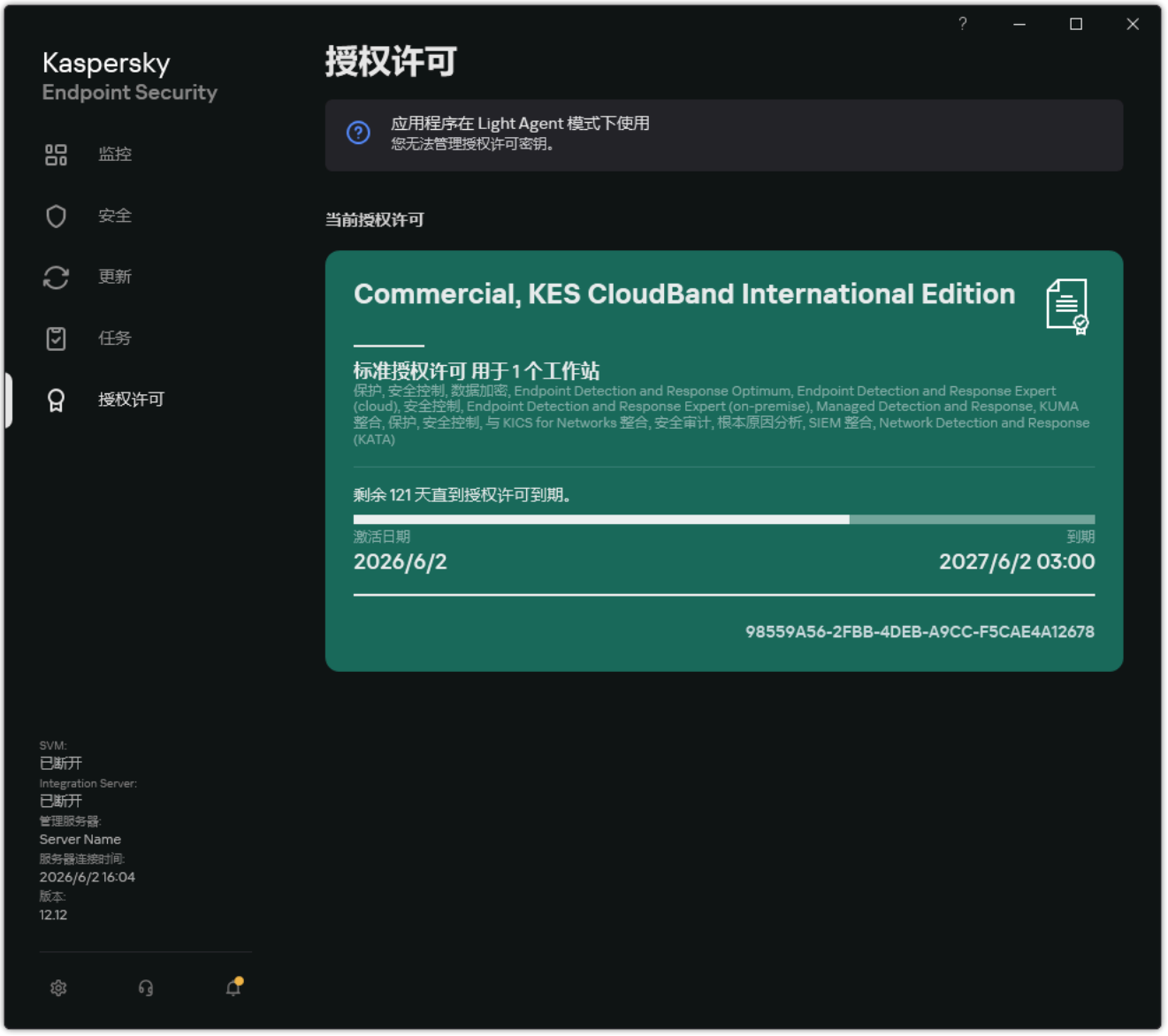
如果在 Light Agent 模式下使用 Kaspersky Endpoint Security 保护虚拟环境，则无需单独激活应用程序。要激活应用程序，您必须添加授权许可密钥到 SVM。您可以使用 Kaspersky Security Center 控制台中的特殊任务添加授权许可密钥到 SVM。您无法在 Light Agent 界面中管理授权许可密钥，但是您可以查看授权许可信息（见下图）。您还可以在命令行上查看 Light Agent 授权许可信息（请参阅下面的说明）。Light Agent 从 SVM 获取此信息。有关激活解决方案和管理授权许可密钥的详细信息，请参阅 Kaspersky Security for Virtualization Light Agent 帮助。

要查看 Light Agent 授权许可信息：

1. 以管理员身份运行命令行解释器 (cmd)。
2. 转到 Kaspersky Endpoint Security 可执行文件所在文件夹。
3. 运行以下命令：

```
avp.com LICENSE /CHECK
```

因此， Kaspersky Endpoint Security 会显示授权许可信息：Light Agent 连接到的 SVM 的地址、授权许可到期前的天数以及其他信息。如果您在激活 Light Agent 时遇到任何问题，请参阅技术支持知识库。



"授权许可"窗口

KSVLA Light Agent 至 KES Light Agent 迁移指南

Kaspersky Security for Virtualization 5.2 Light Agent 包含 Light Agent for Windows 5.2 组件（以下也称为“KSVLA Light Agent”）。在 Kaspersky Security for Virtualization Light Agent 6.2 中， Light Agent 模式下的 Kaspersky Endpoint Security 被用作 Light Agent 组件。要将解决方案更新至 6.2 版，您必须从 KSVLA Light Agent 5.2 迁移至 Light Agent 模式下的 Kaspersky Endpoint Security （以下也称为“KES Light Agent”）。有关更新 Kaspersky Security for Virtualization Light Agent 解决方案版本的详细信息，请参阅 Kaspersky Security for Virtualization Light Agent 帮助。

软件要求

在开始从 KSVLA Light Agent 迁移到 KES Light Agent 之前，请确保您的虚拟机满足 Kaspersky Endpoint Security for Windows 的硬件和软件要求。KES 和 KSWS 支持的操作系统版本列表不同。例如，KES 不支持运行 Windows Server 2003 的服务器。

从 KSVLA Light Agent 迁移至 KES Light Agent 的最低软件要求：

- Kaspersky Endpoint Security for Windows 12.8。
- Kaspersky Security for Virtualization Light Agent 6.2（包括 Protection Server 和 Integration Server 组件）。
- Kaspersky Security Center 14.2。

  如果您安装了早期版本的 Kaspersky Security Center，请将其更新到 14.2 或更高版本。在此版本的 Kaspersky Security Center 中，策略和任务批量转换向导可让您将策略迁移到配置文件中，而不是迁移到策略中。在此版本的 Kaspersky Security Center 中，策略和任务批量转换向导还允许您迁移范围更广的策略设置。

迁移步骤

从 KSVLA Light Agent 到 KES Light Agent 的迁移是半自动进行的。这是必要的，因为应用程序的体系结构不同。

按以下顺序从 KSVLA Light Agent 迁移到 KES Light Agent：

1. **迁移 KSVLA Light Agent 任务和策略**

   要迁移策略设置，您必须运行策略和任务批量转换向导（迁移向导）。迁移策略设置后，您必须手动配置迁移向导无法自动迁移的设置（例如，数据库更新设置）。迁移后，还建议检查迁移向导是否正确迁移了所有设置。

   如果启用密码保护来限制对 KSVLA Light Agent 的访问，则在安装 KES Light Agent 之前，您需要在 KSVLA Light Agent 的策略中禁用密码保护。您无法在 KES Light Agent 安装包设置中输入卸载密码。在 KSVLA Light Agent 上完成 KES Light Agent 的安装后，您必须在 KES 策略中启用密码保护。

2. **在 Light Agent 模式下安装 Kaspersky Endpoint Security**

您可以通过以下方式安装 KES Light Agent：

- 删除 KSVLA Light Agent 后安装 KES Light Agent（推荐）
- 在 KSVLA Light Agent 上安装 KES Light Agent

3. **确认应用程序在迁移后处于工作状态**

   从 KSVLA Light Agent 迁移到 KES Light Agent 后，确保应用程序正常运行。激活转换的策略。在 Kaspersky Security Center 控制台中查看虚拟机状态（应该是"*正常*"）。确保应用程序没有报告错误，还要检查上次连接到 SVM 的时间和虚拟机保护状态。你不需要激活 Light Agent，因为授权许可密钥已添加到 SVM。

安装 KES Light Agent 而不是 KSVLA Light Agent

您可以通过以下方式安装 KES Light Agent：

- 删除 KSVLA Light Agent 后安装 KES Light Agent（推荐）
- 在 KSVLA Light Agent 上安装 KES Light Agent

删除 KSVLA Light Agent

您可以在虚拟机本地，或在虚拟机模板中使用"*远程安装应用程序*"任务远程删除应用程序。删除 KSVLA Light Agent 后，您可能需要重新启动虚拟机。

移除 KSVLA Light Agent 后，使用任何合适的方法安装 KES Light Agent。

安装 Kaspersky Endpoint Security

> 如果启用密码保护来限制对 KSVLA Light Agent 的访问，则在安装 KES Light Agent 之前，您需要在 KSVLA Light Agent 的策略中禁用密码保护。您无法在 KES Light Agent 安装包设置中输入卸载密码。在 KSVLA Light Agent 上完成 KES Light Agent 的安装后，您必须在 KES 策略中启用密码保护。

安装 Kaspersky Endpoint Security 时，您必须选择"**用于保护虚拟环境的 Light Agent**"模式。在虚拟机上安装 KES Light Agent 之前，安装程序会将 KSVLA Light Agent 检测为不兼容的软件并将其删除。不支持 KSVLA Light Agent 配置的迁移。也就是说，当您安装 KES Light Agent 时，要安装的组件集由您在安装包属性或安装向导中的选择决定。删除 KSVLA Light Agent 后，必须重新启动虚拟机。

安装 KES Light Agent 时，KSVLA Light Agent 的设置和任务不会被迁移。要迁移设置和任务，请运行策略和任务批量转换向导。

您可以使用 `status` 命令在应用程序界面的"**安全**"区域或在"计算机属性"中的 Kaspersky Security Center 控制台中检查已安装组件的列表。您可以在安装后更改组件集，方法是使用*更改应用程序组件*。

KSVLA Light Agent 与 KES Light Agent 组件对应关系

KSVLA Light Agent 和 KES Light Agent 的组件集实际上相同。KES Light Agent 比 KSVLA Light Agent 具有更多设置。迁移后，新的设置具有默认值。

KSVLA Light Agent 与 KES Light Agent 组件对应关系

Light Agent 5.2	KES Light Agent
扫描内核	应用程序核心
文件反病毒	文件威胁防护
邮件反病毒	邮件威胁防护
Web 反病毒	Web 威胁防护
防火墙	防火墙
反网络攻击	网络威胁防护
应用程序权限控制	主机入侵防御
应用程序启动控制	应用程序控制
Web 控制	Web 控制
设备控制	设备控制
系统监控	在 Kaspersky Endpoint Security 中，该组件分为以下组件： • 漏洞利用防御 • 行为检测 • 修复引擎
系统完整性监控	系统完整性监控
与 Kaspersky Endpoint Agent 集成	*（不支持）* 从 Kaspersky Endpoint Security for Windows 11.9.0 开始，Kaspersky Endpoint Agent 分发包不再是分发包的一部分。
AMSI 保护	AMSI 保护

迁移 KSVLA Light Agent 任务和策略

您可以使用策略和任务批量转换向导（以下也称为“迁移向导”）迁移 KSVLA Light Agent 策略和任务的设置。

> KSVLA Light Agent 迁移向导仅在管理控制台（MMC）中可用。无法在 Web 控制台和云控制台中迁移策略和任务设置。

迁移策略和任务时需要特别注意以下事项：

- 新策略名为 *<策略>（已转换）*。
- 新策略具有*非活动策略*状态。
- 禁止修改设置（“挂锁”）不会被迁移。迁移向导设置默认值。
- 策略配置文件不会被迁移。您必须手动添加策略配置文件。

- 改进了受信任区域管理。在 KSVLA Light Agent 中，您只能在创建策略时添加预定义排除项。随后，在策略属性中，您可以配置之前添加的预定义排除项或手动添加排除项。您不能在策略属性中添加预定义的排除项。在 KES Light Agent 中，预定义排除项在策略创建期间以及所创建策略的属性中均可用。您还可以在安装包中选择预定义的排除项。

- Kaspersky Endpoint Security 中的应用程序用户界面的配置已从安装程序移至策略。例如，如果您需要隐藏应用程序的用户界面，管理策略设置。

- 在 Kaspersky Endpoint Security 和 KSVLA Light Agent 中配置基于权限的访问控制 (RBAC) 的功能集不同。您必须从头开始配置用户对功能区域的访问权限。

如何使用策略和任务批量转换向导迁移 KSVLA Light Agent 策略设置

1. 在管理控制台中，选择管理服务器并右键单击以打开上下文菜单。

2. 选择“**所有任务**” → “**策略和任务批量转换向导**”。

策略和任务批量转换向导将启动。按照向导的说明进行操作。

步骤 1. 选择您要转换其策略和任务的应用程序

在此步骤，您需要选择“Kaspersky Endpoint Security for Windows”。转到下一步。

步骤 2. 策略转换

选择要转换的 Kaspersky Security for Virtualization 5.2 Light Agent for Windows 策略。转到下一步。

然后，迁移向导将开始转换策略。在转换过程中，迁移向导会提示您接受 KSN 声明的条件。新策略名为 *<策略>（已转换）*。

步骤 3. 任务转换

迁移向导为 Kaspersky Endpoint Security for Windows 创建新任务。在任务列表中，选择要为 Kaspersky Endpoint Security 创建的 KSVLA Light Agent 任务。新任务将被命名为 *<任务名称> (转换)*。转到下一步。

步骤 4. 向导完成

退出向导。

迁移策略后，您必须打开该策略的属性，检查其设置并保存该策略。如果您不完成这些步骤，KES Light Agent 可能会忽略转换后的策略。

特别注意 Light Agent 的 SVM 连接设置、排除项列表、受信任应用程序、受信任网址、应用程序控制规则的迁移。

迁移 [KSVLA Light Agent+KEA] 配置到 [KES Light Agent+内置代理] 配置

要支持使用 Kaspersky Endpoint Security for Windows 作为 EDR（KATA）、EDR Optimum、Kaspersky Sandbox 的一部分，内置代理已添加到应用程序中。使用这些解决方案您不再需要单独的 Kaspersky Endpoint Agent 应用程序。

从 KSVLA Light Agent 迁移到 KES Light Agent 时，EDR（KATA）、EDR Optimum、Kaspersky Sandbox 解决方案继续与 Kaspersky Endpoint Security 内置代理协同工作。此外，Kaspersky Endpoint Agent 将被从计算机卸载。

从 KSVLA Light Agent 迁移到 KES Light Agent 之前，您必须将 Kaspersky Security for Virtualization 的所有组件更新至版本 6.2，包括 Protection Server 和 Integration Server。有关更新 Kaspersky Security for Virtualization Light Agent 解决方案版本的详细信息，请参阅 Kaspersky Security for Virtualization Light Agent 帮助。

迁移 [KSVLA Light Agent+KEA] 配置到 [KES Light Agent+内置代理] 配置涉及以下步骤：

1. **迁移策略和任务**

   迁移 [KSVLA Light Agent+KEA] 策略和任务到 [KES Light Agent+内置代理] 需要以下步骤：

   1. 使用策略和任务批量转换向导将策略和任务从 KSVLA Light Agent 迁移到 KES Light Agent（仅在管理控制台 (MMC) 上可用）。

      因此，将创建一个名为“*<策略>（已转换）*”的新策略。还创建了新的名为“*<任务名称>（已转换）*”的 KES 任务。

   2. 使用用于从 Kaspersky Endpoint Agent 迁移的向导将策略和任务从 KEA 迁移到 KES（仅在 Web Console 和云控制台上可用）。

      结果，创建了一个名为 *<Kaspersky Endpoint Security 策略名称>&<Kaspersky Endpoint Agent 策略名称>*的新策略。还创建了新任务和 KES 任务。

2. **从 KSVLA Light Agent 迁移至 KES Light Agent**

   从 KSVLA Light Agent 迁移到 KES Light Agent 涉及安装 KES Light Agent 而不是 KSVLA Light Agent。

管理员通常启用密码保护以限制对 KSVLA Light Agent 和 KEA 的访问。您只能在“*远程安装应用程序*”任务的属性中输入 KEA 卸载密码。为了进行迁移，您必须禁用 KSVLA Light Agent 的密码保护。

要执行迁移，您必须选择支持 Detection and Response 解决方案所需的组件作为 Kaspersky Endpoint Security 的一部分。安装应用程序后，Kaspersky Endpoint Security 切换到使用内置代理并卸载 Kaspersky Endpoint Agent。

3. **授权许可功能**

   如果在 Light Agent 模式下使用应用程序，则无需激活应用程序。要激活应用程序，您必须添加授权许可密钥到 SVM。您还必须向 SVM 添加用于激活附加功能（例如，EDR Optimum）的授权许可密钥。也就是说，作为迁移的一部分，功能授权许可会自动进行。

4. **检查 Kaspersky Endpoint Detection and Response Optimum 和 Kaspersky Sandbox 的健康**

   升级之后，计算机在 Kaspersky Security Center 控制台显示*严重*状态：

   - 确保计算机安装了网络代理版本 13.2 或更高版本。
   - 通过查看“*应用程序组件状态报告*”检查内置代理的操作状态。如果组件具有*未安装*状态，使用“*更改应用程序组件*”任务安装组件。
   - 确保您在 Kaspersky Endpoint Security for Windows 的新策略中接受了卡巴斯基安全网络声明。
   - 确保使用以下方式激活 EDR Optimum 功能：*应用程序组件状态报告*。如果组件具有“*授权许可不支持*”状态，确保 EDR Optimum 的授权许可密钥自动分发功能已关闭。
   - 检查虚拟机与 SVM 的连接状态。您可以在 Kaspersky Endpoint Security 中获取有关 Light Agent 与 SVM 的连接状态的信息，也可以使用应用程序命令。

从命令行管理应用程序

您可以从命令行管理 Kaspersky Endpoint Security。您可以通过运行 `avp.com HELP` 命令来查看用于管理应用程序的命令列表。要阅读特定命令的语法，请输入 `avp.com HELP <command>`。

命令中的特殊字符必须转义。要转义字符 `&`、`|`、`(`,`)`、`<`、`>`、`^`，请使用 `^` 字符（例如，要使用 `&` 字符，输入 `^&`）。要转义 `%` 字符，输入 `%%`。

`1` 值的替代值可为 `yes`, `on`, `enable`, `enabled` 和 `true`。`0` 值的替代值可为 `no`, `off`, `disable`, `disabled` 和 `false`。

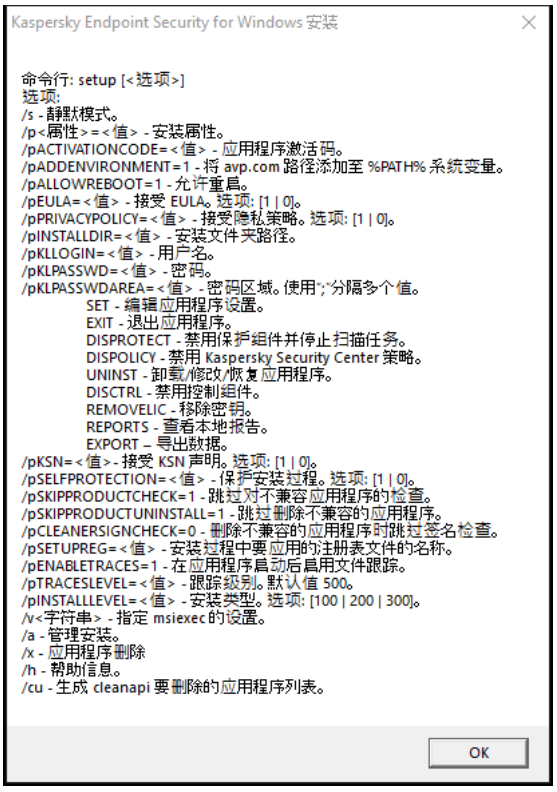
Setup。安装应用程序

可以在以下模式之一下从命令行安装 Kaspersky Endpoint Security：

- 使用应用程序安装向导互动模式。
- 在静默模式下。以静默模式启动安装后，安装过程不再需要您的参与（静默安装）。要在静默模式下安装应用程序，请使用 `/s` 和 `/qn` 键。

  在静默模式下安装应用程序之前，请打开并阅读最终用户授权许可协议和隐私策略文本。最终用户授权许可协议和隐私策略文本包含在 Kaspersky Endpoint Security 分发包中。只有在您已经完全阅读、理解和接受最终用户授权许可协议的规定和条款，理解并同意您的数据将按照隐私策略进行处理和传输（包括传输到第三方国家/地区），并且您已经完全阅读和理解隐私策略的情况下，您才可以继续安装应用程序。如果您不接受最终用户授权许可协议的规定和条款以及隐私策略，请不要安装或使用 Kaspersky Endpoint Security。

您可以通过运行 /h 命令来查看用于安装应用程序的命令列表。要获得安装命令语法的帮助，请输入 setup_kes.exe /h。因此，安装程序将显示一个窗口，其中包含命令选项的说明（请参见下图）。



安装命令选项说明

要安装应用程序或升级以前版本的应用程序：

1. 以管理员身份运行命令行解释器 (cmd.exe)。
2. 转到 Kaspersky Endpoint Security 分发包所在文件夹。
3. 运行以下命令：

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 [/pKSN=1|0] [/pCONFIGPATH=<path to the configuration file>]
[/pALLOWREBOOT=1] [/pSKIPPRODUCTCHECK=1] [/pSKIPPRODUCTUNINSTALL=1] [/pKLLOGIN=<user name> /pKLPASSWD=
<password> /pKLPASSWDAREA=<password scope>] [/pENABLETRACES=1|0 /pTRACESLEVEL=<tracing level>]
[/pSKIPKB5007186CHECK=1] [/s]
```

或

```
msiexec /i <distribution kit name> EULA=1 PRIVACYPOLICY=1 [KSN=1|0] [CONFIGPATH=<path to the configuration
file>] [ALLOWREBOOT=1] [SKIPPRODUCTCHECK=1] [KLLOGIN=<user name> KLPASSWD=<password> KLPASSWDAREA=<password
scope>] [ENABLETRACES=1|0 TRACESLEVEL=<tracing level>] [SKIPKB5007186CHECK=1] [/qn]
```

至此，应用程序被安装在计算机上。您可以通过发出status命令确认应用程序已安装并检查应用程序设置。

EULA=1	接受最终用户授权许可协议的条款。许可协议的内容包括在 Kaspersky Endpoint Security 分发套装中。 必须接受最终用户授权许可协议的条款才能安装应用程序或升级应用程序版本。
PRIVACYPOLICY=1	接受隐私策略。隐私策略的文本包含在 Kaspersky Endpoint Security 分发包中。 要安装应用程序或升级应用程序版本，您必须接受隐私策略。
KSN	接受或拒绝参与卡巴斯基安全网络（KSN）。如果没有为此参数设置任何值，在首次启动 Kaspersky Endpoint Security 时，Kaspersky Endpoint Security 将提示您确认同意或拒绝加入 KSN。可用值： • 1 – 同意加入 KSN。 • 0 – 拒绝加入 KSN（默认值）。 Kaspersky Endpoint Security 分发包已针对与卡巴斯基安全网络（KSN）配合使用进行优化。如果您选择不加入卡巴斯基安全网络，则应该在安装完成后立即更新 Kaspersky Endpoint Security。
CONFIGPATH=<path to the configuration file>	使用预定义设置安装应用程序。为此，您需要上传定义了 Kaspersky Endpoint Security 设置的文件。您可以在应用程序的本地界面中创建配置文件。
ALLOWREBOOT=1	自动重新启动计算机（如果安装或升级应用程序后需要重新启动）。如果未为此参数设置任何值，则阻止计算机自动重启。 安装 Kaspersky Endpoint Security 时，不需要重新启动。仅当在安装前必须删除不兼容的应用程序时，才需要重新启动。更新应用程序版本时也可能需要重新启动。
SKIPPRODUCTCHECK=1	禁用已安装软件检查。可能导致兼容性问题的软件列表位于分发包中的 incompatible.txt 文件中。如果没有为该参数设置值并且检测到来自列表的软件，则将终止 Kaspersky Endpoint Security 的安装。
SKIPPRODUCTUNINSTALL=1	禁用从 incompatible.txt 列表中自动删除检测到的软件。如果没有为此参数设置任何值，则 Kaspersky Endpoint Security 将尝试删除可能导致兼容性问题的软件。 使用 msiexec 安装程序安装 Kaspersky Endpoint Security 时，无法启用软件的自动删除。要自动删除可能导致兼容性问题的软件，请使用 setup_kes.exe 文件。
CLEANERSIGNCHECK=0|1	验证 incompatible.txt 列表中检测到的软件文件的数字签名。要删除该软件，Kaspersky Endpoint Security 会运行软件安装程序文件。如果安装程序文件没有数字签名，Kaspersky Endpoint Security 会认为该文件不受信任，并停止软件卸载，以避免运行潜在的恶意代码。如果应用程序无法验证检测到的软件文件的数字签名，Kaspersky Endpoint Security 安装将停止并出现错误。 默认值因软件安装方法而异： • 0 表示禁用了数字签名验证（如果通过 Kaspersky Security Center 部署，则为默认值）。 • 1 表示启用了数字签名验证（如果应用程序正在本地安装，则为默认值）。
STANDALONEMODE=1	在 Endpoint Detection and Response Agent (EDR Agent) 配置下安装应用程序，用于与 Kaspersky Endpoint Detection and Response (KATA) 或 Kaspersky Endpoint Detection and Response Expert（本地部署）解决方案集成。如果有 第三方端点保护平台 (EPP) 和 Kaspersky Endpoint Detection and Response 解决方案一起部署在您的组织中，则需要此配置。这使得在 Endpoint Detection and Response Agent 配置下的 Kaspersky Endpoint Security 与第三方 EPP 应用程序兼容。
KLLOGIN	设置用于访问 Kaspersky Endpoint Security 功能和设置的用户名（“密码保护”组件）。该用户名与“KLPASSWD”和“KLPASSWDAREA”设置一起进行设置。默认使用用户名 KLAdmin。
KLPASSWD	指定用于访问 Kaspersky Endpoint Security 功能和设置的密码（该密码与“KLLOGIN”和“KLPASSWDAREA”参数一起指定）。 如果您指定了口令，但没有指定带有 KLLOGIN 参数的用户名，将默认使用 KLAdmin 用户名。

KLPASSWDAREA	指定用于访问 Kaspersky Endpoint Security 的密码范围。当用户尝试执行包含在此范围中的操作时，Kaspersky Endpoint Security 将提示用户输入账户凭据（“KLLOGIN”和“KLPASSWD”参数）。使用“;”字符以指定多个值。 可用值： • SET – 修改应用程序设置。 • EXIT – 退出应用程序。 • DISPROTECT – 禁用保护组件并停止扫描任务。 • DISPOLICY – 禁用 Kaspersky Security Center 策略。 • UNINST – 从计算机中删除应用程序。 • DISCTRL – 禁用控制组件。 • REMOVELIC – 删除密钥。 • REPORTS – 查看报告。 • EXPORT – 导出应用程序设置。 例如，KLPASSWDAREA=SET;KLPASSWDAREA=UNINST;KLPASSWDAREA=EXIT。 KLAdmin 账户有权执行任何受密码保护的操作。因此，配置 KLAdmin 账户的密码范围是不可能的。如果您尝试为 KLAdmin 账户配置密码范围，应用程序将禁止“Everyone”组执行指定的操作。
PROTECTOSSERVICES	保护操作系统服务功能。操作系统服务保护防止第三方应用程序干扰操作系统服务的操作。例如，这样的服务包括应用程序自动启动服务。 • 1 表示操作系统服务的保护已启用（默认值）。 • 0 表示操作系统服务的保护被禁用。
ENABLETRACES	启用或禁用应用程序跟踪。Kaspersky Endpoint Security 在启动后将跟踪文件保存在文件夹 %ProgramData%\Kaspersky Lab\KES.14.1\Traces 中。可用值： • 1 – 启用跟踪。 • 0 – 禁用跟踪（默认值）。
TRACESLEVEL	跟踪详细级别。可用值： • 100（关键）。仅包含有关致命错误的消息。 • 200（高）。有关所有错误的消息，包括致命错误。 • 300（诊断）。有关所有错误的消息以及警告。 • 400（重要）。所有错误消息、警告和其他信息。 • 500（常规）。有关所有错误的消息和警告，以及有关正常模式下应用程序操作的详细信息（默认）。 • 600（低）。所有消息。
ENABLEAZURESUPPORT	启用或禁用 Azure WVD 兼容模式。可用值： • 1 – 启用 Azure WVD 兼容模式。 • 0 – 禁用 Azure WVD 兼容模式（默认值）。 此功能可确保在 Kaspersky Anti Targeted Attack Platform 控制台中正确显示 Azure 虚拟机状态。为了监控计算机的性能，Kaspersky Endpoint Security 将遥测数据发送到 KATA 服务器。遥测包括计算机的 ID（Sensor ID）。Azure WVD 兼容模式允许为这些虚拟机分配永久唯一的 Sensor ID。如果关闭兼容模式，由于 Azure 虚拟机的工作方式，Sensor ID 可能会在计算机重新启动后发生变化。这可能会导致控制台上出现重复的虚拟机。
AMPPL	启用或禁用 Kaspersky Endpoint Security 进程使用 AM-PPL 技术（Antimalware Protected Process Light）提供的保护。有关 AM-PPL 技术的详细信息，请访问 Microsoft 网站。 AM-PPL 技术适用于 Windows 10 版本 1703 (RS2) 或更高版本以及 Windows Server 2019 操作系统。 可用值： • 1 – 启用 Kaspersky Endpoint Security 进程使用 AM-PPL 技术提供的保护。 • 0 – 禁用 Kaspersky Endpoint Security 进程使用 AM-PPL 技术提供的保护。
UPGRADEMODE	应用程序升级模式： • Seamless 意味着通过计算机重启升级应用程序（默认值）。 • Force 意味着在不重新启动的情况下升级应用程序。 从 11.10.0 版开始，无需重新启动即可升级应用程序。要升级应用程序的早期版本，必须重新启动计算机。从 11.11.0 版开始，您也可以无需重新启动即可安装补丁。 安装 Kaspersky Endpoint Security 时，不需要重新启动。因此，应用程序的升级模式将在应用程序设置中指定。您可以在应用程序设置或策略中更改此参数。 升级已安装的应用程序时，命令行参数的优先级低于应用程序设置或 setup.ini 文件中指定的参数的优先级。例如，如果在命令行中指定了“Force”升级模式，而在应用程序设置中指定了“Seamless”模式，则升级将在计算机重新启动时安装（Seamless）。

RESTAPI	通过 REST API 管理应用程序。要通过 REST API 管理应用程序，必须指定用户名（RESTAPI_User 参数）。 可用值： • 1 –允许通过 REST API 进行管理。 • 0 –阻止通过 REST API 进行管理（默认值）。 要通过 REST API 管理应用程序，必须允许使用管理系统进行管理。要执行此操作，请设置 AdminKitConnector=1 参数。如果通过 REST API 管理应用程序，则无法使用 Kaspersky 的管理系统来管理应用程序。
RESTAPI_User	用于通过 REST API 管理应用程序的 Windows 域账户的用户名。只有此用户可以通过 REST API 管理应用程序。输入格式为 <DOMAIN>\<UserName> 的用户名（例如，RESTAPI_User=COMPANY\Administrator）。您只能选择一个用户来使用 REST API。 添加用户名是通过 REST API 管理应用程序的先决条件。
RESTAPI_Port	用于通过 REST API 管理应用程序的端口。默认情况下使用 6782 端口。确保端口空闲。
RESTAPI_Certificate	识别请求的证书（例如，RESTAPI_Certificate=C:\cert.pem）。Kaspersky Endpoint Security 与 REST 客户端的安全交互需要配置请求标识。为此，您必须安装证书，然后对每个请求的有效负载进行签名。
ADMINKITCONNECTOR	使用管理系统管理应用程序。例如，管理系统包括 Kaspersky Security Center。除了 Kaspersky 管理系统，您还可以使用第三方解决方案。Kaspersky Endpoint Security 为此提供了一个 API。 可用值： • 1 - 允许在管理系统的帮助下管理应用程序（默认值）。 • 0 - 仅允许通过本地界面管理应用程序。
EnableUniqueSensorID	在安装或更新应用程序期间创建唯一的计算机标识符 (Sensor ID)。Sensor ID 在 Kaspersky Anti Targeted Attack Platform 解决方案中用于识别向服务器发送遥测数据的计算机。在创建 Sensor ID 时，应用程序使用一种考虑到计算机配置（例如主板序列号）的算法。在某些情况下，例如在虚拟环境中使用应用程序时，Sensor ID 可能会重复。因此，Kaspersky Anti Targeted Attack Platform 无法识别发送遥测数据的计算机。要创建唯一的 Sensor ID，您需要设置参数 EnableUniqueSensorID=1。因此，应用程序将使用不同的算法来创建 Sensor ID，该算法会考虑有关计算机的其他数据。这确保了 Sensor ID 的唯一。 默认情况下，没有设置该参数。应用程序在以下情况下继承 Sensor ID： • 更新应用程序版本； • 迁移 [KES+KEA] 配置到 [KES+内置代理] 配置 作为应用程序修复的一部分，安装程序尝试继承 Sensor ID。如果 Sensor ID 无法恢复，应用程序会创建一个新的 Sensor ID。
SKIPKB5007186CHECK=1	禁用对已安装的操作系统更新 KB5007186 的检查。 在安装应用程序之前，安装程序会检查已安装的操作系统更新。KB5007186 更新位于可能导致应用程序出现问题的操作系统更新列表中。有关详细信息，请参阅技术支持知识库。因此，如果发现此更新，安装程序将中止安装。要继续安装，请设置 SKIPKB5007186CHECK=1。

示例

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1
```

```
msiexec /i kes_win.msi EULA=1 PRIVACYPOLICY=1 KSN=1 KLLOGIN=Admin KLPASSWD=Password
KLPASSWDAREA=EXIT;DISPOLICY;UNINST /qn
```

```
setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pENABLETRACES=1 /pTRACESLEVEL=600 /s
```

安装 Kaspersky Endpoint Security 后，将激活试用版授权许可，除非您在 setup.ini 文件中提供了激活码。试用版授权许可通常拥有较短的有效期。当试用版授权许可过期时，所有 Kaspersky Endpoint Security 功能都将被禁用。要继续使用应用程序，您需要使用应用程序激活向导或特殊命令以商业授权许可激活应用程序。

以静默模式安装应用程序或升级应用程序版本时，支持以下文件的使用：

- setup.ini – 应用程序安装的常规设置。

  要应用 setup.ini 文件中的设置，请将该文件放入包含 Kaspersky Endpoint Security 分发包的文件夹。

- install.cfg – Kaspersky Endpoint Security 的运行设置

  要应用 install.cfg 配置文件中的设置，您需要在以下应用程序安装命令中指定文件路径：`CONFIGPATH=<path to the configuration file>`。

- setup.reg – 注册表项。

  只有在 setup.ini 文件中为 `SetupReg` 参数设置 `setup.reg` 值时，setup.reg 文件中的注册表项才会写入注册表。setup.reg 文件由卡巴斯基专家生成。不建议修改该文件的内容。要应用 setup.reg 文件中的设置，请将该文件放入包含 Kaspersky Endpoint Security 分发包的文件夹。您也可以放置 setup.reg 文件到不同的文件夹。如果这样，您需要在以下应用程序安装命令中指定文件路径：`SETUPREG=<path to the setup.reg file>`。

Setup /x。卸载应用程序

可以通过以下方式之一从命令行卸载 Kaspersky Endpoint Security：

- 使用应用程序安装向导互动模式。
- 在静默模式下。以静默模式启动卸载后，卸载过程不再需要您的参与（静默卸载）。要在静默模式下卸载应用程序，请使用 `/s` 和 `/qn` 开关。

要在静默模式下卸载应用程序：

1. 以管理员身份运行命令行解释器 (cmd.exe)。
2. 转到 Kaspersky Endpoint Security 分发包所在文件夹。
3. 运行以下命令：

   - 如果卸载过程没有密码保护：

     ```
     setup_kes.exe /s /x
     ```

     或

     ```
     msiexec.exe /x <GUID> /qn
     ```

     `<GUID>` 是应用程序的唯一 ID。您可以在技术支持知识库或使用以下命令找到应用程序的 GUID：

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
     ```

   - 如果卸载过程有密码保护：

     ```
     setup_kes.exe /pKLLOGIN=<user name> /pKLPASSWD=<password> /s /x
     ```

     或

     ```
     msiexec.exe /x <GUID> KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

您还可以使用 SAVEQB 参数来保存应用程序扫描的文件并放置在备份中。文件的备份副本存储在 C:\ProgramData\Kaspersky Lab\KES.14.1\QB 文件夹中。默认情况下，保存文件到备份中是禁用的（SAVEQB=0）。

示例

```
msiexec.exe /x {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

msiexec /i。恢复应用程序

恢复时，应用程序会检查并恢复所有损坏的应用程序模块和在应用程序安装过程中创建的系统注册表键的完整性。

可以在以下模式之一下从命令行恢复 Kaspersky Endpoint Security：

- 使用应用程序安装向导互动模式。
- 在静默模式下。以静默模式启动恢复后，恢复过程不再需要您的参与。

如果 Kaspersky Endpoint Security 安装程序在恢复模式下运行，并且应用程序不需要恢复，则安装程序不会进行任何更改。

如果 Kaspersky Endpoint Security 安装程序在恢复模式下运行，并且应用程序未安装，则安装程序将启动安装过程。

要在静默模式下恢复应用程序：

1. 以管理员身份运行命令行解释器 (cmd.exe)。
2. 转到 Kaspersky Endpoint Security 分发包所在文件夹。
3. 运行以下命令：
   - 如果恢复过程没有密码保护：

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL /qn
     ```

     <GUID> 是应用程序的唯一 ID。您可以在技术支持知识库或使用以下命令找到应用程序的 GUID：

     ```
     wmic product where "Name like '%Kaspersky Endpoint Security%'" get Name, IdentifyingNumber
     ```

   - 如果恢复过程有密码保护：

     ```
     msiexec.exe /i <GUID> REINSTALL=ALL KLLOGIN=<user name> KLPASSWD=<password> /qn
     ```

示例

```
msiexec.exe /i {9A017278-F7F4-4DF9-A482-0B97B70DD7ED} REINSTALL=ALL KLLOGIN=KLAdmin KLPASSWD=samplePassword /qn
```

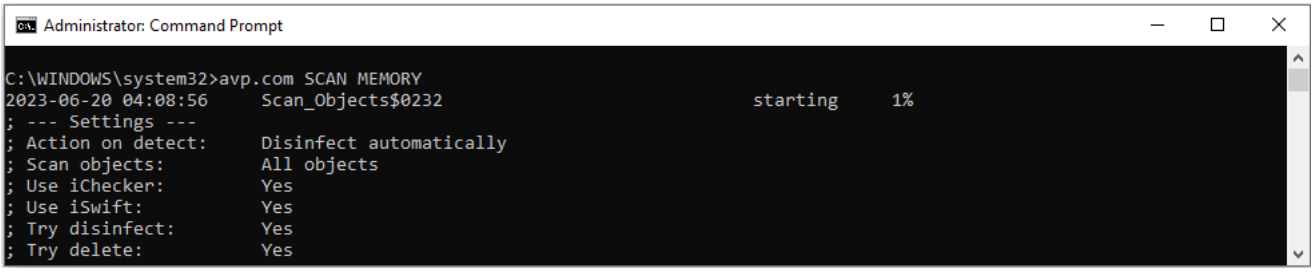
AVP 命令

要从命令行管理 Kaspersky Endpoint Security：

1. 以管理员身份运行命令行解释器 (cmd.exe)。
2. 转到 Kaspersky Endpoint Security 可执行文件所在文件夹。
   您可以在应用程序安装期间将可执行文件的路径添加到 %PATH% 系统变量中。
3. 使用以下模板执行命令：

   ```
   avp.com <command> [options]
   ```

   结果，Kaspersky Endpoint Security 将执行该命令（参见下图）。



从命令行管理应用程序

SCAN。恶意软件扫描

运行“*恶意软件扫描*”任务。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com SCAN [<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>] [/C:<file with scan settings>]
```

扫描范围	
`<files to scan>`	以空格分隔的文件和文件夹列表。长路径必须用引号括起来。短路径（MS-DOS 格式）不需要用引号括起来。例如： • `"C:\Program Files (x86)\Example Folder"` – 长路径。 • `C:\PROGRA~2\EXAMPL~1` – 短路径。

/ALL	运行"*恶意软件扫描*"任务。Kaspersky Endpoint Security 扫描以下对象： • 内核内存 • 操作系统启动时加载的对象 • 引导扇区 • 操作系统备份 • 所有硬盘和可移动驱动器 在 Kaspersky Endpoint Security for Windows 12.12 中，电子邮件被排除在应用程序扫描范围之外。对传入和传出电子邮件的扫描由邮件威胁防护组件执行。如果您使用的是较早版本的管理插件，即使策略中包含电子邮件，该应用程序也会将电子邮件排除在扫描范围之外。
/MEMORY	扫描内核内存
/STARTUP	扫描在操作系统启动时加载的对象
/REMDRIVES	扫描可移动驱动器。
/FIXDRIVES	扫描硬盘驱动器。
/NETDRIVES	扫描网络驱动器。
/QUARANTINE	扫描 Kaspersky Endpoint Security 备份区中的文件。
/@:<file list.lst>	扫描列表中的文件和文件夹。列表中的每个文件都必须另起一行。长路径必须用引号括起来。短路径（MS-DOS 格式）不需要用引号括起来。例如： • "C:\Program Files (x86)\Example Folder" – 长路径。 • C:\PROGRA~2\EXAMPL~1 – 短路径。

检测到威胁后的操作	
/i0	"**通知**"。如果选择此选项，Kaspersky Endpoint Security 会在检测到受感染文件时将这些文件的相关信息添加到活动威胁列表。
/i1	"**清除；如果清除失败则通知**"。如果选择该选项，Kaspersky Endpoint Security 将自动尝试对已经检测到的所有受感染的文件执行清除操作。如果清除失败，Kaspersky Endpoint Security 会将检测到的受感染文件的相关信息添加到活动威胁列表。
/i2	"**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。 默认情况下已选择此操作。
/i3	"**清除失败则删除**"。如果无法清除或删除已感染文件，还会删除复合文件（例如，存档）。
/i4	"**删除**"。如果无法删除已感染文件，还会删除复合文件（例如，存档）。

文件类型	
/fe	"**按扩展名扫描文件**"。如果启用该设置，则应用程序仅扫描被感染的文件。此时，系统将根据文件的扩展名确定文件格式。
/fi	"**按格式扫描文件**"。如果启用该设置，则应用程序仅扫描被感染的文件。在扫描文件以查找恶意代码之前，系统将分析文件的内部头以确定文件的格式（例如，.txt、.doc 或 .exe）。该扫描也查找具有特殊文件扩展名的文件。
/fa	"**所有文件**"。如果启用该设置，应用程序将毫无例外地扫描所有文件（所有格式和扩展名）。 这是默认设置。

扫描排除项	
-e:a	RAR、ARJ、ZIP、CAB、LHA、JAR 和 ICE 压缩文件将从扫描范围中排除。
-e:<file mask>	与文件掩码匹配的文件将从扫描范围中排除。例如： • 掩码 *.exe 将包括具有 exe 扩展名的文件的所有路径。 • 掩码 example* 将包括名为 EXAMPLE 的文件的所有路径。

-e:<seconds>	扫描时间长于指定时间限制（以秒为单位）的文件将从扫描范围中排除。
-es:<megabytes>	大于指定大小限制（以兆字节为单位）的文件将从扫描范围中排除。

将事件保存到报告文件模式（仅适用于扫描、更新和回滚配置文件）	
/R:<report file>	仅将关键事件保存到报告文件中。
/RA:<report file>	将所有事件保存到报告文件中。

扫描技术	
/iChecker=on|off	该技术允许通过排除特定文件不扫描的方式提高扫描速度。该技术将使用特殊算法将文件排除在扫描范围之外，该算法会考虑 Kaspersky Endpoint Security 数据库的发布日期、文件的上次扫描日期以及对扫描设置的任何修改。iChecker 技术受到一些限制：它无法操作大型文件，并且仅能应用于具有应用程序可识别结构的文件（例如：EXE、DLL、LNK、TTF、INF、SYS、COM、CHM、ZIP 和 RAR）。
/iSwift=on|off	该技术允许通过排除特定文件不扫描的方式提高扫描速度。该技术将使用特殊算法将文件排除在扫描范围之外，该算法会考虑 Kaspersky Endpoint Security 数据库的发布日期、文件的上次扫描日期以及对扫描设置的任何修改。iSwift 技术是对用于 NTFS 文件系统的 iChecker 技术的增强版。

高级设置	
/C:<file with scan settings>	包含“*恶意软件扫描*”任务设置的文件。必须手动创建该文件并以 TXT 格式保存。该文件可以具有以下内容：[<scan scope>] [<action on threat detection>] [<file types>] [<scan exclusions>] [/R[A]:<report file>] [<scan technologies>]。

示例

```
avp.com SCAN /R:log.txt /MEMORY /STARTUP "C:\Documents and Settings\All Users\My Documents" "C:\Program Files"
```

UPDATE。更新数据库和程序软件模块

运行“*数据库和应用程序模块更新*”任务。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

> 如果应用程序安装在 Light Agent 模式，此命令无法运行。

命令语法

```
avp.com UPDATE [local] ["<update source>"] [/R[A]:<report file>] [/C:<file with update settings>]
```

更新任务设置	
local	应用程序安装后自动创建的“*数据库和应用程序模块更新*”任务的启动。您可以在本地应用程序界面或在 Kaspersky Security Center 控制台更改“*数据库和应用程序模块更新*”任务的设置。如果该设置未被配置，Kaspersky Endpoint Security 使用默认设置或命令中指定的设置启动“*数据库和应用程序模块更新*”任务。您可以如下配置“*数据库和应用程序模块更新*”任务设置： • UPDATE 用默认设置启动“*数据库和应用程序模块更新*”任务：更新源是卡巴斯基更新服务器，账户是 System，和其它默认设置。 • UPDATE local 启动安装后自动创建的“*数据库和应用程序模块更新*”任务（预定义任务）。 • UPDATE <update settings> 用手动定义的设置启动“*数据库和应用程序模块更新*”任务（见下文）。

更新源	
"<update source>"	HTTP 或 FTP 服务器的地址，或具有更新包的共享文件夹的地址。只能指定一个更新源。如果更新源未指定，Kaspersky Endpoint Security 使用默认源：卡巴斯基更新服务器。

将事件保存到报告文件模式（仅适用于扫描、更新和回滚配置文件）	
/R:<report file>	仅将关键事件保存到报告文件中。
/RA:<report file>	将所有事件保存到报告文件中。

高级设置	
/C:<file with update settings>	包含*"数据库和应用程序模块更新"*任务设置的文件。必须手动创建该文件并以 TXT 格式保存。该文件可以具有以下内容：["<update source>"] [/R[A]:<report file>]。

示例

```
avp.com UPDATE local
```

```
avp.com UPDATE "ftp://my_server/kav updates" /RA:avbases_upd.txt
```

ROLLBACK。上次更新回滚

回滚上次反病毒数据库更新。这允许您在必要时将数据库和应用程序模块回滚到以前的版本，例如，当新数据库版本包含无效签名而导致 Kaspersky Endpoint Security 阻止了安全的应用程序时。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

如果应用程序安装在 Light Agent 模式，此命令无法运行。

命令语法

```
avp.com ROLLBACK [/R[A]:<report file>]
```

将事件保存到报告文件模式（仅适用于扫描、更新和回滚配置文件）	
/R:<report file>	仅将关键事件保存到报告文件中。
/RA:<report file>	将所有事件保存到报告文件中。

示例

```
avp.com ROLLBACK /RA:rollback.txt
```

TRACES。跟踪

只要应用程序在使用中，就会在计算机中存储跟踪文件，当应用程序被删除后，跟踪文件将被永久删除。跟踪文件（身份验证代理的跟踪文件除外）存储在 %ProgramData%\Kaspersky Lab\KES.14.1\Traces 文件夹中。默认情况下，禁用跟踪。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com TRACES on|off [<tracing level>] [<advanced settings>]
```

跟踪级别	
`<tracing level>`	跟踪详细级别。可用值： • `100`（关键）。仅包含有关致命错误的消息。 • `200`（高）。有关所有错误的消息，包括致命错误。 • `300`（诊断）。有关所有错误的消息以及警告。 • `400`（重要）。所有错误消息、警告和其他信息。 • `500`（常规）。有关所有错误的消息和警告，以及有关正常模式下应用程序操作的详细信息（默认）。 • `600`（低）。所有消息。

高级设置	
`all`	使用“`file`”和“`mem`”参数运行命令。
`file`	保存一个跟踪文件（无大小限制）。
`rot`	将跟踪保存到有限数量的大小有限的文件集中，并在达到最大大小时覆盖旧文件。
`mem`	将跟踪保存到 dump 文件。

示例

```
avp.com TRACES on 500
```

```
avp.com TRACES off
```

```
avp.com TRACES on 500 mem
```

```
avp.com TRACES off file
```

START。启动配置文件

启动配置文件（例如，开始更新数据库或启用保护组件）。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com START <profile> [/R[A]:<report file>]
```

配置文件	
`<profile>`	配置文件名称。*配置文件*是 Kaspersky Endpoint Security 组件、任务或功能。您可以通过运行 `HELP START` 命令来查看可用配置文件列表。

将事件保存到报告文件模式（仅适用于扫描、更新和回滚配置文件）	
/R:<report file>	仅将关键事件保存到报告文件中。
/RA:<report file>	将所有事件保存到报告文件中。

示例

```
avp.com START Scan_Objects
```

STOP。停止配置文件

停止配置文件执行（例如，停止可移动驱动器扫描或禁用保护组件）。

> 要执行此命令，必须启用密码保护。用户必须具有“**禁用保护组件**”和“**禁用控制组件**”权限。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com STOP <profile> /login=<user name> /password=<password>
```

配置文件	
<profile>	配置文件名称。*配置文件*是 Kaspersky Endpoint Security 组件、任务或功能。您可以通过运行 `HELP STOP` 命令来查看可用配置文件列表。

身份验证	
/login=<user name> /password=<password>	带有所需密码保护权限的用户账户凭证。

STATUS。配置文件状态

显示应用程序配置文件的状态信息（例如，“`running`”或“`completed`”）。您可以运行 `HELP STATUS` 命令来查看可用配置文件列表。

> Kaspersky Endpoint Security 还会显示有关服务配置文件状态的信息。联系 Kaspersky 技术支持时，可能需要有关服务配置文件状态的信息。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com STATUS [<profile>]
```

如果您输入不带配置文件的命令，Kaspersky Endpoint Security 显示应用程序所有配置文件的状态。

STATISTICS。配置文件操作统计

显示应用程序配置文件的统计信息（例如，扫描持续时间或检测到的威胁数）。您可以运行 `HELP STATISTICS` 命令来查看可用配置文件列表。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com STATISTICS <profile>
```

RESTORE。从备份区中还原文件

将文件从备份区恢复到原始文件夹。如果指定路径中已存在具有相同名称的文件，应用程序将要求确认以替换该文件。要还原的文件将保留其原始名称进行复制。

> 要执行此命令，必须启用密码保护。用户必须具有“**从备份区恢复**”权限。

*备份*存储保存在清除过程中删除或修改的文件的副本。*备份副本*是指对文件进行病毒清除或删除前创建的文件副本。文件的备份副本以特定格式保存并且不会带来威胁。

文件的备份副本存储在 `C:\ProgramData\Kaspersky Lab\KES.14.1\QB` 文件夹中。

管理员组中的用户被授予访问该文件夹的完整权限。其账户用于安装 Kaspersky Endpoint Security 的用户被授予该文件夹的有限访问权限。

> Kaspersky Endpoint Security 不提供用于配置文件备份副本的用户访问权限的功能。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

高级设置	
`/REPLACE`	覆盖现有文件。
`<file name>`	要还原的文件的名称。

身份验证	
/login=<user name> /password=<password>	带有所需密码保护权限的用户账户凭证。

示例

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

EXPORT。导出应用程序设置

将 Kaspersky Endpoint Security 设置导出到文件。如果命令仅包含要导出设置的文件的名称，则应用程序将按如下方式放置文件：

- 如果将 avp.com 的路径添加到 %PATH% 系统变量中，则应用程序会将文件放置在 `C:\Windows\SysWOW64` 文件夹。
- 如果从应用程序安装文件夹运行该命令，则导出将失败，因为应用程序的自我保护会阻止在应用程序文件夹中创建新文件。要将应用程序设置导出到文件，请输入文件路径。

要执行此命令，必须启用密码保护。用户必须具有“**导出设置**”权限。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com EXPORT <profile> <file name> /login=<user name> /password=<password>
```

配置文件	
<profile>	配置文件名称。*配置文件*是 Kaspersky Endpoint Security 组件、任务或功能。您可以通过运行 `HELP EXPORT` 命令来查看可用配置文件列表。

要导出的文件	
<file name>	应用程序设置将导出到的文件的名称。您也可以输入文件路径。您可以将 Kaspersky Endpoint Security 设置导出为 DAT 或 CFG 配置文件、TXT 文本文件或 XML 文档。

身份验证	
/login=<user name> /password=<password>	带有所需密码保护权限的用户账户凭证。

示例

```
avp.com EXPORT ids ids_C:\Users\Fred123\Documents\config.dat
```

```
avp.com EXPORT fm fm_config.txt
```

IMPORT。导入应用程序设置

从使用 `EXPORT` 命令创建的文件导入 Kaspersky Endpoint Security 设置。

> 要执行此命令，必须启用密码保护。用户必须具有“**配置应用程序设置**”权限。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com IMPORT <file name> /login=<user name> /password=<password>
```

要导入的文件	
`<file name>`	将从中导入应用程序设置的文件的名称。您可以从 DAT 或 CFG 配置文件、TXT 文本文件或 XML 文档导入 Kaspersky Endpoint Security 设置。

身份验证	
`/login=<user name> /password=<password>`	带有所需密码保护权限的用户账户凭证。

示例

```
avp.com IMPORT config.dat /login=KLAdmin /password=samplePassword
```

ADDKEY。应用密钥文件

使用密钥文件激活 Kaspersky Endpoint Security。如果应用程序已激活，则该密钥将作为备用密钥添加。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

> 如果应用程序安装在 Light Agent 模式，此命令无法运行。

命令语法

```
avp.com ADDKEY <file name> [/login=<user name> /password=<password>]
```

密钥文件	
`<file name>`	密钥文件名。

身份验证	
/login=<user name> /password=<password>	用户账户凭据。只有启用了密码保护时，才需要输入这些凭据。

示例

```
avp.com ADDKEY file.key
```

LICENSE。授权许可

管理 Kaspersky Endpoint Security、EDR Optimal 或 EDR Expert（Kaspersky Endpoint Detection and Response 插件）的授权许可密钥。

要执行此命令并删除授权许可密钥，必须启用密码保护。用户必须具有“**删除密钥**”权限。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

如果应用程序安装在 Light Agent 模式，此命令无法运行。

命令语法

```
avp.com LICENSE <operation> [/login=<user name> /password=<password>]
```

操作	
/ADD <file name>	使用密钥文件激活 Kaspersky Endpoint Security。如果应用程序已激活，则该密钥将作为备用密钥添加。
/ADD <activation code>	使用激活码激活 Kaspersky Endpoint Security。如果应用程序已激活，则该密钥将作为备用密钥添加。
/REFRESH	更新 Kaspersky Endpoint Security 授权许可的状态。因此，应用程序从卡巴斯基激活服务器接收最新的授权许可状态信息。
/REFRESH <license ID>	使用授权许可 ID 更新授权许可状态。使用此命令，您可以更新 EDR 加载项、MDR 加载项、KUMA 加载项或其他授权许可的状态。您可以从授权许可证书中获取授权许可 ID。因此，应用程序从卡巴斯基激活服务器接收最新的授权许可状态信息。
/CHECK	获取授权许可信息。Kaspersky Endpoint Security 显示有关所有添加的授权许可密钥的信息，包括备用密钥、EDR 插件、MDR 插件、KUMA 插件密钥和其他密钥。 Kaspersky Endpoint Security 显示以下授权许可信息： • 授权许可名称； • 授权许可标识符； • 在 Light Agent 模式下安装应用程序的虚拟机所连接的 Protection Server (SVM) 的地址； • 授权许可类型：试用版、商业版、Beta 版、订阅； • 应用程序激活的日期和时间； • 授权许可到期的日期和时间； • 授权许可到期前的天数。
/CHECK <license ID>	通过 ID 获取授权许可信息。您可以使用此命令来获取授权许可信息。您可以从授权许可证书中获取授权许可 ID。
/DEL /login=<user name> /password=<password>	删除应用程序的授权许可密钥。备用密钥也将被删除。
/DEL <license ID> /login= <user name> /password= <password>	使用授权许可 ID 删除密钥。使用此命令，您可以从 EDR 加载项、MDR 加载项、KUMA 加载项或其他授权许可中删除密钥。您可以从授权许可证书中获取授权许可 ID。

身份验证	
/login=<user name> /password=<password>	带有所需密码保护权限的用户账户凭证。

示例
```
avp.com LICENSE /ADD file.key
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

示例

```
avp.com LICENSE /ADD file.key
```

```
avp.com LICENSE /ADD AAAAA-BBBBB-CCCCC-DDDDD
```

```
avp.com LICENSE /DEL 3084-000789-456AB78C /login=KLAdmin /password=samplePassword
```

RENEW。购买授权许可

打开卡巴斯基网站以购买或续费授权许可。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

如果应用程序安装在 Light Agent 模式，此命令无法运行。

PBATESTRESET。在加密磁盘之前重置磁盘检查结果

重置完整磁盘加密 (FDE) 的兼容性检查结果，包括卡巴斯基磁盘加密和 BitLocker 驱动器加密技术。

在运行完整磁盘加密之前，应用程序会执行大量检查以验证是否可以对计算机进行加密。如果计算机不支持完整磁盘加密，Kaspersky Endpoint Security 会记录有关不兼容性的信息。下次尝试加密时，应用程序不会执行此检查，并警告您无法进行加密。如果计算机的硬件配置已更改，则必须重置应用程序先前记录的兼容性检查结果，以重新检查系统硬盘驱动器与卡巴斯基磁盘加密或 BitLocker 驱动器加密技术的兼容性。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

EXIT。退出应用程序

退出 Kaspersky Endpoint Security。应用程序将从计算机的 RAM 中卸载。

要执行此命令，必须启用密码保护。用户必须具有“**退出应用程序**”权限。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com EXIT /login=<user name> /password=<password>
```

EXITPOLICY。禁用策略

在计算机上禁用 Kaspersky Security Center 策略。所有 Kaspersky Endpoint Security 设置均可进行配置，包括策略中已上锁的设置 (🔒)。

> 要执行此命令，必须启用密码保护。用户必须具有“**禁用 Kaspersky Security Center 策略**”权限。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com EXITPOLICY /login=<user name> /password=<password>
```

STARTPOLICY。启用策略

在计算机上启用 Kaspersky Security Center 策略。将根据策略配置应用程序设置。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

DISABLE。禁用保护

禁用具有过期的 Kaspersky Endpoint Security 授权许可的计算机上的文件威胁防护。无法在装有未激活或具有无效授权许可的应用程序的计算机上运行此命令。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

SPYWARE。间谍软件检测

管理间谍软件检测。默认情况下已启用间谍软件检测。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com SPYWARE on|off
```

KSN。在 KSN / KPSN 之间切换

选择卡巴斯基解决方案以决定文件或网站信誉。Kaspersky Endpoint Security 支持以下用于使用卡巴斯基信誉数据库的基础设施解决方案：

- *卡巴斯基安全网络（KSN）*是大多数卡巴斯基应用程序使用的解决方案。KSN 参与者从卡巴斯基接收信息，并向卡巴斯基发送用户计算机上检测到的对象的信息，以便 卡巴斯基分析人员进行额外分析，并包括在卡巴斯基安全网络的信誉和统计数据库中。

- *卡巴斯基私有安全网络*是让运行 Kaspersky Endpoint Security 或其他卡巴斯基应用程序的计算机的用户获得卡巴斯基信誉数据库以及其他统计数据的访问权限的解决方案，无需从他们自己的计算机向卡巴斯基发送数据。KPSN 专为因以下任一原因无法参与卡巴斯基安全网络的公司客户所设计：

  - 本地工作站未连接 Internet。

  - 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。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

如果应用程序安装在 Light Agent 模式，此命令无法运行。

命令语法

```
avp.com KSN /global | /private <file name>
```

卡巴斯基安全网络配置文件	
`<file name>`	包含卡巴斯基私人安全网络设置的配置文件的名称。此文件具有 PKCS7 或 PEM 扩展名。

示例

```
avp.com KSN /global
avp.com KSN /private C:\ksn_config.pkcs7
```

示例

```
avp.com KSN /global
```

```
avp.com KSN /private C:\ksn_config.pkcs7
```

SERVERBINDINGDISABLE。禁用服务器连接保护

运行“*管理服务器连接保护*”任务，该任务将删除计算机与管理服务器连接的密码。通过这种方式，该任务将禁用对管理服务器连接的保护。

> 要执行此命令，必须启用密码保护。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com SERVERBINDINGDISABLE [/password=<password>]
```

密码	
`/password=<password>`	KLAdmin 用户账户的密码或“*管理服务器连接保护*”任务的密码。 如果未指定参数，Kaspersky Endpoint Security 会在下一行提示您输入密码。

KESCLI 命令

KESCLI 命令允许您使用 OPSWAT 组件接收有关计算机保护状态的信息，并允许您执行标准任务，如“*恶意软件扫描*”和“*数据库和应用程序模块更新*”任务。

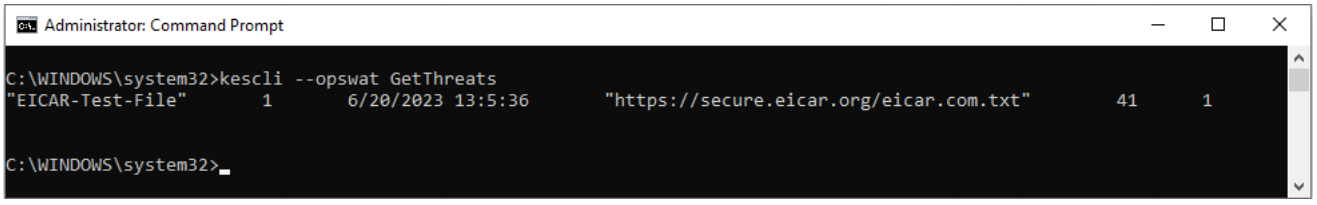
您可以使用 `kescli --help` 命令或缩写命令 `kescli -h` 来查看 KESCLI 命令的列表。

要从命令行管理 Kaspersky Endpoint Security：

1. 以管理员身份运行命令行解释器 (cmd.exe)。
2. 转到 Kaspersky Endpoint Security 可执行文件所在文件夹。
   您可以在应用程序安装期间将可执行文件的路径添加到 %PATH% 系统变量中。
3. 使用以下模板执行命令：

   ```
   Kescli <命令> [选项]
   ```

   结果，Kaspersky Endpoint Security 将执行该命令（参见下图）。



从命令行管理应用程序

SCAN。恶意软件扫描

运行“*恶意软件扫描*（全盘扫描）”任务。

> 要运行任务，管理员必须在策略中允许使用本地任务。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。

命令语法

```
kescli --opswat Scan "<scan scope>" <action on threat detection>
```

您可以使用 `GetScanState` 命令检查“*恶意软件扫描*”任务的完成状态，以及使用 `GetLastScanTime` 命令查看上一次扫描完成时的日期和时间。

扫描范围	
`<scan scope>`	`;`-分隔的文件和文件夹列表。例如，`"C:\Program Files (x86)\Example Folder"`。

检测到威胁后的操作	
`0`	“**通知**”。如果选择此选项，Kaspersky Endpoint Security 会在检测到受感染文件时将这些文件的相关信息添加到活动威胁列表。
`1`	“**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。 默认情况下已选择此操作。

示例

```
kescli --opswat Scan "C:\Documents and Settings\All Users\My Documents;C:\Program Files" 1
```

GetScanState。扫描完成状态

显示“ *恶意软件扫描*（*全盘扫描*）”任务完成状态信息：

- `1` – 扫描进行中。
- `0` – 扫描不在运行。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。

命令语法

```
kescli --opswat GetScanState
```

GetLastScanTime。决定扫描完成时间

显示上一次“*恶意软件扫描（全盘扫描）*”任务完成的日期和时间信息。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。

命令语法

```
kescli --opswat GetLastScanTime
```

GetThreats。获取检测到的威胁的数据

显示检测到的威胁列表（*威胁报告*）。此报告包含创建报告前 30 天内有关威胁和病毒活动的信息。

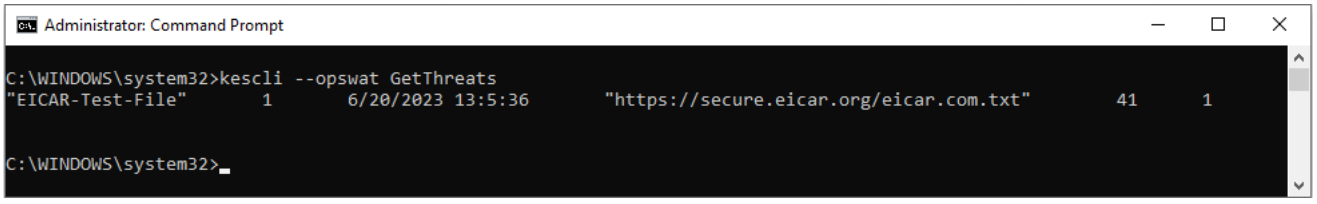
要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。

命令语法

```
kescli --opswat GetThreats
```

当执行该命令时，Kaspersky Endpoint Security 将用以下格式发送响应：

```
<name of detected object> <type of object> <detection date and time> <path to file>
<action on threat detection> <threat danger level>
```



从命令行管理应用程序

对象类型	
0	未知（Unknown）。
1	病毒（Virware）。
2	木马程序（Trojware）。
3	恶意程序（Malware）。
4	广告程序（Adware）。
5	自动拨号程序（Pornware）。
6	可以被犯罪分子利用以损害用户计算机或数据的应用程序（Riskware）。
7	可能被用来保护恶意代码的打包对象（Packed）。
20	未知对象（Xfiles）。
21	未知应用程序（Software）。
22	隐藏的文件（Hidden）。

23	需要注意的应用程序(Pupware)。
24	反常行为(Anomaly)。
30	未确定(Undetect)。
40	广告横幅(Banner)。
50	网络攻击(Attack)。
51	注册表访问(Registry)。
52	可疑活动(Suspicion)。
60	漏洞(Vulnerability)。
70	钓鱼（Phishing）。
80	不需要的电子邮件附件(Attachment)。
90	卡巴斯基安全网络检测到的恶意软件(Urgent)。
100	未知链接(Suspic URL)。
110	其他恶意软件(Behavioral)。

检测到威胁后的操作	
0	未知(unknown)。
1	威胁已修复(ok)。
2	对象已感染，尚未清除(infected)。
5	对象在存档中并且尚未清除(archive)。
9	对象已被清除(disinfected)。
10	对象未被清除(not disinfected)。
11	对象已被删除(deleted)。
13	对象的备份副本已创建(backupped)。
15	对象已被移到备份区(quarantined)。
23	对象已在计算机重启时被删除(delete on reboot)。
25	对象已在计算机重启时被清除(disinfect on reboot)。
29	对象已被用户移到备份区(added by user)。
30	对象已被添加到排除项(added to exclude)。
31	对象已在计算机重启时被移到备份区(quarantine on reboot)。
36	误报(false alarm)。
38	进程别终止(terminated)。
40	未检测到对象(not found)。
41	无法解决威胁(untreatable)。
42	对象已被恢复(rolled back)。
43	对象是由于威胁活动而创建的。(produced by threat)。
44	对象已在计算机重启时被恢复(roll back on reboot)。
0xffffffff	对象未被处理(discarded)。

威胁危险等级	
`0`	未知
`1`	高

2	中度扫描
4	低
8	信息（少于*低*）

UpdateDefinitions。更新数据库和程序软件模块

运行"*数据库和应用程序模块更新*"任务。Kaspersky Endpoint Security 使用默认源：卡巴斯基更新服务器。

> 要运行任务，管理员必须在策略中允许使用本地任务。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。

> 如果应用程序安装在 Light Agent 模式，此命令无法运行。

命令语法

```
kescli --opswat UpdateDefinitions
```

您可以使用 `GetDefinitionsetState` 命令查看当前反病毒数据库的发布日期和时间。

GetDefinitionState。确定数据库上次更新的日期和时间

显示有关正在使用的反病毒数据库上次更新的日期和时间的信息。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。

命令语法

```
kescli --opswat GetDefinitionState
```

EnableRTP。启用保护

在计算机上启用 Kaspersky Endpoint Security 保护组件：文件威胁防护、Web 威胁防护、邮件威胁防护、网络威胁防护、主机入侵防御。

> 要启用保护组件，管理员必须确保相关的策略设置可以被修改（属性是开放的）。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。

命令语法

```
kescli --opswat EnableRTP
```

因此，即使您使用密码保护禁止修改应用程序设置，保护组件也被启用。

您可以使用 `GetRealTimeProtectionState` 命令查看文件威胁防护的操作状态。

GetRealTimeProtectionState。“文件威胁防护”状态

显示文件威胁防护组件的状态信息：

- `1` – 组件已启用。
- `0` – 组件已禁用。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。

命令语法

```
kescli --opswat GetRealTimeProtectionState
```

GetEncryptionState。磁盘加密状态

显示有关磁盘加密状态的信息：

- `1` 表示磁盘受卡巴斯基或 BitLocker 磁盘加密技术保护。
- `0` 表示磁盘未加密。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。

命令语法

```
kescli --opswat GetEncryptionState
```

Version。识别应用程序版本

显示 Kaspersky Endpoint Security for Windows 的版本。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。

命令语法

```
kescli --Version
```

您也可以使用缩写命令 `-v`。

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（例如，Kaspersky Sandbox 或 Kaspersky Endpoint Detection and Response Optimum）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。您可以通过运行 `HELP` 命令来查看用于管理应用程序的命令列表。要阅读特定命令的语法，请输入 `HELP <command>`。

要使用命令行管理 Detection and Response 解决方案的内置功能，请执行以下操作：

1. 以管理员身份运行命令行解释器 (cmd.exe)。
2. 转到 Kaspersky Endpoint Security 可执行文件所在文件夹。
3. 使用以下模板执行命令：

```
avp.com <command> [options]
```

结果，Kaspersky Endpoint Security 将执行该命令。

SANDBOX。管理 Sandbox

管理 Sandbox 组件的命令：

- 启用或禁用 Sandbox 组件。

  Sandbox 组件提供与 Kaspersky Sandbox 解决方案和 KATA Sandbox 组件的交互，后者是 Kaspersky Anti Targeted Attack Platform 的一部分。

- 配置 Kaspersky Sandbox 组件：

  - 连接计算机到 Sandbox 服务器。

    服务器使用部署的 Microsoft Windows 操作系统虚拟映像来运行需要扫描的对象。您可以输入 IP 地址（IPv4 或 IPv6）或完全限定的域名。有关部署虚拟镜像和配置 Sandbox 服务器的详细信息，请参阅 Kaspersky Sandbox 帮助 和 Kaspersky Anti Targeted Attack Platform 帮助 。

  - 配置服务器的连接超时。

    Sandbox 服务器（对于 Kaspersky Sandbox）或 Central Node 服务器（对于 KATA）的连接超时。配置的超时时间过后，Kaspersky Endpoint Security 将向下一台服务器发送请求。如果连接速度低或连接不稳定，您可以增加服务器的连接超时。建议的请求超时是 0.5 秒或更少。

  - 配置计算机和服务器之间的受信任连接。

    要配置与 Sandbox 服务器（对于 Kaspersky Sandbox）或 Central Node 服务器（对于 KATA）的受信任连接，您必须准备 TLS 证书。您必须使用策略将证书添加到计算机。您还需要将证书添加到 Sandbox 服务器（对于 Kaspersky Sandbox）或 Central Node 服务器（对于 KATA）。

  - 配置集成模式。

您需要选择包含 Sandbox 功能的解决方案，即 Kaspersky Sandbox 或 KATA Sandbox。*Kaspersky Sandbox* 是卡巴斯基的独立 Detection and Response 解决方案。*KATA Sandbox* 是 Kaspersky Anti Targeted Attack Platform 解决方案的一个组件。与 KATA Sandbox 集成后，该组件可以以以下模式运行：

- "**手动**"。用户从上下文菜单手动提交文件进行扫描（**发送到 Sandbox**）。
- "**自动**"。应用程序自动检测对象并将其提交到 Sandbox 进行扫描。
- "**组合的**"。

- 显示组件的当前设置。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com stop sandbox [/login=<user name> /password=<password>]
```

```
avp.com start sandbox
```

```
avp.com sandbox /set [--servers=<address:port>] [--pinned-certificate=<path to the TLS certificate>] [--client-certificate=<path to the PFX archive>] [--client-certificate-password=<password>] [--timeout=<Sandbox server connection timeout (ms)>] [--mode=<KSB|KATAManual|KATAAuto|KATAFull>] [/login=<user name> /password=<password>]
```

操作	
`stop`	禁用 Sandbox 组件。
`start`	启用 Sandbox 组件。

`set`	配置 Sandbox 组件。您可以配置以下设置：
	• 添加 Sandbox 服务器（`--servers`）
	• 添加 TLS 证书（`--pinned-certificate`）
	• 添加加密容器（`--client-certificate`）
	• 指定加密容器的密码（`--client-certificate-password`）；
	• 设置服务器连接超时（`--timeout`）
	• 选择一种集成模式（`--mode`）：
	  • `KSB` – 与 Kaspersky Sandbox 的集成；
	  • `KATAManual` – 手动与 KATA Sandbox 集成；
	  • `KATAAuto` – 自动与 KATA Sandbox 集成；
	  • `KATAFull` – 与 KATA Sandbox 的组合集成。

`show`	显示组件的当前设置。您获得以下响应：
	`sandbox.timeout=<Sandbox server connection timeout (ms)>`
	`sandbox.servers=<list of Sandbox servers>`
	`sanbox.mode=<integration mode>`
	`sandbox.tls=<trusted connection status>`

身份验证	
`/login=<user name> /password=<password>`	带有所需密码保护权限的用户账户凭证。

示例

```
avp.com SANDBOX /SET --servers=127.0.0.1:8080;127.0.0.2:8080 --pinned-certificate=c:\my_certs\my.cer --mode=KSB /login=login /password=password
```

PREVENTION。管理执行防护

禁用执行防护组件或显示组件的当前设置，包括执行防护规则列表。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com prevention disable
```

```
avp.com prevention /show
```

在执行 `prevention /show` 命令时，您将得到以下响应：

```
prevention.enable=true|false

prevention.mode=audit|prevent

prevention.rules

id: <rule ID>
target: script|process|document
md5: <MD5 hash of the file>
sha256: <SHA256 hash of the file>
pattern: <path to the object>
case-sensitive: true|false
```

命令返回值：

- `-1` 表示计算机上安装的应用程序版本不支持该命令。
- `0` 表示命令已成功执行。
- `1` 表示未将强制参数传递给命令。
- `2` 表示发生一般性错误。
- `4` 表示存在语法错误。
- `9` – 错误操作（例如，在组件已禁用时尝试禁用该组件）。

ISOLATION。管理网络隔离

禁用计算机的网络隔离或显示组件的当前设置。组件设置还包括添加到排除项的网络连接列表。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com isolation /OFF /login=<user name> /password=<password>
```

```
avp.com isolation /STAT
```

作为运行 `stat` 命令的结果，您接收以下响应：`Network isolation on|off`。

RESTORE。从隔离区中恢复文件

将文件从隔离区恢复到原始文件夹。*隔离区*是计算机上的一个特别的本地存储区。用户可以隔离用户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 仅在与 Kaspersky Detection and Response 解决方案集成时使用隔离。在其他情况下，Kaspersky Endpoint Security 将相关文件置于备份中。有关将隔离管理作为解决方案的一部分的详细信息，请参阅 Kaspersky Sandbox 帮助、Kaspersky Endpoint Detection and Response Optimum 帮助、Kaspersky Endpoint Detection and Response Expert 帮助、Kaspersky Anti Targeted Attack Platform 帮助 和 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助。

要执行此命令，必须启用密码保护。用户必须具有“**从备份区恢复**”权限。

对象在系统账户 (SYSTEM) 下隔离。

从隔离恢复文件涉及以下特殊注意事项：

- 如果目标文件夹已被删除或用户没有该文件夹的访问权限，则应用程序会将该文件放在 `%DataRoot%\QB\Restored` 文件夹中。然后必须手动将文件移动到目标文件夹。
- 应用程序对要还原的文件的名称区分大小写。如果您在输入文件名时没有观察到这种情况，则应用程序不会恢复文件。
- 如果目标文件夹中已有同名文件，则应用程序将取消恢复该文件。
- 如果您使用的是 KATA（EDR）解决方案，应用程序会在恢复文件后将文件副本保存在隔离区中。您可以手动清空隔离区。对于 EDR Optimum 和 EDR Expert 解决方案，应用程序在恢复后删除文件。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com RESTORE [/REPLACE] <file name> /login=<user name> /password=<password>
```

高级设置	
`/REPLACE`	覆盖现有文件。
`<file name>`	要还原的文件的名称。

身份验证	
/login=<user name> /password=<password>	带有所需密码保护权限的用户账户凭证。

示例

```
avp.com RESTORE /REPLACE true_file.txt /login=KLAdmin /password=samplePassword
```

命令返回值：

- -1 表示计算机上安装的应用程序版本不支持该命令。
- 0 表示命令已成功执行。
- 1 表示未将强制参数传递给命令。
- 2 表示发生一般性错误。
- 4 表示存在语法错误。

IOCSCAN。妥协的指标 (IOC) 扫描

运行"*IOC 扫描*"任务。*妥协的指标 (IOC)* 是一组关于对象或活动的数据，表示未经授权访问计算机（数据泄露）。例如，许多登录系统的尝试都不成功，这可能构成妥协的指标。*IOC 扫描*任务允许在计算机上查找妥协的指标，并采取威胁响应措施。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

在与 IOC 文件中描述的入侵指标进行 128 次匹配后，IOC 扫描将中止。有必要限制 IOC 扫描任务报告中的条目数量，以便于分析，并防止由于不精确制定的入侵指标而产生大量匹配而导致报告溢出。

命令语法

```
avp.com IOCSCAN <full path to the IOC file>|/path=<path to the IOC files folder> [/process=on|off] [/hint=<full
path to executable file of a process|full file path>] [/registry=on|off] [/dnsentry=on|off] [/arpentry=on|off]
[/ports=on|off] [/services=on|off] [/system=on|off] [/users=on|off] [/volumes=on|off] [/eventlog=on|off]
[/datetime=<event publication date>] [/channels=<list of channels>] [/files=on|off] [/drives=
<all|system|critical|custom>] [/excludes=<list of exclusions>][/scope=<list of folders to scan>]
```

IOC 文件	
<full path to the IOC file>	您要用于扫描的 IOC 文件的完整路径。您可以指定多个由空格分隔的 IOC 文件。IOC 文件的完整路径不可以使用 /path 参数输入。 例如，C:\Users\Admin\Desktop\IOC\file1.ioc
/path=<path to the folder with IOC files>	您要用于扫描的 IOC 文件的文件夹路径。*IOC 文件*是包含应用程序尝试匹配以计数检测的指标集的文件。IOC 文件必须符合 OpenIOC 标准。 例如，C:\Users\Admin\Desktop\IOC

用于 IOC 扫描的数据类型	
`/process=on|off`	执行 IOC 扫描时分析进程数据（ProcessItem 术语）。 如果参数的值为"`off`"，则在执行扫描时，Kaspersky Endpoint Security 不会分析计算机上运行的进程。如果 IOC 文件包含 ProcessItem IOC 文档的 IOC 术语，则忽略这些术语（检测为不匹配）。 如果未指定参数，则仅当为扫描提供的 IOC 文件中描述了 ProcessItem IOC 文档时，Kaspersky Endpoint Security 才会分析进程数据。
`/hint=<full path to the executable file of the process|full path to the file>`	执行 IOC 扫描时分析文件数据（ProcessItem 和 FileItem 术语）。 您可以采用以下方式之一选择文件： • `<full path to the executable file of the process>` – ProcessItem 术语； • `<full path to the file>` – FileItem 术语。
`/registry=on|off`	执行 IOC 扫描时分析 Windows 注册表数据（RegistryItem 术语）。 如果参数的值为`off`，Kaspersky Endpoint Security 不会扫描 Windows 注册表。如果 IOC 文件包含 RegistryItem IOC 文档术语，则忽略这些术语（检测为不匹配）。 如果未指定参数，则仅当为扫描提供的 IOC 文件中描述了 RegistryItem IOC 文档时，Kaspersky Endpoint Security 才会分析 Windows 注册表。 对于数据类型 RegistryItem，Kaspersky Endpoint Security 扫描一组注册表键集合。
`/dnsentry=on|off`	执行 IOC扫描（DnsEntryItem 术语）时，分析有关本地 DNS 缓存中记录的数据。 如果参数的值为`off`，Kaspersky Endpoint Security 不会扫描本地 DNS 缓存。如果 IOC 文件包含 DnsEntryItem IOC 文档术语，则忽略这些术语（检测为不匹配）。 如果未指定参数，则仅当为扫描提供的 IOC 文件中描述了 DnsEntryItem IOC 文档时，Kaspersky Endpoint Security 才会分析本地 DNS 缓存。
`/arpentry=on|off`	执行 IOC扫描（ArpEntryItem术语）时，分析有关 ARP 表中记录的数据。 如果参数的值为`off`，Kaspersky Endpoint Security 不会扫描 ARP 表。如果 IOC 文件包含 ArpEntryItem IOC 文档术语，则忽略这些术语（检测为不匹配）。 如果未指定参数，则仅当为扫描提供的 IOC 文件中描述了 ArpEntryItem IOC 文档时，Kaspersky Endpoint Security 才会分析 ARP 表。
`/ports=on|off`	分析有关在执行 IOC 扫描时打开以进行侦听的端口的数据（PortItem 术语）。 如果参数的值为`off`，Kaspersky Endpoint Security 不会扫描设备上的活动连接表。如果 IOC 文件包含 PortItem IOC 文档术语，则忽略这些术语（检测为不匹配）。 如果未指定参数，则仅当为扫描提供的 IOC 文件中描述了 PortItem IOC 文档时，Kaspersky Endpoint Security 才会分析设备上的活动连接表。
`/services=on|off`	执行 IOC 扫描（ServiceItem 术语）时，分析有关设备上安装的服务的数据。 如果参数的值为`off`，Kaspersky Endpoint Security 不会扫描设备上安装的服务的数据。如果 IOC 文件包含 ServiceItem IOC 文档术语，则忽略这些术语（检测为不匹配）。 如果未指定参数，则仅当为扫描提供的 IOC 文件中描述了 ServiceItem IOC 文档时，Kaspersky Endpoint Security 才会分析服务数据。
`/system=on|off`	执行 IOC 扫描时分析环境数据（SystemInfoItem 术语）。 如果参数的值为`off`，Kaspersky Endpoint Security 不会分析环境数据。如果 IOC 文件包含 SystemInfoItem IOC 文档术语，则忽略这些术语（检测为不匹配）。 如果未指定参数，则仅当为扫描提供的 IOC 文件中描述了 SystemInfoItem IOC 文档时，Kaspersky Endpoint Security 才会分析环境数据。
`/users=on|off`	执行 IOC 扫描时分析用户数据（UserItem 术语）。 如果参数的值为`off`，Kaspersky Endpoint Security 不会分析系统中创建的用户的数据。如果 IOC 文件包含 UserItem IOC 文档术语，则忽略这些术语（检测为不匹配）。 如果未指定参数，则仅当为扫描提供的 IOC 文件中描述了 UserItem IOC 文档时，Kaspersky Endpoint Security 才会分析系统中创建的用户的数据。
`/volumes=on|off`	执行 IOC 扫描时分析卷数据（VolumeItem 术语）。 如果参数的值为`off`，Kaspersky Endpoint Security 不会扫描设备上的卷的数据。如果 IOC 文件包含 VolumeItem IOC 文档术语，则忽略这些术语（检测为不匹配）。 如果未指定参数，则仅当为扫描提供的 IOC 文件中描述了 VolumeItem IOC 文档时，Kaspersky Endpoint Security 才会分析卷数据。

`/eventlog=on|off`	执行 IOC扫描（EventLogItem 术语）时，分析有关 Windows 事件日志中的记录的数据。 如果参数的值为 `off`，Kaspersky Endpoint Security 不会扫描 Windows 事件日志中的记录。如果 IOC 文件包含 EventLogItem IOC 文档术语，则忽略这些术语（检测为不匹配）。 如果未指定参数，则仅当为扫描提供的 IOC 文件中描述了 EventLogItem IOC 文档时，Kaspersky Endpoint Security 才会分析 Windows 事件日志。
`/datetime=<event publication date>`	在确定相应 IOC 文档的 IOC 扫描范围时，请考虑事件在 Windows 事件日志中发布的日期。 在执行 IOC 扫描时，Kaspersky Endpoint Security 会扫描从指定时间和日期到任务运行期间发布的 Windows 事件日志条目。 Kaspersky Endpoint Security 允许将事件发布日期指定为参数值。仅对在指定日期之后和运行扫描之前在 Windows 事件日志中发布的事件执行扫描。 如果未指定参数，Kaspersky Endpoint Security 将扫描具有任何发布日期的事件。"`TaskSettings::BaseSettings::EventLogItem::datetime`"设置无法编辑。 仅当为扫描提供的 IOC 文件中描述了 EventLogItem IOC 文档时，才使用该设置。
`/channel=<list of channels>`	要对其执行 IOC 扫描的通道（日志）名称列表。 如果指定了参数，Kaspersky Endpoint Security 将扫描在指定日志中发布的记录。IOC 文件必须描述 EventLogItem 术语。 根据日志属性（"Full Name"参数）或事件属性（事件 xml 架构中的"`<Channel></Channel>`"参数）中指定的日志（通道）名称，将日志名称指定为字符串。您可以指定多个由空格分隔的通道。 如果未指定参数，Kaspersky Endpoint Security 将扫描记录中的 `Application`，`System`，`Security` 通道。
`/files=on|off`	执行 IOC 扫描时分析文件数据（FileItem 术语）。 如果参数的值为 `off`，Kaspersky Endpoint Security 不会分析文件数据。如果 IOC 文件包含 FileItem IOC 文档术语，则忽略这些术语（检测为不匹配）。 如果未指定参数，则仅当为扫描提供的 IOC 文件中描述了 FileItem IOC 文档时，Kaspersky Endpoint Security 才会分析文件数据。
`/drives=<all|system|critical|custom>`	在分析 FileItem IOC 文档的数据时设置 IOC 扫描范围。 您可以为扫描范围设置以下值： • `<all>` 用于所有可用的文件范围。 • `<system>` 用于安装操作系统的文件夹中的文件。 • `<critical>` 用于用户和系统文件夹中的临时文件。 • `<custom>` 用于用户定义的范围（`/scope=<list of folders to scan>`）。 如果未指定参数，则对关键区域执行扫描。
`/excludes=<list of exclusions>`	在分析 FileItem IOC 文档的数据时设置排除范围。您可以指定多个由空格分隔的路径。
`/scope=<list of folders to scan>`	在分析 FileItem IOC 文档的数据时设置的用户定义的 IOC 扫描范围（`/drives=custom`）。您可以指定多个由空格分隔的路径。
`/retro /<number of days>`	*回顾性 IOC 扫描*是 *IOC 扫描* 任务的一种模式，在该模式下，Kaspersky Endpoint Security 使用特定时间段的数据扫描入侵指标。此模式旨在通过受保护计算机的遥测数据（例如网络活动、进程、文件和其他遥测数据）来搜索入侵指标。 您可以设置 1 到 14 天的时间段。默认情况下，该应用程序会扫描入侵指标一天。
`/network=on|off`	网络数据分析（NetworkItem 术语）。
`/url=on|off`	浏览器日志数据分析（UrlHistoryItem 术语）。 回顾性 IOC 扫描分析以下浏览器的日志：Google Chrome、Mozilla Firefox、Microsoft Edge（版本 79 或更高版本）。
`/email`	邮件对象分析（EmailItem 术语）。
`/route`	路由和转发表分析（RouteEntryItem 术语）。

命令返回值：

- `-1` 表示计算机上安装的应用程序版本不支持该命令。
- `0` 表示命令已成功执行。
- `1` 表示未将强制参数传递给命令。

- 2 表示发生一般性错误。
- 4 表示存在语法错误。

如果命令成功执行（返回值 0），并且在执行过程中检测到妥协的指标，Kaspersky Endpoint Security 将向命令行输出以下任务结果信息：

Uuid	IOC 文件结构头中的 IOC 文件 ID（<ioc id=""> 标记）
Name	IOC 文件结构头中的 IOC 文件描述（<description></description> 标记）
Matched Indicator Items	所有匹配的指示器 ID 列表。
Matched objects	与之匹配的每个 IOC 文件的数据。

MDRLICENSE。MDR 激活

添加 BLOB 配置文件以激活 Managed Detection and Response。BLOB 文件包含客户端 ID 和 Kaspersky Managed Detection and Response 授权许可信息。BLOB 文件存在于 MDR 配置文件的 ZIP 存档中。您可以在 Kaspersky Managed Detection and Response 控制台获取 ZIP 存档。对于 BLOB 文件的详情，请参考 Kaspersky Managed Detection and Response 帮助。

需要管理员权限以使用 BLOB 文件执行操作。策略中的 Managed Detection and Response 设置必须可以编辑 ()。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com MDRLICENSE <operation> [/login=<user name> /password=<password>]
```

操作	
/ADD <file name>	应用 BLOB 配置文件用于与 Kaspersky Managed Detection and Response 的整合 (P7 文件格式)。您仅可以应用一个 BLOB 文件。如果一个 BLOB 文件已经添加到计算机，文件将被替换。
/DEL	删除 BLOB 配置文件。

身份验证	
/login=<user name> /password=<password>	带有所需密码保护权限的用户账户凭证。

示例

```
avp.com MDRLICENSE /ADD file.key
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

示例

```
avp.com MDRLICENSE /ADD file.key
```

```
avp.com MDRLICENSE /DEL /login=KLAdmin /password=samplePassword
```

EDRKATA。与 EDR（KATA）集成

用于管理 Endpoint Detection and Response 组件（KATA）的命令：

- 启用或禁用 EDR（KATA）组件。

  EDR 组件（KATA）提供与 Kaspersky Anti Targeted Attack Platform 解决方案的互操作性。

- 配置与 Kaspersky Anti Targeted Attack Platform 服务器的连接。

- 显示组件的当前设置。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com START EDRKATA
```

```
avp.com STOP EDRKATA
```

```
avp.com edrkata /set /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
<Central Node server connection timeout (s)>] [/sync-period=<Central Node server synchronization period (min)>]
```

```
avp.com edrkata /show
```

操作	
stop	禁用 EDR（KATA）组件。
start	启用 EDR（KATA）组件。
set	配置 EDR（KATA）组件。您可以配置以下设置： • 添加 Central Node 服务器（servers=<server address>:<port>） • 添加 TLS 证书（server-certificate=<path to the TLS certificate>） • 设置 Central Node 服务器连接超时（/timeout=<Central Node server connection timeout (s)>） • 设置与 Central Node 服务器同步的周期（/sync-period=<Central Node server synchronization period (min)>）
show	显示组件的当前设置。

KUMA。与 KUMA 的整合

用于管理内置 KUMA 代理的命令：

- 启用或禁用 KUMA 集成。

  内置 KUMA 代理可与 Kaspersky Unified Monitoring and Analysis Platform 解决方案实现互操作性。

- 配置与 Kaspersky Unified Monitoring and Analysis Platform 服务器的连接。

- 显示组件的当前设置。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com START KUMA
```

```
avp.com STOP KUMA [/login=<user name> /password=<password>]
```

```
avp.com KUMA /SET /servers=<server address>:<port> /server-certificate=<path to the TLS certificate> [/timeout=
<KUMA server connection timeout (s)>] [/client-certificate=<path to the crypto-container>] [ /client-certificate-
password=<password>] [/maximum-data-transfer-time=<maximum events transmission delay (sec)>]
```

```
avp.com KUMA /SHOW
```

操作	
stop	禁用 KUMA 集成。
start	启用 KUMA 集成。
set	配置内置 KUMA 代理。您可以配置以下设置： • 添加 KUMA 服务器(/servers=<protocol>://<server address>:<port>) 该应用程序支持以下服务器连接协议：tcp、udp、http、https。 • 添加 TLS 证书（/server-certificate=<path to the TLS certificate>） • 设置服务器连接超时（/timeout=<KUMA server connection timeout (s)>） • 添加加密容器（/client-certificate=<path to the crypto-container> /client-certificate-password=<password>） • 配置事件传输延迟（/maximum-data-transfer-time=<maximum events transmission delay (sec)>）
show	显示组件的当前设置。

身份验证	
/login=<user name> /password=<password>	带有所需密码保护权限的用户账户凭证。

示例

```
avp.com start kuma
```

```
avp.com KUMA /SET /servers=https://127.0.0.1:8080 /server-certificate=c:\\folder\\certificate.cer /timeout=15
/login=login /password=password
```

```
avp.com KUMA /SET /servers=https://kuma.server.com:8000 /server-certificate=c:\\folder\\certificate.cer
/login=login /password=password
```

YARA。运行 YARA 扫描

运行“*运行 YARA 扫描*”任务。应用程序使用 YARA 规则数据库来扫描文件和对象，以查找针对企业 IT 基础设施的针对性攻击的指标。*YARA 规则*是对针对企业 IT 基础设施的定向攻击和入侵的特征描述，Kaspersky Endpoint Security 使用这些特征来扫描对象。

要运行 YARA 扫描，您必须准备描述规则的 YARA 文件。创建 YARA 文件时，请考虑以下要求：

- Kaspersky Endpoint Security 支持带有 YARA 或 YAR 和 YARA 文件，这些文件遵循 YARA 4.2.3 开放标准，用于描述入侵指标。
- 只能为任务指定具有 YARA 规则的文件。*“运行 YARA 扫描”*任务不支持其他规则类型。
- 如果您添加了 Kaspersky Endpoint Security 不支持的 YARA 文件，或者规则包含语法错误，则任务将中止并显示相应的错误消息。
- 单个任务中使用的所有 YARA 文件的标识符必须是唯一的。如果存在具有相同标识符的 YARA 文件，则可能会影响任务执行结果。
- 在与 YARA 规则中描述的指标进行 128 次匹配后，YARA 扫描将中止。有必要限制 YARA 扫描报告中的条目数量，以便于分析，并防止由于不精确制定的 YARA 规则而产生大量匹配而导致报告溢出。

卡巴斯基建议每个 YARA 文件创建一条规则。这使得扫描结果更具可读性。

YARA 扫描可能需要相当长的时间。根据驱动器大小、任务设置和磁盘上的对象数量，YARA 扫描可持续几分钟到几小时。应用程序不显示进度指示器。无法停止或取消 YARA 扫描。建议您等到 YARA 扫描结果可用。

命令语法

```
avp.com YARA <full path to the YARA file>|/path=<path to the folder with YARA files> [<advanced settings>]
```

YARA 文件	

`<full path to the YARA file>`	您要用于扫描的 YARA 文件的完整路径。您可以指定多个由空格分隔的 YARA 文件的路径。
	如果未指定 `/path=<path to the folder with YARA files>` 值，则是必需参数。
	例如：
	`C:\Users\Admin\Desktop\YARA\file1.yar`
	`C:\Users\Admin\Desktop\YARA\file2.yar`

`/path=<path to the folder with YARA files>`	您要用于扫描的 YARA 文件的文件夹完整路径。 如果未指定 `<full path to the YARA file>` 值，则是必需参数。 例如： `/path=C:\Users\Admin\Desktop\YARA`

高级设置	
`/fastScan=<on|off>`	快速 YARA 扫描。对于每个对象，应用程序都会记录一次检测到的指标。应用程序还隐藏日志中检测到的指标的重复项。快速 YARA 扫描可以更快地扫描大文件。 如果未指定此设置，应用程序将执行标准 YARA 扫描。在这种模式下，应用程序会记录检测到的指标的重复项。
`/maxRules=<maximum number of scan rules>`	当达到唯一触发规则的数量限制时，应用程序将停止 YARA 扫描。 如果未指定此设置的值，或者 `0` 被指定时，应用程序将无限制执行 YARA 扫描。
`/timeOut=<stop scan after the specified time in seconds>`	YARA 扫描需要多长时间（以秒为单位）。当此时间用完时，应用程序将停止 YARA 扫描。 如果未指定此设置的值，或者 `0` 被指定时，应用程序将无限制执行 YARA 扫描。
`/recursive=<on|off>`	此参数启动 `/scanFolders` 自定义扫描中子文件夹的递归扫描。
`/scanFolders=<list of folders to be scanned>`	此参数启动对指定文件夹列表中的文件的 YARA 扫描。您可以指定多个由空格分隔的值。输入文件夹路径掩码时，Kaspersky Endpoint Security 支持 `*` 字符和 `?` 字符。 如果未指定此设置，应用程序将对除网络共享、云驱动器和可移动媒体之外的所有本地磁盘执行 YARA 扫描。
`/scanMemory=<on|off>`	扫描所有正在运行的进程的内存。

/scanProcess=<process name>	仅为指定进程扫描内存。指定以空格分隔的进程可执行文件的完整路径。您也可以使用 * 和 ? 字符来输入掩码。
/maxSize=<file size in bytes>	限制 YARA 扫描的文件大小。应用程序会跳过较大的文件。
/includes=<list of objects to be scanned>>	编辑扫描范围。您可以指定多个由空格分隔的值。以下值可用： • 文件名 • 文件扩展名 必须使用 /scanFolders 参数指定扫描范围。 例如： /scanFolders C:*.* /includes=*.exe *.dll – 应用程序扫描 C 盘上所有扩展名为 .EXE 和 .DLL 的文件。
/excludes=<list of objects to be scanned>	从 YARA 扫描中排除文件。您可以指定多个由空格分隔的值。以下值可用： • 文件路径 • 文件路径掩码 必须使用 /scanFolders 参数指定排除项。 例如： /scanFolders C:*.* /excludes readme.txt C:\trusted*.* *.xml – 应用程序跳过 readme.txt 文件、C:\trusted 文件夹中的所有文件以及 C 盘根文件夹中所有以 xml 为扩展名的文件。
/scanAutoruns=<on|off>	自动运行点对象的 YARA 扫描。
/excludeAutoruns=<list of autorun point areas to skip>	从扫描范围内排除自动运行点对象。指定以空格分隔的进程可执行文件的完整路径。您也可以使用 * 和 ? 字符来输入掩码。
/logFolder=<path to the folder for saving the scan results in a TXT file>	如果您指定文件夹路径，应用程序会将扫描结果保存在指定路径下名为 yara_<计算机名称>_<扫描完成时间>.txt 的文件中。 如果您指定特定 TXT 文件的路径，应用程序会将扫描结果保存在该文件中。 例如： /logFolder=C:\test 或 /logFolder=C:\test\abc.txt。 扫描结果将输出到命令行，无论是否指定了 /logFolder 选项。

命令返回值：

- -1 表示计算机上安装的应用程序版本不支持该命令。
- 0 表示命令已成功执行。
- 1 表示未将强制参数传递给命令。
- 2 表示发生一般性错误。
- 4 表示存在语法错误。
- 5 表示未找到一个或多个带有参数中指定的 YARA 规则的文件。

如果命令成功执行（返回值 0），并且在执行过程中检测到妥协的指标，Kaspersky Endpoint Security 将向命令行输出以下任务结果信息：

Started at <time> Finished at <time>	扫描的开始时间和完成时间。
Host name: <computer name>	检测到对象的计算机名称。
Result: <error>	运行任务时发生的错误的错误代码。如果没有错误，应用程序将输出 0x00000000。
Comment: <comment text>	运行任务时发生的错误的错误描述。例如，Operation timeout。
Object Name: 或者 Process: （扫描进程内存时）	触发 YARA 规则的对象或进程的名称。
Md5: <md5 hash> Sha256: <sha256 hash>	触发 YARA 规则的对象的哈希。
Rule Name	触发的 YARA 规则的名称。

`Meta:`
`Author: <author>`
`Date: <date>`
`Description: <description>`
	YARA 规则中指定的元数据。

`Detects:`
`Offset : String name : String data`
`<offset> : <string name> : <string data>`
	在对象中找到符合 YARA 规则条件的匹配项：
	• 进程内存或文件中检测到匹配项的偏移量（`Offset`）。
	• YARA 规则中匹配字符串的名称（`String name`）。
	• 进程内存或文件中的匹配字符串（`String data`）。

TELEMETRYFILTERS。过滤要发送到 KUMA 的事件

默认情况下，向 KUMA 服务器发送事件是禁用的。为确保 KUMA 正常工作，您必须启用遥测发送功能。您可以从标准日志中选择事件源：*Application*、*Security*或*System*。为了提高性能并优化向 KUMA 服务器的数据传输，您可以手动从遥测中添加或排除单个事件。例如，您可以排除 Sysmon 事件。

您可以从命令行将排除列表导出到 JSON 文件。

如果命令仅包含要导出设置的文件的名称，则应用程序将按如下方式放置文件：

- 如果将 avp.com 的路径添加到 %PATH% 系统变量中，则应用程序会将文件放置在 `C:\Windows\SysWOW64` 文件夹。
- 如果从应用程序安装文件夹运行该命令，则导出将失败，因为应用程序的自我保护会阻止在应用程序文件夹中创建新文件。要将应用程序设置导出到文件，请输入文件路径。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com TELEMETRYFILTERS /export <file name>
```

```
avp.com TELEMETRYFILTERS /import <file name>
```

操作	
`export`	导出要发送到 KUMA 的事件过滤器。
`import`	导入要发送到 KUMA 的事件过滤器。如果计算机上已经存在事件过滤规则，Kaspersky Endpoint Security 会在导入时替换这些规则。

要导出或导入的文件	
`<file name>`	要发送给 KUMA 的包含事件过滤器的文件的名称。您也可以输入文件路径。您可以将发送给 KUMA 的过滤器导出到 JSON 文件。

Light Agent 管理命令

您可以在 Light Agent 中管理应用程序以在命令行上保护虚拟环境。如果无法使用 Kaspersky Security Center 控制台进行管理，您可以在 Light Agent 模式下管理应用程序。您可以通过运行 `HELP` 命令来查看用于管理应用程序的命令列表。要阅读特定命令的语法，请输入 `HELP <command>`。

要从命令行管理 Light Agent 模式下的应用程序：

1. 以管理员身份运行命令行解释器 (cmd.exe)。
2. 转到 Kaspersky Endpoint Security 可执行文件所在文件夹。
3. 使用以下模板执行命令：

```
avp.com <command> [options]
```

结果，Kaspersky Endpoint Security 将执行该命令。

在 Light Agent 模式下安装的应用程序支持几乎所有以标准模式安装的应用程序的 AVP 命令。在 Light Agent 模式下，反病毒数据库更新任务和授权许可密钥管理任务受到限制。

KSVLAINFO。确定 Light Agent 模式

确定 Light Agent 模式。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com KSVLAINFO
```

该命令向控制台输出以下信息：

- 用于保护虚拟环境的 Light Agent 模式：启用或禁用。

  如果启用了 Light Agent 模式，应用程序将被用作 Kaspersky Security for Virtualization Light Agent 解决方案的一部分。

- VDI 保护模式：已启用或者已禁用。

  VDI 保护模式能够在临时虚拟机上优化 Kaspersky Endpoint Security 的性能。如果启用了 VDI 保护模式，则非持久虚拟机上不会安装需要重启受保护虚拟机的更新。在接收需要重新启动的更新时，非持久虚拟机上安装的 Light Agent 向 Kaspersky Security Center 发送消息，通知它受保护的虚拟机模板需要更新。

- 受保护虚拟机的类型：持久或非持久。
- 受保护虚拟机在虚拟基础架构中的角色：服务器或工作站。
- 标识符：UUID。

VIISINFO。Light Agent 与 Integration Server 的连接状态

查看 Agent 与 Integration Server 的连接信息。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com VIISINFO
```

该命令向控制台输出以下信息：

- Light Agent 连接的 Integration Server 的地址和端口。
- Integration Server 连接状态。
- Light Agent 与 Integration Server 之间最后一次连接的日期和时间。

SVMINFO。Light Agent 与 Protection Server 的连接状态

查看有关 Light Agent 与 Protection Server 的连接的信息。

要运行命令，请转到 Kaspersky Endpoint Security 可执行文件所在文件夹。您还可以将可执行文件路径添加到 %PATH% 系统变量并运行该命令，而无需导航到应用程序文件夹。

命令语法

```
avp.com SVMINFO
```

该命令向控制台输出以下信息：

- Light Agent 连接到的 SVM 的地址，以及虚拟基础架构中 SVM 相对于 Light Agent 的位置：本地或非本地。
- Light Agent 使用的 SVM 发现方法：使用 Integration Server 或使用 SVM 地址的自定义列表。
- 如果选择 SVM 地址列表作为 SVM 发现方法，则为 SVM 地址列表。
- 用于将 Light Agent 连接到 SVM 的标签。
- SVM 选择算法：标准或扩展。如果使用扩展 SVM 选择算法，还会显示 SVM 在虚拟基础架构中的路径类型。
- Light Agent 与 Protection Server 之间连接的保护状态。

错误代码

通过命令行使用应用程序时，可能会发生错误。发生错误时，Kaspersky Endpoint Security 会显示错误消息，例如，“`Error: Cannot start task 'EntAppControl'`”。Kaspersky Endpoint Security 还可以显示代码形式的其他信息，例如，`error=8947906D`（请参见下表）。

错误代码	描述
09479001	该密钥已在使用中。
0947901D	授权许可已到期，数据库更新不可用。
89479002	未找到密钥。
89479003	数字签名丢失或已损坏。
89479004	数据已损坏。
89479005	密钥文件已损坏。
89479006	授权许可已到期。
89479007	未指定密钥文件。
89479008	无效的密钥文件。
89479009	保存数据失败。
8947900A	读取数据失败。
8947900B	I/O 错误。
8947900C	未找到数据库。
8947900E	授权许可库未加载。
8947900F	数据库已损坏或已经手动更新。
89479010	数据库损坏。
89479011	不能使用无效的密钥文件添加备用密钥。
89479012	系统错误。
89479013	密钥拒绝列表已损坏。
89479014	文件数字签名与卡巴斯基的数字签名不符。
89479015	无法使用试用授权许可密钥做为商业授权许可密钥。
89479016	需要 Beta 测试授权许可以使用应用程序的 Beta 版本。
89479017	密钥文件与该应用程序不兼容。无法使用其他应用程序的密钥激活 Kaspersky Endpoint Security for Windows。请检查已安装的应用程序。
89479018	授权许可密钥被卡巴斯基阻止。
89479019	该应用程序已经使用了试用版授权许可。无法再次为试用版授权许可添加密钥。
8947901A	密钥文件已损坏。
8947901B	数字签名已丢失、已损坏或者与卡巴斯基数字签名不匹配。
8947901C	如果对应的非商业授权许可已到期，则无法添加密钥。
8947901E	密钥文件的创建或使用日期无效。请检查系统日期。
8947901F	无法添加试用版授权许可密钥: 已经在使用其他试用版授权许可密钥。
89479020	密钥拒绝列表已损坏或丢失。
89479021	更新描述丢失或已损坏。
89479022	密钥不适合此应用程序。
89479023	不能使用无效的密钥文件添加备用密钥。
89479025	发送激活服务器请求时出错。可能原因: 互联网连接错误或激活服务器临时故障。请稍后(1-2 小时后)尝试使用激活码激活应用程序。如果问题仍然存在，请联系您的互联网提供商。
89479026	请求包含错误的激活码。
89479027	无法获取响应状态。
89479028	保存临时文件时出错。

错误代码	描述
89479029	输入的激活码不正确，或计算机上设置的系统日期不正确。请检查计算机上的系统日期。
8947902A	密钥与该应用程序不兼容，或授权许可已到期
8947902B	无法接收密钥文件。输入了错误的激活码。
8947902C	激活服务器返回错误 400。
8947902D	激活服务器返回错误 401。
8947902E	激活服务器返回错误 403。
8947902F	激活服务器上的必要资源不可用。 激活服务器返回错误 404。 请检查互联网连接设置。
89479030	激活服务器返回错误 405。
89479031	激活服务器返回错误 406。
89479032	需要代理服务器身份验证，请检查您的网络设置。
89479033	请求超时。
89479034	激活服务器返回错误 409。
89479035	激活服务器上的必要资源不可用。 激活服务器返回错误 410。 请检查互联网连接设置。
89479036	激活服务器返回错误 411。
89479037	激活服务器返回错误 412。
89479038	激活服务器返回错误 413。
89479039	激活服务器返回错误 414。
8947903A	激活服务器返回错误 415。
8947903C	内部服务器错误。
8947903D	不支持该功能。
8947903E	网关响应无效。请检查您的网络设置
8947903F	资源暂时不可用。
89479040	网关响应超时。请检查您的网络设置。
89479041	服务器不支持该协议。
89479043	未知的 HTTP 错误。
89479044	无效的资源 ID。
89479046	无效网址。
89479047	目标文件夹无效。
89479048	内存分配错误。
89479049	将参数转换为 ANSI 字符串(URL、文件夹、代理)时出错。
8947904A	创建工作线程时出错。
8947904B	工作线程已运行。
8947904C	工作线程未运行。
8947904D	激活服务器上未找到密钥文件。
8947904E	密钥被阻止。
8947904F	激活服务器内部错误。
89479050	激活请求中的数据不足。
89479053	对应于所添加密钥的授权许可已到期。
89479054	计算机上的系统日期设置不正确。请检查系统日期值。
89479055	试用授权许可已到期。

错误代码	描述
89479056	应用程序激活期限已到期。
89479057	已超过使用指定激活码激活应用程序的最大数量。
89479058	激活过程返回系统错误
89479059	无法使用试用授权许可密钥做为商业授权许可密钥。
8947905C	需要激活码。
89479062	无法连接到激活服务器。
89479064	激活服务器不可用。请检查您的互联网连接设置并再次尝试激活。
89479065	授权许可已到期
89479066	无法用过期密钥代替活动密钥。
89479067	如果对应的授权许可在当前授权许可之前过期，则无法添加备用密钥。
89479068	更新的订阅密钥丢失。
8947906A	激活码无效。
8947906B	密钥已经激活。
8947906C	与活动和备用密钥相对应的授权许可类型不匹配。
8947906D	授权许可不支持组件
8947906E	无法添加订阅密钥作为备用密钥。
89479213	传输层一般错误
89479214	未能连接激活服务器
89479215	无效的网址格式
89479216	未能转换代理服务器地址
89479217	未能转换服务器地址，请检查互联网连接设置
89479218	服务器连接尝试失败
89479219	访问被远程拒绝
8947921A	操作超时
8947921B	发送 HTTP 请求时出错
8947921C	SSL 连接错误
8947921D	操作被回调函数中断
8947921E	重定向过多
8947921F	接受者检查失败
89479220	来自服务器的空响应
89479221	发送数据时出错
89479222	接收数据时出错
89479223	SSL 证书相关问题
89479224	SSL 加密相关问题
89479225	SSL 证书中心相关问题
89479226	无效的网络数据包内容
89479227	账户访问被拒绝
89479228	无效的 SSL 证书文件
89479229	无法断开 SSL 连接
8947922A	重复性错误

错误代码	描述
8947922B	无效的带有已撤销证书的文件
8947922C	SSL 证书请求错误
89479401	未知的服务器错误
89479402	内部服务器错误
89479403	所输入的激活码没有可用的密钥
89479404	活动密钥被阻止
89479405	激活请求所需的参数丢失
89479406	无效的客户端号码或密码
89479407	激活码无效。
89479408	激活码与该应用程序不兼容。无法使用其他应用程序的激活码激活 Kaspersky Endpoint Security for Windows。请检查已安装的应用程序。
89479409	需要激活码
8947940B	激活期限已到期
8947940C	该激活码的激活次数已超过限制
8947940D	请求 ID 的格式无效
8947940E	激活码已在使用中
8947940F	未能续期激活码
89479410	激活码在该区域无效
89479411	该激活码不适用于该本地化程序。
89479412	该激活码设计用于该程序的新版本，请获取其他激活码以激活所安装版本的程序
89479413	激活服务器返回错误 643
89479414	激活服务器返回错误 644
89479415	激活服务器返回错误 645
89479416	激活服务器返回错误 646
89479417	需要激活服务器版本 1.0
89479418	错误的激活码格式
89479419	计算机时间没有与激活服务器时间同步
8947941A	错误的程序版本
8947941B	订阅已到期
8947941C	超出激活数量
8947941D	无效的工单签名
8947941E	需要额外的数据
8947941F	数据验证失败
89479420	订阅未激活
89479421	激活服务器正在维护中
89479501	意外错误
89479502	传输的参数无效，例如激活服务器地址列表为空
89479503	激活码无效(哈希值无效)
89479504	无效的用户 ID
89479505	无效的用户密码

错误代码	描述
89479506	来自激活服务器的响应无效
89479507	激活请求已中断
89479509	激活服务器返回了空的转发列表

附录。应用程序配置文件

*配置文件*是 Kaspersky Endpoint Security 组件、任务或功能。配置文件用于从命令行管理应用程序。您可以使用配置文件执行 `START`、`STOP`、`STATUS`、`STATISTICS` 和 `EXPORT` 命令。使用配置文件，您可以配置应用程序设置（例如，`STOP DeviceControl`）或运行任务（例如，`START Scan_My_Computer`）。

以下配置文件可用：

- `AdaptiveAnomaliesControl` – 自适应异常控制
- `AMSI` – AMSI 保护
- `AntiCryptor`
- `BehaviorDetection` – 行为检测
- `DeviceControl` – 设备控制
- `EntAppControl` - 应用程序控制
- `File_Monitoring` 或者 `FM` – 文件威胁防护
- `Firewall` 或 `FW` – 防火墙
- `HIPS` – 主机入侵防御
- `IDS` – 关于网络威胁防护
- `IntegrityCheck` – 完整性检查
- `LogInspector` – 日志审查
- `Mail_Monitoring` 或 `EM` – 邮件威胁防护
- `Rollback` – 更新回滚（如果应用程序安装在 Light Agent 模式下，则无法应用配置文件）
- `Scan_ContextScan` – 从上下文菜单扫描
- `Scan_IdleScan` – 后台扫描
- `Scan_Memory` - 内核内存扫描
- `Scan_My_Computer` – 全盘扫描
- `Scan_Objects` – 自定义扫描

- `Scan_Qscan` - 扫描在操作系统启动时加载的对象
- `Scan_Removable_Drive` – 可移动驱动器扫描
- `Scan_Startup` 或 `STARTUP` – 关键区域扫描
- `Updater` – 更新（如果应用程序安装在 Light Agent 模式下，则无法应用配置文件）
- `Web_Monitoring` 或 `WM` – Web 威胁防护
- `WebControl` – Web 控制

Kaspersky Endpoint Security 还支持服务配置文件。联系 Kaspersky 技术支持时，可能需要服务配置文件。

通过 REST API 管理应用程序

Kaspersky Endpoint Security 允许您使用第三方解决方案配置应用程序设置，运行扫描，更新反病毒数据库以及执行其他任务。Kaspersky Endpoint Security 为此提供了一个 API。Kaspersky Endpoint Security REST API 通过 HTTP 运行，并且由一组请求/响应方法组成。换句话说，您可以通过第三方解决方案而不是本地应用程序界面或 Kaspersky Security Center 管理控制台来管理 Kaspersky Endpoint Security。

要开始使用 REST API，您需要安装带 REST API 支持的 Kaspersky Endpoint Security。REST 客户端和 Kaspersky Endpoint Security 必须安装在同一台计算机上。

要确保 Kaspersky Endpoint Security 和 REST 客户端之间的安全交互：

- 根据 REST 客户端开发者的建议配置对非授权访问 REST 的客户端保护。在 Discretionary Access Control List (DACL) 的帮助下配置对 REST 客户端文件夹的写入保护。
- 要运行 REST 客户端，使用带有管理员权限的账户。对该账户拒绝交互式系统登录。

通过位于 http://127.0.0.1 或 http://localhost 的 REST API 管理应用程序。无法通过 REST API 远程管理 Kaspersky Endpoint Security。

打开 REST API 文档

使用 REST API 安装应用程序

要通过 REST API 管理应用程序，您需要安装带 REST API 支持的 Kaspersky Endpoint Security。如果通过 REST API 管理 Kaspersky Endpoint Security，则无法使用 Kaspersky Security Center 管理该应用程序。

准备使用 REST API 安装应用程序

Kaspersky Endpoint Security 与 REST 客户端的安全交互需要配置请求标识。为此，您必须安装证书，然后对每个请求的有效负载进行签名。

要创建证书，您可以使用 OpenSSL 等。

```
例如：
$ openssl req -x509 -newkey rsa:4096 -keyout key.pem -out cert.pem -days 1825 -nodes
```

使用带有 2048 位或更长的密钥的 RSA 加密算法。

结果，您将获得一个 `cert.pem` 证书和一个 `key.pem` 私钥。

使用 REST API 安装应用程序

要安装带 REST API 支持的 Kaspersky Endpoint Security：

1. 以管理员身份运行命令行解释器 (cmd.exe)。
2. 转到包含 Kaspersky Endpoint Security 版本 11.2.0 或更高版本分发包的文件夹。
3. 使用以下设置安装 Kaspersky Endpoint Security：

   - `RESTAPI=1`
   - `RESTAPI_User=<user name>`

     用于通过 REST API 管理应用程序的用户名。输入格式为 `<DOMAIN>\<UserName>` 的用户名（例如，`RESTAPI_User=COMPANY\Administrator`）。您只能在此账户下通过 REST API 管理应用程序。您只能选择一个用户来使用 REST API。
   - `RESTAPI_Port=<port>`

     用于通过 REST API 管理应用程序的端口。默认情况下使用 6782 端口。确保端口空闲。可选参数。
   - `RESTAPI_Certificate=<path to certificate>`

     识别请求的证书（例如，`RESTAPI_Certificate=C:\cert.pem`）。

     您可以在安装应用程序后安装证书，也可以在证书过期后更新证书。

     如何为 REST API 请求标识安装证书

     1. 禁用 Kaspersky Endpoint Security 自我保护

        自我保护机制防止更改或删除硬盘驱动器上的应用程序文件、内存进程和系统注册表中的条目。
     2. 转到包含 REST API 设置的注册表键：
        `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\KasperskyLab\protected\KES\settings\RestAp`
     3. 输入证书路径，例如 `Certificate = C:\Folder\cert.pem`。
     4. 启用 Kaspersky Endpoint Security 自我保护。
     5. 重启应用程序。
   - `AdminKitConnector=1`

     使用管理系统管理应用程序。默认情况下允许管理。

   您还可以使用 setup.ini 文件来定义 REST API 的使用设置。

   例如：
   ```
   setup_kes.exe /pEULA=1 /pPRIVACYPOLICY=1 /pKSN=1 /pALLOWREBOOT=1 /pAdminKitConnector=1 /pRESTAPI=1
   /pRESTAPI_User=COMPANY\Administrator /pRESTAPI_Certificate=C:\cert.pem /s
   ```

结果，您将能够通过 REST API 管理应用程序。要验证其操作，请使用 GET 请求打开 REST API 文档。

```
例如：
GET http://localhost:6782/kes/v1/api-docs
```

如果您安装了支持 REST API 的应用程序，Kaspersky Endpoint Security 会在 Web 控件设置中自动创建一个允许规则，用于访问 Web 资源（*REST API 的服务规则*）。需要此规则才能允许 REST 客户端始终访问 Kaspersky Endpoint Security。例如，如果您限制了用户对 Web 资源的访问，这将不会影响通过 REST API 管理应用程序。建议您不要删除规则或更改 *REST API 服务规则*设置。如果您删除了该规则，Kaspersky Endpoint Security 将在重新启动应用程序后恢复该规则。

使用 API

无法使用密码保护通过 REST API 限制对应用程序的访问。例如，无法阻止用户通过 REST API 禁用保护。您可以通过 REST API 配置密码保护，并通过本地界面限制用户对应用程序的访问。

要通过 REST API 管理应用程序，需要在安装带 REST API 支持的应用程序时指定的账户下运行 REST 客户端。您只能选择一个用户来使用 REST API。

打开 REST API 文档

通过 REST API 管理应用程序包括以下步骤：

1. 获取应用程序设置的当前值。为此，请发送一个 GET 请求。

   ```
   例如：
   GET http://localhost:6782/kes/v1/settings/ExploitPrevention
   ```

2. 应用程序将发送包含设置的结构和值的响应。Kaspersky Endpoint Security 支持 XML 和 JSON 格式。

   ```
   例如：
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": true,
   "enabled": true
   }
   ```

3. 编辑应用程序设置。使用在对 GET 请求的响应中收到的设置结构。

   ```
   例如：
   {
   "action": 0,
   "enableSystemProcessesMemoryProtection": false,
   "enabled": true
   }
   ```

4. 将应用程序设置（有效负载）保存在 JSON (payload.json) 中。

5. 以 PKCS7 格式对 JSON 进行签名。

   ```
   例如：
   $ openssl smime -sign -in payload.json -signer cert.pem -inkey key.pem -nodetach -binary -outform pem -out signed_payload.pem
   ```

   如此，您将获得一个带有请求负载的签名文件 (`signed_payload.pem`)。

6. 编辑应用程序设置。为此，发送 POST 请求并附加签名文件到请求有效负载中 (`signed_payload.pem`)。

应用程序应用新设置并发送包含应用程序配置结果的响应（响应可以为空）。您可以使用 GET 请求验证设置是否已更新。

关于应用程序的信息源

本节描述了有关应用程序的信息来源。

您可以根据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 Kaspersky Endpoint Security 页面，您可以查看有关应用程序及其功能和特性的一般信息。

Kaspersky Endpoint Security 页面包含在线商店的链接。您可以在那里购买或更新应用程序。

知识库中的 Kaspersky Endpoint Security 页面

*知识库*是技术支持网站上的一个部分。

在知识库中的 Kaspersky Endpoint Security 页面，您可以阅读提供有关如何购买、安装和使用该应用程序的有用信息、建议和常见问题解答的文章。

知识库文章不仅可以回答与 Kaspersky Endpoint Security 相关的问题，还可以回答与其他卡巴斯基应用程序相关的问题。知识库中的文章还可能包含来自技术支持的新闻。

论坛中关于卡巴斯基应用程序的讨论

如果您的问题不需要紧急回答，您可以在我们的论坛上与卡巴斯基专家和其他用户讨论。

在论坛中，您可以查看现有主题、发表您自己的评论以及创建新的讨论主题。

联系技术支持

如果您无法在文档中或其他 Kaspersky Endpoint Security 相关信息源中找到您问题的解决方案，建议您联系技术支持。技术支持将回答您关于 Kaspersky Endpoint Security 安装和使用的问题。

Kaspersky 在应用程序的生存周期提供对 Kaspersky Endpoint Security 的支持（参见应用程序生存周期页）。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 门户向卡巴斯基实验室技术支持发送请求

将您的问题通知 Kaspersky 技术支持专家后，他们可能会请您创建一个*跟踪文件*。使用跟踪文件可以跟踪逐步执行应用程序命令的过程，并确定应用程序操作中发生错误的阶段。

技术支持专家可能还需要更多相关信息，关于操作系统、计算机中运行的进程、应用程序组件操作的详细报告。

运行诊断时，技术支持专家将要求您通过以下方式更改应用程序设置：

- 激活用于接收扩展诊断信息的功能。
- 通过更改无法通过标准用户界面访问的特殊设置来配置应用程序的各个组件。
- 更改诊断信息存储的设置。
- 配置网络流量的拦截和记录。

技术支持专家会提供执行这些操作所需的所有信息（步骤顺序说明、要修改的设置、配置文件、脚本、附加的命令行功能、调试模块、特定用途的实用程序等），并会告知您调试时所使用的数据的范围。扩展诊断信息保存在用户的计算机中。数据不会自动传输到 Kaspersky。

上述操作必须按照技术支持专家的说明，在其监督下执行操作。以在线帮助或技术支持建议中未描述的方式自行更改应用程序设置可能会导致操作系统速度减慢和崩溃，降低计算机的保护级别，并损坏正在处理的信息的可用性和完整性。

跟踪文件的内容和存储

您亲自负责计算机上存储的数据的安全性，尤其是在数据提交到 Kaspersky 前监控和限制对数据的访问。

只要应用程序在使用中，就会在计算机中存储跟踪文件，当应用程序被删除后，跟踪文件将被永久删除。

跟踪文件（身份验证代理的跟踪文件除外）存储在 `%ProgramData%\Kaspersky Lab\KES.14.1\Traces` 文件夹中。

跟踪文件按如下方式命名：`KES<14.1_dateXX.XX_timeXX.XX_pidXXX.><trace file type>.log`。

您可以查看跟踪文件中保存的数据。

所有跟踪文件都包含下列通用数据：

- 事件时间
- 执行线程编号

  > 身份验证代理跟踪文件不包含该信息。

- 引起该事件的应用程序组件
- 事件严重程度（通知性事件、警告、严重事件、错误）
- 关于应用程序组件命令执行和命令执行结果的事件说明。

SRV.log、GUI.log 和 ALL.log 跟踪文件的内容

`SRV.log`、`GUI.log` 和 `ALL.log` 跟踪文件可存储常规数据之外的下列信息：

- 个人数据，包括姓氏、名字和中间名，如果此数据包含在本地计算机文件的路径中。
- 计算机上安装的硬件的数据（如 BIOS/UEFI 固件数据）。当执行卡巴斯基磁盘加密时，此数据将写入跟踪文件。
- 用户名和密码，如果它们公开发送。在互联网流量扫描期间，此数据可被记录跟踪文件中。
- 用户名和密码，如果它们包含在 HTTP 标题中。
- Microsoft Windows 帐户名，如果该帐户名包含在文件名中。
- 包含您的帐户名和密码的电子邮件地址或网页地址，如果它们包含在被检测的对象名中。
- 您访问的网站和从这些网站被重定向的网站。当应用程序扫描网站时，将会把此数据写入跟踪文件。
- 登录代理服务器的代理服务器地址、计算机名称、端口、IP 地址和用户名。当应用程序使用代理服务器时，将会把此数据写入跟踪文件。
- 您的计算机要与其建立连接的远程 IP 地址。
- 邮件主题、ID、社交网络发件人网页的发件人名称和地址。当启用 Web 控制组件时，将会把此数据写入跟踪文件。
- 网络流量数据。如果启用流量监控组件（如 Web 控制），则此数据将写入跟踪文件。
- 从 Kaspersky 服务器接收的数据（如反病毒数据库的版本）。
- Kaspersky Endpoint Security 组件的状态及其操作数据。

- 应用程序中的用户活动的数据。
- 操作系统事件。

HST.log、BL.log、Dumpwriter.log、WD.log 和 AVPCon.dll.log 跟踪文件的内容

除了常规数据之外，`HST.log` 跟踪文件包含关于数据库执行和程序模块更新任务的信息。

除了常规数据之外，`BL.log` 跟踪文件包含应用程序运行期间发生的事件信息，以及对应用程序错误进行故障排除所需的数据。如果使用 avp.exe –bl 参数启动应用程序，将创建此文件。

除了常规数据之外，当进行应用程序内存转储时，`Dumpwriter.log` 跟踪文件包含对错误进行故障排除时的必要服务信息。

除了常规数据之外，`WD.log` 跟踪文件包含 avpsus 服务运行期间所发生的事件信息，包括应用程序模块更新事件。

除了常规数据之外，`AVPCon.dll.log` 跟踪文件包含 Kaspersky Security Center 连接模块运行期间所发生的事件信息。

性能跟踪文件的内容

性能跟踪文件按如下方式命名：`KES<14.1_dateXX.XX_timeXX.XX_pidXXX.>PERF.HAND.etl`。

除了常规数据，性能跟踪文件还包含有关处理器负载的信息、有关操作系统和应用程序的加载时间的信息以及有关正在运行的进程的信息。

AMSI 保护组件跟踪文件的内容

除了常规数据，`AMSI.log` 跟踪文件还包含有关对第三方应用程序的请求执行扫描的结果的信息。

“邮件威胁防护”组件的跟踪文件的内容

除常规数据外，跟踪文件 `mcou.OUTLOOK.EXE.log` 可能还包含电子邮件的一部分，包括电子邮件地址。

“从上下文菜单扫描”组件的跟踪文件的内容

除常规信息外，`shellex.dll.log` 跟踪文件还包含有关扫描任务完成情况的信息以及调试应用程序所需的数据。

应用程序 Web 插件的跟踪文件的内容

应用程序 Web 插件的跟踪文件存储在部署了 Kaspersky Security Center Web Console 的计算机上的 `Program Files\Kaspersky Lab\Kaspersky Security Center Web Console\logs` 文件夹中。

应用程序 Web 插件的跟踪文件按如下方式命名： `logs-kes_windows-<type of trace file>.DESKTOP-<date of file update>.log`。Web Console 在安装后开始写入数据，在删除 Web Console 后会删除跟踪文件。

除了常规数据外，应用程序 Web 插件的跟踪文件包含以下信息：

- 用于解锁 Kaspersky Endpoint Security 界面的 KLAdmin 用户密码（密码保护）。
- 用于解锁 Kaspersky Endpoint Security 界面的临时密码（密码保护）。
- SMTP 邮件服务器的用户名和密码（电子邮件通知）。
- Internet 代理服务器的用户名和密码（代理服务器）。
- "*更改应用程序组件*"任务的用户名和密码。
- 在 Kaspersky Endpoint Security 任务和策略属性中指定的账户凭据和路径。

身份验证代理跟踪文件的内容

身份验证代理跟踪文件保存在 System Volume Information 文件夹中，并按如下方式命名： `KLFDE.{EB2A5993-DFC8-41a1-B050-F0824113A33A}.PBELOG.bin`。

除了常规数据之外，身份验证代理跟踪文件包含身份验证代理运行信息和用户使用身份验证代理所执行操作的信息。

应用程序操作跟踪

*应用程序跟踪*是应用程序执行的操作以及有关应用程序运行期间发生的事件的消息的详细记录。在跟踪过程中，应用程序创建带有有关不同应用程序组件的操作的数据的一组文件（例如，SRV.log、WD.log 等）。

> 应用程序跟踪应在 Kaspersky 技术支持的监督下执行。

要创建应用程序跟踪文件：

1. 打开主应用程序窗口并单击 按钮。
2. 在打开的窗口中，单击"**支持工具**"按钮。
3. 使用**启用应用程序跟踪**开关启用或禁用应用程序操作跟踪。

4. 在**跟踪**下拉列表，选择应用程序跟踪模式：

   - “**有大小限制**”。将跟踪保存到有限数量的大小有限的文件集中，并在达到最大大小时覆盖旧文件。如果该模式被选择，您可以定义用于循环的文件集的最大数量和每个文件集的最大大小。

     默认情况下，应用程序保存五组跟踪文件。每组文件的大小为 3072 MB。这样，您需要 15 GB 的可用磁盘空间来保存跟踪文件。

   - “**没有限制**”。保存一个跟踪文件（无大小限制）。

5. 在“**级别**”下拉列表中，选择跟踪级别：

   - **正常**，意味着跟踪文件保存有关所有错误、警告的消息，以及有关应用程序正常运行的信息（默认）。

   - **详细**，意味着跟踪文件保存有关应用程序运行的所有信息。

   如果您在命令行上管理应用程序跟踪设置，则可以获得其他跟踪级别。我们建议您通过技术支持专家了解所需跟踪级别。如果技术支持专家未提供指导，请将跟踪级别设置为“**正常**”。

   > 如果在命令行上启用了应用程序跟踪，并且设置的跟踪级别不是**正常**或者**详细**，则**级别**下拉列表设置为**正常**。

6. 要停止跟踪进程，返回**支持工具**窗口并禁用跟踪。

> 您也可以在从命令行安装应用程序时（包括使用 setup.ini 文件）创建跟踪文件。

结果，将在文件夹 `%ProgramData%\Kaspersky Lab\KES.14.1\Traces` 中创建应用程序操作跟踪文件。创建跟踪文件后，将文件发送给卡巴斯基技术支持。

Kaspersky Endpoint Security 在应用程序被卸载后自动删除跟踪文件。您也可以手动删除文件。为此，您必须禁用跟踪并停止应用程序。

应用程序性能跟踪

Kaspersky Endpoint Security 允许您在使用应用程序时接收有关计算机操作问题的信息。例如，您可以在安装应用程序后收到有关操作系统加载延迟的信息。为此，Kaspersky Endpoint Security 会创建性能跟踪文件。*性能跟踪*是指为了诊断 Kaspersky Endpoint Security 的性能问题而对应用程序执行的操作进行记录。为接收信息，Kaspersky Endpoint Security 使用 Windows 事件跟踪服务 (ETW)。Kaspersky 技术支持负责诊断 Kaspersky Endpoint Security 的问题并确定这些问题的原因。

> 应用程序跟踪应在 Kaspersky 技术支持的监督下执行。

要创建性能跟踪文件：

1. 打开主应用程序窗口并单击 ⚙ 按钮。

2. 在打开的窗口中，单击“**支持工具**”按钮。

3. 使用**启用性能跟踪**开关启用或禁用应用程序性能跟踪。

4. 在**跟踪**下拉列表，选择应用程序跟踪模式：

   - “**有大小限制**”。将跟踪保存到有限数量的大小有限的文件中，并在达到最大大小时覆盖旧文件。如果该模式被选中，您可以为每个文件定义最大大小。

   - “**没有限制**”。保存一个跟踪文件（无大小限制）。

5. 在“**级别**”下拉列表中，选择跟踪级别：

   - “**轻度**”。Kaspersky Endpoint Security 会分析与性能相关的最重要的操作系统进程。

   - “**详细**”。Kaspersky Endpoint Security 会分析与性能相关的所有操作系统进程。

6. 在“**跟踪类型**”下拉列表中，选择跟踪类型：

   - “**基本信息**”。Kaspersky Endpoint Security 在操作系统运行时分析进程。如果在加载操作系统后问题仍然存在（例如在浏览器中访问 Internet 时出现问题），请使用此跟踪类型。

   - “**重启时**”。Kaspersky Endpoint Security 仅在操作系统加载时分析进程。操作系统加载后，Kaspersky Endpoint Security 将停止跟踪。如果问题与操作系统的延迟加载有关，请使用此跟踪类型。

7. 重新启动计算机并尝试重现该问题。

8. 要停止跟踪进程，返回支持工具窗口并禁用跟踪。

结果，将在文件夹 `%ProgramData%\Kaspersky Lab\KES.14.1\Traces` 中创建性能跟踪文件。创建跟踪文件后，将文件发送给 Kaspersky 技术支持。

转储写入

转储文件包含该文件创建时 Kaspersky Endpoint Security 进程的工作内存的所有相关信息。

> 已保存的转储文件可能包含机密数据。要控制对数据的访问，必须单独确保转储文件的安全性。

只要应用程序在使用中，就会在计算机中存储转储文件，当应用程序被卸载后，转储文件将被永久删除。转储文件存储在 `%ProgramData%\Kaspersky Lab\KES.14.1\Traces` 文件夹中。

如何在管理控制台（MMC）中启用转储写入

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。

2. 选择必要的策略并双击以打开策略属性。

3. 在策略窗口中，选择 **常规设置** → **应用程序设置**。

4. 在“**调试信息**”块中单击“**设置**”按钮。

5. 在打开的窗口中，使用“**启用转储写入**”复选框启用或禁用应用程序转储写入。

6. 保存更改。

如何在 Web Console 和云控制台中启用转储写入

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **技术支持**。
5. 在**调试信息**块，使用**转储写入已启用**复选框启用或禁用应用程序转储写入。
6. 保存更改。

如何在应用程序界面中启用转储写入

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**应用程序设置**”。

Kaspersky Endpoint Security for Windows 设置

3. 在**调试信息**块，使用**启用转储写入**复选框启用或禁用应用程序转储写入。
4. 保存更改。

保护转储文件和跟踪文件

转储文件和跟踪文件包含操作系统的信息，可能还包含用户数据。为了防止未经授权地访问此类数据，您可以启用保护转储文件和跟踪文件。

如果启用了转储文件和跟踪文件保护，则以下用户可以访问这些文件：

- 系统管理员和本地管理员以及启用写入转储文件和跟踪文件的用户可以访问转储文件。
- 只有系统管理员和本地管理员可以访问跟踪文件。

如何在管理控制台 (MMC) 中启用转储文件和跟踪文件的保护

1. 在 Kaspersky Security Center 管理控制台树中，选择“**策略**”。
2. 选择必要的策略并双击以打开策略属性。
3. 在策略窗口中，选择 **常规设置** → **应用程序设置**。
4. 在“**调试信息**”块中单击“**设置**”按钮。
5. 在打开的窗口中，使用“**启用转储和跟踪文件保护**”复选框启用或禁用文件保护。
6. 保存更改。

如何在 Web Console 和云控制台中启用对转储文件和跟踪文件的保护

1. 在 Web Console 的主窗口中，选择“**资产管理**” → “**策略**”。
2. 单击 Kaspersky Endpoint Security 策略的名称。
   策略属性窗口将打开。
3. 选择**应用程序设置**选项卡。
4. 选择 **常规设置** → **技术支持**。
5. 在**调试信息**块，使用**转储和跟踪文件保护已启用**复选框启用或禁用文件保护。
6. 保存更改。

如何在应用程序界面中启用对转储文件和跟踪文件的保护

1. 打开主应用程序窗口并单击 ⚙ 按钮。
2. 在应用程序设置窗口中，选择“**常规设置**” → “**应用程序设置**”。

Kaspersky Endpoint Security for Windows 设置

3. 在**调试信息**块，使用**启用转储和跟踪文件保护**复选框启用或禁用文件保护。
4. 保存更改。

保护有效期间写入的转储文件和跟踪文件即使该功能被禁用也会保持为保护状态。

获取操作系统数据（Kaspersky Get System Info）

安装 Kaspersky Endpoint Security 应用程序后，操作系统或应用程序可能无法正常运行。应用程序与计算机组件的软件或驱动程序之间存在冲突。

为了确定问题的原因，卡巴斯基技术支持需要 Kaspersky Get System Info 实用程序（以下简称 GSI）的报告。有关使用实用程序的详细信息，请参阅卡巴斯基知识库。

限制和警告

Kaspersky Endpoint Security 设计了众多不会影响应用程序运行的限制。

安装应用程序

- 有关对 Microsoft Windows 10、Microsoft Windows Server 2016 和 Microsoft Windows Server 2019 操作系统的支持的详细信息，请参阅技术支持知识库。
- 有关对 Microsoft Windows 11 和 Microsoft Windows Server 2022 操作系统的支持的详细信息，请参阅技术支持知识库。
- 在被安装到已感染的计算机后，应用程序不通知用户运行计算机扫描。您可能在激活应用程序时遇到问题。要解决这些问题，启动关键区域扫描。
- 如果非 ASCII 字符（例如，俄罗斯字符）被用于 setup.ini 和 setup.reg 文件，建议您使用 notepad.exe 编辑文件并使用 UTF-16LE 编码保存文件。其他编码不被支持。
- 在安装包设置中指定应用程序安装路径时，应用程序不支持使用非ASCII字符。
- 从 CFG 文件导入应用程序设置时，不应用参与卡巴斯基安全网络定义的设置值。导入设置后，请阅读卡巴斯基安全网络声明的文本并确认您同意加入卡巴斯基安全网络。您可以在应用程序界面或包含应用程序分发包的文件夹中的 ksn_*.txt 文件中读取声明的文本。
- 如果要卸载并重新安装加密（FLE 或 FDE）或设备控制组件，则必须在重新安装之前重新启动系统。
- 使用 Microsoft Windows 10 操作系统时，必须在删除文件级加密（FLE）组件后重新启动系统。
- 删除单个应用程序组件时（例如，使用"*更改应用程序组件*"任务），可能需要重新启动计算机。
- 在"*更改应用程序组件*"任务的属性中，当切换安装模式（**单独模式/组合模式**）时，不支持模式间组件集的同步。重新打开任务属性后，应用程序会在模式之间同步组件集。
- 应用程序的安装可能会以错误结束，提示*您的计算机上安装了名称缺失或不可读的应用程序*。这意味着不兼容的应用程序或其碎片仍保留在您的计算机上。要删除不兼容应用程序的工件，请通过 Kaspersky CompanyAccount 向 Kaspersky 技术支持部门发送一份请求，其中包含对情况的详细描述。
- 如果您取消了 Kaspersky Endpoint Security 的删除，请在重新启动计算机后开始应用程序恢复。
- 应用程序需要 Microsoft .NET Framework 4.0 或更高版本。Microsoft .NET Framework 4.6.1 存在漏洞。如果您正在使用 Microsoft .NET Framework 4.6.1，您必须安装安全更新。关于 Microsoft .NET Framework 安全更新的详情，请参考 Microsoft 技术支持网站。
- 如果在服务器操作系统中选择了 Kaspersky Endpoint Agent 组件而未能成功安装应用程序，并且出现了 *Windows Installer Coordinator 错误*窗口，请参阅 Microsoft 技术支持网站上的说明。
- 如果应用程序是以非交互模式本地安装的，请使用提供的 setup.ini 文件替换已安装的组件。
- 在 Kaspersky Endpoint Security for Windows 被安装到 Windows 7 上后，Windows Defender 继续工作。建议您手动禁用 Windows Defender 以防止系统性能降低。

- 在安装了 Kaspersky Security for Windows Server (KSWS) 和 Windows Defender 应用程序的服务器上安装 Kaspersky Endpoint Security for Windows 时，您必须重新启动系统。即使启用了安装应用程序而不重新启动系统，也需要重新启动系统。Windows Defender for Windows Server 包含在与 Kaspersky Endpoint Security for Windows 不兼容的软件列表中。安装应用程序之前，安装程序会卸载 Windows Defender for Windows Server。卸载不兼容的软件使系统重新启动成为必要。

- 在安装了 Kaspersky Security for Windows Server (KSWS) 的服务器上安装 Kaspersky Endpoint Security for Windows (KES) 之前，您必须关闭 KSWS 密码保护。从 KSWS 迁移到 KES 后，请在应用程序设置中启用密码保护。

- 要在运行 Windows 7 或 Windows Server 2008 R2 并部署了"Veeam Backup & Replication"软件的计算机上安装应用程序，您可能需要重新启动计算机并再次运行安装。

- 从 KSOS 21.16.*.* 版本开始，可以从 Kaspersky Small Office Security (KSOS) 迁移到启用了密码保护的 Kaspersky Endpoint Security (KES)。要迁移早期版本的 KSOS，必须禁用密码保护或手动删除 KSOS。已正确执行从 KSOS 到禁用密码保护的 KES 的迁移。

- 您无法在可启动的可移动驱动器上安装 Kaspersky Endpoint Security。安装时，Kaspersky Endpoint Security 显示错误消息：*您选择的文件夹或磁盘无效，程序必须安装在本地磁盘磁盘上*。如果您设法使用第三方工具将应用程序安装在可移动驱动器上，这可能会导致操作系统在启动过程中崩溃（BSOD）。这意味着 Kaspersky Endpoint Security 不支持 Windows To Go 和类似的解决方案。要从可移动驱动器扫描计算机，您可以使用免费使用的卡巴斯基应急磁盘 应用程序。

- 在具有多用户 RDP 会话的终端服务器上安装带有网络组件的 Kaspersky Endpoint Security 需要注意一些特殊事项。管理员会话结束后，操作系统强制所有用户会话结束。要连接到终端服务器，您必须重新启动服务器或在本地登录系统。这种行为是由 Windows 操作系统的特性决定的。

- 如果 Kaspersky Endpoint Security for Windows（内部版本 12.11.0.2004）和 Kaspersky Endpoint Security for Linux（内部版本 12.4.0.1354）的 Web 插件安装在 Kaspersky Security Center 16.0 或 Kaspersky Security Center 16.1 中，则将 Kaspersky Endpoint Security for Windows Web 插件更新到 12.11.0.6004 版本可能会导致 Kaspersky Endpoint Security for Linux 策略出现故障。

  可能的解决方案：转到"**设置**" → "**Web 插件**"窗口，并从列表中删除 Kaspersky Endpoint Security for Windows Web 插件、Kaspersk Endpoint Security for Linux Web 插件和 Unified Protection and Management Plug-in。然后，首先安装 Kaspersky Endpoint Security for Linux Web 插件，然后安装 Kaspersky Endpoint Security for Windows Web 插件。

- 在 Web Console 中， Kaspersky Endpoint Security 12.11 for Windows 的安装包属性中的组件列表显示不正确。此版本的应用程序中不提供单独的反加密组件 。行为检测组件中包含了保护共享文件夹免受外部加密的功能。在 Kaspersky Endpoint Security 12.12 for Windows 中，此功能是一个单独的组件。同时，在管理控制台（MMC）中，组件列表显示正确。

升级应用程序

- 从 11.0.0 应用程序版本开始，您可以在先前插件版本的基础上安装 Kaspersky Endpoint Security for Windows MMC 插件。要返回到先前的插件版本，请删除当前插件并安装该插件的先前版本。

- 升级 Kaspersky Endpoint Security 11.0.0 或 11.0.1 for Windows 时，不会保存"*数据库和应用程序模块更新*"、"*关键区域扫描*"、"*自定义扫描*"和"*应用程序完整性检查*"任务的本地任务计划设置。

- 在运行 Windows 10 版本 1903 和 1909 的计算机上，从安装了文件级加密(FLE)组件的 Kaspersky Endpoint Security 10 for Windows Service Pack 2 Maintenance Release 3 (内部版本 10.3.3.275)、Service Pack 2 Maintenance Release 4 (内部版本 10.3.3.304)、11.0.0 和 11.0.1 升级可能会以错误结束。这是因为在 Windows 10 版本 1903 和 1909 中，这些版本的 Kaspersky Endpoint Security for Windows 不支持文件加密。建议您在安装此升级之前删除文件加密组件。

- 应用程序需要 Microsoft .NET Framework 4.0 或后续版本。Microsoft .NET Framework 4.6.1 具有漏洞。如果您正在使用 Microsoft .NET Framework 4.6.1，您必须安装安全更新。关于 Microsoft .NET Framework 安全更新的详情，请参考 Microsoft 技术支持网站。

- 等升级 Kaspersky Endpoint Security 时，应用程序禁用 KSN 的使用，直到卡巴斯基安全网络声明被接受。此外，Kaspersky Security Center 中的计算机状态可能变成"*严重*"；您会接收到"*KSN 服务器不可用*"事件。如果您使用 Kaspersky Managed Detection and Response，您将收到有关解决方案操作中违规的事件。Kaspersky Managed Detection and Response 的操作需要使用 KSN。Kaspersky Endpoint Security 在应用管理员接受 KSN 使用条款的策略后启用对 KSN 的使用。一旦卡巴斯基安全网络声明被接受，Kaspersky Endpoint Security 便恢复其操作。

- 不重启而将 Kaspersky Endpoint Security 升级到 11.10.0 或更高版本后，计算机将安装两个 Kaspersky Endpoint Security 应用程序。不要手动卸载应用程序的早期版本。重新启动计算机时，将自动卸载以前的版本。

- 在运行 Microsoft Windows 11 的计算机上升级 Kaspersky Endpoint Security 后，文件上下文菜单可能会显示先前和新应用程序版本的条目。重新启动计算机两次以确保文件上下文菜单的正确操作。

- 如果关闭应用程序的自我保护并停止所有网络适配器，则在应用程序升级结束和计算机重新启动之间，应用程序的网络组件将无法工作。该应用程序的网络组件包括 Web 威胁防护、邮件威胁防护、网络威胁防护、防火墙、主机入侵防御和 Web 控制。重新启动计算机以使应用程序正常工作。

- BadUSB 攻击防护组件在应用程序升级结束和计算机重新启动之间不起作用。重新启动计算机以使应用程序正常工作。

- 如果之前的升级过程尚未完成，则无法升级应用程序。重新启动计算机以使应用程序正常工作。

- 应用程序从早于 Kaspersky Endpoint Security 11 for Windows 的版本升级后，必须重新启动计算机。

- 如果您使用 Kaspersky Security Center 云控制台管理 Kaspersky Endpoint Security，则不允许在本地更新应用程序。在本地更新应用程序时，无法接受 Kaspersky Security Center 云控制台的数据处理协议。

对 Arm 架构的支持

- 不支持在基于 Arm 的虚拟机上以 Light Agent 模式安装 Kaspersky Endpoint Security。

- 卡巴斯基磁盘加密不支持基于 Arm 的计算机。

- 基于 Arm 架构的计算机不支持文件加密。

- 基于 Arm 架构的计算机不支持对可移动驱动器加密。

- 在运行 Windows 11 for Arm64 的计算机上，EDR Agent 与以下系统不兼容：Bitdefender Endpoint Security Tools。

- 基于 Arm 架构的计算机不支持音频信号保护功能和网络摄像头访问保护功能。

- 在基于 Arm 的计算机上，邮件威胁防护扩展程序支持 32 位和 64 位版本的 Outlook 2016、Outlook 2021、Outlook 2024 和 Outlook 365 for Arm64。

- Kaspersky Endpoint Security 不会将面向 Arm 架构的对象发送到 Kaspersky Sandbox。

- 基于 Arm 架构的计算机不支持打印控制。

- 在基于 Arm 的计算机上不支持与 Kaspersky Endpoint Detection and Response Expert (cloud) 集成。

- 在基于 Arm 的计算机上，“*IOC 扫描*”任务仅支持来自以下邮件客户端的电子邮件文件：适用于 Arm64 的 Outlook 2016 和 Outlook 2021、2024 和 365 的 32 位和 64 位版本。

支持服务器平台

- 在启用了“*重复数据删除*”的服务器上，您需要添加 fsdmhost.exe 文件到受信任的应用程序列表。这有助于优化应用程序的性能并防止 CPU 负载过大。

- ReFS 文件系统被有限制支持：

  - Kaspersky Endpoint Security 可能会错误地处理威胁清除事件。例如，如果应用程序删除了恶意文件，则报告可能有一个“对象未处理”条目。同时，Kaspersky Endpoint Security 根据应用程序设置清除威胁。Kaspersky Endpoint Security 也可以为相同对象创建*对象将在重启后清除*事件。

  - 文件威胁防护可能会跳过某些威胁。同时，恶意软件扫描工作正常。

  - 启动*恶意软件扫描*任务后，当服务器重新启动时，将重置使用 iChecker 添加的扫描排除项。

  - iSwift 技术不被支持。Kaspersky Endpoint Security 不考虑使用 iSwift 技术添加的扫描排除。

  - 如果在安装 Kaspersky Endpoint Security 之前计算机上存在 meicar.exe 文件，则 Kaspersky Endpoint Security 不会检测 eicar.com 和 susp-eicar.com 文件。

  - Kaspersky Endpoint Security 可能错误地显示威胁清除通知。例如，应用程序可能显示先前清除的威胁的通知。

- 服务器平台不支持文件级加密（FLE）和卡巴斯基磁盘加密技术（FDE）技术。同时，Kaspersky Endpoint Security 可能错误地处理数据加密事件。

- 在服务器操作系统中，不会显示有关需要高级清除的警告。

- Microsoft Windows Server 2008 已从支持范围中排除。不支持在运行 Microsoft Windows Server 2008 操作系统的计算机上安装该应用程序。

- 安装在部署了 Microsoft Data Protection Manager (DPM) 的服务器上的 Kaspersky Endpoint Security 可能会导致 DPM 出现故障。这与 DPM 操作中的限制有关。为了消除故障，您应该将本地服务器驱动器添加到文件威胁防护组件和*恶意软件扫描*任务的排除项中。

- Server Core 模式受到以下限制：

  - 本地图形用户界面不可用，包括通知、弹出通知和其他界面控件。应用程序无法显示提示窗口，包括以下窗口：

    - 应用程序版本和模块升级确认提示；

    - 计算机重启提示；

    - 提示输入代理服务器身份验证凭据；

    - 获取设备访问权限的提示（设备控制）。

  - 以下组件不可用：Web 威胁防护、邮件威胁防护、Web 控制、BadUSB 攻击防护。

  - 反桥接不可用。

- 您只能接受 Kaspersky Security Center 控制台中应用程序策略中的卡巴斯基安全网络声明。
- BitLocker 驱动器加密仅适用于受信任的平台模块（TPM）。PIN/密码不能用于加密，因为应用程序无法显示预引导身份验证的密码提示窗口。如果操作系统已启用联邦信息处理标准（FIPS）兼容模式，请在开始加密驱动器之前连接可移动驱动器以保存加密密钥。

支持的虚拟平台

- Hyper-V 虚拟机上不支持完整磁盘加密（FDE）。
- 在 Citrix 虚拟平台上不支持完整加密（FDE）。
- 支持 Windows 10 Enterprise 多会话，但有以下限制：
  - Kaspersky Endpoint Security 清除活动威胁而不通知用户，就像清除服务器上的活动威胁时。由于操作系统继续以多会话模式运行，如果威胁未立即解决，其他活动用户可能会丢失其数据。
  - 完整磁盘加密 (FDE)不被支持。
  - BitLocker 管理不被支持。
  - 对可移动驱动器使用 Kaspersky Endpoint Security 不被支持。Microsoft Azure 基础架构定义可移动驱动器为网络驱动器。
- 不支持在 Citrix 虚拟平台上安装和使用文件级加密（FLE）。
- 要支持 Kaspersky Endpoint Security for Windows 与 Citrix PVS 的兼容性，请在启用“**确保与 Citrix PVS 兼容**”选项的情况下执行安装。此选项可以在安装向导中启用，也可以使用命令行参数 `/pCITRIXCOMPATIBILITY=1` 来启用。在远程安装的情况下，必须通过添加以下参数来编辑 KUD 文件：`/pCITRIXCOMPATIBILITY=1`。
- Citrix XenDesktop。开始克隆之前，必须禁用自我保护才能克隆使用 vDisk 的虚拟机。
- 在为预装了 Kaspersky Endpoint Security for Windows 和 Kaspersky Security Center 网络代理的 Citrix XenDesktop 主映像准备模板计算机时，请将以下类型的排除项添加到配置文件中：

  ```
  [Rule-Begin]
  Type=File-Catalog-Construction
  Action=Catalog-Location-Guest-Modifiable
  name="%ALLUSERSPROFILE%\Kaspersky Lab\**\*"
  name="%ALLUSERSPROFILE%\KasperskyLab\**\*"
  [Rule-End]
  ```

  对于 Citrix XenDesktop 的详情，请访问 Citrix 支持网站。
- 在某些情况下，在部署在 VMware ESXi hypervisor 上的虚拟机上，尝试安全断开可移动驱动器的连接可能会失败。再次尝试安全断开设备。
- Kaspersky Endpoint Security 与 VMware ESXi Hypervisor 兼容，但有以下限制：
  - Kaspersky Endpoint Security 可能与 Guest Introspection 驱动程序（vnetWFP.sys、vnetFLT.sys 等）不兼容。要解决不兼容问题，请将驱动程序更新到最新版本或卸载驱动程序。
  - 在某些情况下，尝试安全删除虚拟机上的可移动磁盘可能会失败。再次尝试安全断开设备。

- 在具有 Citrix VDA 代理的虚拟机上安装 Kaspersky Endpoint Security 可能会出现兼容性错误。发生这种情况是因为 Citrix Provisioning Services 与反病毒解决方案的兼容性有限。有关将反病毒解决方案与 Citrix Provisioning Services 结合使用的最佳实践，请参阅 Citrix 支持网站。

- 如果可移动驱动器驱动器连接到 Citrix Hypervisor 上的虚拟机，Kaspersky Endpoint Security 将跳过对该驱动器的扫描（*可移动驱动器扫描*任务）。在这样的设备上，操作系统会将连接的可移动驱动器识别为网络驱动器。在这种情况下，您可以使用*自定义扫描*任务。应用程序在标准模式和 Light Agent 模式下的行为是相同的。

- 如果 Kaspersky Endpoint Security 安装在采用 Citrix App Layering 技术的基础架构中的虚拟机上，则应用程序检测到的感染状态为"*对象将在重启后删除*"的文件在虚拟机重新启动时不会自动删除。

  要删除此类文件，您必须将包含用户层的 VHDX 文件挂载到 Citrix App Layering 管理员的计算机上，并对挂载的磁盘运行恶意软件扫描。

与 Kaspersky Security Center 的兼容性

- 在 Kaspersky Security Center Web Console 14.1 和更早版本中，日志检查和文件完整性监控组件的功能区域名称未正确显示在管理服务器属性的用户访问权限设置部分。

- 修复应用程序后，将禁用对计算机与管理服务器连接的保护。修复应用程序后，请再次运行"*管理服务器连接保护*"任务。

- 在 Kaspersky Security Center 管理控制台中，"**选择一个用户或一组用户**"窗口仅显示 Kaspersky Security Center 用户列表中的前 50,000 个用户。有关详细信息，请参见 Kaspersky Security Center 帮助。

- 在 Kaspersky Security Center 管理控制台中搜索受管理设备时，"**应用程序组件**"选项卡可能会同时显示同一应用程序组件名称的多个变体，包括与旧版 Kaspersky Endpoint Security 对应的名称。某些组件的名称也可能重复。

  要按组件搜索，您只需选择显示的其中一个变体即可。有关设备发现的详细信息，请参阅 Kaspersky Security Center 帮助。

授权许可

- 如果显示*错误接收数据*系统消息，请验证执行激活的计算机是否具有网络访问权限，或通过 Kaspersky Security Center 激活代理配置激活设置。

- 在应用程序界面中，授权许可到期日期以计算机的本地时间显示。

- 在互联网访问不稳定的计算机上安装带有嵌入密钥文件的应用程序可能会导致临时显示事件，提示应用程序未激活或授权许可不允许组件操作。这是因为在安装过程中应用程序首先激活了嵌入式试用授权许可。它需要互联网接入。

- 在试用期内，在互联网访问不稳定的计算机上安装任何应用程序升级或补丁程序可能会导致临时显示事件，提示应用程序未激活。这是因为在更新安装过程中应用程序首先激活了嵌入式试用授权许可。它需要互联网接入。

- 如果在应用程序安装过程中自动激活了试用授权许可，然后在未保存授权许可信息的情况下卸载了该应用程序，则在重新安装时，将不会使用试用授权许可自动激活该应用程序。在这种情况下，请手动激活应用程序。

- 如果您使用的是 Kaspersky Security Center 版本 11 和 Kaspersky Endpoint Security 版本 14.1，组件性能报告可能工作不正确。如果您安装了不包括在授权许可中的 Kaspersky Endpoint Security 组件，网络代理可能会把组件状态错误发送到 Windows 事件日志。为了避免错误，请删除不包括在授权许可中的组件。

邮件威胁防护

- 使用 Microsoft Outlook 的邮件威胁防护扩展程序扫描邮件时，建议您使用缓存的 Exchange 模式（“使用缓存的 Exchange 模式”选项）。
- Kaspersky Endpoint Security 不支持 64 位版本的 Microsoft Outlook 邮件客户端。这意味着，如果计算机上安装了 64 位版本的 Microsoft Outlook，即使邮件包含在扫描范围内，Kaspersky Endpoint Security 也不会扫描 Microsoft Outlook 文件（PST 和 OST 文件）。
- Kaspersky Endpoint Security 不支持 Microsoft Outlook New 邮件客户端。

修复引擎

- 应用程序只能还原文件系统为 NTFS 或 FAT32 的设备上的文件。
- 应用程序可恢复最大 100 MB 的文件。
- 应用程序可还原具有以下扩展名的文件：odt, ods, odp, odm, odc, odb, doc, docx, docm, wps, xls, xlsx, xlsm, xlsb, xlk, ppt, pptx, pptm, mdb, accdb, pst, dwg, dxf, dxg, wpd, rtf, wb2, pdf, mdf, dbf, psd, pdd, eps, ai, indd, cdr, jpg, jpe, dng, 3fr, arw, srf, sr2, bay, crw, cr2, dcr, kdc, erf, mef, mrw, nef, nrw, orf, raf, raw, rwl, rw2, r3d, ptx, pef, srw, x3f, der, cer, crt, pem, pfx, p12, p7b, p7c, 1cd。
- 无法还原位于网络驱动器或可擦写 CD/DVD 上的文件。
- 无法还原使用加密文件系统 (EFS) 加密的文件。有关 EFS 操作的详细信息，请访问 Microsoft 网站。
- 应用程序不会监控由操作系统内核级别的进程对文件执行的修改。

防火墙

- 如果网络包规则或应用程序网络规则指定了 DNS 名称， Kaspersky Endpoint Security 可能会向 DNS 服务器发送请求以确定这些资源的 IP 地址。防火墙使用 IP 地址来监控网络活动。因此应用程序将 DNS 名称解析为 IP 地址。建议您在规则中仅对 LAN 计算机或内部服务使用 DNS 名称。
- 要为所有 IPv6 地址指定规则，请添加 ::-ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff 地址范围。防火墙不支持 ::/0 掩码。
- 在以下情况下，支持按本地地址、物理接口和数据包生存时间（TTL）过滤数据包或连接：
  - 在 TCP 和 UDP 应用程序规则和数据包规则中，为出站数据包或连接按本地地址。
  - 在阻止应用程序规则和数据包规则中，按入站数据包或连接（UDP 除外）的本地地址。
  - 在入站或出站数据包的包规则中，按数据包生存时间（TTL）。
  - 在包规则中，为入站和出站数据包或连接按网络接口。
- 如果您为允许包规则配置了网络适配器或包生存时间(TTL)，则该规则的优先级低于阻止应用程序规则。换言之，如果应用程序的网络活动被阻止（例如，应用程序在“*高限制*”信任组），您无法使用带有这些设置的包规则允许应用程序的网络活动。在其他所有情况下，包规则的优先级高于应用程序网络规则。
- 当导入防火墙包规则时，Kaspersky Endpoint Security 可能修改规则名称。应用程序使用相同的通用参数集确定规则：协议、方向、远程和本地端口、数据包生存时间 (TTL)。如果该通用参数集在多个规则中匹配，则应用程序分配相同的名称到这些规则或添加参数标签到名称。这样，Kaspersky Endpoint Security 导入所有包规则，但是具有相同通用参数的规则的名称可能被更改。

- 如果您在网络规则中启用了应用程序事件报告，则在将应用程序移动到其他信任组时，将不会应用此信任组的限制。因此，如果应用程序位于“受信任组”中，它将没有网络限制。然后，您为此应用程序启用了事件报告，并将其移动到“*不信任*”。防火墙不会对此应用程序实施网络限制。我们建议您首先将应用程序移动到适当的信任组，然后启用事件报告。如果此方法不适用，可以在网络规则设置中手动配置应用程序的限制。该限制仅适用于应用程序的本地接口。在策略中的信任组之间移动应用程序可以正常工作。

- 防火墙和入侵防御组件具有通用设置：应用程序权限和受保护的资源。如果您更改防火墙的这些设置，Kaspersky Endpoint Security 将自动将新设置应用于入侵防御。例如，如果您允许更改防火墙策略的常规设置（挂锁打开），入侵防御设置也将变为可编辑。

- 当网络数据包规则在 Kaspersky Endpoint Security 11.6.0 或更早版本中被触发时，防火墙报告中的“**应用程序名称**”列将总是显示“*Kaspersky Endpoint Security*”值。此外，防火墙将阻止所有应用程序在数据包级别的连接。此行为已针对 Kaspersky Endpoint Security 11.7.0 或更高版本进行了修改。“**规则类型**”列已添加到防火墙报告中。触发网络数据包规则时，“**应用程序名称**”列中的值保持为空。

- 如果您使用防火墙禁止所有网络活动，网络威胁防护组件可能会检测到端口扫描类型的攻击。发生这种情况的原因是应用程序在防火墙之前启动网络威胁防护来检测网络中的可疑活动。

BadUSB 攻击防护

- Kaspersky Endpoint Security 在计算机锁定时重置 USB 设备锁的超时（例如，屏幕锁超时已过）。也就是说，如果您多次输入错误的 USB 设备授权代码，并且应用程序锁定 USB 设备，Kaspersky Endpoint Security 允许您在解锁计算机后重复授权尝试。在这种情况下，Kaspersky Endpoint Security 不会在 BadUSB 攻击防护组件设置中指定的时间内锁定 USB 设备。

- Kaspersky Endpoint Security 在计算机保护暂停时重置 USB 设备锁定超时。也就是说，如果您多次输入错误的 USB 设备授权代码，并且应用程序锁定 USB 设备，Kaspersky Endpoint Security 允许您在恢复计算机保护后重复授权尝试。在这种情况下，Kaspersky Endpoint Security 不会在 BadUSB 攻击防护组件设置中指定的时间内锁定 USB 设备。

卡巴斯基安全网络

- 如果服务器地址包含非拉丁字母（非 ASCII 符号），当连接到 KSN 代理时，Kaspersky Endpoint Security 不支持 HTTPS（KSN 代理连接设置中选择了“**使用 HTTPS**”复选框）。

- 在 Kaspersky Security Center 中，当从使用全球卡巴斯基安全网络切换到使用私有卡巴斯基安全网络(KPSN)时，或反之，特定产品策略中参与卡巴斯基安全网络的选项被禁用。切换后，请仔细阅读卡巴斯基安全网络声明的文本，并确认您同意参与 KSN。您可以在应用程序界面或编辑产品策略时阅读声明的文本。

- 从 Kaspersky Endpoint Security 12.9 for Windows 开始，从 KPSN 切换到全球 KSN 时，您需要重新确认您同意卡巴斯基安全网络声明。为此，您需要在策略属性或应用程序界面中启用卡巴斯基安全网络的使用，并确认您同意卡巴斯基安全网络声明。如果您已经使用全球 KSN，您必须先禁用 KSN 使用，然后重新启用它并确认您同意卡巴斯基安全网络声明。如果您不同意卡巴斯基安全网络声明，应用程序将无法访问卡巴斯基安全网络的数据。

- Kaspersky Endpoint Security 不会将文本文件（例如不包含宏的 TXT、CSV、LOG 和 DOCX 文件）发送到卡巴斯基安全网络进行扫描。应用程序发送可能构成威胁的文件到 KSN 进行扫描。这些文件包括可执行文件或可能包含可执行代码的文件（例如 DOCX 文件中的宏）。应用程序的其他组件负责扫描文本文件。您也可以从文件上下文菜单手动检查文本文件的信誉。如果一个文本文件具有“*不受信任(卡巴斯基安全网络)*”信誉，应用程序将忽略为检测到的威胁定义的操作。

应用程序控制

- 使用应用程序控制规则时，推荐不要为不同类别的应用程序添加超过 100,000 个包含和排除条件，前提是 Kaspersky Endpoint Security 运行在满足最低硬件要求并在 Microsoft Windows 10 上运行的计算机上。

- 在 Kaspersky Security Center Web Console 中使用应用程序控制规则时，仅支持 ZIP 格式的存档。不支持其他格式的存档，例如 RAR 或 7z。如果您在管理控制台 (MMC) 中使用应用程序控制规则，则没有此类限制。

- 在 Kaspersky Security Center Web Console 中使用应用程序控制规则时，支持的上传文件的最大大小为 104 MB。如果您在管理控制台 (MMC) 中使用应用程序控制规则，则没有此类限制。

- 在 Microsoft Windows 10 中以应用程序拒绝列表模式工作时，可能会错误地应用块规则，这可能会导致阻止在规则中未指定的应用程序。

- 如果您在升级 Kaspersky Endpoint Security 时添加了新的*预定义应用程序控制规则*，您无法将这些规则应用于应用程序的先前版本。

- 当渐进式 Web 应用（PWA）被应用程序控制组件阻止时，appManifest.xml 在报告中显示为阻止的应用。

- 将标准记事本应用程序添加到 Windows 11 的应用程序控制规则时，建议不要指定应用程序的路径。在运行 Windows 11 的计算机上，操作系统使用位于文件夹 `C:\Program Files\WindowsApps\Microsoft.WindowsNotepad*\Notepad\Notepad.exe` 中的 Metro Notepad。在以前版本的操作系统中，记事本位于以下文件夹中：

  - `C:\Windows\notepad.exe`

  - `C:\Windows\System32\notepad.exe`

  - `C:\Windows\SysWOW64\notepad.exe`

  将记事本添加到应用程序控制规则时，可以从正在运行的应用程序的属性中指定应用程序名称和文件哈希。

- 将 KSWS 策略迁移到 KES 策略配置文件时，如果类别名称包含禁用以下字符，策略和任务批量转换向导（迁移向导）会重命名应用程序类别：`'` `*` `<` `>` `?` `\` `:` `|`。迁移向导将这些字符替换为 `_` 字符。例如，`KSWS::\Everyone:[C61F-3B7C-4D89-96A1]` 应用程序类别将被重命名为 `KSWS_Everyone_[C61F-3B7C-4D89-96A1]`。

设备控制

- Kaspersky Endpoint Security 可以记录外部设备的连接和断开连接事件。Windows 服务使用系统用户账户来连接或断开设备。这使得无法知道哪个用户正在连接或断开设备。Kaspersky Endpoint Security 在事件中指定 SYSTEM 用户账户。

- 设备和总线阻止规则阻止对添加到受信任列表的打印机设备的访问。

- 对于 MTP 设备，如果使用操作系统的内置 Microsoft 驱动程序，则支持对读、写和连接操作的控制。如果用户安装了用于操作设备的自定义驱动程序（例如，作为 iTunes 或 Android 调试桥的一部分），则对读写操作的控制可能无法工作。

- 使用 MTP 设备时，重新连接设备后访问规则会更改。

- 设备控制组件注册与被监视设备相关的事件，例如设备的连接和断开、从设备读取文件、将文件写入设备以及其他事件。Kaspersky Endpoint Security 仅注册以下设备类型的断开连接事件： 便携式设备(MTP)、可移动驱动器、软盘、CD/DVD 驱动器。对于其他设备类型，应用程序不会注册断开连接事件。该应用程序为所有设备类型注册将设备连接到计算机的操作。

- 如果要基于型号掩码将设备添加到受信任列表中，并且使用的字符包含在 ID 中，但不包含在型号名称中，则不会添加这些设备。在工作站上，这些设备将基于 ID 掩码添加到受信任列表中。

- 当应用程序升级而不重新启动计算机时，设备控制不会将访问规则应用于重新连接的设备。但是，如果设备在升级之前已连接，则设备控制会正确应用规则。重新启动计算机，应用程序才能在重新连接的设备上正常工作。

- 在安装了 Kaspersky Endpoint Security 12.0 版的计算机上，如果在计算机上应用了 Kaspersky Endpoint Security 12.1 版策略，**网络打印机**设备类型的**允许且不记录**打印机访问模式被称为**取决于连接总线**。在这些模式下，应用程序执行相同的操作。在 Kaspersky Endpoint Security 12.1 版中，网络打印机的访问模式被正确命名为**允许且不记录**。

- 从 Kaspersky Endpoint Security 12.0 for Windows 开始，该应用程序允许为打印机配置打印规则（打印控制）。安装带打印控制的应用程序或将应用程序升级到带打印控制的版本后，必须重新启动计算机。在计算机重新启动之前，Kaspersky Endpoint Security 不会应用打印规则并且只能控制对打印机的访问。如果重新启动计算机对您组织中的工作流程产生不利影响，您可以只重新启动 spoolsv 服务（后台打印程序）。基于 Arm 架构的计算机不支持打印控制。

- 从 Kaspersky Endpoint Security 12.0 for Windows 开始，应用程序对"**Wi-Fi**"类型的设备支持 WPA3 协议。如果在计算机上应用 Kaspersky Endpoint Security 12.2 版策略，则在 Kaspersky Endpoint Security 11.11.0 及更早版本的计算机上选择 WPA2 协议；12.0 到 12.1 版本选择 WPA2 / WPA3；12.2 及更高版本选择 WPA3。

- Apple 设备分为便携式设备（MTP）和 iTunes 设备。操作系统可能会错误地识别 Apple 设备的连接，并且无法将 Apple 设备确定为便携式设备（MTP）。因此，Apple 设备将在文件管理器中不可用，但在 iTunes 应用程序中可以访问。因此，Kaspersky Endpoint Security 将仅在 iTunes 应用程序中控制对 Apple 设备的访问。要将您的 Apple 设备作为便携式设备（MTP）访问，您需要转到设备管理器，并从 USB 控制器列表中删除 Apple Mobile device USB Driver。计算机重新启动后，操作系统会将 Apple 设备识别为便携式设备（MTP）和 iTunes 设备。Kaspersky Endpoint Security 将在 iTunes 应用程序和文件管理器中控制对设备的访问。

- 在 Kaspersky Endpoint Security 12.3 for Windows 中，"**蓝牙**"设备类型的访问设置不同。如果您在先前版本的应用程序中指定了"**取决于连接总线**"值，则将应用程序升级到版本 12.3 后，配置的值更改为"**允许且不记录**"。这不会改变设备的行为。

- 设备控制仅通过 Microsoft Windows 蓝牙堆栈支持蓝牙设备。设备控制可能无法与第三方蓝牙堆栈一起正常运行。

- 如果蓝牙设备隐藏或欺骗其设备类别（COD），则设备控制可能无法正常工作。

- 在装有某些 Realtek 蓝牙适配器驱动程序的 Windows 7 或 Windows 8 计算机上，可能无法仅允许连接蓝牙设备作为输入设备（HID 类）。也就是说，如果您在应用程序设置中禁止访问蓝牙设备并将输入设备添加到排除项，则设备控制可能会阻止访问所有蓝牙设备。

Web 控制

- OGV 和 WEBM 格式不被支持。

- RTMP 协议不被支持。

- Web 控制仅支持 WSL1。用程序不控制 WSL2 流量。

自适应异常控制

- 建议根据事件自动创建排除项。当手动添加排除项时，在指定目标对象时，将 * 字符添加到路径的开头。

- 如果样本中甚至包含一个名称包含超过 260 个字符的事件，则无法生成自适应异常控制规则报告。

- 如果对象或进程的属性具有大于 256 位字符的值（例如，目标对象路径）就，则从自适应异常控制触发规则存储库添加排除项不被支持。您可以在策略设置中手动添加排除项。您也可以在自适应异常控制规则触发报告中添加排除项。

- Kaspersky Security Center 15.1 无法生成针对特定规则的详细"**有关自适应异常控制规则状态的报告**"报告。

驱动器加密（FDE）

- 卡巴斯基磁盘加密不支持基于 Arm 的计算机。
- 运行 Windows Home 的计算机不支持 BitLocker 驱动器加密。
- 安装应用程序后，必须重新启动操作系统才能使硬盘加密正常工作。
- 身份验证代理不支持象形文字或特殊字符 | 和 \。
- 为了在加密后获得更好的计算机性能，处理器必须支持 AES-NI 指令集(Intel Advanced Encryption Standard New Instructions)。如果处理器不支持 AES-NI，则计算机性能可能降低。
- 如果有进程在应用程序授予对加密设备的访问权限之前尝试访问这些设备，则应用程序将显示一条警告，指出必须终止这些进程。如果进程无法终止，请重新连接加密设备。
- 硬盘驱动器的唯一 ID 以反转格式显示在设备加密统计信息中。
- 不建议在加密设备时格式化它们。
- 当多个可移动驱动器同时连接到一台计算机时，加密策略只能应用于一个可移动驱动器。重新连接可移动设备时，将正确应用加密策略。
- 加密可能无法在碎片严重的硬盘驱动器上启动。整理硬盘碎片。
- 加密硬盘时，从加密任务开始到第一次重新启动运行 Microsoft Windows 7/8/8.1/10 的计算机，以及安装硬盘驱动器加密之后，直到 Microsoft Windows 8/8.1/10 操作系统首次重新启动，休眠都将被阻止。当硬盘驱动器被解密时，从引导驱动器完全解密到操作系统第一次重新启动时，休眠将被阻止。当在 Microsoft Windows 8/8.1/10 中启用快速启动选项时，阻止休眠将阻止您关闭操作系统。
- 当磁盘使用 BitLocker 技术加密时，Windows 7 计算机不允许在恢复过程中更改密码。在输入了恢复密钥且操作系统加载后，Kaspersky Endpoint Security 不提示用户更改密码或 PIN 码。因此，无法设置新密码或 PIN 码。该问题源于操作系统特色。要继续，您需要重新加密硬盘驱动器。
- 不建议使用启用了附加提供程序的 xbootmgr.exe 工具。例如，调度程序、网络或驱动程序。
- 安装了 Kaspersky Endpoint Security for Windows 的计算机不支持格式化加密的可移动驱动器。
- 不支持使用 FAT32 文件系统格式化加密的可移动驱动器（驱动器显示为加密）。要格式化驱动器，请将其格式化到 NTFS 文件系统。
- 多个下载代理不能在一台加密的计算机上共存。
- 尝试在未加密状态下恢复可启动 GPT 磁盘的镜像，操作系统可能会使系统无法运行。为避免这种情况，请遵循以下建议：
  - 从备份恢复镜像之前，请先完全解密磁盘。
  - 创建镜像时使用逐扇区复制的方式。
  - 在恢复镜像并重新初始化磁盘之前，从加密磁盘的第一个扇区中删除数据。

- 当同时满足以下所有条件时，无法访问先前在另一台计算机上加密的可移动驱动器：
  - 没有到 Kaspersky Security Center 服务器的连接。
  - 用户正在尝试使用新令牌或密码进行授权。

  如果出现类似情况，请重新启动计算机。重新启动计算机后，将授予对加密可移动驱动器的访问权限。
- 在 BIOS 设置中启用 USB 的 xHCI 模式时，可能不支持身份验证代理发现 USB 设备。
- SSHD 设备不支持用于缓存最常用数据的设备 SSD 部分的卡巴斯基磁盘加密（FDE）。
- 不支持在 UEFI 模式下运行的 32 位 Microsoft Windows 8/8.1/10 操作系统中加密硬盘驱动器。
- 重新加密已解密的硬盘驱动器之前，请重新启动计算机。
- 硬盘加密与用于 UEFI 的卡巴斯基反病毒软件不兼容。不建议在安装了用于 UEFI 的卡巴斯基反病毒软件的计算机上使用硬盘加密。
- 支持基于 Microsoft 账户创建身份验证代理帐户，但有以下限制：
  - 不支持单一登录技术。
  - 如果选择了为最近 N 天内登录系统的用户创建帐户的选项，则不支持自动创建身份验证代理帐户。
- 如果身份验证代理帐户的名称的格式为 `<domain>/<Windows account name>`，则在更改计算机名称后，还需要更改为此计算机的本地用户创建的帐户的名称。例如，假设在 `Ivanov` 计算机上有一个本地用户 `Ivanov`，并且已经为该用户创建了一个名为 `Ivanov/Ivanov` 的身份验证代理帐户。如果计算机名 `Ivanov` 已更改为 `Ivanov-PC`，则需要将用户 `Ivanov` 的身份验证代理帐户的名称从 `Ivanov/Ivanov` 更改为 `Ivanov-PC/Ivanov`。您可以使用身份验证代理的本地账户管理任务更改账户名。在更改账户名之前，可以使用旧名称（例如，`Ivanov/Ivanov`）在预引导环境中进行身份验证。
- 如果只允许用户使用令牌访问使用卡巴斯基磁盘加密技术加密的计算机，并且该用户需要完成访问恢复过程，请确保在恢复对加密计算机的访问后，授予该用户基于密码的访问权限。可能无法保存用户在恢复访问时设置的密码。在这种情况下，用户必须在下次重新启动计算机时完成恢复对加密计算机的访问的过程。
- 使用 FDE 恢复工具解密硬盘驱动器时，如果源设备上的数据被解密数据覆盖，则解密过程可能会以错误结束。硬盘上的部分数据将保持加密。使用 FDE 恢复工具时，建议在设备解密设置中选择将解密数据保存到文件的选项。
- 如果身份验证代理密码已更改，则包含*您的密码已成功更改文本的消息被显示。单击“确定”*出现，用户重新启动计算机，新密码不会保存。旧密码必须用于预引导环境中的后续身份验证。
- 磁盘加密与英特尔快速启动技术不兼容。
- 磁盘加密与 ExpressCache 技术不兼容。
- 在某些情况下，当尝试使用 FDE 恢复工具解密加密驱动器时，该工具会在“请求-响应”过程完成后错误地将设备状态检测为“未加密”。工具的日志显示一个事件，提示设备已成功解密。在这种情况下，必须重新启动数据恢复过程才能解密设备。
- 在 Web Console 中更新 Kaspersky Endpoint Security for Windows 插件后，客户端计算机属性在 Web Console 服务重新启动之前不会显示 BitLocker 恢复密钥。
- 要查看完整磁盘加密支持的其他限制以及受限制支持硬盘加密的设备列表，请参阅技术支持知识库。

文件级加密 (FLE)

- 基于 Arm 架构的计算机不支持文件加密。
- Microsoft Windows Embedded 操作系统不支持文件和文件夹加密。
- 您安装应用程序后，必须重新启动操作系统才能使文件和文件夹加密正常工作。
- 该应用程序仅在具有 NTFS 和 FAT32 文件系统的设备上支持文件加密。如果加密文件被传输到具有不受支持的文件系统（例如，exFAT）的设备，则该设备上的文件将不会被加密，并且可以进行修改。
- 如果加密文件存储在具有可用加密功能的计算机上，并且您从加密不可用的计算机访问该文件，则将提供对该文件的直接访问。存储在具有可用加密功能的计算机上的网络文件夹中的加密文件将以解密形式复制到没有可用加密功能的计算机上。
- 建议您在使用 Kaspersky Endpoint Security for Windows 加密文件之前，先对使用Encrypting File System加密的文件进行解密。
- 文件加密后，其大小将增加 4 KB。
- 文件加密后，将在"文件属性"中设置"*存档*"属性。
- 例如，将解密的文件复制到可移动媒体时，该文件可能保持加密状态。发生这种情况的原因是，当文件管理器（例如，explorer.exe）尝试访问加密文件时，它会将文件的哈希值保存到进程的特殊列表中。解密文件后，当文件管理器尝试访问该文件时，该进程会在列表中搜索该文件的哈希值。如果找到哈希值， Kaspersky Endpoint Security 将保持文件加密。为了避免这种情况，您需要清除进程列表。当进程列表填满时，操作系统会自动清除该列表。您页可以手动清除列表。为此，您可以重新启动计算机，重新启动用于访问文件的进程（例如，explorer.exe），或者使用未使用过的其他文件管理器来访问加密文件。
- 如果从加密存档中解包的文件与计算机上已有的文件同名，则后者将被从加密存档中解包的新文件覆盖。覆盖操作不会通知用户。
- 在您之前解压缩加密档案，确保您有足够的可用磁盘空间来容纳解压缩的文件。如果您没有足够的磁盘空间，存档解包可能已完成，但文件可能已损坏。在这种情况下，Kaspersky Endpoint Security 可能不显示任何错误消息。
- 便携式文件管理器界面不显示有关在其操作期间发生的错误的消息。
- 对于安装了文件级加密组件的计算机，Kaspersky Endpoint Security for Windows 不会启动便携式文件管理器。
- 如果以下条件同时被满足，您无法使用便携式文件管理器访问可移动驱动器：
  - 没有到 Kaspersky Security Center 的连接；
  - 计算机上安装了 Kaspersky Endpoint Security for Windows；
  - 数据加密 (FDE 或 FLE) 在计算机上没有运行。

  即便您知道便携式文件管理器的密码，访问也不可行。
- 使用文件加密时，应用程序与 Sylpheed 邮件客户端不兼容。

- Kaspersky Endpoint Security for Windows 不支持对某些应用程序的加密文件的访问限制规则。这是因为一些文件操作是由第三方应用程序执行的。例如，文件复制由文件管理器执行，而不是由应用程序本身执行。这样，如果 Outlook 邮件客户端拒绝访问加密文件，如果用户已通过剪贴板或使用拖放功能将文件复制到电子邮件，则 Kaspersky Endpoint Security 将允许邮件客户端访问加密文件。复制操作是由文件管理器执行的，未指定对加密文件的访问限制规则，即允许访问。

- 使用便携模式支持对可移动驱动器进行加密时，无法禁用密码期限控制。

- 不支持更改页面文件设置。操作系统使用默认值而不是指定的参数值。

- 使用加密的可移动驱动器时使用安全删除。如果无法安全移除可移动驱动器，我们无法保证数据的完整性。

- 文件加密后，未加密的原始文件将被安全删除。

- 不支持使用Client-Side Caching（CSC）同步脱机文件。加密脱机文件或通过 SMB 的 Branch Caching 技术也不受支持。建议在组策略级别禁止脱机管理共享资源。可以编辑处于脱机模式的文件。同步后，对脱机文件所做的更改可能会丢失。

- 不支持在系统硬盘驱动器的根目录中创建加密的存档文件。

- 通过网络访问加密文件时可能会遇到问题。建议您将文件移到其他源，或确保用作文件服务器的计算机由同一 Kaspersky Security Center 管理服务器管理。

- 更改键盘布局可能会导致加密的自解压存档的密码输入窗口挂起。要解决此问题，请关闭“密码输入”窗口，切换到操作系统中的键盘布局，然后重新输入加密存档的密码。

- 当在一个磁盘上有多个分区的系统上使用文件加密时，建议您使用自动确定 pagefile.sys 文件大小的选项。计算机重新启动后，pagefile.sys 文件可能在磁盘分区之间移动。

- 应用文件加密规则（包括“*我的文档*”文件夹中的文件）后，请确保已应用加密的用户可以成功访问加密的文件。为此，当 Kaspersky Security Center 连接可用时，让每个用户登录到系统。如果用户试图在没有连接 Kaspersky Security Center 的情况下访问加密文件，系统可能会挂起。

- 如果系统文件以某种方式包含在文件级加密的范围内，则有关加密这些文件时出错的事件可能会出现在报告中。在这些事件中指定的文件实际上没有加密。

- 不支持 Pico 进程。

- 不支持区分大小写的路径。应用加密规则或解密规则时，产品事件中的路径以小写形式显示。

- 不建议对系统启动时使用的文件进行加密。如果这些文件是加密的，在没有连接到 Kaspersky Security Center 的情况下尝试访问加密文件可能会导致系统挂起或导致提示访问未加密文件。

- 如果用户通过使用文件到内存映射方法的应用程序（如 WordPad 或 FAR）和为处理大文件而设计的应用程序（如 Notepad++），根据 FLE 规则在网络上共同处理文件，未加密形式的文件可能会被无限期地阻止，而无法从其所在的计算机访问它。

- Kaspersky Endpoint Security 不会加密位于 OneDrive 云存储中的文件或以 OneDrive 作为名称的其他文件夹中的文件。如果加密文件未添加到解密规则中，Kaspersky Endpoint Security 还会阻止将加密文件复制到 OneDrive 文件夹。

- 安装文件级加密组件后，用户和组的管理在 WSL 模式（Windows Subsystem for Linux）下不起作用。

- 安装文件级加密组件后，不支持用于重命名和删除文件的 POSIX（Portable Operating System Interface）。

- 不建议加密临时文件，因为这可能导致数据丢失。例如，Microsoft Word 在处理文档时创建临时文件。如果临时文件已加密，但原始文件未加密，则用户在尝试保存文档时可能会收到*访问被拒绝*错误。此外，Microsoft Word 可能会保存文件，但下次无法打开文档，即数据将丢失。为了防止数据丢失，您需要从加密规则中排除临时文件文件夹。

Detection and Response (EDR、NDR、MDR、XDR、Sandbox)

- 您无法扫描被"*移动文件到隔离区*"任务隔离的对象。

- 无法隔离大于 4 MB 的Alternate Data Stream（ADS）。Kaspersky Endpoint Security 跳过任何如此大的 ADS，而不通知用户。

- 如果任务属性中的文件夹路径以驱动器号开头，则 Kaspersky Endpoint Security 不会在网络驱动器上运行"*IOC 扫描*"任务。Kaspersky Endpoint Security 仅支持网络驱动器上"*IOC 扫描*"任务的 UNC 路径格式。例如，`\\server\shared_folder`。

- 为了确保使用 EmailItem 术语的"*IOC 扫描*"任务能够正常工作，Kaspersky Endpoint Security Web 插件必须更新到最新版本。

- 在基于 Arm 的计算机上，"*IOC 扫描*"任务仅支持来自以下邮件客户端的电子邮件文件：适用于 Arm64 的 Outlook 2016 和 Outlook 2021、2024 和 365 的 32 位和 64 位版本。

- 如果在配置文件中启用了与 Kaspersky Sandbox 集成设置，则导入应用程序配置文件将以错误结束。在导出应用程序设置之前，请禁用 Kaspersky Sandbox。然后执行导出/导入过程。导入配置文件后，启用 Kaspersky Sandbox。

- 从 KLP 文件导入策略时，用于确定是否接受《Kaspersky Detection and Response Expert 协议》条款和条件的参数值不会应用。因此，导入策略后，Kaspersky Endpoint Security 不会执行 EDR Agent 的功能。要使 EDR Agent 正常工作，请打开策略，更改任意参数，然后保存策略设置。

- 当在运行"*IOC 扫描*"任务时检测到妥协的指标时，应用程序仅针对 FileItem 术语隔离文件。不支持为其他术语隔离文件。

- 管理警报详细信息需要 Kaspersky Endpoint Security for Windows Web 插件 11.7.0 或更高版本。使用 Endpoint Detection and Response 解决方案（EDR Optimal 和 EDR Expert）时，需要警报详细信息。警报详细信息仅在 Kaspersky Security Center Web Console 和 Kaspersky Security Center 云控制台中可用。

- 将 [KES+KEA] 配置迁移到 [KES+内置代理] 配置可能会导致 Kaspersky Endpoint Agent 应用程序卸载错误。最新版本的 Kaspersky Endpoint Agent 修复了应用程序卸载错误。要卸载 Kaspersky Endpoint Agent，请重新启动计算机并创建应用程序卸载任务。

- 不支持[KES+KEA+内置代理]配置。此类配置会破坏应用程序与组织中部署的 Detection and Response 解决方案之间的交互。此外，在同一台计算机上使用 Kaspersky Endpoint Agent 和内置代理会导致重复遥测并增加计算机和网络的负载。迁移到[KES+内置代理]配置后，请确保 Kaspersky Endpoint Agent 已从计算机中删除。如果 Kaspersky Endpoint Agent 在迁移后继续工作，请手动卸载应用程序（例如，使用*远程卸载应用程序*任务）。

  安装程序允许您在安装了 Kaspersky Endpoint Security 和内置代理的计算机上部署 Kaspersky Endpoint Agent。Kaspersky Endpoint Agent 和内置代理也可以安装在一台计算机上，作为*更改应用程序组件*任务的结果。该行为取决于 Kaspersky Endpoint Security 和 Kaspersky Endpoint Agent 的版本。

- 在生成警报详细信息时，应用程序会提供有关检测到的威胁的信息，包括修改文件的哈希值。Kaspersky Endpoint Security 在生成警报详细信息时计算文件的哈希值。考虑到生成文件修改事件时文件的原始哈希值可能与生成警报详细信息时计算的哈希值不同。

- 内置代理 EDR（KATA）在计算机重新启动后恢复计算机的网络隔离，即使隔离期已过。为防止重复计算机隔离，您需要在 Kaspersky Anti Targeted Attack Platform 控制台中关闭网络隔离。

- 我们建议在网络隔离完成后升级应用程序。升级 Kaspersky Endpoint Security 后，可以停止网络隔离。

- EDR (KATA)、EDR Optimum 和 EDR Expert 的内置代理彼此不兼容。因此，如果您激活了具有不同 EDR 功能的 Kaspersky Endpoint Security，则可以跳过使用独立的 Kaspersky Endpoint Detection and Response 加载项授权许可激活 EDR 内置代理。例如，如果您已使用 [KES EDR Optimum] 授权许可激活 Kaspersky Endpoint Security，则将跳过使用独立授权许可激活 EDR (KATA) 内置代理。

- 在 Kaspersky Endpoint Security 12.1 版中，内置 EDR（KATA）代理不支持*获取 NTFS 元文件*任务的以下元文件：$Secure:$SDH:$INDEX_ROOT；$Secure:$SDH:$INDEX_ALLOCATION；$Secure:$SDH:$BITMAP；$Secure:$SII:$INDEX_ROOT；$Secure:$SII:$INDEX_ALLOCATION；$Secure:$SII:$BITMAP；$Extend\$UsnJrnl:$J:$DATA；$Extend\$UsnJrnl:$Max:$DATA。Kaspersky Endpoint Security 版本 12.2 增加了对这些元文件的支持。

- 对于 Kaspersky Anti Targeted Attack Platform (EDR) 解决方案，当从 Kaspersky Endpoint Agent 迁移到 Kaspersky Endpoint Security 时，您将计算机连接到 Central Node 服务器时可能会遇到错误。原因是 Web Console 中的迁移向导跳过了以下策略设置并且不迁移它们：

  - 设置修改禁止 **连接设置** （“锁”）。

    默认情况下，可以修改设置（“锁”是打开的）。因此，这些设置不会应用到计算机上。您必须禁止设置修改并关闭“锁”。

  - 加密容器。

    如果您使用双向身份验证连接到 Central Node 服务器，则必须重新添加加密容器。迁移向导正确迁移了服务器的 TLS 证书。

  管理控制台（MMC）中的策略和任务迁移向导会迁移 Kaspersky Anti Targeted Attack Platform (EDR) 解决方案的所有设置。

- 当在 Endpoint Detection and Response Agent 模式下安装应用程序以支持 Kaspersky Managed Detection and Response 解决方案时（不连接 Kaspersky Security Center），应用程序激活状态显示不正确。BLOB 文件下载后，Windows 任务栏通知区域显示错误状态：*应用程序未激活*。然而，应用程序界面会正确显示激活状态。重新启动计算机以使应用程序正常工作。

- Kaspersky Endpoint Security 允许使用 EDR (KATA) 组件或 Endpoint Sensor（不受支持）与 Kaspersky Anti Targeted Attack Platform 解决方案集成。请注意，您只能使用其中一个组件与 Kaspersky Anti Targeted Attack Platform 进行交互。要查看组件的状态，请在管理控制台 (MMC) 中打开计算机属性，在“**应用程序**”部分，打开 Kaspersky Endpoint Security for Windows 的属性，然后转到“**组件**”部分。在显示与 Kaspersky Anti Targeted Attack Platform 交互的组件状态时，需特别注意以下事项：

  - 对于管理插件 12.0 及更早版本，应用程序显示 **端点传感器** 的当前状态。在 Kaspersky Endpoint Security 12.0 及更早版本中，EDR (KATA) 组件不可用。EDR (KATA) 组件是在 12.1 版本中引入的。

  - 对于管理插件 12.1 及更高版本，应用程序显示 **Endpoint Detection and Response (KATA)** 的总体状态，可以表示 Endpoint Sensor 状态，也可以表示 EDR (KATA) 组件状态。这取决于用户计算机上安装的应用程序版本以及可用于与 Kaspersky Anti Targeted Attack Platform 交互的可用组件。

- 从 Kaspersky Endpoint Security 12.6 及更高版本开始，Kaspersky Security Center Web Console 14.2 及更低版本无法在计算机属性中正确显示 **Endpoint Detection and Response (KATA)** 组件的名称。应用程序显示的名称不是 **Endpoint Detection and Response (KATA)** 组件，而是 **Endpoint Detection and Response Expert (KATA EDR)** 组件。要查看组件列表，请在 Web Console 中打开计算机属性，在“**应用程序**”部分，打开 Kaspersky Endpoint Security for Windows 的属性，然后转到“**组件**”部分。从 Kaspersky Security Center Web Console 15.1 及更高版本开始，应用程序可以正确显示组件名称。

- 将 Web Console 版本 14.0–14.2 中安装的 Kaspersky Endpoint Detection and Response 管理插件更新至版本 15.3 时，警报详细信息显示不正确。为了使警报详细信息正常工作，请重新启动 Kaspersky Security Center 管理服务器。

- Kaspersky Endpoint Detection and Response 管理插件版本 15.4 及更高版本不支持 Kaspersky Security Center 版本 14.0。更新管理插件后，警报详细信息显示不正确。

- Kaspersky Extended Detection and Response (XDR) 1.4 版解决方案不支持 Kaspersky Endpoint Security for Windows Web 插件 12.12 版或更高版本。您可以保留当前的 Web 插件版本，或者将 XDR 解决方案更新到 2.0 版本或更高版本。

- Kaspersky Endpoint Security 不会将面向 Arm 架构的对象发送到 Kaspersky Sandbox。

- 在基于 Arm 的计算机上不支持与 Kaspersky Endpoint Detection and Response Expert 集成。

- Kaspersky Endpoint Security 总共支持多达 10,000 个 EDR Expert (on-premises) 包含和排除事件过滤规则。

- 如果存储的过滤规则数量超过了支持的限制，则 EDR Expert (on-premises) 事件过滤规则将不会从策略传递到运行 Kaspersky Endpoint Security 14.0 或更早版本的受管设备。应用程序将显示相应的警告。

其他限制

- Windows 操作系统从版本 11 24H2 开始支持 UDP Receive Segment Coalescing Offload （URO）技术。如果计算机上安装了兼容的网卡和驱动程序，则默认启用该技术。在用户的计算机上禁用 URO 会显著降低应用程序的性能。

- Kaspersky Endpoint Security 支持 WSL 子系统 (Windows Subsystem for Linux)，但有限制：

  - WSL 1 应用程序监控网络流量并通过 HTTP/HTTPS 检测威胁。由于 Kaspersky Endpoint Security 使用自己的证书扫描安全的 HTTPS 连接，某些第三方应用程序的运行可能会中断。

  - WSL 2 应用程序不支持 WSL 2。

- 如果该应用程序返回错误，或者在运行期间挂起，它可能会自动重新启动。如果程序遇到反复导致程序崩溃的错误，它将执行以下操作：

  1. 禁用控制和保护功能（加密功能仍启用）。

  2. 通知用户某些功能已被禁用。

  3. 更新反病毒数据库或应用程序模块更新之后尝试恢复程序的功能。

- 添加到受信任列表的网址可能处理不正确。

- 在 Kaspersky Security Center 控制台中，您无法将文件从以下位置保存到磁盘：“**高级**” → “**存储库**” → “**活动威胁**”文件夹。要保存文件，您必须清除受感染的文件。清除时，应用程序会在备份中保存文件的副本。现在您可以将文件从以下位置保存到磁盘：“**高级**” → “**存储库**” → “**备份**”文件夹。

- 数据传输到管理服务器的设置的继承（**常规设置** → **报告和存储** → **到管理服务器的数据传输**) 与其他设置的继承不同。如果您允许更改策略中的数据传输设置（“锁”打开），则这些设置将在控制台的本地计算机属性中重置为默认值（如果之前未定义）。如果之前定义了这些设置，则它们的值将被恢复。删除策略时，将以相同的方式继承设置。在这些情况下，本地计算机属性中的其他设置将从策略继承。

- Kaspersky Endpoint Security 监控与 RFC 2616、RFC 7540、RFC 7541、RFC 7301 标准兼容的 HTTP 流量。如果 Kaspersky Endpoint Security 在 HTTP 流量中检测到其他数据交换格式， 则应用程序阻止该连接以防止从互联网下载恶意文件。

- Kaspersky Endpoint Security 防止通过 QUIC 协议进行通信。浏览器使用标准传输协议（TLS 或 SSL），无论浏览器中是否启用 QUIC 支持。

- 当第三方软件使用 Libcurl 库时，可能会出现 TLS 连接错误。这可能与 Kaspersky Endpoint Security 用于扫描加密连接的卡巴斯基证书有关。要继续工作，您可以禁用第三方软件的证书验证（不推荐）或将卡巴斯基证书主体添加到 cURL 证书存储。有关详细信息，请参阅卡巴斯基知识库。

- 第一次启动 Kaspersky Endpoint Security for Windows 时，数字签名的应用程序可能会临时放入错误的组中。数字签名的应用程序稍后将被放入正确的组中。

- 在重新扫描被第三方软件阻止的恶意对象期间，当再次检测到威胁时，不会通知用户。威胁重新检测事件显示在应用程序报告和 Kaspersky Security Center 报告中。

- Kaspersky Security Center 设备加密报告将不包括在服务器平台或未安装设备控制组件的工作站上使用 Microsoft BitLocker 加密的设备的信息。

- 无法在 Kaspersky Security Center Web Console 中启用对所有报告条目的显示。在 Web Console 中，您只能更改报告中显示的条目数。默认下，Kaspersky Security Center Web Console 显示 1000 个报告条目。您可以在管理控制台(MMC)中启用所有报告条目的显示。

- 无法在 Kaspersky Security Center 控制台中设置 1000 多个报告条目的显示。如果您设置的值高于 1000，Kaspersky Security Center 控制台将仅显示 1000 个报告条目。

- 使用策略层级时，如果父策略禁止修改可移动驱动器加密部分的设置，则可以在子策略中进行编辑。

- 必须在操作系统设置中启用审计登录，以确保保护共享文件夹免受外部加密的排除功能正常运行。

- 如果启用了共享文件夹保护，则 Kaspersky Endpoint Security for Windows 会监视在启动 Kaspersky Endpoint Security for Windows 之前启动的每个远程访问会话加密共享文件夹的尝试，包括启动远程访问会话的计算机已被添加到排除中时。如果您不希望 Kaspersky Endpoint Security for Windows 监视从添加到排除的计算机上启动的远程访问会话以及在 Kaspersky Endpoint Security for Windows 启动之前启动的远程访问会话对共享文件夹的加密尝试，请终止并重新建立远程访问会话，或重新启动安装了 Kaspersky Endpoint Security for Windows 的计算机。

- 如果更新任务是以特定用户帐户的权限运行的，则从需要授权的源更新时，将不会下载产品补丁程序。

- 由于系统性能不足，应用程序可能无法启动。要解决此问题，请使用Ready Boot选项或增加启动服务的操作系统超时。

- 应用程序无法在 Windows Safe Mode下运行。

- 在安装应用程序后的第一次重新启动之前，我们不能保证音频控制工作正常。

- 在管理控制台(MMC)中，在配置应用程序权限窗口中的入侵预防设置中，**删除**按钮不可用。您可以通过应用程序的上下文菜单从信任组中删除应用程序。

- 在应用程序的本地界面中，在入侵预防设置中，如果计算机由策略管理，则应用程序权限和受保护的资源不可查看。滚动、搜索、过滤器和其他窗口控件不可用。您可以在 Kaspersky Security Center 控制台的策略属性中查看应用程序权限。

- 启用旋转跟踪文件后，不会为 AMSI 组件和 Outlook 插件创建跟踪。

- 无法在 Windows Server 2008 中手动收集性能跟踪。

- 不支持“重新启动”跟踪类型的性能跟踪。

- Pico 进程不支持转储日志记录。

- 关闭“**禁用系统服务的外部管理(D)**”选项将不允许您停止使用 `AMPPL=1` 参数安装的应用程序的服务（默认情况下，从 Windows 10RS2 操作系统版本开始，参数值设置为 `1`）。值为 `1` 的 `AMPPL` 参数允许对产品服务使用保护过程技术。

- 要运行文件夹的自定义扫描，启动自定义扫描的用户必须具有读取此文件夹属性的权限。否则自定义文件夹扫描将无法进行，并将以错误结束。

- 当策略中定义的扫描规则包含结尾没有 `\` 字符的路径时，例如 `C:\folder1\folder2`，将对路径 `C:\folder1\` 运行扫描。

- 如果您正使用软件限制策略(Software Restriction Policies, SRP)，计算机可能加载失败（黑屏）。为了防止出现故障，您需要允许在 SRP 属性中使用应用程序库。在 SRP 属性中，为 khkum.dll 文件添加具有“**Unrestricted**”安全级别的规则（“**New Hash Rule**”菜单项）。该文件位于 `C:\Program Files (x86)\Common Files\Kaspersky Lab\KES.14.1\klhk\klhk_x64\` 文件夹。如果您选择了此方法，则还需要清除 Kaspersky Endpoint Security 的“*更新*”任务设置中的“**下载应用程序模块更新**”复选框。有关使用 SRP 的详细信息，请参阅 Microsoft 文档。

  您还可以禁用 SRP 并使用 Kaspersky Endpoint Security 的“应用程序控制”组件来控制应用程序的使用。

- 如果计算机属于 Windows 组策略对象 (Group Policy Object, GPO) 下的域，并且 DriverLoadPolicy 参数设置为 8（Good only），则重新启动安装了 Kaspersky Endpoint Security 的计算机会导致 BSOD。为了防止失败，组策略中的 Early Launch Antimalware (ELAM) 参数必须设置为 1（Good and unknown）。ELAM 设置位于策略中的以下位置：**Computer Configuration → Administrative Templates → System → Early Launch Antimalware**。

- 不支持通过 Rest API 管理 Outlook 插件设置。

- 无法通过配置文件在设备之间传输特定用户的任务运行设置。从配置文件应用设置后，请手动指定用户名和密码。

- 安装更新后，完整性检查任务在系统重新启动以应用更新之前不起作用。

- 当通过远程诊断实用程序更改旋转的跟踪级别时，Kaspersky Endpoint Security for Windows 错误地显示跟踪级别的空白值。然而，跟踪文件是根据正确的跟踪级别编写的。当通过应用程序的本地接口更改旋转的跟踪级别时，跟踪级别被正确修改，但远程诊断实用程序错误地显示了该实用程序上次定义的跟踪级别。这可能导致管理员没有关于当前跟踪级别的最新信息，并且如果用户在应用程序的本地界面中手动更改跟踪级别，则跟踪中可能缺少相关信息。

- 在本地界面中，密码保护设置不允许更改管理员账户名称（默认是KLAdmin）。要更改管理员账户名称，您需要禁用密码保护，然后启用密码保护并指定管理员账户的新名称。

- 当安装在 Windows Server 2019 服务器时，Kaspersky Endpoint Security 应用程序与 Docker 不兼容。在具有 Kaspersky Endpoint Security 的计算机上部署 Docker 容器会导致崩溃（BSOD）。

- 如果 Kaspersky Endpoint Security 安装在 SQL Server DBMS 服务器，应用程序向服务器实例发送请求。这对于扫描 SQL Server 代理的作业和阻止恶意作业的运行是必要的。Kaspersky Endpoint Security 使用 SQL Server 用户账户来扫描作业。应用程序在扫描系统内存时和更新反病毒数据库后向服务器发送请求。

- Kaspersky Endpoint Security 和 Secret Net Studio 软件的兼容性有限：

  - Kaspersky Endpoint Security 应用程序与 Secret Net Studio 软件的反病毒组件不兼容。

    应用程序无法安装在部署了带有反病毒组件的 Secret Net Studio 的计算机上。要实现互操作性，您必须从 Secret Net Studio 中删除反病毒组件。

- Kaspersky Endpoint Security 应用程序与 Secret Net Studio 软件的磁盘保护和数据加密组件不兼容。

  应用程序无法安装在部署了带有磁盘保护和数据加密组件的 Secret Net Studio 的计算机上。要实现互操作性，您必须从 Secret Net Studio 中删除磁盘保护和数据加密组件。

- Secret Net Studio 与 Kaspersky Endpoint Security 的文件级加密（FLE）组件不兼容。

  当您安装带有文件级加密（FLE）组件的 Kaspersky Endpoint Security 时，Secret Net Studio 可能会出错。为了确保互操作性，必须从 Kaspersky Endpoint Security 中删除文件级加密（FLE）组件。

- 导入系统完整性监控规则时，应用程序会检查规则的 ID 和名称。如果规则 ID 相同，Kaspersky Endpoint Security 会用新规则替换现有规则。导出规则时，应用程序会自动分配 ID。如果您手动编辑了导出的规则 XML 文件，则可能存在具有相同 ID 的规则。如果规则 ID 唯一，但规则名称相同，Kaspersky Endpoint Security 会添加 `(1)`（依此类推）到规则名称。

- 从 Kaspersky Endpoint Security for Windows 12.11 版本开始，无法在 Web Console 中查看在子组中打开的父策略的设置。Web Console 还显示一条警告：*该策略是继承的。您仅可以在创建策略的管理组编辑策略设置。*

- 超过 256 个字符的弹出通知不会显示在管理控制台(MMC)中。

- 策略中的组件名称和安装包中的组件名称可能不同。例如，Endpoint Detection and Response Expert (on-premises) 可以命名为 Endpoint Detection and Response (KATA)、Endpoint Detection and Response Expert (on-premises)、Kaspersky Anti Targeted Attack Platform Integration。组件名称也可能因应用程序版本而异。

术语表

Integration Server

Kaspersky Endpoint Security for Virtualization Light Agent 组件。在 Kaspersky Endpoint Security 组件和虚拟基础架构之间交互。

IOC

妥协的指标。关于恶意对象或活动的一组数据。

IOC 文件

一个文件，其中包含一组妥协的指标 (IOCs)，应用程序试图匹配这些指标以计算检测次数。如果扫描后发现目标与多个 IOC 文件完全匹配，则检测的可能性会更高。

Kerberos 身份验证

客户端和服务器在建立连接之前进行相互身份验证的机制，使得在不安全的网络上进行通信成为可能。该机制基于票据，用户从受信任身份验证中心获得该票据。

Light Agent

Kaspersky Endpoint Security for Virtualization Light Agent 组件。它安装在需要保护的每个虚拟机上。

OLE 对象

附加的文件或嵌入到其他文件中的文件。Kaspersky 应用程序允许扫描 OLE 对象以查找病毒。例如，如果您在 Microsoft Office Word 文档中插入一个 Microsoft Office Excel® 表格，此表格将作为 OLE 对象被扫描。

OpenIOC

基于 XML 的开放标准的妥协的指标 (IOC) 描述，包括 500 多种不同的妥协的指标。

SVM

安全虚拟机 — 安装了扫描服务器服务（保护虚拟机，即 Kaspersky Endpoint Security for Virtualization Light Agent 的组件）的特殊虚拟机。

云发现

云发现管理用户对云服务的访问。云服务包括，例如，Microsoft Teams、Salesforce 和 Microsoft Office 365。云服务按类别分组，例如，*文件共享*、*消息软件*、*电子邮件*。

任务

卡巴斯基应用程序作为任务执行的功能，例如：实时文件保护、全盘设备扫描、数据库更新。

便携式文件管理器

这是一个应用程序，用于在计算机上没有加密功能时通过提供的界面处理可移动驱动器上的加密文件。

保护范围

在运行时被关键威胁防护组件持续扫描的对象。不同组件的保护范围有不同的参数。

反病毒数据库

数据库包含截至反病毒数据库发布时 Kaspersky 已知的计算机安全威胁的信息。反病毒数据库特征码有助于检测扫描对象中的恶意代码。反病毒数据库由 Kaspersky 专家创建并且每小时都会更新。

受信任平台模块

一个与安全相关的提供基本功能的微芯片（例如用于存储加密密钥）。受信任平台模块通常安装在计算机主板上并且通过硬件总线与其他所有系统组件进行互动。

受感染的文件

包含恶意代码（在扫描文件时检测到已知恶意软件的代码）的文件。Kaspersky 推荐您不要使用此类文件，原因是它们可能会感染您的计算机。

可疑网址的数据库

其内容被视为存在危险的网址列表。这是一个由 Kaspersky 专家创建的列表。它会定期更新，并且会包含在 Kaspersky 应用程序分发包中。

存档

打包到单一压缩文件的一个或几个文件。需要一个名叫 archiver 的应用程序以打开和解包数据。

已感染文件

基于文件的结构或格式，某些文件可能会作为存储和传播恶意代码的“容器”而成为入侵者的工具。一般来说，此类文件是可执行文件，例如扩展名为 .com、.exe 和 .dll 的文件。恶意代码入侵此类文件的风险相当高。

扫描范围

Kaspersky Endpoint Security 在运行扫描任务时扫描的对象。

授权许可证书

与密钥文件或激活码一起由 Kaspersky 传输给用户的文档。该文档包含授予用户的授权许可信息。

掩码

使用通配符表示文件名和扩展名。

文件掩码可包含文件名中允许使用的任何字符，包括通配符：

- `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\*\*.txt` 将包括位于 C: 驱动器的文件夹（但不包括子文件夹）中所有具有 TXT 扩展名的文件的路径。

- 两个连续 `*` 字符在文件或文件夹名称中代表任意一组字符（包括空集），包括 `\` 和 `/` 字符（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\**\*.txt` 将包括位于 `Folder` 嵌套子文件夹（除了 `Folder` 本身）中所有带 TXT 扩展名的文件的路径。掩码必须包含至少一个嵌套级别。掩码 `C:\**\*.txt` 不是有效掩码。** 掩码仅可用于创建扫描排除项。

- `?`（问号）字符代表任意单个字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\???.txt` 将包括位于 `Folder` 文件夹中所有带 TXT 扩展名且名称由三个字符构成的文件的路径。

活动密钥

程序当前正在使用的密钥。

清除

能够完全或部分恢复对象数据的一种处理已感染对象的处理方法。并非所有受感染的对象都能被杀毒。

管理组

一组共享通用功能的设备和一组在这些设备上安装的 Kaspersky 应用程序。对设备分组可将其作为单个单元轻松管理。一个组可包含其他组。您可以为组中每个安装的应用程序创建组策略和组任务。

网络代理

一个 Kaspersky Security Center 组件，它实现了管理服务器和特定网络节点（工作站或服务器）上安装的 Kaspersky 应用程序之间的交互。该组件对在 Windows 下运行的所有 Kaspersky 应用程序通用。网络代理的独立版本是为在其他操作系统下运行的应用程序而设计。

网页资源地址的规范化格式

网页资源的规范化格式地址是通过规范化获得的网页资源地址的文字表达。*规范化*是一个 Web 资源地址文字表达根据特定规则而改变的过程，例如从 Web 资源地址的文字表示中排除用户登录、密码和连接端口；此外 Web 资源地址的字符将从大写更改为小写。

在保护组件的运行中，规范化网页资源地址的目的是为了防止再次扫描实际上等效但是语法不同的网站地址。

例如：
非规范化格式的地址：www.Example.com\。
规范化格式的地址：www.example.com。

证书发布者

发布证书的认证中心。

误报

当 Kaspersky 应用程序由于未受感染文件的签名与病毒的签名类似而将其报告为受感染的文件时，就发生了误报。

身份验证代理

可启动硬盘驱动器加密后，让您完成身份验证以访问加密的硬盘驱动器并加载操作系统的接口。

钓鱼网页地址数据库

Kaspersky 专家确定的与钓鱼有关的网址列表。该数据库会定期更新，并且会包含在 Kaspersky 应用程序分发包中。

附录

本节包含的信息是对文档正文的补充。

附录 1.应用程序设置

您可以使用策略、任务或应用程序界面配置 Kaspersky Endpoint Security。有关应用程序组件的详细信息，请参见相应章节。

文件威胁防护

文件威胁防护组件可防止计算机文件系统受到感染。默认情况下，文件威胁防护组件永久驻留在计算机的 RAM 中，并实时扫描所有打开、保存和启动的文件。该组件扫描所有计算机驱动器（包括连接的驱动器）上的文件。该组件借助反病毒数据库、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。

该组件将扫描用户或应用程序访问的文件。如果检测到恶意文件，Kaspersky Endpoint Security 将阻止文件操作。应用程序随后将根据“文件威胁防护”组件的设置来清除或删除恶意文件。

当尝试访问其内容驻留在 OneDrive 云存储中的文件时，Kaspersky Endpoint Security 会下载并扫描文件内容。

文件威胁防护组件设置

参数	描述
安全级别 *（仅在管理控制台（MMC）和 Kaspersky Endpoint Security 界面可用）*	对于文件威胁防护，Kaspersky Endpoint Security 可以应用不同的设置组。存储在应用程序中的设置组叫做*安全级别*: • “**高**”。选择该文件安全级别后，“文件威胁防护”组件将对打开、保存和运行的所有文件实施最严格的控制。“文件威胁防护”组件会扫描计算机的所有硬盘驱动器、可移动驱动器和网络驱动器上的所有文件类型。它还扫描存档、安装包和嵌入式 OLE 对象。 • “**建议**”。该文件安全级别被 Kaspersky 专家推荐。“文件威胁防护”组件仅扫描计算机的所有硬盘驱动器、可移动驱动器和网络驱动器上的指定文件格式，以及嵌入式 OLE 对象。“文件威胁防护”组件不扫描压缩包或安装包。 • “**低**”。该文件安全级别的设置确保最大的扫描速度。“文件威胁防护”组件仅扫描计算机的所有硬盘驱动器、可移动驱动器以及网络驱动器上拥有指定扩展名的文件。“文件威胁防护”组件不扫描复合文件。
文件类型 *（仅在管理控制台（MMC）和 Kaspersky Endpoint Security 界面可用）*	“**所有文件**”。如果启用该设置，Kaspersky Endpoint Security 将毫无例外地扫描所有文件（所有格式和扩展名）。 “**按格式扫描文件**”。如果启用该设置，则应用程序仅扫描被感染的文件。在扫描文件以查找恶意代码之前，系统将分析文件的内部头以确定文件的格式（例如，.txt、.doc 或 .exe）。该扫描也查找具有特殊文件扩展名的文件。 “**按扩展名扫描文件**”。如果启用该设置，则应用程序仅扫描被感染的文件。此时，系统将根据文件的扩展名确定文件格式。
扫描范围	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）。
机器学习和特征码分析 *（仅在管理控制台（MMC）和 Kaspersky Endpoint Security 界面可用）*	机器学习和签名分析方法使用 Kaspersky Endpoint Security 数据库，其中包含已知威胁的描述以及消除它们的方法。使用此方法的保护提供了可接受的最低安全级别。 根据 Kaspersky 专家的推荐，机器学习和签名分析始终启用。

参数	描述
启发式分析 *（仅在管理控制台（MMC）和 Kaspersky Endpoint Security 界面可用）*	开发该技术的目的是检测使用当前版本的卡巴斯基应用程序数据库无法检测到的威胁。它可以检测可能受未知病毒或已知病毒新变种感染的文件。 当扫描文件以查找恶意代码时，启发式分析执行可执行文件中的指令。启发式分析执行的指令数量取决于启发式分析级别。启发式分析级别可在全面搜索新威胁、加载操作系统资源和启发式分析持续时间之间进行平衡。
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。 "**清除；如果清除失败则阻止**"。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，应用程序将阻止这些文件。 "**阻止**"。如果选择该选项，应用程序将自动阻止受感染的文件，而不试图对其进行清除或删除。 在对感染的文件进行清除或删除操作之前，应用程序会创建一个备份，以免日后会需要恢复该文件或对该文件进行清除。
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。
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	扫描第三方应用程序的分发包。
扫描 Microsoft Office 格式文件	扫描 Microsoft Office 文件（DOC、DOCX、XLS、PPT 和其他 Microsoft 扩展程序）。Office 格式文件也包括 OLE 对象。应用程序扫描小于 1 MB 的 office 格式文件，无论该复选框是否被选中。
扫描电子邮件格式文件	扫描电子邮件格式的文件。应用程序扫描 MSG 和 EML 文件。电子邮件格式的文件也包括 OLE 对象和 MHT 文件。Kaspersky Endpoint Security 扫描小于 1 MB 的电子邮件格式的文件，无论该复选框是否被选中。
复合文件大于指定值时不解压	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。
在后台解压复合文件	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。
扫描模式 *（仅在管理控制台（MMC）和 Kaspersky Endpoint Security 界面可用）*	Kaspersky Endpoint Security 扫描被用户、操作系统或使用该用户的账户运行的应用程序访问的文件。 "**智能模式**"。在该模式中，文件威胁防护将基于对象所做操作进行分析以扫描对象。例如，当操作某个 Microsoft Office 文档时，Kaspersky Endpoint Security 将在其首次打开和最后一次关闭时扫描该文件。覆盖文件的中间操作不会引起文件扫描。 "**在访问和修改时**"。在该模式中，文件威胁防护将在出现打开/修改文件的尝试时扫描对象。 "**在访问时**"。在该模式中，文件威胁防护将在出现打开对象的尝试时进行扫描。 "**执行时**"。在该模式中，文件威胁防护仅在出现运行文件的尝试时扫描对象。
使用 iSwift 技术 *（仅在管理控制台（MMC）和 Kaspersky Endpoint Security 界面可用）*	该技术允许通过排除特定文件不扫描的方式提高扫描速度。该技术将使用特殊算法将文件排除在扫描范围之外，该算法会考虑 Kaspersky Endpoint Security 数据库的发布日期、文件的上次扫描日期以及对扫描设置的任何修改。iSwift 技术是对用于 NTFS 文件系统的 iChecker 技术的增强版。
使用 iChecker 技术 *（仅在管理控制台（MMC）和 Kaspersky Endpoint Security 界面可用）*	该技术允许通过排除特定文件不扫描的方式提高扫描速度。该技术将使用特殊算法将文件排除在扫描范围之外，该算法会考虑 Kaspersky Endpoint Security 数据库的发布日期、文件的上次扫描日期以及对扫描设置的任何修改。iChecker 技术受到一些限制：它无法操作大型文件，并且仅能应用于具有应用程序可识别结构的文件（例如：EXE、DLL、LNK、TTF、INF、SYS、COM、CHM、ZIP 和 RAR）。

参数	描述
暂停文件威胁防护 *（仅在管理控制台（MMC）和 Kaspersky Endpoint Security 界面可用）*	这将在指定时间或使用指定应用程序时暂时和自动暂停文件威胁防护操作。
扫描在 Windows 容器中执行的文件操作	如果在容器内检测到威胁，该应用程序将应用为文件威胁防护组件选择的操作。 “**如果清除失败，则停止容器**”。应用程序可能没有足够的对检测到的对象进行读写的权限。在这种情况下，不可能对检测到的对象进行清除或删除。如果选中此复选框，应用程序将阻止检测到的对象并停止容器。如果清除此复选框，应用程序将仅阻止检测到的对象。 “**不扫描在 Windows 容器中执行的文件操作**”。如果选中该复选框，应用程序仅在容器启动时扫描容器。如果清除该复选框，应用程序将实时连续扫描容器。

Web 威胁防护

“Web 威胁防护”组件可防止从 Internet 下载恶意文件，同时阻止恶意网站和钓鱼网站。该组件借助反病毒数据库、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。

Kaspersky Endpoint Security 扫描 HTTP、HTTPS 和 FTP 流量。Kaspersky Endpoint Security 扫描 URL 和 IP 地址。

要使用 Web 威胁防护，您必须完成应用程序的初始配置：

- 对于 HTTPS 流量监控，启用加密连接扫描（默认情况下启用）。
- 选择 Kaspersky Endpoint Security 必须监控的端口（默认情况下，应用程序监控所有端口）。
- 选择您希望 Kaspersky Endpoint Security 监控其流量的应用程序。大多数浏览器已经存在于卡巴斯基推荐的应用程序列表中。如果列表中缺少您的浏览器，请手动添加。
- 我们建议将网页交互脚本注入到 Web 流量中（默认情况下，脚本注入是禁用的）。该脚本启用将 Web 威胁防护事件注册到应用程序事件日期、OS 事件日志和报告。

当用户尝试打开恶意网站或钓鱼网站时，Kaspersky Endpoint Security 将阻止访问并显示警告。

Web 威胁防护组件设置

参数	描述
安全级别 *（仅在管理控制台（MMC）和 Kaspersky Endpoint Security 界面可用）*	对于 Web 威胁防护，应用程序可以应用不同的设置组。存储在应用程序中的设置组叫做*安全级别*： • “**高**”。在此安全级别下，“Web 威胁防护”组件对计算机通过 HTTP 和 FTP 收到的 Web 流量执行最大限度的扫描。“Web 威胁防护”使用整个程序应用数据库详细扫描所有 Web 流量对象，并尽可能执行最深度的启发式分析。 • “**建议**”。在应用程序的性能和 Web 流量的安全性之间提供最佳平衡的安全级别。“Web 威胁防护”组件执行“中度扫描”扫描级别的启发式分析。Kaspersky 专家推荐使用此 Web 流量安全级别。 • “**低**”。此 Web 流量安全级别的设置可确保 Web 流量的最快扫描。“Web 威胁防护”组件执行“轻度扫描”扫描级别的启发式分析。
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。 “**通知**”。如果选择此选项并且在 Web 流量中检测到受感染对象，Kaspersky Endpoint Security 将允许将该对象下载到计算机，但会将受感染对象的相关信息添加到活动威胁列表中。

参数	描述
检查网址是否在恶意网址数据库中 *（仅在管理控制台（MMC）和 Kaspersky Endpoint Security 界面可用）*	扫描链接以决定它们是否被包含在恶意网址数据库中，这样您可以跟踪被列入拒绝列表的网站。恶意网址数据库由 Kaspersky 维护，包含在程序安装包中，并通过 Kaspersky Endpoint Security 数据库更新进行补充。
使用启发式分析 *（仅在管理控制台（MMC）和 Kaspersky Endpoint Security 界面可用）*	开发该技术的目的是检测使用当前版本的卡巴斯基应用程序数据库无法检测到的威胁。它可以检测可能受未知病毒或已知病毒新变种感染的文件。 当 Web 流量被扫描以查找病毒和其他威胁应用程序时，启发式分析执行可执行文件中的指令。启发式分析执行的指令数量取决于启发式分析级别。启发式分析级别可在全面搜索新威胁、加载操作系统资源和启发式分析持续时间之间进行平衡。
检查网址是否在钓鱼网址数据库中 *（仅在管理控制台（MMC）和 Kaspersky Endpoint Security 界面可用）*	钓鱼网址数据库包含当前用于启动钓鱼攻击的已知网站的地址。Kaspersky 使用从国际组织 Anti-Phishing Working Group 获取的网址补充该钓鱼链接数据库。钓鱼地址数据库包含在程序安装包中，并通过 Kaspersky Endpoint Security 数据库更新进行补充。
不扫描受信任网址的 Web 流量	如果选中此选项，“Web 威胁防护”组件将不再扫描其网址包含在受信任网址列表中的网页或网站的内容。您可以将网页/网站的特定地址和地址掩码添加至受信任网址列表。 您也可以为加密连接创建排除项常规列表。此种情况下，在 Web 威胁防护、邮件威胁防护和 Web 控制组件正常运行的情况下，Kaspersky Endpoint Security 不扫描受信任网址的 HTTPS 流量。

邮件威胁防护

“邮件威胁防护”组件扫描传入和传出电子邮件的附件是否有病毒和其他威胁。该组件借助反病毒数据库、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。

邮件威胁防护可以扫描传入和传出的邮件。该应用程序在以下邮件客户端中支持 POP3、SMTP、IMAP 和 NNTP：

- Microsoft Office Outlook
- Mozilla Thunderbird
- Windows Mail
- MyOffice Mail
- R7-Office Organizer

要扫描 Mozilla Thunderbird、MyOffice Mail 和 R7-Office Organizer 邮件客户端中的流量，您需要将卡巴斯基证书添加到证书存储并选择自己的证书存储。

邮件威胁防护不支持其他协议和邮件客户端。

邮件威胁防护可能并不总是能够获得邮件的*协议级*访问权限（例如，使用 Microsoft Exchange 解决方案时）。为此，邮件威胁防护包括 Microsoft Office Outlook 扩展程序。该扩展程序允许在*邮件客户端级别*扫描邮件。邮件威胁防护扩展程序支持 Outlook 2010、2013、2016、2019、2021、2024 和 365 的 32 位和 64 位版本。在基于 Arm 的计算机上，邮件威胁防护扩展程序支持 32 位和 64 位版本的 Outlook 2016、Outlook 2021、Outlook 2024 和 Outlook 365 for Arm64。

如果在浏览器中打开邮件客户端，“邮件威胁防护”组件不会扫描邮件。

当在附件中检测到恶意文件时，Kaspersky Endpoint Security 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>*。

邮件威胁防护组件设置

参数	描述
安全级别 *（仅在管理控制台（MMC）和 Kaspersky Endpoint Security 界面可用）*	对于邮件威胁防护，应用程序可以应用不同的设置组。存储在应用程序中的设置组叫做*安全级别*： • "**高**"。选择此电子邮件安全级别时，"邮件威胁防护"组件会最彻底地扫描电子邮件。"邮件威胁防护"组件将扫描发送和接收的电子邮件消息，并执行深度启发式分析。"高"邮件安全级别被推荐用于高风险环境。这种情况的一个例子就是，未获得集中式电子邮件保护的家庭网络连接免费的电子邮件服务。 • "**建议**"。在应用程序性能和电子邮件安全性之间提供最佳平衡的电子邮件安全级别。"邮件威胁防护"组件将扫描发送和接收的电子邮件，并执行中度启发式分析。Kaspersky 专家推荐采用这一邮件流量安全级别。 • "**低**"。选择此电子邮件安全级别时，"邮件威胁防护"组件只扫描接收的电子邮件消息，执行轻度启发式分析，不扫描电子邮件的压缩包附件。在这一邮件安全级别中，"邮件威胁防护"组件将使用最少的操作系统资源，以最大速度扫描电子邮件。在保护良好的环境中工作时，推荐使用"低"邮件安全级别。这类环境的例子包括具有集中式电子邮件保护的企业局域网。
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的对象时，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>*。 "**清除；如果清除失败则阻止**"。在入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。在出站邮件中检测到受感染的对象时，应用程序会尝试对检测到的对象进行清除。如果无法清除对象，应用程序会阻止邮件的传输，邮件客户端会显示错误。 "**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。
保护范围 *（仅在管理控制台（MMC）和 Kaspersky Endpoint Security 界面可用）*	*保护范围*包括组件在运行时检查的对象：接收和发送的消息或仅接收的消息。 为了保护您的计算机，您仅需要扫描接收邮件消息。您可以开启扫描发送邮件消息以防范发送在存档中的受感染文件。如果您要防范发送的特殊格式的文件，例如音频和视频文件，您也可以开启扫描发送邮件消息。
扫描 POP3、SMTP、NNTP 和 IMAP 流量	"邮件威胁防护"组件对通过 POP3、SMTP、NNTP 和 IMAP 协议传送的流量进行扫描。
连接 Microsoft Outlook 扩展程序	如果选中该复选框，则在 Microsoft Outlook 中集成的扩展程序一侧启用对通过 POP3、SMTP、NNTP、IMAP 协议传输的电子邮件的扫描。 如果使用 Microsoft Outlook 的扩展程序扫描邮件，建议使用Cached Exchange Mode。有关缓存 Exchange 模式的详细信息和对其用途的建议，请参阅 Microsoft 知识库 。
启发式分析 *（仅在管理控制台（MMC）和 Kaspersky Endpoint Security 界面可用）*	开发该技术的目的是检测使用当前版本的卡巴斯基应用程序数据库无法检测到的威胁。它可以检测可能受未知病毒或已知病毒新变种感染的文件。 当扫描文件以查找恶意代码时，启发式分析执行可执行文件中的指令。启发式分析执行的指令数量取决于启发式分析级别。启发式分析级别可在全面搜索新威胁、加载操作系统资源和启发式分析持续时间之间进行平衡。
扫描附加的压缩包	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。 如果在扫描过程中，应用程序检测到邮件文本中的存档密码，则该密码将用于扫描存档内容以查找恶意应用程序。在这种情况下，不会保存密码。在扫描过程中，存档被解包。如果在解包过程中发生应用程序错误，您可以手动删除保存到以下路径的解包文件：%systemroot%\temp。文件具有 PR 前缀。
扫描 Microsoft Office 格式的附加文件	扫描 Microsoft Office 文件（DOC、DOCX、XLS、PPT 和其他 Microsoft 扩展程序）。Office 格式文件也包括 OLE 对象。应用程序扫描小于 1MB 的 office 格式文件，无论该复选框是否被选中。
不扫描大于该值的存档 N MB	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。

参数	描述
限制检查存档的时间到 N 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。
附件过滤器	附件过滤器不适用于传出电子邮件。 “**禁用过滤**”。如果选择此选项，“邮件威胁防护”组件将不过滤属于电子邮件附件的文件。 “**重命名选定类型的附件**”。如果您选择该选项，邮件威胁防护组件将使用下划线字符（例如，attachment.doc_）替换上一个在指定类型的附加文件中找到的扩充字符。因此，为了打开文件，用户必须重命名文件。 “**删除选定类型的附件**”。如果选择此选项，“邮件威胁防护”组件将从电子邮件中删除指定的附件类型。 在文件掩码列表中，可以指定要重命名或从电子邮件中删除的附加文件的类型。

网络威胁防护

*网络威胁防护组件*组件（也称Intrusion Detection System，IDS）监控入站网络流量以查找网络攻击的活动特征。当应用程序在用户计算机上检测到网络攻击企图时，它将阻止与攻击计算机的网络连接。应用程序数据库提供了当前已知类型的网络攻击以及应对方法的描述。“网络威胁防护”组件检测到的网络攻击列表在数据库和应用程序模块更新期间更新。

网络威胁防护组件设置

参数	描述
将端口扫描和网络 Flooding 视为攻击	*网络 Flooding* 是对网络资源或组织（例如 Web 服务器）的攻击。该攻击包括发送大量的请求以让网络资源过载。当发生此类事情时，用户无法访问组织的网络资源。 *端口扫描*攻击包括扫描计算机上的 UDP 端口、TCP 端口和网络服务。该攻击允许攻击者识别计算机的漏洞程度，然后再发起更危险的网络攻击。端口扫描也允许攻击者识别计算机上的操作系统并选择针对性的网络攻击。 若选中此复选框，则 Kaspersky Endpoint Security 将监控网络流量以检测这些攻击。如果检测到攻击，应用程序会通知用户并将相应事件发送到 Kaspersky Security Center。该应用程序提供有关攻击计算机的信息，这是及时威胁响应操作所必需的。 如果一些您允许的应用程序执行了类似某些类型攻击的操作，您可以禁用对这些类型攻击的检测。这将帮助避免误报。
阻止攻击设备 N 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。 您可以在网络监控工具窗口查看阻止列表。 当应用程序重启和网络威胁防护设置被更改时，Kaspersky Endpoint Security 清空阻止列表。
排除项	该列表包含某些 IP 地址，“网络威胁防护”不会阻止这些 IP 地址发起的网络攻击。 您可以添加指定端口和协议的 IP 地址。 应用程序不会记录有关来自排除列表中的 IP 地址的网络攻击的信息。
MAC 欺骗防护	*MAC 欺骗攻击*包括更改网络设备（网卡）的 MAC 地址。结果，攻击者可以将发送到某台设备的数据重定向到另一台设备，并获得对该数据的访问权限。Kaspersky Endpoint Security 允许您阻止 MAC 欺骗攻击并接收关于攻击的通知。

防火墙

在互联网或局域网上工作时，防火墙组件会阻止未经授权的计算机连接。防火墙还控制计算机上应用程序的网络活动。这允许您保护公司局域网免受身份盗窃和其他攻击。该组件借助反病毒数据库、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。

网络代理被用于与 Kaspersky Security Center 的交互。防火墙自动创建应用程序和网络代理工作所需的网络规则。结果，防火墙打开计算机上的若干个端口。打开哪些端口取决于计算机的角色（例如，分发点）。要了解要在计算机上打开的端口，请参阅 Kaspersky Security Center 帮助。

网络规则

您可以在以下级别配置网络规则：

- *网络数据包规则*。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。Kaspersky Endpoint Security 具有预定义的网络数据包规则，其中权限由 Kaspersky 专家推荐。
- *应用程序网络规则*。应用程序网络规则将对特定应用程序的网络活动进行限制。它们不仅将网络数据包的特征列入重要参考因素，还把接收或发送该网络数据包的应用程序列入重要参考因素中。

应用程序对操作系统资源、进程和个人数据的受控访问由“主机入侵防御”组件通过*应用程序权限*提供。

在应用程序首次启动期间，“防火墙”执行以下操作：

1. 使用下载的反病毒数据库检查应用程序的安全性。
2. 在卡巴斯基安全网络中检查应用程序安全性。

   建议您加入卡巴斯基安全网络以帮助“防火墙”更有效地工作。
3. 将应用程序置于其中一个信任组中：*受信任*、*低限制*、*高限制*、*不信任*。

   信任组定义了在控制应用程序活动时 Kaspersky Endpoint Security 所引用的权限。Kaspersky Endpoint Security 会将应用程序放置在某个信任组中，具体取决于该应用程序可能对计算机造成的危险级别。

   Kaspersky Endpoint Security 将应用程序放置在“防火墙”和“主机入侵防御”组件的信任组中。您不能仅更改“防火墙”或“主机入侵防御”的信任组。

   如果您拒绝加入 KSN 或没有网络，Kaspersky Endpoint Security 会根据“主机入侵防御”组件的设置将应用程序放置在某个信任组中。从 KSN 收到应用程序的信誉后，可以自动更改信任组。
4. 它根据信任组阻止应用程序的网络活动。例如，不允许“*高限制*”信任组中的应用程序使用任何网络连接。

当应用程序下一次启动时，Kaspersky Endpoint Security 会检查该应用程序的完整性。如果应用程序未更改，则该组件对其应用当前网络规则。如果应用程序已经过修改，Kaspersky Endpoint Security 会分析应用程序，就像它首次启动时一样。

网络规则优先级

每条规则都有优先级。规则在列表中的位置越高，优先级越高。如果将网络活动添加到多条规则中，“防火墙”会根据优先级最高的规则来管理网络活动。

网络数据包规则的优先级比应用程序网络规则高。如果网络数据包规则和应用程序网络规则指定了同一类别的网络活动，则该网络活动将根据网络数据包规则进行处理。

应用程序的网络规则以特定方式工作。应用程序的网络规则包括基于网络状态的访问规则：*公用网络*、*本地网络*、*受信任网络*。例如，默认情况下，“*高限制*”信任组中的应用程序在所有状态的网络中均不允许进行任何网络活动。如果为单个应用程序（父应用程序）指定了网络规则，则其他应用程序的子进程将依据父应用程序的网络规则运行。如果没有为应用程序指定网络规则，则子进程将依据应用程序信任组的网络访问规则运行。

例如，对于除浏览器 X 之外的所有应用程序，您已禁止所有状态的网络中的任何网络活动。如果从浏览器 X（父应用程序）中启动浏览器 Y 的安装（子进程），则浏览器 Y 安装程序将能够访问网络并下载必要的文件。安装之后，浏览器 Y 将根据防火墙设置被拒绝任何网络连接。要禁止作为子进程的浏览器 Y 安装程序的网络活动，必须为浏览器 Y 的安装程序添加网络规则。

网络连接类型

“防火墙”允许您根据网络连接的类型来控制网络活动。Kaspersky Endpoint Security 从计算机的操作系统接收网络连接类型。操作系统中的网络连接类型由用户在建立连接时设置。您可以在 Kaspersky Endpoint Security 设置中更改网络连接的类型。“防火墙”将根据 Kaspersky Endpoint Security 设置中而不是操作系统中指定的网络类型来监控网络活动。

有以下网络连接类型可用：

- “**公用网络**”。网络不受反病毒应用程序、防火墙或过滤器保护（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，防火墙可阻止对此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访问数据和远程访问该计算机的桌面。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。

  防火墙默认给互联网分配“*公用网络*”类型。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**”。其中的计算机不会暴露于攻击或未经授权的数据访问尝试的安全网络。防火墙允许在具有此状态的网络中进行任何网络活动。

参数	描述
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 Microsoft Windows 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。
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。 默认情况下已将“*公用网络*”状态分配给互联网。您无法更改互联网的状态。
应用程序规则	“**应用程序**”。“防火墙”组件控制的应用程序表。应用程序分配到信任组中。信任组定义 Kaspersky Endpoint Security 控制应用程序的网络活动时使用的权限。 您可以从受策略影响的计算机上安装的所有应用程序的单一列表中选择应用程序，并将该应用程序添加到信任组。 “**网络规则**”。属于信任组的应用程序的网络规则表。防火墙按照这些规则管理应用程序的网络活动。 该表显示了 Kaspersky 专家推荐的预定义网络规则。这些网络规则已添加，以最佳方式保护运行 Windows 操作系统的计算机的网络流量。无法删除预定义网络规则。

BadUSB 攻击防护

某些病毒会修改 USB 设备的固件以欺骗操作系统，将 USB 伪装为键盘。结果，病毒可能在您的用户账户下执行命令以下载恶意软件。

BadUSB 攻击防护组件可以防止受感染的模拟键盘 USB 设备连接至计算机。

当 USB 设备连接至计算机并被操作系统识别为键盘时，应用程序将提示用户从该键盘输入其生成的数字代码或使用屏幕键盘（如果可用）（参见下图）。这个步骤称为键盘授权。

如果代码输入正确，应用程序会将识别参数（键盘的 VID/PID 及其连接的端口号）保存在已授权键盘列表中。重启操作系统后重新连接键盘时无需重复键盘授权。

经授权的键盘连接至该计算机不同的 USB 端口时，应用程序将提示为该键盘再次授权。

如果错误输入数字代码，则程序将生成新的代码。您可以配置尝试输入数字代码的次数。如果数字代码多次输入错误或键盘授权窗口关闭（参见下图），应用程序将阻止从该键盘输入。当达到 USB 设备阻止时间或者操作系统重启后，程序将再次提示用户重新执行键盘授权。

程序将允许使用经过授权的键盘并阻止未经授权的键盘。

默认情况下，未安装“BadUSB 攻击防护”组件。如果需要“BadUSB 攻击防护”组件，可以在安装应用程序前在安装包的属性中添加该组件，或者在安装应用程序后更改可用应用程序组件。

键盘授权

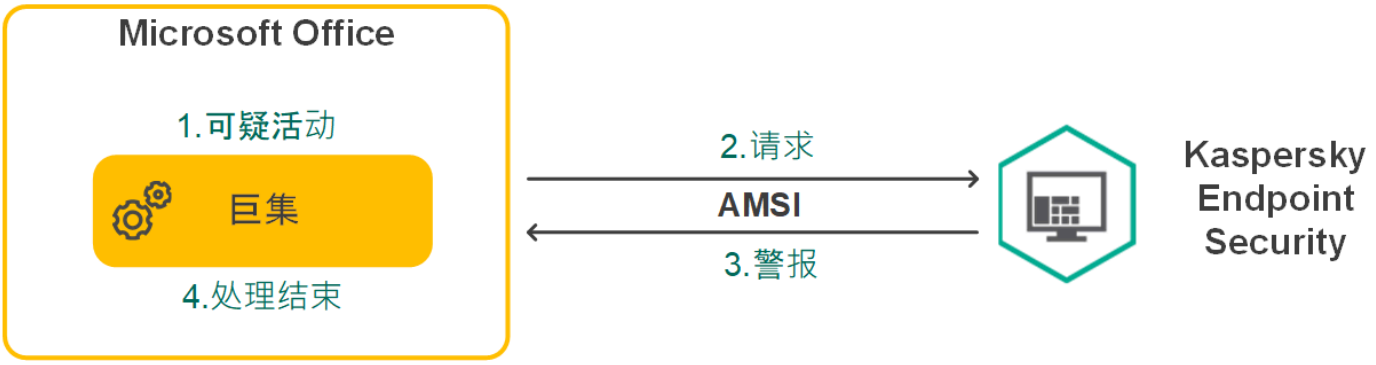
BadUSB 攻击防护组件设置

参数	描述
禁止使用屏幕键盘授权 USB 设备	如果此切换按钮被打开，应用程序将阻止使用屏幕键盘认证无法输入认证码的 USB 设备。
禁止使用条形码授权 USB 设备	如果此切换开关被启用，应用程序将不会在条形码扫描器身份验证通知中显示条形码。
USB 设备授权尝试的最大数量	如果授权码输入不正确达到指定次数，则自动阻止 USB 设备。有效值为 1 到 10。例如，如果允许 5 次尝试输入授权码，则在第五次尝试失败后，应用程序将阻止 USB 设备。Kaspersky Endpoint Security 显示 USB 设备的阻塞持续时间。此时间过后，您还可以再尝试 5 次输入授权代码。
达到最大尝试数量的超时时间	在指定次数的授权码输入失败后，USB 设备将被阻止。有效值为 1 到 180（分钟）。

AMSI 保护

AMSI 保护组件旨在支持 Microsoft 的反恶意软件扫描接口。*反恶意软件扫描接口 (AMSI)* 允许具有 AMSI 支持的第三方应用程序将对象（例如，PowerShell 脚本）发送到 Kaspersky Endpoint Security 进行附加扫描，然后接收这些对象的扫描结果。例如，第三方应用程序可能包括 Microsoft Office 应用程序（请参见下图）。有关 AMSI 的详细信息，请参阅 Microsoft 文档。

AMSI 保护组件只能检测威胁并将检测到的威胁通知给第三方应用程序。在收到威胁通知后，第三方应用程序不允许恶意操作（例如，它会终止操作）。



AMSI 操作示例

AMSI 保护组件可能会拒绝第三方应用程序的请求，例如，如果该应用程序超出了指定间隔内的最大请求数。Kaspersky Endpoint Security 将有关来自第三方应用程序的被拒绝请求的信息发送至管理服务器。AMSI 保护组件不会拒绝来自已启用与 AMSI 保护组件持续集成的第三方应用程序的请求。

AMSI 保护组件可用于以下适用于工作站和服务器的操作系统：

- Windows 10 Home / Pro / Pro for Workstations / Education / Enterprise / Enterprise multi-session
- Windows 11 Home / Pro / Pro for Workstations / Education / Enterprise
- Windows Server 2016 Essentials / Standard / Datacenter (包括 Server Core 模式)
- Windows Server 2019 Essentials / Standard / Datacenter (包括 Server Core 模式)
- Windows Server 2022 Standard / Datacenter / Datacenter: Azure Edition (包括 Server Core 模式)
- Windows Server 2025 Standard / Datacenter

AMSI 保护设置

参数	描述
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	扫描第三方应用程序的分发包。
扫描 Microsoft Office 格式文件	扫描 Microsoft Office 文件（DOC、DOCX、XLS、PPT 和其他 Microsoft 扩展程序）。Office 格式文件也包括 OLE 对象。应用程序扫描小于 1 MB 的 office 格式文件，无论该复选框是否被选中。
复合文件大于指定值时不解压	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。

漏洞利用防御

“漏洞利用防御”组件可检测利用计算机漏洞来利用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。

漏洞利用防御组件还会监控可能威胁计算机安全的应用程序进程的网络端口。应用程序通过反病毒数据库获取有关此类进程的信息。

漏洞利用防御组件设置

参数	描述
检测到漏洞时	“**阻止**”。如果选择此项，在检测到漏洞时，Kaspersky Endpoint Security 会阻止此漏洞的操作，并生成一条包含此漏洞相关信息的日志条目。 “**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。
启用系统进程内存保护	如果打开此切换按钮，Kaspersky Endpoint Security 将阻止尝试访问系统进程内存的外部进程。

行为检测

“行为检测”组件接收您计算机上的应用程序操作的信息，并将此信息提供给其他保护组件以提高性能。“行为检测”组件将行为流签名 (BSS) 用于应用程序。如果应用程序操作匹配行为流签名，Kaspersky Endpoint Security 将执行选定的响应操作。Kaspersky Endpoint Security 功能基于行为流签名，并为计算机提供主动防御。

行为检测组件还会监控可能威胁计算机安全的应用程序进程的网络端口。应用程序通过反病毒数据库获取有关此类进程的信息。

行为检测组件设置

参数	描述
检测到恶意软件活动时的操作	“**删除**”。如果选择此选项，在检测到恶意活动时，Kaspersky Endpoint Security 会删除恶意应用程序的可执行文件，同时在备份区创建该文件的备份副本。 “**阻止**”。如果选择此选项，在检测到恶意活动时，Kaspersky Endpoint Security 会终止该应用程序。 “**通知**”。如果选择此选项并且检测到应用程序的恶意活动，Kaspersky Endpoint Security 不会终止该应用程序，但会将该应用程序的恶意活动的相关信息添加至活动威胁列表。

主机入侵防御

“主机入侵防御”组件可避免应用程序执行可能给操作系统带来危险的操作，并确保控制对操作系统资源和个人数据的访问。该组件借助反病毒数据库和卡巴斯基安全网络云服务来提供计算机保护。

该组件通过*应用程序权限*来控制应用程序的操作。应用程序权限包括以下访问参数：

- 对操作系统资源（例如，自动启动选项、注册表项）的访问权限
- 对个人数据（例如文件和应用程序）的访问权限

应用程序的网络活动由防火墙组件使用*网络规则*控制。

在应用程序首次启动期间，“主机入侵防御”组件执行以下操作：

1. 使用下载的反病毒数据库检查应用程序的安全性。
2. 在卡巴斯基安全网络中检查应用程序安全性。

   建议您加入卡巴斯基安全网络以帮助“主机入侵防御”组件更有效地工作。

3. 将应用程序置于其中一个信任组中：*受信任*、*低限制*、*高限制*、*不信任*。

   信任组定义了在控制应用程序活动时 Kaspersky Endpoint Security 所引用的权限。Kaspersky Endpoint Security 会将应用程序放置在某个信任组中，具体取决于该应用程序可能对计算机造成的危险级别。

   Kaspersky Endpoint Security 将应用程序放置在“防火墙”和“主机入侵防御”组件的信任组中。您不能仅更改“防火墙”或“主机入侵防御”的信任组。

   如果您拒绝加入 KSN 或没有网络，Kaspersky Endpoint Security 会根据“主机入侵防御”组件的设置将应用程序放置在某个信任组中。从 KSN 收到应用程序的信誉后，可以自动更改信任组。

4. 根据信任组阻止应用程序操作。例如，“*高限制*”信任组中的应用程序被拒绝访问操作系统模块。

当应用程序下一次启动时，Kaspersky Endpoint Security 会检查该应用程序的完整性。如果应用程序未更改，则该组件对其应用当前应用程序权限。如果应用程序已经过修改，Kaspersky Endpoint Security 会分析应用程序，就像它首次启动时一样。

主机入侵防御组件设置

参数	描述
应用程序权限	“主机入侵防御”组件监控的应用程序表。应用程序分配到信任组中。信任组定义了在控制应用程序活动时 Kaspersky Endpoint Security 所引用的权限。 您可以从受策略影响的计算机上安装的所有应用程序的单一列表中选择应用程序，并将该应用程序添加到信任组。 下表显示了应用程序访问权限： • “**文件和系统注册表**”。属于信任组的应用程序的操作系统资源和个人数据访问权限表。 • “**权限**”。属于信任组的应用程序的进程和操作系统资源的访问权限表。 • “**网络规则**”。属于信任组的应用程序的网络规则表。防火墙按照这些规则管理应用程序的网络活动。该表显示了 Kaspersky 专家推荐的预定义网络规则。这些网络规则已添加，以最佳方式保护运行 Windows 操作系统的计算机的网络流量。无法删除预定义网络规则。
受保护资源	该表包含分类的计算机资源。“主机入侵防御”组件监控其他应用程序访问该表资源的尝试。 资源可以是注册表类别、文件或文件夹或注册表项。
Kaspersky Endpoint Security 启动之前启动的应用程序的信任组	Kaspersky Endpoint Security 将在其中放置应用程序的信任组，这些应用程序在 Kaspersky Endpoint Security 启动之前启动。

参数	描述
从 KSN 为之前未知应用程序更新规则	如果选中该复选框，“主机入侵防御”组件将通过使用卡巴斯基安全网络数据库来更新以前未知的应用程序的权限。
信任具有数字签名的应用程序	如果选中该选框，“主机入侵防御”组件会将带有受信任供应商数字签名的应用程序放置在“*受信任*”组中。 *受信任供应商*是被 Kaspersky 信任的软件供应商。您也可以手动添加供应商证书到受信任证书存储。 如果清空该选框，“主机入侵防御”组件将不再信任此类应用程序，并使用其他参数以确定它们的信任组。
删除超过以下时间未启动的应用程序的规则 N 天(从 1 到 90)	如果选中该复选框，则在满足以下条件的情况下，Kaspersky Endpoint Security 会自动删除有关该应用程序的信息（信任组和访问权限）： • 您手动将应用程序放入信任组或配置其访问权限。 • 该应用程序在定义的时间段内未启动。 如果应用程序的信任组和权限已自动确定，Kaspersky Endpoint Security 将在 30 天后删除有关此应用程序的信息。不能更改应用程序信息的存储期限或关闭自动删除。 下次启动该应用程序时，Kaspersky Endpoint Security 会像首次启动该应用程序一样对其进行分析。
未包含在其他组中的应用程序的信任组	此下拉列表中的项目决定了 Kaspersky Endpoint Security 将未知应用程序分配到哪个信任组。 您可以选择以下项目之一： • “**低限制**”。 • “**高限制**”。 • “**不信任**”。

修复引擎

修复引擎组件允许 Kaspersky Endpoint Security 回滚恶意软件在操作系统中执行的操作。

回滚操作系统中的恶意软件活动时，Kaspersky Endpoint Security 将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（在除网络驱动器外的所有介质上）创建的可执行文件。
  - 删除已被恶意软件入侵的程序所创建的可执行文件。
  - 恢复被恶意软件修改或删除的文件。

  文件恢复功能有一些限制.

- **注册表活动**

  Kaspersky Endpoint Security 执行以下操作：

  - 删除由恶意软件创建的注册表项。
  - 不会恢复被恶意软件修改或删除的注册表项。

- **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。
- 终止被恶意应用程序渗透的进程。
- 不恢复被恶意软件挂起的进程。

- **网络活动**

  Kaspersky Endpoint Security 执行以下操作：

  - 阻止恶意软件的网络活动。
  - 阻止被恶意软件入侵的进程的网络活动。

“文件威胁防护”或“行为检测”组件或在恶意软件扫描过程中可以启动恶意软件操作回滚。

回滚恶意软件操作会影响一组严格定义的数据。回滚对操作系统或计算机数据完整性无不良影响。

卡巴斯基安全网络

	为了更有效地保护您的计算机，Kaspersky Endpoint Security 使用从全球用户处接收的数据。卡巴斯基安全网络设计用于收集此数据。

KSN 功能可能无法在美国的应用程序中使用。

卡巴斯基安全网络 (KSN) 是一个云服务的基础架构。它可以访问在线卡巴斯基知识库。该知识库中包含了文件信誉、网页资源和软件的相关信息。使用卡巴斯基安全网络的数据可确保 Kaspersky Endpoint Security 能够更快地对新威胁作出响应，提高一些保护组件的性能，并减少误报风险。如果您正在参与卡巴斯基安全网络，KSN 服务为 Kaspersky Endpoint Security 提供有关已扫描网址的信誉的信息，以及有关已扫描文件的类别和信誉的信息。有关配置对 KSN 的访问的更多详细信息，请参阅 Kaspersky Security Center 帮助。

卡巴斯基安全网络的使用是自愿的。应用程序将在初始配置期间提示您使用 KSN。用户可以随时开始或停止加入 KSN。

有关在参与 KSN 期间生成的卡巴斯基统计信息的发送详情，以及有关此类信息的存储和销毁，请参阅卡巴斯基安全网络声明和卡巴斯基网站。含有卡巴斯基安全网络声明文本的 ksn_<语言 ID>.txt 文件包括在应用程序分发包中。

卡巴斯基信誉数据库的基础设施

Kaspersky Endpoint Security 支持以下用于使用卡巴斯基信誉数据库的基础设施解决方案：

- *卡巴斯基安全网络（KSN）*是大多数卡巴斯基应用程序使用的解决方案。KSN 参与者从卡巴斯基接收信息，并向卡巴斯基发送用户计算机上检测到的对象的信息，以便 卡巴斯基分析人员进行额外分析，并包括在卡巴斯基安全网络的信誉和统计数据库中。

- *卡巴斯基私有安全网络*是让运行 Kaspersky Endpoint Security 或其他卡巴斯基应用程序的计算机的用户获得卡巴斯基信誉数据库以及其他统计数据的访问权限的解决方案，无需从他们自己的计算机向卡巴斯基发送数据。KPSN 专为因以下任一原因无法参与卡巴斯基安全网络的公司客户所设计：

  - 本地工作站未连接 Internet。

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。

卡巴斯基安全网络设置

参数	描述
启用扩展 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。
启用云模式	*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。 如果打开该切换按钮，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。 如果关闭该切换按钮，Kaspersky Endpoint Security 将使用反病毒数据库的完全版本。 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。
KSN 服务器不可用时计算机状态 *（仅在 Kaspersky Security Center 控制台可用）*	此下拉列表中的项可确定当 KSN 服务器不可用时计算机在 Kaspersky Security Center 中的状态。
使用管理服务器作为 KSN 代理服务器 *（仅在 Kaspersky Security Center 控制台可用）*	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 *（仅在 Kaspersky Security Center 控制台可用）*	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）。

日志审查

如果 Kaspersky Endpoint Security 安装在运行 Windows for Servers 的计算机上，则该组件可用。如果 Kaspersky Endpoint Security 安装在运行 Windows for Workstations 的计算机上，则该组件不可用。

从版本 11.11.0 开始，Kaspersky Endpoint Security for Windows 包含日志审查组件。日志检查根据 Windows 事件日志分析监控受保护环境的完整性。当应用程序在系统中检测到非典型行为的迹象时，它会通知管理员，因为该行为可能表示试图进行网络攻击。

Kaspersky Endpoint Security 分析 Windows 事件日志，并根据规则检测违规行为。该组件包括预定义规则。预定义规则由启发式分析提供支持。您还可以添加自己的规则（自定义规则）。当规则触发时，应用程序将创建具有“*严重*”状态的事件（参见下图）。

如果您要使用日志审查，请确保已配置审计策略安全设置，并且系统正在记录相关事件（有关详细信息，请参阅 Microsoft 技术支持网站）。

日志审查通知

日志审查设置

参数	描述
预定义规则	日志审查规则列表。预定义规则包括受保护计算机上异常活动的模板。异常活动可能表示攻击未遂。
自定义规则	用户添加的日志审查规则列表。您可以设置自己的日志审查规则和触发条件。为此，您必须输入事件 ID 并选择事件源。您可以从标准日志中选择事件源：*Application*、*Security*或*System*。您还可以指定第三方应用程序的日志。

反加密

反加密组件分析共享文件夹中的活动。如果该活动与外部加密的典型行为流签名匹配，Kaspersky Endpoint Security 将执行选定操作。

Kaspersky Endpoint Security 可防止只在具有 NTFS 文件系统的介质上且未被 EFS 系统加密的文件被外部加密。

参数	描述
按名称或 IP 地址的排除项	"**按名称或 IP 地址的排除项**"。尝试加密共享文件夹的计算机的列表不会受到监控。 要应用防止共享文件夹被外部加密的计算机排除列表，必须在 Windows 安全审核策略中启用审核登录。默认情况下，审核登录处于禁用状态。有关 Windows 安全审核策略的详细信息，请访问 Microsoft 网站。 "**按掩码的排除项**"。保护范围排除项。如果您的组织在使用共享文件夹交换文件时使用数据加密，则从保护范围排除文件夹可以减少误报量。例如，当用户处理共享文件夹中具有 ENC 扩展名的文件时，行为检测可能会引发误报。这种活动与外部加密的典型行为模式相匹配。如果您在共享文件夹中有加密文件以保护数据，请将该文件夹添加到排除项。 使用掩码： • `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\*\*.txt` 将包括位于 C: 驱动器的文件夹（但不包括子文件夹）中所有具有 TXT 扩展名的文件的路径。 • 两个连续 `*` 字符在文件或文件夹名称中代表任意一组字符（包括空集），包括 `\` 和 `/` 字符（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\**\*.txt` 将包括位于 `Folder` 嵌套子文件夹（除了 `Folder` 本身）中所有带 TXT 扩展名的文件的路径。掩码必须包含至少一个嵌套级别。掩码 `C:\**\*.txt` 不是有效掩码。 • `?`（问号）字符代表任意单个字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\???.txt` 将包括位于 `Folder` 文件夹中所有带 TXT 扩展名且名称由三个字符构成的文件的路径。
检测到威胁后的操作	• "**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 会将有关此尝试的信息添加到活动威胁列表中，并添加条目到本地应用程序界面报告，并将有关检测到的恶意活动的信息发送到 Kaspersky Security Center。 • **阻止连接时长(分钟) N 分钟**。如果选择此选项，当 Kaspersky Endpoint Security 检测到有人试图修改共享文件夹中的文件时，它将阻止启动恶意活动的会话对文件修改的访问，并创建已修改文件的备份副本。 如果启用了"修复引擎"组件，并且选择"**阻止连接时长(分钟) N 分钟**"选项，被修改的文件将被从备份副本恢复。
保护范围	*保护范围*是 Kaspersky Endpoint Security 监控文件活动的共享文件夹路径列表。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。默认情况下，应用程序会自动识别共享文件夹并监控所有文件夹中的文件活动。

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（请参见下图）。

要使用 Web 控制，您必须完成应用程序的初始配置：

- 对于 HTTPS 流量监控，启用加密连接扫描（默认情况下启用）。
- 选择 Kaspersky Endpoint Security 必须监控的端口（默认情况下，应用程序监控所有端口）。
- 选择您希望 Kaspersky Endpoint Security 监控其流量的应用程序。大多数浏览器已经存在于卡巴斯基推荐的应用程序列表中。如果列表中缺少您的浏览器，请手动添加。
- 我们建议将网页交互脚本注入到 Web 流量中（默认情况下，脚本注入是禁用的）。该脚本启用将 Web 控制事件注册到应用程序事件日期、OS 事件日志和报告。

管理对网站的访问的方法

“Web 控制”允许您使用以下方法配置对网站的访问：

- **网站类别**。网站按照卡巴斯基安全网络云服务、启发式分析和已知网站数据库（包含在应用程序数据库中）进行分类。例如，您可以限制用户对“*社交网络*”类别或其他类别的访问。
- **数据类型**。例如，您可以限制用户访问网站上的数据，并隐藏图像。Kaspersky Endpoint Security 根据文件格式确定数据类型，而不是基于其扩展名。

  > Kaspersky Endpoint Security 不扫描压缩文件内的文件。例如，如果图像文件放在压缩文件中，Kaspersky Endpoint Security 会识别“*存档*”数据类型而不是“*图形*”。

- **单个地址**。您可以输入网址或使用掩码。

可以同时使用多种方法来管理对网站的访问。例如，您可以仅针对“*基于 Web 的邮件*”网站类别限制对“*Office 应用程序文件*”数据类型的访问。

网站访问规则

“Web 控制”通过使用*访问规则*管理用户对网站的访问。您可以为网站访问规则配置以下高级设置：

- 规则适用的用户。

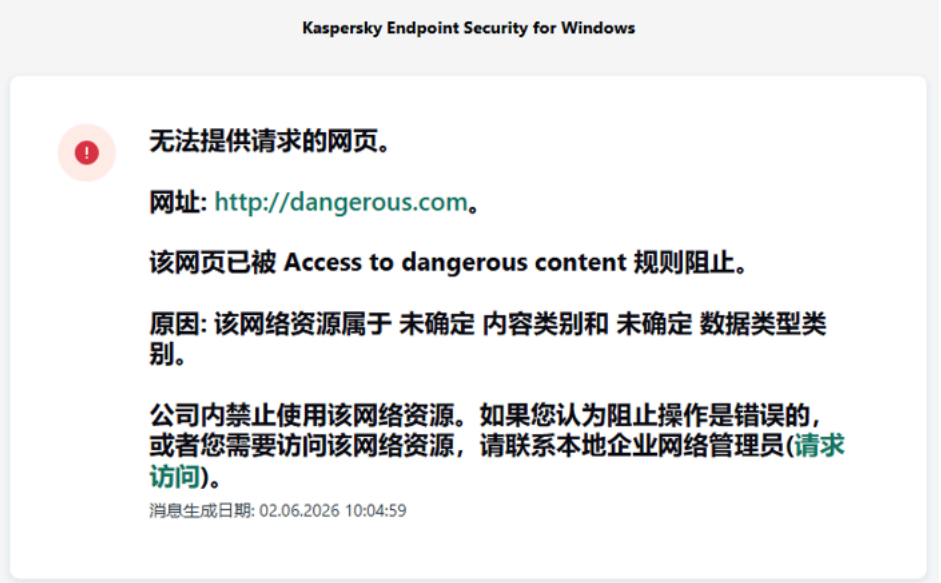
  例如，您可以限制公司内除 IT 部门以外的所有用户通过浏览器访问 Internet。

- 规则计划。

  例如，您可以限制只能在工作时间通过浏览器访问 Internet。

访问规则优先级

每条规则都有优先级。规则在列表中的位置越高，优先级越高。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。例如，Kaspersky Endpoint Security 可能将公司门户识别为社交网络。要限制对社交网络的访问并提供对公司 Web 门户的访问权限，请创建两条规则：一条针对“*社交网络*”网站类别的阻止规则和一条针对公司 Web 门户的允许规则。公司 Web 门户访问规则的优先级必须高于社交网络访问规则的优先级。



"Web 控制"消息

Web 控制组件设置

参数	描述
网络资源访问规则	包含 Web 资源访问规则的列表。每条规则都有优先级。规则在列表中的位置越高，优先级越高。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。
默认规则	*默认规则*是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**，也叫禁止的网站的拒绝列表模式。 • **拒绝除规则列表外的所有内容**，也叫允许的网站的允许列表模式。
应用规则后终止活动用户浏览器会话	如果选中该复选框，Web 控制将在应用策略之后立即终止与被阻止的 Web 资源的连接。浏览器立即停止从网页下载数据。当您刷新网页或转到另一个禁止的网页时，应用程序会显示警告。 Web 控制仅允许在 Web 浏览器中立即断开 Web 资源。对于其他应用程序，Web 控制仅限制新连接。 如果清除该复选框，Web 控制将仅限制与禁止的 Web 资源的新连接。Web 控制不会终止活动连接。

参数	描述
模板	"**警告**"。该条目字段包含一个消息模板，尝试访问不需要的网页资源触发警告消息规则时就会显示警告消息。 "**阻止消息**"。该条目字段包含某个阻止访问网页资源的规则被触发时要显示的消息的模板。 "**给管理员的消息**"。用户认为被错误地阻止了访问资源时要发送给局域网管理员的消息模板。在用户请求提供访问权限后，Kaspersky Endpoint Security 向 Kaspersky Security Center 发送一个事件： **发送给管理员的网页访问阻止消息**。事件描述包含一条给管理员的消息，其中包含替换变量。您可以使用预定义事件分类"**用户请求**"在 Kaspersky Security Center 控制台中查看这些事件。如果您的组织没有部署 Kaspersky Security Center 或者没有连接到管理服务器，应用程序将向管理员发送一条消息到指定的电子邮件地址。 提供了特殊变量来管理消息模板（例如，`%USER_NAME%`）。变量允许将单个消息模板用于不同的计算机。
记录允许页面的打开	Kaspersky Endpoint Security 会记录对所有网站（包括允许的网站）的访问数据。Kaspersky Endpoint Security 将事件发送到 Kaspersky Security Center、Kaspersky Endpoint Security 本地日志和 Windows 事件日志。要监控用户 Internet 活动，您需要配置用于保存事件的设置。 支持监控功能的浏览器：Microsoft Edge、Microsoft Internet Explorer、Google Chrome、Yandex Browser、Mozilla Firefox。用户活动监控在其他浏览器中不起作用。 在解密 HTTPS 流量时，监控用户 Internet 活动可能需要更多计算机资源。

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（例如，硬盘驱动器、相机或 Wi-Fi 模块）的访问。这样可以在连接此类设备时保护计算机免受感染，并防止数据丢失或数据泄漏。

如果设备控制被启用，应用程序转发已连接的设备信息到 Kaspersky Security Center。您可以在 Kaspersky Security Center 的"**高级**" → "**存储库**" → "**硬件**"文件夹中查看已连接设备列表。

设备访问级别

"设备控制"控制以下级别的访问权限：

- **设备类型**。例如，打印机、可移动驱动器和 CD/DVD 驱动器。
  您可以按如下方式配置设备访问权限：
  - 允许 – ✓。
  - 阻止 – ⊘。
  - 根据规则（仅对打印机和便携式设备） – 。
  - 取决于连接总线（除了 Wi-Fi） – 。
  - 阻止但带有例外（仅 Wi-Fi） – .
- **连接总线**。"*连接总线*"是用于将设备连接到计算机的接口（例如 USB 或 FireWire）。如果为设备类型选择了"**取决于连接总线**"模式，应用程序根据连接接口（例如 USB）允许或拒绝访问设备。

您可以按如下方式配置设备访问权限：

- 允许 – ✓。
- 阻止 – ⊘。

- **受信任设备**。*受信任的设备*是指在受信任设备设置中指定的用户可随时进行完全访问的设备。

  您可以根据以下数据添加受信任设备：

  - "**按 ID 添加设备**"。每个设备都有一个唯一的标识符（硬件 ID 或 HWID）。您可以使用操作系统工具在设备属性中查看 ID。设备 ID 示例：`SCSI\CDROM&VEN_NECVMWAR&PROD_VMWARE_SATA_CD00\5&354AE4D7&0&000000`。如果要添加多个特定设备，则按 ID 添加设备很方便。
  - "**按型号添加设备**"。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在设备属性中查看 ID。用于输入 VID 和 PID 的模板：`VID_1234&PID_5678`。如果在组织中使用特定型号的设备，则按型号添加设备很方便。这样，您可以添加该型号的所有设备。
  - "**按 ID 掩码添加设备**"。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。`*` 字符可替换任意一组字符。输入掩码时，Kaspersky Endpoint Security 不支持 `?` 字符。例如，`WDC_C*`。
  - "**按型号掩码列出的设备**"。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。`*` 字符可替换任意一组字符。输入掩码时，Kaspersky Endpoint Security 不支持 `?` 字符。例如，`VID_05AC&PID_*`。

"设备控制"通过使用*访问规则*来管理用户对设备的访问。"设备控制"还允许您保存设备连接/断开连接事件。要保存事件，您需要在策略中配置事件注册。

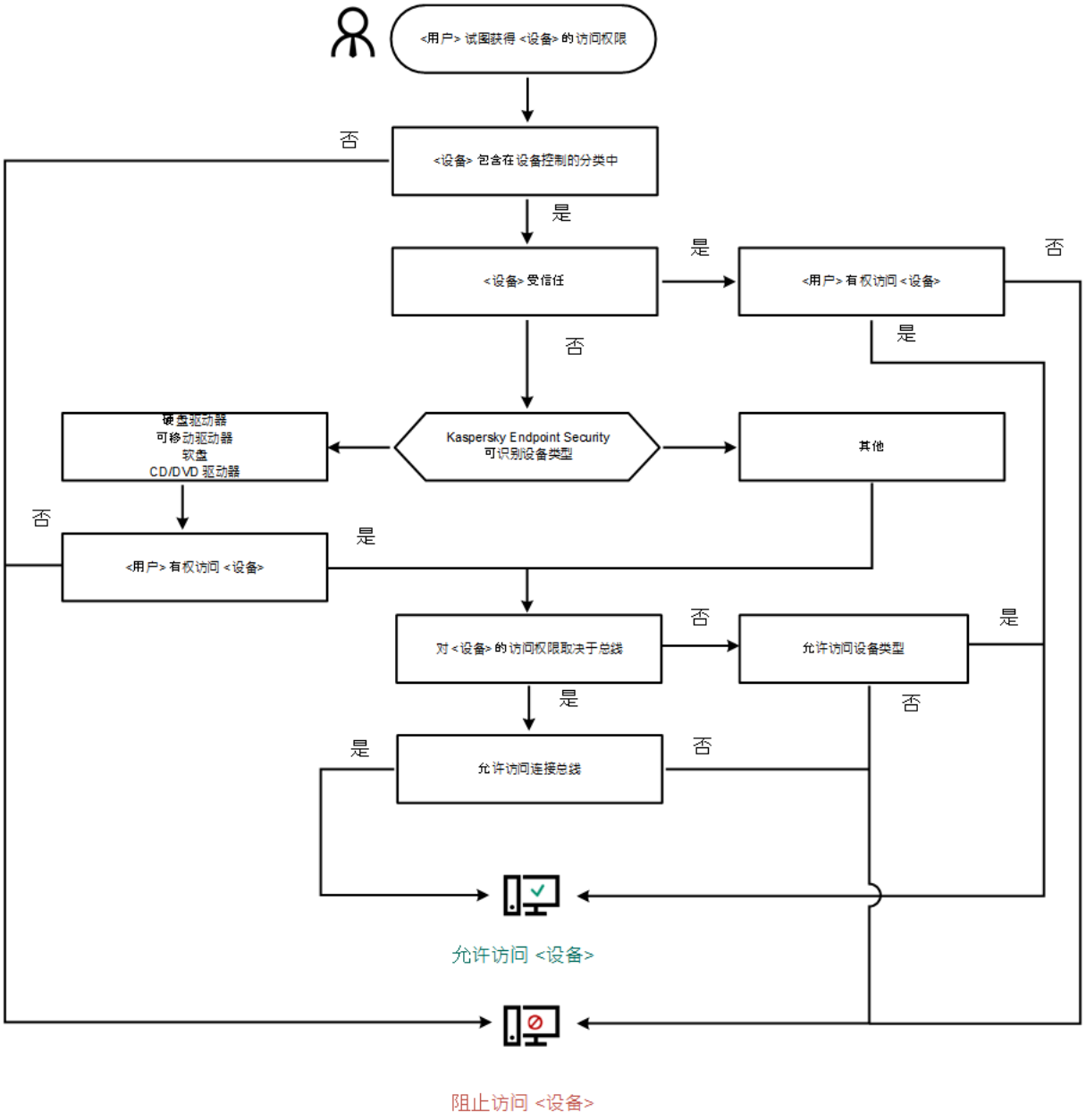
> 如果对设备的访问权限取决于连接总线（状态），Kaspersky Endpoint Security 不会保存设备连接/断开连接事件。要使 Kaspersky Endpoint Security 保存设备连接/断开连接事件，请允许访问相应的设备类型（✓状态）或将设备添加到信任列表。

当被"设备控制"阻止的设备连接到计算机时，Kaspersky Endpoint Security 将阻止访问并显示通知（请参见下图）。

"设备控制"通知

设备控制运行算法

Kaspersky Endpoint Security 在用户将设备连接到计算机之后做出是否允许访问该设备的决定（请参见下图）。



设备控制运行算法

如果已连接设备并允许访问，您可以编辑访问规则并阻止访问。在这种情况下，下次有人尝试访问该设备（例如查看文件夹树或执行读取或写入操作）时，Kaspersky Endpoint Security 会阻止访问。没有文件系统的设备仅在该设备下一次连接时被阻止。

如果已安装有 Kaspersky Endpoint Security 的计算机上的用户需要请求被错误阻止的设备的访问权限，则向该用户发送请求访问说明。

参数	描述
允许临时访问请求 *（仅在 Kaspersky Security Center 控制台可用）*	如果选中此选框，“**请求访问**”按钮将在 Kaspersky Endpoint Security 的本地界面中可用。使用此按钮，用户可以请求临时访问被阻止的设备。
设备和 Wi-Fi 网络	该表包含根据设备控制组件的分类所有可能的设备类型，包括这些设备类型各自的访问状态。
连接总线	符合“设备控制”组件分类的所有可用连接总线的列表，包括这些连接总线各自的访问状态。如果选择了“**取决于连接总线**”模式，Kaspersky Endpoint Security 根据连接总线的类型允许或拒绝访问设备。
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。
继承时合并值 *（仅在 Kaspersky Security Center 控制台可用）*	这将合并 Kaspersky Security Center 父策略和子策略中的受信任设备列表。要合并列表，子策略必须被配置为继承 Kaspersky Security Center 的父策略设置。 如果该复选框被选中，Kaspersky Security Center 父策略中的列表项目显示在子策略。这样，您可以为整个组织创建受信任设备的统一列表。 子策略中继承的列表项目无法被删除或编辑。在继承过程中合并的受信任设备列表上的项目仅在父策略中可以被删除和编辑。您可以添加、编辑或删除较低级别策略中的列表项目。 如果子策略和父策略中的列表项目匹配，这些项目被显示为父策略中的相同项目。 如果未选中该复选框，则在继承 Kaspersky Security Center 策略设置时不会合并列表项。 此功能还允许合并策略配置文件中的列表。要合并列表，请在最高优先级的配置文件中启用从较低优先级的配置文件继承设置。有关策略配置文件属性的详细信息，请参阅 Kaspersky Security Center 帮助。
反桥接	反桥接通过阻止为一台计算机同时建立多个网络连接来禁止创建网桥。这样可以保护公司网络避免未受保护和未经授权的网络上的攻击。 反桥接根据设备的优先级阻止建立多个连接。设备在列表中的位置越高，优先级越高。 如果活动连接和新连接属于同一类型（例如 Wi-Fi），则 Kaspersky Endpoint Security 会阻止活动连接并允许建立新连接。 如果活动连接和新连接属于不同类型（例如，网络适配器和 Wi-Fi），则 Kaspersky Endpoint Security 会阻止具有较低优先级的连接，允许具有较高优先级的连接。 反桥接支持以下类型的设备的操作：网络适配器、Wi-Fi 和调制解调器。
消息模板	“**阻止消息**”。当用户尝试访问阻止的设备时所显示的消息的模板。当用户尝试对被阻止使用的设备内容执行操作时，也会显示此消息。 “**给管理员的消息**”。当用户确信设备的访问权限或设备内容操作被错误地禁止时，发送给 LAN 管理员的消息的模板。在用户请求提供访问权限后，Kaspersky Endpoint Security 向 Kaspersky Security Center 发送一个事件：**发送给管理员的设备访问阻止消息**。事件描述包含一条给管理员的消息，其中包含替换变量。您可以使用预定义事件分类**用户请求**在 Kaspersky Security Center 控制台中查看这些事件。如果您的组织没有部署 Kaspersky Security Center 或者没有连接到管理服务器，应用程序将向管理员发送一条消息到指定的电子邮件地址。

应用程序控制

“应用程序控制”管理用户计算机上的应用程序启动。这允许您在使用应用程序时实施公司安全策略。“应用程序控制”还通过限制对应用程序的访问来降低计算机感染的风险。

配置“应用程序控制”包括以下步骤：

1. 创建应用程序类别。

   管理员创建管理员想要管理的应用程序类别。应用程序类别适用于公司网络中的所有计算机，与管理组无关。要创建类别，您可以使用以下条件：KL 类别（例如，*浏览器*或其他类别）、文件哈希、应用程序供应商和其他条件。

2. 创建应用程序控制规则。

   管理员在管理组的策略中创建应用程序控制规则。该规则包括应用程序类别和这些类别中的应用程序的启动状态：已阻止或已允许。管理员可以创建许多规则。一个应用程序可能符合多个规则的条件。阻止规则的优先级高于允许规则的优先级。Kaspersky Endpoint Security 每次启动时都会检查应用程序是否符合规则。Kaspersky Endpoint Security 按顺序将应用程序与所有应用程序控制规则进行匹配。

3. 选择应用程序控制模式。

   管理员选择对未包含在以下任何规则中的应用程序的处理模式（应用程序拒绝列表或允许列表）。

当用户尝试启动已禁止的应用程序时，Kaspersky Endpoint Security 将阻止该应用程序启动并显示通知（请参见下图）。

系统提供了一种*测试模式*来检查“应用程序控制”的配置。在此模式下，Kaspersky Endpoint Security 执行以下操作：

- 允许启动应用程序，包括已禁止的应用程序。
- 显示有关已禁止的应用程序启动的通知，并将信息添加到用户计算机上的报告中。
- 将有关已禁止的应用程序启动的数据发送到 Kaspersky Security Center。

“应用程序控制”通知

“应用程序控制”运行模式

“应用程序控制”组件在两种模式下运行：

- “**拒绝列表**”。在此模式下，“应用程序控制”允许用户启动除了应用程序控制规则中禁止的应用程序以外的所有应用程序。

  默认情况下启用“应用程序控制”的这一模式。

- “**允许列表**”。在此模式下，“应用程序控制”阻止用户启动除了应用程序控制规则中允许和未禁止的应用程序以外的任何应用程序。

  如果完整配置了“应用程序控制”的允许规则，则该组件将阻止启动所有未经局域网管理员验证的新应用程序，同时允许运行用户在工作中依赖的操作系统和受信任应用程序。

  您可以阅读有关在允许列表模式下配置应用程序控制规则的建议。

可以使用 Kaspersky Endpoint Security 本地界面和 Kaspersky Security Center 将“应用程序控制”配置为在这些模式下运行。

但是，Kaspersky Security Center 提供了在 Kaspersky Endpoint Security 本地界面中不可用的工具，例如以下任务所需的工具：

- 创建应用程序类别。

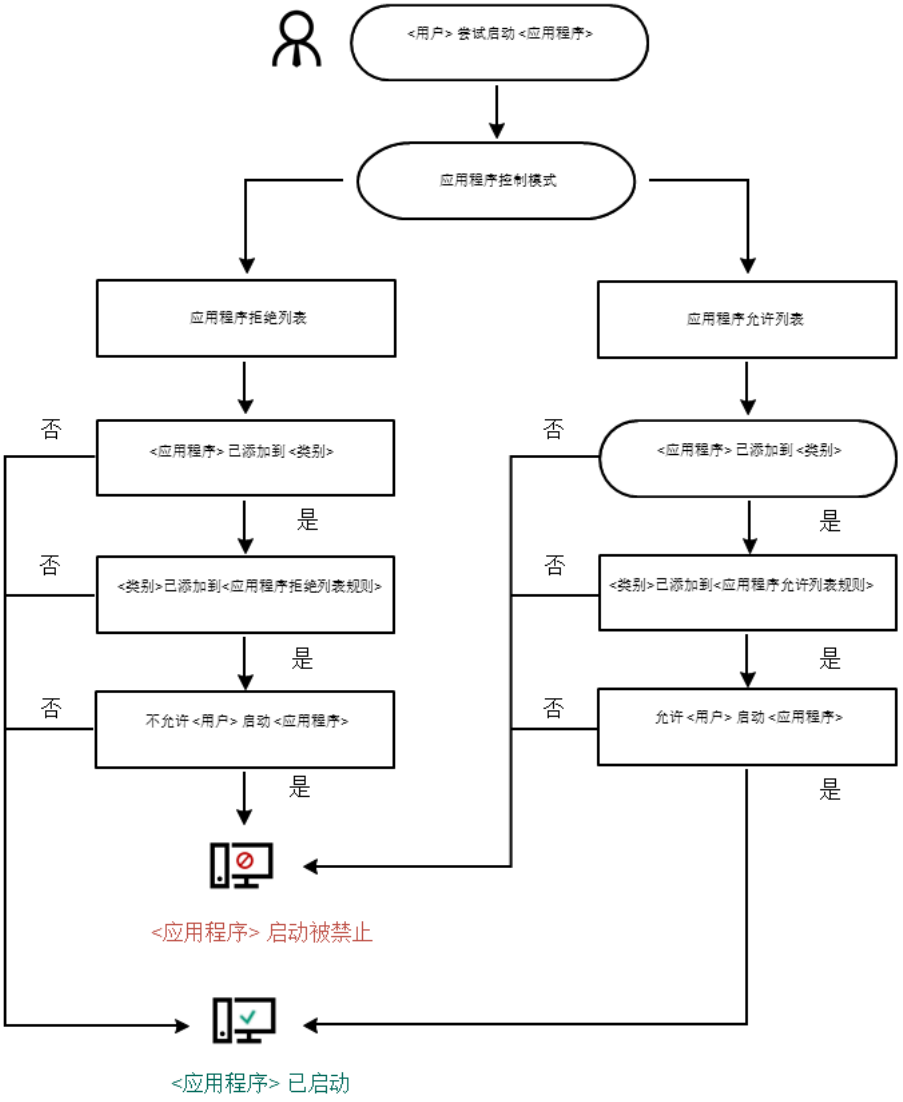
  在 Kaspersky Security Center 管理控制台中创建的应用程序控制规则基于您的自定义应用程序类别，而不是基于像 Kaspersky Endpoint Security 本地界面中的包含和排除条件。

- 接收有关安装在公司局域网计算机上的应用程序的信息。

因此，建议使用 Kaspersky Security Center 配置“应用程序控制”组件的运行。

“应用程序控制”运行算法

Kaspersky Endpoint Security 使用算法来决定是否启动应用程序（请参见下图）。



“应用程序控制”运行算法

参数	描述
启动被规则阻止的应用程序时的操作	"**应用规则**"。Kaspersky Endpoint Security 根据所选模式管理应用程序的启动。 "**测试规则**"。Kaspersky Endpoint Security 将允许启动在当前应用程序控制模式中阻止的应用程序，但是在报告中记录应用程序启动信息。
应用程序启动控制模式	您可以选择以下选项之一： • "**拒绝列表**"。如果选择该选项，应用程序控制将允许所有用户启动所有应用程序，符合应用程序控制阻止规则的应用程序除外。 • "**允许列表**"。如果选择该选项，应用程序控制将阻止所有用户启动任何应用程序，符合应用程序控制允许规则的应用程序除外。 选择**允许列表**模式后，会自动创建两个应用程序控制规则： • "**黄金镜像**"。 • "**受信任更新程序**"。 您不能编辑自动创建的规则的设置，也不能删除这些规则。您可以启用或禁用这些规则。
监控 DLL 模块的加载	如果选定该复选框，Kaspersky Endpoint Security 将在用户启动应用程序时控制 DLL 模块的加载。有关 DLL 模块和加载该 DLL 模块的应用程序的信息将记录在该报告中。 当启用对加载 DLL 模块和驱动程序的控制时，请确保在"应用程序控制"设置中已启用以下规则之一：默认"**黄金镜像**"规则或其他包含"**黄金镜像\受信任证书**"KL 类别的规则，并确保在启动 Kaspersky Endpoint Security 之前加载受信任的 DLL 模块和驱动程序。如果在禁用"**黄金镜像**"规则时启用对加载 DLL 模块和驱动程序的控制，可能导致操作系统不稳定。 Kaspersky Endpoint Security 仅监控自选中该复选框后加载的 DLL 模块和驱动程序。选择复选框后，建议重启计算机以确保应用程序监控所有 DLL 模块和驱动程序，包括那些在 Kaspersky Endpoint Security 启动之前加载的。
使用严格的数字签名验证	您可以选择证书作为应用程序控制规则的触发条件。 如果选中此复选框，Kaspersky Endpoint Security 将规则应用于仅使用以下证书签名的应用程序：受信任的系统证书存储。使用此类证书签名的应用程序也被视为受到保护组件（例如"*恶意软件扫描*"任务）的信任。但是，如果您在应用程序控制规则中指定来自不同存储的证书，Kaspersky Endpoint Security 将不会应用此类规则。 如果清除该复选框， Kaspersky Endpoint Security 会将规则应用于由 Windows 受信任根证书存储区的证书签名的应用程序。此类应用程序不属于受信任区域的一部分。保护组件监控此类应用程序的活动。
关于应用程序阻止的消息模板	"**阻止消息**"。当触发了某个阻止应用程序启动的应用程序控制规则时所显示的消息模板。 "**给管理员的消息**"。当用户相信某个应用程序被错误地阻止时可以发送给公司局域网管理员的消息模板。在用户请求提供访问权限后，Kaspersky Endpoint Security 向 Kaspersky Security Center 发送一个事件： **发送给管理员的应用程序启动阻止消息**。事件描述包含一条给管理员的消息，其中包含替换变量。您可以使用预定义事件分类"**用户请求**"在 Kaspersky Security Center 控制台中查看这些事件。如果您的组织没有部署 Kaspersky Security Center 或者没有连接到管理服务器，应用程序将向管理员发送一条消息到指定的电子邮件地址。

自适应异常控制

如果 Kaspersky Endpoint Security 安装在运行 Windows for Workstations 的计算机上，则该组件可用。如果 Kaspersky Endpoint Security 安装在运行 Windows for Servers 的计算机上，则该组件不可用。

自适应异常控制组件会监视并阻止不是公司网络内计算机典型操作的相关操作。自适应异常控制使用一组规则来跟踪非典型行为（例如，*从 office 应用程序启动 Microsoft PowerShell* 规则）。规则由 Kaspersky 专家根据恶意活动的典型情景创建。您可以配置"自适应异常控制"处理每条规则的方式，例如，允许执行使某些工作流任务自动化的 PowerShell 脚本。Kaspersky Endpoint Security 会同时更新规则集和应用程序数据库。规则集的更新必须手动确认。

“自适应异常控制”设置

配置“自适应异常控制”包括以下步骤：

1. 训练“自适应异常控制”。

   启用“自适应异常控制”后，其规则在*训练模式*下工作。在训练期间，“自适应异常控制”监控规则触发并将触发事件发送到 Kaspersky Security Center。每条规则都有自己的训练模式持续时间。训练模式持续时间由 Kaspersky 专家设置。通常，训练模式保持活动两周。

   如果在训练期间某条规则完全未触发，“自适应异常控制”会将与此规则关联的操作视为非典型操作。Kaspersky Endpoint Security 将阻止与该规则相关的所有操作。

   如果在训练期间触发了某条规则，Kaspersky Endpoint Security 会将事件记录在规则触发报告和“**智能培训状态下的规则触发器**”存储库中。

2. 分析规则触发报告。

   管理员分析规则触发报告或“**智能培训状态下的规则触发器**”存储库的内容。然后管理员可以选择在触发规则时“自适应异常控制”的行为：阻止或允许。管理员还可以继续监控规则的工作方式并延长训练模式的持续时间。如果管理员未采取任何操作，应用程序也将继续在训练模式下工作。训练模式期限重新开始。

“自适应异常控制”通过以下通道实时配置：

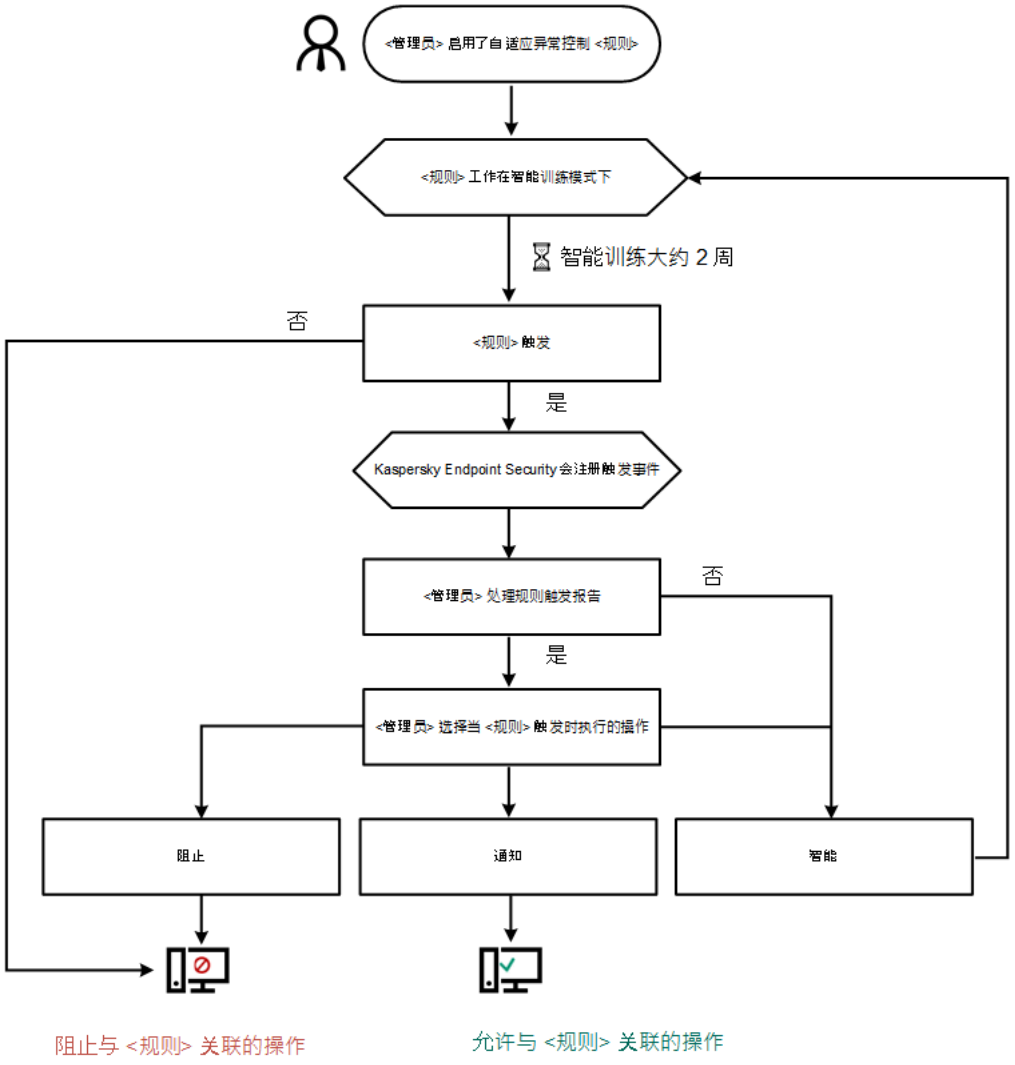
- “自适应异常控制”自动开始阻止与从未在训练模式中触发的规则相关联的操作。
- Kaspersky Endpoint Security 添加新规则或删除过时规则。
- 管理员在查看规则触发报告和“**智能培训状态下的规则触发器**”存储库的内容后配置“自适应异常控制”的操作。我们建议检查有关规则触发的报告以及“**智能培训状态下的规则触发器**”存储的内容。

当恶意应用程序尝试执行操作时，Kaspersky Endpoint Security 将阻止该操作并显示通知（请参见下图）。

“自适应异常控制”通知

“自适应异常控制”操作算法

Kaspersky Endpoint Security 根据以下算法决定是允许还是阻止与某条规则关联的操作（请参见下图）。



“自适应异常控制”操作算法

自适应异常控制组件设置

参数	描述
有关自适应异常控制规则状态的报告 *（仅在 Kaspersky Security Center 控制台可用）*	该报告包含有关自适应异常控制检测规则状态的信息（例如，*已禁用*或*阻止*）。该报告针对所有管理组生成。
有关触发的自适应异常控制规则的报告 *（仅在 Kaspersky Security Center 控制台可用）*	该报告包含使用“自适应异常控制”检测到的非典型操作的相关信息。该报告针对所有管理组生成。

参数	描述
规则	自适应异常控制规则表。规则由 Kaspersky 专家根据恶意活动的典型情景创建。
模板	"**阻止消息**"。当阻止非典型操作的自适应异常控制规则触发时，显示给用户的消息的模板。 "**给管理员的消息**"。当用户认为阻止是错误的时可以发送给本地公司网络管理员的消息的模板。在用户请求提供访问权限后，Kaspersky Endpoint Security 向 Kaspersky Security Center 发送一个事件： **发送给管理员的应用程序活动阻止消息**。事件描述包含一条给管理员的消息，其中包含替换变量。您可以使用预定义事件分类"**用户请求**"在 Kaspersky Security Center 控制台中查看这些事件。如果您的组织没有部署 Kaspersky Security Center 或者没有连接到管理服务器，应用程序将向管理员发送一条消息到指定的电子邮件地址。

系统完整性监控

如果 Kaspersky Endpoint Security 安装在运行 Windows for Servers 的计算机上，则该组件可用。如果 Kaspersky Endpoint Security 安装在运行 Windows for Workstations 的计算机上，则该组件不可用。

从 12.6 版本开始，Kaspersky Endpoint Security for Windows 包含系统完整性监控组件，而不是文件完整性监控组件。系统完整性监控组件包括文件完整性监控的所有功能，另外还允许监控注册表更改和外部设备的连接。

系统完整性监控组件监控操作系统中可能预示计算机安全漏洞的变化。当检测到此类变化时，Kaspersky Endpoint Security 会生成相应的事件并向管理员发出警报。系统完整性监控可以实时运行，也可以根据需要执行系统完整性检查。

实时系统完整性监控

在实时模式下，系统完整性监控跟踪组件范围（*监控范围*）中包含的对象中的更改。系统完整性监控还允许实时阻止对此类对象的未经授权的访问。

按需系统完整性检查

按需系统完整性检查是一项您可以手动或按计划运行的任务。要运行"*系统完整性检查*"任务，您必须配置组件的范围（*监控范围*）并创建基线。*基线*是系统中对象的记录状态，应用程序在与当前状态进行比较时以其作为参考。

系统完整性监控设置

参数	描述
阻止规则的操作模式	• "**阻止**"。在此模式下，系统完整性监控会阻止对监控范围内的文件和注册表项的操作，并生成相应的事件。 • "**通知**"。在此模式下，系统完整性监控会允许对监控范围内的文件和注册表项的操作，并生成相应的事件。
实时系统完整性监控	在实时模式下，系统完整性监控跟踪组件范围（*监控范围*）中包含的对象中的更改。系统完整性监控还允许实时阻止对此类对象的未经授权的访问。
监控设备	系统完整性监控监控外部设备的连接和断开连接。
监控文件和注册表	系统完整性监控监控文件、文件夹和注册表的更改。
系统完整性检查	按需系统完整性检查是一项您可以手动或按计划运行的任务。要运行"*系统完整性检查*"任务，您必须配置组件的范围（*监控范围*）并创建基线。*基线*是系统中对象的记录状态，应用程序在与当前状态进行比较时以其作为参考。

Endpoint Sensor

Kaspersky Endpoint Security 11.4.0 不包含 Endpoint Sensor。

您可以在 Kaspersky Security Center Web Console 和 Kaspersky Security Center 管理控制台中管理 Endpoint Sensor。无法在 Kaspersky Security Center 云控制台中管理 Endpoint Sensor。

Endpoint Sensor 设计用于与 Kaspersky Anti Targeted Attack Platform 进行交互。*Kaspersky Anti Targeted Attack Platform* 是旨在及时检测复杂威胁（如针对性攻击、高级持久性威胁 (APT)、零日攻击等）的解决方案。Kaspersky Anti Targeted Attack Platform 包括三个功能单元：

- Kaspersky Anti Targeted Attack Platform（*KATA*）
- Kaspersky Endpoint Detection and Response（*EDR（KATA）*）
- Network Detection and Response（*NDR（KATA）*）

您可以购买所有功能单元，也可以单独购买单个功能单元。有关解决方案的详细信息，请参阅 Kaspersky Anti Targeted Attack Platform 帮助。

管理 Endpoint Sensor 具有以下限制：

- 如果计算机上安装了 Kaspersky Endpoint Security 版本 11.0.0 至 11.3.0，则可以使用策略配置 Endpoint Sensor 设置。有关使用策略配置 Endpoint Sensor 设置的更多信息，请参阅适用于 Kaspersky Endpoint Security 早期版本的帮助文章。
- 如果计算机上安装了 Kaspersky Endpoint Security 版本 11.4.0 及更高版本，则无法使用策略配置 Endpoint Sensor 设置。

Endpoint Sensor 安装在客户端计算机上。在这些计算机上，该组件持续监控进程、活动网络连接和被修改的文件。Endpoint Sensor 将信息中继给 KATA 服务器。

该组件的功能在以下操作系统下可用：

- Windows 7 Service Pack 1 Home / Professional / Enterprise；
- Windows 8.1.1 Professional / Enterprise；
- Windows 10 RS3 Home / Professional / Education / Enterprise;
- Windows 10 RS4 Home / Professional / Education / Enterprise;
- Windows 10 RS5 Home / Professional / Education / Enterprise;
- Windows 10 RS6 Home / Professional / Education / Enterprise;
- Windows Server 2008 R2 Foundation / Standard / Enterprise (64-bit);
- Windows Server 2012 Foundation / Standard / Enterprise（64 位）；

- Windows Server 2012 R2 Foundation / Standard / Enterprise (64-bit);
- Windows Server 2016 Essentials / Standard（64 位）。

有关 KATA 操作的详细信息，请参阅 Kaspersky Anti Targeted Attack Platform 帮助。

Sandbox

Kaspersky Endpoint Security for Windows 包含一个用于与 Kaspersky Sandbox 解决方案集成的内置代理。*Sandbox* 组件检测并自动阻止计算机上的高级威胁。Sandbox 分析对象行为，以检测恶意活动和针对组织 IT 基础设施的攻击的活动特征。Sandbox 使用部署的 Microsoft Windows 操作系统虚拟映像（Sandbox 服务器）分析和扫描特殊服务器上的对象。有关解决方案的详细信息，请参阅 Kaspersky Sandbox 帮助和 Kaspersky Anti Targeted Attack Platform 帮助。

从 12.7 版本开始，Kaspersky Endpoint Security for Windows 支持作为 Kaspersky Anti Targeted Attack Platform 解决方案一部分的 Sandbox 组件。与 Kaspersky Sandbox 解决方案相比，KATA Sandbox 组件允许不仅自动扫描文件，还可以从文件上下文菜单手动扫描文件。

KATA Sandbox 需要部署 Kaspersky Anti Targeted Attack Platform 7.0 或更高版本。

该组件只能使用 Kaspersky Security Center Web Console 进行管理。您无法使用管理控制台（MMC）管理此组件。

Sandbox 组件设置

参数	描述
整合模式	"**Kaspersky Sandbox**"。与 Kaspersky Sandbox 解决方案集成。应用程序仅在自动模式下发送文件以在 Kaspersky Sandbox 中进行扫描。 "**KATA Sandbox**"。与 Kaspersky Anti Targeted Attack Platform 解决方案的 Sandbox 组件集成。您可以选择扫描的文件提交模式： • "**手动**"。用户从上下文菜单手动提交文件进行扫描（**发送到 Sandbox**）。 • "**自动**"。应用程序自动检测对象并将其提交到 Sandbox 进行扫描。 • "**组合的**"。
服务器连接设置	"**超时(豪秒)**"。Sandbox 服务器（对于 Kaspersky Sandbox）或 Central Node 服务器（对于 KATA）的连接超时。配置的超时时间过后，Kaspersky Endpoint Security 将向下一台服务器发送请求。如果连接速度低或连接不稳定，您可以增加服务器的连接超时。建议的请求超时是 0.5 秒或更少。 "**请求队列**"。请求队列文件夹的大小。在发送多个对象以在 Sandbox 中进行扫描时，Kaspersky Endpoint Security 会创建一个请求队列。默认情况下，请求队列文件夹的大小限制为 100 MB。达到最大大小后，Sandbox 停止向队列添加新请求，并将相应的事件发送到 Kaspersky Security Center。您可以根据您的服务器配置来配置请求队列文件夹的大小。 "**服务器 TLS 证书**"。要配置与 Sandbox 服务器（对于 Kaspersky Sandbox）或 Central Node 服务器（对于 KATA）的受信任连接，您必须准备 TLS 证书。您必须使用策略将证书添加到计算机。您还需要将证书添加到 Sandbox 服务器（对于 Kaspersky Sandbox）或 Central Node 服务器（对于 KATA）。 **使用双向身份验证** （仅适用于 KATA Sandbox）。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。
连接到 Sandbox 服务器	**Kaspersky Sandbox**。Sandbox 服务器连接设置。服务器使用部署的 Microsoft Windows 操作系统虚拟映像来运行需要扫描的对象。您可以输入 IP 地址（IPv4 或 IPv6）或完全限定的域名。 **KATA Sandbox**。Central Node 服务器连接设置。Central Node 选择最佳扫描设置并平衡 Sandbox 服务器之间的负载。

参数	描述
检测到威胁后的操作	"**将副本移动到隔离区，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 运行*关键区域扫描*任务。默认情况下，Kaspersky Endpoint Security 会扫描内核内存、运行进程和磁盘的引导扇区。 "**创建 IOC 扫描任务**"。如果选择此选项，Kaspersky Endpoint Security 将自动创建 *IOC 扫描*（*自主 IOC 扫描任务*）。对于此任务，您可以配置运行模式、扫描范围以及检测到 IOC 时执行的操作（*将副本移动到隔离区*，*删除对象* 或 *运行关键区域扫描*）。要修改 *IOC 扫描*任务的其他设置，请转到任务设置。
IOC 扫描范围	"**关键文件区域**"。如果选择此选项，Kaspersky Endpoint Security 仅在计算机的关键文件区域（内核内存和引导扇区）执行 IOC 扫描。 "**计算机系统驱动器上的文件区域**"。如果选择此选项，Kaspersky Endpoint Security 在计算机的系统驱动器上执行 IOC 扫描。
运行 IOC 扫描任务	"**手动**"。您可以在方便时手动启动"*IOC 扫描*"任务的运行模式。 "**自动**"。在此运行模式下，Kaspersky Endpoint Security 会在检测到威胁后自动运行 *IOC 扫描* 任务。 "**仅在计算机空闲时运行**"。Kaspersky Endpoint Security 在屏幕保护程序处于活动状态或屏幕被锁定时运行 *IOC 扫描*任务。如果用户解锁计算机，Kaspersky Endpoint Security 将暂停任务。这意味着任务可能需要几天才能完成。

Managed Detection and Response

Kaspersky Endpoint Security for Windows 支持与 Managed Detection and Response 解决方案集成。*Kaspersky Managed Detection and Response (MDR)* 解决方案自动检测和分析您基础架构中的安全事故。为此，MDR 使用从端点和机器学习接收的遥测数据。MDR 发送事故数据到 Kaspersky 专家。然后专家便可以处理事故，例如，添加新条目到反病毒数据库。或者，专家可以发布处理事件的建议，例如，建议将计算机从网络隔离。对于该解决方案如何工作的详情，请参考 Kaspersky Managed Detection and Response 帮助。

Managed Detection and Response 设置

参数	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 文件存在于 MDR 配置文件的 ZIP 存档中。您可以在 Kaspersky Managed Detection and Response 控制台获取 ZIP 存档。对于 BLOB 文件的详情，请参考 Kaspersky Managed Detection and Response 帮助。

Endpoint Detection and Response

Kaspersky Endpoint Security for Windows 包含 Kaspersky Endpoint Detection and Response Optimum 解决方案（也叫"EDR Optimum"）的内置代理。从 11.8.0 开始，Kaspersky Endpoint Security for Windows 包含 Kaspersky Endpoint Detection and Response Expert 解决方案（也叫"EDR Expert"）的内置代理。*Kaspersky Endpoint Detection and Response* 是一种保护企业 IT 基础架构免受高级网络威胁的一系列解决方案。该解决方案的功能将自动检测威胁与应对这些威胁的能力结合起来，以抵御高级攻击，包括新的漏洞利用、勒索软件、无文件攻击以及使用合法系统工具的方法。EDR Expert 比 EDR Optimum 提供更多的威胁监控和响应功能。有关解决方案的更多信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助和 Kaspersky Endpoint Detection and Response Expert 帮助。

Kaspersky Endpoint Detection and Response 查看和分析威胁发展，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 在单独的窗口显示警报详情。*警报*是企业 IT 基础设施中发生的事件，应用程序将其识别为异常或可疑，并可能对企业 IT 基础设施构成安全威胁。*警报详情*是一种工具，用于查看所收集的有关检测到的威胁的全部信息。警报详情包括，例如，出现在计算机的文件历史。有关管理警报详情的更多信息，请参阅 Kaspersky Endpoint Detection and Response Optimum 帮助和 Kaspersky Endpoint Detection and Response Expert 帮助。

您可以在 Web Console 和云控制台中配置 Endpoint Detection and Response Optimum 组件。Endpoint Detection and Response Expert (cloud) 组件设置仅在云控制台中可用。

参数	描述
启用高级系统活动日志记录	扩展遥测提高了 IOC 检测的准确性，但会占用更多的计算机资源。我们建议在计算机上启用扩展遥测以进行回顾性 IOC 扫描。*回顾性 IOC 扫描*是 *IOC 扫描* 任务的一种模式，在该模式下，Kaspersky Endpoint Security 使用特定时间段的数据扫描入侵指标。此模式旨在通过受保护计算机的遥测数据（例如网络活动、进程、文件和其他遥测数据）来搜索入侵指标。 如果禁用扩展遥测，Kaspersky Endpoint Security 可能会轮换有关检测到的入侵指标的信息。
网络隔离	为响应检测到的威胁，自动将计算机与网络隔离。 打开网络隔离后，应用程序将断开所有活动连接并阻止计算机上的所有新 TCP/IP 连接。应用程序仅保留以下连接处于活动状态： • 网络隔离排除中列出的连接。 • 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。默认情况下，Kaspersky Endpoint Security 在隔离开始 5 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。当网络隔离打开时，符合规则的网络连接不会在计算机上被阻止。 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，排除项包括网络配置文件，其中包含确保具有 DNS/DHCP 服务器和 DNS/DHCP 客户端角色的设备不间断运行的规则。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 控制台的"计算机属性"中或警报详情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。
执行或打开禁止的对象时的操作	"**阻止并添加到事件日志**"。在此模式下，应用程序将阻止执行符合防护规则标准的对象或打开这样的文档。应用程序还将尝试执行对象或打开文档的事件发布到 Windows 事件日志和 Kaspersky Security Center 事件日志。 "**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对象或打开这样的文档的事件到 Windows 事件日志和 Kaspersky Security Center，但不会阻止尝试运行对象或打开文档。默认情况下已选择此模式。
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，以识别恶意活动并决定其信誉。这些文件上的数据随后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。 Cloud Sandbox 技术是永久启用的，可供所有卡巴斯基安全网络用户使用，无论他们使用的授权许可类型如何。 如果选中此复选框，Kaspersky Endpoint Security 将在主应用程序窗口的"**威胁检测技术**"下启用使用 Cloud Sandbox 检测到的威胁的计数器。Kaspersky Endpoint Security 还将在应用程序事件和 Kaspersky Security Center 控制台的*威胁报告*中指示 Cloud Sandbox 威胁检测技术。

Endpoint Detection and Response Expert（本地部署）

Endpoint Detection and Response Expert (on-premises)

Kaspersky Endpoint Security for Windows 支持与 Kaspersky Endpoint Detection and Response Expert (on-premises) 解决方案集成。*Kaspersky Endpoint Detection and Response Expert (on-premises)* 是一款企业网络安全解决方案，其中包括卡巴斯基应用程序，可帮助组织防御大多数类型的网络风险并涵盖最重要的威胁传播场景。EDR Expert (on-premises) 组件部署在 Open Single Management Platform (OSMP) 上。该平台可在单一界面中运行跨平台方案，并允许将卡巴斯基应用程序与第三方应用程序集成到全面的安全系统中。

解决方案的核心要素之一是 *SIEM*。SIEM 跟踪来自所有组件的事件，并使用供应商和用户定义的规则将这些事件相互关联起来。EDR Expert (on-premises) 会查看从企业基础设施接收的日志和遥测数据，以自动检测攻击，并允许使用统一的调查图来调查事件，该调查图结合了 EDR Expert (on-premises) 中采集的所有事件，包括来自卡巴斯基应用程序和第三方信息安全产品的事件。

对于高级事件的响应，EDR Expert (on-premises) 使用预设方案和用户自定义方案。您还可以使用来自第三方应用程序的响应操作以及涉及多个应用程序的响应方案。

Endpoint Detection and Response（KATA）

Kaspersky Endpoint Security for Windows 支持作为 Kaspersky Anti Targeted Attack Platform (EDR (KATA)) 解决方案的一部分使用 Kaspersky Endpoint Detection and Response 组件。*Kaspersky Anti Targeted Attack Platform* 是旨在及时检测复杂威胁（如针对性攻击、高级持久性威胁 (APT)、零日攻击等）的解决方案。Kaspersky Anti Targeted Attack Platform 包括三个功能单元：

- Kaspersky Anti Targeted Attack Platform（*KATA*）
- Kaspersky Endpoint Detection and Response（*EDR（KATA）*）
- Network Detection and Response（*NDR（KATA）*）

您可以购买所有功能单元，也可以单独购买单个功能单元。有关解决方案的详细信息，请参阅 Kaspersky Anti Targeted Attack Platform 帮助。

Kaspersky Endpoint Security 安装在公司 IT 基础设施的各个计算机上，并持续监视流程、开放式网络连接和正在修改的文件。有关计算机上事件的信息（遥测数据）被发送到 Kaspersky Anti Targeted Attack Platform 服务器。此种情况下，Kaspersky Endpoint Security 也将应用程序发现的威胁信息和威胁处理结果信息发送到 Kaspersky Anti Targeted Attack Platform 服务器。

EDR (KATA) 和 NDR (KATA) 集成在 Kaspersky Security Center 控制台上配置。然后使用 Kaspersky Anti Targeted Attack Platform 控制台管理内置代理，包括运行任务、管理隔离对象、查看报告和其他操作。

参数	描述
连接到遥测采集服务器	*遥测采集服务器* 是 SIEM 解决方案的一部分，用于收集、规范化、关联、分析和存储有关计算机上发生的事件的信息。 配置以下内容以连接到遥测采集服务器（KUMA）： • "**超时(秒)**"。最大服务器响应超时。当超时用完时，Kaspersky Endpoint Security 会尝试连接到不同的服务器。 • "**服务器证书**"。用于与服务器建立受信任连接的 TLS 证书。您可以在 Open Single Management Platform 上获取 TLS 证书（请参阅 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助中的说明）。 • "**使用双向身份验证**"。在 Kaspersky Endpoint Security 和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 Open Single Management Platform 上获取加密容器（请参阅 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助中的说明）。配置服务器设置后，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。
地址和**端口**（遥测采集服务器）	连接遥测采集服务器的设置。您可以输入 IP 地址（IPv4 或 IPv6）。 您可以添加多个遥测采集服务器地址。Kaspersky Endpoint Security 尝试使用第一个 IP 地址连接到服务器。如果连接建立失败，Kaspersky Endpoint Security 将尝试使用列表中的第二个 IP 地址进行连接，依此类推。
将遥测发送到遥测采集服务器	此功能使您可以完全关闭向 KATA 服务器发送遥测数据。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。 • "**仅发送带有 IOA 的遥测**"。这允许优化遥测并仅发送带有 IOA 的遥测。*攻击指标 (IOA)* 是一条包含系统中可能表明有针对性攻击的可疑行为描述的规则。应用程序将系统中正在进行的行为与这些规则进行比较，并记录表明有针对性攻击的事件。应用程序使用*流式扫描*技术，可以实时跟踪此类事件。 • "**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。默认设置是 30 秒。 • "**限制每次传输的事件数据包数量**"。当缓冲区充满事件时，应用程序会与服务器同步。默认设置是 1024 个事件。此功能允许在与服务器同步之前禁用事件缓冲。
启用请求限制	该功能有助于优化服务器上的负载。如果启用此功能，应用程序将限制事件传输。如果事件数量超过配置的限制，Kaspersky Endpoint Security 将停止发送事件。 配置遥测设置： • "**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。默认设置是每小时 3000 个事件。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。默认设置为 15%。
发送同步请求到服务器的间隔(分钟)	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。
连接到响应服务器	*响应服务器* 是一个用于接收和扫描数据、研究对象行为和发布此类研究结果的服务器。 为响应服务器连接配置以下内容： • "**超时(秒)**"。最大服务器响应超时。当超时用完时，Kaspersky Endpoint Security 会尝试连接到不同的服务器。 • "**服务器证书**"。用于与服务器建立受信任连接的 TLS 证书。您可以在 Open Single Management Platform 上获取 TLS 证书（请参阅 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助中的说明）。 • "**使用双向身份验证**"。在 Kaspersky Endpoint Security 和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 Open Single Management Platform 上获取加密容器（请参阅 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助中的说明）。配置服务器设置后，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。
地址和**端口**（响应服务器）	连接到响应服务器的设置。您可以输入 IP 地址（IPv4 或 IPv6）。 您可以添加多个遥测采集服务器地址。Kaspersky Endpoint Security 尝试使用第一个 IP 地址连接到服务器。如果连接建立失败，Kaspersky Endpoint Security 将尝试使用列表中的第二个 IP 地址进行连接，依此类推。

参数	描述
发送同步请求到服务器的间隔(分钟)	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	为 Central Node 服务器连接配置以下内容： • "**超时(秒)**"。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。
地址和**端口**（KATA 服务器）	连接到 Kaspersky Anti Targeted Attack Platform 服务器的设置。输入要连接的 Central Node 服务器的 IP 地址（IPv4 或 IPv6）和端口。 您可以添加多个 Central Node 服务器地址。Kaspersky Endpoint Security 尝试使用第一个 IP 地址连接到服务器。如果连接建立失败，Kaspersky Endpoint Security 将尝试使用列表中的第二个 IP 地址进行连接，依此类推。
发送遥测到 KATA	此功能使您可以完全关闭向 KATA 服务器发送遥测数据。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。 配置遥测设置： • "**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。默认设置是 30 秒。 • "**事件包的最大数量**"。当缓冲区充满事件时，应用程序会与服务器同步。默认设置是 1024 个事件。
启用请求限制	该功能有助于优化服务器上的负载。如果启用此功能，应用程序将限制事件传输。如果事件数量超过配置的限制，Kaspersky Endpoint Security 将停止发送事件。 配置遥测设置： • "**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。默认设置是每小时 3000 个事件。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。默认设置为 15%。

Network Detection and Response（KATA）

Kaspersky Endpoint Security for Windows 支持作为 Kaspersky Anti Targeted Attack Platform (EDR (KATA)) 解决方案的一部分使用 Kaspersky Network Detection and Response 组件。*Kaspersky Anti Targeted Attack Platform* 是旨在及时检测复杂威胁（如针对性攻击、高级持久性威胁 (APT)、零日攻击等）的解决方案。Kaspersky Anti Targeted Attack Platform 包括三个功能单元：

- Kaspersky Anti Targeted Attack Platform（*KATA*）
- Kaspersky Endpoint Detection and Response（*EDR（KATA）*）
- Network Detection and Response（*NDR（KATA）*）

您可以购买所有功能单元，也可以单独购买单个功能单元。有关解决方案的详细信息，请参阅 Kaspersky Anti Targeted Attack Platform 帮助。

Kaspersky Endpoint Security 安装在公司 IT 基础设施的各个计算机上，并持续监视流程、开放式网络连接和正在修改的文件。有关计算机上事件的信息（遥测数据）被发送到 Kaspersky Anti Targeted Attack Platform 服务器。此种情况下，Kaspersky Endpoint Security 也将应用程序发现的威胁信息和威胁处理结果信息发送到 Kaspersky Anti Targeted Attack Platform 服务器。

EDR (KATA) 和 NDR (KATA) 集成在 Kaspersky Security Center 控制台上配置。然后使用 Kaspersky Anti Targeted Attack Platform 控制台管理内置代理，包括运行任务、管理隔离对象、查看报告和其他操作。

Network Detection and Response (KATA) 参数

参数	描述
服务器连接设置	"**超时(秒)**"。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 TLS 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）。 "**使用双向认证**"。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。
地址 和 **端口**	连接到 Kaspersky Anti Targeted Attack Platform 服务器的设置。输入要连接的 Central Node 服务器的 IP 地址（IPv4 或 IPv6）和端口。 您可以添加多个 Central Node 服务器地址。Kaspersky Endpoint Security 尝试使用第一个 IP 地址连接到服务器。如果连接建立失败，Kaspersky Endpoint Security 将尝试使用列表中的第二个 IP 地址进行连接，依此类推。
发送同步请求到 NDR 服务器的间隔(分钟)	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。
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。默认设置是 30 秒。
启用请求限制	该功能有助于优化服务器上的负载。如果启用此功能，应用程序将限制事件传输。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。默认设置是每小时 3000 个事件。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。默认设置为 15%。

与 KUMA 的整合

Kaspersky Endpoint Security for Windows 支持 Kaspersky Unified Monitoring and Analysis Platform 解决方案。*Kaspersky Unified Monitoring and Analysis Platform (KUMA)* 是针对组织 IT 基础设施的安全信息和事件管理 (SIEM) 解决方案。KUMA 可以在安全威胁造成危害之前检测、分析和减轻它们。

参数	描述
发送事件时的最大延时（秒）	应用程序在同步间隔到期后与服务器同步以发送事件。默认设置是 30 秒。
连接到 KUMA 服务器	"**超时(秒)**"。最大 KUMA 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 KUMA 服务器。 "**服务器证书**"。用于与 KUMA 服务器建立受信任连接的 TLS 证书。您可以在 Kaspersky Unified Monitoring and Analysis Platform 控制台中获取 TLS 证书（请参阅 Kaspersky Unified Monitoring and Analysis Platform 中的说明）。 要建立受信任连接，在 KUMA 控制台的 TCP 连接器设置中，必须选择"**With verification**"TLS 模式（请参阅 Kaspersky Unified Monitoring and Analysis Platform 帮助 中的 tcp 类型连接器设置）。 "**使用双向身份验证**"。在 Kaspersky Endpoint Security 和 KUMA 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，在 KUMA 控制台的 TCP 连接器设置中，必须选择"**Custom PFX**"TLS 模式（请参阅 Kaspersky Unified Monitoring and Analysis Platform 帮助 中的 tcp 类型连接器设置）。然后您必须获取一个加密容器并设置一个密码来保护该加密容器。*加密容器*是带有证书和私钥的 PFX 存档。配置 KUMA 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。
KUMA 服务器	与 Kaspersky Unified Monitoring and Analysis Platform 服务器的连接设置。您可以输入 IP 地址（IPv4 或 IPv6）。 您可以添加多个 KUMA 服务器地址。Kaspersky Endpoint Security 尝试使用第一个 IP 地址连接到服务器。如果连接建立失败，Kaspersky Endpoint Security 将尝试使用列表中的第二个 IP 地址进行连接，依此类推。

完整磁盘加密

您可以选择加密技术：卡巴斯基磁盘加密 或 BitLocker 驱动器加密（以下简称"BitLocker"）。

卡巴斯基磁盘加密

卡巴斯基磁盘加密不支持基于 Arm 的计算机。

加密系统硬盘驱动器后，在下次计算机启动时，用户能够访问硬盘驱动器并且操作系统加载前，用户必须通过身份验证代理的身份验证。这需要输入连接至计算机的令牌或智能卡的密码，或者本地局域网管理员使用"*管理身份验证代理账户*"任务创建的身份验证代理账户的用户名或密码。这些账户以用户登录操作系统的 Microsoft Windows 账户为基础。这些帐户以用户登录操作系统的 Microsoft Windows 帐户为基础。您还可以使用 Single Sign-On (SSO) 技术，该技术允许您使用身份验证代理账户的用户名和密码自动登录到操作系统。

可以通过两种方式在身份验证代理中执行用户身份验证：

- 输入局域网管理员使用 Kaspersky Security Center 工具创建的身份验证代理帐户的用户名和密码。
- 输入连接至计算机的令牌的密码或智能卡的密码。

仅当计算机硬盘驱动器使用 AES256 加密算法进行加密时，才可以使用令牌或智能卡。如果使用 AES56 算法加密了计算机硬盘驱动器，添加电子证书文件到命令将被拒绝。

BitLocker 驱动器加密

BitLocker 是 Windows 操作系统内置的加密技术。Kaspersky Endpoint Security 允许您使用 Kaspersky Next 基础设施控制和管理 Bitlocker。BitLocker 可对逻辑卷进行加密。BitLocker 不能用于可移动驱动器的加密。有关 BitLocker 的详细信息，请参阅 Microsoft 文档。

> 加密磁盘时，BitLocker 将引导加载程序和其他辅助文件放入 system partition。此分区未加密。操作系统在安装 Windows 时会自动创建系统分区。如果在安装 Windows 之前磁盘已完全分区，则操作系统无法创建系统分区。在这种情况下，当启动 BitLocker 磁盘加密时，操作系统会提示您对磁盘重新分区，并创建系统分区。创建系统分区后，操作系统启动 BitLocker 加密。

BitLocker 使用受信任平台模块提供对访问密钥的安全存储。 *Trusted Platform Module*(TPM) 是一个与安全相关的提供基本功能的微芯片（例如用于存储加密密钥）。受信任平台模块通常安装在计算机主板上，并通过硬件总线与其他所有系统组件进行交互。使用 TPM 是存储 BitLocker 访问密钥的最安全方式，因为 TPM 提供了启动前系统完整性验证。您仍然可以在没有 TPM 的计算机上对驱动器进行加密。在这种情况下，将使用密码对访问密钥进行加密。BitLocker 使用以下身份验证方式：

- TPM。
- TPM 和 PIN。
- 密码。

对系统硬盘驱动器进行加密后，用户需要通过 BitLocker 身份验证才能启动操作系统。身份验证完成后，BitLocker 允许用户登录。BitLocker 不支持单点登录技术 (SSO)。

在对驱动器进行加密后，BitLocker 会创建一个恢复密钥。Kaspersky Endpoint Security 会将恢复密钥发送到 Kaspersky Security Center，以便您可以恢复对磁盘的访问，例如，如果用户忘记了密码。

如果用户使用 BitLocker 对磁盘进行加密，Kaspersky Endpoint Security 会将恢复密钥和有关磁盘加密的信息发送到 Kaspersky Security Center。

> 如果正在使用 Windows 组策略，请在策略设置中关闭 BitLocker 管理。Windows 策略设置可能与 Kaspersky Endpoint Security 策略设置冲突。在对驱动器进行加密时，可能会发生错误。

卡巴斯基磁盘加密组件设置

参数	描述
加密模式	“**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。 如果计算机安装了多个操作系统，在加密后，您将能够只加载安装了应用程序的操作系统。 “**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。 “**保留不变**”。如果选定了该项，应用策略后，应用程序将保留硬盘驱动器不动。如果驱动器已加密，则其仍加密。如果驱动器已解密，则其仍解密。默认情况下已选定此项。
在加密过程中，为 Windows 用户自动创建身份验证代理账户	如果该复选框被选中，应用程序基于计算机上的 Windows 用户账户创建身份验证代理账户。默认情况下，Kaspersky Endpoint Security 使用在过去 30 天内登录到操作系统的用户所使用的所有本地账户和域账户。

参数	描述
身份验证代理账户创建设置	"**计算机上的所有账户**"。计算机上曾经处于活动状态的所有账户。 "**计算机上的所有域账户**"。计算机上属于某个域且曾经处于活动状态的所有账户。 "**计算机上的所有本地账户**"。计算机上曾经处于活动状态的所有本地账户。 "**使用一次性密码的服务账户**"。服务账户是访问计算机所必需的，例如，当用户忘记密码时。您还可以将服务账户用作备用账户。您必须输入账户名称（默认是 `ServiceAccount`）。Kaspersky Endpoint Security 自动创建密码。您可以在 Kaspersky Security Center 控制台查找密码。 "**本地管理员**"。Kaspersky Endpoint Security 为计算机的本地管理员创建身份验证代理用户账户。 "**计算机管理者**"。Kaspersky Endpoint Security 为计算机的管理者账户创建身份验证代理用户账户。您可以在 Active Directory 的计算机属性中查看哪些账户具有计算机管理者角色。默认情况下，计算机管理者角色未定义，即不对应于任何账户。 "**活动账户**"。Kaspersky Endpoint Security 为在磁盘加密过程中活动的账户自动创建身份验证代理账户。
登录时为该计算机的所有用户自动创建身份验证代理账户	如果该复选框被选中，应用程序在启动身份验证代理之前检查计算机上的 Windows 用户账户信息。如果 Kaspersky Endpoint Security 检测到有 Windows 用户账户没有身份验证代理账户，应用程序将创建新账户以访问加密驱动器。新身份验证代理账户将具有以下默认设置：仅密码保护的登录、第一次身份验证时的密码更改。因此，您不需要使用"*管理身份验证代理账户*"任务对存在已加密驱动器的计算机手动添加身份验证代理账户。
保存在身份验证代理中输入的用户名	如果选中该复选框，应用程序将保存身份验证代理账户的名称。下次使用同一账户在身份验证代理中尝试完成认证时不会被提示输入账户名。
仅加密使用的磁盘空间(减少加密时间)	该复选框可启用/禁用将加密区域仅限为已用硬盘驱动器扇区的选项。该限制可减少加密时间。 加密开始后启用或禁用**仅加密使用的磁盘空间(减少加密时间)**功能在硬盘驱动器被加密之前并不修改该设置。开始加密之前您必须选择或清除该复选框。 如果选定该复选框，则仅加密使用的硬盘驱动器部分。Kaspersky Endpoint Security 将自动加密添加的新数据。 如果清空该复选框，整个硬盘驱动器将被加密，包括先前删除和修改文件残留的碎片。 推荐对尚未修改或删除数据的新硬盘驱动器使用该选项。如果对已在使用中的硬盘驱动器应用加密，则推荐加密整个硬盘驱动器。这样可确保保护所有数据，甚至已删除的数据也能够部分恢复。 默认下，复选框被清除。
使用 Legacy USB Support (不推荐)	此复选框启用或禁用"Legacy USB Support"功能。*Legacy USB Support* **是**一种 BIOS/UEFI 功能，允许您在启动操作系统（BIOS 模式）之前，在计算机的引导阶段使用 USB 设备（例如安全令牌）。"Legacy USB Support"不会影响操作系统启动后对 USB 设备的支持。 如果选中该复选框，在计算机初始启动期间对 USB 设备的支持将启用。 启用"Legacy USB Support"功能时，BIOS 模式下的身份验证代理不支持通过 USB 使用令牌。推荐仅当存在硬件兼容性问题时并仅对发生问题的计算机使用此选项。
密码设置	身份验证代理账户密码强度设置。使用单点登录技术时，身份验证代理将忽略 Kaspersky Security Center 中指定的密码强度要求。您可以在操作系统设置中设置密码强度要求。
使用单点登录 (SSO) 技术	SSO 技术允许使用同一个账户凭证访问加密硬盘驱动器并登录操作系统。 如果选中该复选框，您必须输入用于访问加密硬盘驱动器以及随后自动登录操作系统的帐户凭证。 如果清除该复选框，要访问加密硬盘驱动器并随后登录操作系统，您必须分别输入用于访问加密硬盘驱动器的凭证和操作系统用户帐户凭证。
包装第三方凭证提供者	Kaspersky Endpoint Security 支持第三方凭证提供程序 ADSelfService Plus。 使用第三方凭证提供程序时，身份验证代理会在加载操作系统之前拦截密码。这意味着用户在登录 Windows 时只需输入一次密码。例如，在登录到 Windows 之后，用户可以利用第三方凭证提供程序的功能在公司服务中进行身份验证。第三方凭证提供程序还允许用户独立重置自己的密码。在这种情况下，Kaspersky Endpoint Security 将自动更新身份验证代理的密码。 如果您使用的是应用程序不支持的第三方凭证提供程序，则在单点登录技术操作中可能会遇到一些限制。
帮助	"**身份验证**"。输入账户凭据时，"身份验证代理"窗口中显示的帮助文本。 "**更改密码**"。更改身份验证代理账户的密码时，"身份验证代理"窗口中显示的帮助文本。 "**恢复密码**"。恢复身份验证代理账户的密码时，"身份验证代理"窗口中显示的帮助文本。

参数	描述
加密模式	"**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。 如果计算机安装了多个操作系统，在加密后，您将能够只加载安装了应用程序的操作系统。 "**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。 "**保留不变**"。如果选定了该项，应用策略后，应用程序将保留硬盘驱动器不动。如果驱动器已加密，则其仍加密。如果驱动器已解密，则其仍解密。默认情况下已选定此项。
启用需要在平板电脑上预启动键盘输入的 BitLocker 身份验证	使用在预启动环境中需要数据输入的身份验证，即使该平台没有能力进行预启动输入（例如使用平板电脑上的触摸屏键盘）。 平板电脑的触摸屏在预启动环境中不可用。例如，要在平板电脑上完成 BitLocker 身份验证，用户必须连接 USB 键盘。 如果选定该复选框，则允许使用需要预启动输入的身份验证。我们推荐在预启动环境中仅对拥有备用数据输入工具的设备（例如除了触摸屏键盘之外的 USB 键盘）使用该设置。 如果清除此复选框，则无法在平板电脑上使用 BitLocker 驱动器加密。
使用硬件加密(OS Windows 8 和后续版本)	如果选定该复选框，则应用程序将应用硬件加密。这可以提高加密速度并使用较少的计算机资源。
仅加密使用的磁盘空间(Windows 8 和后续版本)	该复选框可启用/禁用将加密区域仅限为已用硬盘驱动器扇区的选项。该限制可减少加密时间。 加密开始后启用或禁用**仅加密使用的磁盘空间(减少加密时间)**功能在硬盘驱动器被加密之前并不修改该设置。开始加密之前您必须选择或清除该复选框。 如果选定该复选框，则仅加密使用的硬盘驱动器部分。Kaspersky Endpoint Security 将自动加密添加的新数据。 如果清空该复选框，整个硬盘驱动器将被加密，包括先前删除和修改文件残留的碎片。 推荐对尚未修改或删除数据的新硬盘驱动器使用该选项。如果对已在使用中的硬盘驱动器应用加密，则推荐加密整个硬盘驱动器。这样可确保保护所有数据，甚至已删除的数据也能够部分恢复。 默认下，复选框被清除。

参数	描述
身份验证方法	**仅密码(Windows 8 和后续版本)** 如果选定该选项，Kaspersky Endpoint Security 将在用户尝试访问加密磁盘时提示用户输入密码。 没有使用受信任平台模块 (TPM) 时可以选择该选项。 **受信任平台模块 (TPM)** 如果选定该复选框，则 BitLocker 使用受信任平台模块 (TPM)。 *Trusted Platform Module*(TPM) 是一个与安全相关的提供基本功能的微芯片（例如用于存储加密密钥）。受信任平台模块通常安装在计算机主板上并且通过硬件总线与其他所有系统组件进行互动。 对于运行 Windows 7 或 Windows Server 2008 R2 的计算机，只能使用 TPM 模块进行加密。如果未安装 TPM 模块，则无法进行 BitLocker 加密。不支持在这些计算机上使用密码。 配有受信任平台模块的设备可以创建只能使用该设备解密的加密密钥。受信任平台模块将使用其自有的根存储密钥加密加密密钥。根存储密钥存储在受信任平台模块中。这提供了防御黑客攻击加密密钥的附加保护。 默认情况下已选择此操作。 您可以为访问加密密钥设置额外的保护层，并使用密码或 PIN 加密密钥： • "**为 TPM 使用 PIN**"。如果选中该复选框，用户可以使用 PIN 码获得对存储在受信任平台模块 (TPM) 中的加密密钥的访问权限。如果清除此复选框，则禁止用户使用 PIN 码。要访问加密密钥，用户必须输入密码。 • "**受信任平台模块 (TPM)，或密码(如果 TMP 不可用)**"。如果选定该选项，当受信任平台模块 (TPM) 不可用时，用户可使用密码访问加密密钥。如果清除该复选框且 TPM 不可用，则将不会启动完整磁盘加密。 必须通过指定密码或 PIN 来配置所选的身份验证方法： • "**最小 PIN 码长度(字符数)**"。 • "**最小密码长度(字符数)**"。 • "**为 TPM 限制密码/PIN 有效期(天)**"。 • **使用增强 PIN (字母和数字)**。*增强 PIN* 允许使用数字字符以外的其他字符：大写和小写拉丁字母、特殊字符和空格。
自动重新创建恢复密钥(天)	自动更新密码以恢复对受 BitLocker 保护的驱动器的访问权限。如果选中该复选框，请指定恢复密钥密码的有效期。这有助于防止重复使用恢复密钥密码。

文件级加密

基于 Arm 架构的计算机不支持文件加密。

如果 Kaspersky Endpoint Security 安装在运行 Windows for Workstations 的计算机上，则该组件可用。如果 Kaspersky Endpoint Security 安装在运行 Windows for Servers 的计算机上，则该组件不可用。

您可以根据扩展名或扩展名组编制文件列表，和存储在本地计算机驱动器上的文件夹列表，并为特定应用程序创建的文件创建加密规则。应用策略后，Kaspersky Endpoint Security 将加密和解密以下文件：

- 单独添加到加密和解密列表中的文件；
- 存储在添加到加密和解密列表中的文件夹内的文件；
- 单独应用程序创建的文件。

文件加密具有以下特殊功能：

- Kaspersky Endpoint Security 仅为操作系统的本地用户配置文件加密/解密预定义文件夹内的文件。Kaspersky Endpoint Security 不会加密/解密预定义文件夹内的漫游用户配置文件、强制用户配置文件、临时用户配置文件或重定向的文件夹。

- Kaspersky Endpoint Security 不会加密其修改可能损害操作系统和安装的应用程序的文件。例如，加密排除项列表中包含的以下文件和包含所有嵌套文件夹在内的文件：

  - %WINDIR%；

  - %PROGRAMFILES% 和 %PROGRAMFILES(X86)%；

  - Windows 注册表文件。

  您无法查看或编辑这个加密排除项列表。尽管加密排除项列表中的文件和文件夹可以添加至加密列表，但在文件加密期间，它们不会被加密。

文件级加密组件设置

参数	描述
加密模式	"**保留不变**"。如果选定该项，Kaspersky Endpoint Security 将不更改文件和文件夹，不进行加密或解密。 "**根据规则**"。如果选择此项目，则 Kaspersky Endpoint Security 会根据加密规则对文件和文件夹进行加密，根据解密规则对文件和文件夹进行解密，并根据应用程序规则来控制应用程序对加密文件的访问。 "**全部解密**"。如果选定该选项，Kaspersky Endpoint Security 将解密所有加密的文件和文件夹。
加密	该选项卡将显示本地驱动器上存储的文件的加密规则。您可以添加文件，如下所示： • "**预定义文件夹**"。Kaspersky Endpoint Security 允许您添加以下区域： "**文档**"。操作系统的"*文档*"文件夹及其子文件夹中的文件。 "**收藏夹**"。操作系统的标准"*收藏夹*"文件夹及其子文件夹中的文件。 "**桌面**"。操作系统的"*桌面*"文件夹及其子文件夹中的文件。 "**临时文件**"。与计算机上安装的应用程序的操作有关的临时文件。例如，Microsoft Office 应用程序会创建包含文档备份副本的临时文件。 "**Outlook 文件**"。与 Outlook 邮件客户端操作有关的文件：数据文件 (PST)、离线数据文件 (OST)、离线地址簿文件 (OAB) 和个人地址簿文件 (PAB)。 • "**自定义文件夹**"。您可以输入文件夹的路径。添加文件夹路径时，请遵循以下规则： 使用环境变量（例如，`%FOLDER%\UserFolder\`）。您只能在路径的开头使用一次环境变量。 不要使用相对路径。 不要使用 `*` 和 `?` 字符。 不要使用 UNC 路径。 使用 `;` 或 `,` 作为分隔符。 • "**按扩展名选择文件**"。您可以从列表中选择扩展名组，例如"*压缩文件*"扩展名组。您也可以手动添加文件扩展名。
解密	该选项卡将显示本地驱动器上存储的文件的解密规则。
应用程序规则	该选项卡将显示包含应用程序加密文件访问规则的的表以及由单个应用程序创建或修改的文件的加密规则。
加密数据包	创建加密数据包时要满足的密码强度要求。

可移动驱动器加密

基于 Arm 架构的计算机不支持对可移动驱动器加密。

如果 Kaspersky Endpoint Security 安装在运行 Windows for Workstations 的计算机上，则该组件可用。如果 Kaspersky Endpoint Security 安装在运行 Windows for Servers 的计算机上，则该组件不可用。

Kaspersky Endpoint Security 支持加密 FAT32 和 NTFS 文件系统中的文件。如果将具有不支持的文件系统的可移动驱动器连接到计算机，对该可移动驱动器的加密任务将以出错结束，Kaspersky Endpoint Security 会为该可移动驱动器分配只读状态。

要保护可移动驱动器上的数据，可以使用以下类型的加密：

- Full Disk Encryption (FDE)。

  加密整个可移动驱动器，包括文件系统。

  无法在公司网络外部访问加密数据。如果计算机未连接到 Kaspersky Security Center（例如，“来宾”计算机），也无法访问公司网络内部的加密数据。

- File Level Encryption (FLE)。

  仅加密可移动驱动器上的文件。文件系统保持不变。

  可移动驱动器上的文件加密使用一种称为*便携模式*的特殊模式提供了访问公司网络外部数据的功能。

在加密期间，Kaspersky Endpoint Security 会创建一个主密钥。Kaspersky Endpoint Security 将主密钥保存在以下存储库中：

- Kaspersky Security Center。
- 用户的计算机。

  主密钥使用用户的密钥加密。

- 可移动驱动器。

  主密钥使用 Kaspersky Security Center 的公钥加密。

加密完成后，可在公司网络内访问可移动驱动器上的数据，就像数据在普通的未加密可移动驱动器上一样。

访问加密数据

连接带有加密数据的可移动驱动器后，Kaspersky Endpoint Security 执行以下操作：

1. 检查用户计算机的本地存储中的主密钥。

   如果找到主密钥，用户将获得可移动驱动器上的数据的访问权限。

   如果找不到主密钥，Kaspersky Endpoint Security 会执行以下操作：

   a. 向 Kaspersky Security Center 发送请求。

      收到请求后，Kaspersky Security Center 将发送一个包含主密钥的响应。

   b. Kaspersky Endpoint Security 将主密钥保存在用户计算机的本地存储中，以供以后对加密的可移动驱动器进行操作。

2. 解密数据。

可移动驱动器加密的特殊功能

可移动驱动器加密具有以下特殊功能：

- 已经为指定受管理计算机组形成了针对可移动驱动器加密的带有预设设置的策略。因此，应用为加密/解密可移动驱动器配置的 Kaspersky Security Center 策略的结果取决于可移动驱动器连接到的计算机。
- Kaspersky Endpoint Security 不会加密/解密可移动驱动器上存储的只读文件。
- 支持以下设备类型的可移动驱动器：
  - 通过 USB 总线连接的数据媒体
  - 通过 USB 和 FireWire 总线连接的硬盘磁盘驱动器
  - 通过 USB 和 FireWire 总线连接的 SSD 磁盘驱动器

可移动驱动器加密组件设置

参数	描述
加密模式	“**加密整个可移动驱动器**”。如果选定了该项，为可移动驱动器应用带有指定加密设置的策略时，Kaspersky Endpoint Security 将会逐个扇区加密可移动驱动器，包括其文件系统。 “**加密所有文件**”。如果选定了该选项，为可移动驱动器应用带有指定加密设置的策略时，Kaspersky Endpoint Security 将会加密可移动驱动器上存储的所有文件。Kaspersky Endpoint Security 不会对已经加密的文件重新加密。可移动驱动器的文件系统的内容，包括加密文件的文件夹结构和名称在内都不会被加密，仍可以被访问。 “**仅加密新文件**”。如果选定了该选项，为可移动驱动器应用带有指定加密设置的策略时，Kaspersky Endpoint Security 将只会加密在上次应用 Kaspersky Security Center 策略之后在可移动驱动器上添加或修改的文件。当某个可移动驱动器由两个人使用或在工作中使用时，该加密模式很有用。该加密模式可以使您保留所有旧的未更改过的文件，加密那些用户在已安装 Kaspersky Endpoint Security 并启用加密功能的工作计算机创建的文件。结果是个人文件是否可以被访问，与启用了加密功能的计算机上是否安装了 Kaspersky Endpoint Security 无关。 “**解密整个可移动驱动器**”。如果选定了该项，为可移动驱动器应用带有指定加密设置的策略时，Kaspersky Endpoint Security 将会解密可移动驱动器上存储的先前加密的所有文件和文件系统。 “**保留不变**”。如果选定了该项，应用策略后，应用程序将保留硬盘驱动器不动。如果驱动器已加密，则其仍加密。如果驱动器已解密，则其仍解密。默认情况下已选定此项。

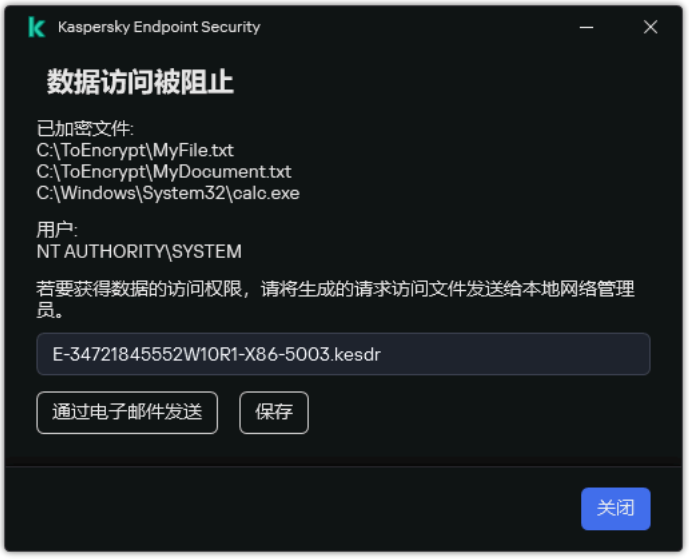
参数	描述
便携模式	该复选框可启用/禁用准备可移动驱动器，以便能够在公司网络外部的计算机上访问该可移动驱动器中存储的文件。 如果选定该复选框，Kaspersky Endpoint Security 将提示用户在根据策略加密可移动驱动器之前指定一个密码。在公司网络外部的计算机上访问可移动驱动器中的加密文件时需要该密码。您可以配置密码强度。 便携模式可用于“**加密所有文件**”或“**仅加密新文件**”模式。
仅加密使用的磁盘空间	该复选框将启用/禁用加密模式，其中仅加密已使用磁盘扇区。推荐为尚未修改或删除数据的新设备使用该模式。 如果选定该复选框，则仅加密使用的磁盘部分。Kaspersky Endpoint Security 将自动加密添加的新数据。 如果清空该复选框，整个驱动器将被加密，包括先前删除和修改文件残留的碎片。 仅加密已占用的空间的功能仅在“**加密整个可移动驱动器**”模式下可用。 开始加密后，启用/禁用“**仅加密使用的磁盘空间**”功能不会更改该设置。开始加密之前您必须选择或清除该复选框。

自定义规则	该表包含了已其定义自定义加密规则的设备。您可以通过以下方式为单个可移动驱动器创建加密规则：
	• 从“设备控制”的受信任设备列表中添加可移动驱动器。
	• 手动添加可移动驱动器：
	  • 按设备 ID（Hardware ID 或 HWID）
	  • 按设备型号： Vendor ID （VID）和 Product ID （PID）

允许在离线模式下加密可移动驱动器	如果选中该复选框，则即使没有连接至 Kaspersky Security Center，Kaspersky Endpoint Security 也会加密可移动驱动器。在这种情况下，解密可移动驱动器所需的数据存储在与可移动驱动器连接的计算机的硬盘驱动器上，不会传输到 Kaspersky Security Center。 如果清除该复选框，则 Kaspersky Endpoint Security 无法在未连接至 Kaspersky Security Center 的情况下加密可移动驱动器。
加密密码设置 / 便携式文件管理器	便携式文件管理器的密码强度设置。

模板（数据加密）

进行数据加密后，Kaspersky Endpoint Security 可能会限制对数据的访问，例如，由于组织基础结构发生变化和 Kaspersky Security Center 管理服务器发生变化。如果用户无权访问加密数据，用户可以请管理员提供数据访问权限。换句话说，用户需要将请求访问文件发送给管理员。然后，用户需要将从管理员处收到的响应文件上传到 Kaspersky Endpoint Security。Kaspersky Endpoint Security 允许您通过电子邮件向管理员请求数据访问权限（请参见下图）。



请求加密数据访问权限

系统提供了一个模板，用于报告缺少对加密数据的访问权限。为方便用户，您可以填写以下字段：

- “**收件人**”。输入拥有数据加密功能权限的管理员组的电子邮件地址。
- “**主题**”。输入包含加密文件访问请求的电子邮件的主题。例如，您可以添加标签以过滤邮件。
- “**用户消息**”。如有必要，可更改邮件的内容。您可以使用变量来获取必要数据（例如，`%USER_NAME%` 变量）。

排除

受*信任区域*是由系统管理员配置的、Kaspersky Endpoint Security 在活动期间不予监控的对象和应用程序的列表。

考虑到所处理对象的特点和安装在计算机上的应用程序，管理员可以自主创建受信任区域。当 Kaspersky Endpoint Security 阻止访问特定对象或应用程序时，如果您确定此对象或应用程序是无害的，则有必要将其包含在受信任区域中。管理员也可以允许用户为特定计算机创建他们自己的本地受信任域。这样，除了策略中的常规受信任域，用户可以创建他们自己的本地排除项和受信任应用程序列表。

从 Kaspersky Endpoint Security 12.5 for Windows 开始，您可以将 EDR 遥测添加到受信任区域。这允许优化应用程序发送到 Kaspersky Anti Targeted Attack Platform (EDR) 解决方案的遥测采集服务器的数据。

从 Kaspersky Endpoint Security 12.6 for Windows 开始，扫描排除项和受信任的应用程序被添加到信任区域。预定义的扫描排除项和受信任的应用程序有助于在 SQL 服务器、Microsoft Exchange 服务器和 System Center Configuration Manager 上快速配置 Kaspersky Endpoint Security。这意味着您不需要在服务器上为应用程序手动设置信任区域。

从 Kaspersky Endpoint Security 12.8 for Windows 开始，您可以在 Light Agent 模式下安装该应用程序来保护虚拟环境。预定义的扫描排除项和受信任的应用程序可以帮助您在 Citrix 和 VMware 虚拟环境中快速配置 Kaspersky Endpoint Security。

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。有关可被入侵者用来破坏计算机或个人数据的合法软件的详细信息，请访问 Kaspersky IT 百科全书网站。

这类应用程序可以被 Kaspersky Endpoint Security 阻止。若要防止它们被阻止，您可以为正在使用的应用程序排除扫描排除项。为此，请将 Kaspersky IT 百科全书中列出的名称或名称掩码添加到受信任区域。例如，您经常使用 Radmin 应用程序来远程管理计算机。Kaspersky Endpoint Security 会将这些活动看做可疑活动并进行阻止。若要防止应用程序被阻止，请使用 Kaspersky IT 百科全书中列出的名称或名称掩码创建扫描排除项。

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 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 从扫描中排除该应用程序。

扫描排除项可用于下列特定应用程序组件和系统管理员配置的任务：

- 行为检测
- 漏洞利用防御
- 主机入侵防御
- 文件威胁防护
- Web 威胁防护
- 邮件威胁防护
- "*恶意软件扫描*"任务

受信任应用程序列表

*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。

扫描排除项和受信任的应用程序之间的区别在于，对于排除项，Kaspersky Endpoint Security 不扫描文件，而对于受信任的应用程序，它不控制启动的进程。如果受信任的应用程序在未包含在扫描排除项中的文件夹中创建恶意文件，Kaspersky Endpoint Security 将检测该文件并消除威胁。如果该文件夹被添加到排除项，Kaspersky Endpoint Security 将跳过该文件。

例如，如果您认为被标准 Microsoft Windows 记事本使用的对象是安全的，也即您信任此应用程序，则可将 Microsoft Windows 记事本添加到受信任的应用程序列表中，从而不监控该应用程序所使用的对象。这将提高计算机性能，这在使用服务器应用程序时尤为重要。

此外，被 Kaspersky Endpoint Security 分类为可疑操作的某些操作，在很多应用程序的功能环境中可能是安全的。例如，拦截键盘键入的文本，是自动键盘布局切换器中的一种例行程序（例如 Punto Switcher）。考虑到此类程序的特点并将其行为从监控中排除，我们建议您可将此类程序添加到受信任应用程序列表中。

受信任的应用程序有助于避免 Kaspersky Endpoint Security 与其他应用程序之间的兼容性问题（例如，Kaspersky Endpoint Security 和另一个反病毒应用程序对第三方计算机的网络流量进行双重扫描的问题）。

同时，受信任应用程序的可执行文件和进程仍然会扫描病毒和其他恶意软件。您可以通过扫描排除项将应用程序从 Kaspersky Endpoint Security 扫描中完全排除。

排除项设置

参数	描述

检测对象类型

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、蠕虫和木马。它们可能会给计算机带来巨大的损害。

- **病毒和蠕虫**

  子类别：病毒和蠕虫 (Viruses_and_Worms)

  危险级别：高

  典型的病毒和蠕虫会执行未经用户授权的操作。它们会创建可自我复制的副本。

  典型病毒

  典型病毒侵入计算机后，会感染文件，激活并执行恶意操作，以及将自身的副本添加到其他文件中。

  典型病毒仅在计算机本地资源上复制副本，不会自行侵入其他计算机。仅当该病毒将其副本添加至存储在共享文件夹或放入计算机中的 CD 中的文件时，或者在用户发送附有受感染文件的电子邮件消息时，该病毒才会传染给其他计算机。

  典型病毒代码可以入侵计算机、操作系统和应用程序的各种区域。根据具体的环境，病毒可分为*文件病毒*、*引导区病毒*、*脚本病毒*和*宏病毒*。

  病毒可以使用多种不同的技术来感染文件。*Overwriting*病毒会使用其代码覆盖受感染文件的代码，从而抹除文件的内容。感染的文件会停止发挥作用，且无法恢复。*Parasitic*病毒会修改文件，从而使之发挥全部或部分功能。*Companion*不会修改文件，而是创建副本。当您打开受感染的文件时会启动该文件的副本（实际上是病毒）。您也会遇到以下类型的病毒：*Link viruses*、*OBJ 病毒*、*LIB 病毒*、*源代码病毒*和许多其他病毒。

  蠕虫

  与典型病毒一样，蠕虫在侵入计算机后，其代码将激活并执行恶意操作。之所以称为蠕虫，是因为它们能够从一台计算机"爬"到另一台计算机，并不需用户权限即可通过许多数据通道来传播副本。

  可用于区分各种类型蠕虫的主要特征是蠕虫的传播方式。下表提供了各种类型蠕虫的概览，这些蠕虫按其传播方式进行了分类。

  蠕虫传播方式

类型	名称	描述
电子邮件蠕虫	电子邮件蠕虫	这些蠕虫通过电子邮件传播。 受感染的电子邮件消息包含带有蠕虫副本的附件，或指向上传到可能已被攻击或者专门创建用于传播蠕虫的网站上某文件的链接。打开该附件时，蠕虫将被激活。在您单击该链接，进行下载，然后打开文件时，蠕虫还会开始执行其恶意操作。之后，蠕虫会继续传播其副本，搜索其他电子邮件地址，并向它们发送受感染的邮件。
IM 蠕虫	IM 客户端蠕虫	它们通过 IM 传播。 通常，此类蠕虫会利用用户的联系人列表发送消息，其中包含指向某网站上带有蠕虫副本的文件的链接。用户下载并打开文件时，蠕虫将被激活。
IRC 蠕虫	互联网聊天蠕虫	它们会通过Internet Relay Chats（允许通过互联网与其他人实时通信的服务系统）传播。 这些蠕虫会在互联网聊天中年发布包含自身副本的文件或指向该文件的链接。用户下载并打开文件时，蠕虫将被激活。
网络蠕虫	网络蠕虫	这些蠕虫通过计算机网络传播。 与其他类型的蠕虫不同，典型的网络蠕虫不需用户参与即可传播。它会扫描本地网来寻找安装了有漏洞的程序的计算机。为此，它会发送特殊格式的网络数据包（漏洞），其中包含蠕虫代码或部分蠕虫代码。如果网络上存在"有漏洞"的计算机，该计算机会接收到此种网络数据包。蠕虫完全入侵计算机后，将被激活。
P2P 蠕虫	文件共享网络蠕虫	它们通过点对点文件共享网络传播。 为了渗透到 P2P 网络，蠕虫会将自身复制到通常位于用户计算机上的文件共享文件夹中。P2P 网络会显示有关该文件的信息，以便用户可以在网络中像任何其他文件一样"找到"受感染的文件，然后下载并打开该文件。 更加狡猾的蠕虫会模仿特定 P2P 网络的网络协议：它们会返回对搜索程序的积极响应，并提供自身的副本供下载。
蠕虫	其他类型的蠕虫	其他类型的蠕虫包括： • 通过网络资源传播自身副本的蠕虫。通过使用操作系统的功能，它们扫描可用的网络文件夹，连接到互联网上的计算机，并尝试获取对磁盘驱动器的完全访问。与之前描述的蠕虫类型不同，其他类型的蠕虫不会自行激活，而是在用户打开包含蠕虫副本的文件时激活。 • 不使用上表中所述的任何方法进行传播的蠕虫（例如，通过手机传播的蠕虫）。

- **木马(包含勒索软件)**

  子类别：木马

  危险级别：高

  与蠕虫和病毒不同，木马不能进行自我复制。例如，用户访问受感染的网页时，它们会通过电子邮件或浏览器侵入计算机。木马通过用户参与而启动。木马启动后即会开始执行恶意操作。

  在受感染的计算机上，不同的木马会表现出不同的行为。木马的主要功能包括阻止、修改或破坏信息，以及禁用计算机或网络。木马还可以接收或发送文件，在屏幕上显示消息，请求网页，下载和安装程序，以及重启计算机。

  黑客通常使用各种不同木马的"集合"。

  下表中介绍了木马行为的类型。

  受感染计算机上木马行为的类型

类型	名称	描述
木马炸弹	木马 –"压缩文件炸弹"	解压缩时，这些压缩文件的大小会急剧增加，从而影响计算机的操作。 用户尝试解压缩这种压缩文件时，计算机可能会运行缓慢或停止运行；硬盘可能会充满"空白"数据。"压缩文件炸弹"对于文件和邮件服务器尤为危险。如果服务器使用自动系统处理接收信息，则"压缩文件炸弹"可能会中断服务器运行。
后门	用于远程管理的木马	此种木马被视为最危险的木马类型。在功能方面，这些木马与安装在计算机上的远程管理应用程序相似。 这些程序会在不被用户发觉的情况下将自身安装到计算机上，以便入侵者远程管理计算机。
木马	木马	木马包括以下恶意应用程序： • **典型木马**。这些程序仅执行木马的主要功能：阻止、修改或破坏信息，以及禁用计算机或网络。它们没有任何高级功能，与表中描述的其他类型的木马不同。 • **万能木马**。这些程序具有多种典型木马类型的高级功能。
勒索木马	勒索木马	这些木马将用户信息作为"人质"，修改或阻止信息，或者影响计算机的操作，以使用户无法使用信息。入侵者向用户进行勒索，许诺发送应用程序来恢复计算机的性能以及计算机上存储的数据。
木马点击器	木马点击器	这些木马通过自行向浏览器发送命令或更改在操作系统文件中指定的网址的方式，从用户的计算机访问网页。 通过使用这些程序，入侵者进行网络攻击并提高网站访问量，从而增加条幅广告的显示次数。
木马下载器	木马下载器	这些木马会访问入侵者的网页，从中下载其他恶意应用程序，并将它们安装到用户的计算机。这些木马包含要下载的恶意应用程序的文件名，或从访问的网页中接收该文件名。
木马释放器	木马释放器	这些木马包含安装在硬盘驱动器上并随后进行安装的其他木马。 入侵者可能会使用木马释放器类型的程序来达到以下目的： • 未通知用户就安装恶意应用程序：木马释放器类型的程序不会显示消息，或者会显示虚假消息，例如通知压缩文件中存在错误或操作系统的版本不兼容。 • 保护另一个已知恶意应用程序不被检测：并非所有反病毒软件都可检测到木马释放器类型应用程序中的恶意应用程序。
通知型木马	通知型木马	这些木马会通知入侵者受感染的计算机可供访问，并向入侵者发送有关计算机的信息：IP 地址、已开放端口号或电子邮件地址。它们通过电子邮件、FTP、访问入侵者的网页或以其他方式与入侵者联系。 通知型木马类型的程序通常用于包含多种木马的集合中。这些木马会通知入侵者其他木马已成功安装到用户的计算机。
代理型木马	代理型木马	这些木马允许入侵者使用用户的计算机匿名访问网页，它们通常用于发送垃圾邮件。
PSW 木马	密码盗窃软件	密码盗劫软件是盗窃用户账户（如软件注册数据）的一种木马。这些木马会查找系统文件和注册表中的机密数据，并通过电子邮件、FTP、访问入侵者的网页或以其他方式将其发送给"攻击者"。 部分这些木马分类为此表中描述的单独类型。这些木马会盗窃银行账户（网银窃贼木马），窃取 IM 客户端用户的数据（IM 木马），以及盗窃在线游戏用户的信息（游戏窃贼木马）。
间谍木马	间谍木马	这些木马暗中监视用户，收集有关用户使用计算机时所做的操作的信息。它们可能会拦截用户通过键盘输入的数据，截取屏幕，或收集活动应用程序的列表。收到信息后，这些木马会通过电子邮件、FTP、访问入侵者的网页或以其他方式将信息传输给入侵者。
分布式拒绝服务攻击木马	木马网络攻击者	这些木马会从用户计算机将大量请求发送至远程服务器。服务器缺少资源来处理所有请求，因此会停止运行（拒绝服务，或简称为 DoS）。黑客通常会使用这些程序感染许多计算机，以使用这些计算机来同时攻击一个服务器。 DoS 程序在用户知悉的情况下从一台计算机发起攻击。DDoS（分布式 DoS）程序在不被受感染计算机用户发觉的情况下从多台计算机发起分布式攻击。
IM 木马	从 IM 客户端用户那里窃取信息的木马	它们会窃取 IM 客户端用户的帐号和密码。这些木马会通过电子邮件、FTP、访问入侵者的网页或以其他方式将数据传输给入侵者。
Rootkit	Rootkit	这些木马会掩盖其他恶意应用程序及其活动，从而延长这些应用程序在操作系统中持续存在的时间。它们还会隐藏文件、受感染计算机内存中的进程或运行恶意应用程序的注册表键。Rootkit 会掩盖用户计算机上的应用程序与网络上其他计算机之间进行的数据交换。
SMS 木马	SMS格式的木马	这些木马会感染手机，向额外收费的手机号码发送 SMS。
游戏窃贼木马	从在线游戏用户那里窃取信息的木马	这些木马会窃取在线游戏用户的账户凭据，然后将这些凭据通过电子邮件、FTP、访问黑客的网页或以其他方式发送给黑客。
网银窃贼木马	窃取银行账户的木马	这些木马会窃取银行账户数据或电子货币系统数据；将这些数据通过电子邮件、FTP、访问黑客的网页或以其他方式发送给黑客。
邮件侦测木马	收集电子邮件地址的木马	这些木马会收集存储在计算机上的电子邮件地址，然后通过电子邮件、FTP、访问入侵者的网页或以其他方式将它们发送给入侵者。入侵者可能会向收集到的地址发送垃圾邮件。

- ## 恶意工具

子类别：恶意工具

危险级别：中

与其他类型的恶意软件不同，恶意工具在启动过后不会执行其操作。恶意工具可以在用户的计算机上安全地存储和启动。入侵者通常使用这些程序的功能来创建病毒、蠕虫和木马，对远程服务器进行网络入侵，攻击计算机或执行其他恶意操作。

恶意工具的各种功能按下表中所述的类型进行分组。

恶意工具的功能

类型	名称	描述
构建器	构建器	通过它们可以创建新的病毒、蠕虫和木马。一些构建器扬言构建了基于窗口的标准界面，用户可在该界面中选择要创建的恶意应用程序的类型，对付调试程序的方式，以及其他功能。
拒绝服务攻击	网络攻击	这些木马会从用户计算机将大量请求发送至远程服务器。服务器缺少资源来处理所有请求，因此会停止运行（拒绝服务，或简称为 DoS）。
漏洞	漏洞	"*漏洞*"是一组数据或程序代码，利用处理它们的应用程序的缺陷对计算机执行恶意操作。例如，漏洞可以写入或读取文件，或请求"受感染"的网页。 不同的漏洞会利用不同应用程序或网络服务的缺陷。漏洞会伪装成网络数据包通过网络传输到许多计算机，然后搜索网络服务存在缺陷的计算机。DOC 文件中的漏洞会利用文本编辑器的缺陷。在用户打开受感染的文件时，它可能会开始执行黑客编程的操作。嵌入在电子邮件消息中的漏洞会搜索电子邮件客户端的缺陷。用户在电子邮件客户端中打开受感染的邮件时，漏洞会立即开始执行恶意操作。 网络蠕虫会使用漏洞通过网络进行传播。Nuker 漏洞是可禁用计算机的网络数据包。

文件加密器	加密器	加密器会加密其他恶意应用程序，以隐藏它们不被反病毒应用程序发现。
洪水攻击器	用于“污染”网络的程序	这些程序会通过网络通道发送大量邮件。例如，该类型的工具包括污染互联网中继聊天的程序。 洪水攻击器工具不包括“污染”电子邮件、IM 客户端以及移动通信系统所使用通道的程序。这些程序可分为表中介绍的各种类型（电子邮件洪水攻击器、IM 洪水攻击器和 SMS 洪水攻击器）。
黑客工具	黑客工具	这些工具可以破坏其所在的计算机，或攻击其他计算机（例如，未经用户许可添加新系统账户，或清除系统日志以隐藏在操作系统中的存在路径）。这种类型的工具包括一些具有恶意功能的嗅探器，例如密码截取。嗅探器是允许查看网络流量的程序。
恶作剧程序	恶作剧程序	这些程序会警告用户类似病毒的消息：它们可能会在未受感染的文件中“检测到病毒”，或通知用户磁盘已被格式化，尽管这些情况实际并未发生。
地址欺骗程序	地址欺骗工具	这些工具使用伪造的发件人地址发送邮件和网络请求。例如，入侵者会使用地址欺骗程序类型的工具来掩盖他们作为邮件实际发件人的事实。
病毒修改工具	修改恶意应用程序的工具	通过这些工具可以修改其他恶意软件，隐藏它们不被反病毒程序发现。
电子邮件洪水攻击器	“污染”电子邮件地址的程序	这些程序会向各种电子邮件地址发送大量邮件，从而“污染”这些地址。大量的接收邮件会妨碍用户查看收件箱中的有用邮件。
IM 洪水攻击器	“污染”IM 流量的程序	它们向 IM 的用户发送大量消息。大量的信息会妨碍用户查看有用的接收信息。
SMS 洪水攻击器	使用 SMS“污染”流量的程序	这些程序向手机发送大量 SMS。

- **广告软件**

  子类别：广告软件；

  危险级别：中

  广告软件向用户显示广告信息。广告软件程序会在其他程序的界面中显示条幅广告，并将搜索查询重定向至广告网页。某些广告软件程序会收集有关用户的营销信息，并将其发送给开发者：该信息可能包括用户访问的网站的名称，或用户搜索查询的内容。与间谍木马类型的程序不同，广告软件程序会在用户许可的情况下将该信息发送给开发者。

- **自动拨号程序**

  子类别：可能会被入侵者用来破坏计算机或个人数据的合法软件。

  危险级别：中

  大多数这些应用程序都很有用，因此有许多用户使用它们。这些应用程序包括 IRC 客户端、自动拨号程序、文件下载程序、计算机系统活动监控器、密码实用程序以及用于 FTP、HTTP 和 Telnet 的互联网服务器。

  但是，如果入侵者获得了这些程序的访问权限，或如果他们在用户的计算机上安置这些程序，应用程序的某些功能可能会被用来危害安全。

  这些应用程序具有不同的功能，下表介绍了它们的类型。

类型	名称	描述
客户端 IRC	互联网聊天客户端	用户安装这些程序与他人进行互联网中继聊天。入侵者使用这些程序来传播恶意软件。
下载器	用于下载的程序	这些程序可以在隐藏模式下从网页下载文件。
监控器	用于监控的程序	这些程序可监控其安装到的计算机上的活动（查看哪些应用程序正在活动，以及它们如何与安装在其他计算机上的应用程序交换数据）。
密码工具	密码恢复器	通过它们可以查看和恢复已忘记的密码。入侵者出于相同的目的，秘密地将它们安置在用户的计算机上。
远程管理程序	远程管理程序	系统管理员广泛使用的一些程序。通过这些程序可以获取对远程计算机界面的访问权限，以监控和管理该计算机。入侵者出于同样的目的，秘密地将它们安置在用户的计算机上：用于监控和管理远程计算机。 合法的远程管理程序与实现远程管理的后门类型的木马不同。木马能够独自入侵操作系统并自行安装；合法的程序则无法做到这些。
FTP 服务程序	FTP 服务器	这些程序可起到 FTP 服务器的作用。入侵者将它们安置在用户计算机上，以打开通过 FTP 对该计算机的远程访问。
代理服务程序	代理服务器	这些程序可起到代理服务器的作用。入侵者将它们安置在用户计算机上，以用户名义发送垃圾邮件。
Telnet 服务程序	Telnet 服务器	这些程序可起到 Telnet 服务器的作用。入侵者将它们安置在用户计算机上，以打开通过 Telnet 对该计算机的远程访问。
Web 服务程序	Web 服务器	这些程序可起到 Web 服务器的作用。入侵者将它们安置在用户计算机上，以打开通过 HTTP 对该计算机的远程访问。
风险工具	在本地计算机上工作的工具	在用户自己的计算机上工作时，这些工具会为用户提供其他选项。通过这些工具，用户可以隐藏文件或活动应用程序的窗口，并终止活动的进程。
网络工具	网络工具	与网络上的其他计算机配合工作时，这些工具会为用户提供其他选项。通过这些工具可以进行重启，检测开放的端口，以及启动安装在计算机上的应用程序。
P2P 客户端	P2P 网络客户端	通过它们可以在对等网络中工作。入侵者可能会利用它们传播恶意软件。
客户端 SMTP	SMTP 客户端	它们未经用户的同意便发送电子邮件。入侵者将它们安置在用户计算机上，以用户名义发送垃圾邮件。
Web 工具栏	Web 工具栏	它们会向其他应用程序的界面中添加工具栏，以使用搜索引擎。
欺骗工具	欺骗程序	这些程序将自己伪装为其他程序。例如，一些欺骗反病毒程序会显示有关恶意软件检测的信息。但实际上，它们并未找到任何内容或进行清除。

- **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**

  子类别：可能会被入侵者用来破坏计算机或个人数据的合法软件。

  危险级别：中

  大多数这些应用程序都很有用，因此有许多用户使用它们。这些应用程序包括 IRC 客户端、自动拨号程序、文件下载程序、计算机系统活动监控器、密码实用程序以及用于 FTP、HTTP 和 Telnet 的互联网服务器。

  但是，如果入侵者获得了这些程序的访问权限，或如果他们在用户的计算机上安置这些程序，应用程序的某些功能可能会被用来危害安全。

  这些应用程序具有不同的功能，下表介绍了它们的类型。

类型	名称	描述
客户端 IRC	互联网聊天客户端	用户安装这些程序与他人进行互联网中继聊天。入侵者使用这些程序来传播恶意软件。
下载器	用于下载的程序	这些程序可以在隐藏模式下从网页下载文件。
监控器	用于监控的程序	这些程序可监控其安装到的计算机上的活动（查看哪些应用程序正在活动，以及它们如何与安装在其他计算机上的应用程序交换数据）。
密码工具	密码恢复器	通过它们可以查看和恢复已忘记的密码。入侵者出于相同的目的，秘密地将它们安置在用户的计算机上。
远程管理程序	远程管理程序	系统管理员广泛使用的一些程序。通过这些程序可以获取对远程计算机界面的访问权限，以监控和管理该计算机。入侵者出于同样的目的，秘密地将它们安置在用户的计算机上：用于监控和管理远程计算机。 合法的远程管理程序与实现远程管理的后门类型的木马不同。木马能够独自入侵操作系统并自行安装；合法的程序则无法做到这些。
FTP 服务程序	FTP 服务器	这些程序可起到 FTP 服务器的作用。入侵者将它们安置在用户计算机上，以打开通过 FTP 对该计算机的远程访问。
代理服务程序	代理服务器	这些程序可起到代理服务器的作用。入侵者将它们安置在用户计算机上，以用户名义发送垃圾邮件。
Telnet 服务程序	Telnet 服务器	这些程序可起到 Telnet 服务器的作用。入侵者将它们安置在用户计算机上，以打开通过 Telnet 对该计算机的远程访问。
Web 服务程序	Web 服务器	这些程序可起到 Web 服务器的作用。入侵者将它们安置在用户计算机上，以打开通过 HTTP 对该计算机的远程访问。
风险工具	在本地计算机上工作的工具	在用户自己的计算机上工作时，这些工具会为用户提供其他选项。通过这些工具，用户可以隐藏文件或活动应用程序的窗口，并终止活动的进程。
网络工具	网络工具	与网络上的其他计算机配合工作时，这些工具会为用户提供其他选项。通过这些工具可以进行重启，检测开放的端口，以及启动安装在计算机上的应用程序。
P2P 客户端	P2P 网络客户端	通过它们可以在对等网络中工作。入侵者可能会利用它们传播恶意软件。
客户端 SMTP	SMTP 客户端	它们未经用户的同意便发送电子邮件。入侵者将它们安置在用户计算机上，以用户名义发送垃圾邮件。
Web 工具栏	Web 工具栏	它们会向其他应用程序的界面中添加工具栏，以使用搜索引擎。
欺骗工具	欺骗程序	这些程序将自己伪装为其他程序。例如，一些欺骗反病毒程序会显示有关恶意软件检测的信息。但实际上，它们并未找到任何内容或进行清除。

- **可能被用来保护恶意代码的打包对象**

  子类别：可能造成危害的打包文件。

  危险级别：中。

  该文件使用专门用于打包恶意软件（病毒、蠕虫、特洛伊木马）的特殊打包程序进行打包。Kaspersky Endpoint Security 会扫描 SFX（自解压）存档中的解包工具模块。

  为了隐藏恶意软件以避免被反病毒软件检测到，黑客使用特殊的打包程序对其进行打包。卡巴斯基专家已识别出黑客最常使用的解包工具。

- **多层打包对象**

  子类别：可能造成危害的打包文件。

  危险级别：中。

  该文件使用专门用于打包恶意软件（病毒、蠕虫、特洛伊木马）的特殊打包程序进行打包。Kaspersky Endpoint Security 会扫描 SFX（自解压）存档中的解包工具模块。

  为了隐藏恶意软件以避免被反病毒软件检测到，黑客使用特殊的打包程序对其进行打包。卡巴斯基专家已识别出黑客最常使用的解包工具。

排除项

此表包含扫描排除项的相关信息。

> 我们建议指定相对路径而不是绝对路径。这不仅允许排除文件系统对象，还允许排除无文件对象。例如，`*\Program Files (x86)\Folder\Subfolder`。

	可以使用以下方法从扫描中排除对象：
	• 指定文件或文件夹的路径。
	• 输入对象哈希。
	• 使用掩码：
	  • `*`（星号）字符代表任意一组字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\*\*.txt` 将包括位于 C: 驱动器的文件夹（但不包括子文件夹）中所有具有 TXT 扩展名的文件的路径。
	  • 两个连续 `*` 字符在文件或文件夹名称中代表任意一组字符（包括空集），包括 `\` 和 `/` 字符（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\**\*.txt` 将包括位于 `Folder` 嵌套子文件夹（除了 `Folder` 本身）中所有带 TXT 扩展名的文件的路径。掩码必须包含至少一个嵌套级别。掩码 `C:\**\*.txt` 不是有效掩码。
	  • `?`（问号）字符代表任意单个字符，但 `\` 和 `/` 字符除外（这两个字符是文件和文件夹路径中的文件和文件夹名称的分隔符）。例如，掩码 `C:\Folder\???.txt` 将包括位于 `Folder` 文件夹中所有带 TXT 扩展名且名称由三个字符构成的文件的路径。
	  您可以在文件或文件夹路径中的任何位置使用掩码。例如，如果您希望扫描范围包括计算机上所有用户账户的下载文件夹，请输入 `C:\Users\*\Downloads\` 掩码。
	  Kaspersky Endpoint Security 支持环境变量
	  使用 Kaspersky Security Center 控制台生成排除项列表时，Kaspersky Endpoint Security 不支持 `%userprofile%` 环境变量。要应用条目到所有用户账户，您可以使用 * 字符（例如，`C:\Users\*\Documents\File.exe`）。无论何时添加新的环境变量，都需要重新启动应用程序。
	• 根据 Kaspersky 百科全书 输入对象类型名称（例如，`Email-Worm`、`Rootkit` 或 `RemoteAdmin`）。您可以使用带有 `?` 字符（取代单个字符）和 * 字符（取代任意数量字符）的掩码。例如，如果 `Client*` 掩码被指定，应用程序从扫描中排除 `Client-IRC`、`Client-P2P` 和 `Client-SMTP` 对象。
	如果管理员在控制台中阻止扫描排除项的配置（"关闭锁"符号）并且本地扫描排除项被禁止（**允许使用本地排除项**复选框被清除），则 Kaspersky Endpoint Security 会在应用程序的用户界面中隐藏扫描排除项的综合列表。

受信任应用程序	此表列出了受信任应用程序，其活动在操作过程中不受 Kaspersky Endpoint Security 监控。 当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。 在 Kaspersky Security Center 控制台上生成受信任应用程序列表时，Kaspersky Endpoint Security 不支持 `%userprofile%` 环境变量。要应用条目到所有用户账户，您可以使用 * 字符（例如，`C:\Users\*\Documents\File.exe`）。无论何时添加新的环境变量，都需要重新启动应用程序。 "应用程序控制"组件控制每个应用程序的启动，不管该应用程序是否包括在受信任应用程序表中。 如果管理员在控制台中阻止受信任应用程序的配置（"关闭锁"符号）并且本地受信任应用程序被禁止（**允许使用本地受信任应用程序**复选框被清除），则 Kaspersky Endpoint Security 会在应用程序的用户界面中隐藏受信任应用程序的综合列表。
继承时合并值 *（仅在 Kaspersky Security Center 控制台可用）*	这将合并 Kaspersky Security Center 父策略和子策略中的扫描排除项和受信任应用程序列表。要合并列表，子策略必须被配置为继承 Kaspersky Security Center 的父策略设置。 如果该复选框被选中，Kaspersky Security Center 父策略中的列表项目显示在子策略。这样，您可以为整个组织创建受信任应用程序的统一列表。 子策略中继承的列表项目无法被删除或编辑。在继承过程中合并的扫描排除项列表项目和受信任应用程序列表项目仅在父策略中可以被删除和编辑。您可以添加、编辑或删除较低级别策略中的列表项目。 如果子策略和父策略中的列表项目匹配，这些项目被显示为父策略中的相同项目。 如果未选中该复选框，则在继承 Kaspersky Security Center 策略设置时不会合并列表项。 此功能还允许合并策略配置文件中的列表。要合并列表，请在最高优先级的配置文件中启用从较低优先级的配置文件继承设置。有关策略配置文件属性的详细信息，请参阅 Kaspersky Security Center 帮助。

允许使用本地排除项 / 允许使用本地受信任应用程序 *（仅在 Kaspersky Security Center 控制台可用）*	*本地排除项和本地受信任应用程序（本地受信任域）* – 用户为特定计算机在 Kaspersky Endpoint Security 中定义的对象和应用程序列表。Kaspersky Endpoint Security 不监控受信任域中的对象和应用程序。这样，除了策略中的常规受信任域，用户可以创建他们自己的本地排除项和受信任应用程序列表。 如果该复选框被选中，用户可以创建扫描排除项本地列表和受信任应用程序本地列表。管理员可以使用 Kaspersky Security Center 在计算机属性中查看、添加、编辑或删除列表项目。 如果复选框被清空，用户仅可以访问策略中生成的扫描排除项和受信任应用程序常规列表。
EDR (KATA) / NDR (KATA) 遥测 *（仅在 Kaspersky Security Center 控制台可用）*	此表包含 EDR 遥测排除项的相关信息。
KUMA 遥测 *（仅在 Kaspersky Security Center 控制台可用）*	要发送到 Kaspersky Unified Monitoring and Analysis Platform (KUMA) 的事件列表。Kaspersky Endpoint Security 在以下模式下工作： • "**发送所有事件**"。在此模式下，应用程序会发送 Windows 日志中的所有事件（添加到排除规则的事件除外）。 • "**仅发送选定的事件**"。在此模式下，应用程序仅发送包含规则中添加的事件。
受信任的系统证书存储	如果受信任的系统证书存储之一被选择，Kaspersky Endpoint Security 从扫描排除使用受信任数字签名签署的应用程序。Kaspersky Endpoint Security 自动分配此类应用程序到"**受信任**"组。 如果**不使用**被选择，Kaspersky Endpoint Security 扫描应用程序而不考虑其是否具有数字签名。Kaspersky Endpoint Security 会将应用程序放置在某个信任组中，具体取决于该应用程序可能对计算机造成的危险级别。

应用程序设置

您可以配置应用程序的以下常规设置：

- 操作模式
- 自我保护
- 性能
- 调试信息
- 应用设置时的计算机状态

应用程序设置

参数	描述
在计算机开启时启动应用程序(建议)	选中该选项后，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。 清除该选项后，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。
使用高级清除技术(需要大量计算机资源)	通常情况下，Kaspersky Endpoint Security 会在计算机被感染之前终止检测到的恶意软件。高级清除技术可保护计算机免受已活动的恶意软件（活动感染）的侵害，从而最大限度地降低数据丢失和威胁扩散的风险。 如果启用此技术，当检测到恶意活动时，Kaspersky Endpoint Security 会显示弹出通知。在该通知中，Kaspersky Endpoint Security 将提供用户执行计算机高级清除的选项。用户批准此操作后，Kaspersky Endpoint Security 将消除威胁，然后重新启动计算机。高级清除技术会占用相当多的计算资源，这可能会降低其他应用程序的运行速度。 当应用程序正在检测活动感染时，某些操作系统功能可能不可用。高级清除完成并重新启动计算机后，操作系统的可用性将恢复。 如果 Kaspersky Endpoint Security 安装在运行 Windows for Servers 的计算机上，Kaspersky Endpoint Security 不显示通知。因此，您无法选择操作以清除活动威胁。要清除威胁，您需要在应用程序设置中启用高级清除技术以及在"*恶意软件扫描*"任务设置中立即启动高级清除。然后您需要启动"*恶意软件扫描*"任务。

参数	描述
将 Kaspersky Security Center 用作代理服务器以进行激活 *（仅在 Kaspersky Security Center 控制台可用）*	如果选中此复选框，应用程序将使用 Kaspersky Security Center 管理服务器作为连接到激活服务器的代理服务器。当您使用激活码在无法访问互联网的隔离网段中激活应用程序时，这是必要的。如果您正使用密钥文件激活应用程序，不需要互联网访问。
启用自我保护	如果启用此功能，Kaspersky Endpoint Security 可避免修改或删除硬盘驱动器中的应用程序文件、内存进程和系统注册表中的条目。
阻止应用程序服务的外部管理	如果禁用此功能，Kaspersky Endpoint Security 不允许使用第三方应用程序（如 CMD）管理应用程序服务。当有使用第三方应用程序管理应用程序服务的尝试时，则有通知显示在 Microsoft Windows 任务栏，位于应用程序图标上方（除非通知服务被用户禁用）。 您只能在不支持 AM-PPL 技术的计算机或禁用该技术的计算机上允许对应用程序服务进行外部管理。
使用电池供电时推迟计划任务	如果选中此复选框，则当计算机使用电池供电时，将启用节能模式。Kaspersky Endpoint Security 延迟计划任务。如果需要，您可以手动启动扫描和更新任务。 启用节能模式且计算机使用电池运行时，即使计划了以下任务，以下任务也不会运行： • *全盘扫描* • *关键区域扫描* • *自定义扫描* • *应用程序完整性检查* • *IOC 扫描* • *数据库和应用程序模块更新*（仅限补丁） 只有当笔记本电脑使用电池供电且电池电量低于 30% 时，应用程序才会跳过计划的数据库更新。 在其他所有情况下，无论笔记本电脑是连接电源还是使用电池供电，也无论应用程序是否处于节能模式，Kaspersky Endpoint Security软件都会按计划更新数据库。
为其他应用程序让出资源	Kaspersky Endpoint Security 在扫描计算机时消耗计算机资源可能会增加 CPU 和硬盘驱动器子系统的负载。这可能会减慢其他应用程序的速度。为了优化性能，Kaspersky Endpoint Security 提供了*一种将资源传输到其他应用程序的模式*。在这种模式下，当 CPU 负载高时，操作系统可以降低 Kaspersky Endpoint Security 扫描任务线程的优先级。这允许将操作系统资源重新分配给其他应用程序。因此，扫描任务将获得更少的 CPU 时间。因此，Kaspersky Endpoint Security 将需要更长的时间来扫描计算机。默认情况下，程序已配置为允许其他应用程序使用资源。
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。 如果选中该复选框，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。 默认下，复选框被清除。
启用转储写入	如果选择该复选框，Kaspersky Endpoint Security 将在崩溃时写入转储文件。 如果清除该复选框，Kaspersky Endpoint Security 将不再写入转储。应用程序也会从计算机硬盘驱动器中删除现有的转储文件。
启用转储和跟踪文件保护	如果选中该复选框，本地管理员和系统管理员以及启用了转储写入的用户可以访问转储文件。只有系统和本地管理员可以访问跟踪文件。 如果清空该复选框，任何用户可以访问转储文件和跟踪文件。
应用设置时的计算机状态 *（仅在 Kaspersky Security Center 控制台可用）*	应用策略或执行任务出错时，安装了 Kaspersky Endpoint Security 的客户端计算机的状态在 Web 控制台中的显示设置。有以下状态可用：*正常*、*警告*和*严重*。
安装更新而不重启计算机	在不重新启动计算机的情况下升级应用程序可以确保服务器的不间断运行。 从 11.10.0 版开始，无需重新启动即可升级应用程序。要升级应用程序的早期版本，必须重新启动计算机。 从版本 11.11.0 版开始，您无需重新启动计算机即可执行以下操作： • 安装补丁 • 更改应用程序组件集 • 在 Kaspersky Security for Windows Server 之上安装 Kaspersky Endpoint Security 参数的默认值因操作系统类型而异。如果应用程序安装在工作站上，则禁用在不重新启动的情况下升级应用程序选项。如果应用程序安装在服务器上，则启用在不重新启动的情况下升级应用程序选项。

参数	描述
与远程管理软件的兼容性 *（仅在 Kaspersky Security Center 控制台可用）*	如果将 Kaspersky Endpoint Security 与远程管理工具（RAT）一起使用会导致问题，您可以启用兼容模式。这些问题可能与 RAT 与应用程序“Secure Desktop”功能不兼容有关。此功能的目的是确认可能降低计算机安全级别的操作。此功能允许应用程序显示与其他进程隔离的确认对话框。此功能使用提升的权限来保护请求。这样，只有用户才能确认操作，而恶意软件无法确认。 如果选中此选项，则启用 RAT 兼容模式。应用程序会显示一个没有此功能的确认对话框。这可能降低计算机的安全级别。如果 Kaspersky Endpoint Security 不会导致您的 RAT 出现问题，我们不建议启用兼容模式。 如果清除该选项，则禁用 RAT 兼容模式。默认下，复选框被清除。 示例：在 RemoteApp 模式下使用浏览器时，Kaspersky Endpoint Security 在访问具有不受信任证书的网站时可能不会显示确认窗口，因为 RemoteApp 不支持应用程序的安全桌面功能。这可能会导致浏览器无响应。为了使浏览器在 RemoteApp 模式下正常工作，您必须启用兼容模式。如果您在使用其他第三方软件时遇到安全桌面功能问题，也可以尝试启用兼容模式。

报告和存储

报告

有关每个 Kaspersky Endpoint Security 组件的操作、数据加密事件、每个扫描任务的性能、更新任务和完整性检查任务以及应用程序的整体操作的信息都记录在报告中。

报告存储在 `C:\ProgramData\Kaspersky Lab\KES.14.1\Report` 文件夹中。

备份

*备份*存储保存在清除过程中删除或修改的文件的副本。*备份副本*是指对文件进行病毒清除或删除前创建的文件副本。文件的备份副本以特定格式保存并且不会带来威胁。

文件的备份副本存储在 `C:\ProgramData\Kaspersky Lab\KES.14.1\QB` 文件夹中。

管理员组中的用户被授予访问该文件夹的完整权限。其账户用于安装 Kaspersky Endpoint Security 的用户被授予该文件夹的有限访问权限。

> Kaspersky Endpoint Security 不提供用于配置文件备份副本的用户访问权限的功能。

隔离

*隔离区*是计算机上的一个特别的本地存储区。用户可以隔离用户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 仅在与 Kaspersky Detection and Response 解决方案集成时使用隔离。在其他情况下，Kaspersky Endpoint Security 将相关文件置于备份中。有关将隔离管理作为解决方案的一部分的详细信息，请参阅 Kaspersky Sandbox 帮助、Kaspersky Endpoint Detection and Response Optimum 帮助、Kaspersky Endpoint Detection and Response Expert 帮助、Kaspersky Anti Targeted Attack Platform 帮助 和 Kaspersky Endpoint Detection and Response Expert (on-premises) 帮助。

隔离只能使用 Web Console 进行配置。您还可以使用 Web Console 管理隔离对象（恢复、删除、添加等）。您可以使用命令行在计算机上本地恢复对象。

Kaspersky Endpoint Security 使用系统帐户 (SYSTEM) 隔离文件。

报告和存储的设置

参数	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。报告的默认最大存储条件为 30 天。在此时间之后，Kaspersky Endpoint Security 将自动删除报告文件中的最早条目。
限制报告文件大小为 (MB)	如果选中该复选框，则最大报告文件大小限制为定义值。默认情况下，最大文件大小数据为 1024 MB。要避免超过最大报告文件大小，当达到最大报告文件大小时，Kaspersky Endpoint Security 将自动删除报告文件中的最早条目。
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。文件的默认最大存储条件为 30 天。最长存储期限到期后，Kaspersky Endpoint Security 将删除备份区中最旧的文件。
限制备份区大小为 (MB)	如果选中该复选框，则最大存储大小限制为定义值。默认情况下，最大大小为 1024 MB。为避免超过最大存储大小，当达到最大存储大小时，Kaspersky Endpoint Security 将自动删除存储中的最早文件。
限制隔离区大小	如果选中该复选框，则最大隔离区大小限制为定义值。默认情况下，最大大小为 1024 MB。当隔离区达到最大大小时，Kaspersky Endpoint Security 将"*隔离区存储空间不足*"事件发送到 Kaspersky Security Center，并在 Windows 事件日志中发布该事件。同时，应用程序停止隔离新对象。您必须手动清空隔离区。
当隔离区存储达到此值时通知(%)	隔离的阈值。例如，您可以将隔离阈值设置为 50%。当隔离区达到阈值时，Kaspersky Endpoint Security 将相应的事件发送到 Kaspersky Security Center，并在 Windows 事件日志中发布该事件。同时，应用程序继续隔离新对象。
到管理服务器的数据传输 *（仅在 Kaspersky Security Center 可用）*	其信息必须发送到管理服务器的客户端计算机上的事件类别。您可以禁用某些数据的传输以优化管理服务器上的磁盘空间。 应用程序发送以下类别的事件： • "**关于隔离区文件**"。您可以在 Kaspersky Security Center 控制台中查看隔离文件的列表，位于"**高级 → 存储库 → 隔离**"文件夹。Kaspersky Endpoint Security 仅在与 Kaspersky Detection and Response 解决方案集成时使用隔离。 • "**关于备份区中的文件**"。您可以在 Kaspersky Security Center 控制台中查看备份文件的列表，位于"**高级 → 存储库 → 备份**"文件夹。 • "**关于未处理的文件**"。您可以在 Kaspersky Security Center 控制台中查看未处理文件的列表，位于"**高级 → 存储库 → 活动威胁**"文件夹。 • "**关于已安装的设备**"。您可以在 Kaspersky Security Center 控制台的"**高级**" → "**存储库**" → "**硬件**"文件夹中查看已连接设备列表。设备列表也可在计算机属性和 Kaspersky Endpoint Security for Windows 策略中找到（"**设备控制**"部分）。 • "**关于已启动的应用程序**"。您可以在 Kaspersky Security Center 控制台中查看可执行文件的列表，位于"**高级 → 应用程序管理 → 可执行文件**"文件夹。可执行文件列表也可在计算机属性中找到。 • "**关于文件加密错误**"。您可以在 Kaspersky Security Center 控制台中查看文件加密错误列表，位于"**高级 → 数据加密和保护 → 加密事件**"文件夹。错误列表也可在计算机属性中找到。 • "**有关自适应异常控制规则状态的报告**"。你可以在 Kaspersky Security Center 控制台中的"**管理服务器**"节点上的"**报告**"选项卡上查看报告。此报告也可在 Kaspersky Endpoint Security for Windows 策略属性（"**自适应异常控制**"部分）中找到。 • "**有关触发的自适应异常控制规则的报告**"。你可以在 Kaspersky Security Center 控制台中的"**管理服务器**"节点上的"**报告**"选项卡上查看报告。此报告也可在 Kaspersky Endpoint Security for Windows 策略属性（"**自适应异常控制**"部分）中找到。 • "**关于威胁发展链**"。您可以在 Kaspersky Security Center Web Console 中的"**监控 → 警报**"部分中查看检测详情。有关威胁发展链的信息由 Kaspersky Endpoint Detection and Response 解决方案使用。

网络设置

您可以配置用于连接到互联网和更新反病毒数据库的代理服务器，选择网络端口监控模式，以及设置加密连接扫描。

参数	描述
限制计量连接的流量	如果选定该复选框，应用程序将在互联网连接受限时限制其网络流量。Kaspersky Endpoint Security 会将高速移动互联网连接识别为受限制连接，将 Wi-Fi 连接识别为无限制连接。 计量网络运行在 Windows 8 或更新版本的计算机上。
注入脚本到 Web 流量从而与网页交互	如果选定该复选框，Kaspersky Endpoint Security 会将网页监听脚本注入网页流量。该脚本确保 Web 控制组件的正常工作。该脚本确保 Web 控制事件的注册。没有该脚本，您无法启用用户互联网活动监控。 Kaspersky 专家建议注入该网页交互脚本到流量以确保 Web 控制的正确操作。
代理服务器设置	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。 为了自动配置代理服务器，Kaspersky Endpoint Security 使用了 WPAD 协议（Web 代理自动发现协议）。如果使用该协议无法确定代理服务器的 IP 地址，则应用程序使用在 Microsoft Internet Explorer 浏览器设置中指定的代理服务器地址。
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。
代理服务器身份验证设置	要验证代理服务器上用于互联网访问的应用程序，您必须输入用户的凭证。Kaspersky Endpoint Security 支持在代理服务器上进行自动身份验证。如果自动身份验证失败，应用程序将提示您输入凭证。 "**不使用身份验证**"。 "**NTLM 身份验证**"。使用当前用户账户进行的 NTLM 身份验证（默认）。 "**使用用户名和密码的 NTLM 身份验证**"。使用手动指定凭证的 NTLM 身份验证。 "**用户名和密码**"。使用手动指定的凭证进行身份验证。 "**自动身份验证**"。 "**Kerberos 身份验证**"。使用当前用户账户进行的 Kerberos 身份验证。 为确保在使用 CNAME 记录作为代理服务器地址时 Kerberos 身份验证正常工作，您必须为每个 CNAME 记录注册一个服务主体名称 (SPN)。 "**使用用户名和密码的 Kerberos 身份验证**"。使用手动指定凭证的 Kerberos 身份验证。 如果选择 Kerberos 身份验证，Kaspersky Endpoint Security 可以根据代理服务器设置，使用 Kerberos 或 NTLM 协议执行身份验证。
受监控端口	"**监控所有网络端口**"。在此网络端口监控模式下，保护组件（文件威胁防护、Web 威胁防护和邮件威胁防护）会监控通过任何开放的计算机网络端口传输的数据流。 "**仅监控选定网络端口**"。在该网络端口监控模式中，保护组件监控应用程序的所选端口和所选应用程序的网络活动。通常用于传输电子邮件和网络流量的网络端口的列表按照 Kaspersky 专家的建议进行配置。 "**监控卡巴斯基推荐的列表中的应用程序的所有端口**"。这将使用被 Kaspersky Endpoint Security 监控其网络端口的预定义应用程序列表。例如，该列表包括 Google Chrome、Adobe Reader、Java 和其他应用程序。 "**监控指定应用程序的所有端口**"。这将使用被 Kaspersky Endpoint Security 监控其网络端口的应用程序列表。
加密连接扫描	Kaspersky Endpoint Security 将扫描通过以下协议传输的加密网络流量： • SSL 3.0。 • TLS 1.0、TLS 1.1、TLS 1.2、TLS 1.3。 Kaspersky Endpoint Security 支持以下加密连接扫描模式： • "**不扫描加密连接**"。Kaspersky Endpoint Security 将无法访问地址以 `https://` 开头的网站的内容。 • "**根据保护组件的请求扫描加密连接**"。Kaspersky Endpoint Security 只有在得到文件威胁防护、Web 威胁防护和 Web 控制组件的请求时才扫描加密流量。 • "**始终扫描加密连接**"。即使保护组件被禁用，Kaspersky Endpoint Security 也将扫描加密网络流量。 Kaspersky Endpoint Security 不扫描由禁用了流量扫描的受信任应用程序建立的加密连接。Kaspersky Endpoint Security 不扫描预定义的受信任网站的加密连接。预定义的受信任网站列表由 Kaspersky 专家创建。该列表与应用程序的反病毒数据库一起更新。您仅可以在 Kaspersky Endpoint Security 界面查看预定义的受信任网站列表。您无法在 Kaspersky Security Center 控制台查看列表。

参数	描述
受信任根证书	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。要添加到系统证书存储，您可以使用 Active Directory 组策略。
访问带有不受信任证书的域	• "**允许**"。当访问具有不受信任证书的域时，Kaspersky Endpoint Security 将允许网络连接。 在浏览器中打开具有未受信任证书的域时，Kaspersky Endpoint Security 会显示一个 HTML 页面，其中显示警告和不建议访问该域的原因。用户可以单击 HTML 警告页面中的链接来获取对所请求 Web 资源的访问权限。 如果第三方应用程序或服务与具有不受信任的证书的域建立连接，Kaspersky Endpoint Security 将创建自己的证书来扫描流量。新证书具有"*不信任组*"状态。这对于警告第三方应用程序不受信任的连接是必要的，因为在这种情况下无法显示 HTML 页面，并且连接可以在后台模式下建立。 • "**阻止**"。当访问具有不受信任证书的域时，Kaspersky Endpoint Security 将阻止网络连接。在浏览器中打开具有未受信任证书的域时，Kaspersky Endpoint Security 会显示一个 HTML 页面，其中显示阻止该域的原因。
访问带有加密连接扫描错误的域	• "**阻止**"。如果发生加密连接扫描错误，Kaspersky Endpoint Security 会阻止网络连接。 • "**允许并添加域到排除项**"。在发生加密连接扫描错误时，Kaspersky Endpoint Security 将导致错误的域添加到具有扫描错误的域列表中，并且在访问此域时不监控加密网络流量。您只能在应用程序的本地界面中查看具有加密连接扫描错误的域列表。要清除列表内容，您需要选择"**阻止**"。Kaspersky Endpoint Security 也为加密连接扫描错误生成事件。
阻止 SSL 2.0 连接	如果选中该复选框，应用程序将监控并阻止通过 SSL 2.0 协议建立的网络连接。 如果清除该复选框，应用程序将不会阻止通过 SSL 2.0 协议建立的网络连接。但是，应用程序不会监控通过该协议的网络流量。
阻止 SSL 3.0 连接	如果选中该复选框，应用程序将阻止通过 SSL 3.0 协议建立的网络连接。 如果清除该复选框，应用程序将不会阻止通过 SSL 3.0 协议建立的网络连接。应用程序监控通过该协议的网络流量。应用程序的所有组件均不受限制地运行。
阻止 TLS 1.0 连接	如果选中该复选框，应用程序将阻止通过 TLS 1.0 协议建立的网络连接。 如果清除该复选框，应用程序将不会阻止通过 TLS 1.0 协议建立的网络连接。应用程序监控通过该协议的网络流量。应用程序的所有组件均不受限制地运行。
解密与使用 EV 证书的网站之间的加密连接	EV 证书（Extended Validation Certificate）确认网站的真实性并增强连接的安全性。浏览器在地址栏中使用锁定图标来指示网站具有 EV 证书。浏览器还可能将地址栏的全部或部分填充绿色。 如果选中该复选框，应用程序将解密并监控与使用 EV 证书的网站的加密连接。 如果清除该复选框，应用程序无权访问 HTTPS 流量的内容。为此，应用程序仅基于网址（例如 `https://bing.com`）监控 HTTPS 流量。 如果您第一次打开具有 EV 证书的网站，则无论是否选中该复选框，加密连接都将被解密。
配置受信任地址	这将使用 Kaspersky Endpoint Security 不对其扫描网络连接的网址列表。此种情况下，在 Web 威胁防护、邮件威胁防护和 Web 控制组件正常运行的情况下，Kaspersky Endpoint Security 不扫描受信任网址的 HTTPS 流量。 您可以输入域名或 IP 地址。Kaspersky Endpoint Security 支持使用 `*` 字符在域名中输入掩码。 Kaspersky Endpoint Security 不支持 IP 地址的 `*` 符号。您可以使用子网掩码选择一个 IP 地址范围（例如，198.51.100.0/24）。 例如： • `domain.com` – 该记录包括以下地址：`https://domain.com`、`https://www.domain.com`、`https://domain.com/page123`。该记录不包括子域（例如，`subdomain.domain.com`）。 • `subdomain.domain.com` – 该记录包括以下地址：`https://subdomain.domain.com`、`https://subdomain.domain.com/page123`。该记录不包括 `domain.com` 域。 • `*.domain.com` – 该记录包括以下地址：`https://movies.domain.com`、`https://images.domain.com/page123`。该记录不包括 `domain.com` 域。
配置受信任应用程序	其活动在操作过程中不受 Kaspersky Endpoint Security 监控的应用程序列表。您可以选择 Kaspersky Endpoint Security 不会监控的应用程序活动的类型（例如，不扫描网络流量）。当输入掩码时，Kaspersky Endpoint Security 支持环境变量和 `*` 以及 `?` 字符。
要使用自己的证书存储扫描应用程序中的加密连接，请使用 *（仅在 Kaspersky Endpoint Security 界面可用）*	如果该复选框被清空，应用程序扫描 Mozilla Firefox 浏览器和 Thunderbird 邮件客户端中的加密流量。通过 HTTPS 协议访问一些网站可能被阻止。 要扫描 Mozilla Firefox 浏览器和 Thunderbird 邮件客户端中的流量，您必须"启用加密连接扫描"。如果"加密连接扫描"被禁用，应用程序不扫描 Mozilla Firefox 浏览器和 Thunderbird 邮件客户端中的流量。 应用程序使用 Kaspersky 根证书解密和分析加密流量。您可以选择包含 Kaspersky 根证书的证书存储。 • "**Windows 证书存储(推荐)**"。在 Kaspersky Endpoint Security 安装期间，Kaspersky 根证书被添加到该存储。 • "**自己的证书存储**"。Mozilla Firefox 和 Thunderbird 使用它们自己的证书存储。如果 Mozilla 证书存储被选择，您需要通过浏览器属性手动添加 Kaspersky 根证书到该存储。

界面

您可以配置应用程序界面的设置。

界面设置

参数	描述
用户交互 *（仅在 Kaspersky Security Center 控制台可用）*	"**显示简化界面**"。在客户端计算机上，主应用程序窗口不可访问，只有 Windows 通知区域中的图标可用。在该图标的上下文菜单中，用户可以使用 Kaspersky Endpoint Security 执行有限数量的操作。Kaspersky Endpoint Security 也仅在应用程序图标上方显示需要用户操作的通知。 "**显示用户界面**"。在客户端计算机上，Kaspersky Endpoint Security 的主窗口和 Windows 通知区域中的图标均可用。在该图标的上下文菜单中，用户可以使用 Kaspersky Endpoint Security 执行操作。Kaspersky Endpoint Security 还会在应用程序图标上方显示通知。 "**隐藏应用程序活动监控区域**"。在客户端计算机上，在 Kaspersky Endpoint Security 的主窗口中，**应用程序活动监控**按钮不可用。*应用程序活动监控器*是一个用于实时查看用户计算机应用程序活动信息的工具。 "**不显示用户界面**"。在客户端计算机上，不显示 Kaspersky Endpoint Security 操作的迹象。Windows 通知区域中的图标和通知不可用。
配置通知	该表包含在组件、任务或整个应用程序操作过程中可能发生的具有不同重要级别的事件的相关通知的设置。Kaspersky Endpoint Security 将在屏幕上显示这些事件的通知，通过电子邮件发送它们或者在日志中记录它们。
配置电子邮件通知	SMTP 服务器设置，用于发送有关应用程序运行期间注册的事件的通知。 默认情况下，Kaspersky Endpoint Security 使用来自 Kaspersky Security Center 的电子邮件通知设置。有关电子邮件通知设置的详细信息，请参阅 Kaspersky Security Center 帮助。 如果您需要配置单个电子邮件通知，您可以编辑以下设置： • "**发件人邮件地址**"。发件人的电子邮件地址。不建议使用不存在的地址。 • "**SMTP 服务器**"。您组织的电子邮件服务器的一个或多个地址（例如，`mail.company.com`）。您可以输入 IP 地址（IPv4 或 IPv6）。 要在 SMTP 服务器上验证用户，请在相应字段中输入发件人凭据。要测试电子邮件通知，您可以发送测试消息。 • "**收件人邮件地址**"。应用程序将向其发送通知的收件人的电子邮件地址。 • "**发送方式**"。电子邮件通知的发送模式。Kaspersky Endpoint Security 可以在事件发生时立即发送消息；或者，它可以遵循预先配置的时间表。
在通知区域显示应用程序状态	使 Kaspersky Endpoint Security 图标在 Microsoft Windows 任务栏通知区域中发生变化（ 或 ）并生成弹出通知的应用程序事件的类别。
本地反恶意软件数据库状态通知	应用程序使用的反病毒数据库过期的通知设置。
密码保护	如果打开切换按钮，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。
用户支持 / 网络资源链接 *（仅在 Kaspersky Security Center 控制台可用）*	Web 资源链接列表，包含有关 Kaspersky Endpoint Security 技术支持的信息。所添加的链接显示在 Kaspersky Endpoint Security 本地界面的"**支持**"窗口中，而不是标准链接。
用户支持 / 描述 *（仅在 Kaspersky Security Center 控制台可用）*	Kaspersky Endpoint Security 本地界面的"**支持**"窗口中显示的消息。

管理设置

您可以保存当前 Kaspersky Endpoint Security 设置到文件并使用它们快速配置其他计算机上的应用程序。您也可以在通过带有安装包的 Kaspersky Security Center 部署应用程序时使用配置文件。您可以随时恢复默认设置。

应用程序配置管理设置仅在 Kaspersky Endpoint Security 界面可用。

应用程序配置管理设置

设置	描述
导入	以 CFG 格式获取应用程序设置并应用它们。
导出	以 CFG 格式将当前应用程序设置保存至文件。
恢复	您可以随时恢复卡巴斯基建议的应用程序设置。在设置被恢复后，应用程序将为所有保护组件设置"**建议**"安全级别。

更新数据库和程序软件模块

更新 Kaspersky Endpoint Security 的数据库和程序模块可为您的计算机提供最新保护。新病毒和其他类型的恶意软件每天都在全世界出现。Kaspersky Endpoint Security 数据库包含有关威胁的信息和使其失效的方法。要快速检测到威胁，建议您定期更新数据库和应用程序模块。

在美国境内，本软件中将不再提供更新功能（包括提供反病毒签名更新和代码库更新）。

常规更新要求具有已生效的授权许可。如果当前没有授权许可，您将只能执行一次更新。

您的计算机必须连接到互联网才能成功下载来自卡巴斯基更新服务器的更新包。默认情况下，系统将自动确定互联网连接设置。如果您使用代理服务器，则需要配置代理服务器设置。

通过 HTTPS 协议下载更新。当无法通过 HTTPS 协议下载更新时，也可以通过 HTTP 协议下载。

当执行更新时，以下对象将下载并安装到您的计算机中：

- Kaspersky Endpoint Security 数据库。该程序使用包含病毒签名和其他威胁签名以及清除方法的数据库实现计算机保护。当搜索并为受感染文件清除时，保护组件将使用此信息。数据库将不断更新应对它们的方法和新威胁记录。因此，我们建议您定期更新数据库。

  除了 Kaspersky Endpoint Security 数据库之外，系统也会更新已启用程序组件以拦截网络流量的网络驱动程序。

- 程序模块。除了 Kaspersky Endpoint Security 数据库，您也可以更新程序模块。更新程序模块可以修补 Kaspersky Endpoint Security 中的漏洞、添加新功能或增强现有功能。

更新时，您的计算机上的程序模块和数据库将与最新版本更新源进行对比。如果您当前数据库和程序模块与相应的最新版本不同，缺少的更新部分将安装在您的计算机上。

如果数据库过时，更新包可能会很大，这可能会花费更多的互联网流量（最多达几十 MB）。

有关 Kaspersky Endpoint Security 数据库的当前状态的信息显示在主应用程序窗口中，或将光标悬停在通知区域中的应用程序图标上时看到的工具提示中。

有关更新任务运行期间更新结果和所有发生事件的信息将记录在 Kaspersky Endpoint Security 报告中。

如果应用程序正在 Light Agent 模式下运行，更新应用程序数据库和模块时将有特殊考虑。

应用程序模块和数据库更新设置

参数	描述
数据库更新计划	"**自动**"。在该模式下，应用程序将按特定频率检查更新源，以确定新更新软件包的可用性。检查更新软件包的频率在病毒爆发期间会增加，在其他时候会减小。在检测到全新的更新软件包之后，Kaspersky Endpoint Security 会下载并将其安装到您的计算机上。 "**手动**"。使用该更新任务运行模式可以手动启动更新任务。 "**根据计划**"。在该更新任务运行模式下，Kaspersky Endpoint Security 将按照您已经指定的计划运行更新任务。如果选择该更新任务运行模式，您也可以手动启动 Kaspersky Endpoint Security 更新任务。
运行错过的任务	如果选中该复选框，Kaspersky Endpoint Security 将在可能的情况下尽快启动已忽略的任务。任务在某些情况下可能被略过，例如，计算机在启动计划任务时处于关闭状态。当应用程序有机会执行略过的任务时，它会在一定的时间间隔内随机运行任务，以分配计算机上的负载。 如果清除该复选框，Kaspersky Endpoint Security 不会运行已略过的任务。它将按照当前计划运行下一次任务。
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。 如果卡巴斯基更新服务器不可用，Kaspersky Endpoint Security 可以使用备用域来更新其数据库和应用程序软件模块。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"*数据库和应用程序模块更新*"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。 如果应用程序正在 Light Agent 模式下运行，一个 SVM 上的文件夹选为更新源。
运行数据库更新身份	默认情况下，Kaspersky Endpoint Security 使用您用来登陆操作系统的帐户执行更新任务。但是，Kaspersky Endpoint Security 可以从用户没有访问权限的更新源（例如，含有更新包的共享文件夹）进行更新，或者从没有配置过代理服务器身份验证的更新源进行更新。在应用程序设置中，您可以指定一个拥有以上权限的用户，然后使用该用户帐户开始 Kaspersky Endpoint Security 更新任务。
下载应用程序模块更新	下载应用程序模块更新和应用程序数据库更新。 如果选中此选框，Kaspersky Endpoint Security 将会向用户发送关于可用应用程序模块更新的通知，并在运行更新任务时将应用程序模块更新包含到更新软件包中。应用程序模块更新的方式取决于以下设置： • "**安装关键和批准的更新**"。如果选择此选项，当有应用程序模块更新可用时，仅在这些更新通过应用程序界面或在 Kaspersky Security Center 一侧被本地批准后，Kaspersky Endpoint Security 才会自动安装关键更新和所有其他应用程序模块更新。 • "**仅安装批准的更新**"。如果选择该选项，当有应用程序模块更新可用时，仅在这些更新通过应用程序界面或在 Kaspersky Security Center 一侧被本地批准后，Kaspersky Endpoint Security 才会安装它们。默认情况下已选定该选项。 如果不选中此选框，Kaspersky Endpoint Security 将不会向用户发送关于可用应用程序模块更新的通知，并且在运行更新任务时不将应用程序模块更新包含的更新软件包中。 如果应用程序模块更新需要查看和接受最终用户授权许可协议，应用程序将在最终用户授权许可协议被接受后，安装更新。 默认选中该复选框。

参数	描述
将更新复制到文件夹	如果选择该复选框，Kaspersky Endpoint Security 会将更新软件包复制到该复选框下指定的共享文件夹。然后，您的本地网中其他计算机可从这一共享文件夹中接收更新包。这可以减少互联网流量，因为更新软件包仅下载一次。默认情况下指定了以下文件夹：`C:\ProgramData\Kaspersky Lab\KES.14.1\Update distribution\`。
运行更新的代理服务器 *（仅在 Kaspersky Endpoint Security 界面可用）*	客户端计算机用户访问互联网的代理服务器设置，用以更新应用程序模块和数据库。 为了自动配置代理服务器，Kaspersky Endpoint Security 使用 WPAD 协议（Web Proxy Auto-Discovery Protocol）。如果使用该协议无法确定代理服务器的 IP 地址，则 Kaspersky Endpoint Security 使用在 Microsoft Internet Explorer 浏览器设置中指定的代理服务器地址。
对本地地址不使用代理服务器 *（仅在 Kaspersky Endpoint Security 界面可用）*	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。

附录 2.应用程序信任组

Kaspersky Endpoint Security 会将计算机上启动的所有应用程序归类到信任组中。系统将根据应用程序给操作系统造成威胁的级别将其归类到信任组中。

受信任组包括下列组：

- “**受信任**”。该组包括满足以下一个或多个条件的应用程序：
  - 应用程序由受信任的生产厂商进行数字签名。
  - 应用程序记录在卡巴斯基安全网络的受信任应用程序数据库中。
  - 用户已将应用程序放置在“*受信任*”组中。

  不禁止这些应用程序执行任何操作。
- “**低限制**”。该组包括满足以下条件的应用程序：
  - 应用程序未由受信任的生产厂商进行数字签名。
  - 应用程序未记录在卡巴斯基安全网络的受信任应用程序数据库中。
  - 用户已将应用程序放置在“*低限制*”组中。

  此类应用程序在访问操作系统资源时受到的限制最少。
- “**高限制**”。该组包括满足以下条件的应用程序：
  - 应用程序未由受信任的生产厂商进行数字签名。
  - 应用程序未记录在卡巴斯基安全网络的受信任应用程序数据库中。
  - 用户已将应用程序放置在“*高限制*”组中。

  此类应用程序在访问操作系统资源时受到较高的限制。

- “**不信任**”。该组包括满足以下条件的应用程序：
  - 应用程序未由受信任的生产厂商进行数字签名。
  - 应用程序未记录在卡巴斯基安全网络的受信任应用程序数据库中。
  - 用户已将应用程序放置在“*不信任*”组中。

  对于此类应用程序，所有操作都将被阻止。

附录 3.快速可移动驱动器扫描的文件扩展名

com – 大小不超过 64 KB 的应用程序的可执行文件

exe – 可执行文件或自解压存档

sys – Microsoft Windows 系统文件

prg – dBase™ 程序文字、Clipper 或 Microsoft Visual FoxPro®，或 WAVmaker 程序

bin – 二进制文件

bat – 批文件

cmd – Microsoft Windows NT 的命令文件（与 DOS 批处理文件类似）、OS/2

dpl – 压缩的 Borland Delphi 库

dll – 动态链接库

scr – Microsoft Windows 屏保

cpl – Microsoft Windows 控制面板模块

ocx – Microsoft OLE（对象链接和嵌入）对象

tsp – 以分时模式运行的程序

drv – 设备驱动程序

vxd – Microsoft Windows 虚拟设备驱动程序

pif – 程序信息文件

lnk – Microsoft Windows 链接文件

reg – Microsoft Windows 系统注册表键文件

ini – 包含 Microsoft Windows、Windows NT 和某些应用程序配置数据的配置文件

cla – Java 类

vbs – Visual Basic® 脚本

vbe – BIOS 视频扩展程序

js, jse – JavaScript source text

htm – 超文本文档

htt – Microsoft Windows 超文本标头

hta – Microsoft Internet Explorer® 超文本程序

asp – Active Server Pages 脚本

chm – 编撰的 HTML 文件

pht – 带有 PHP 脚本的 HTML 文件

php – 集成到 HTML 文件的脚本

wsh – Microsoft Windows Script Host 文件

wsf – Microsoft Windows 脚本

the – Microsoft Windows 95 桌面壁纸文件

hlp – Win 帮助文件

msg – Microsoft Mail 邮件

plg – 邮件

mbx – 已保存的 Microsoft Office Outlook 邮件

doc* – Microsoft Office Word 文档，例如：doc（Microsoft Office Word 文档）、docx（带 XML 支持的 Microsoft Office Word 2007 文档）、docm（带宏支持的 Microsoft Office Word 2007 文档）

dot* – Microsoft Office Word 文档模块，例如 dot（Microsoft Office Word 文档模板）、dotx（Microsoft Office Word 2007 文档模板）、dotm（带宏支持的 Microsoft Office Word 2007 文档模板）

fpm – 数据库程序，Microsoft Visual FoxPro 启动文件

rtf – 富文本格式文档

shs – Windows Shell Scrap Object Handler 片段

dwg – AutoCAD® 图纸数据库

msi – Microsoft Windows Installer 安装包

otm – 适用于 Microsoft Office Outlook 的 VBA 项目

pdf – Adobe Acrobat 文档

swf – Shockwave® Flash 数据包文档

jpg, jpeg – 压缩图像格式

emf – 增强元文件格式文件；

ico – 对象图标文件

ov? – Microsoft Office Word 可执行文件

xl* – Microsoft Office Excel 文档和文件，例如：xla 对应 Microsoft Office Excel、xlc 对应图表、xlt 对应文档模板、xlsx 对应 Microsoft Office Excel 2007 工作簿、xltm 对应支持宏的 Microsoft Office Excel 2007 工作簿、xlsb 对应二进制格式（非 XML）的 Microsoft Office Excel 2007 工作簿、xltx 对应于 Microsoft Office Excel 2007 模板、xlsm 对应于支持宏的 Microsoft Office Excel 2007 模板、xlam 对应于支持宏的 Microsoft Office Excel 2007 插件

pp* – Microsoft Office PowerPoint® 文档和文件，例如：pps 代表 Microsoft Office PowerPoint 幻灯片、ppt 代表幻灯片、pptx 代表 Microsoft Office PowerPoint 2007 幻灯片、pptm 代表支持宏的 Microsoft Office PowerPoint 2007 幻灯片、potx 代表 Microsoft Office PowerPoint 2007 幻灯片模板、potm 代表支持宏的 Microsoft Office PowerPoint 2007 幻灯片、ppsx 代表 Microsoft Office PowerPoint 2007 幻灯片、ppsm 代表支持宏的 Microsoft Office PowerPoint 2007 幻灯片、ppam 代表支持宏的 Microsoft Office PowerPoint 2007 插件

md* – Microsoft Office Access® 文档和文件，例如：mda 代表 Microsoft Office Access 工作组，mdb 代表数据库

sldx – Microsoft PowerPoint 2007 幻灯片

sldm – 支持宏的 Microsoft PowerPoint 2007 幻灯片

thmx – Microsoft Office 2007 主题

附录 4.邮件威胁防护附件过滤的文件类型

请注意文件的实际格式可能不匹配其文件名扩展名。

如果您启用了电子邮件附件过滤，则“邮件威胁防护”组件可能重命名或删除带有以下扩展名的文件：

com – 大小不超过 64 KB 的应用程序的可执行文件

exe – 可执行文件或自解压存档

sys – Microsoft Windows 系统文件

prg – dBase™ 程序文字、Clipper 或 Microsoft Visual FoxPro®，或 WAVmaker 程序

bin – 二进制文件

bat – 批文件

cmd – Microsoft Windows NT 的命令文件（与 DOS 批处理文件类似）、OS/2

dpl – 压缩的 Borland Delphi 库

dll – 动态链接库

scr – Microsoft Windows 屏保

cpl – Microsoft Windows 控制面板模块

ocx – Microsoft OLE（对象链接和嵌入）对象

tsp – 以分时模式运行的程序

drv – 设备驱动程序

vxd – Microsoft Windows 虚拟设备驱动程序

pif – 程序信息文件

lnk – Microsoft Windows 链接文件

reg – Microsoft Windows 系统注册表键文件

ini – 包含 Microsoft Windows、Windows NT 和某些应用程序配置数据的配置文件

cla – Java 类

vbs – Visual Basic® 脚本

vbe – BIOS 视频扩展程序

js, jse – JavaScript source text

htm – 超文本文档

htt – Microsoft Windows 超文本标头

hta – Microsoft Internet Explorer® 超文本程序

asp – Active Server Pages 脚本

chm – 编撰的 HTML 文件

pht – 带有 PHP 脚本的 HTML 文件

php – 集成到 HTML 文件的脚本

wsh – Microsoft Windows Script Host 文件

wsf – Microsoft Windows 脚本

the – Microsoft Windows 95 桌面壁纸文件

hlp – Win 帮助文件

msg – Microsoft Mail 邮件

plg – 邮件

mbx – 已保存的 Microsoft Office Outlook 邮件

doc* – Microsoft Office Word 文档，例如：doc（Microsoft Office Word 文档）、docx（带 XML 支持的 Microsoft Office Word 2007 文档）、docm（带宏支持的 Microsoft Office Word 2007 文档）

dot* – Microsoft Office Word 文档模块，例如 dot（Microsoft Office Word 文档模板）、dotx（Microsoft Office Word 2007 文档模板）、dotm（带宏支持的 Microsoft Office Word 2007 文档模板）

fpm – 数据库程序，Microsoft Visual FoxPro 启动文件

rtf – 富文本格式文档

shs – Windows Shell Scrap Object Handler 片段

dwg – AutoCAD® 图纸数据库

msi – Microsoft Windows Installer 安装包

otm – 适用于 Microsoft Office Outlook 的 VBA 项目

pdf – Adobe Acrobat 文档

swf – Shockwave® Flash 数据包文档

jpg, jpeg – 压缩图像格式

emf – 增强元文件格式文件；

ico – 对象图标文件

ov? – Microsoft Office Word 可执行文件

xl* – Microsoft Office Excel 文档和文件，例如：xla 对应 Microsoft Office Excel、xlc 对应图表、xlt 对应文档模板、xlsx 对应 Microsoft Office Excel 2007 工作簿、xltm 对应支持宏的 Microsoft Office Excel 2007 工作簿、xlsb 对应二进制格式（非 XML）的 Microsoft Office Excel 2007 工作簿、xltx 对应于 Microsoft Office Excel 2007 模板、xlsm 对应于支持宏的 Microsoft Office Excel 2007 模板、xlam 对应于支持宏的 Microsoft Office Excel 2007 插件

pp* – Microsoft Office PowerPoint® 文档和文件，例如：pps 代表 Microsoft Office PowerPoint 幻灯片、ppt 代表幻灯片、pptx 代表 Microsoft Office PowerPoint 2007 幻灯片、pptm 代表支持宏的 Microsoft Office PowerPoint 2007 幻灯片、potx 代表 Microsoft Office PowerPoint 2007 幻灯片模板、potm 代表支持宏的 Microsoft Office PowerPoint 2007 幻灯片、ppsx 代表 Microsoft Office PowerPoint 2007 幻灯片、ppsm 代表支持宏的 Microsoft Office PowerPoint 2007 幻灯片、ppam 代表支持宏的 Microsoft Office PowerPoint 2007 插件

md* – Microsoft Office Access® 文档和文件，例如：mda 代表 Microsoft Office Access 工作组，mdb 代表数据库

sldx – Microsoft PowerPoint 2007 幻灯片

sldm – 支持宏的 Microsoft PowerPoint 2007 幻灯片

附录 5.与外部服务交互的网络设置

Kaspersky Endpoint Security 和 Kaspersky Security Center 使用 TLS（传输层安全）加密通信通道来配合使用卡巴斯基外部服务。

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)。 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 使用公共 DNS 服务器，则数据处理受相关服务的隐私策略控制。如果您要阻止 Kaspersky Endpoint Security 使用公共 DNS 服务器，请联系技术支持以获取专用补丁。
`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。

设置，用于加密

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)。

附录 6.应用程序事件

有关每个 Kaspersky Endpoint Security 组件的操作、数据加密事件、每个恶意软件扫描任务的完成、更新任务和完整性检查任务以及应用程序的整体操作的信息都记录在 Kaspersky Security Center 事件日志和 Windows 事件日志中。

Kaspersky Endpoint Security 可生成以下类型的事件：一般事件和特别事件。特别事件仅由 Kaspersky Endpoint Security for Windows 创建。特别事件具有简单 ID，例如 `000000cb`。特别事件包含以下所需参数：

- `GNRL_EA_DESCRIPTION` 是事件的内容。
- `GNRL_EA_ID` 是事件的服务 ID。
- `GNRL_EA_SEVERITY` 是事件的状态。`1` – *信息*, `2` – *警告*, `3` – *功能失败*, `4` – *严重*。
- `EVENT_TYPE_DISPLAY_NAME` 是事件的标题。
- `TASK_DISPLAY_NAME` 是启动事件的应用程序组件的名称。

一般事件可以由 Kaspersky Endpoint Security for Windows 和其他 Kaspersky 应用程序创建（例如，Kaspersky Security for Windows Server）。一般事件具有更复杂的 ID，例如 `GNRL_EV_VIRUS_FOUND`。除了必需的设置外，一般事件还包含高级设置。

事件在服务器上的存储时长

严重

授权许可已过期

状态	⊘
组件	系统审计
Windows 事件 ID	`201`
Kaspersky Security Center 事件 ID	`GNRL_EV_LICENSE_EXPIRATION`
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

授权许可即将到期

状态	⊘
组件	系统审计
Windows 事件 ID	`203`
Kaspersky Security Center 事件 ID	`000000cb`
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

数据库丢失或损坏

状态	!
组件	系统审计
Windows 事件 ID	206
Kaspersky Security Center 事件 ID	000000ce
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

数据库严重过期

状态	!
组件	系统审计
Windows 事件 ID	207
Kaspersky Security Center 事件 ID	000000cf
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

应用程序自动运行已禁用

状态	!
组件	系统审计
Windows 事件 ID	209
Kaspersky Security Center 事件 ID	000000d1
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

激活错误

状态	!
组件	系统审计
Windows 事件 ID	229
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

检测到活动威胁。应该启动高级清除

状态	!
组件	系统审计
Windows 事件 ID	231
Kaspersky Security Center 事件 ID	000000e7
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

KSN 服务器不可用

状态	!
组件	系统审计
Windows 事件 ID	2023
Kaspersky Security Center 事件 ID	000007e7
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

隔离区存储空间不足

状态	!
组件	系统审计
Windows 事件 ID	343
Kaspersky Security Center 事件 ID	00000157
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

对象未从隔离区中恢复

状态	!
组件	系统审计
Windows 事件 ID	346
Kaspersky Security Center 事件 ID	0000015a
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

对象未从隔离区中删除

状态	!
组件	系统审计
Windows 事件 ID	348
Kaspersky Security Center 事件 ID	0000015c
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

应用程序建立了与具有不受信任证书的网站的连接

状态	!
组件	系统审计
Windows 事件 ID	57
Kaspersky Security Center 事件 ID	00000039
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

验证加密连接失败。域已被添加到排除项列表

状态	!
组件	系统审计
Windows 事件 ID	60
Kaspersky Security Center 事件 ID	0000003c
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

检测到恶意对象 (本地数据库)

状态	!
组件	文件威胁防护 Web 威胁防护 邮件威胁防护 AMSI 保护 主机入侵防御 行为检测 反加密勒索 漏洞利用防御 恶意软件扫描
Windows 事件 ID	302
Kaspersky Security Center 事件 ID	GNRL_EV_VIRUS_FOUND
事件参数	• GNRL_EA_PARAM_1 是对象的哈希 (SHA256)。 • GNRL_EA_PARAM_2 是对象的名称。 当检测到共享文件夹的外部加密时，应用程序会显示目标文件的路径。 • GNRL_EA_PARAM_5 是威胁的名称，与 Kaspersky 分类法一致，例如 EICAR-Test-File。 • GNRL_EA_PARAM_7 是会话用户的名称。 • GNRL_EA_PARAM_8 是威胁类型（type）。 • GNRL_EA_PARAM_9 是检测到的对象的附加信息： 应用程序组件 (engine)。 威胁检测技术 (method)。 卡巴斯基私人安全网络检测到的威胁（blacklist）：true 或者 false。 EDR 版本。 EDR 中的威胁标识符。 对象的 MD5 哈希。
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

检测到恶意对象 (KSN)

状态	!
组件	文件威胁防护 Web 威胁防护 邮件威胁防护 AMSI 保护 主机入侵防御 行为检测 反加密勒索 漏洞利用防御 恶意软件扫描
Windows 事件 ID	302

Kaspersky Security Center 事件 ID	GNRL_EV_VIRUS_FOUND_BY_KSN
事件参数	• GNRL_EA_PARAM_1 是对象的哈希 (SHA256)。 • GNRL_EA_PARAM_2 是对象的名称。 • GNRL_EA_PARAM_5 是威胁的名称，与 Kaspersky 分类法一致，例如 EICAR-Test-File。 • GNRL_EA_PARAM_7 是会话用户的名称。 • GNRL_EA_PARAM_8 是威胁类型（type）。 • GNRL_EA_PARAM_9 是检测到的对象的附加信息： 应用程序组件 (engine)。 威胁检测技术 (method)。 卡巴斯基私人安全网络检测到的威胁（blacklist）：true 或者 false。 EDR 版本。 EDR 中的威胁标识符。 对象的 MD5 哈希。
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

无法清除

状态	!
组件	文件威胁防护 邮件威胁防护 主机入侵防御 行为检测 反加密勒索 恶意软件扫描
Windows 事件 ID	312
Kaspersky Security Center 事件 ID	GNRL_EV_OBJECT_NOTCURED
事件参数	• GNRL_EA_PARAM_1 是对象的哈希 (SHA256)。 • GNRL_EA_PARAM_2 是对象的名称。 • GNRL_EA_PARAM_5 是威胁的名称，与 Kaspersky 分类法一致，例如 EICAR-Test-File。 • GNRL_EA_PARAM_7 是会话用户的名称。 • GNRL_EA_PARAM_8 是威胁类型（type）。 • GNRL_EA_PARAM_9 是检测到的对象的附加信息： 应用程序组件 (engine)。 威胁检测技术 (method)。 卡巴斯基私人安全网络检测到的威胁（blacklist）：true 或者 false。 EDR 版本。 EDR 中的威胁标识符。 对象的 MD5 哈希。
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

无法删除

状态	!
组件	文件威胁防护 主机入侵防御 行为检测 反加密勒索 恶意软件扫描
Windows 事件 ID	313
Kaspersky Security Center 事件 ID	00000139
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

处理错误

状态	!
组件	文件威胁防护 Web 威胁防护 邮件威胁防护 主机入侵防御 AMSI 保护 恶意软件扫描
Windows 事件 ID	317
Kaspersky Security Center 事件 ID	0000013d
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

进程已终止

状态	!
组件	文件威胁防护 主机入侵防御 行为检测 恶意软件扫描
Windows 事件 ID	452
Kaspersky Security Center 事件 ID	000001c4
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

无法终止进程

状态	!
组件	文件威胁防护 主机入侵防御 行为检测 恶意软件扫描
Windows 事件 ID	453
Kaspersky Security Center 事件 ID	000001c5
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

已阻止危险链接

状态	!
组件	Web 威胁防护
Windows 事件 ID	362
Kaspersky Security Center 事件 ID	GNRL_EV_VIRUS_FOUND_AND_BLOCKED
事件参数	• GNRL_EA_PARAM_2 是对象的路径。 • GNRL_EA_PARAM_5 是根据卡巴斯基分类的对象的名称。 • GNRL_EA_PARAM_7 是会话用户的名称。 • GNRL_EA_PARAM_8 是威胁类型（type）。 • GNRL_EA_PARAM_9 是检测到的对象的附加信息： 应用程序组件（engine）。 威胁检测技术（method）。 私有 KSN 检测到的威胁（blacklist）：true 或者 false。

Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

已打开危险链接

状态	!
组件	Web 威胁防护
Windows 事件 ID	363
Kaspersky Security Center 事件 ID	GNRL_EV_VIRUS_FOUND_AND_REPORTED
事件参数	• GNRL_EA_PARAM_2 是对象的路径。 • GNRL_EA_PARAM_5 是根据卡巴斯基分类的对象的名称。 • GNRL_EA_PARAM_7 是会话用户的名称。 • GNRL_EA_PARAM_8 是威胁类型（type）。 • GNRL_EA_PARAM_9 是检测到的对象的附加信息： 应用程序组件（engine）。 威胁检测技术（method）。 私有 KSN 检测到的威胁（blacklist）：true 或者 false。
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

检测到先前打开的危险链接

状态	!
组件	Web 威胁防护
Windows 事件 ID	1201
Kaspersky Security Center 事件 ID	GNRL_EV_VIRUS_FOUND_AND_PASSED
事件参数	• GNRL_EA_PARAM_2 是对象的路径。 • GNRL_EA_PARAM_5 是根据卡巴斯基分类的对象的名称。 • GNRL_EA_PARAM_7 是会话用户的名称。 • GNRL_EA_PARAM_8 是威胁类型（type）。 • GNRL_EA_PARAM_9 是检测到的对象的附加信息： 应用程序组件（engine）。 威胁检测技术（method）。 私有 KSN 检测到的威胁（blacklist）：true 或者 false。
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

进程操作已阻止

状态	!
组件	自适应异常控制
Windows 事件 ID	2200
Kaspersky Security Center 事件 ID	GNRL_EV_ADSEC_DETECT
事件参数	• GNRL_EA_PARAM_1 是自适应异常控制规则名称。 • GNRL_EA_PARAM_2 是启发式规则 ID。 • GNRL_EA_PARAM_3 是会话用户的名称。 • GNRL_EA_PARAM_4 是源进程。 • GNRL_EA_PARAM_5 是源对象。 • GNRL_EA_PARAM_6 是目标进程。 • GNRL_EA_PARAM_7 是目标对象。 • GNRL_EA_PARAM_8 是检测到的对象的附加信息： 源进程/对象和目标进程/对象的校验和。 进程被阻止（verdict_type）：true或false。 用户安全 ID（SID）.

Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

键盘未授权

状态	ⓘ
组件	BadUSB 攻击防护
Windows 事件 ID	`2051`
Kaspersky Security Center 事件 ID	`00000803`
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

AMSI 请求被阻止

状态	ⓘ
组件	AMSI 保护
Windows 事件 ID	`2200`
Kaspersky Security Center 事件 ID	`00000898`
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

网络活动已阻止

状态	ⓘ
组件	防火墙
Windows 事件 ID	`602`
Kaspersky Security Center 事件 ID	`00000329`
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

检测到网络攻击

状态	ⓘ
组件	网络威胁防护
Windows 事件 ID	`651`
Kaspersky Security Center 事件 ID	`GNRL_EV_ATTACK_DETECTED`
事件参数	• `GNRL_EA_PARAM_1` 是攻击的名称。 • `GNRL_EA_PARAM_2` 是协议。 • `GNRL_EA_PARAM_3` 是作为网络攻击源的计算机的 IP 地址。IP 地址以主机的字节顺序表示。例如，`2886729929` 对应于 `172.16.0.201`。 • `GNRL_EA_PARAM_4` 是端口号。 • `GNRL_EA_PARAM_5` 是 IPv6 地址，例如，`12B012B012B012B012B012B012B012B0`。 • `GNRL_EA_PARAM_6` 是网络攻击目标计算机的 IP 地址。IP 地址以主机的字节顺序表示。例如，`2886729929` 对应于 `172.16.0.201`。
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

已禁止应用程序启动

状态	!
组件	应用程序控制
Windows 事件 ID	702
Kaspersky Security Center 事件 ID	GNRL_EV_APPLICATION_LAUNCH_DENIED
事件参数	• GNRL_EA_PARAM_2 是会话用户的名称。 • GNRL_EA_PARAM_3 是手动创建的类别识别符。 • GNRL_EA_PARAM_4 是应用程序类别 ID。 • GNRL_EA_PARAM_5 是应用程序的数字签名信息。 • GNRL_EA_PARAM_6 是应用程序可执行文件的名称（例如，chrome.exe）。 • GNRL_EA_PARAM_7 是可执行文件的路径。 • GNRL_EA_PARAM_8 是对象的哈希 (SHA256)。 • GNRL_EA_PARAM_9 是用户正在试图运行的应用程序的版本。
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

阻止的进程在 Kaspersky Endpoint Security 启动前启动

状态	!
组件	应用程序控制
Windows 事件 ID	710
Kaspersky Security Center 事件 ID	000002c6
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

访问被拒绝(本地数据库)

状态	!
组件	Web 控制
Windows 事件 ID	752
Kaspersky Security Center 事件 ID	GNRL_EV_WEB_URL_BLOCKED
事件参数	• GNRL_EA_PARAM_1 是网址。 • GNRL_EA_PARAM_2 是会话用户的名称。 • GNRL_EA_PARAM_3 是 Web 控制规则名称。
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

访问被拒绝 (KSN)

状态	!
组件	Web 控制
Windows 事件 ID	752
Kaspersky Security Center 事件 ID	GNRL_EV_WEB_URL_BLOCKED_BY_KSN
事件参数	• GNRL_EA_PARAM_1 是网址。 • GNRL_EA_PARAM_2 是会话用户的名称。 • GNRL_EA_PARAM_3 是 Web 控制规则名称。

Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

已禁止对设备执行操作

状态	!
组件	设备控制
Windows 事件 ID	802
Kaspersky Security Center 事件 ID	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
事件参数	• GNRL_EA_PARAM_1 是硬件 ID (HWID)。 • GNRL_EA_PARAM_2 是会话用户的名称。
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

已阻止网络连接

状态	!
组件	设备控制
Windows 事件 ID	809
Kaspersky Security Center 事件 ID	00000329
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

更新组件时出错

状态	!
组件	更新
Windows 事件 ID	1011
Kaspersky Security Center 事件 ID	000003f3
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

分发组件更新时出错

状态	!
组件	更新
Windows 事件 ID	1012
Kaspersky Security Center 事件 ID	000003f4
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

本地更新错误

状态	!
组件	更新
Windows 事件 ID	1014

Kaspersky Security Center 事件 ID	000003f6
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

网络更新错误

状态	ⓘ
组件	更新
Windows 事件 ID	1015
Kaspersky Security Center 事件 ID	000003f7
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

不能同时启动两项任务

状态	ⓘ
组件	更新
Windows 事件 ID	1017
Kaspersky Security Center 事件 ID	000003f9
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

验证应用程序数据库和模块时出错

状态	ⓘ
组件	更新
Windows 事件 ID	1018
Kaspersky Security Center 事件 ID	000003fa
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

与 Kaspersky Security Center 交互时出错

状态	ⓘ
组件	更新
Windows 事件 ID	1019
Kaspersky Security Center 事件 ID	000003fb
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

未更新所有组件

状态	ⓘ
组件	更新
Windows 事件 ID	1021

Kaspersky Security Center 事件 ID	000003fd
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

成功完成更新，更新分发失败

状态	!
组件	更新
Windows 事件 ID	1023
Kaspersky Security Center 事件 ID	000003ff
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

内部任务错误

状态	!
组件	系统审计
Windows 事件 ID	101
Kaspersky Security Center 事件 ID	00000065
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

补丁安装失败

状态	!
组件	更新
Windows 事件 ID	2153
Kaspersky Security Center 事件 ID	00000869
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

补丁回滚失败

状态	!
组件	更新
Windows 事件 ID	2156
Kaspersky Security Center 事件 ID	0000086c
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

应用文件加密/解密规则时出错

状态	!
组件	数据加密
Windows 事件 ID	904

Kaspersky Security Center 事件 ID	00000388
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

文件加密/解密错误

状态	!
组件	数据加密
Windows 事件 ID	912
Kaspersky Security Center 事件 ID	GNRL_EV_ENCRYPTION_ERROR
事件参数	• GNRL_EA_PARAM_1 是文件的路径。 • GNRL_EA_PARAM_2 是错误原因。 • GNRL_EA_PARAM_3 是设备类型。
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

文件访问被阻止

状态	!
组件	数据加密
Windows 事件 ID	940
Kaspersky Security Center 事件 ID	GNRL_EV_ENCRYPTION_DATAACCESS_VIOLATION
事件参数	• GNRL_EA_PARAM_1 是目标对象。 • GNRL_EA_PARAM_2 是会话用户的名称。 • GNRL_EA_PARAM_3 是试图访问该文件的应用程序的可执行文件（例如，chrome.exe）的名称。
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

启用便携模式时出错

状态	!
组件	数据加密
Windows 事件 ID	951
Kaspersky Security Center 事件 ID	000003b7
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

禁用便携模式时出错

状态	!
组件	数据加密
Windows 事件 ID	953
Kaspersky Security Center 事件 ID	000003b9
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

创建加密数据包时出错

状态	!
组件	数据加密
Windows 事件 ID	931
Kaspersky Security Center 事件 ID	000003a3
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

加密/解密设备时出错

状态	!
组件	数据加密
Windows 事件 ID	1305
Kaspersky Security Center 事件 ID	00000519
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

无法加载加密模块

状态	!
组件	数据加密
Windows 事件 ID	1311
Kaspersky Security Center 事件 ID	0000051f
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

用于管理身份验证代理账户的任务以出错结束

状态	!
组件	数据加密
Windows 事件 ID	1340
Kaspersky Security Center 事件 ID	0000053c
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

无法应用策略

状态	!
组件	系统审计
Windows 事件 ID	1312
Kaspersky Security Center 事件 ID	00000520
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

FDE 升级失败

状态	!
组件	数据加密
Windows 事件 ID	1342
Kaspersky Security Center 事件 ID	0000053e
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

FDE 升级回滚失败(要了解更多信息，请参阅 Kaspersky Endpoint Security for Windows 在线帮助)

状态	!
组件	数据加密
Windows 事件 ID	1344
Kaspersky Security Center 事件 ID	00000540
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

Kaspersky Anti Targeted Attack Platform 服务器不可用

状态	!
组件	Endpoint Sensor
Windows 事件 ID	2100
Kaspersky Security Center 事件 ID	00000834
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

删除对象失败

状态	!
组件	Sandbox
Windows 事件 ID	2252
Kaspersky Security Center 事件 ID	000008cc
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

对象未隔离(Sandbox)

状态	!
组件	Sandbox
Windows 事件 ID	2603
Kaspersky Security Center 事件 ID	00000a2b
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

发生了内部错误

状态	!
组件	Sandbox
Windows 事件 ID	2607
Kaspersky Security Center 事件 ID	00000a2f
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

无效的 Sandbox 服务器证书

状态	!
组件	Sandbox
Windows 事件 ID	2613
Kaspersky Security Center 事件 ID	00000a35
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

Sandbox 节点不可用

状态	!
组件	Sandbox
Windows 事件 ID	2614
Kaspersky Security Center 事件 ID	00000a36
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

在 Sandbox 中处理对象失败

状态	!
组件	Sandbox
Windows 事件 ID	2617
Kaspersky Security Center 事件 ID	00000a39
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

已超过 Sandbox 的最大负载

状态	!
组件	Sandbox
Windows 事件 ID	2618
Kaspersky Security Center 事件 ID	00000a3a
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

找到 IOC

状态	!
组件	Endpoint Detection and Response
Windows 事件 ID	2651
Kaspersky Security Center 事件 ID	00000a5b
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

Sandbox 授权许可验证失败

状态	!
组件	Sandbox
Windows 事件 ID	2620
Kaspersky Security Center 事件 ID	00000a3c
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

用户将扫描任务提交到 Sandbox 失败

状态	!
组件	Sandbox
Windows 事件 ID	2623
Kaspersky Security Center 事件 ID	00000a3e
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

创建 Sandbox 任务时出错

状态	!
组件	Sandbox
Windows 事件 ID	2621
Kaspersky Security Center 事件 ID	00000a3d
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

对象启动已阻止

状态	!
组件	Endpoint Detection and Response
Windows 事件 ID	2553
Kaspersky Security Center 事件 ID	000009f9
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

进程启动已阻止

状态	!
组件	Endpoint Detection and Response
Windows 事件 ID	2551
Kaspersky Security Center 事件 ID	000009f7
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

脚本执行已阻止

状态	!
组件	Endpoint Detection and Response
Windows 事件 ID	2559
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

对象未隔离(Endpoint Detection and Response)

状态	!
组件	Endpoint Detection and Response
Windows 事件 ID	2556
Kaspersky Security Center 事件 ID	000009fc
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

进程启动未阻止

状态	!
组件	Endpoint Detection and Response
Windows 事件 ID	2561
Kaspersky Security Center 事件 ID	00000a01
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

对象未阻止

状态	!
组件	Endpoint Detection and Response
Windows 事件 ID	2562
Kaspersky Security Center 事件 ID	00000a02
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

脚本执行未阻止

状态	!
组件	Endpoint Detection and Response
Windows 事件 ID	2563
Kaspersky Security Center 事件 ID	00000a03
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

更改应用程序组件时出错

状态	!
组件	系统审计
Windows 事件 ID	1401
Kaspersky Security Center 事件 ID	00000579
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

系统中存在可能的暴力攻击模式

状态	!
组件	日志审查
Windows 事件 ID	2800
Kaspersky Security Center 事件 ID	00000af0
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

存在可能的 Windows 事件日志滥用模式

状态	!
组件	日志审查
Windows 事件 ID	2801
Kaspersky Security Center 事件 ID	00000af1
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

检测到代表安装了新服务的非典型操作

状态	!
组件	日志审查
Windows 事件 ID	2802
Kaspersky Security Center 事件 ID	00000af2
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

检测到使用显式凭证的非典型登录

状态	!
组件	日志审查
Windows 事件 ID	2803
Kaspersky Security Center 事件 ID	00000af3
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

系统中存在可能的 Kerberos 伪造的 PAC (MS14-068) 攻击模式

状态	!
组件	日志审查
Windows 事件 ID	2804
Kaspersky Security Center 事件 ID	00000af4
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

在特权内置管理员组中检测到可疑更改

状态	!
组件	日志审查
Windows 事件 ID	2805
Kaspersky Security Center 事件 ID	00000af5
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

在网络登录会话期间检测到非典型活动

状态	!
组件	日志审查
Windows 事件 ID	2806
Kaspersky Security Center 事件 ID	00000af6
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

日志审查规则已触发

状态	!
组件	日志审查
Windows 事件 ID	2807
Kaspersky Security Center 事件 ID	00000af7
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

非典型事件发生得太频繁。事件聚合已启动

状态	!
组件	日志审查
Windows 事件 ID	2808
Kaspersky Security Center 事件 ID	00000af8
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

关于聚合期非典型事件的报告

状态	!
组件	日志审查
Windows 事件 ID	2809
Kaspersky Security Center 事件 ID	00000af9
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

连接到 EDR Expert 服务器错误

状态	!
组件	Endpoint Detection and Response Expert (on-premises)
Windows 事件 ID	2850
Kaspersky Security Center 事件 ID	00000b22
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

EDR Expert 服务器的证书无效

状态	!
组件	Endpoint Detection and Response Expert (on-premises)
Windows 事件 ID	2851
Kaspersky Security Center 事件 ID	00000b23
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

EDR Expert 服务器上代理的证书无效

状态	!
组件	Endpoint Detection and Response Expert (on-premises)
Windows 事件 ID	2852
Kaspersky Security Center 事件 ID	00000b24
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

连接到 EDR Expert 响应服务器错误

状态	!
组件	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows 事件 ID	2858
Kaspersky Security Center 事件 ID	00000b22
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

EDR Expert 响应服务器的证书无效

状态	!
组件	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows 事件 ID	2859
Kaspersky Security Center 事件 ID	00000b23
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

EDR Expert 响应服务器上代理的证书无效

状态	!
组件	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows 事件 ID	2860
Kaspersky Security Center 事件 ID	00000b24
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

EDR Expert 遥测采集服务器连接错误

状态	!
组件	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows 事件 ID	2854
Kaspersky Security Center 事件 ID	00000b22
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

EDR Expert 遥测采集服务器的证书无效

状态	!
组件	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows 事件 ID	2855
Kaspersky Security Center 事件 ID	00000b23

Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

EDR Expert 遥测采集服务器上代理的证书无效

状态	!
组件	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows 事件 ID	`2856`
Kaspersky Security Center 事件 ID	`00000b24`
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

连接到 NDR 服务器错误

状态	!
组件	Network Detection and Response (KATA)
Windows 事件 ID	`3080`
Kaspersky Security Center 事件 ID	`00000c08`
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

NDR 服务器的证书无效

状态	!
组件	Network Detection and Response (KATA)
Windows 事件 ID	`3081`
Kaspersky Security Center 事件 ID	`00000c09`
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

NDR 服务器上代理的证书无效

状态	!
组件	Network Detection and Response (KATA)
Windows 事件 ID	`3082`
Kaspersky Security Center 事件 ID	`00000c0a`
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

您的设备已连接到不受信任的管理服务器。请联系管理员。

状态	!
组件	管理服务器连接保护
Windows 事件 ID	`3301`
Kaspersky Security Center 事件 ID	`00000ce5`

Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

检测到文件或文件夹更改

状态	ⓘ / ⚠ / ⓘ
组件	系统完整性监控
Windows 事件 ID	2950
Kaspersky Security Center 事件 ID	00000b86
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

要配置此事件的保留期，请转至策略的"**事件配置**"部分并设置一般系统完整性监控事件（*检测到文件或文件夹更改*）的保留期。

对象更改太频繁。事件聚合已启动

状态	ⓘ / ⚠ / ⓘ
组件	系统完整性监控
Windows 事件 ID	2955
Kaspersky Security Center 事件 ID	00000b8b
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

聚合期间的对象更改报告

状态	ⓘ / ⚠ / ⓘ
组件	系统完整性监控
Windows 事件 ID	2956
Kaspersky Security Center 事件 ID	00000b8c
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

要配置此事件的保留期，请转至策略的"**事件配置**"部分并设置一般系统完整性监控事件（*检测到文件或文件夹更改*）的保留期。

监控范围包括错误对象

状态	ⓘ
组件	系统完整性监控
Windows 事件 ID	2953
Kaspersky Security Center 事件 ID	00000b89
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

检测到注册表更改

状态	ⓘ / ⚠ / ⓘ
组件	系统完整性监控
Windows 事件 ID	2951
Kaspersky Security Center 事件 ID	00000b87
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

要配置此事件的保留期，请转至策略的“**事件配置**”部分并设置一般系统完整性监控事件（*检测到文件或文件夹更改*）的保留期。

检测到设备连接/断开

状态	ⓘ / ⚠ / ⓘ
组件	系统完整性监控
Windows 事件 ID	2952
Kaspersky Security Center 事件 ID	00000b88
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

要配置此事件的保留期，请转至策略的“**事件配置**”部分并设置一般系统完整性监控事件（*检测到文件或文件夹更改*）的保留期。

监控范围包括错误对象

状态	ⓘ / ⚠ / ⓘ
组件	系统完整性监控
Windows 事件 ID	2903
Kaspersky Security Center 事件 ID	00000b89
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

要配置此事件的保留期，请转至策略的“**事件配置**”部分并设置一般系统完整性监控事件（*检测到文件或文件夹更改*）的保留期。

尝试对对象执行受限操作的次数太多。事件聚合已启动

状态	ⓘ
组件	系统完整性监控
Windows 事件 ID	2963
Kaspersky Security Center 事件 ID	00000b93
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

对监控范围内的文件操作被阻止

状态	ⓘ
组件	系统完整性监控
Windows 事件 ID	2959
Kaspersky Security Center 事件 ID	00000b8f
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

要配置此事件的保留期，请转至策略的"**事件配置**"部分并设置一般系统完整性监控事件（*检测到文件或文件夹更改*）的保留期。

注册表修改已阻止

状态	ⓘ
组件	系统完整性监控
Windows 事件 ID	2960
Kaspersky Security Center 事件 ID	00000b90
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

要配置此事件的保留期，请转至策略的"**事件配置**"部分并设置一般系统完整性监控事件（*检测到文件或文件夹更改*）的保留期。

处理错误

状态	ⓘ
组件	系统完整性监控
Windows 事件 ID	2954
Kaspersky Security Center 事件 ID	00000b8a
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

系统完整性监控: 对没有匹配的安全标识符 (SID) 的用户账户禁用规则触发

状态	ⓘ
组件	系统完整性监控
Windows 事件 ID	2964
Kaspersky Security Center 事件 ID	00000b94
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

应用程序控制: 对没有匹配的安全标识符 (SID) 的本地用户账户禁用规则触发

状态	ⓘ
组件	应用程序控制
Windows 事件 ID	711

Kaspersky Security Center 事件 ID	000002c7
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

设备控制: 对没有匹配的安全标识符 (SID) 的用户账户禁用规则触发

状态	!
组件	设备控制
Windows 事件 ID	810
Kaspersky Security Center 事件 ID	0000032a
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

Web 控制: 对没有匹配的安全标识符 (SID) 的用户账户禁用规则触发

状态	!
组件	Web 控制
Windows 事件 ID	757
Kaspersky Security Center 事件 ID	000002f5
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

自适应异常控制: 对没有匹配的安全标识符 (SID) 的用户账户禁用规则触发

状态	!
组件	自适应异常控制
Windows 事件 ID	504
Kaspersky Security Center 事件 ID	000001f8
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

日志审查: 对没有匹配的安全标识符 (SID) 的用户账户禁用规则触发

状态	!
组件	日志审查
Windows 事件 ID	2810
Kaspersky Security Center 事件 ID	00000afa
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

无法连接到 Integration Server 的时间超过 6 小时。检查 Integration Server 状态和网络设置

状态	!
组件	Light Agent
Windows 事件 ID	3103

Kaspersky Security Center 事件 ID	00000c1f
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

SVM 不可用

状态	!
组件	Light Agent
Windows 事件 ID	3151
Kaspersky Security Center 事件 ID	00000c4f
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

检测到恶意对象。应在虚拟机模板上启动高级清除

状态	!
组件	Light Agent
Windows 事件 ID	3182
Kaspersky Security Center 事件 ID	00000c6e
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

通过已弃用协议建立的网络连接被阻止

状态	!
组件	保护
Windows 事件 ID	75
Kaspersky Security Center 事件 ID	0000004b
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

KUMA 服务器连接错误

状态	!
组件	KUMA 整合
Windows 事件 ID	2854
Kaspersky Security Center 事件 ID	00000b26
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

KUMA 服务器的证书无效

状态	!
组件	KUMA 整合
Windows 事件 ID	2855

Kaspersky Security Center 事件 ID	00000b27
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

KUMA 服务器上代理的证书无效

状态	ⓘ
组件	KUMA 整合
Windows 事件 ID	2856
Kaspersky Security Center 事件 ID	00000b28
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

功能失败

无法执行任务

状态	ⓘ
组件	系统审计
Windows 事件 ID	212
Kaspersky Security Center 事件 ID	000000d4
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

任务设置无效，未应用设置

状态	ⓘ
组件	系统审计
Windows 事件 ID	707
Kaspersky Security Center 事件 ID	000002c3
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

警告

应用程序在先前会话中崩溃

状态	⚠
组件	系统审计
Windows 事件 ID	237
Kaspersky Security Center 事件 ID	–

Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

授权许可即将到期

状态	⚠
组件	系统审计
Windows 事件 ID	204
Kaspersky Security Center 事件 ID	000000cc
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

数据库已过期

状态	⚠
组件	系统审计
Windows 事件 ID	208
Kaspersky Security Center 事件 ID	000000d0
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

自动更新已禁用

状态	⚠
组件	系统审计
Windows 事件 ID	210
Kaspersky Security Center 事件 ID	000000d2
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

自我保护被禁用

状态	⚠
组件	系统审计
Windows 事件 ID	211
Kaspersky Security Center 事件 ID	000000d3
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

保护组件已禁用

状态	⚠
组件	系统审计
Windows 事件 ID	214
Kaspersky Security Center 事件 ID	000000d6

Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

计算机正在安全模式下运行

状态	⚠
组件	系统审计
Windows 事件 ID	215
Kaspersky Security Center 事件 ID	000000d7
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

存在未处理的文件

状态	⚠
组件	系统审计
Windows 事件 ID	216
Kaspersky Security Center 事件 ID	000000d8
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

组策略已应用

状态	⚠
组件	系统审计
Windows 事件 ID	219
Kaspersky Security Center 事件 ID	000000db
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

任务已停止

状态	⚠
组件	系统审计
Windows 事件 ID	222
Kaspersky Security Center 事件 ID	000000de
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

退出并重新打开应用程序以完成更新

状态	⚠
组件	系统审计
Windows 事件 ID	224
Kaspersky Security Center 事件 ID	0000057b

Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

需要重启计算机

状态	⚠
组件	系统审计
Windows 事件 ID	225
Kaspersky Security Center 事件 ID	000000e1
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

授权许可允许使用尚未安装的组件

状态	⚠
组件	系统审计
Windows 事件 ID	226
Kaspersky Security Center 事件 ID	000000e2
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

高级清除已启动

状态	⚠
组件	系统审计
Windows 事件 ID	232
Kaspersky Security Center 事件 ID	000000e8
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

高级清除已完成

状态	⚠
组件	系统审计
Windows 事件 ID	233
Kaspersky Security Center 事件 ID	000000e9
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

备用密钥不正确

状态	⚠
组件	系统审计
Windows 事件 ID	230
Kaspersky Security Center 事件 ID	000000e6

Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

订阅即将到期

状态	⚠
组件	系统审计
Windows 事件 ID	`240`
Kaspersky Security Center 事件 ID	`000000f0`
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

已阻止

状态	⚠
组件	行为检测 反加密勒索 漏洞利用防御 Web 威胁防护
Windows 事件 ID	`331`
Kaspersky Security Center 事件 ID	`GNRL_EV_OBJECT_BLOCKED`
事件参数	• `GNRL_EA_PARAM_1` 是对象的哈希 (SHA256)。 • `GNRL_EA_PARAM_2` 是对象的名称。 当检测到共享文件夹的外部加密时，应用程序会显示目标文件的路径。 • `GNRL_EA_PARAM_5` 是威胁的名称，与 Kaspersky 分类法一致，例如 `EICAR-Test-File`。 • `GNRL_EA_PARAM_7` 是会话用户的名称。 • `GNRL_EA_PARAM_8` 是威胁类型（`type`）。 • `GNRL_EA_PARAM_9` 是检测到的对象的附加信息： 应用程序组件 (`engine`)。 威胁检测技术 (`method`)。 卡巴斯基私人安全网络检测到的威胁（`blacklist`）：`true` 或者 `false`。 EDR 版本。 EDR 中的威胁标识符。 对象的 MD5 哈希。
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

操作系统设置不允许控制对 Wi-Fi 网络的访问

状态	⚠
组件	设备控制
Windows 事件 ID	`249`
Kaspersky Security Center 事件 ID	`000000f9`
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

对象未从备份区中恢复

状态	⚠
组件	系统审计
Windows 事件 ID	336
Kaspersky Security Center 事件 ID	00000150
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

检测到可疑的网络活动

状态	⚠
组件	系统审计
Windows 事件 ID	2001
Kaspersky Security Center 事件 ID	000007d1
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

加密连接已终止

状态	⚠
组件	系统审计
Windows 事件 ID	250
Kaspersky Security Center 事件 ID	000007d3
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

已禁用参与 KSN

状态	⚠
组件	系统审计
Windows 事件 ID	2021
Kaspersky Security Center 事件 ID	000007e5
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

已禁用某些操作系统功能的处理

状态	⚠
组件	系统审计
Windows 事件 ID	245
Kaspersky Security Center 事件 ID	000000f5
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

隔离区存储空间几乎用完

状态	⚠
组件	系统审计
Windows 事件 ID	344
Kaspersky Security Center 事件 ID	00000158
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

已阻止网络连接

状态	⚠
组件	系统审计
Windows 事件 ID	809
Kaspersky Security Center 事件 ID	00000abe
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

无法创建备份副本

状态	⚠
组件	文件威胁防护 邮件威胁防护 主机入侵防御 AMSI 保护 恶意软件扫描
Windows 事件 ID	314
Kaspersky Security Center 事件 ID	GNRL_EV_OBJECT_REPORTED
事件参数	• GNRL_EA_PARAM_1 是对象的哈希 (SHA256)。 • GNRL_EA_PARAM_2 是对象的名称。 • GNRL_EA_PARAM_5 是威胁的名称，与 Kaspersky 分类法一致，例如 EICAR-Test-File。 • GNRL_EA_PARAM_7 是会话用户的名称。 • GNRL_EA_PARAM_8 是威胁类型（type）。 • GNRL_EA_PARAM_9 是检测到的对象的附加信息： 应用程序组件 (engine)。 威胁检测技术 (method)。 卡巴斯基私人安全网络检测到的威胁（blacklist）：true 或者 false。 EDR 版本。 EDR 中的威胁标识符。 对象的 MD5 哈希。
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

状态	⚠
组件	文件威胁防护 行为检测 反加密勒索 主机入侵防御 恶意软件扫描
Windows 事件 ID	310
Kaspersky Security Center 事件 ID	00000136

Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

对象已加密

状态	⚠
组件	主机入侵防御
Windows 事件 ID	320
Kaspersky Security Center 事件 ID	00000140
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

对象已损坏

状态	⚠
组件	文件威胁防护 Web 威胁防护 邮件威胁防护 AMSI 保护 主机入侵防御 恶意软件扫描
Windows 事件 ID	321
Kaspersky Security Center 事件 ID	00000141
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

检测到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(本地库)

状态	⚠
组件	文件威胁防护 Web 威胁防护 邮件威胁防护 主机入侵防御 AMSI 保护 行为检测 反加密勒索 反加密勒索 恶意软件扫描
Windows 事件 ID	303
Kaspersky Security Center 事件 ID	GNRL_EV_VIRUS_FOUND
事件参数	• GNRL_EA_PARAM_1 是对象的哈希 (SHA256)。 • GNRL_EA_PARAM_2 是对象的名称。 • GNRL_EA_PARAM_5 是威胁的名称，与 Kaspersky 分类法一致，例如 EICAR-Test-File。 • GNRL_EA_PARAM_7 是会话用户的名称。 • GNRL_EA_PARAM_8 是威胁类型（type）。
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

检测到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(KSN)

状态	⚠
组件	文件威胁防护 Web 威胁防护 邮件威胁防护 主机入侵防御 AMSI 保护 行为检测 反加密勒索 反加密勒索 恶意软件扫描
Windows 事件 ID	303
Kaspersky Security Center 事件 ID	GNRL_EV_VIRUS_FOUND_BY_KSN
事件参数	• GNRL_EA_PARAM_1 是对象的哈希 (SHA256)。 • GNRL_EA_PARAM_2 是对象的名称。 • GNRL_EA_PARAM_5 是威胁的名称，与 Kaspersky 分类法一致，例如 EICAR-Test-File。 • GNRL_EA_PARAM_7 是会话用户的名称。 • GNRL_EA_PARAM_8 是威胁类型（type）。
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

对象已删除

状态	⚠
组件	文件威胁防护 邮件威胁防护 主机入侵防御 漏洞利用防御 行为检测 反加密勒索 恶意软件扫描
Windows 事件 ID	307
Kaspersky Security Center 事件 ID	GNRL_EV_OBJECT_DELETED
事件参数	• GNRL_EA_PARAM_1 是对象的哈希 (SHA256)。 • GNRL_EA_PARAM_2 是对象的名称。 • GNRL_EA_PARAM_5 是威胁的名称，与 Kaspersky 分类法一致，例如 EICAR-Test-File。 • GNRL_EA_PARAM_7 是会话用户的名称。 • GNRL_EA_PARAM_8 是威胁类型（type）。 • GNRL_EA_PARAM_9 是检测到的对象的附加信息： 应用程序组件 (engine)。 威胁检测技术 (method)。 卡巴斯基私人安全网络检测到的威胁（blacklist）：true 或者 false。 EDR 版本。 EDR 中的威胁标识符。 对象的 MD5 哈希。
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

对象已清除

状态	⚠
组件	文件威胁防护 邮件威胁防护 主机入侵防御 恶意软件扫描
Windows 事件 ID	306

Kaspersky Security Center 事件 ID	GNRL_EV_OBJECT_CURED
事件参数	• GNRL_EA_PARAM_1 是对象的哈希 (SHA256)。 • GNRL_EA_PARAM_2 是对象的名称。 • GNRL_EA_PARAM_5 是威胁的名称，与 Kaspersky 分类法一致，例如 EICAR-Test-File。 • GNRL_EA_PARAM_7 是会话用户的名称。 • GNRL_EA_PARAM_8 是威胁类型（type）。 • GNRL_EA_PARAM_9 是检测到的对象的附加信息： 应用程序组件 (engine)。 威胁检测技术 (method)。 卡巴斯基私人安全网络检测到的威胁（blacklist）：true 或者 false。 EDR 版本。 EDR 中的威胁标识符。 对象的 MD5 哈希。
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

对象将在重启后清除

状态	⚠
组件	主机入侵防御 文件威胁防护 恶意软件扫描
Windows 事件 ID	324
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

对象将在重启后删除

状态	⚠
组件	行为检测 反加密勒索 漏洞利用防御 主机入侵防御 文件威胁防护 恶意软件扫描
Windows 事件 ID	323
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

对象根据设置被删除

状态	⚠
组件	邮件威胁防护
Windows 事件 ID	342
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

回滚已完成

状态	⚠
组件	文件威胁防护 行为检测 反加密勒索 漏洞利用防御 恶意软件扫描
Windows 事件 ID	455
Kaspersky Security Center 事件 ID	000001c7
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

对象下载被阻止

状态	⚠
组件	Web 威胁防护
Windows 事件 ID	341
Kaspersky Security Center 事件 ID	GNRL_EV_OBJECT_BLOCKED
事件参数	• GNRL_EA_PARAM_1 是对象的哈希 (SHA256)。 • GNRL_EA_PARAM_2 是对象的名称。 • GNRL_EA_PARAM_5 是威胁的名称，与 Kaspersky 分类法一致，例如 EICAR-Test-File。 • GNRL_EA_PARAM_7 是会话用户的名称。 • GNRL_EA_PARAM_8 是威胁类型（type）。 • GNRL_EA_PARAM_9 是检测到的对象的附加信息： 应用程序组件 (engine)。 威胁检测技术 (method)。 卡巴斯基私人安全网络检测到的威胁（blacklist）：true 或者 false。 EDR 版本。 EDR 中的威胁标识符。 对象的 MD5 哈希。
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

键盘授权错误

状态	⚠
组件	BadUSB 攻击防护
Windows 事件 ID	2052
Kaspersky Security Center 事件 ID	00000804
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

对象扫描结果已发送至第三方应用程序

状态	⚠
组件	AMSI 保护
Windows 事件 ID	1512

Kaspersky Security Center 事件 ID	GNRL_EV_OBJECT_REPORTED
事件参数	• GNRL_EA_PARAM_1 是对象的哈希 (SHA256)。 • GNRL_EA_PARAM_2 是对象的名称。 • GNRL_EA_PARAM_5 是威胁的名称，与 Kaspersky 分类法一致，例如 EICAR-Test-File。 • GNRL_EA_PARAM_7 是会话用户的名称。 • GNRL_EA_PARAM_8 是威胁类型（type）。 • GNRL_EA_PARAM_9 是检测到的对象的附加信息： 应用程序组件 (engine)。 威胁检测技术 (method)。 卡巴斯基私人安全网络检测到的威胁（blacklist）：true 或者 false。 EDR 版本。 EDR 中的威胁标识符。 对象的 MD5 哈希。
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

任务设置已成功应用

状态	⚠
组件	应用程序控制
Windows 事件 ID	708
Kaspersky Security Center 事件 ID	000002c4
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

有关不良内容的警告 (本地数据库)

状态	⚠
组件	Web 控制
Windows 事件 ID	708
Kaspersky Security Center 事件 ID	GNRL_EV_WEB_URL_WARNING
事件参数	• GNRL_EA_PARAM_1 是网址。 • GNRL_EA_PARAM_2 是会话用户的名称。 • GNRL_EA_PARAM_3 是 Web 控制规则名称。
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

有关不良内容的警告 (KSN)

状态	⚠
组件	Web 控制
Windows 事件 ID	708
Kaspersky Security Center 事件 ID	GNRL_EV_WEB_URL_WARNING
事件参数	• GNRL_EA_PARAM_1 是网址。 • GNRL_EA_PARAM_2 是会话用户的名称。 • GNRL_EA_PARAM_3 是 Web 控制规则名称。
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

在警告后访问了不良内容

状态	⚠
组件	Web 控制
Windows 事件 ID	754
Kaspersky Security Center 事件 ID	000002f2
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

已激活对设备的临时访问

状态	⚠
组件	设备控制
Windows 事件 ID	803
Kaspersky Security Center 事件 ID	000002f2
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

操作被用户取消

状态	⚠
组件	更新
Windows 事件 ID	1016
Kaspersky Security Center 事件 ID	000003f8
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

用户选择了退出加密策略

状态	⚠
组件	数据加密
Windows 事件 ID	1306
Kaspersky Security Center 事件 ID	0000051a
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

已中断应用文件加密/解密规则

状态	⚠
组件	数据加密
Windows 事件 ID	903
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

文件加密/解密已中断

状态	⚠
组件	数据加密
Windows 事件 ID	914
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

设备加密/解密已中断

状态	⚠
组件	数据加密
Windows 事件 ID	1303
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

无法在 WinRE 映像中安装或升级卡巴斯基磁盘加密驱动程序

状态	⚠
组件	数据加密
Windows 事件 ID	1345
Kaspersky Security Center 事件 ID	00000541
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

模块签名检查失败

状态	⚠
组件	系统完整性检查
Windows 事件 ID	2002
Kaspersky Security Center 事件 ID	000007d2
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

已阻止应用程序启动

状态	⚠
组件	Endpoint Sensor
Windows 事件 ID	2105
Kaspersky Security Center 事件 ID	00000839
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

已阻止打开文档

状态	⚠
组件	Endpoint Sensor
Windows 事件 ID	2106
Kaspersky Security Center 事件 ID	0000083a
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

进程已被 Kaspersky Anti Targeted Attack Platform 服务器管理员终止

状态	⚠
组件	Endpoint Sensor
Windows 事件 ID	2112
Kaspersky Security Center 事件 ID	00000840
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

应用程序已被 Kaspersky Anti Targeted Attack Platform 服务器管理员终止

状态	⚠
组件	Endpoint Sensor
Windows 事件 ID	2113
Kaspersky Security Center 事件 ID	00000841
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

文件或流已被 Kaspersky Anti Targeted Attack Platform 服务器管理员删除

状态	⚠
组件	Endpoint Sensor
Windows 事件 ID	2111
Kaspersky Security Center 事件 ID	0000083f
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

文件已被管理员从 Kaspersky Anti Targeted Attack Platform 服务器上的隔离区恢复

状态	⚠
组件	Endpoint Sensor
Windows 事件 ID	2110
Kaspersky Security Center 事件 ID	0000083e
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

文件已被管理员隔离在 Kaspersky Anti Targeted Attack Platform 服务器上

状态	⚠
组件	Endpoint Sensor
Windows 事件 ID	2109
Kaspersky Security Center 事件 ID	0000083d
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

所有第三方应用程序的网络活动均已阻止

状态	⚠
组件	Endpoint Sensor
Windows 事件 ID	2107
Kaspersky Security Center 事件 ID	0000083b
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

所有第三方应用程序的网络活动均已解除阻止

状态	⚠
组件	Endpoint Sensor
Windows 事件 ID	2108
Kaspersky Security Center 事件 ID	0000083c
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

对象将在重启后删除(Sandbox)

状态	⚠
组件	Sandbox
Windows 事件 ID	2605
Kaspersky Security Center 事件 ID	00000a2d
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

扫描任务总大小已超过限制

状态	⚠
组件	Sandbox
Windows 事件 ID	2612
Kaspersky Security Center 事件 ID	00000a34
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

对象启动已允许，事件已记录

状态	⚠
组件	Endpoint Detection and Response
Windows 事件 ID	2553
Kaspersky Security Center 事件 ID	000009fa
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

进程启动已允许，事件已记录

状态	⚠
组件	Endpoint Detection and Response
Windows 事件 ID	2554
Kaspersky Security Center 事件 ID	000009f8
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

对象将在重启后删除(Endpoint Detection and Response)

状态	⚠
组件	Endpoint Detection and Response
Windows 事件 ID	2558
Kaspersky Security Center 事件 ID	000009fe
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

网络隔离

状态	⚠
组件	Endpoint Detection and Response
Windows 事件 ID	2700
Kaspersky Security Center 事件 ID	00000a8c
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

终止网络隔离

状态	⚠
组件	Endpoint Detection and Response
Windows 事件 ID	2701
Kaspersky Security Center 事件 ID	00000a8d
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

完成任务需要重启

状态	⚠
组件	系统审计
Windows 事件 ID	225
Kaspersky Security Center 事件 ID	0000057b
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

发送给管理员的应用程序启动阻止消息

状态	⚠
组件	应用程序控制
Windows 事件 ID	503
Kaspersky Security Center 事件 ID	GNRL_EV_AC_USER_REQUEST
事件参数	• GNRL_EA_DESCRIPTION 是给用户的消息。 • GNRL_EA_PARAM_2 是会话用户的名称。 • GNRL_EA_PARAM_6 是应用程序可执行文件的名称（例如，chrome.exe）。 • GNRL_EA_PARAM_7 是可执行文件的路径。 • GNRL_EA_PARAM_8 是对象的哈希 (SHA256)。 • GNRL_EA_PARAM_9 是用户正在试图运行的应用程序的版本。
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

发送给管理员的设备访问阻止消息

状态	⚠
组件	设备控制
Windows 事件 ID	804
Kaspersky Security Center 事件 ID	GNRL_EV_DC_USER_REQUEST
事件参数	• c_er_descr 是给用户的消息。 • GNRL_EA_PARAM_1 是硬件 ID (HWID)。 • GNRL_EA_PARAM_2 是会话用户的名称。
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

发送给管理员的网页访问阻止消息

状态	⚠
组件	Web 控制
Windows 事件 ID	755
Kaspersky Security Center 事件 ID	GNRL_EV_WC_USER_REQUEST
事件参数	• GNRL_EA_DESCRIPTION 是给用户的消息。 • GNRL_EA_PARAM_1 是网址。 • GNRL_EA_PARAM_2 是会话用户的名称。
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

已阻止设备连接

状态	⚠
组件	设备控制
Windows 事件 ID	807
Kaspersky Security Center 事件 ID	GNRL_EV_DEVCTRL_DEV_PLUG_DENIED
事件参数	• GNRL_EA_PARAM_1 是硬件 ID (HWID)。 • GNRL_EA_PARAM_2 是会话用户的名称。
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

发送给管理员的应用程序活动阻止消息

状态	⚠
组件	文件完整性监控
Windows 事件 ID	2901
Kaspersky Security Center 事件 ID	00000b55
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

状态	⚠
组件	文件完整性监控
Windows 事件 ID	2900
Kaspersky Security Center 事件 ID	00000b54
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

状态	⚠
组件	自适应异常控制
Windows 事件 ID	503
Kaspersky Security Center 事件 ID	GNRL_EV_ADSEC_USER_REQUEST
事件参数	• GNRL_EA_DESCRIPTION 是给用户的消息。 • GNRL_EA_PARAM_1 是自适应异常控制规则名称。 • GNRL_EA_PARAM_2 是启发式规则 ID。 • GNRL_EA_PARAM_3 是会话用户的名称。 • GNRL_EA_PARAM_4 是源进程。 • GNRL_EA_PARAM_5 是源对象。 • GNRL_EA_PARAM_6 是目标进程。 • GNRL_EA_PARAM_7 是目标对象。 • GNRL_EA_PARAM_8 是检测到的对象的附加信息：源进程/对象和目标进程/对象的哈希。进程被阻止（verdict_type）：true或false。用户安全 ID（SID）.
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

阻止启动云服务客户端应用程序

状态	⚠
组件	Cloud Discovery
Windows 事件 ID	2212
Kaspersky Security Center 事件 ID	000008a4
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

阻止访问云服务

状态	⚠
组件	Cloud Discovery
Windows 事件 ID	2213
Kaspersky Security Center 事件 ID	000008a5
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

检测到文件或文件夹更改

状态	ⓘ / ⚠ / ⓘ
组件	系统完整性监控
Windows 事件 ID	2950
Kaspersky Security Center 事件 ID	00000b86
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

要配置此事件的保留期，请转至策略的"**事件配置**"部分并设置一般系统完整性监控事件（*检测到文件或文件夹更改*）的保留期。

对象更改太频繁。事件聚合已启动

状态	ⓘ / ⚠ / ⓘ
组件	系统完整性监控
Windows 事件 ID	2955
Kaspersky Security Center 事件 ID	00000b8b
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

聚合期间的对象更改报告

状态	ⓘ / ⚠ / ⓘ
组件	系统完整性监控
Windows 事件 ID	2956
Kaspersky Security Center 事件 ID	00000b8c
Windows 事件日志（默认）	–

Kaspersky Security Center 事件日志（默认）	✓

要配置此事件的保留期，请转至策略的"**事件配置**"部分并设置一般系统完整性监控事件（*检测到文件或文件夹更改*）的保留期。

检测到注册表更改

状态	ⓘ / ⚠ / ⓘ
组件	系统完整性监控
Windows 事件 ID	2951
Kaspersky Security Center 事件 ID	00000b87
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

要配置此事件的保留期，请转至策略的"**事件配置**"部分并设置一般系统完整性监控事件（*检测到文件或文件夹更改*）的保留期。

检测到设备连接/断开

状态	ⓘ / ⚠ / ⓘ
组件	系统完整性监控
Windows 事件 ID	2952
Kaspersky Security Center 事件 ID	00000b88
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

要配置此事件的保留期，请转至策略的"**事件配置**"部分并设置一般系统完整性监控事件（*检测到文件或文件夹更改*）的保留期。

监控范围包括错误对象

状态	ⓘ / ⚠ / ⓘ
组件	系统完整性监控
Windows 事件 ID	2903
Kaspersky Security Center 事件 ID	00000b89
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

要配置此事件的保留期，请转至策略的"**事件配置**"部分并设置一般系统完整性监控事件（*检测到文件或文件夹更改*）的保留期。

在测试模式下允许执行禁止的操作

状态	⚠
组件	系统完整性监控
Windows 事件 ID	2961

Kaspersky Security Center 事件 ID	00000b91
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

无法连接到 Integration Server 的时间超过 30 分钟。检查 Integration Server 状态和网络设置。

状态	⚠
组件	Light Agent
Windows 事件 ID	3102
Kaspersky Security Center 事件 ID	00000c1e
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

无法连接到 Integration Server。检查 Integration Server 状态和网络设置。

状态	⚠
组件	Light Agent
Windows 事件 ID	3101
Kaspersky Security Center 事件 ID	00000c1d
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

虚拟机模板需要更新

状态	⚠
组件	Light Agent
Windows 事件 ID	3181
Kaspersky Security Center 事件 ID	00000c6d
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

标准授权许可已终止。应用程序正在企业授权许可下运行

状态	⚠
组件	Light Agent
Windows 事件 ID	3171
Kaspersky Security Center 事件 ID	00000c64
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

信息性消息

应用程序已启动

状态	ⓘ
组件	系统审计
Windows 事件 ID	235
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

应用程序已停止

状态	ⓘ
组件	系统审计
Windows 事件 ID	236
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

自我保护限制了对受保护资源的访问

状态	ⓘ
组件	系统审计
Windows 事件 ID	213
Kaspersky Security Center 事件 ID	000000d5
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

报告已清理

状态	ⓘ
组件	系统审计
Windows 事件 ID	217
Kaspersky Security Center 事件 ID	000000d9
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

组策略已禁用

状态	ⓘ
组件	系统审计
Windows 事件 ID	220
Kaspersky Security Center 事件 ID	000000dc
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

应用程序设置已更改

状态	ⓘ
组件	系统审计
Windows 事件 ID	218
Kaspersky Security Center 事件 ID	000000da
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

任务已启动

状态	ⓘ
组件	系统审计
Windows 事件 ID	221
Kaspersky Security Center 事件 ID	000000dd
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

任务已完成

状态	ⓘ
组件	系统审计
Windows 事件 ID	223
Kaspersky Security Center 事件 ID	000000df
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

授权许可定义的所有应用程序组件均已安装并且以正常模式运行

状态	ⓘ
组件	系统审计
Windows 事件 ID	227
Kaspersky Security Center 事件 ID	000000e3
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

订阅设置已更改

状态	ⓘ
组件	系统审计
Windows 事件 ID	238
Kaspersky Security Center 事件 ID	000000ee
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

订阅已续费

状态	ⓘ
组件	系统审计
Windows 事件 ID	239
Kaspersky Security Center 事件 ID	000000ef
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

对象已从备份区中恢复

状态	ⓘ
组件	系统审计
Windows 事件 ID	335
Kaspersky Security Center 事件 ID	0000014f
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

用户名和密码输入

状态	ⓘ
组件	系统审计
Windows 事件 ID	2000
Kaspersky Security Center 事件 ID	000007d0
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

已启用参与 KSN

状态	ⓘ
组件	系统审计
Windows 事件 ID	2020
Kaspersky Security Center 事件 ID	000007e4
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

KSN 服务器可用

状态	ⓘ
组件	系统审计
Windows 事件 ID	2022
Kaspersky Security Center 事件 ID	000007e6
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

应用程序根据相关法律工作和处理数据并使用适当的基础架构

状态	ⓘ
组件	系统审计
Windows 事件 ID	2024
Kaspersky Security Center 事件 ID	000007e8
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

对象已从隔离区中恢复

状态	ⓘ
组件	系统审计
Windows 事件 ID	345
Kaspersky Security Center 事件 ID	00000159
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

对象已从隔离区中删除

状态	ⓘ
组件	系统审计
Windows 事件 ID	347
Kaspersky Security Center 事件 ID	0000015b
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

对象的备份副本已创建

状态	ⓘ
组件	文件威胁防护 邮件威胁防护 行为检测 反加密勒索 主机入侵防御 Sandbox 恶意软件扫描
Windows 事件 ID	308
Kaspersky Security Center 事件 ID	00000134
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

已被先前清除的副本覆盖

状态	ⓘ
组件	文件威胁防护 主机入侵防御 恶意软件扫描
Windows 事件 ID	327
Kaspersky Security Center 事件 ID	00000147

Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

检测到密码保护的存档

状态	ⓘ
组件	文件威胁防护 Web 威胁防护 邮件威胁防护 AMSI 保护 主机入侵防御 恶意软件扫描
Windows 事件 ID	322
Kaspersky Security Center 事件 ID	GNRL_EV_PASSWD_ARCHIVE_FOUND
事件参数	• GNRL_EA_PARAM_2 是对象的名称。 • GNRL_EA_PARAM_3 是对象的创建日期（可选）。 • GNRL_EA_PARAM_7 是会话用户的名称。 • GNRL_EA_PARAM_9 是检测到的对象的附加信息： 应用程序组件（engine）。 威胁检测技术（method）。 由私人 KSN 检测到的威胁（拒绝列表）：启用或禁用。
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

有关检测到的对象的信息

状态	ⓘ
组件	文件威胁防护 Web 威胁防护 邮件威胁防护 AMSI 保护 主机入侵防御 恶意软件扫描
Windows 事件 ID	332
Kaspersky Security Center 事件 ID	0000014c
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

该对象在卡巴斯基私人安全网络允许列表中

状态	ⓘ
组件	文件威胁防护 Web 威胁防护 邮件威胁防护 AMSI 保护 主机入侵防御 恶意软件扫描
Windows 事件 ID	340
Kaspersky Security Center 事件 ID	00000154
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

对象已重命名

状态	ⓘ
组件	邮件威胁防护 漏洞利用防御 行为检测 反加密勒索 恶意软件扫描
Windows 事件 ID	329
Kaspersky Security Center 事件 ID	00000149
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

对象已处理

状态	ⓘ
组件	主机入侵防御 文件威胁防护 Web 威胁防护 邮件威胁防护 恶意软件扫描
Windows 事件 ID	301
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

对象已跳过

状态	ⓘ
组件	主机入侵防御 文件威胁防护 AMSI 保护 恶意软件扫描
Windows 事件 ID	315
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

检测到存档

状态	ⓘ
组件	主机入侵防御 文件威胁防护 Web 威胁防护 邮件威胁防护 AMSI 保护 恶意软件扫描
Windows 事件 ID	318
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

检测到打包对象

状态	ⓘ
组件	主机入侵防御 文件威胁防护 Web 威胁防护 邮件威胁防护 AMSI 保护 恶意软件扫描
Windows 事件 ID	319
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

已处理链接

状态	ⓘ
组件	Web 威胁防护
Windows 事件 ID	361
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

已允许应用程序启动

状态	ⓘ
组件	应用程序控制
Windows 事件 ID	701
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

已选定更新源

状态	ⓘ
组件	更新
Windows 事件 ID	1001
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

已选定代理服务器

状态	ⓘ
组件	更新
Windows 事件 ID	1002
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

该链接在卡巴斯基私人安全网络允许列表中

状态	ⓘ
组件	Web 威胁防护
Windows 事件 ID	370
Kaspersky Security Center 事件 ID	00000172
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

应用程序被放置在受信任组

状态	ⓘ
组件	主机入侵防御
Windows 事件 ID	401
Kaspersky Security Center 事件 ID	00000191
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

应用程序被放置在受限制组

状态	ⓘ
组件	主机入侵防御
Windows 事件 ID	402
Kaspersky Security Center 事件 ID	00000192
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

主机入侵防御已触发

状态	ⓘ
组件	主机入侵防御
Windows 事件 ID	403
Kaspersky Security Center 事件 ID	00000193
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

文件已恢复

状态	ⓘ
组件	行为检测 反加密勒索 漏洞利用防御 主机入侵防御
Windows 事件 ID	457
Kaspersky Security Center 事件 ID	000001c9

Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

注册表值已恢复

状态	ⓘ
组件	行为检测 漏洞利用防御
Windows 事件 ID	`458`
Kaspersky Security Center 事件 ID	`000001ca`
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

注册表值已删除

状态	ⓘ
组件	行为检测 漏洞利用防御
Windows 事件 ID	`459`
Kaspersky Security Center 事件 ID	`000001cb`
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

进程操作已跳过

状态	ⓘ
组件	自适应异常控制
Windows 事件 ID	`2201`
Kaspersky Security Center 事件 ID	`GNRL_EV_ADSEC_DETECT`
事件参数	• `GNRL_EA_PARAM_1` 是自适应异常控制规则名称。 • `GNRL_EA_PARAM_2` 是启发式规则 ID。 • `GNRL_EA_PARAM_3` 是会话用户的名称。 • `GNRL_EA_PARAM_4` 是源进程。 • `GNRL_EA_PARAM_5` 是源对象。 • `GNRL_EA_PARAM_6` 是目标进程。 • `GNRL_EA_PARAM_7` 是目标对象。 • `GNRL_EA_PARAM_8` 是检测到的对象的附加信息：源进程/对象和目标进程/对象的哈希。进程被阻止（`verdict_type`）：`true`或`false`。用户安全 ID（SID）.
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

键盘已授权

状态	ⓘ
组件	BadUSB 攻击防护
Windows 事件 ID	`2050`
Kaspersky Security Center 事件 ID	`00000802`

Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

网络活动已允许

状态	ⓘ
组件	防火墙
Windows 事件 ID	601
Kaspersky Security Center 事件 ID	00000259
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

禁止应用程序在测试模式下启动

状态	ⓘ
组件	应用程序控制
Windows 事件 ID	703
Kaspersky Security Center 事件 ID	GNRL_EV_APP_LAUNCH_TESTED_DENIED
事件参数	• GNRL_EA_PARAM_2 是会话用户的名称。 • GNRL_EA_PARAM_3 是手动创建的类别识别符。 • GNRL_EA_PARAM_4 是账户安全识别符（SID）。 • GNRL_EA_PARAM_5 是应用程序的数字签名信息。 • GNRL_EA_PARAM_6 是应用程序可执行文件的名称（例如，chrome.exe）。 • GNRL_EA_PARAM_7 是可执行文件的路径。 • GNRL_EA_PARAM_8 是对象的哈希 (SHA256)。 • GNRL_EA_PARAM_9 是用户正在试图运行的应用程序的版本。
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

允许应用程序在测试模式下启动

状态	ⓘ
组件	应用程序控制
Windows 事件 ID	704
Kaspersky Security Center 事件 ID	GNRL_EV_APP_LAUNCH_TESTED_ALLOW
事件参数	• GNRL_EA_PARAM_2 是会话用户的名称。 • GNRL_EA_PARAM_3 是手动创建的类别识别符。 • GNRL_EA_PARAM_4 是账户安全识别符（SID）。 • GNRL_EA_PARAM_5 是应用程序的数字签名信息。
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

打开了一个允许的页面

状态	ⓘ
组件	Web 控制
Windows 事件 ID	751
Kaspersky Security Center 事件 ID	000002f4

Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

已允许对设备执行操作

状态	ⓘ
组件	设备控制
Windows 事件 ID	801
Kaspersky Security Center 事件 ID	00000321
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

文件操作已执行

状态	ⓘ
组件	设备控制
Windows 事件 ID	808
Kaspersky Security Center 事件 ID	GNRL_EV_USB_FILE_OPERATION
事件参数	• GNRL_EA_PARAM_1 是文件操作（写或删除）。 • GNRL_EA_PARAM_2 是文件的路径。 • GNRL_EA_PARAM_3 是设备名称。 • GNRL_EA_PARAM_4 是会话用户的名称。 • GNRL_EA_PARAM_5 是硬件 ID (HWID)。
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

没有可用更新

状态	ⓘ
组件	更新
Windows 事件 ID	1020
Kaspersky Security Center 事件 ID	000003fc
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

已成功完成更新分发

状态	ⓘ
组件	更新
Windows 事件 ID	1022
Kaspersky Security Center 事件 ID	000003fe
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

正在下载文件

状态	ⓘ
组件	更新
Windows 事件 ID	1003
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

已下载文件

状态	ⓘ
组件	更新
Windows 事件 ID	1004
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

已安装文件

状态	ⓘ
组件	更新
Windows 事件 ID	1005
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

文件已更新

状态	ⓘ
组件	更新
Windows 事件 ID	1006
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

由于更新错误，文件已回滚

状态	ⓘ
组件	更新
Windows 事件 ID	1007
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

正在更新文件

状态	ⓘ
组件	更新
Windows 事件 ID	1008
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

正在分发更新

状态	ⓘ
组件	更新
Windows 事件 ID	1009
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

正在回滚文件

状态	ⓘ
组件	更新
Windows 事件 ID	1010
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

正在创建下载文件列表

状态	ⓘ
组件	更新
Windows 事件 ID	1013
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

正在下载补丁

状态	ⓘ
组件	更新
Windows 事件 ID	2150
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

正在安装补丁

状态	ⓘ
组件	更新
Windows 事件 ID	2151
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

已安装补丁

状态	ⓘ
组件	更新
Windows 事件 ID	2152
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

正在回滚补丁

状态	ⓘ
组件	更新
Windows 事件 ID	2154
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

已回滚补丁

状态	ⓘ
组件	更新
Windows 事件 ID	2155
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

已开始应用文件加密/解密规则

状态	ⓘ
组件	数据加密
Windows 事件 ID	901
Kaspersky Security Center 事件 ID	00000385
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

已完成应用文件加密/解密规则

状态	ⓘ
组件	数据加密
Windows 事件 ID	902
Kaspersky Security Center 事件 ID	00000386
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

已恢复应用文件加密/解密规则

状态	ⓘ
组件	数据加密
Windows 事件 ID	905
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

文件加密/解密已启动

状态	ⓘ
组件	数据加密
Windows 事件 ID	910
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

文件加密/解密已完成

状态	ⓘ
组件	数据加密
Windows 事件 ID	911
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

文件未被加密，因为它属于被排除的文件

状态	ⓘ
组件	数据加密
Windows 事件 ID	913
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

已启用便携模式

状态	ⓘ
组件	数据加密
Windows 事件 ID	950
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

已禁用便携模式

状态	ⓘ
组件	数据加密
Windows 事件 ID	952
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

设备加密/解密已开始

状态	ⓘ
组件	数据加密
Windows 事件 ID	1301
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

设备加密/解密已完成

状态	ⓘ
组件	数据加密
Windows 事件 ID	1302
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

设备加密/解密已恢复

状态	ⓘ
组件	数据加密
Windows 事件 ID	1304
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

设备未加密

状态	ⓘ
组件	数据加密
Windows 事件 ID	1307
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

已将设备加密/解密过程切换到主动模式

状态	ⓘ
组件	数据加密
Windows 事件 ID	1308
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

已将设备加密/解密过程切换到被动模式

状态	ⓘ
组件	数据加密
Windows 事件 ID	1309
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

加密模块已加载

状态	ⓘ
组件	数据加密
Windows 事件 ID	1310
Kaspersky Security Center 事件 ID	0000051e
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

已创建新的身份验证代理账户

状态	ⓘ
组件	数据加密
Windows 事件 ID	1330
Kaspersky Security Center 事件 ID	00000532
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

已删除身份验证代理账户

状态	ⓘ
组件	数据加密
Windows 事件 ID	1331
Kaspersky Security Center 事件 ID	00000533
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

身份验证代理账户密码已更改

状态	ⓘ
组件	数据加密
Windows 事件 ID	1332
Kaspersky Security Center 事件 ID	00000534
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

身份验证代理登录成功

状态	ⓘ
组件	数据加密
Windows 事件 ID	1333
Kaspersky Security Center 事件 ID	00000535
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

身份验证代理登录尝试失败

状态	ⓘ
组件	数据加密
Windows 事件 ID	1334
Kaspersky Security Center 事件 ID	00000536
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

已使用请求加密设备访问权限的方式访问硬盘驱动器

状态	ⓘ
组件	数据加密
Windows 事件 ID	1335
Kaspersky Security Center 事件 ID	00000537
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

使用请求加密设备访问权限的方式访问硬盘驱动器失败

状态	ⓘ
组件	数据加密
Windows 事件 ID	1336
Kaspersky Security Center 事件 ID	00000538
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

未添加账户，此账户已存在

状态	ⓘ
组件	数据加密
Windows 事件 ID	1337
Kaspersky Security Center 事件 ID	00000539
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

未修改账户，此账户不存在

状态	ⓘ
组件	数据加密
Windows 事件 ID	1338
Kaspersky Security Center 事件 ID	0000053a
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

未删除账户，此账户不存在

状态	ⓘ
组件	数据加密
Windows 事件 ID	1339
Kaspersky Security Center 事件 ID	0000053b
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

FDE 升级成功

状态	ⓘ
组件	数据加密
Windows 事件 ID	1341
Kaspersky Security Center 事件 ID	0000053d
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

FDE 升级回滚成功

状态	ⓘ
组件	数据加密
Windows 事件 ID	1343
Kaspersky Security Center 事件 ID	0000053f
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

无法从 WinRE 映像中卸载卡巴斯基磁盘加密驱动程序

状态	ⓘ
组件	数据加密
Windows 事件 ID	1346
Kaspersky Security Center 事件 ID	00000542
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

BitLocker 恢复密钥已更改

状态	ⓘ
组件	数据加密
Windows 事件 ID	1370
Kaspersky Security Center 事件 ID	0000055a
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

BitLocker 密码/PIN 已更改

状态	ⓘ
组件	数据加密
Windows 事件 ID	1371
Kaspersky Security Center 事件 ID	0000055b
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

BitLocker 恢复密钥已保存在可移动驱动器上

状态	ⓘ
组件	数据加密
Windows 事件 ID	1372
Kaspersky Security Center 事件 ID	0000055c
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

对来自 Kaspersky Anti Targeted Attack Platform 服务器的任务的处理处于非活动状态

状态	ⓘ
组件	Endpoint Sensor
Windows 事件 ID	2103
Kaspersky Security Center 事件 ID	00000837
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

Endpoint Sensor 已连接到服务器

状态	ⓘ
组件	Endpoint Sensor
Windows 事件 ID	2101
Kaspersky Security Center 事件 ID	00000835
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

已恢复与 Kaspersky Anti Targeted Attack Platform 服务器的连接

状态	ⓘ
组件	Endpoint Sensor
Windows 事件 ID	2102
Kaspersky Security Center 事件 ID	00000836
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

正在处理来自 Kaspersky Anti Targeted Attack Platform 服务器的任务

状态	ⓘ
组件	Endpoint Sensor
Windows 事件 ID	2104
Kaspersky Security Center 事件 ID	00000838
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

对象已删除

状态	ⓘ
组件	擦除数据
Windows 事件 ID	2251
Kaspersky Security Center 事件 ID	000008cb
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	–

擦除任务统计信息

状态	ⓘ
组件	Endpoint Detection and Response Expert (on-premises)
Windows 事件 ID	2853
Kaspersky Security Center 事件 ID	00000b25
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

状态	ⓘ
组件	擦除数据
Windows 事件 ID	2253
Kaspersky Security Center 事件 ID	000008cd
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

对象已隔离(Sandbox)

状态	ⓘ
组件	Sandbox
Windows 事件 ID	2602
Kaspersky Security Center 事件 ID	00000a2a
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

对象已删除(Sandbox)

状态	ⓘ
组件	Sandbox
Windows 事件 ID	2604
Kaspersky Security Center 事件 ID	00000a2c
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

IOC 扫描已开始

状态	ⓘ
组件	Endpoint Detection and Response
Windows 事件 ID	2652
Kaspersky Security Center 事件 ID	00000a5c
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

IOC 扫描已完成

状态	ⓘ
组件	Endpoint Detection and Response
Windows 事件 ID	2653
Kaspersky Security Center 事件 ID	00000a5d
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

对象已隔离(Endpoint Detection and Response)

状态	ⓘ
组件	Endpoint Detection and Response
Windows 事件 ID	2555
Kaspersky Security Center 事件 ID	000009fb
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

对象已删除(Endpoint Detection and Response)

状态	ⓘ
组件	Endpoint Detection and Response
Windows 事件 ID	2557
Kaspersky Security Center 事件 ID	000009fd
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

应用程序组件已成功更改

状态	ⓘ
组件	系统审计
Windows 事件 ID	1402
Kaspersky Security Center 事件 ID	0000057a
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

状态	ⓘ
组件	Sandbox
Windows 事件 ID	2606
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

状态	ⓘ
组件	Sandbox
Windows 事件 ID	2609

Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

状态	ⓘ
组件	Sandbox
Windows 事件 ID	2610
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

状态	ⓘ
组件	Sandbox
Windows 事件 ID	2616
Kaspersky Security Center 事件 ID	–
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	–

您设备连接到的管理服务器被设置为受信任。

状态	ⓘ
组件	管理服务器连接保护
Windows 事件 ID	3300
Kaspersky Security Center 事件 ID	00000ce4
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

您的设备已连接到新的受信任的管理服务器。

状态	ⓘ
组件	管理服务器连接保护
Windows 事件 ID	3302
Kaspersky Security Center 事件 ID	00000ce6
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

您设备连接到的管理服务器不再设置为受信任。

状态	ⓘ
组件	管理服务器连接保护
Windows 事件 ID	3303
Kaspersky Security Center 事件 ID	00000ce7
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

异步 Sandbox 检测

状态	ⓘ
组件	Sandbox
Windows 事件 ID	2619
Kaspersky Security Center 事件 ID	GNRL_EV_APP_INCIDENT_OCCURED
事件参数	• GNRL_EA_PARAM_1 是"Sandbox"组件的参数。 • GNRL_EA_PARAM_2 是对象的路径。 • GNRL_EA_PARAM_3 是事故 ID。 • GNRL_EA_PARAM_4 是对象的哈希 (SHA256)。
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

用户已成功将扫描任务发送到 Sandbox

状态	ⓘ
组件	Sandbox
Windows 事件 ID	2622
Kaspersky Security Center 事件 ID	00000a3e
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

设备已连接

状态	ⓘ
组件	设备控制
Windows 事件 ID	805
Kaspersky Security Center 事件 ID	GNRL_EV_DEVCTRL_DEV_PLUGGED
事件参数	• GNRL_EA_PARAM_1 是硬件 ID (HWID)。 • GNRL_EA_PARAM_2 是会话用户的名称。
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

设备已断开

状态	ⓘ
组件	设备控制
Windows 事件 ID	806
Kaspersky Security Center 事件 ID	GNRL_EV_DEVCTRL_DEV_UNPLUGGED
事件参数	• GNRL_EA_PARAM_1 是硬件 ID (HWID)。 • GNRL_EA_PARAM_2 是会话用户的名称。
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

卸载先前版本的应用程序发生错误

状态	ⓘ
组件	系统审计
Windows 事件 ID	246
Kaspersky Security Center 事件 ID	000000f6
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

成功连接到 EDR Expert 服务器

状态	ⓘ
组件	Endpoint Detection and Response Expert (on-premises)
Windows 事件 ID	2853
Kaspersky Security Center 事件 ID	00000b25
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

成功连接到 EDR Expert 响应服务器

状态	ⓘ
组件	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows 事件 ID	2853
Kaspersky Security Center 事件 ID	00000b25
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

成功连接到 EDR Expert 遥测采集服务器

状态	ⓘ
组件	Endpoint Detection and Response Expert (on-premises) Endpoint Detection and Response Expert (cloud)
Windows 事件 ID	2857
Kaspersky Security Center 事件 ID	00000b26
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

成功连接到 NDR 服务器

状态	ⓘ
组件	Network Detection and Response (KATA)
Windows 事件 ID	3083
Kaspersky Security Center 事件 ID	00000c0b
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

允许启动云服务客户端应用程序

状态	ⓘ
组件	Cloud Discovery
Windows 事件 ID	2210
Kaspersky Security Center 事件 ID	000008a2
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

允许访问云服务

状态	ⓘ
组件	Cloud Discovery
Windows 事件 ID	2211
Kaspersky Security Center 事件 ID	000008a3
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

访问受保护区域

状态	ⓘ
组件	系统审计
Windows 事件 ID	2004
Kaspersky Security Center 事件 ID	000007d4
Windows 事件日志（默认）	✓
Kaspersky Security Center 事件日志（默认）	✓

检测到文件或文件夹更改

状态	ⓘ / ⚠ / ⓘ
组件	系统完整性监控
Windows 事件 ID	2950
Kaspersky Security Center 事件 ID	00000b86
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

要配置此事件的保留期，请转至策略的“**事件配置**”部分并设置一般系统完整性监控事件（*检测到文件或文件夹更改*）的保留期。

对象更改太频繁。事件聚合已启动

状态	ⓘ / ⚠ / ⓘ
组件	系统完整性监控
Windows 事件 ID	2955
Kaspersky Security Center 事件 ID	00000b8b

Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

聚合期间的对象更改报告

状态	ⓘ / ⚠ / ⓘ
组件	系统完整性监控
Windows 事件 ID	2956
Kaspersky Security Center 事件 ID	00000b8c
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

要配置此事件的保留期，请转至策略的"**事件配置**"部分并设置一般系统完整性监控事件（*检测到文件或文件夹更改*）的保留期。

检测到注册表更改

状态	ⓘ / ⚠ / ⓘ
组件	系统完整性监控
Windows 事件 ID	2951
Kaspersky Security Center 事件 ID	00000b87
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

要配置此事件的保留期，请转至策略的"**事件配置**"部分并设置一般系统完整性监控事件（*检测到文件或文件夹更改*）的保留期。

检测到设备连接/断开

状态	ⓘ / ⚠ / ⓘ
组件	系统完整性监控
Windows 事件 ID	2952
Kaspersky Security Center 事件 ID	00000b88
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

要配置此事件的保留期，请转至策略的"**事件配置**"部分并设置一般系统完整性监控事件（*检测到文件或文件夹更改*）的保留期。

监控范围包括错误对象

状态	ⓘ / ⚠ / ⓘ
组件	系统完整性监控
Windows 事件 ID	2903
Kaspersky Security Center 事件 ID	00000b89
Windows 事件日志（默认）	–

Kaspersky Security Center 事件日志（默认）	✓

要配置此事件的保留期，请转至策略的"**事件配置**"部分并设置一般系统完整性监控事件（*检测到文件或文件夹更改*）的保留期。

基线已创建

状态	ⓘ
组件	系统完整性监控
Windows 事件 ID	2957
Kaspersky Security Center 事件 ID	00000b8d
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

基线已更新

状态	ⓘ
组件	系统完整性监控
Windows 事件 ID	2958
Kaspersky Security Center 事件 ID	00000b8e
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

由受信任的用户执行了一个操作

状态	ⓘ
组件	系统完整性监控
Windows 事件 ID	2962
Kaspersky Security Center 事件 ID	00000b92
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

要配置此事件的保留期，请转至策略的"**事件配置**"部分并设置一般系统完整性监控事件（*检测到文件或文件夹更改*）的保留期。

已连接到 SVM

状态	ⓘ
组件	Light Agent
Windows 事件 ID	3152
Kaspersky Security Center 事件 ID	00000c50
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

已创建新的临时密码

状态	ⓘ
组件	系统审计
Windows 事件 ID	265
Kaspersky Security Center 事件 ID	00000109
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

已连接到 Integration Server

状态	ⓘ
组件	Light Agent
Windows 事件 ID	3105
Kaspersky Security Center 事件 ID	00000c21
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

正在恢复到 Integration Server 的连接

状态	ⓘ
组件	Light Agent
Windows 事件 ID	3104
Kaspersky Security Center 事件 ID	00000c20
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

成功连接到 KUMA 服务器

状态	ⓘ
组件	KUMA 整合
Windows 事件 ID	2857
Kaspersky Security Center 事件 ID	00000b29
Windows 事件日志（默认）	–
Kaspersky Security Center 事件日志（默认）	✓

附录 7.执行防护支持的文件扩展名

Kaspersky Endpoint Security 支持防止在某些应用程序中打开 Office 格式文件。下表列出了有关支持的文件扩展名和应用程序的信息。

执行防护支持的文件扩展名

应用程序名称	可执行文件	文件扩展名
Microsoft Word	winword.exe	rtf doc dot docm docx dotx dotm docb
WordPad	wordpad.exe	docx rtf
Microsoft Excel	excel.exe	xls xlt xlm xlsx xlsm xltx xltm xlsb xla xlam xll xlw
Microsoft PowerPoint	powerpnt.exe	ppt pot pps pptx pptm potx potm ppam ppsx ppsm sldx sldm
Adobe Acrobat Foxit PDF Reader STDU Viewer Microsoft Edge Google Chrome Mozilla Firefox Yandex Browser Tor Browser	acrord32.exe FoxitReader.exe STDUViewerApp.exe MicrosoftEdge.exe chrome.exe firefox.exe browser.exe tor.exe	pdf

附录 8.执行防护预防的脚本解释器

执行防护支持以下脚本解释器：

- AutoHotkey.exe
- AutoHotkeyA32.exe
- AutoHotkeyA64.exe
- AutoHotkeyU32.exe
- AutoHotkeyU64.exe
- InstallUtil.exe
- RegAsm.exe
- RegSvcs.exe
- autoit.exe
- cmd.exe
- control.exe
- cscript.exe
- hh.exe
- mmc.exe
- msbuild.exe
- mshta.exe
- msiexec.exe
- perl.exe
- powershell.exe
- python.exe
- reg.exe
- regedit.exe
- regedt32.exe
- regsvr32.exe

- ruby.exe
- rubyw.exe
- rundll32.exe
- runlegacycplelevated.exe
- wscript.exe
- wwahost.exe

执行防护支持在 Java 运行时环境（Java.exe 和 javaw.exe 进程）中使用 Java 应用程序。

附录 9.注册表中的 IOC 扫描范围 (RegistryItem)

当您添加 **Windows 注册表 – RegistryItem** 数据类型到 IOC 扫描范围时，Kaspersky Endpoint Security 默认扫描以下注册表键：

```
HKEY_CLASSES_ROOT\htafile

HKEY_CLASSES_ROOT\batfile

HKEY_CLASSES_ROOT\exefile

HKEY_CLASSES_ROOT\comfile

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Print\Monitors

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\NetworkProvider

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Class

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\SecurityProviders

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Session Manager

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

HKEY_LOCAL_MACHINE\Software\Classes\piffile

HKEY_LOCAL_MACHINE\Software\Classes\htafile

HKEY_LOCAL_MACHINE\Software\Classes\exefile

HKEY_LOCAL_MACHINE\Software\Classes\comfile
```

```
HKEY_LOCAL_MACHINE\Software\Classes\CLSID

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\ShellServiceObjectDelayLoad

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer

HKEY_LOCAL_MACHINE\Software\Wow6432Node\Microsoft\Windows\CurrentVersion\Run

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Active Setup\Installed Components

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution
Options

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Aedebug

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon
```

附录 10.IOC 文件需求

当创建 IOC 扫描任务时，考虑以下 IOC 文件需求和限制：

- 该应用程序支持开放标准 OpenIOC 版本 1.0 和 1.1 中具有 IOC 和 XML 扩展名的 IOC 文件，用于描述妥协的指标。
- 上传 IOC 文件后，您可以直接在任务属性中手动在内置编辑器中编辑文件。Kaspersky Endpoint Security 支持编辑符合 OpenIOC 1.1 标准的 IOC 文件。无法修改符合 OpenIOC 1.0 版本的 IOC 文件的内容。
- 如果在命令行创建一个 *IOC 扫描*任务，则您上传 IOC 文件（其中一些文件不受支持），则当任务运行时，应用程序仅使用受支持的 IOC 文件。如果在命令行创建一个 *IOC 扫描*任务，你上传的所有 IOC 文件都不受支持，任务仍然可以运行，但它不会检测到任何泄露迹象。无法使用 Web 控制台或云控制台上传不受支持的 IOC 文件。
- 语义错误和 IOC 文件中不支持的 IOC 术语和标记不会导致任务执行失败。在 IOC 文件的这些部分中，应用程序检测不到匹配。
- 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。如果存在具有相同标识符的 IOC 文件，则可能会影响任务执行结果。
- 单个 IOC 文件的大小不得超过 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能超过 10 MB。如果所有文件的总大小超过 10 MB，您需要拆分 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*”任务的结果更加容易。

您可以通过单击下面的链接下载该文件，该文件包含一个表，其中包含 OpenIOC 标准的 IOC 术语的完整列表。

下载 IOC_TERMS.XLSX 文件

下表显示了应用程序支持 OpenIOC 标准的特性和限制。

OpenIOC 版本 1.0 和 1.1 的功能和支持限制。

支持条件	OpenIOC 1.0：
	
	`is`
	`isnot` （作为集合中的例外）
	`contains`
	`containsnot` （作为集合中的例外）
	OpenIOC 1.1：
	
	`is`
	`contains`
	`starts-with`
	`ends-with`
	`matches`
	`greater-than`
	`less-than`
	
	对于 Email/*，仅支持 `contains` 和 `is` 条件。为了使回顾性 IOC 扫描正常工作，在使用“`is`”条件时，IOC 文件中的电子邮件地址必须采用以下格式指定： `"name@example.org" <SMTP:name@example.org>` 。通常情况下，在运行“*IOC 扫描*”任务时，只需按以下格式指定电子邮件地址即可： `name@example.org`。

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"`：持续秒数（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"` 和 `"base64Binary"` 数据类型被解释为字符串。
	
	当 `int` 和 `date` 数据类型以间隔形式设置时，应用程序支持对其 `Content` 设置的解释：
	
	OpenIOC 1.0：
	在 `Content` 字段使用 `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` 字段使用 `TO` 运算符
	应用程序支持对“`date`”和“`duration`”数据类型的解释，如果标志设置了“`ISO 8601, Zulu time zone, UTC`”格式。

附录 11.EDR 威胁响应 API

Kaspersky Endpoint Security 12.9 for Windows 引入了对 EDR 威胁响应操作的支持 (EDR responses)，使用 Kaspersky Security Center OpenAPI。也就是说，您可以使用 Python 调用 OpenAPI 方法自动化 EDR 威胁响应。当与 SIEM 解决方案集成时，您可以调用这些方法。*Kaspersky Unified Monitoring and Analysis Platform*，卡巴斯基 SIEM 解决方案从 3.4.1 版本开始支持 EDR 威胁响应 OpenAPI。有关示例脚本，请参阅 KUMA 文档。

要执行 EDR 威胁响应操作，您需要创建一个请求并使用 KSC Open API (`AddIncident`) 发送它。处理请求后，将在 Kaspersky Security Center 控制台中创建一个特殊任务。

> 要在响应 EDR 威胁时创建任务，您必须在管理服务器和 Kaspersky Security Center Web Console 之间建立后台连接。后台连接服务在 Kaspersky Security Center Windows 14.2 或更高版本以及 Kaspersky Security Center Linux 15.2 或更高版本中可用。不支持其他控制台，包括 Kaspersky Detection and Response 解决方案的控制台。

对于 EDR 威胁响应，您需要指定基本请求参数，例如以 JSON 格式：

- `task` 是任务的类型（见下文）。
- `targetHost` 是必须运行脚本的计算机的 ID。必需参数。脚本从事件中获取此参数。
- `responseEventIncidentArea` 是运行脚本的应用程序的名称（例如，`KUMA`）。该参数添加到所创建任务的名称中。

要配置 EDR 威胁响应，您需要在“`"KLINCDT_BODY": json.dumps(data)`”参数中以 JSON 格式指定任务设置。因此，应用程序在 Kaspersky Security Center 控制台中创建“`[Response][KUMA] <task type> - <Date> <Time> - <ID>`”。

连接到 Kaspersky Security Center OpenAPI

作为 EDR 威胁响应的一部分，应用程序在 Kaspersky Security Center 控制台中创建特殊任务。创建这些任务需要在计算机和 Kaspersky Security Center 之间建立连接。为此，必须在请求中指定 Kaspersky Security Center 连接参数。

> 在 Kaspersky XDR 2.1 版本中，请求授权方法发生了变化。Kaspersky XDR 使用 PAT 令牌而不是用户名和密码身份验证。因此，无法在 Kaspersky XDR 中运行脚本。有关请求授权的更多信息，请参阅 KKaspersky XDR 帮助。

Kaspersky Security Center 连接参数

参数	类型	描述
`kscHost`	`string`	Kaspersky Security Center 管理服务器地址。必需参数。
`kscPort`	`int`	管理服务器连接端口。必需参数。
`kscCert`	`string`	用于连接到 Kaspersky Security Center 管理服务器的证书文件的路径。默认情况下，该参数设置为“`False`”。
`kscUser`	`string`	用户账户名称。必需参数。
`kscPassword`	`string`	用户账户密码。必需参数。

示例

```
# KSC connection info
# reads Environment variables by default, change with corresponding values
# KSC host, string, required
kscHost = "kscHost"
# KSC port, required, default is "13299"
kscPort = "13299"
# KSC certificate file path, default is False
kscCert = False
# KSC user, string, required
kscUser = "kscUser"
```

```
# KSC password, string, required
kscPassword = "kscPassword"

server_url = 'https://' + kscHost + ':' + str(kscPort)
    server = KlAkAdmServer.Create(
        server_url, kscUser, kscPassword, verify=kscCert)

    params = validate(args)

    data = {"targetHost": <MyHost>,
            "task": task,
            "params": params,
            "responseEventIncident": True,
            "responseEventIncidentArea":"Kuma"}

    oHostGroup = KlAkHostGroup(server)

    incdnt = oHostGroup.AddIncident({"KLINCDT_SEVERITY": 2,
                                     "KLINCDT_ADDED": paramDateTime(datetime.datetime.now()),
                                     "KLINCDT_BODY": json.dumps(data),
                                     "KLHST_WKS_HOSTNAME":  args.targetHost}).RetVal()

    oHostGroup.UpdateIncident(incdnt, {"KLINCDT_IS_HANDLED": False,
                                       "KLHST_WKS_HOSTNAME":  args.targetHost})
```

用户账户数据不受保护，因此您需要指定一个单独的用户来执行这些操作。

获取文件 – getFile

获取文件 任务设置

参数	类型	描述
md5hash	`string`	您想要获取的文件的 MD5 哈希值。
sha256hash	`string`	您想要获取的文件的 SHA256 哈希值。
path	`string`	您想要获取的文件的路径。

示例

```
type getFile = {
  task: 'getFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

删除文件 – deleteFile

删除文件 任务设置

参数	类型	描述
md5hash	`string`	您要删除的文件的 MD5 哈希值。
sha256hash	`string`	您要删除的文件的 SHA256 哈希值。

参数	类型	描述
path	`string`	您要删除的文件的路径。
searchInSubfolders?	`boolean`	在子文件夹中搜索要删除的文件。

示例

```
type deleteFile = {
  task: 'deleteFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // recursive search for a file (subfolder), optional
    searchInSubfolders?: boolean;
  };
  responseEventIncidentArea: string;
};
```

移动文件到隔离区 – quarantineFile

移动文件到隔离区 任务设置

参数	类型	描述
md5hash	`string`	您要隔离的文件的 MD5 哈希值。
sha256hash	`string`	您要隔离的文件的 SHA256 哈希值。
path	`string`	您想要隔离的文件的路径。

示例

```
type quarantineFile = {
  task: 'quarantineFile';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
  };
  responseEventIncidentArea: string;
};
```

IOC 扫描 – iocScan

IOC 扫描 任务设置

参数	类型	描述
ioc	`string`	您要用于扫描的带有 IOC 文件的 ZIP 存档的路径。
isolateHost	`boolean`	当检测到入侵指标时将计算机与网络隔离，以防止威胁蔓延。

参数	类型	描述
scanCriticalAreas	boolean	当检测到入侵指标时运行"*关键区域扫描*"任务。
quarantineObject	boolean	当检测到入侵指标时删除恶意对象。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。

示例

```
type iocScan = {
  task: 'iocScan';
  targetHost: string;
  params: {
    // the path to the zip archive with ioc files in base64 encoding
    ioc: string;
    // isolation of the computer from the network
    isolateHost: boolean;
    // critical areas scan
    scanCriticalAreas: boolean;
    // quarantine the file
    quarantineObject: boolean;
  };
  responseEventIncidentArea: string;
};
```

启动进程 – startProcess

启动进程 任务设置

参数	类型	描述
executablePath	string	用于启动进程的可执行文件的路径。
arguments?	string	用于启动进程的附加命令行参数。
workingFolder?	string	进程工作文件夹的路径。

示例

```
type startProcess = {
  task: 'startProcess';
  targetHost: string;
  params: {
    // the path to the file
    executablePath: string;
    // command line arguments, optional
    arguments?: string;
    // a working folder, optional
    workingFolder?: string;
  };
  responseEventIncidentArea: string;
};
```

终止进程 – terminateProcess

终止进程 任务设置

参数	类型	描述
md5hash	string	您想要终止其进程的文件的 MD5 哈希值。
sha256hash	string	您想要终止其进程的文件的 SHA256 哈希值。

参数	类型	描述
path	`string`	您要删除的文件的路径。
caseSensitive	`boolean`	搜索文件时区分大小写。

示例

```
type terminateProcess = {
  task: 'terminateProcess';
  targetHost: string;
  params: {
    // an empty string or a valid md5 hash of the file
    md5hash: string;
    // an empty string or a valid sha256 hash of the file
    sha256hash: string;
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

计算机网络隔离 – isolateHost

计算机网络隔离设置

参数	类型	描述
`action`	`string`	网络隔离运行模式。

示例

```
type isolateHost = {
  task: 'isolateHost';
  targetHost: string;
  params: {
    // 0 - turning off network isolation, 1 - turning on network isolation
    action: number;
  };
  responseEventIncidentArea: string;
};
```

执行防护 – preventExecution

执行防护设置

参数	类型	描述
hash	`string`	您想要阻止运行的文件的 MD5 哈希值。
path	`string`	您想要阻止运行的文件的路径。
caseSensitive	`boolean`	搜索文件时区分大小写。

示例

```
type preventExecution = {
  task: 'preventExecution';
  targetHost: string;
  params: {
    // a valid md5 hash of the file
    hash: string;
```

```
    // the path to the file
    path: string;
    // case sensitive of the file name
    caseSensitive: boolean;
  };
  responseEventIncidentArea: string;
};
```

恶意软件扫描 – onDemandScan

恶意软件扫描 任务设置

参数	类型	描述
path	string	自定义扫描的文件和文件夹的空格分隔列表。
recursive	boolean	递归扫描模式。
type	number	扫描范围。

```
ScanObjectType = Enum("ScanObjectType",
                      [
                          ("SystemMemory", 14),
                          ("StartupObjectsAndRunningProcesses", 15),
                          ("DiskBootSectors", 16),
                          ("SystemBackupStorage", 17),
                          ("Email", 18),
                          ("Folder", 22),
                          ("AllRemovableDrives", 23),
                          ("AllNetworkDrives", 24),
                          ("AllFixedDrives", 25)])
```

示例

```
type onDemandScan = {
  task: 'onDemandScan';
  targetHost: string;
  // please note, this is an array
  // array of scan object
  params: [{
    // enabling the scan object
    enabled: boolean;
    // an empty string or the path to the folder to scan
    path: string;
    // recursive scan mode
    recursive: boolean;
    // ID scan object
    type: number;
  }];
  responseEventIncidentArea: string;
};
```

附录 12.应用程序组件规则中的用户账户

要配置某些应用程序组件，您必须添加特殊规则。例如，对于 Web 控制，您必须添加包含您希望应用程序阻止的网址列表的规则。在应用程序组件规则中，您还可以配置组件的计划或选择应用程序必须应用规则的用户。

必须添加规则来配置以下应用程序组件：

- 应用程序控制。
- Web 控制。
- 设备控制。

- 日志审查。
- 自适应异常控制。
- 系统完整性监控。

从 Kaspersky Endpoint Security for Windows 12.5 开始，您不仅可以从 Active Directory 中选择用户，还可以从 Kaspersky Security Center 的用户列表中选择用户。您还可以手动输入本地用户账户数据。这意味着您可以通过以下方式添加用户：

- Active Directory（推荐）
- Kaspersky Security Center 中的用户列表
- 本地用户账户

为了正确利用所有的用户选择方法，您需要将 Kaspersky Endpoint Security 应用程序和管理插件升级到 12.5 或更高版本。

卡巴斯基建议仅在特殊情况下使用本地用户账户，当无法使用域用户账户时。使用本地账号的安全风险请参见微软知识库。如果使用本地用户账户，您对计算机的安全承担全部责任；特别是，这包括控制和限制对 Kaspersky Endpoint Security 设置的访问的责任。

应用程序使用用户的 SID（安全标识符）来识别用户。当使用 Active Directory 或 Kaspersky Security Center 用户列表中的用户账户时，应用程序将确定管理服务器上的 SID。这意味着应用程序不会给计算机带来额外的负载来识别用户。如果您向应用程序规则添加了超过 1000 个本地用户账户，应用程序将联系域控制器来识别用户。这意味着计算机的负载增加了。为了优化对计算机性能的影响，我们建议使用 Active Directory 或 Kaspersky Security Center 用户列表中的用户账户。

应用程序使用 NetBIOS 名称来识别手动添加的用户账户，格式为 `<username>` 和 `<hostname>\<username>`。NetBIOS 名称的长度最多可达 16 个字节（15 个字符）。如果计算机名称长度超过 15 个字符，应用程序将无法识别用户。然后应用程序将禁用该规则并生成错误，例如，*Web 控制: 对没有匹配的安全标识符 (SID) 的用户账户禁用规则触发*。为了使规则起作用，您必须手动缩短计算机名称。您可以从 Active Directory 或 Kaspersky Security Center 添加用户账户。在这种情况下，应用程序会自动缩短计算机名称。

Kaspersky Endpoint Security 还支持规则中的内置用户和组（例如“全部”组）。由于用户 SID 的确定方式，应用程序仅允许使用从 Active Directory 或 Kaspersky Security Center 中的用户列表添加的内置用户账户。本地添加内置用户账户的规则不起作用。

法律信息

数据提供

本节包含有关 Kaspersky Endpoint Security 应用程序可能存储在设备上并在运行期间自动传输给卡巴斯基的数据的信息。

Kaspersky 将根据法律和 Kaspersky 应用程序管理规定保护收到的信息。数据通过加密的通信通道传输。

在最终用户授权许可协议下的数据提供

如果应用激活码来激活 Kaspersky Endpoint Security，则您同意为验证应用程序的正确使用而自动定期向 Kaspersky 发送以下信息：

- Kaspersky Endpoint Security 的类型、版本和本地化；
- Kaspersky Endpoint Security 已安装更新的版本；
- 计算机 ID 和该计算机上的特定 Kaspersky Endpoint Security 安装的 ID；
- 序列号和活动密钥标识符；
- 操作系统的类型、版本和比特率，以及虚拟环境的名称（如果 Kaspersky Endpoint Security 安装在虚拟环境中）；
- 权利持有者服务的唯一请求 ID；
- 发送信息时活动的 Kaspersky Endpoint Security 组件的 ID。

Kaspersky 也可以使用这些信息来生成关于 Kaspersky 软件传播和使用的统计信息。

使用激活码，即表明您同意自动发送以上列出的数据。如果您不同意发送这些信息至 Kaspersky，则应该使用密钥文件来激活 Kaspersky Endpoint Security。

同意最终用户授权许可协议的条款，表示您同意自动发送以下信息：

- 升级 Kaspersky Endpoint Security 时：
  - Kaspersky Endpoint Security 的版本；
  - Kaspersky Endpoint Security 的 ID；
  - 活动密钥；
  - 升级任务启动的唯一 ID；
  - Kaspersky Endpoint Security 安装的唯一 ID。

- 点击 Kaspersky Endpoint Security 界面中的链接时：
  - Kaspersky Endpoint Security 的版本；
  - 操作系统版本；
  - Kaspersky Endpoint Security 激活日期；
  - 授权许可到期日期；
  - 密钥创建日期；
  - Kaspersky Endpoint Security 安装日期；
  - Kaspersky Endpoint Security 的 ID；
  - 操作系统中检测到的漏洞的 ID；
  - 为 Kaspersky Endpoint Security 安装的最新更新的 ID；
  - 检测到的带威胁的文件的哈希值，以及按照 Kaspersky 分类确定的威胁名称；
  - Kaspersky Endpoint Security 激活错误类别；
  - Kaspersky Endpoint Security 激活错误代码；
  - 密钥到期前的天数；
  - 添加密钥后经过的天数；
  - 授权许可过期后经过的天数；
  - 应用当前授权许可的计算机数量；
  - 活动密钥；
  - Kaspersky Endpoint Security 授权许可条款；
  - 授权许可当前状态；
  - 当前授权许可的类型；
  - 应用程序类型；
  - 升级任务启动的唯一 ID；
  - 计算机上 Kaspersky Endpoint Security 安装的唯一 ID；
  - Kaspersky Endpoint Security 界面语言。

Kaspersky 将根据法律和 Kaspersky 应用程序管理规定保护收到的信息。数据通过加密的通信通道传输。

请阅读最终用户授权许可协议并访问 Kaspersky 网站 了解当您接受《最终用户授权许可协议》和同意《卡巴斯基安全网络声明》之后我们如何接收、保存和销毁有关程序使用的信息。license.txt 和 ksn_<语言 ID>.txt 文件包含最终用户授权许可协议的文本，卡巴斯基安全网络声明包含在应用程序分发包中。

使用卡巴斯基安全网络时的数据提供

Kaspersky Endpoint Security 发送到 Kaspersky 的数据集取决于授权许可类型和卡巴斯基安全网络使用设置。

在不多于 4 台计算机的授权许可下使用 KSN

同意卡巴斯基安全网络声明，表示您同意自动发送以下信息：

- 有关 KSN 配置更新的信息：活动配置的标识符、收到的配置的标识符、配置更新的错误代码；
- 有关要扫描的文件和 URL 地址的信息：所扫描文件的校验和（MD5、SHA2-256、SHA1）和文件模式 (MD5)，模式大小，检测到的威胁的类型及其在权利持有人分类中的名称，反病毒数据库的标识符，其信誉被请求的 URL 地址，以及引用页 URL 地址，连接协议的标识符和使用的端口号；
- 检测到威胁的扫描任务 ID；
- 有关需要用来验证真实性的数字证书的信息：用于对扫描的对象进行签名的证书的校验和 (SHA256) 以及证书的公钥；
- 执行扫描的软件组件的标识符；
- 反病毒数据库的 ID 以及这些反病毒数据库中的记录的 ID；
- 有关计算机上的软件激活的信息：来自激活服务的已签名票证头（区域激活中心的标识符、激活码的校验和、票证的校验和、票证创建日期、票证的唯一标识符、票证版本、授权许可状态、票证有效期的开始/结束日期和时间、授权许可的唯一标识符、授权许可版本），用于对票证头签名的证书的标识符，密钥文件的校验和 (MD5)；
- 有关权利持有人的软件的信息：完整版本、类型、用于连接到 Kaspersky 服务的协议的版本。

在大于等于 5 台计算机的授权许可下使用 KSN

同意卡巴斯基安全网络声明，表示您同意自动发送以下信息：

如果选中“**卡巴斯基安全网络**”复选框并且清除“**启用扩展 KSN 模式**”复选框，则应用程序发送以下信息：

- 有关 KSN 配置更新的信息：活动配置的标识符、收到的配置的标识符、配置更新的错误代码；
- 有关要扫描的文件和 URL 地址的信息：所扫描文件的校验和（MD5、SHA2-256、SHA1）和文件模式 (MD5)，模式大小，检测到的威胁的类型及其在权利持有人分类中的名称，反病毒数据库的标识符，其信誉被请求的 URL 地址，以及引用页 URL 地址，连接协议的标识符和使用的端口号；
- 检测到威胁的扫描任务 ID；
- 有关需要用来验证真实性的数字证书的信息：用于对扫描的对象进行签名的证书的校验和 (SHA256) 以及证书的公钥；

- 执行扫描的软件组件的标识符；
- 反病毒数据库的 ID 以及这些反病毒数据库中的记录的 ID；
- 有关计算机上的软件激活的信息：来自激活服务的已签名票证头（区域激活中心的标识符、激活码的校验和、票证的校验和、票证创建日期、票证的唯一标识符、票证版本、授权许可状态、票证有效期的开始/结束日期和时间、授权许可的唯一标识符、授权许可版本），用于对票证头签名的证书的标识符，密钥文件的校验和 (MD5)；
- 有关权利持有人的软件的信息：完整版本、类型、用于连接到 Kaspersky 服务的协议的版本。

如果除“**卡巴斯基安全网络** ”复选框外还选中了“**启用扩展 KSN 模式**”复选框，则除上面列出的信息外，应用程序还会发送以下信息：

- 有关对请求的包含主机的被处理 URL 和 IP 地址的 Web 资源进行分类的结果的信息，执行分类的软件组件的版本，分类方法，以及针对 Web 资源定义的类别集；
- 有关计算机上安装的软件的信息：软件应用程序和软件供应商的名称，注册表项及其值，已安装的软件组件的文件信息（校验和（MD5、SHA2-256、SHA1）、名称、文件在计算机上的路径、大小、版本和数字签名）；
- 计算机反病毒保护状态的信息：正在使用的反病毒数据库的版本和发布时间戳、任务的 ID 和执行扫描的软件的 ID；
- 有关最终用户正在下载的文件的信息：下载的文件和下载页的 URL 和 IP 地址，下载协议标识符和连接端口号，表示 URL 是否为恶意的状态，文件的属性、大小和校验和（MD5、SHA2-256、SHA1），下载文件的进程的相关信息（校验和（MD5、SHA2-256、SHA1）、创建/构建日期和时间、自动运行状态、属性、打包程序的名称、签名信息、可执行文件标志、格式标识符和熵），文件名及其在计算机上的路径，文件的数字签名及其生成时的时间戳，发生检测的 URL 地址，页面上看上去可疑或有害的脚本的编号，有关生成的 HTTP 请求以及对它们的响应的信息；
- 有关正在运行的应用程序及其模块的信息：系统中正在运行的进程的数据（进程 ID (PID)，进程名称，有关启动进程的账户的信息，启动进程的应用程序和命令，受信任程序或进程的标志，进程文件的完整路径及其校验和（MD5、SHA2-256、SHA1），启动命令行，进程完整性级别，进程所属产品的描述（产品名称和发布者详细信息），以及所使用的数字证书和验证它们的真实性所需的信息或者关于是否缺少文件数字签名的信息），以及有关加载到进程中的模块的信息（模块的名称、大小、类型、创建日期、属性、校验和（MD5、SHA2-256、SHA1）以及在计算机上的路径），PE 文件头信息，打包程序的名称（如果文件已打包）；
- 有关所有潜在恶意对象和活动的信息：检测到的对象的名称，计算机上对象的完整路径，所处理文件的校验和（MD5、SHA2-256、SHA1），检测日期和时间，感染文件的名称、大小和路径，路径模板代码，可执行文件标志，表示对象是否为容器的指示器，打包程序名称（如果文件已打包），文件类型代码，文件格式 ID，恶意软件执行的操作列表以及软件和用户针对其做出的响应决策，反病毒数据库的 ID 和这些反病毒数据库中用于制定决策的记录的 ID，潜在恶意对象的指示器，检测到的威胁在权利持有人分类中的名称，危险等级，检测状态和检测方法，包含在已分析上下文中的原因及上下文中文件的序列号，校验和（MD5、SHA2-256、SHA1），用于发送感染消息或链接的应用程序的可执行文件的名称和属性，被阻止对象的主机的去个性化 IP 地址（IPv4 和 IPv6），文件熵，文件自动运行指示器，在系统中首次检测到文件的时间，上次发送统计信息后文件被执行的次数，通过其收到恶意对象的邮件客户端的名称、校验和（MD5, SHA2-256, SHA1）和大小，执行扫描的软件任务的 ID，表示文件信誉或签名是否经过检查的指示器，文件处理结果，为对象收集的模式的校验和 (MD5)，模式大小（以字节为单位），以及使用的检测技术的技术规格；
- 有关扫描的对象的信息：文件移入或移出的指定信任组，将文件移入该类别的理由，类别标识符，有关类别源的信息和类别数据库版本，文件的受信任证书标志，文件的供应商名称，文件版本，包含该文件的软件应用程序的名称和版本；
- 有关检测到的漏洞的信息：漏洞数据库中的漏洞 ID，漏洞危险等级；

- 有关可执行文件模拟的信息：文件大小及其校验和（MD5、SHA2-256、SHA1），模拟组件的版本，模拟深度，模拟过程中获得的逻辑块内的一系列属性和函数，可执行文件的 PE 头中的数据；

- 发起攻击的计算机的 IP 地址（IPv4 和 IPv6），被当作网络攻击目标的计算机端口号，包含攻击的 IP 数据包的协议的标识符，攻击目标（组织名称、网站），攻击响应标记，攻击的权重，信任等级；

- 有关与欺诈网络资源相关的攻击的信息，所访问网站的 DNS 和 IP 地址（IPv4 和 IPv6）；

- 请求的 Web 资源的 DNS 和 IP 地址（IPv4 或 IPv6），有关访问该 Web 资源的文件和 Web 客户端的信息，文件的名称、大小和校验和（MD5、SHA2-256、SHA1），文件的完整路径和路径模板代码，检查其数字签名的结果，及其在 KSN 中的状态；

- 有关恶意软件操作回滚的信息：有关其活动被回滚的文件的数据（文件名、文件的完整路径、文件的大小和校验和（MD5、SHA2-256、SHA1）），有关删除、重命名和复制文件以及还原注册表中的值（注册表项的命令和值）的成功和失败操作的数据，有关恶意软件修改的系统文件的信息（回滚前后）；

- 有关为自适应异常控制组件设置的排除项的信息：触发的规则的 ID 和状态，触发规则时软件执行的操作，进程或线程执行可疑活动时所用的用户账户的类型，以及有关受可疑活动支配的进程的信息（脚本 ID 或进程文件名，进程文件的完整路径，路径模板代码，进程文件的校验和（MD5、SHA2-256、SHA1））；有关执行了可疑操作的对象的信息以及受可疑活动支配的对象的信息（注册表项名称或文件名，文件的完整路径，路径模板代码和文件的校验和（MD5、SHA2-256、SHA1））。

- 有关加载的软件模块的信息：模块文件的名称、大小和校验和（MD5、SHA2-256、SHA1），模块文件的完整路径和路径模板代码，模块文件的数字签名设置，签名创建数据和时间，为模块文件签名的主体和组织的名称，加载模块的进程的 ID，模块供应商的名称，以及加载队列中模块的序列号；

- 有关软件与 KSN 服务的交互质量的信息：生成统计信息的时间段的开始和结束日期及时间，有关对所用的每个 KSN 服务的请求和连接的质量的信息（KSN 服务 ID，成功请求数量，含有来自缓存的响应的请求数量，不成功请求数量（网络问题、软件设置中禁用 KSN、路由不正确），成功请求的时间分布，取消的请求的时间分布，超出时间限制的请求的时间分布，与取自缓存的 KSN 的连接数，与 KSN 的成功连接数，与 KSN 的不成功连接数，成功事务数，不成功事务数，与 KSN 的成功连接的时间分布，与 KSN 的不成功连接的时间分布，成功事务的时间分布，不成功事务的时间分布）；

- 如果检测到潜在恶意对象，将提供进程的内存中的数据的相关信息：系统对象层次结构 (ObjectManager) 的元素、UEFI BIOS 内存中的数据、注册表项的名称及其值；

- 有关系统日志中的事件的信息：事件的时间戳，在其中发现事件的日志的名称，事件的类型和类别，事件来源的名称和事件的描述；

- 有关网络连接的信息：启动了开启端口的进程的文件的版本和校验和（MD5、SHA2-256、SHA1），进程文件的路径和数字签名，本地和远程 IP 地址，本地和远程连接端口号，连接状态，端口开启时间戳；

- 有关计算机上软件安装和激活日期的信息：销售授权许可的合作伙伴的 ID、授权许可的序列号、来自激活服务的票证的签名页眉（区域激活中心的 ID、激活代码的校验和、票证的校验和、票证的创建日期、票证的唯一 ID、票证版本、授权许可状态、票证开始/结束日期和时间、授权许可的唯一 ID、授权许可版本）、用于签署票证头的证书 ID、密钥文件的校验和（MD5）、计算机上软件安装的唯一 ID、更新的应用程序的类型和 ID、更新任务的 ID；

- 有关所有已安装的更新集的信息以及最近安装/删除的更新集的信息，导致发送更新信息的事件的类型，上次安装更新后经过的时间，有关任何当前已安装的反病毒数据库的信息；

- 有关计算机上的软件运行的信息：CPU 使用率数据，内存使用率数据（专用字节，未分页缓冲池，分页缓冲池），软件进程中的活动线程数和挂起线程数，以及错误发生前的软件运行时间；

- 自软件安装以来和上次更新以来软件转储和系统转储 (BSOD) 的次数，崩溃的软件模块的标识符和版本，软件进程中的内存堆栈，以及崩溃时的反病毒数据库的相关信息；

- 有关系统转储 (BSOD) 的数据：指示计算机上发生 BSOD 的标志，导致 BSOD 的驱动程序的名称，驱动程序中的地址和内存堆栈，指示发生 BSOD 之前操作系统会话持续时间的标志，崩溃的驱动程序的内存堆栈、存储的内存转储的类型，指示 BSOD 之前操作系统会话持续 10 分钟以上的标志、转储的唯一标识符，BSOD 的时间戳；

- 有关软件组件运行期间出现的错误或性能问题的信息：软件的状态 ID，错误类型，代码和原因以及发生错误的时间，组件的 ID，出现错误的产品的组件、模块和进程的 ID，出现错误的任务或更新类别的 ID，软件使用的驱动程序的日志（错误代码、模块名称、源文件的名称和出现错误的行）；

- 有关反病毒数据库和软件组件更新的信息：在上次更新过程中下载以及当前更新过程中正在下载的索引文件的名称、日期和时间；

- 有关软件操作异常终止的信息：转储的创建时间戳、类型，导致软件操作异常终止的事件的类型（意外断电、第三方应用程序崩溃），意外断电的日期和时间；

- 有关软件驱动程序与硬件和软件的兼容性的信息：有关限制软件组件功能的操作系统属性的信息（安全启动、KPTI、WHQL 强制、BitLocker、区分大小写），安装的下载软件的类型（UEFI、BIOS），受信任平台模块 (TPM) 标识符，TPM 规范版本，有关计算机上安装的 CPU 的信息，代码完整性和 Device Guard 的运行模式和参数，驱动程序的运行模式和使用当前模式的原因，软件驱动程序的版本，计算机的软件和硬件虚拟化支持状态；

- 有关导致出错的第三方应用程序的信息：应用程序名称、版本和本地化，系统应用程序日志中关于该错误的错误代码和信息，发生错误的地址和第三方应用程序的内存堆栈，指示软件组件中出现错误的标志，出错之前第三方应用程序的运行时长，出错的应用程序进程映像的校验和（MD5、SHA2-256、SHA1），应用程序进程映像的路径和路径模板代码，系统日志中与该应用程序相关的错误说明信息，发生错误的应用程序模块的相关信息（异常标识符，应用程序模块中偏移量形式的崩溃内存地址，模块的名称和版本，权利持有人插件中的应用程序崩溃标识符以及崩溃的内存堆栈，崩溃之前应用程序会话的持续时间）；

- 软件更新程序组件的版本，在组件的生命周期内运行更新任务时更新程序组件崩溃的次数，更新任务类型的 ID，更新程序组件完成更新任务的失败尝试次数；

- 有关软件系统监控组件运行的信息：组件的完整版本，启动组件时的日期和时间，溢出事件队列的事件的代码及此类事件的数量，队列溢出事件的总数，有关事件的发起程序的进程的文件的信息（文件名及其在计算机上的路径、文件路径的模板代码、与文件关联的进程的校验和（MD5、SHA2-256、SHA1）、文件版本），发生的事件拦截的标识符，拦截筛选器的完整版本，拦截的事件的类型的标识符，事件队列的大小和队列中第一个事件与当前事件之间的事件数量，队列中过期事件的数量，有关当前事件的发起程序进程的文件的信息（文件名及其在计算机上的路径，文件路径的模板代码，与文件关联的进程的校验和（MD5、SHA2-256、SHA1）），事件处理持续时间，事件处理最大持续时间，发送统计信息的概率，有关超过处理时间限制的操作系统事件的信息（事件的日期和时间，反病毒数据库的重复初始化次数，反病毒数据库更新后最近一次重复初始化的日期和时间，每个系统监控组件的事件处理延迟时间，排队的事件数量，已处理的事件数量，当前类型的延迟事件数量，当前类型的事件的总延迟时间，所有事件的总延迟时间）；

- 发生软件问题时来自 Windows 事件跟踪工具（Windows 事件跟踪，ETW）的信息，Microsoft 的 SysConfig/SysConfigEx/WinSATAssessment 事件的提供方：有关计算机的信息（型号、制造商、外壳外形规格、版本），有关 Windows 性能度量标准的信息（WinSAT 评估、Windows 性能指标），域名，有关物理和逻辑处理器的信息（物理和逻辑处理器数量、制造商、型号、步进等级、核心数、时钟频率、CPUID、缓存特征、逻辑处理器特征、指示的模式和指令的指示器），有关 RAM 模块的信息（类型、外形规格、制造商、型号、容量、内存分配粒度），有关网络接口的信息（IP 和 MAC 地址、名称、描述、网络接口配置、网络数据包按类型细分的数量和大小、网络交换速度、网络错误按类型细分的数量），IDE 控制器的配置，DNS 服务器的 IP 地址，有关视频卡的信息（型号、描述、制造商、兼容性、显存容量、屏幕权限、每像素位数，BIOS 版本），有关即插即用设备的信息（名称、描述、设备标识符 [PnP, ACPI]），有关磁盘和存储设备的信息（磁盘或闪存驱动器数量、制造商、型号、磁盘容量、柱面数、每柱面磁道数、每磁道扇区数、扇区容量、缓存特征、序号、分区数、SCSI 控制器配置），有关逻辑磁盘的信息（序号、分区容量、卷容量、卷号、分区类型、文件系统类型、簇数、簇大小、每簇扇区数、空簇和已占用簇的数量、可启动卷号、相对于磁盘起始处的偏移分区地址）。有关 BIOS 主板的信息（制造商、发布日期、版本），有关主板的信息（制造商、型号、类型），有关物理内存的信息（共享和可用容量），有关操作系统服务的信息（名称、描述、状态、标签、有关进程的信息 [名称和 PID]），计算机的能耗参数，中断控制器的配置，Windows 系统文件夹（Windows 和 System32）的路径，有关操作系统的信息（版本、内部版本号、发布日期、名称、类型、安装日期），页面文件大小，有关监视器的信息（编号、制造商、屏幕权限、分辨率能力、类型），有关视频卡驱动程序的信息（制造商、发布日期、版本）；

- 来自 ETW 的信息，Microsoft 的 EventTrace/EventMetadata 事件的提供方：有关系统事件序列的信息（类型、时间、日期、时区），带跟踪结果的文件元数据（名称、结构、跟踪参数、按类型细分的跟踪操作数），有关操作系统的信息（名称、类型、版本、内部版本号、发布日期、启动时间）；

- 来自 ETW 的信息，Microsoft 的进程/Microsoft Windows 内核进程/Microsoft Windows 内核处理器电源事件的提供方：有关已启动和已完成进程的信息（名称、PID、启动参数、命令行、返回代码、电源管理参数、启动和完成时间、访问令牌类型、SID、SessionID、已安装的描述符数），有关线程优先级变化的信息（TID、优先级、时间），有关进程的磁盘操作的信息（类型、时间、容量、编号），可用内存进程的结构和容量的更改历史记录；

- 来自 ETW 的信息，Microsoft 的 StackWalk/Perfinfo 事件的提供方：有关性能计数器的信息（单个代码段的性能、函数调用的序列、PID、TID 以及 ISR 和 DPC 的地址和属性）；

- 来自 ETW 的信息，Microsoft 的 KernelTraceControl-ImageID 事件的提供方：有关可执行文件和动态库的信息（名称、映像大小、完整路径），有关 PDB 文件的信息（名称、标识符），可执行文件的 VERSIONINFO 资源数据（名称、描述、创建者、本地化、应用程序版本和标识符、文件版本和标识符）；

- 来自 ETW 的信息，Microsoft 的 FileIo/DiskIo/映像/Windows 内核磁盘事件的提供方：有关文件和磁盘操作的信息（类型、容量、开始时间、完成时间、持续时间、完成状态、PID、TID、驱动程序函数调用地址、I/O 请求数据包 (IRP)、Windows 文件对象属性），有关文件和磁盘操作所涉及的文件的信息（名称、版本、大小、完整路径、属性、偏移、映像校验和、打开和访问选项）；

- 来自 ETW 的信息，Microsoft 的 PageFault 事件的提供方：有关内存页面访问错误的信息（地址、时间、容量、PID、TID、Windows 文件对象属性、内存分配参数）；

- 来自 ETW 的信息，Microsoft 的线程事件的提供方：有关线程创建/完成的信息，有关已启动的线程的信息（PID、TID、堆栈大小、CPU 资源的优先级和分配、 I/O 资源、线程间的内存页面、堆栈地址、初始函数地址、线程环境块 (TEB) 的地址、Windows 服务标签）；

- 来自 ETW 的信息，Microsoft 的 Windows 内核内存事件的提供方：有关内存管理操作的信息（完成状态、时间、数量、PID），内存分配结构（类型、容量、SessionID、PID）；

- 有关发生性能问题时软件操作的信息：软件安装标识符，性能下降的类型和值，有关软件内的事件序列的信息（时间、时区、类型、完成状态、软件组件标识符、软件运行场景标识符、TID、PID、函数调用地址），有关要检查的网络连接的信息（URL、连接方向、网络数据包大小），有关 PDB 文件的信息（名称、标识符、可执行文件的映像大小），有关要检查的文件的信息（名称、完整路径、校验和），软件性能监控参数；

- 有关操作系统上次重启失败的信息：操作系统安装以来重启失败的次数，系统转储数据（错误的代码和参数，导致操作系统运行出错的模块的名称、版本和校验和 (CRC32)，模块内偏移量形式的错误地址，系统转储的校验和（MD5、SHA2-256、SHA1））；
- 验证用于对文件进行签名的数字证书的真实性所需的信息：证书的指纹，校验和算法，证书的公钥和序列号，证书颁发者的名称，证书验证的结果和证书的数据库标识符；
- 有关对软件的自我防护执行攻击的进程的信息：进程文件的名称和大小，其校验和（MD5、SHA2-256、SHA1），进程文件的完整路径和文件路径的模板代码，创建/构建时间戳，可执行文件标志，进程文件的属性，用于对进程文件签名的证书的相关信息，用于启动进程的账户的代码，为访问进程所执行的操作的 ID，用于执行操作的资源的类型（进程，文件，注册表对象，FindWindow 搜索函数），用于执行操作的资源的名称，表示操作成功的标志，进程文件的状态及其在 KSN 中的签名；
- 有关权利人软件的信息：所用软件的完整版本、类型、本地化和运行状态、安装的软件组件的版本及其运行状态、安装的软件更新的信息、目标过滤器的值、用于连接到权利人服务的协议的版本；
- 有关计算机上安装的硬件的信息：类型、名称、型号名称、固件版本、内置和所连接设备的参数、带有已安装软件的计算机的唯一标识符；
- 有关操作系统和已安装更新的版本的信息，操作系统运行模式的字大小、版本和参数，操作系统内核文件的版本和检验和（MD5、SHA2-256、SHA1），以及操作系统启动日期和时间；
- 可执行和非可执行文件（完整或部分）；
- 计算机 RAM 的一部分；
- 操作系统引导过程中涉及的扇区；
- 网络流量数据包；
- 包含可疑对象和恶意对象的网页和电子邮件；
- WMI 存储库的类和类实例的描述；
- 应用程序分析报告：
  - 所发送文件的名称、大小和版本、其说明和校验和（MD5、SHA2-256、SHA1）、文件格式标识符、文件供应商名称、文件所属产品名称、计算机上文件的完整路径、路径的模板代码、文件的创建和修改时间戳；
  - 证书有效期的开始和结束日期/时间（如果文件有数字签名）、签名的日期和时间、证书颁发者的名称、证书持有人的信息、指纹、证书的公钥和适当的算法以及证书的序列号；
  - 运行进程的帐户的名称；
  - 运行进程的计算机名称的校验和（MD5、SHA2-256、SHA1）；
  - 进程窗口标题；
  - 反病毒数据库的标识符，根据权利人的分类检测到的威胁的名称；
  - 已安装软件授权许可的数据、ID、类型和到期日期；
  - 提供信息的计算机的本地时间；
  - 进程访问的文件的名称和路径；

- 进程访问的注册表项名称及其值；
- 进程访问的 URL 和 IP 地址；
- 下载正在运行文件的 URL和 IP 地址。

使用 Detection and Response 解决方案时的数据提供

在安装了 Kaspersky Endpoint Security 的计算机上，将存储为自动发送到Kaspersky Endpoint Detection and Response、Kaspersky Sandbox 和 Kaspersky Anti Targeted Attack Platform 服务器而准备的数据。文件以纯文本、未加密的形式存储在计算机上。

具体的数据集取决于使用 Kaspersky Endpoint Security 的解决方案。

Kaspersky Endpoint Detection and Response

当卸载 Kaspersky Endpoint Security 时，应用程序本地存储在计算机上的所有数据将从计算机中删除。

作为“IOC 扫描”任务执行（标准任务）结果收到的数据

Kaspersky Endpoint Security 自动提交“*IOC 扫描*”任务执行结果数据到 Kaspersky Security Center。

“*IOC 扫描*”任务执行结果中的数据可能包含以下信息：

- ARP 表中的 IP 地址
- ARP 表中的物理地址
- DNS 记录类型和名称
- 受保护计算机的 IP 地址
- 受保护计算机的物理地址（MAC 地址）
- 事件日志条目中的标识符
- 日志中的数据源名称
- 日志名称
- 事件时间
- 文件的 MD5 和 SHA256 哈希值
- 文件的全名（包括路径）

- 文件大小
- 扫描期间建立连接的远程 IP 地址和端口
- 本地适配器 IP 地址
- 在本地适配器上打开端口
- 协议作为数字（符合 IANA 标准）
- 进程名称
- 处理参数
- 进程文件的路径
- 进程的 Windows 标识符 (PID)
- 父进程的 Windows 标识符 (PID)
- 启动进程的用户账户
- 进程开始的日期和时间
- 服务名称
- 服务说明
- DLL 服务的路径和名称（对于 svchost）
- 服务可执行文件的路径和名称
- 服务的 Windows 标识符 (PID)
- 服务类型（例如，内核驱动程序或适配器）
- 服务状态
- 服务启动模式
- 用户账户名称
- 卷名
- 卷字母
- 卷类型
- Windows 注册表值
- 注册表巢值
- 注册表项路径（没有巢和值名称）
- 注册表设置

- 系统（环境）
- 计算机上安装的操作系统的名称和版本
- 受保护计算机的网络名称
- 受保护计算机所属的域或组
- 浏览器名称
- 浏览器版本
- 上次访问 Web 资源的时间
- 来自 HTTP 请求的 URL
- 用于 HTTP 请求的账户名称
- 发出 HTTP 请求的进程的文件名
- 发出 HTTP 请求的进程文件的完整路径
- 发出 HTTP 请求的进程的 Windows 标识符 (PID)
- HTTP Referer（HTTP 请求源 URL）
- 通过 HTTP 请求的资源的 URI
- 有关 HTTP 用户代理（发出 HTTP 请求的应用程序）的信息
- HTTP 请求执行时间
- 发出 HTTP 查询的进程的唯一标识符

用于创建威胁发展链的数据

创建威胁发展链的数据默认保存 7 天。数据会自动发送到 Kaspersky Security Center。

用于创建威胁发展链的数据可能包含以下信息：

- 事件日期和时间
- 检测名称
- 扫描模式
- 与检测相关的最后一个操作的状态
- 检测处理失败的原因
- 检测到的对象类型

- 检测到的对象名称
- 对象处理后的威胁状态
- 对对象执行操作失败的原因
- 为回滚恶意操作而执行的操作
- 已处理对象的相关信息：
  - 进程的唯一标识符
  - 父进程的唯一标识符
  - 进程文件的唯一标识符
  - Windows 进程标识符（PID）
  - 进程命令行
  - 启动进程的用户账户
  - 运行进程的登录会话的代码
  - 运行进程的会话类型
  - 正在处理的进程的完整性级别
  - 在特权本地和域组中启动进程的用户账户的成员身份
  - 已处理对象的标识符
  - 已处理对象的全名
  - 受保护设备的标识符
  - 对象的全名（本地文件名或已下载文件网址）
  - 已处理对象的 MD5 或 SHA256 哈希
  - 已处理对象的类型
  - 已处理对象的创建日期
  - 已处理对象最后修改的日期
  - 已处理对象的大小
  - 已处理对象的属性
  - 签署已处理对象的组织
  - 已处理对象数字证书校验结果
  - 已处理对象的安全标识符 (SID)

- 已处理对象的时区标识
- 已处理对象下载网址（仅适用于磁盘文件）
- 下载文件的应用程序的名称
- 下载文件的应用程序的 MD5 和 SHA256 哈希
- 最后修改文件的应用程序的名称
- 最后修改文件的应用程序的 MD5 和 SHA256 哈希
- 已处理对象启动数
- 已处理对象首次启动的日期和时间
- 文件的唯一标识符
- 文件全名（本地文件名或下载文件网址）
- 已处理的 Windows 注册表变量的路径
- 已处理的 Windows 注册表变量的名称
- 已处理的 Windows 注册表变量的值
- 已处理的 Windows 注册表变量的类型
- 自动运行点中已处理注册表项成员关系的指示器
- 已处理的 Web 请求的网址
- 已处理的 Web 请求的链接源
- 已处理的 Web 请求的用户代理
- 已处理的 Web 请求的类型（`GET` 或 `POST`）
- 已处理的 Web 请求的本地 IP 端口
- 已处理的 Web 请求的远程 IP 端口
- 已处理的 Web 请求的连接方向（入站或出站）
- 嵌入恶意代码的进程的标识符

Kaspersky Sandbox

当卸载 Kaspersky Endpoint Security 时，应用程序本地存储在计算机上的所有数据将从计算机中删除。

服务数据

Kaspersky Endpoint Security 存储在自动响应期间处理的以下数据：

- 在配置 Kaspersky Endpoint Security 的内置代理期间由用户输入的已处理文件和数据：
  - 已隔离的文件
  - 用于与 Kaspersky Sandbox 集成的证书的公钥
- Kaspersky Endpoint Security 内置代理的缓存：
  - 扫描结果写入缓存的时间
  - 扫描任务的 MD5 哈希
  - 扫描任务标识符
  - 对象的扫描结果
- 对象扫描请求队列：
  - 队列中对象的 ID
  - 对象放入队列的时间
  - 队列中对象的处理状态
  - 创建对象扫描任务的操作系统中用户会话的 ID
  - 其账户用于创建任务的操作系统用户的系统标识符 (SID)
  - 对象扫描任务的 MD5 哈希
- 有关 Kaspersky Endpoint Security 内置代理正在等待来自 Kaspersky Sandbox 的扫描结果的任务的信息：
  - 收到对象扫描任务的时间
  - 对象处理状态
  - 创建对象扫描任务的操作系统中用户会话的 ID
  - 对象扫描任务的标识符
  - 对象扫描任务的 MD5 哈希
  - 其账户用于创建任务的操作系统用户的系统标识符 (SID)
  - 自动创建的 IOC 的 XML Schema
  - 扫描对象的 MD5 或 SHA256 哈希
  - 处理错误

- 为其创建任务的对象的名称
- 对象的扫描结果

Kaspersky Sandbox 请求中的数据

来自 Kaspersky Endpoint Security 内置代理对 Kaspersky Sandbox 的请求的以下数据存储在本地计算机上：

- 扫描任务的 MD5 哈希
- 扫描任务标识符
- 已扫描对象和所有相关文件

作为“IOC 扫描”任务执行（独立任务）结果接收的数据

Kaspersky Endpoint Security 自动提交“*IOC 扫描*”任务执行结果数据到 Kaspersky Security Center。

“*IOC 扫描*”任务执行结果中的数据可能包含以下信息：

- ARP 表中的 IP 地址
- ARP 表中的物理地址
- DNS 记录类型和名称
- 受保护计算机的 IP 地址
- 受保护计算机的物理地址（MAC 地址）
- 事件日志条目中的标识符
- 日志中的数据源名称
- 日志名称
- 事件时间
- 文件的 MD5 和 SHA256 哈希值
- 文件的全名（包括路径）
- 文件大小
- 扫描期间建立连接的远程 IP 地址和端口
- 本地适配器 IP 地址
- 在本地适配器上打开端口

- 协议作为数字（符合 IANA 标准）
- 进程名称
- 处理参数
- 进程文件的路径
- 进程的 Windows 标识符 (PID)
- 父进程的 Windows 标识符 (PID)
- 启动进程的用户账户
- 进程开始的日期和时间
- 服务名称
- 服务说明
- DLL 服务的路径和名称（对于 svchost）
- 服务可执行文件的路径和名称
- 服务的 Windows 标识符 (PID)
- 服务类型（例如，内核驱动程序或适配器）
- 服务状态
- 服务启动模式
- 用户账户名称
- 卷名
- 卷字母
- 卷类型
- Windows 注册表值
- 注册表巢值
- 注册表项路径（没有巢和值名称）
- 注册表设置
- 系统（环境）
- 计算机上安装的操作系统的名称和版本
- 受保护计算机的网络名称
- 受保护计算机所属的域或组

- 浏览器名称
- 浏览器版本
- 上次访问 Web 资源的时间
- 来自 HTTP 请求的 URL
- 用于 HTTP 请求的账户名称
- 发出 HTTP 请求的进程的文件名
- 发出 HTTP 请求的进程文件的完整路径
- 发出 HTTP 请求的进程的 Windows 标识符 (PID)
- HTTP Referer（HTTP 请求源 URL）
- 通过 HTTP 请求的资源的 URI
- 有关 HTTP 用户代理（发出 HTTP 请求的应用程序）的信息
- HTTP 请求执行时间
- 发出 HTTP 查询的进程的唯一标识符

Kaspersky Endpoint Detection and Response Expert（本地部署）

当卸载 Kaspersky Endpoint Security 时，应用程序本地存储在计算机上的所有数据将从计算机中删除。

服务数据

Kaspersky Endpoint Security 的内置代理在本地存储以下数据：

- 与 EDR Expert（本地部署）组件集成所需的数据：
  - 连接到 KATA Central Node 服务器的地址和端口
  - 连接到遥测传输服务器的地址和端口
  - 连接到响应服务器的地址和端口
  - 有关用于与 KATA Central Node 集成的证书的信息
  - 有关用于与遥测传输服务器集成的证书的信息
  - 有关用于与响应服务器集成的证书的信息
- 已隔离的文件

来自已传输遥测事件的数据

- **遥测数据**
  - 文件数据：
    - 文件的唯一标识符
    - 文件类型
    - 完整文件路径
    - 文件大小
    - 文件属性
    - 区域标识符
    - 创建文件的日期和时间
    - 上次修改文件的日期和时间
    - 原始文件名
    - 应用程序名称
    - 应用程序版本
    - 应用程序供应商
    - 文件描述
    - 文件版本
    - 对象的 MD5 和 SHA256 哈希值
    - 文件签名验证结果
    - 证书颁发机构名称
    - 证书持有人姓名
    - 证书序列号
  - AMSI 扫描相关数据：
    - 发起活动的进程的唯一标识符
    - 传递给 AMSI 的对象的内容类型
    - 传递给 AMSI 的对象的内容

    - 对象名称
    - 对象的 MD5 和 SHA256 哈希值
- 应用程序阻止相关数据：
    - 发起应用程序阻止的进程的唯一标识符
    - 父进程的唯一标识符
    - 进程的唯一系统标识符
    - 用于启动进程的命令
    - 登录会话 ID
    - 进程完整性水平
    - 进程状态
    - 进程文件的唯一标识符
    - 进程命令行
    - 已解释文件的唯一标识符列表
- 关于被阻止的文件打开的数据：
    - 发起文件阻止的进程的唯一标识符
    - 文件的唯一标识符
- 驱动程序加载数据：
    - 已加载驱动程序的唯一标识符
- 与事件相关的数据：
    - 事件的唯一标识符
    - 事件日期和时间
- 文件修改数据：
    - 发起文件修改的进程的唯一标识符
    - 文件的唯一标识符
    - 修改操作的类型
    - 指示该文件将在计算机重启后删除的标志
    - 已修改文件的唯一标识符
    - 文件修改前的唯一标识符

    - 一组位标志，用于确定文件打开方式
    - 关于访问控制列表操作的数据
    - 关于文件所有权或父组变更的数据
- 登录会话数据：
    - 登录会话 ID
    - 登录用户的用户名
    - 用户账户类型
    - 会话类型
- 网络连接数据：
    - 发起连接的进程的唯一标识符
    - 用于发起连接的本地 IP 地址
    - 连接端点的远程 IP 地址
    - 连接方向
    - 数据传输协议
    - HTTP 方法
    - 不带主机名的路径
    - 主机名
    - 连接瞬间的动态过程状态
    - 指示连接在原始套接字级别是否打开的标志
    - 连接会话中使用的 TLS 版本
    - TLS 服务器的名称
    - TLS 服务器证书的 MD5 和 SHA1 哈希值
    - 证书的主题备用名称 (SAN) 列表
    - TLS 证书颁发机构名称
    - 证书序列号
    - 使用的加密算法
    - 证书的生效日期和终止日期

    - TLS 客户端的 JA3 指纹
    - 服务器的 JA3S 指纹
- 在监听网络端口时捕获的数据：
    - 发起连接的进程的唯一标识符
- 命令行输入数据：
    - 发起控制台输入的进程的唯一标识符
    - 控制台输入类型
    - 用户或进程输入的文本
- 进程创建相关数据：
    - 进程的唯一标识符
    - 父进程的唯一标识符
    - 进程的唯一系统标识符
    - 用于启动进程的命令
    - 登录会话 ID
    - 进程完整性水平
    - 进程文件的唯一标识符
    - 已解释文件的唯一标识符列表
    - 进程类型
- 进程加载的模块的相关数据：
    - 发起下载的进程的唯一标识符
    - 上传到进程的文件的完整路径
    - 模块文件的唯一标识符
    - 如果加载的文件是 .NET 模块，则为 .NET 程序集的完整限定名称
    - .NET 程序集清单中定义的标志
- 进程终止相关数据：
    - 终止的进程的唯一标识符

- 注册表修改相关数据：
  - 发起注册表修改的进程的唯一标识符
  - 注册表操作类型
  - 注册表项的完整路径
  - 注册表项中值的名称
  - 注册表项值中存储的数据类型
  - 注册表项值中指定的数据
  - 重命名前的密钥名称
  - 有关密钥或主密钥组所有权变更的信息
  - 密钥访问控制列表 (ACL) 的更改列表
- 关于检测到的威胁及其处理的数据：
  - 表示威胁检测在后台运行的标志
  - 威胁判定
  - 判定名称
  - 数据库记录的唯一标识符
  - 威胁记录保存到数据库的时间
  - 威胁处理模式
  - 受感染的对象类型
  - 受感染的对象名称
  - 对象的 MD5 和 SHA256 哈希值
  - 受感染对象的唯一标识符
  - 从互联网下载受感染对象的进程的唯一标识符
  - 下载受感染对象的 URL
  - 发送受感染对象的发件人电子邮件地址
  - 接收受感染对象的网络协议
  - 接收受感染对象的本地地址
  - 接收受感染对象的外部地址

    - 对象内容类型
    - 对象内容
- 关于进程访问的数据：
    - 尝试访问的进程的唯一标识符
    - 被访问的目标进程的唯一标识符
    - 从目标进程请求的权限集
    - 操作类型
    - 访问进程时发生的调用集合
    - 源进程描述符
    - 目标进程描述符
- DNS 相关数据：
    - 发起 DNS 查询的进程的唯一标识符
    - DNS 服务器 IP 地址
    - 用于管理 DNS 查询行为的标志
    - 请求完成状态
    - DNS 查询中指定的完全限定域名
    - DNS 查询中的数据类型
    - DNS 服务器响应
- 关于代码注入的数据：
    - 尝试注入代码的进程的唯一标识符
    - 已使用的访问方法
    - 检测到注入代码时的调用集合
    - 上传代码的目标进程的唯一标识符
    - 目标进程命令序列变化的相关数据
    - 目标进程地址
    - 上传到目标进程的 DLL 库的名称
    - DDL 文件的完整路径

- 关于命名通道操作的数据：
  - 创建或连接到通道的进程的唯一标识符
  - 命名通道的全名
  - 操作类型（创建或连接）
- 关于 WMI 查询的数据：
  - 发起 WMI 操作的进程的唯一标识符
  - WMI 操作类型
  - WMI 查询的目标设备名称
  - 发起 WMI 查询的用户帐户
  - WMI 查询的文本
  - 执行 WMI 查询的命名空间
  - WMI 过滤器名称
  - 使用者对象的名称
  - 描述使用者对象操作的文本
- 关于 LDAP 查询的数据：
  - 发出 LDAP 查询的进程的唯一标识符
  - LDAP 查询的搜索范围
  - LDAP 过滤器
  - 指定查询所指向的 Active Directory 分区的参数
  - LDAP 搜索属性
- 已连接 USB 设备的相关数据：
  - USB 设备操作类型
  - USB 设备类型
  - USB 设备的标识符
  - USB 设备名称
  - USB 设备的路径
  - 指示 USB 设备为系统驱动器的标志
- 关于计划任务的创建、删除和修改的数据

- 关于服务的创建、删除和修改的数据
- 关于文件系统挂载/卸载的数据
- 关于 EDR Expert on-premise 组件操作的数据：
  - 关于启动/停止代理的信息
  - 有关安装/卸载代理的信息
  - 代理启动的唯一标识符
  - 代理进程的系统标识符
  - 代理进程的唯一标识符
  - 终止代理的原因
  - 代理进程终止代码
- 事件过滤设置：
  - 模块名称
  - 对象完整路径
  - 对象的 MD5 和 SHA256 哈希值
  - Windows 事件日志中条目的标识符
  - 数字证书设置
  - 流量方向、IP 地址、端口、协议、可执行文件的完整路径
  - 用户名
  - 用户登录类型
  - 应用过滤器的遥测事件类型

从 EDR Expert 组件到 Kaspersky Endpoint Security 内置代理的请求数据

- 常规任务设置：
  - 任务类型
  - 任务计划设置
  - 可以运行任务的账户的名称和密码
  - 设置的版本

    - 隔离对象的标识符
    - 对象的路径
    - 对象的 MD5 和 SHA256 哈希值
    - 使用参数启动进程的命令行
    - 完成任务后执行的附加操作的标志
    - 要从服务器检索的 IOC 文件标识符
    - IOC 文件
    - 服务名称
    - 服务启动类型
    - 必须接收*获取取证*任务结果的文件夹
    - *获取取证*任务的对象名称和扩展名的掩码
- 网络隔离设置：
    - 设置类型
    - 设置的版本
    - 网络隔离排除项和排除设置列表：流量方向、IP 地址、端口、协议和可执行文件的完整路径
    - 附加操作的标志
    - 自动隔离禁用时间
- 执行防护设置:
    - 设置类型
    - 设置的版本
    - 执行预防规则和规则设置列表：对象路径、对象类型、对象的 MD5 和 SHA256 哈希值
    - 附加操作的标志

从 Kaspersky Endpoint Security 到 EDR Expert 组件的请求数据

与 EDR Expert（本地部署）解决方案集成时，以下数据将存储在本地计算机上。

- 在同步请求中：
  - 独一 ID
  - 服务器网址的基本部分
  - 计算机名称
  - 计算机 IP 地址
  - 计算机 MAC 地址
  - 计算机上的本地时间
  - Kaspersky Endpoint Security 的自我保护状态
  - 计算机上安装的操作系统的名称和版本
  - Kaspersky Endpoint Security 的版本
  - 应用程序设置和任务设置的版本
  - 任务状态：任务标识符、执行状态、错误代码
- 在从服务器获取文件的请求中：
  - 文件的唯一标识符
  - 唯一的 Kaspersky Endpoint Security 标识符
  - 证书的唯一标识符
  - 安装了 Central Node 组件的服务器网址基本部分
  - 主机 IP 地址
- 在任务执行结果的报告中：
  - 主机 IP 地址
  - 有关在 IOC 扫描或 YARA 扫描期间检测到的对象的信息
  - 完成任务后执行的附加操作的标志
  - 任务执行错误和返回码
  - 任务完成状态
  - 任务完成时间

    - 用于执行任务的设置版本
    - 有关提交到服务器的对象、隔离对象和从隔离区恢复的对象的信息：对象路径、MD5 和 SHA256 哈希值、隔离对象的标识符
    - 有关应服务器请求在计算机上启动或停止的进程的信息：PID 和 UniquePID、错误代码、对象的 MD5 和 SHA256 哈希值
    - 有关应服务器请求在计算机上启动或停止的服务的信息：服务名称、启动类型、错误代码、服务文件映像的 MD5 和 SHA256 哈希值
    - 有关为 YARA 扫描创建内存转储的对象的信息（路径、转储文件标识符）
    - 服务器请求的文件
- 正在运行的进程的数据：
    - 可执行文件名，包括完整路径和扩展名
    - 进程自动运行参数
    - 进程 ID
    - 登录会话 ID
    - 登录会话名称
    - 进程开始的日期和时间
    - 对象的 MD5 和 SHA256 哈希值
- 文件数据：
    - 文件路径
    - 文件名
    - 文件大小
    - 文件属性
    - 创建文件的日期和时间
    - 上次修改文件的日期和时间
    - 文件描述
    - 公司名称
    - 对象的 MD5 和 SHA256 哈希值
    - 注册表项（用于自动运行点）

- 检索有关对象的信息时发生的错误数据：
  - 发生错误时处理的对象全名
  - 错误代码
- YARA 扫描结果中的数据：

  Kaspersky Endpoint Security 内置代理自动将 YARA 扫描结果传输至 Kaspersky Anti Targeted Attack Platform 以构建威胁发展链。

  数据临时存储在本地队列中，用于向 Kaspersky Anti Targeted Attack Platform 服务器发送任务执行结果。发送后，数据将从临时存储中删除。

  - 文件的 MD5 和 SHA256 哈希值
  - 文件全名
  - 文件路径
  - 文件大小
  - 进程名称
  - 处理参数
  - 进程文件的路径
  - 进程的 Windows 标识符 (PID)
  - 父进程的 Windows 标识符 (PID)
  - 启动进程的用户账户
  - 进程开始的日期和时间
- IOC 扫描结果中的数据：
  - ARP 表中的 IP 地址
  - ARP 表中的物理地址
  - DNS 记录名称
  - DNS 记录类型
  - 主机名
  - IP 地址
  - 日志中的事件 ID
  - 日志中的数据源名称
  - 日志名称
  - 用户名

- 事件生成的日期和时间（ISO 格式）
- 文件的 MD5 和 SHA256 哈希值
- 文件全名
- 文件大小
- 扫描期间建立连接的远程 IP 地址和端口
- 本地适配器的 IP 地址和端口
- 协议
- 进程名称
- 处理参数
- 进程文件的路径
- 进程的 Windows 标识符 (PID)
- 父进程的 Windows 标识符 (PID)
- 启动进程的用户账户
- 进程开始的日期和时间
- 注册表项的路径
- 注册表项名称
- 注册表项的文本值
- 服务名称
- 服务说明
- DLL 服务的路径和名称
- 服务可执行文件的路径和名称
- 服务的 Windows 标识符 (PID)
- 服务类型
- 服务状态
- 服务启动模式
- 操作系统名称
- 操作系统版本
- 计算机网络名称（不含域名）

- 域或工作组
- 用户名
- 卷名
- 卷字母
- 卷类型

Kaspersky Network Detection and Response (KATA)

当卸载 Kaspersky Endpoint Security 时，应用程序本地存储在计算机上的所有数据将从计算机中删除。

遥测数据

- **文件数据**
  - 文件的唯一标识符
  - 文件类型
  - 完整文件路径
  - 文件大小
  - 文件属性
  - 区域标识符
  - 创建文件的日期和时间
  - 上次修改文件的日期和时间
  - 原始文件名
  - 应用程序名称
  - 应用程序版本
  - 应用程序供应商
  - 文件描述
  - 文件版本
  - 对象的 MD5 和 SHA256 哈希值
  - 文件签名验证结果

    - 创建文件签名的日期和时间
    - 签名文件中使用的证书链
    - 证书链类型
    - 链中的证书
    - 证书颁发机构名称
    - 证书持有人姓名
    - 证书序列号
    - 证书指纹算法
    - 证书指纹
    - 证书有效期
- **登录会话数据**
    - 登录会话 ID
    - 登录用户的账号名称
    - 用户账户类型
    - 会话类型
    - 发起登录尝试的机器的 IP 地址
    - 尝试登录的本地机器的 IP 地址
    - 表明此事件所代表的会话具有提升的特权和管理权限的标志
    - 指示其他会话是否与此登录会话关联的参数
    - 终端会话使用的协议
    - 终端会话使用的 IPv4 协议
- **网络通信数据**
    - 数据收集的时间间隔的开始和结束时间
    - 连接列表
    - 计算机的本地 IP 地址
    - 计算机的本地 MAC 地址
    - 计算机的远程 IP 地址
    - 计算机的远程 MAC 地址

    - 网关 IP 地址
    - 已传输数据包的数量
    - 已接收数据包的数量
    - 传输的总字节数
    - 数据传输协议
    - 以太网帧 EtherType 字段
    - 时间间隔内第一个数据包的有效载荷前缀
    - 捕获通信所用网络接口的 IPv4 地址
- **网络连接数据**
    - 发起连接的进程的唯一标识符
    - 数据传输协议
    - 用于发起连接的本地 IP 地址
    - 连接端点的远程 IP 地址
    - HTTP 方法
    - 不带主机名的路径
    - 主机名
    - 连接瞬间的动态过程状态
    - 连接方向
    - 动态过程状态
    - 以太网帧 EtherType 字段
- **在监听网络端口时捕获的数据**
    - 发起连接的进程的唯一标识符
    - 数据传输协议
    - 本地地址
    - 连接瞬间的动态过程状态
- **连接验证结果**
    - 主机网络设置
    - 网络接口描述

- DNS 域名
- 计算机的本地 MAC 地址
- IP 连接指标数
- IP 地址列表
- IP 地址
- 网络掩码
- 网关 IP 地址
- 网关 MAC 地址
- 已安装补丁列表
- 补丁编号
- 补丁安装日期
- 设备型号
- 设备供应商
- Kaspersky Security Center 中的主机 ID
- 已安装的卡巴斯基反病毒软件描述
- 已安装的卡巴斯基反病毒软件的组件名称
- 已安装的卡巴斯基反病毒软件的组件版本
- 已安装的卡巴斯基反病毒软件的组件的数据库版本
- 已安装的卡巴斯基反病毒软件的组件的上次数据库更新日期
- 已安装的卡巴斯基反病毒软件的组件状态
- 授权许可密钥列表
- 密钥序列号
- 密钥类型
- 密钥到期日期
- 密钥状态

- **主机上进程创建的相关数据**
  - 进程的唯一标识符
  - 父进程的唯一标识符

    - 进程的唯一系统标识符
    - 用于启动进程的命令
    - 登录会话 ID
    - 终端会话 ID
    - 进程文件的唯一标识符
    - 进程完整性水平
    - 进程权限令牌列表
    - 属性权限
    - 已解释文件的唯一标识符列表
    - 进程状态
    - 用于启动进程的命令
- **进程终止相关数据**
    - 进程的唯一标识符
- **有关检测到的威胁的数据**
    - 威胁信息
    - 威胁判定
    - AMR 记录编号
    - 反病毒数据库版本
    - 威胁检测模式
    - 威胁的唯一标识符
    - 保护技术
    - 受感染对象的信息
    - 受感染的对象类型
    - 受感染的对象名称
    - 对象的 MD5 和 SHA256 哈希值
    - 受感染进程的唯一标识符
    - 受感染对象的唯一标识符
    - 从互联网下载受感染对象的进程的唯一标识符

    - 下载受感染对象的 URL
    - 发送受感染对象的发件人电子邮件地址
    - 接收受感染对象的网络协议
    - 接收受感染对象的本地地址
    - 接收受感染对象的外部地址
    - 对象内容类型
    - 检测到的威胁的上下文
    - 对象内容
    - 表示威胁检测在后台运行的标志
- **关于威胁处理的数据**
    - 威胁信息
    - 威胁判定
    - AMR 记录编号
    - 反病毒数据库版本
    - 威胁检测模式
    - 受感染的对象名称
    - 对象的 MD5 和 SHA256 哈希值
    - 受感染进程的唯一标识符
    - 受感染对象的唯一标识符
    - 接收受感染对象的网络协议
    - 接收受感染对象的本地地址
    - 接收受感染对象的外部地址
    - 威胁处理状态
    - 威胁无法消除的原因
    - 本地物理地址
- **用户数据**
    - 用户 SID
    - 用户 ID

- 用户名
- 用户全名
- 用户描述
- 账户状态（活动或已阻止）
- 密码是否已过期
- 是否需要更改密码
- 是否允许更改密码
- 用户账户类型
- 此账户是否启用自动登录
- 用户所属的群组列表

与 Kaspersky Unified Monitoring and Analysis Platform (KUMA) 集成

当卸载 Kaspersky Endpoint Security 时，应用程序本地存储在计算机上的所有数据将从计算机中删除。

与 Kaspersky Unified Monitoring and Analysis Platform (KUMA) 集成时，连接设置数据以及 Windows 日志中注册的所有事件都会被传输。

主要的 Windows 事件日志包括 System、Security、Application、ForwardedEvents 和 HardwareEvents。用户还可以创建和使用自定义日志，以满足其特定需求。

与欧盟立法兼容(GDPR)

Kaspersky Endpoint Security 可能在以下情景下传输数据到 Kaspersky：

- 使用卡巴斯基安全网络。
- 用激活码激活应用程序。
- 更新应用程序模块和反病毒数据库。
- 遵从应用程序界面的链接。

无论数据分类和接收数据的地区如何，Kaspersky 都坚持高标准的数据安全，并采用各种法律、组织和技术措施来保护用户的数据，保证数据的安全性和保密性，并确保用户权利的实现适用法律。隐私策略的文本包含在应用程序分发工具并在 Kaspersky 网站上可用。

在使用 Kaspersky Endpoint Security 之前，请仔细阅读最终用户授权许可协议和卡巴斯基安全网络声明中传输数据的描述。如果根据当地法律或标准，Kaspersky Endpoint Security 在上述任何情景下传输的特定数据被归类为个人数据，则您必须确保这些数据是合法处理的，并在收集和传输此类数据时获得最终用户的同意。

请阅读最终用户授权许可协议并访问 Kaspersky 网站 了解当您接受《最终用户授权许可协议》和同意《卡巴斯基安全网络声明》之后我们如何接收、保存和销毁有关程序使用的信息。license.txt 和 ksn_<语言 ID>.txt 文件包含最终用户授权许可协议的文本，卡巴斯基安全网络声明包含在应用程序分发包中。

如果您不想传输数据到 Kaspersky，您可以禁用数据提供。

使用卡巴斯基安全网络

通过使用卡巴斯基安全网络，您同意自动提供卡巴斯基安全网络声明中列出的数据。如果您不同意将此数据提供给卡巴斯基，请使用私有卡巴斯基私有安全网络（KPSN）或禁用 KSN 的使用。有关 KPSN 的详细信息，请参阅卡巴斯基私有安全网络的文档。

用激活码激活应用程序

通过使用激活码，您同意自动提供最终用户授权许可协议中列出的数据。如果您不同意提供这些数据给 Kaspersky，请使用密钥文件来激活 Kaspersky Endpoint Security。

更新应用程序模块和反病毒数据库

通过使用 Kaspersky 服务器，您同意自动提供最终用户授权许可协议中列出的数据。Kaspersky 需要这些信息来验证 Kaspersky Endpoint Security 是否被合法使用。如果您不同意将此信息提供给 Kaspersky，请使用 Kaspersky Security Center 进行数据库更新或 Kaspersky 更新实用程序。

遵从应用程序界面的链接

通过使用应用程序界面中的链接，您同意自动提供最终用户授权许可协议中列出的数据。每个特定链接中传输的数据的精确列表取决于链接在应用程序接口中的位置以及它要解决的问题。如果您不同意将此数据提供给 Kaspersky，请使用简化的应用程序界面或隐藏应用程序界面。

转储写入

如果启用了转储写入，Kaspersky Endpoint Security 将创建一个转储文件，该文件将包含创建此转储文件时应用程序进程中的所有内存数据。

商标通知

注册商标和服务标志均为其各自拥有者的财产。

Adobe、Acrobat、Flash、Reader 和 Shockwave 是 Adobe 在美国和/或其他国家/地区的注册商标或商标。

Amazon、Amazon Web Services 和 AWS 是 Amazon.com, Inc. 或其附属公司的商标。

Apple、FireWire、iTunes、Mac 和 Safari 是苹果公司的商标。

Arm 是 Arm Limited（或其子公司）在美国和/或其他地区的注册商标。

AutoCAD 是 Autodesk, Inc. 和/或其子公司和/或附属公司在美国和/或其他国家/地区的商标或注册商标。

Bluetooth 文字、标志和徽标归 Bluetooth SIG, Inc. 所有。

Borland 是 Borland Software Corporation 的商标或注册商标。

Cisco、Cisco AnyConnect、IOS 是 Cisco Systems, Inc. 和/或其附属公司在美国和其他国家/地区的注册商标。

Citrix、Citrix Provisioning、Citrix Provisioning Services、Citrix Virtual Apps and Desktop、 XenDesktop 和 XenServer 是 Cloud Software Group, Inc. 和/或其子公司在美国和/或其他国家/地区的注册商标或商标。

Cloudflare、Cloudflare Workers 和 Cloudflare 徽标是 Cloudflare， Inc. 在美国和其他司法管辖区的商标和/或注册商标。

Core 是英特尔公司或其子公司的商标。

dBase 是 dataBased Intelligence, Inc. 的商标

Dell Technologies, Dell, EMC 和其他商标是 Dell Inc. 或其子公司的商标。

Docker 和 Docker 徽标是 Docker， Inc. 在美国和/或其他国家的商标或注册商标。Docker, Inc. 和其他各方也可能拥有此处使用的其他条款的商标权。

ESET 是 ESET spol. s r.o. 或相应的 ESET 实体的商标或注册商标。

Foxit 是 Foxit Corporation 的注册商标。

Radmin 是 Famatech 的注册商标。

Google、Android、Google Public DNS、Google Chrome 和 Chrome 是 Google LLC. 的商标。

HUAWEI、FusionCompute 和 FusionSphere 是 Huawei Technologies Co., Ltd. 的商标。

ICQ 是 ICQ LLC 的商标和/或服务标志。

Intel 是英特尔公司或其子公司的商标。

IBM 是 International Business Machines Corporation 在全球多个地区注册的商标。

Lenovo 和 Lenovo ThinkPad 是联想在美国和/或其它地区的商标。

Linux 是 Linus Torvalds 在美国和其他国家/地区的注册商标。

Logitech 是 Logitech 在美国和/或其他国家/地区的注册商标或商标。

LogMeIn Pro 和 Remotely Anywhere 是 LogMeIn, Inc. 的商标。

Mail.ru 是 Mail.ru LLC. 的商标。

McAfee 是 McAfee LLC 或其子公司在美国和/或其他国家的商标或注册商标。

Microsoft、Access、Active Directory、ActiveSync、Bing、BitLocker、Excel、Hyper-V、Internet Explorer、JScript、LifeCam Cinema、Microsoft Edge、MSDN、MS-DOS、MultiPoint、Office 365、Outlook、PowerPoint、PowerShell、Skype、SQL Server、Surface、Visual Basic、Visual FoxPro、Windows、Windows Live、Windows PowerShell、Windows Server 和 Windows Store 是 Microsoft 集团公司的商标。

Mozilla、Firefox 和 Thunderbird 是 Mozilla Foundation 在美国和其他国家的商标。

NetApp 是 NetApp, Inc. 在美国和/或其他国家/地区的商标或注册商标。

OpenSSL 是 OpenSSL 软件基金会拥有的商标。

OpenStack 是 OpenStack Foundation 在美国和其他国家/地区的注册商标。

Oracle、Java 和 JavaScript 是 Oracle 和/或其附属公司的注册商标。

Python 是 Python Software Foundation 的商标或注册商标。

Realtek 是 Realtek Semiconductor Corporation 的商标。

SAMSUNG 是 SAMSUNG 在美国或其他国家/地区的商标。

Thawte 是 Symantec Corporation 和/或其附属公司在美国和其他国家/地区的商标或注册商标。

Trend Micro 是 Trend Micro Incorporated 的商标或注册商标。

VERISIGN 是在美国和其他地区的注册商标，或 VeriSign, Inc. 和其附属公司的非注册商标。

VMware、VMware ESXi、VMware Horizon、VMware Workstation、VMware Tools、VMware vSphere 是 VMware, Inc. 在美国和其他国家/地区的商标和/或注册商标。

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中的 legal_notices.txt 文件中。